MT362/462/5462 Cipher Systems

Mark Wildon, mark.wildon@rhul.ac.uk

- **Sessions:**
  - Tuesday 1pm, **Plenary problem solving** (face-to-face) ARTS LT1,
  - Wednesday 12 noon, **Group work** (face-to-face), MFOX-SEM
  - Friday 10am, **Q&A session** (online)
  - Friday 3pm, **Group work** (online)

  Group work sessions **begin in Teaching Week 1**. Your timetable shows face-to-face and online sessions in alternate weeks.
- **Extra session for MT5462:** Tuesday 11 am (BOILER 0-07).
- **Office hour McCrea LGF025 and online:** Thursday 2pm
- **Quizzes on Moodle:** These are easy to medium difficulty questions intended to prepare you for each week's work. Submit the quiz for Week i by Monday evening on Week $i+1$.

  (Exceptionally the Week 1 quiz will be open until Monday of Teaching Week 3.)
- **Slides:** like these! I suggest you start with these slides, do the quizzes in them, and then use the online videos (which cover all the course) when you need extra explanation.

Part A: Introduction: alphabetic ciphers and the language of cryptography

§1 Introduction: Security and Kerckhoffs's Principle

- **Confidentiality**: Eve cannot read the message.
- **Data integrity**: any change made by Malcolm to the ciphertext is detectable
- **Authentication**: Alice and/or Bob are who they claim to be
- **Non-repudiation**: Alice cannot plausibly deny she sent the message

Part A: Introduction: alphabetic ciphers and the language of cryptography

§1 Introduction: Security and Kerckhoffs's Principle

- **Confidentiality**: Eve cannot read the message.
- **Data integrity**: any change made by Malcolm to the ciphertext is detectable
- **Authentication**: Alice and/or Bob are who they claim to be
- **Non-repudiation**: Alice cannot plausibly deny she sent the message

Quiz. True or false: When you log in to gmail, Google is sent your password (through an encrypted channel) and their computer checks it matches their record.

(A) False (B) True

Part A: Introduction: alphabetic ciphers and the language of cryptography

§1 Introduction: Security and Kerckhoffs's Principle

- **Confidentiality**: Eve cannot read the message.
- **Data integrity**: any change made by Malcolm to the ciphertext is detectable
- **Authentication**: Alice and/or Bob are who they claim to be
- **Non-repudiation**: Alice cannot plausibly deny she sent the message

Quiz. True or false: When you log in to gmail, Google is sent your password (through an encrypted channel) and their computer checks it matches their record.

(A) False (B) True

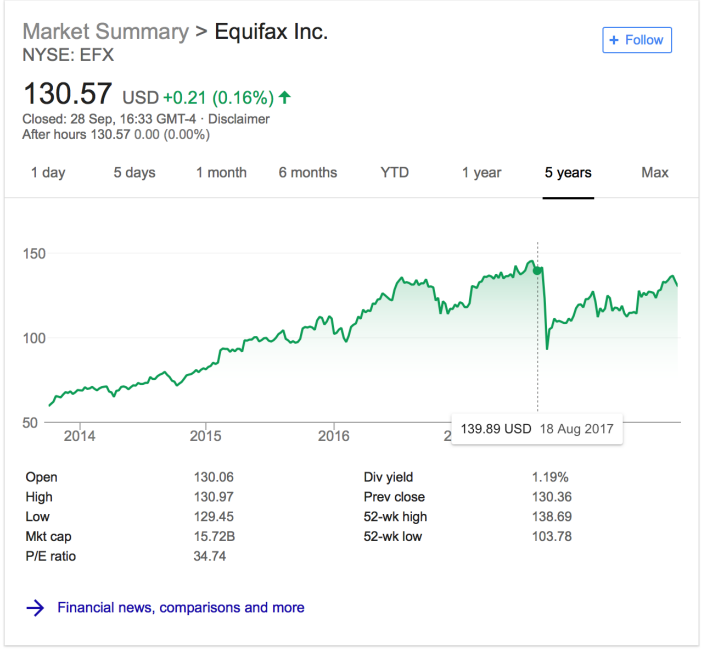
In fact they are sent a 'hash' of your password: see Part D of the course. For instance, the SHA-256 hash of the password used to encrypt this year's exam is

104198906329021394584564236198015074463863749517659335856292837022951400780 21.

Cryptography Matters!

What do the four below have in common?

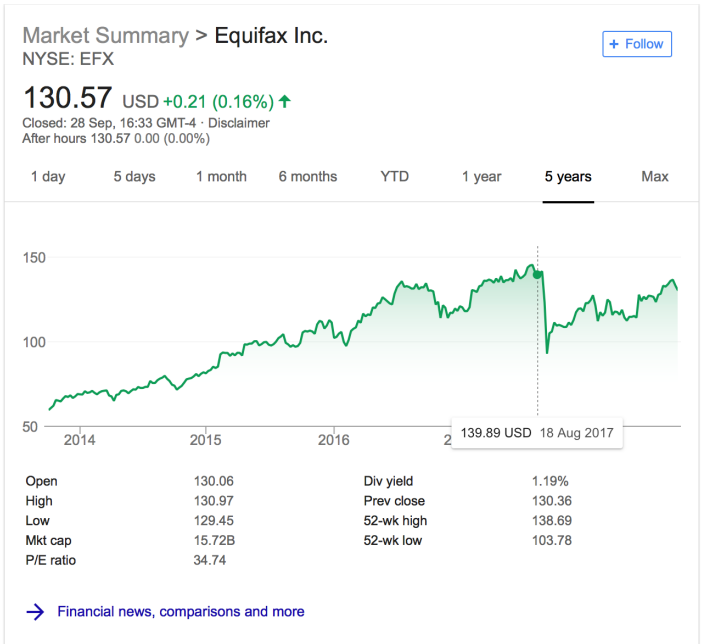
- Mary, Queen of Scots (1542–1587)
- Claus Fuchs (the Los Alamos traitor)
- The Equifax share price.
- Edward Snowden?



Cryptography Matters!

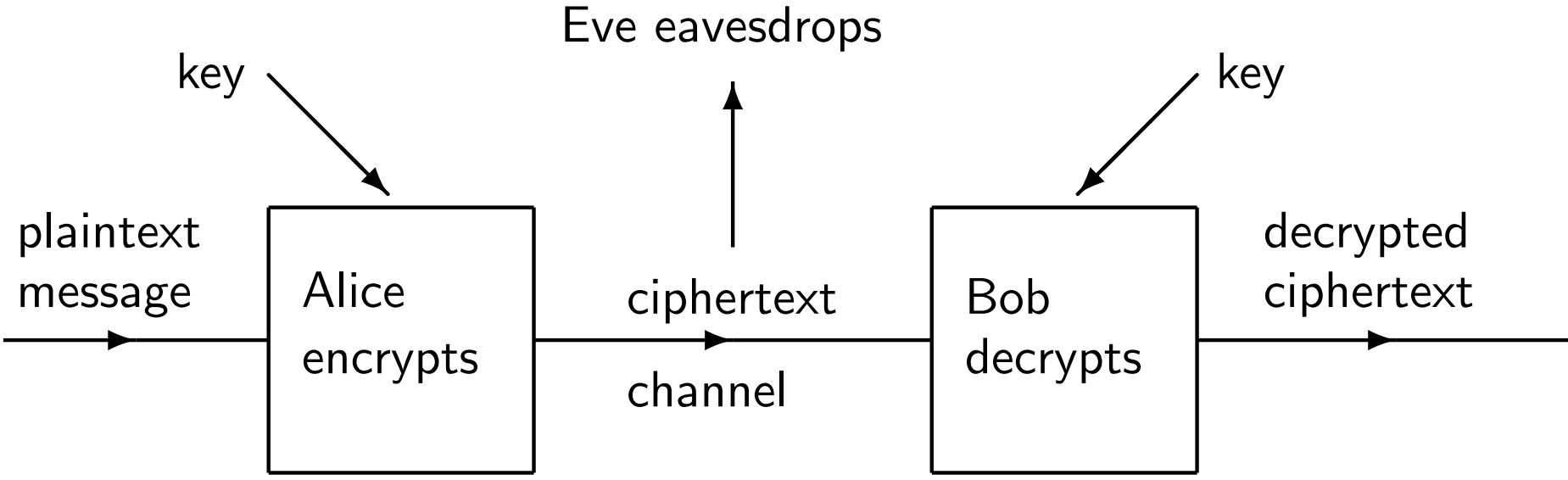
What do the four below have in common?

- Mary, Queen of Scots (1542–1587)
- Claus Fuchs (the Los Alamos traitor)
- The Equifax share price.
- Edward Snowden?



Answer: Their lives (or value) were all changed forever because of cryptographic leaks. Mary, Queen of Scots was executed after her substitution cipher was cracked, Fuchs was imprisoned after reusing a one-time pad, the Equifax share price halved after a server hack. Snowden chose to leak classified information and is exiled in Russia.

The Basic Picture and Kerckhoffs's Principle



Kerckhoffs's Principle is '**all the security is in the key**'. All other details of how the encryption works, the functions used, and how data is sent, are public.

- If this surprises you, consider that the encryption algorithm might be leaked. It is then known forever. A key can be replaced and might only be used once anyway.
- Also what do you trust more: a public encryption algorithm (using secret keys) that has withstood years of public scrutiny, or a secret algorithm that ACME Cryptography assures you is unbeatable?

Alice and Bob's Exam Mark

Example 1.2

On Friday, Alice will learn Bob's final year exam result x while Bob is out of the country. Alice, Bob and their trusted friend Trevor agree this method.

- On Monday, Trevor chooses a key $k \in \{0, 1, \ldots, 99\}$. He meets Alice and secretly tells her k. He meets Bob and secretly tells him k.
- On Tuesday, Bob leaves for Borneo. He can read email. Bob cannot send email or communicate in any other way.
- On Friday, Alice learns the plaintext $x \in \{0, 1, \ldots, 99\}$ and emails Bob the ciphertext $(x + k) \bmod 100$.

By Kerckhoffs's Principle, all this, except for the value of k, is known to the whole world. Eve, the eavesdropper, also learns y, the ciphertext sent by Alice to Bob.

Exercise on Alice and Bob's Exam Mark

In the example we supposed that the ciphertext y sent by Alice to Bob was 20 and that **all keys were equally likely**.

(a) Can Eve learn anything about the plaintext x from the ciphertext y?

(b) Suppose Eve is sure Bob's mark is between 50 and 80. What can Eve learn about the key from Alice's email?

(c) Find some other problems in the scheme.

§2 Alphabetic Ciphers

Example 2.1

The *Caesar cipher* with key $k \in \{0, 1, \ldots, 25\}$ encrypts a word by shifting each letter k positions forward in the alphabet, wrapping round at the end. For example if the key is 3 then '`hello`' becomes `KHOOR` and '`zany`' becomes `CDQB`. The table in the printed notes shows all 26 possible shifts.

Quiz on Caesar Cipher

Assume the plaintext is a common English word.

Exercise 2.2

(a) Mark (the mole) knows that the plaintext 'apple' was encrypted as `CRRNG`. What is the key?

(A) 0 (B) 1 (C) 2 (D) 3

(b) Eve (the eavesdropper) has observed the ciphertext `ACCB`. What is the key?

(A) 11 (B) 12 (C) 13 (D) 14

What is the plaintext?

(c) Suppose instead Eve observes `GVTJPO`. What can she deduce about k?

(A) $k = 1$ (B) $k = 25$ (C) $k = 21$ (D) $k \in \{1, 21\}$

Suppose Eve later observes `BUPN`. Assuming the same key k is used, what does she conclude about k?

(A) $k = 1$ (B) $k = 25$ (C) $k = 21$ (D) $k \in \{1, 21\}$

Quiz on Caesar Cipher

Assume the plaintext is a common English word.

Exercise 2.2

(a) Mark (the mole) knows that the plaintext 'apple' was encrypted as `CRRNG`. What is the key?

(A) 0 (B) 1 (C) 2 (D) 3

(b) Eve (the eavesdropper) has observed the ciphertext `ACCB`. What is the key?

(A) 11 (B) 12 (C) 13 (D) 14

What is the plaintext?

(c) Suppose instead Eve observes `GVTJPO`. What can she deduce about k?

(A) $k = 1$ (B) $k = 25$ (C) $k = 21$ (D) $k \in \{1, 21\}$

Suppose Eve later observes `BUPN`. Assuming the same key k is used, what does she conclude about k?

(A) $k = 1$ (B) $k = 25$ (C) $k = 21$ (D) $k \in \{1, 21\}$

Quiz on Caesar Cipher

Assume the plaintext is a common English word.

Exercise 2.2

(a) Mark (the mole) knows that the plaintext 'apple' was encrypted as `CRRNG`. What is the key?

(A) 0 (B) 1 (C) 2 (D) 3

(b) Eve (the eavesdropper) has observed the ciphertext `ACCB`. What is the key?

(A) 11 (B) 12 (C) 13 (D) 14

What is the plaintext?

(c) Suppose instead Eve observes `GVTJPO`. What can she deduce about k?

(A) $k = 1$ (B) $k = 25$ (C) $k = 21$ (D) $k \in \{1, 21\}$

Suppose Eve later observes `BUPN`. Assuming the same key k is used, what does she conclude about k?

(A) $k = 1$ (B) $k = 25$ (C) $k = 21$ (D) $k \in \{1, 21\}$

Quiz on Caesar Cipher

Assume the plaintext is a common English word.

Exercise 2.2

(a) Mark (the mole) knows that the plaintext 'apple' was encrypted as `CRRNG`. What is the key?

(A) 0 (B) 1 (C) 2 (D) 3

(b) Eve (the eavesdropper) has observed the ciphertext `ACCB`. What is the key?

(A) 11 (B) 12 (C) 13 (D) 14

What is the plaintext?

(c) Suppose instead Eve observes `GVTJPO`. What can she deduce about k?

(A) $k = 1$ (B) $k = 25$ (C) $k = 21$ (D) $k \in \{1, 21\}$

Suppose Eve later observes `BUPN`. Assuming the same key k is used, what does she conclude about k?

(A) $k = 1$ (B) $k = 25$ (C) $k = 21$ (D) $k \in \{1, 21\}$

Quiz on Caesar Cipher

Assume the plaintext is a common English word.

Exercise 2.2

(a) Mark (the mole) knows that the plaintext 'apple' was encrypted as `CRRNG`. What is the key?

(A) 0 (B) 1 (C) 2 (D) 3

(b) Eve (the eavesdropper) has observed the ciphertext `ACCB`. What is the key?

(A) 11 (B) 12 (C) 13 (D) 14

What is the plaintext?

(c) Suppose instead Eve observes `GVTJPO`. What can she deduce about k?

(A) $k = 1$ (B) $k = 25$ (C) $k = 21$ (D) $k \in \{1, 21\}$

Suppose Eve later observes `BUPN`. Assuming the same key k is used, what does she conclude about k?

(A) $k = 1$ (B) $k = 25$ (C) $k = 21$ (D) $k \in \{1, 21\}$

Substitution Ciphers (next slide has still from videos)

Example 2.3

Let $\pi : \{\mathtt{a}, \ldots, \mathtt{z}\} \to \{\mathtt{A}, \ldots, \mathtt{Z}\}$ be a bijection. The *substitution cipher* e_π applies π to each letter of a plaintext in turn. For example, if

$$\pi(\mathtt{a}) = \mathtt{Z}, \pi(\mathtt{b}) = \mathtt{Y}, \ldots, \pi(\mathtt{z}) = \mathrm{A}$$

then $e_\pi(\texttt{hello there}) = \texttt{SVOOL GSVIV}$. (In practice spaces were deleted before encryption, but we will keep them to simplify the cryptanalysis.) The Caesar cipher with key k is the special case where π shifts each letter forward k times.

Quiz: How many substitution ciphers are there?

(A) 26 (B) 26^2 (C) 26! (D) 26^{26}

Substitution Ciphers (next slide has still from videos)

Example 2.3

Let $\pi : \{\mathtt{a}, \ldots, \mathtt{z}\} \to \{\mathtt{A}, \ldots, \mathtt{Z}\}$ be a bijection. The *substitution cipher* e_π applies π to each letter of a plaintext in turn. For example, if

$$\pi(\mathtt{a}) = \mathtt{Z}, \pi(\mathtt{b}) = \mathtt{Y}, \ldots, \pi(\mathtt{z}) = \mathrm{A}$$

then $e_\pi(\texttt{hello there}) = \texttt{SVOOL GSVIV}$. (In practice spaces were deleted before encryption, but we will keep them to simplify the cryptanalysis.) The Caesar cipher with key k is the special case where π shifts each letter forward k times.

Quiz: How many substitution ciphers are there?

(A) 26 (B) 26^2 (C) 26! (D) 26^{26}

Is it feasible to find the key by trying all possibilities?

(A) No (B) Yes

$$26! = 403291461126605635584000000 \approx 4.032 \times 10^{26} \approx 2^{88.38}$$

Substitution Ciphers (next slide has still from videos)

Example 2.3

Let $\pi : \{\mathtt{a}, \ldots, \mathtt{z}\} \to \{\mathtt{A}, \ldots, \mathtt{Z}\}$ be a bijection. The *substitution cipher* e_π applies π to each letter of a plaintext in turn. For example, if

$$\pi(\mathtt{a}) = \mathtt{Z}, \pi(\mathtt{b}) = \mathtt{Y}, \ldots, \pi(\mathtt{z}) = \mathrm{A}$$

then $e_\pi(\texttt{hello there}) = \texttt{SVOOL GSVIV}$. (In practice spaces were deleted before encryption, but we will keep them to simplify the cryptanalysis.) The Caesar cipher with key k is the special case where π shifts each letter forward k times.

Quiz: How many substitution ciphers are there?

(A) 26 (B) 26^2 (C) 26! (D) 26^{26}

Is it feasible to find the key by trying all possibilities?

(A) No (B) Yes

$$26! = 403291461126605635584000000 \approx 4.032 \times 10^{26} \approx 2^{88.38}$$

Substitution Ciphers (next slide has still from videos)

Example 2.3

Let $\pi : \{\mathtt{a}, \ldots, \mathtt{z}\} \to \{\mathtt{A}, \ldots, \mathtt{Z}\}$ be a bijection. The *substitution cipher* e_π applies π to each letter of a plaintext in turn. For example, if

$$\pi(\mathtt{a}) = \mathtt{Z}, \pi(\mathtt{b}) = \mathtt{Y}, \ldots, \pi(\mathtt{z}) = \mathrm{A}$$

then $e_\pi(\texttt{hello there}) = \texttt{SVOOL GSVIV}$. (In practice spaces were deleted before encryption, but we will keep them to simplify the cryptanalysis.) The Caesar cipher with key k is the special case where π shifts each letter forward k times.

Quiz: How many substitution ciphers are there?

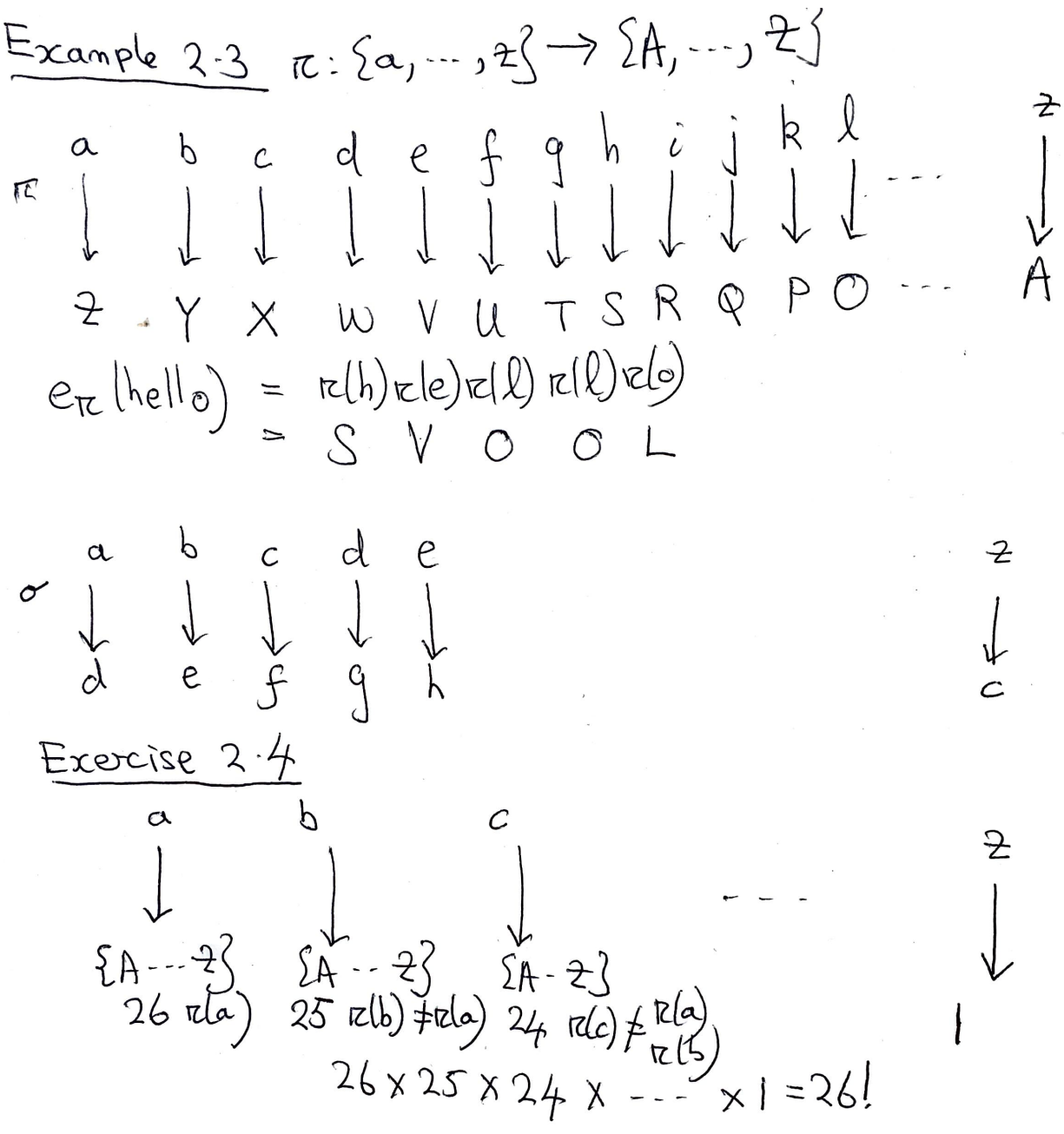
(A) 26 (B) 26^2 (C) 26! (D) 26^{26}

Is it feasible to find the key by trying all possibilities?

(A) No (B) Yes

$$26! = 403291461126605635584000000 \approx 4.032 \times 10^{26} \approx 2^{88.38}$$

Diagram Drawn in Video for Example 2.3 and Exercise 2.4

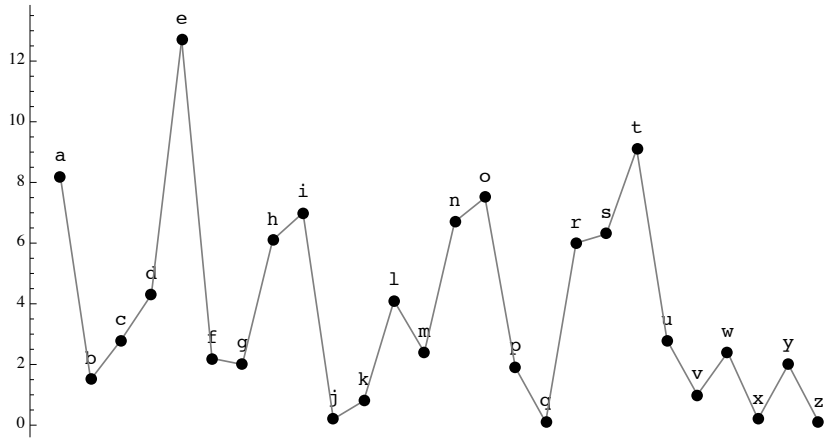


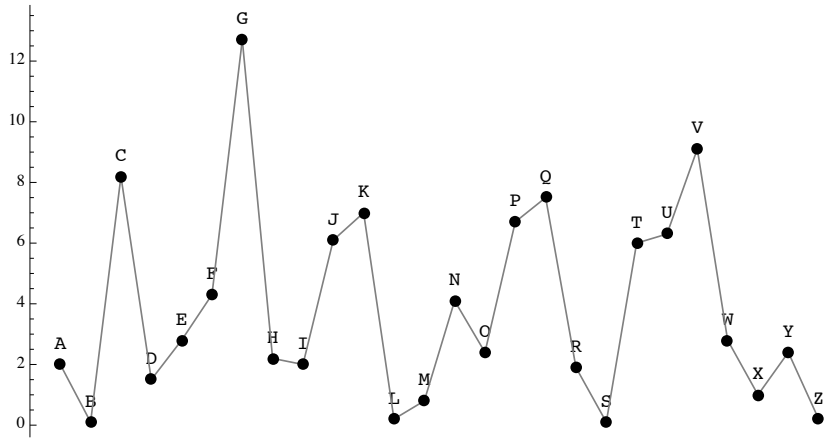
Frequency Analysis

The table below shows the frequency distribution of typical English, most frequent letters first. Probabilities are given as percentages.

e	t	a	o	i	n	s	h	r	d
12.7	9.1	8.2	7.5	7.0	6.7	6.3	6.1	6.0	4.3

All frequencies are shown in the graph left below.





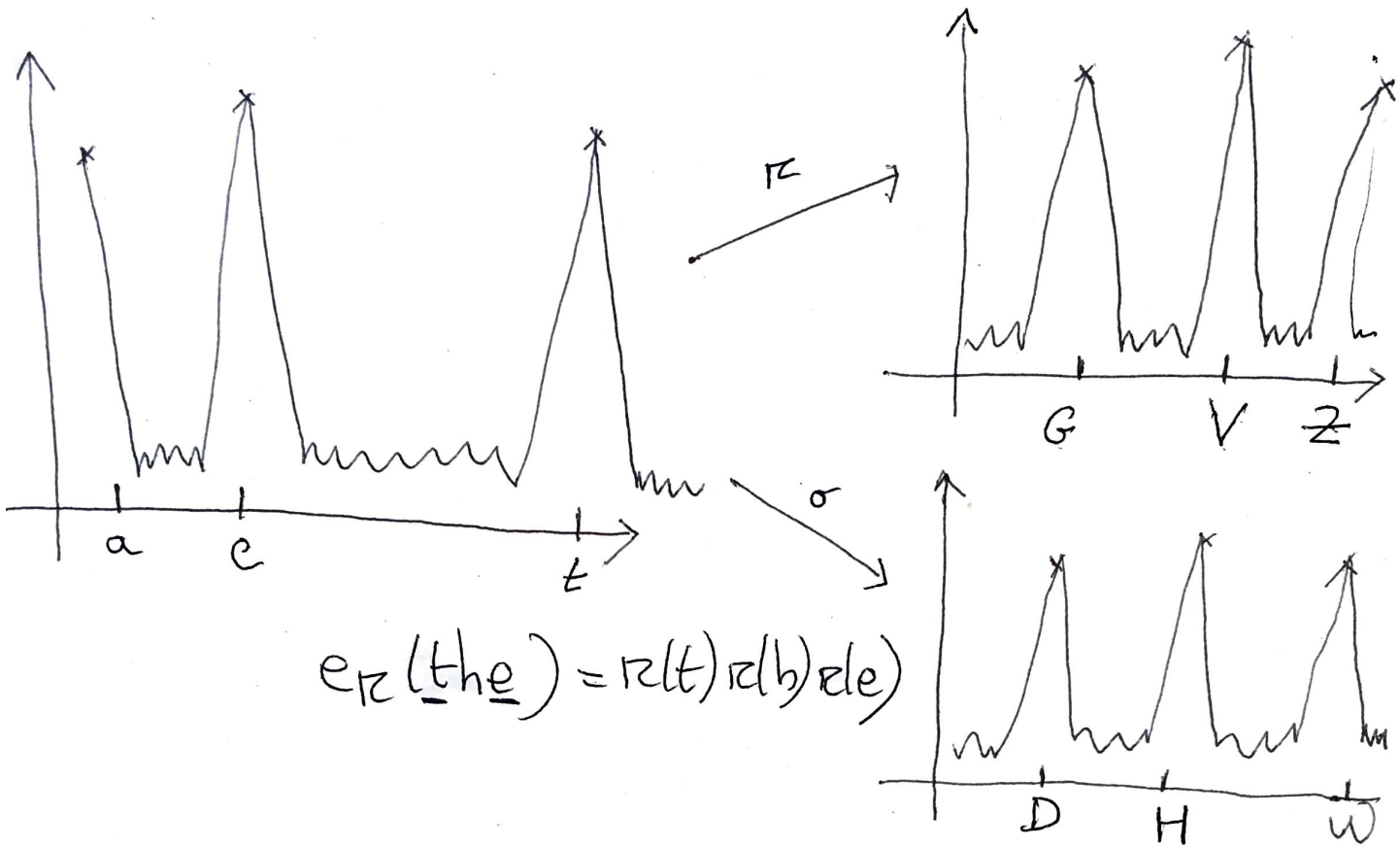
Using a substitution cipher, the probability distribution of ciphertext letters is a rearrangement of the probability distribution of plaintext letters. In particular, there are still three peaks, corresponding to e, t, and a. The graph on the right shows the special case where π is the Caesar shift by 2.

Frequency Analysis: Frequency Graph in Video

In the video we pretended that English had three common letters, a, e, t and all the rest were rare. I drew the graphs below showing how the frequency distribution is changed by

- the Caesar shift by 3 (special case of a substitution cipher)
- the substitution cipher reversing the alphabet

Note that there are still three peaks, just in different positions.



Frequency Analysis

Example′ 2.5

(Here ′ means this is similar, but not the same, as the example in the printed notes.) Eve intercepts the ciphertext

```
IFJAJ DAJ BNXKBWM UADLIKLDE AJDMBTM PBA MIWOCKTQ
LACUIBQADUFC IFJ MWNRJLI KM DEMB PWEE BP HDIFJHDIKLDE
KTIJAJMI IFJAJ DAJ LBTTJLIKBTM IB EKTJDA DEQJNAD TWHNJA
IFJBAC MIDIKMIKLM DTO UABNDNKEKIC IFJBAC DM GJEE DM
IFJBAJIKLDE LBHUWIJA MLKJTLJ
```

We will decrypt this using the MATHEMATICA notebook `AlphabetCiphers` on Moodle to do the donkey work.

Frequency Analysis

Example′ 2.5

(Here ′ means this is similar, but not the same, as the example in the printed notes.) Eve intercepts the ciphertext

```
IFJAJ DAJ BNXKBWM UADLIKLDE AJDMBTM PBA MIWOCKTQ
LACUIBQADUFC IFJ MWNRJLI KM DEMB PWEE BP HDIFJHDIKLDE
KTIJAJMI IFJAJ DAJ LBTTJLIKBTM IB EKTJDA DEQJNAD TWHNJA
IFJBAC MIDIKMIKLM DTO UABNDNKEKIC IFJBAC DM GJEE DM
IFJBAJIKLDE LBHUWIJA MLKJTLJ
```

We will decrypt this using the MATHEMATICA notebook `AlphabetCiphers` on Moodle to do the donkey work.

Frequency distribution of English and of the ciphertext.

e	t	a	o	i	n	s	h	r	d
12.7	9.1	8.2	7.5	7.0	6.7	6.3	6.1	6.0	4.3

J	I	D	A	M	B	K	L	E	T
11.2	10.7	9.2	8.8	7.3	7.3	6.8	5.8	5.3	4.9

Frequency analysis and then easy guessing quickly revealed the plaintext in Example 2.5′.

```
there are obvious practical reasons for studying cryptography
IFJAJ DAJ BNXKBWM UADLIKLDE AJDMBTM PBA MIWOCKTQ LACUIBQADUFC
the subject is also full of mathematical interest there are
IFJ MWNRJLI KM DEMB PWEE BP HDIFJHDIKLDE KTIJAJMI IFJAJ DAJ
connections to linear algebra number theory statistics and
LBTTJLIKBTM IB EKTJDA DEQJNAD TWHNJA IFJBAC MIDIKMIKLM DTO
probability theory as well as theoretical computer science
UABNDNKEKIC IFJBAC DM GJEE DM IFJBAJIKLDE LBHUWIJA MLKJTLJ
```

Exercise′ 2.6

(a) After deciphering, we know that $\pi(a) = D$, $\pi(b) = N$, . . . , $\pi(e) = J$, . . . and so on. Do we know the key π?

(A) No (B) Yes

J	I	D	A	M	B	K	L	E	T	F	W	N
11.2	10.7	9.2	8.8	7.3	7.3	6.8	5.8	5.3	4.9	3.9	3.0	3.0
C	U	H	Q	P	O	X	R	G	Z	Y	V	S
3.0	2.4	2.0	1.5	1.5	1.0	0.5	0.5	0.5	0	0	0	0

Frequency analysis and then easy guessing quickly revealed the plaintext in Example 2.5′.

```
there are obvious practical reasons for studying cryptography
IFJAJ DAJ BNXKBWM UADLIKLDE AJDMBTM PBA MIWOCKTQ LACUIBQADUFC
the subject is also full of mathematical interest there are
IFJ MWNRJLI KM DEMB PWEE BP HDIFJHDIKLDE KTIJAJMI IFJAJ DAJ
connections to linear algebra number theory statistics and
LBTTJLIKBTM IB EKTJDA DEQJNAD TWHNJA IFJBAC MIDIKMIKLM DTO
probability theory as well as theoretical computer science
UABNDNKEKIC IFJBAC DM GJEE DM IFJBAJIKLDE LBHUWIJA MLKJTLJ
```

Exercise′ 2.6

(a) After deciphering, we know that $\pi(a) = D$, $\pi(b) = N$, . . . , $\pi(e) = J$, . . . and so on. Do we know the key π?

(A) No (B) Yes

J	I	D	A	M	B	K	L	E	T	F	W	N
11.2	10.7	9.2	8.8	7.3	7.3	6.8	5.8	5.3	4.9	3.9	3.0	3.0
C	U	H	Q	P	O	X	R	G	Z	Y	V	S
3.0	2.4	2.0	1.5	1.5	1.0	0.5	0.5	0.5	0	0	0	0

Frequency analysis and then easy guessing quickly revealed the plaintext in Example 2.5′.

Exercise′ 2.6

(a) After deciphering, we know that $\pi(a) = D$, $\pi(b) = N$, . . . , $\pi(e) = J$, . . . and so on. Do we know the key π?

(A) No (B) Yes

(b) Will we have any difficulty in decrypting further messages encrypted using the same substitution cipher?

(A) No (B) Yes

(c) How many keys are possible, given our decrypted cipher text?

(A) 1 (B) 4 (C) 16 (D) 24

J	I	D	A	M	B	K	L	E	T	F	W	N
11.2	10.7	9.2	8.8	7.3	7.3	6.8	5.8	5.3	4.9	3.9	3.0	3.0
C	U	H	Q	P	O	X	R	G	Z	Y	V	S
3.0	2.4	2.0	1.5	1.5	1.0	0.5	0.5	0.5	0	0	0	0

Frequency analysis and then easy guessing quickly revealed the plaintext in Example 2.5′.

Exercise′ 2.6

(a) After deciphering, we know that $\pi(a) = D$, $\pi(b) = N$, ..., $\pi(e) = J$, ... and so on. Do we know the key π?

(A) No (B) Yes

(b) Will we have any difficulty in decrypting further messages encrypted using the same substitution cipher?

(A) No (B) Yes

(c) How many keys are possible, given our decrypted cipher text?

(A) 1 (B) 4 (C) 16 (D) 24

J	I	D	A	M	B	K	L	E	T	F	W	N
11.2	10.7	9.2	8.8	7.3	7.3	6.8	5.8	5.3	4.9	3.9	3.0	3.0
C	U	H	Q	P	O	X	R	G	Z	Y	V	S
3.0	2.4	2.0	1.5	1.5	1.0	0.5	0.5	0.5	0	0	0	0

Frequency analysis and then easy guessing quickly revealed the plaintext in Example 2.5′.

Exercise′ 2.6

(a) After deciphering, we know that $\pi(a) = D$, $\pi(b) = N$, ..., $\pi(e) = J$, ... and so on. Do we know the key π?

(A) No (B) Yes

(b) Will we have any difficulty in decrypting further messages encrypted using the same substitution cipher?

(A) No (B) Yes

(c) How many keys are possible, given our decrypted cipher text?

(A) 1 (B) 4 (C) 16 (D) 24

J	I	D	A	M	B	K	L	E	T	F	W	N
11.2	10.7	9.2	8.8	7.3	7.3	6.8	5.8	5.3	4.9	3.9	3.0	3.0
C	U	H	Q	P	O	X	R	G	Z	Y	V	S
3.0	2.4	2.0	1.5	1.5	1.0	0.5	0.5	0.5	0	0	0	0

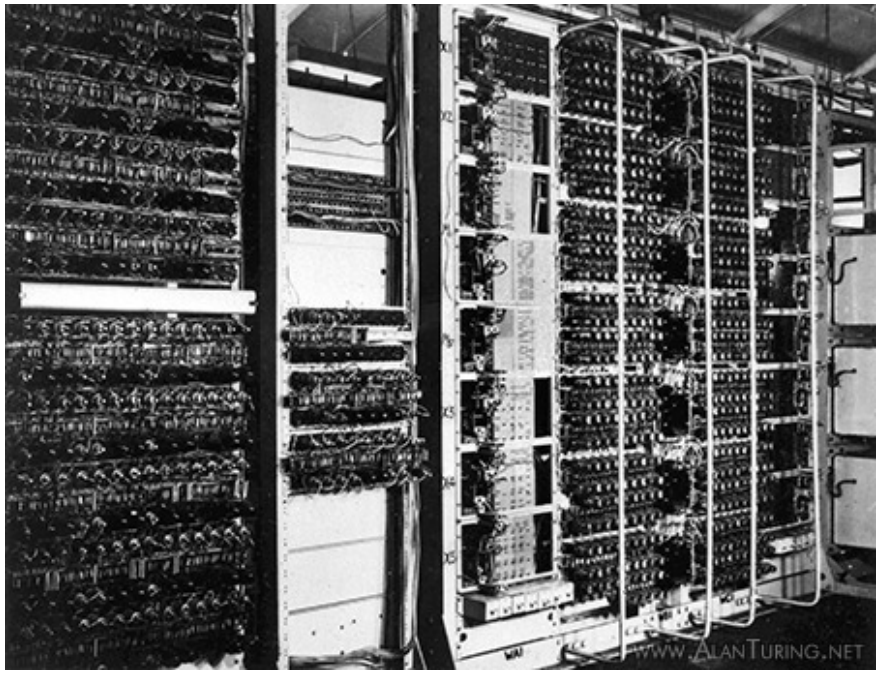
In Praise of Programming

You can get MATHEMATICA for free from the College: see the top hit for Google on 'RHUL Mathematica'.

This is a chance to develop some useful transferable programming skills!

> "What I mean is that if you really want to understand something, the best way is to try and explain it to someone else. That forces you to sort it out in your own mind. And the more slow and dim-witted your pupil, the more you have to break things down into more and more simple ideas. And that's really the essence of programming. By the time you've sorted out a complicated idea into little steps that even a stupid machine can deal with, you've certainly learned something about it yourself."
>
> Douglas Adams, *Dirk Gently's Holistic Detective Agency* (1987)

Colossus at Bletchley Park and Cyber Attacks Now



Russia accused of cyber-attack on chemical weapons watchdog

Netherlands expelled four GRU officers after alleged attacks on OPCW and UK Foreign Office

▲ Four men believed to be in a military intelligence 'cleanup' unit pictured at Schiphol airport. Photograph: Netherlands defence ministry

A Russian cyber-attack on the headquarters of the international chemical weapons watchdog was disrupted by Dutch military intelligence weeks after the Salisbury novichok attack, the Netherlands defence minister has said.

The incident, which was thwarted with the help of British officials, came after the Sandworm cybercrime unit of the Russian military intelligence agency GRU attempted unsuccessful spear phishing attacks on the UK Foreign Office in March and the Porton Down chemical weapons facility in April.

Four Russian intelligence officers, believed to have been part of a GRU "cleanup" unit for earlier failed operations, travelled to The Hague on diplomatic passports in April after unsuccessfully launching a remote attack.

The Guardian
4th October 2018

Hill Climbing

We saw that the substitution cipher is weak because it is possible to start with a guess for the key, say π, that is partially correct, and then improve it step-by-step by looking at the decrypted ciphertext $e_\pi^{-1}(y)$ implied by this key.

Example 2.7

To make this process automatic, we need a quantitative way to measure how 'close to English' $e_\pi^{-1}(y)$ is. Recall that a *trigram* is three consecutive letters. A good scoring function is $\sum_t \log p_t$ where the sum is over all trigrams t in $e_\pi^{-1}(y)$ and p_t is the probability of the trigram t in English ...

[See printed notes and the two videos: the picture I drew in the second didn't come through very well on the camera: there is a sharper scan as the next slide.]

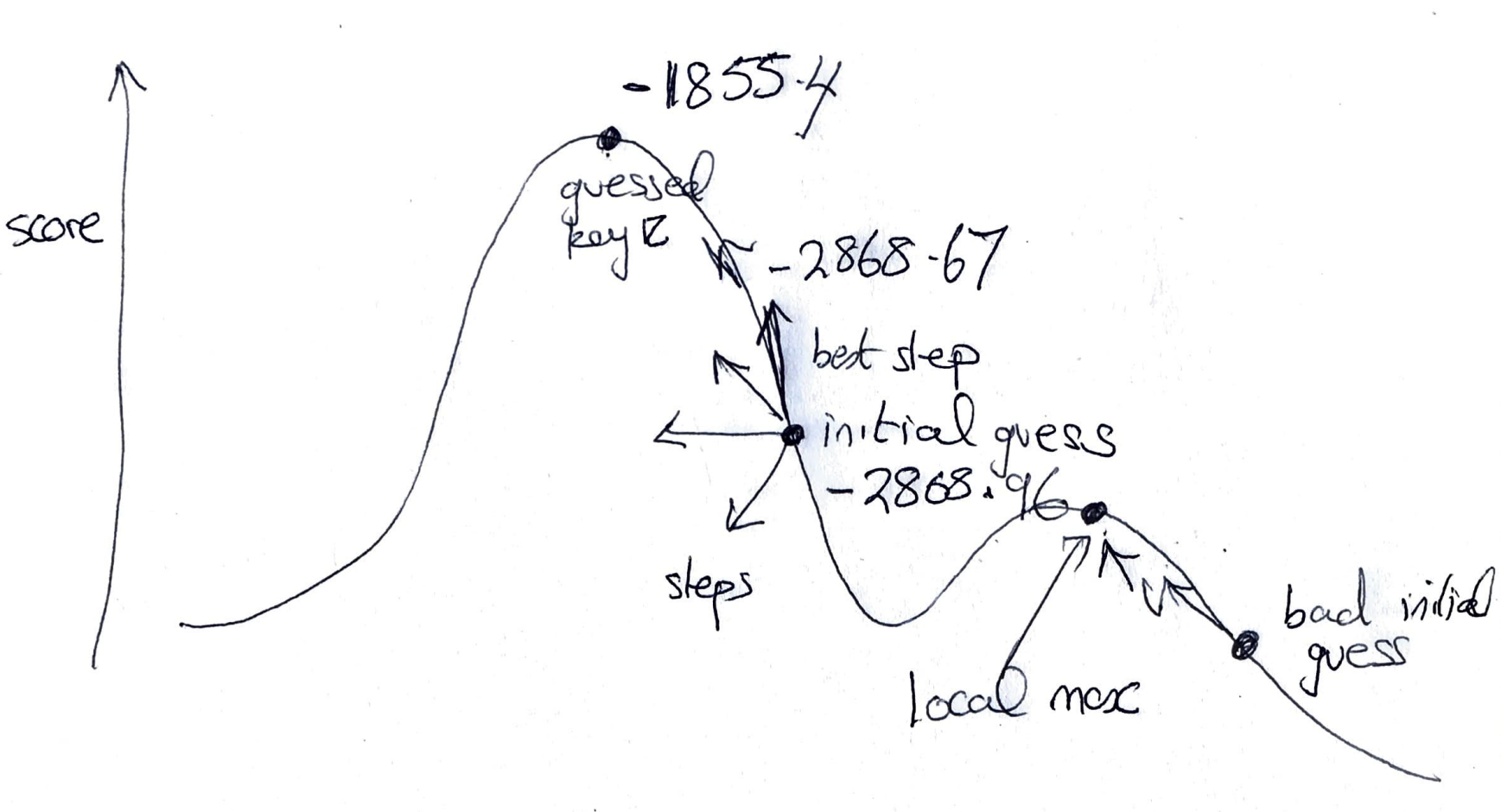
You can try the code online at

`http://repl.it/@mwildon/SubstitutionHillClimbWeb`.

Exercise 2.8

The strategy in Example 2.7 is called 'hill-climbing'. Why this name?

Answer: See the second video on the hill climb where I drew the picture below: scores are from decrypting the ciphertext in Example 2.5.



Vigenère Cipher

Define a bijection between the alphabet and $\{0, 1, \ldots, 25\}$ by

$$a \longleftrightarrow 0, b \longleftrightarrow 1, \ldots, z \longleftrightarrow 25.$$

Using this bijection we identify a word of length ℓ with an element of $\{0, 1, \ldots, 25\}^\ell$. For example,

$$\text{`}\texttt{hello}' \longleftrightarrow (7, 4, 11, 11, 14) \in \{0, 1, \ldots, 25\}^5.$$

After converting letters to numbers, the Caesar cipher with shift s becomes the function $x \mapsto x + s \bmod 26$.

Vigenère Cipher

Define a bijection between the alphabet and $\{0, 1, \ldots, 25\}$ by

$$a \longleftrightarrow 0, b \longleftrightarrow 1, \ldots, z \longleftrightarrow 25.$$

Using this bijection we identify a word of length ℓ with an element of $\{0, 1, \ldots, 25\}^\ell$. For example,

$$\text{`}\texttt{hello}' \longleftrightarrow (7, 4, 11, 11, 14) \in \{0, 1, \ldots, 25\}^5.$$

After converting letters to numbers, the Caesar cipher with shift s becomes the function $x \mapsto x + s \bmod 26$.

Quiz. In this course it is most convenient to number positions in tuples from 0, so a 3-tuple x is (x_0, x_1, x_2).

One of these statement is false. Which one?

(A) $\{1, 2, 2\} = \{2, 1, 1\}$ is a set of size 2,
(B) $(0, 1, 1, 0, 0, 1) \in \{0, 1\}^6$ is a binary form of $16 + 8 + 1 = 25$,
(C) $(1, 2, 2) = (2, 1, 1)$,
(D) If $u = (0, 1, 2, \ldots, 25)$ then $u_i = i$ for $i \in \{0, 1, \ldots, 25\}$.

(A) (B) (C) (D)

Vigenère Cipher

Define a bijection between the alphabet and $\{0, 1, \ldots, 25\}$ by

$$a \longleftrightarrow 0, b \longleftrightarrow 1, \ldots, z \longleftrightarrow 25.$$

Using this bijection we identify a word of length ℓ with an element of $\{0, 1, \ldots, 25\}^\ell$. For example,

$$\text{`}\texttt{hello}' \longleftrightarrow (7, 4, 11, 11, 14) \in \{0, 1, \ldots, 25\}^5.$$

After converting letters to numbers, the Caesar cipher with shift s becomes the function $x \mapsto x + s \bmod 26$.

Quiz. In this course it is most convenient to number positions in tuples from 0, so a 3-tuple x is (x_0, x_1, x_2).

One of these statement is false. Which one?

(A) $\{1, 2, 2\} = \{2, 1, 1\}$ is a set of size 2,
(B) $(0, 1, 1, 0, 0, 1) \in \{0, 1\}^6$ is a binary form of $16 + 8 + 1 = 25$,
(C) $(1, 2, 2) = (2, 1, 1)$,
(D) If $u = (0, 1, 2, \ldots, 25)$ then $u_i = i$ for $i \in \{0, 1, \ldots, 25\}$.

(A) (B) (C) (D)

Vigenère Cipher

Define a bijection between the alphabet and $\{0, 1, \ldots, 25\}$ by

$$a \longleftrightarrow 0, b \longleftrightarrow 1, \ldots, z \longleftrightarrow 25.$$

Using this bijection we identify a word of length ℓ with an element of $\{0, 1, \ldots, 25\}^\ell$. For example,

$$\text{`}\texttt{hello}' \longleftrightarrow (7, 4, 11, 11, 14) \in \{0, 1, \ldots, 25\}^5.$$

After converting letters to numbers, the Caesar cipher with shift s becomes the function $x \mapsto x + s \bmod 26$.

Definition 2.9

The key k for the *Vigenère cipher* is a string. Suppose that k has length ℓ. Given a plaintext x with its spaces deleted, we define its encryption by

$$e_k(x) = (x_0 + k_0, x_1 + k_1, \ldots, x_{\ell-1} + k_{\ell-1}, x_\ell + k_0, x_{\ell+1} + k_1, \ldots)$$

where $x_i + k_i$ is computed by converting x_i and k_i to numbers and adding them mod 26.

Vigenère Example

Example 2.10

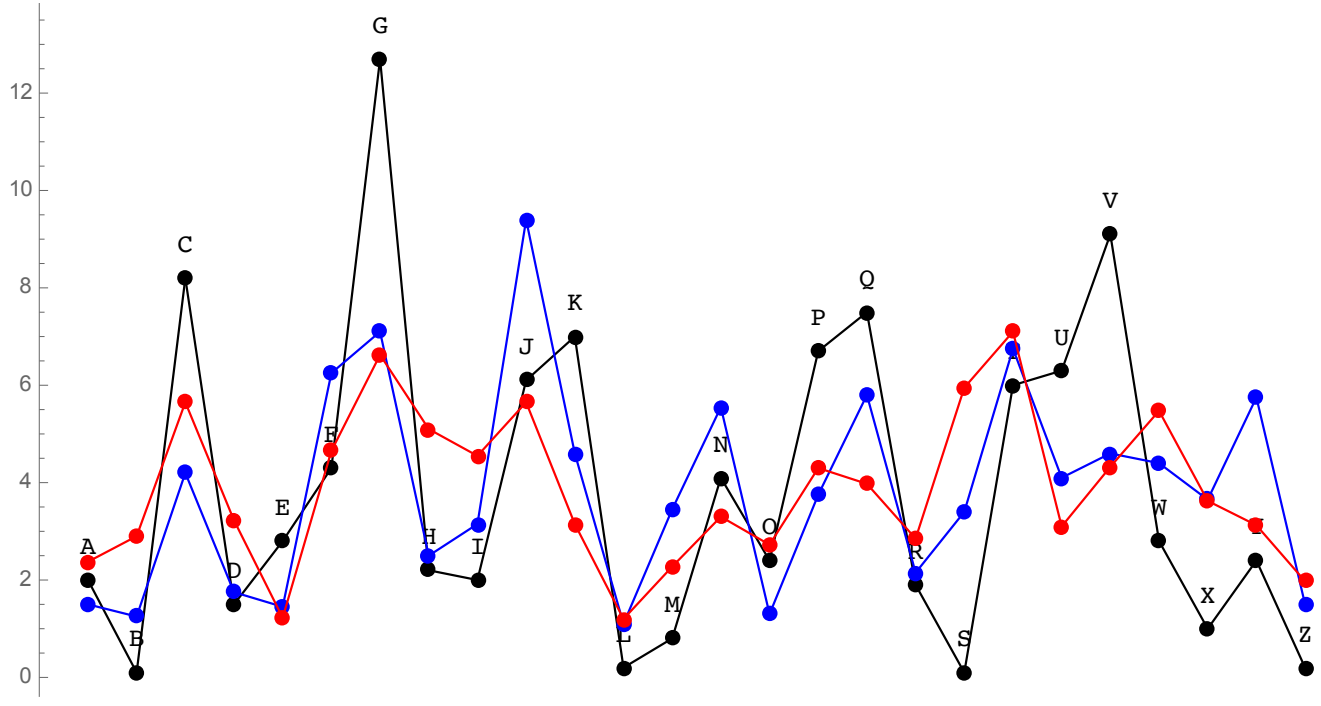
Take $k = \texttt{bead}$, so k has length 4. Under the bijection between letters and numbers, $\texttt{bead} \longleftrightarrow (1, 4, 0, 3)$. The table below shows that

$$e_{\texttt{bead}}(\texttt{meetatmidnightnear}) = \texttt{NIEWBXMLERIJIXNHBV}.$$

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
x_i	m	e	e	t	a	t	m	i	d	n	i	g	h	t	n	e	a	r
	12	4	4	19	0	19	12	8	3	13	8	6	7	19	13	4	0	17
k_i	b	e	a	d	b	e	a	d	b	e	a	d	b	e	a	d	b	e
	1	4	0	3	1	4	0	3	1	4	0	3	1	4	0	3	1	4
$x_i + k_i$	13	8	4	22	1	23	12	11	4	17	8	9	8	23	13	7	1	21
	N	I	E	W	B	X	M	L	E	R	I	J	I	X	N	H	B	V

Frequencies for one, two and four Caesar shifts applied to typical English (made using `AlphabetCiphers.nb` in video)

- Black: one shift by 2: note peaks at `C`, `G`, `V` for `a`, `e`, `t`.
- Blue: shifts by 2 and 5: now `C` comes from the common `a` and the rare `x`, so no peak!
- Red: shifts by 2, 5, 14, 15



A Weakness in the Vigenère Cipher

Exercise 2.11

(i) Which text below is more likely to be a be a sample of letters (not necessarily adjacent) from a Caesar Cipher ciphertext?

(A) `UWBBJSNMXUBSOWGFZTUIFFBIIJUBSTBUNGFIBSJETSGMJPTOOB`

(B) `UIWRBKBDJTSONEMOXSULBTSNOEWLGEFAZATEUIINFBFIBEIHID`

(C) `ULIVWIRBBAKZBVDKJWTRSCOINVEOMMOWXESVUMLOBJTHSENLOX`

(A) (B) (C)

Each sample has 50 characters. The ten most frequent letters, with frequencies, and the total frequency of the rest are:

(A)	B	U	S	T	J	I	F	O	G	W	the rest
	8	5	5	4	4	4	4	3	3	2	8
(B)	D	V	L	K	C	Y	F	Z	U	R	the rest
	6	5	5	3	3	3	3	3	3	2	14
(C)	L	X	D	C	Y	M	K	I	F	B	the rest
	5	4	4	3	3	3	3	3	3	2	17

A Weakness in the Vigenère Cipher

Exercise 2.11

(i) Which text below is more likely to be a be a sample of letters (not necessarily adjacent) from a Caesar Cipher ciphertext?

(A) `UWBBJSNMXUBSOWGFZTUIFFBIIJUBSTBUNGFIBSJETSGMJPTOOB`

(B) `UIWRBKBDJTSONEMOXSULBTSNOEWLGEFAZATEUIINFBFIBEIHID`

(C) `ULIVWIRBBAKZBVDKJWTRSCOINVEOMMOWXESVUMLOBJTHSENLOX`

(A) (B) (C)

Each sample has 50 characters. The ten most frequent letters, with frequencies, and the total frequency of the rest are:

(A)	B	U	S	T	J	I	F	O	G	W	the rest
	8	5	5	4	4	4	4	3	3	2	8
(B)	D	V	L	K	C	Y	F	Z	U	R	the rest
	6	5	5	3	3	3	3	3	3	2	14
(C)	L	X	D	C	Y	M	K	I	F	B	the rest
	5	4	4	3	3	3	3	3	3	2	17

A Weakness in the Vigenère Cipher

Exercise 2.11

(i) Which text below is more likely to be a be a sample of letters (not necessarily adjacent) from a Caesar Cipher ciphertext?

(A) `UWBBJSNMXUBSOWGFZTUIFFBIIJUBSTBUNGFIBSJETSGMJPTOOB`

(B) `UIWRBKBDJTSONEMOXSULBTSNOEWLGEFAZATEUIINFBFIBEIHID`

(C) `ULIVWIRBBAKZBVDKJWTRSCOINVEOMMOWXESVUMLOBJTHSENLOX`

(A) (B) (C)

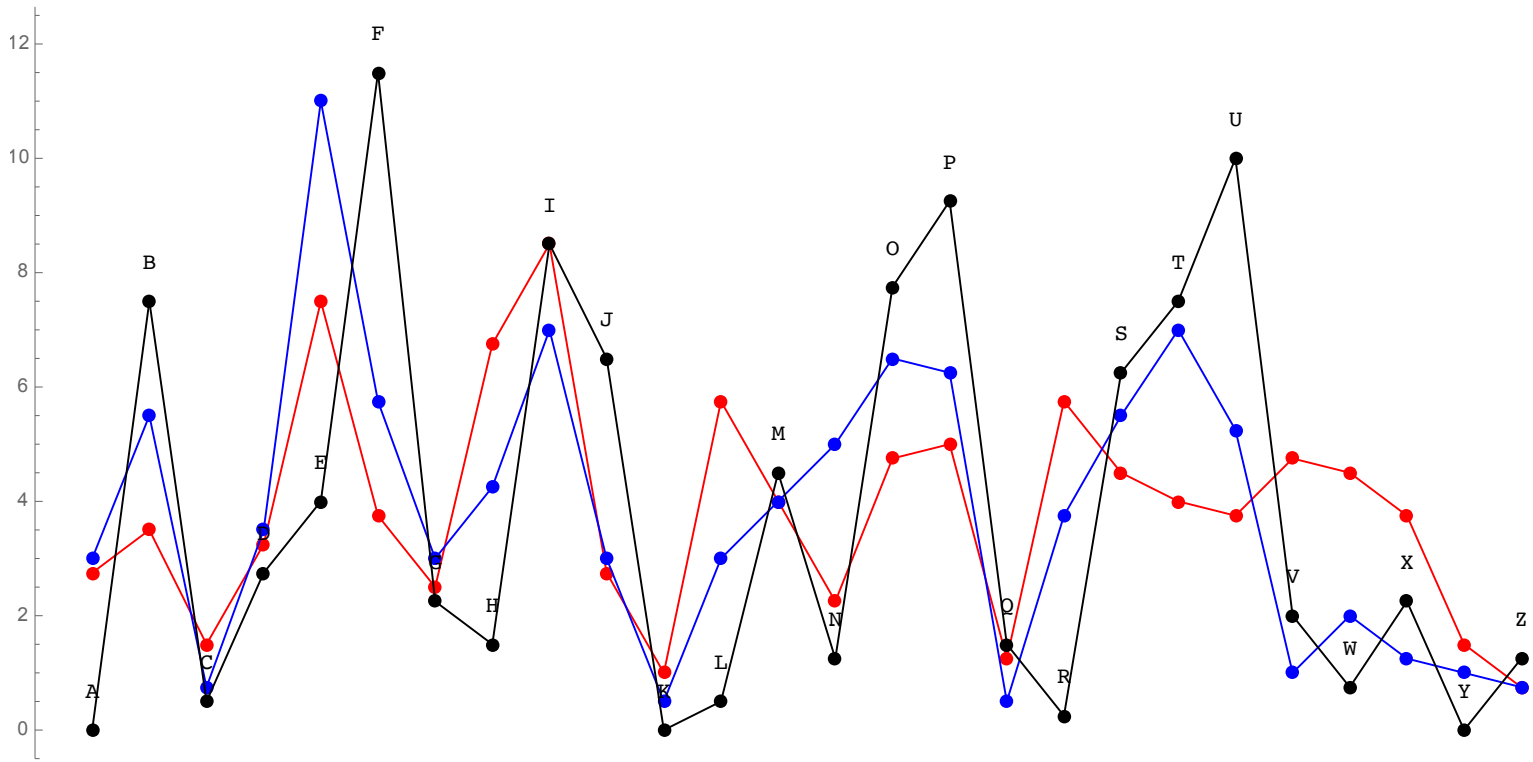
(ii) The samples in (i) are every 4th, every 2nd and every character from the ciphertext y in Example 2.16 below, encrypted using the Vigenère cipher with the **four letter** key `bead`.

Why should we expect the split ciphertext from a Vigènere cipher to have the most 'spiky' frequency distribution at the length of the keyword?

Hint: think about the number of Caesar shifts that are relevant and look again at the graph on the previous slide.

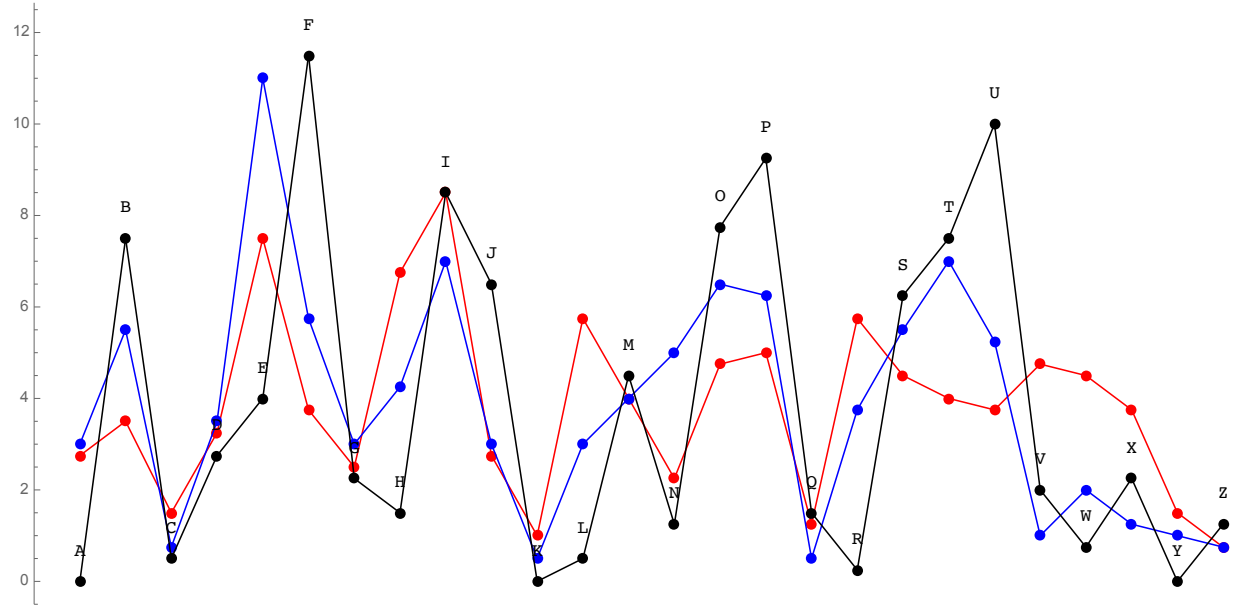
Vigenère Cipher and Spikiness

The graph below shows the frequencies (as percentages as usual) for every 4th, every 3rd, every 2nd and every character from the ciphertext y in Example 2.16 below, encrypted using the Vigenère cipher with the **four letter** key `bead` $\longleftrightarrow (1, 4, 0, 3)$. (See end of `AustenVigenereExample.nb` on Moodle.)



This is the final graph in the video 'Vigenère Cipher and Spikiness'.

Shifts from Vigenère Ciphertext, key bead $\leftrightarrow (1, 4, 0, 3)$



Quiz (four questions!): How many different shifts are used to encrypt

- the red sample obtained by taking every character in the ciphertext?

  (A) 1 (B) 2 (C) 3 (D) 4

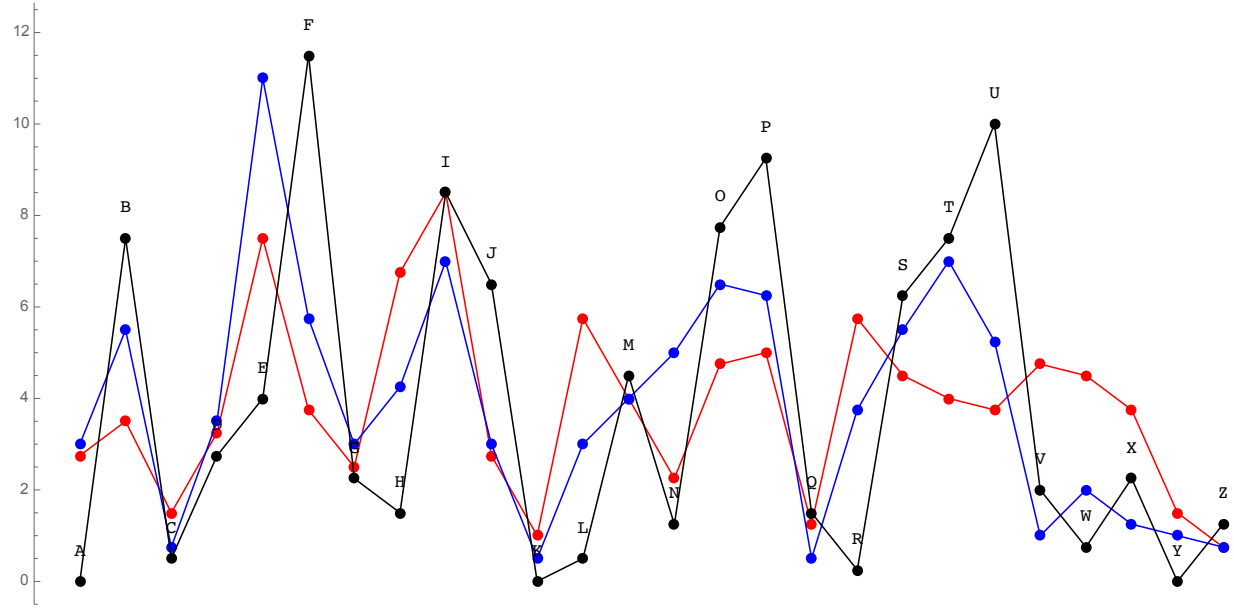
- the blue sample obtained by taking every other character?

  (A) 1 (B) 2 (C) 3 (D) 4

- the black sample obtained by taking every 4th character?

  (A) 1 (B) 2 (C) 3 (D) 4

Shifts from Vigenère Ciphertext, key bead $\leftrightarrow (1, 4, 0, 3)$



Quiz (four questions!): How many different shifts are used to encrypt

- the red sample obtained by taking every character in the ciphertext?

  (A) 1 (B) 2 (C) 3 (D) 4

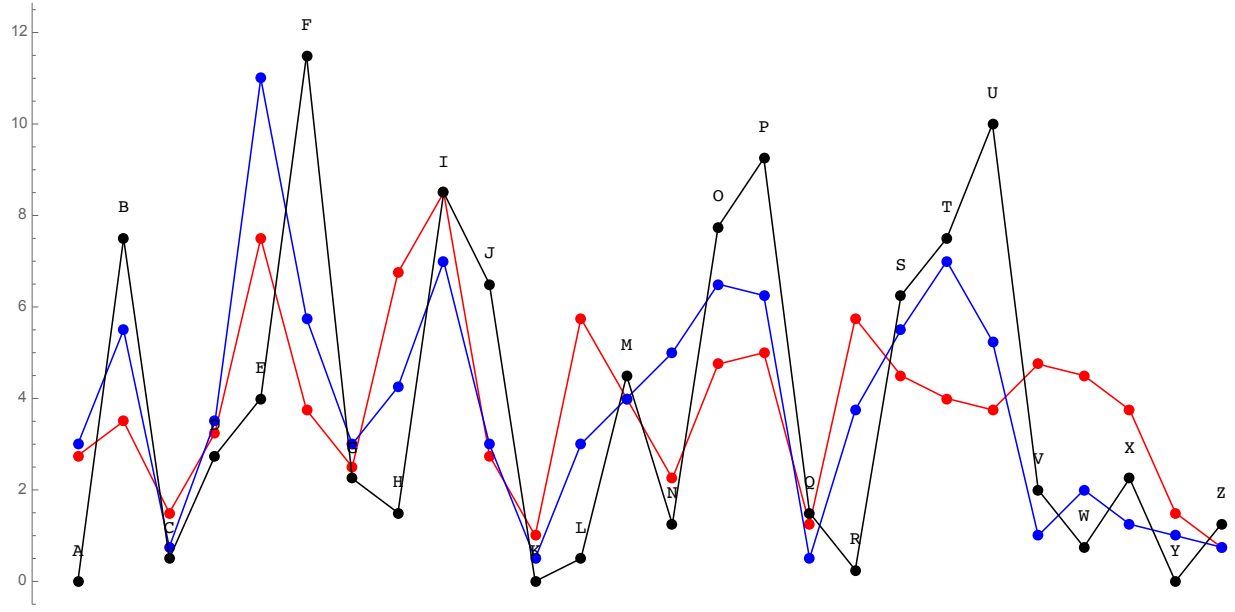
- the blue sample obtained by taking every other character?

  (A) 1 (B) 2 (C) 3 (D) 4

- the black sample obtained by taking every 4th character?

  (A) 1 (B) 2 (C) 3 (D) 4

Shifts from Vigenère Ciphertext, key bead $\leftrightarrow (1, 4, 0, 3)$



Quiz (four questions!): How many different shifts are used to encrypt

- the red sample obtained by taking every character in the ciphertext?

  (A) 1 (B) 2 (C) 3 (D) 4

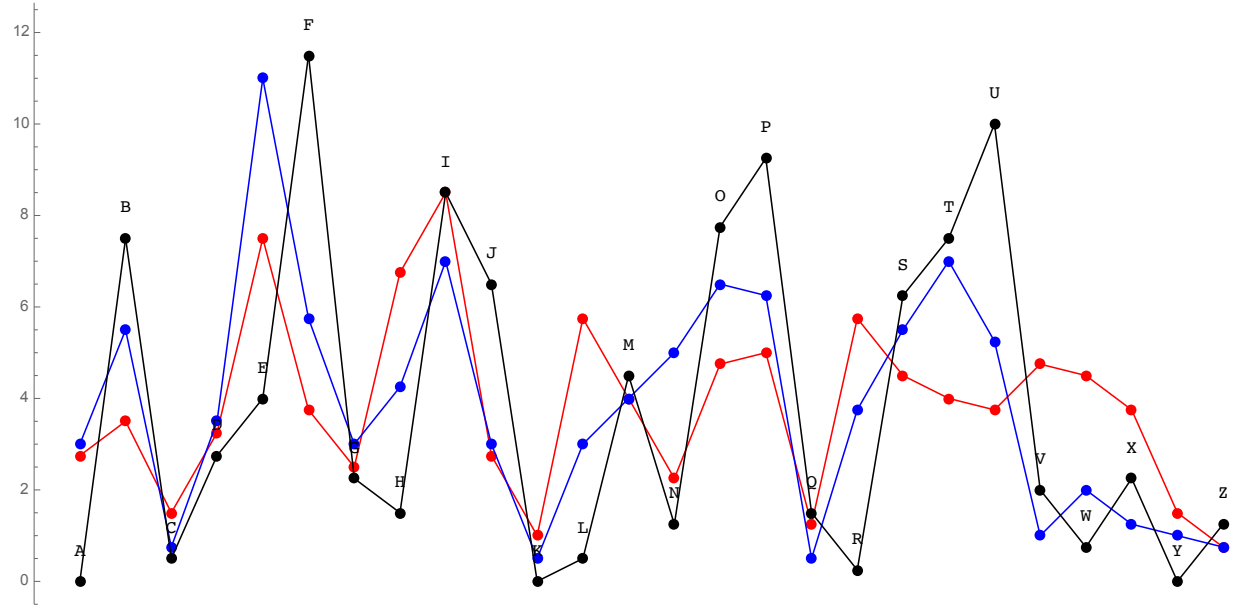
- the blue sample obtained by taking every other character?

  (A) 1 (B) 2 (C) 3 (D) 4

- the black sample obtained by taking every 4th character?

  (A) 1 (B) 2 (C) 3 (D) 4

Shifts from Vigenère Ciphertext, key bead $\leftrightarrow (1, 4, 0, 3)$



Quiz (four questions!): How many different shifts are used to encrypt

- the red sample obtained by taking every character in the ciphertext?

  (A) 1 (B) 2 (C) 3 (D) 4

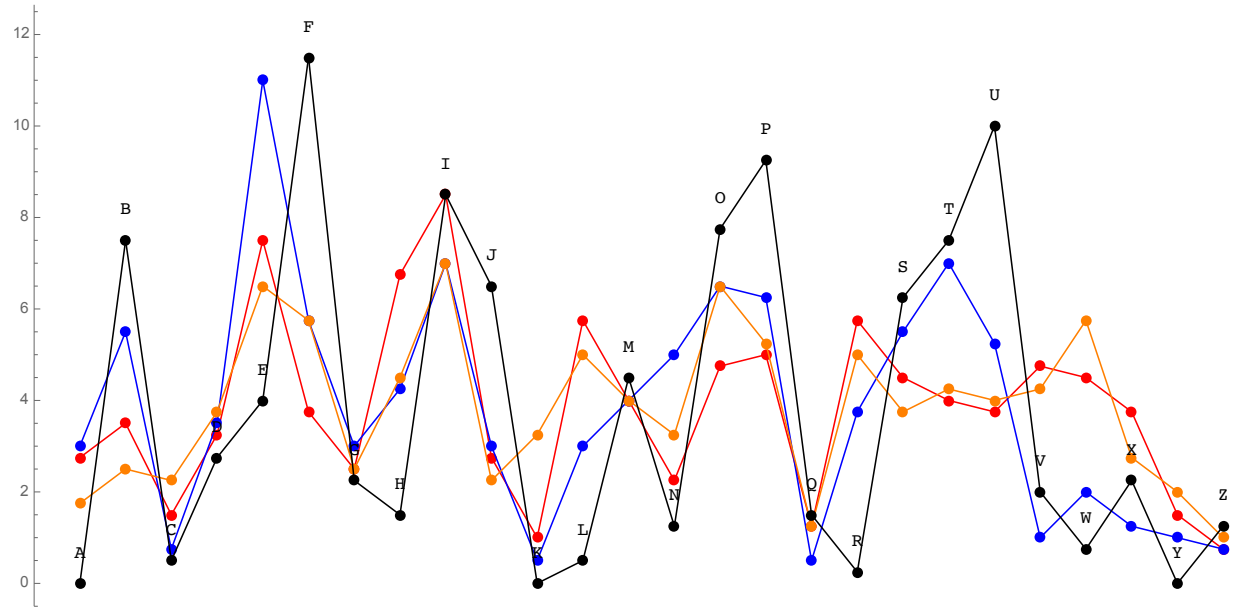
- the blue sample obtained by taking every other character?

  (A) 1 (B) 2 (C) 3 (D) 4

- the black sample obtained by taking every 4th character?

  (A) 1 (B) 2 (C) 3 (D) 4

Shifts from Vigenère Ciphertext, key bead $\leftrightarrow (1, 4, 0, 3)$



Quiz (four questions!): How many different shifts are used to encrypt

- the red sample obtained by taking every character in the ciphertext?

  (A) 1 (B) 2 (C) 3 (D) 4

- the blue sample obtained by taking every other character?

  (A) 1 (B) 2 (C) 3 (D) 4

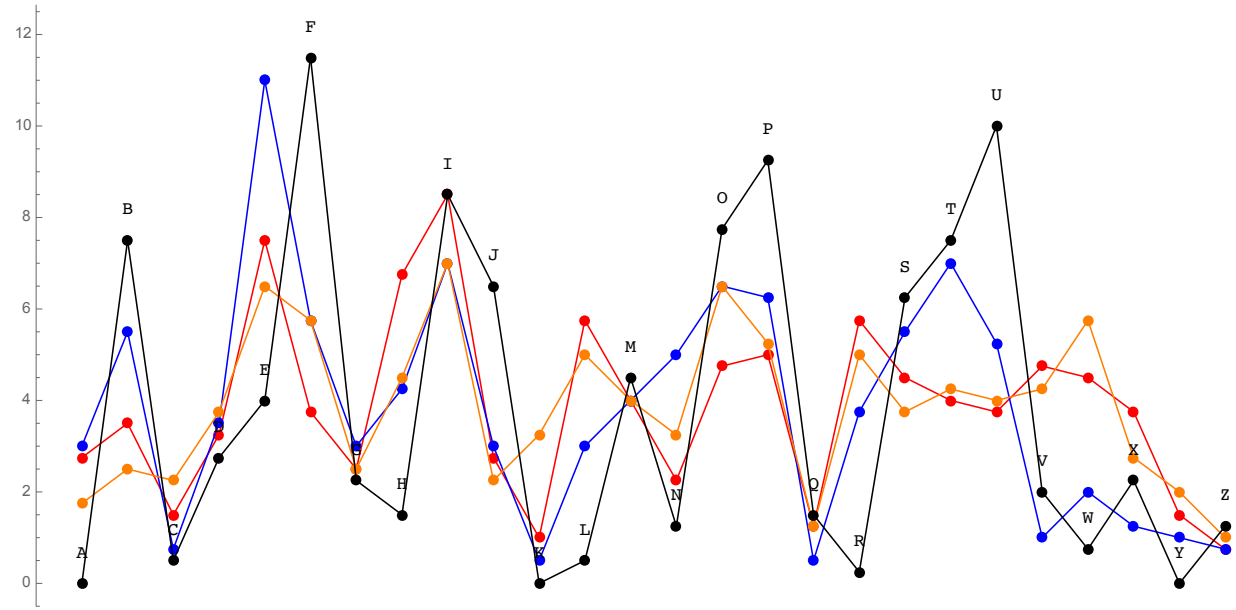
- the black sample obtained by taking every 4th character?

  (A) 1 (B) 2 (C) 3 (D) 4

- the orange sample obtained by taking every 3rd character?

  (A) 1 (B) 2 (C) 3 (D) 4

Shifts from Vigenère Ciphertext, key bead $\leftrightarrow (1, 4, 0, 3)$



Quiz (four questions!): How many different shifts are used to encrypt

- the red sample obtained by taking every character in the ciphertext?

  (A) 1 (B) 2 (C) 3 (D) 4

- the blue sample obtained by taking every other character?

  (A) 1 (B) 2 (C) 3 (D) 4

- the black sample obtained by taking every 4th character?

  (A) 1 (B) 2 (C) 3 (D) 4

- the orange sample obtained by taking every 3rd character?

  (A) 1 (B) 2 (C) 3 (D) 4

Index of Coincidence or 'The Measure of Spikiness'

Definition 2.12

The *Index of Coincidence* of a ciphertext y, denoted $I(y)$, is the probability that two entries of y, chosen at random from different positions, are equal.

Exercise 2.13

Explain why $I(\texttt{QXNURA}) = I(\texttt{QNRFLX}) = 0$ and check that $I(\texttt{MOODLE}) = I(\texttt{LOOMED}) = \frac{1}{15}$. What is $I(\texttt{AAABBC})$?

(A) $\frac{1}{5}$ (B) $\frac{4}{15}$ (C) $\frac{3}{10}$ (D) $\frac{11}{30}$

What $I(\texttt{AAAAAABBBCCZ})$?

(A) $\frac{17}{66}$ (B) $\frac{3}{11}$ (C) $\frac{19}{66}$ (D) $\frac{39}{132}$

Index of Coincidence or 'The Measure of Spikiness'

Definition 2.12

The *Index of Coincidence* of a ciphertext y, denoted $I(y)$, is the probability that two entries of y, chosen at random from different positions, are equal.

Exercise 2.13

Explain why $I(\texttt{QXNURA}) = I(\texttt{QNRFLX}) = 0$ and check that $I(\texttt{MOODLE}) = I(\texttt{LOOMED}) = \frac{1}{15}$. What is $I(\texttt{AAABBC})$?

(A) $\frac{1}{5}$ (B) $\frac{4}{15}$ (C) $\frac{3}{10}$ (D) $\frac{11}{30}$

What $I(\texttt{AAAAAABBBCCZ})$?

(A) $\frac{17}{66}$ (B) $\frac{3}{11}$ (C) $\frac{19}{66}$ (D) $\frac{39}{132}$

Lemma 2.14 (Examinable: see video or click on for main idea)

If the ciphertext y of length n has exactly f_i letters corresponding to i, for each $i \in \{0, 1, \ldots, 25\}$ then

$$I(y) = \sum_{i=0}^{25} \frac{f_i(f_i - 1)}{n(n-1)}.$$

Index of Coincidence or 'The Measure of Spikiness'

Definition 2.12

The *Index of Coincidence* of a ciphertext y, denoted $I(y)$, is the probability that two entries of y, chosen at random from different positions, are equal.

Exercise 2.13

Explain why $I(\texttt{QXNURA}) = I(\texttt{QNRFLX}) = 0$ and check that $I(\texttt{MOODLE}) = I(\texttt{LOOMED}) = \frac{1}{15}$. What is $I(\texttt{AAABBC})$?

(A) $\frac{1}{5}$ (B) $\frac{4}{15}$ (C) $\frac{3}{10}$ (D) $\frac{11}{30}$

What $I(\texttt{AAAAAABBBCCZ})$?

(A) $\frac{17}{66}$ (B) $\frac{3}{11}$ (C) $\frac{19}{66}$ (D) $\frac{39}{132}$

Lemma 2.14 (Examinable: see video or click on for main idea)

If the ciphertext y of length n has exactly f_i letters corresponding to i, for each $i \in \{0, 1, \ldots, 25\}$ then

$$I(y) = \sum_{i=0}^{25} \frac{f_i(f_i - 1)}{n(n-1)}.$$

Index of Coincidence or 'The Measure of Spikiness'

Definition 2.12

The *Index of Coincidence* of a ciphertext y, denoted $I(y)$, is the probability that two entries of y, chosen at random from different positions, are equal.

Exercise 2.13

Explain why $I(\texttt{QXNURA}) = I(\texttt{QNRFLX}) = 0$ and check that $I(\texttt{MOODLE}) = I(\texttt{LOOMED}) = \frac{1}{15}$. What is $I(\texttt{AAABBC})$?

(A) $\frac{1}{5}$ (B) $\frac{4}{15}$ (C) $\frac{3}{10}$ (D) $\frac{11}{30}$

What $I(\texttt{AAAAAABBBCCZ})$?

(A) $\frac{17}{66}$ (B) $\frac{3}{11}$ (C) $\frac{19}{66}$ (D) $\frac{39}{132}$

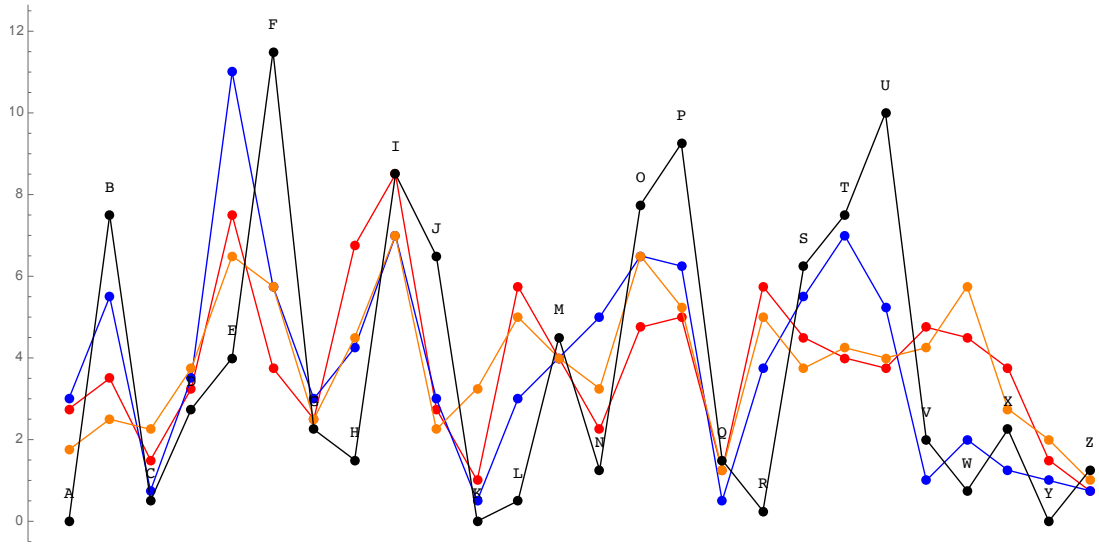
Idea of proof: let X and Z be the first and second characters chosen. Condition on X, and then find the probability that $Z = x$ *given that* $X = x$. (I did warn you that you would need conditional probability.) If you understand why

$$I(\texttt{AAABBC}) = \mathbb{P}[Z = \texttt{A}|X = \texttt{A}]\tfrac{3}{6} + \mathbb{P}[Z = \texttt{B}|X = \texttt{B}]\tfrac{2}{6} + \mathbb{P}[Z = \texttt{C}|X = \texttt{C}]\tfrac{1}{6}$$

then you have all the tools needed to write a general proof.

The IOC Works to Measure Spikiness

The graph below shows the frequencies (as percentages as usual) for every 4th, every 3rd, every 2nd and every character from the full ciphertext y in Example 2.16 below, encrypted using the Vigenère cipher with the **four letter** key bead $\longleftrightarrow (1, 4, 0, 3)$.

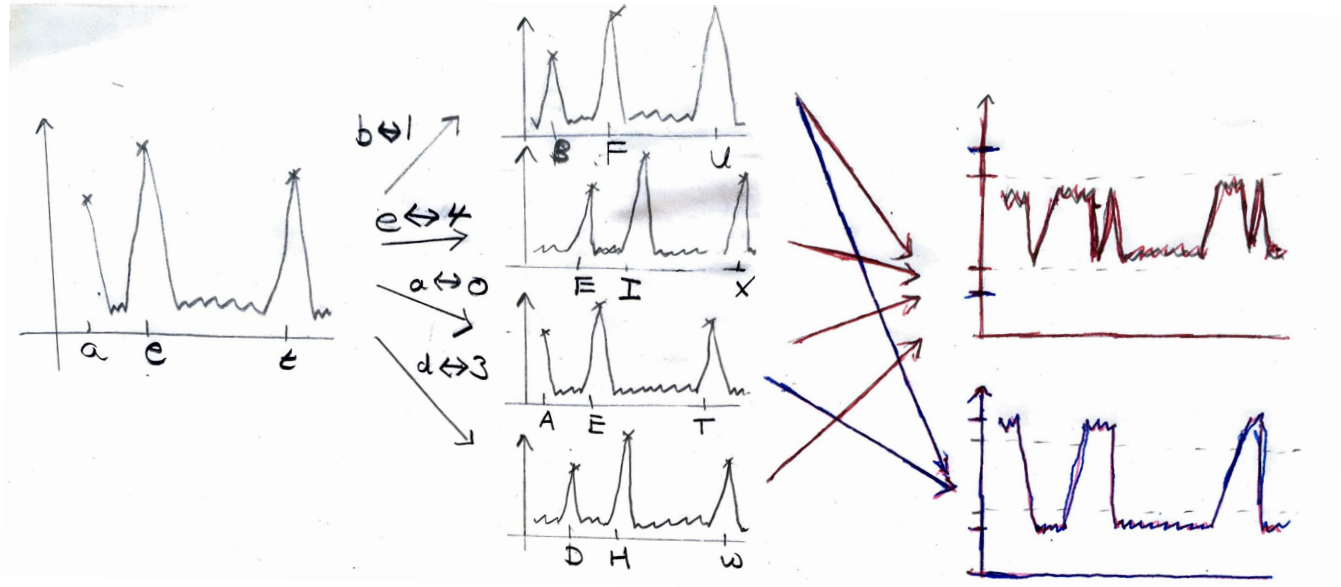


This table shows the IOC for the samples taking every kth letter for $k \in \{1, 2, 3, 4, 5, 6\}$. Produced in MATHEMATICA at the start of the 'Vigenère attack using Index of Coincidence'.

k	1	2	3	4	5	6
IOC	0.0458	0.0528	0.0431	0.0687	0.0452	0.0546

Quiz: Vigenère Cipher with Key 'bead'

Imagine that English has common letters 'a' 'e' 't' and all other letters are rare, so the frequency graph is as shown on the left.

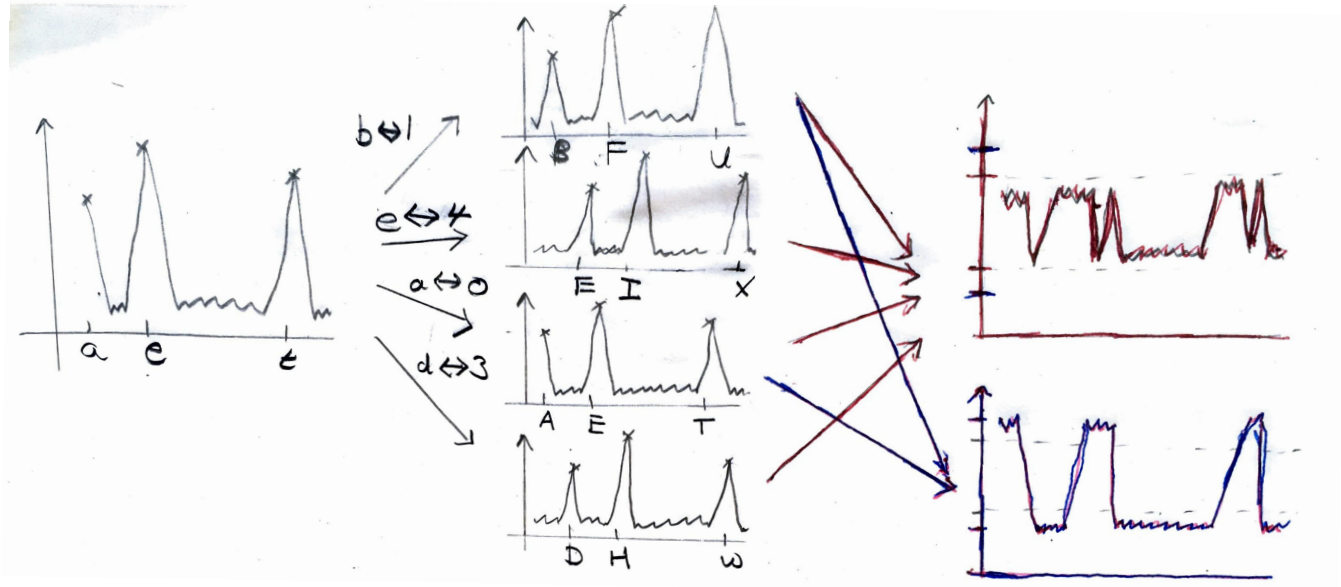


- Suppose we split the ciphertext, encrypted using a Vigenère key of length 4, taking every third position. What will the frequency graph look more like?

(A) red (B) blue

Quiz: Vigenère Cipher with Key 'bead'

Imagine that English has common letters 'a' 'e' 't' and all other letters are rare, so the frequency graph is as shown on the left.



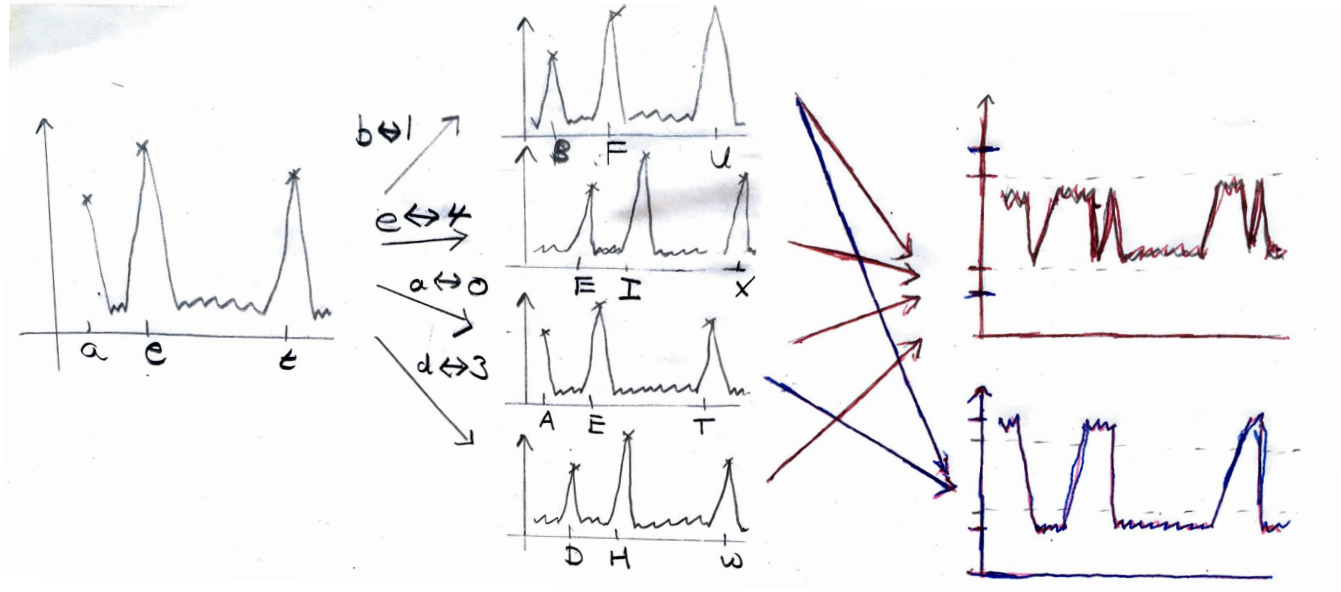
- Suppose we split the ciphertext, encrypted using a Vigenère key of length 4, taking every third position. What will the frequency graph look more like?

  (A) red (B) blue

  Since all four shifts are seen.

Quiz: Vigenère Cipher with Key 'bead'

Imagine that English has common letters 'a' 'e' 't' and all other letters are rare, so the frequency graph is as shown on the left.



- Let I_k be the Index of Coincidence computed by taking every kth character. What order do you expect for I_1, I_2, I_3, I_4?

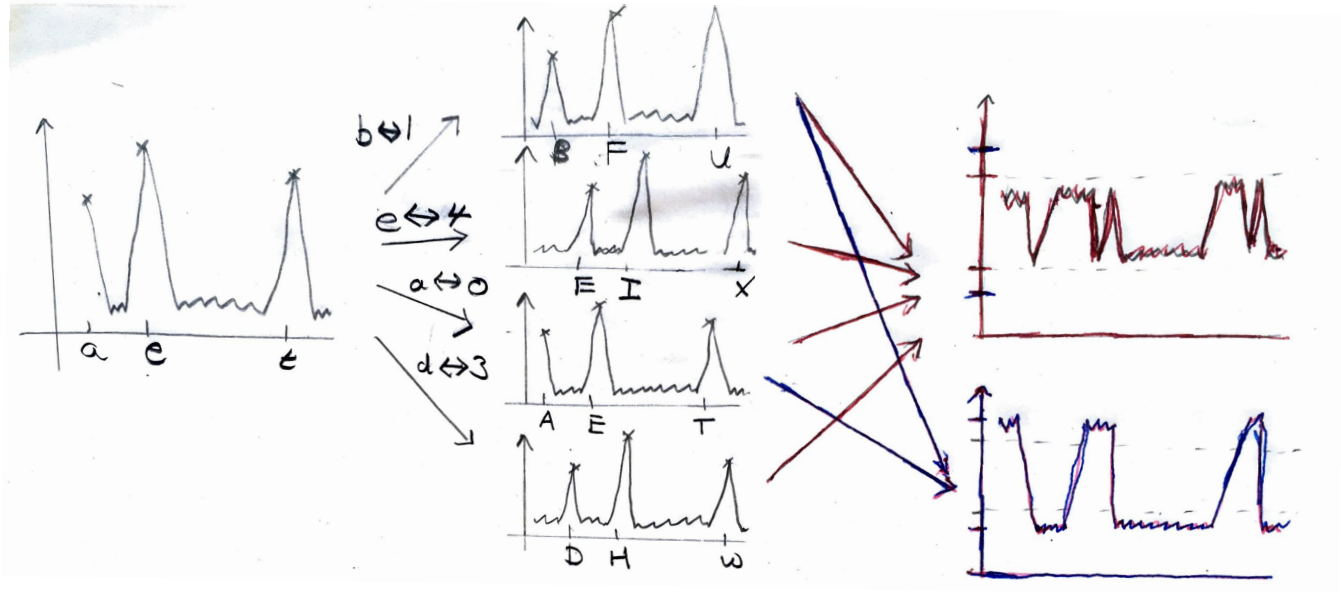
  (A) $I_1 < I_2 < I_3 < I_4$; (B) $I_1 < I_3 < I_2 < I_4$;

  (C) $I_1 \approx I_3 < I_2 < I_4$; (D) $I_1 \approx I_2 \approx I_3 < I_4$.

(A) (B) (C) (D)

Quiz: Vigenère Cipher with Key 'bead'

Imagine that English has common letters 'a' 'e' 't' and all other letters are rare, so the frequency graph is as shown on the left.



- Let I_k be the Index of Coincidence computed by taking every kth character. What order do you expect for I_1, I_2, I_3, I_4?

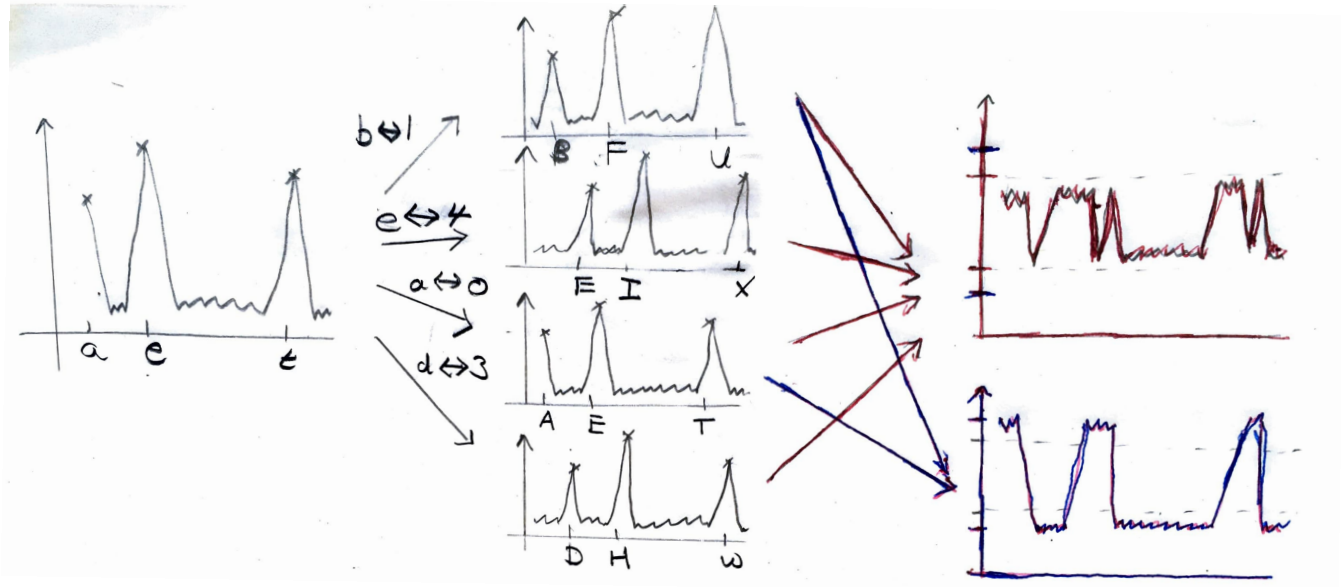
  (A) $I_1 < I_2 < I_3 < I_4$; (B) $I_1 < I_3 < I_2 < I_4$;

  (C) $I_1 \approx I_3 < I_2 < I_4$; (D) $I_1 \approx I_2 \approx I_3 < I_4$.

(A) (B) (C) (D)

Quiz: Vigenère Cipher with Key 'bead'

Imagine that English has common letters 'a' 'e' 't' and all other letters are rare, so the frequency graph is as shown on the left.



- Let I_k be the Index of Coincidence computed by taking every kth character. What order do you expect for I_1, I_2, I_3, I_4?

  (A) $I_1 < I_2 < I_3 < I_4$; (B) $I_1 < I_3 < I_2 < I_4$;

  (C) $I_1 \approx I_3 < I_2 < I_4$; (D) $I_1 \approx I_2 \approx I_3 < I_4$.

  (A) (B) (C) (D)

  Why (C)? Since the IOC measures how many different shifts are used in the ciphertext sample: 4 shifts for $k = 1$ and for 3 (see 'Index of Coincidence' video); 2 shifts for $k = 2$; 1 shift for $k = 4$.

Attack on the Vigenère Cipher

We now have a strategy for decrypting a Vigenère ciphertext.

Attack 2.15

Given a Vigenère ciphertext y, take every k-th letter for all small k. For instance when $k = 3$ the sample is $y_0y_3y_6y_9\ldots$ and when $k = 4$ the sample is $y_0y_4y_8\ldots$. The Index of Coincidence will be greatest (for long samples) when we split at the key length, ℓ.

- Now $y_0y_\ell y_{2\ell}\ldots$ have all been encrypted by shifting by k_0: assuming that the most common letter is the shift of 'e' determines the shift.
- Repeat with $y_1y_{\ell+1}y_{2\ell+1}\ldots$ to determine k_1
- ... and so on, up to $k_{\ell-1}$.

Example 2.16

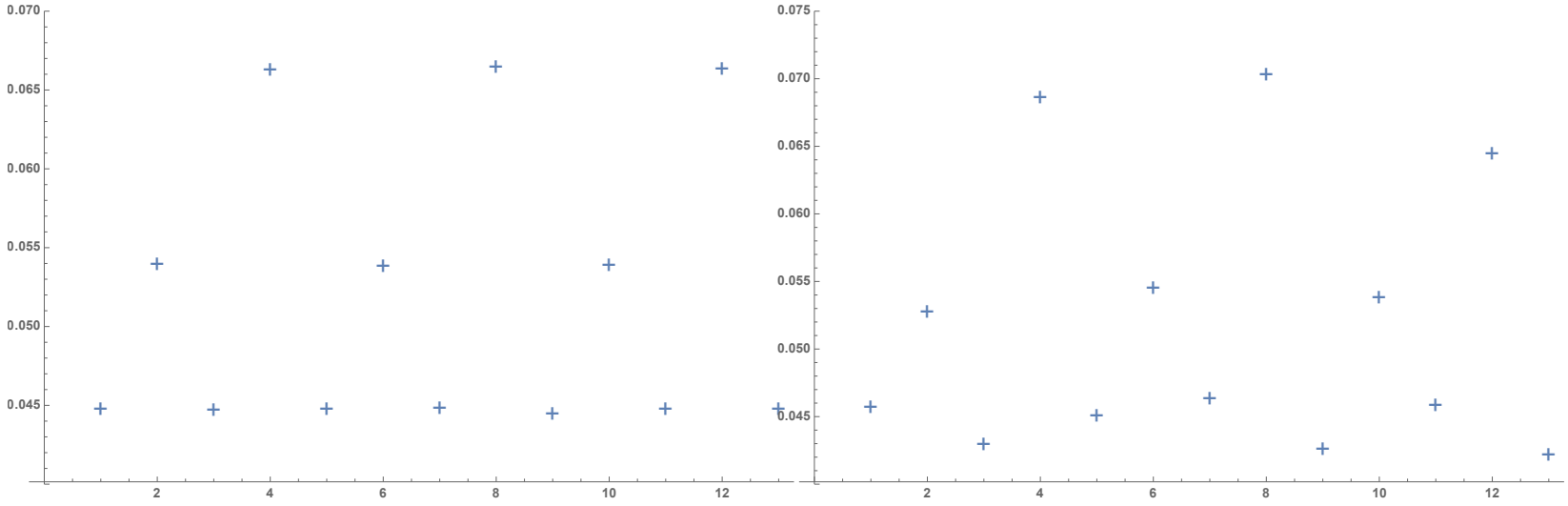
The following ciphertext is the output of a Vigènre cipher:

`ULIVWIRBBAKZBVDKJWTRSCOINVEOMMOWXESVUMLOBJTHSENL ...`

(A fuller ciphertext is in the printed notes and the whole lot is in the MATHEMATICA notebook `VigenereAustenExample.nb`.)

Example 2.16 [continued] Attack on Vigenère Cipher

The graph left below shows the mean Index of Coincidence when the ciphertext is split taking every kth letter, for $k \in \{1, 2, \ldots, 13\}$.



- Improving on Attack 2.15, we took the average of the samples by starting at each of the initial k letters in turn.
- If we just take samples starting at the first letter, the IOCs vary more (see right), but one would still correctly guess the key length is 4, since the increase from 4 to 8 is very small.

Example 2.16 [continued] Attack on Vigenère Cipher

Taking every four letter of the ciphertext, starting at the zeroth:

$$y_0 y_4 y_8 \ldots = \text{`UWBBJSNMXUBSOWGFZTUIFFBIIJUB}\ldots\text{'}$$

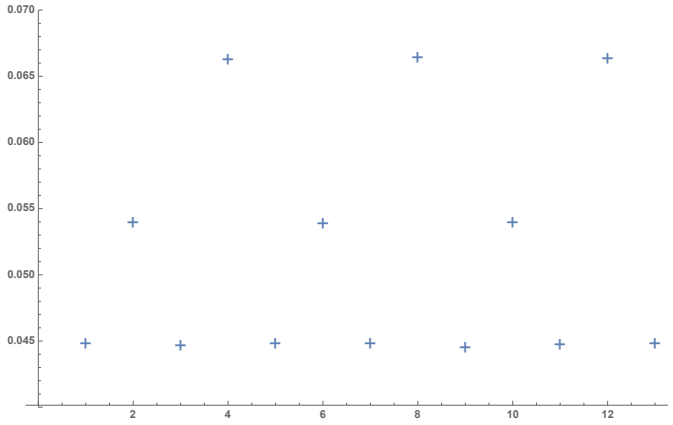
This is the first sample in the quiz earlier. The frequency table (as in Example 2.5) begins

F	P	U	O
12.5	8.3	8.0	8.0

Assuming 'F' $\longleftrightarrow$ 5 is the encryption of 'e' $\longleftrightarrow$ 4, the shift in the Caesar cipher is 1 $\longleftrightarrow$ '*b*', so we guess the first letter of the key is 'b'. The MATHEMATICA notebook `VigenereAustenExample` on Moodle shows this simple strategy works in all 4 positions to reveal the key bead.

Smaller Peaks when only some Shifts are Relevant

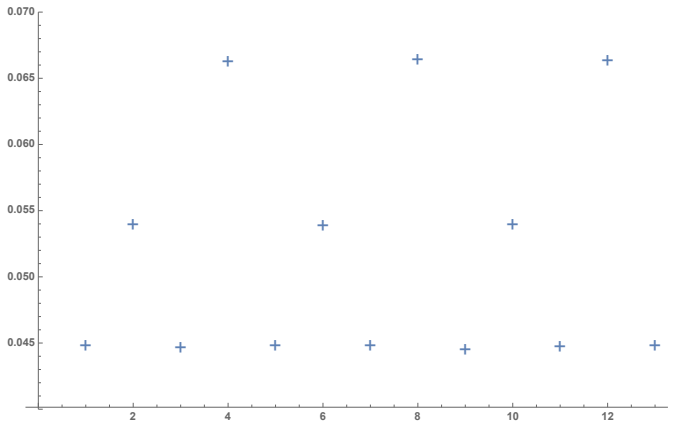
Exercise 2.17



Explain why there are smaller peaks at 2, 6 and 10 in the plot of Indices of Coincidence above.

Smaller Peaks when only some Shifts are Relevant

Exercise 2.17



Explain why there are smaller peaks at 2, 6 and 10 in the plot of Indices of Coincidence above.

Explanation: when we take every 2nd character from the beginning, we see the shifts for `b` and `a`:

be**a**d**b**e**a**d ....

(Or if we start at the second character the shifts are `e` and `d`.) Similarly if we take every 6th character: the relevant shifts are again `b` and `a`:

beadbe**a**dbead**b**eadbe**a**dbead**b**dbe ....

Since the IOC measures the number of different shifts involved, it is in the middle when $k = 2, 6, 10, \ldots$. We have already seen it is highest when $k = 4, 8, \ldots$ is a multiple of the key length (only one shift) and lowest when all four shifts are relevant, so $k = 1, 3, 5, 7, \ldots$.

Second Quiz on Vigenère Splits

Suppose that the key has length 12 with 12 different letters. Recall that $y_i = x_i + k_{i \bmod 12}$ for each i. For instance

$$y_0 = x_0 + k_0,\ y_1 = x_1 + k_1, \ldots, y_{12} = x_{12} + k_0,\ y_{13} = x_{13} + k_1.$$

(a) How many different shifts are seen when the ciphertext is split taking every 6th position?

(A) 1 (B) 2 (C) 3 (D) 4

(b) How many different shifts are seen when the ciphertext is split taking every 4th position?

(A) 1 (B) 2 (C) 3 (D) 4

(c) How many different shifts are seen when the ciphertext is split taking every 8th position?

(A) 1 (B) 2 (C) 3 (D) 4

Second Quiz on Vigenère Splits

Suppose that the key has length 12 with 12 different letters. Recall that $y_i = x_i + k_{i \bmod 12}$ for each i. For instance

$$y_0 = x_0 + k_0,\ y_1 = x_1 + k_1, \ldots, y_{12} = x_{12} + k_0,\ y_{13} = x_{13} + k_1.$$

(a) How many different shifts are seen when the ciphertext is split taking every 6th position?

(A) 1 (B) 2 (C) 3 (D) 4

(b) How many different shifts are seen when the ciphertext is split taking every 4th position?

(A) 1 (B) 2 (C) 3 (D) 4

(c) How many different shifts are seen when the ciphertext is split taking every 8th position?

(A) 1 (B) 2 (C) 3 (D) 4

Second Quiz on Vigenère Splits

Suppose that the key has length 12 with 12 different letters. Recall that $y_i = x_i + k_{i \bmod 12}$ for each i. For instance

$$y_0 = x_0 + k_0,\ y_1 = x_1 + k_1, \ldots, y_{12} = x_{12} + k_0,\ y_{13} = x_{13} + k_1.$$

(a) How many different shifts are seen when the ciphertext is split taking every 6th position?

(A) 1 (B) 2 (C) 3 (D) 4

(b) How many different shifts are seen when the ciphertext is split taking every 4th position?

(A) 1 (B) 2 (C) 3 (D) 4

(c) How many different shifts are seen when the ciphertext is split taking every 8th position?

(A) 1 (B) 2 (C) 3 (D) 4

Second Quiz on Vigenère Splits

Suppose that the key has length 12 with 12 different letters. Recall that $y_i = x_i + k_{i \bmod 12}$ for each i. For instance

$$y_0 = x_0 + k_0,\ y_1 = x_1 + k_1, \ldots, y_{12} = x_{12} + k_0,\ y_{13} = x_{13} + k_1.$$

(a) How many different shifts are seen when the ciphertext is split taking every 6th position?

(A) 1 (B) 2 (C) 3 (D) 4

(b) How many different shifts are seen when the ciphertext is split taking every 4th position?

(A) 1 (B) 2 (C) 3 (D) 4

(c) How many different shifts are seen when the ciphertext is split taking every 8th position?

(A) 1 (B) 2 (C) 3 (D) 4

Second Quiz on Vigenère Splits

Suppose that the key has length 12 with 12 different letters. Recall that $y_i = x_i + k_{i \bmod 12}$ for each i. For instance

$$y_0 = x_0 + k_0,\ y_1 = x_1 + k_1, \ldots, y_{12} = x_{12} + k_0,\ y_{13} = x_{13} + k_1.$$

The table below shows the number of shifts for each ℓ.

ℓ	1	2	3	4	5	6	7	8	9	10	11
number of shifts	12	6	4	3	12	2	12	3	4	6	12

- When the ciphertext is split taking every ℓth letter, the Index of Coincidence is maximized when $\ell = 12$. What value(s) of ℓ will give the second highest?

  (A) 2, 4, 6, 8, or 10 (B) 3, 6 or 9 (C) 4 or 8 (D) 6
- What value(s) of ℓ will give the third highest?

  (A) 2, 4, 6, 8 or 10 (B) 3, 6 or 9 (C) 4 or 8 (D) 6

Second Quiz on Vigenère Splits

Suppose that the key has length 12 with 12 different letters. Recall that $y_i = x_i + k_{i \bmod 12}$ for each i. For instance

$$y_0 = x_0 + k_0,\ y_1 = x_1 + k_1, \ldots, y_{12} = x_{12} + k_0,\ y_{13} = x_{13} + k_1.$$

The table below shows the number of shifts for each ℓ.

ℓ	1	2	3	4	5	6	7	8	9	10	11
number of shifts	12	6	4	3	12	2	12	3	4	6	12

- When the ciphertext is split taking every ℓth letter, the Index of Coincidence is maximized when $\ell = 12$. What value(s) of ℓ will give the second highest?

  (A) 2, 4, 6, 8, or 10 (B) 3, 6 or 9 (C) 4 or 8 (D) 6
- What value(s) of ℓ will give the third highest?

  (A) 2, 4, 6, 8 or 10 (B) 3, 6 or 9 (C) 4 or 8 (D) 6

Second Quiz on Vigenère Splits

Suppose that the key has length 12 with 12 different letters. Recall that $y_i = x_i + k_{i \bmod 12}$ for each i. For instance

$$y_0 = x_0 + k_0,\ y_1 = x_1 + k_1, \ldots, y_{12} = x_{12} + k_0,\ y_{13} = x_{13} + k_1.$$

The table below shows the number of shifts for each ℓ.

ℓ	1	2	3	4	5	6	7	8	9	10	11
number of shifts	12	6	4	3	12	2	12	3	4	6	12

- When the ciphertext is split taking every ℓth letter, the Index of Coincidence is maximized when $\ell = 12$. What value(s) of ℓ will give the second highest?

  (A) 2, 4, 6, 8, or 10 (B) 3, 6 or 9 (C) 4 or 8 (D) 6
- What value(s) of ℓ will give the third highest?

  (A) 2, 4, 6, 8 or 10 (B) 3, 6 or 9 (C) 4 or 8 (D) 6

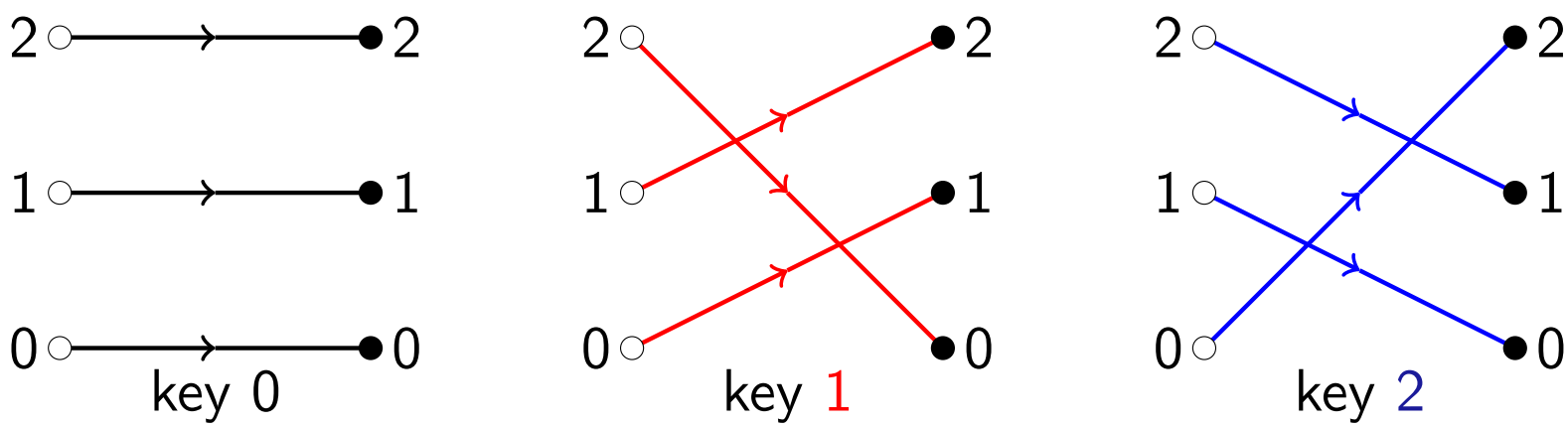
Problem Sheet 1

- If you have no message to attack in Question 3 (c), email me at `mark.wildon@rhul.ac.uk` and I will send you a ciphertext encrypted using the key of the lazy pair in your block.
- If you have problems with `AlphabetCiphers.nb`, or any other notebook in the course, please:
  - Quit MATHEMATICA
  - Download a fresh copy of the notebook from Moodle.
    Rename `AlphabetCiphers.nb.txt` to `AlphabetCiphers.nb` if necessary.
    This is a Moodle bug affecting Safari on Mac OS X and maybe other browsers.
    It looks like it might have gone away after one of the recent Moodle updates.
  - Restart MATHEMATICA
  - Load the fresh copy of `AlphabetCiphers.nb`
  - **Select 'Evaluate Notebook' in the 'Evaluation' menu**. (As it says at the top of the notebook.)

  Then remember that it's always **shift-return** to evaluate. If you ever press return, you are probably doing things wrong.
- If you are confused on Question 5(e) see Exercise 2.17 and the quiz afterwards, the earlier quiz, and the first and second videos on the Vigènere Cipher and Index of Coincidence. Yes, I really want you to get this idea!

§3 Cryptosystems and Perfect Secrecy

The three different encryption functions for the Caesar cipher on the 'alphabet' $\{0, 1, 2\}$ are shown in the diagram below.



Definition of Cryptosystems

Definition 3.1

Let $\mathcal{K}, \mathcal{P}, \mathcal{C}$ be finite sets. A *cryptosystem* is a family of *encryption functions* $e_k : \mathcal{P} \to \mathcal{C}$ and *decryption functions* $d_k : \mathcal{C} \to \mathcal{P}$, one for each $k \in \mathcal{K}$, such that for each $k \in K$,

$$d_k\big(e_k(x)\big) = x \qquad (\star)$$

for all $x \in \mathcal{P}$. We call $\mathcal{K}$ the *keyspace*, $\mathcal{P}$ the set of *plaintexts*, and $\mathcal{C}$ the set of *ciphertexts*.

Definition of Cryptosystems

Definition 3.1

Let $\mathcal{K}, \mathcal{P}, \mathcal{C}$ be finite sets. A *cryptosystem* is a family of *encryption functions* $e_k : \mathcal{P} \to \mathcal{C}$ and *decryption functions* $d_k : \mathcal{C} \to \mathcal{P}$, one for each $k \in \mathcal{K}$, such that for each $k \in K$,

$$d_k\big(e_k(x)\big) = x \qquad (\star)$$

for all $x \in \mathcal{P}$. We call $\mathcal{K}$ the *keyspace*, $\mathcal{P}$ the set of *plaintexts*, and $\mathcal{C}$ the set of *ciphertexts*.

Recall that a function $f : \mathcal{P} \to \mathcal{C}$ is injective if

- for all $x, x' \in \mathcal{P}$, $f(x) = f(x')$ implies $x = x'$.

Equivalently (take the contrapositive), if $x \neq x'$ then $f(x) \neq f(x')$.

Exercise 3.2

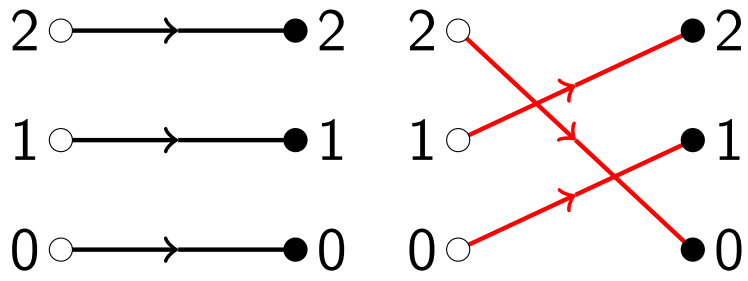
(i) Use $(\star)$ to show that for each $k \in \mathcal{K}$, the encryption functions $e_k : \mathcal{P} \to \mathcal{C}$ is injective.

(ii) Why do we want the encryption functions in a cryptosystem to be injective?

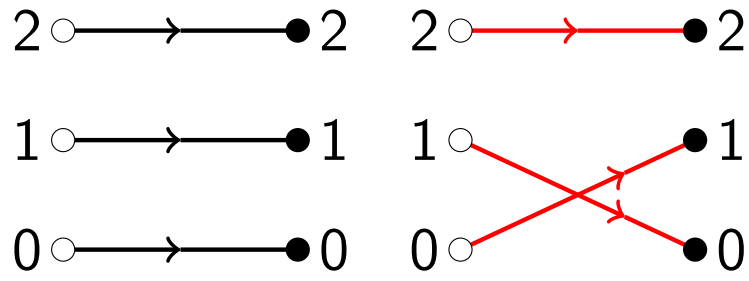
Exercise 3.3

Each diagram (i)–(vi) below each show two purported functions. Which illustrate the encryption functions in a cryptosystem with two keys (one **black**, one **red**)? In each case $\mathcal{P}$ is on left-hand side and $\mathcal{C} = \{0, 1, 2\}$ is on right-hand side. Next two slides gives all answers.

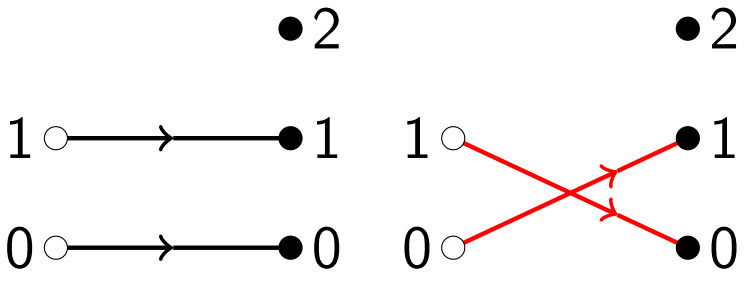
(i)



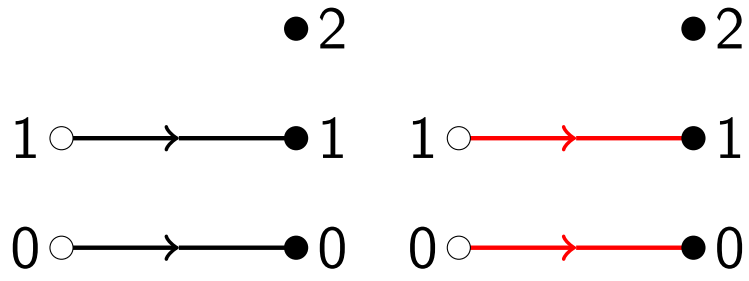
(ii)



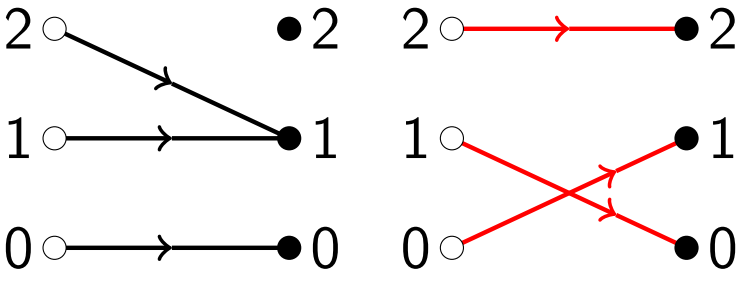
(iii)



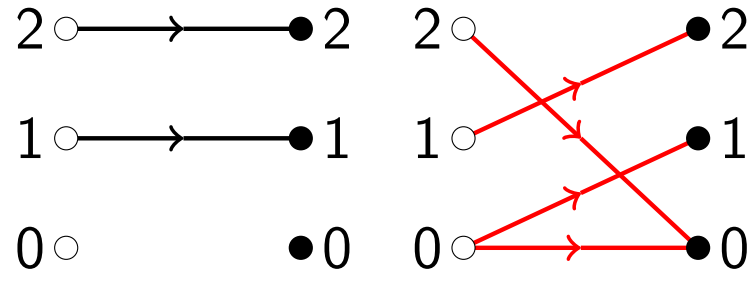
(iv)



(v)



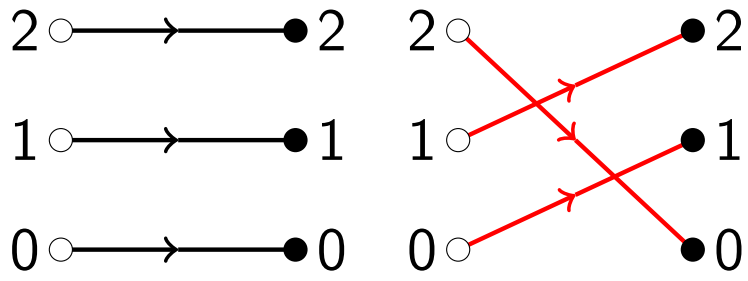
(vi)



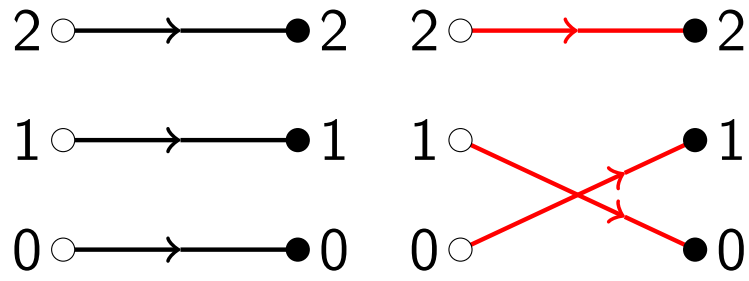
Exercise 3.3

Each diagram (i)–(vi) below each show two purported functions. Which illustrate the encryption functions in a cryptosystem with two keys (one **black**, one **red**)? In each case $\mathcal{P}$ is on left-hand side and $\mathcal{C} = \{0, 1, 2\}$ is on right-hand side. Next two slides gives all answers.

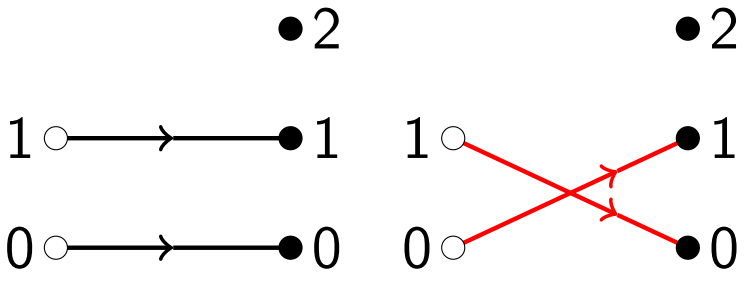
(i)



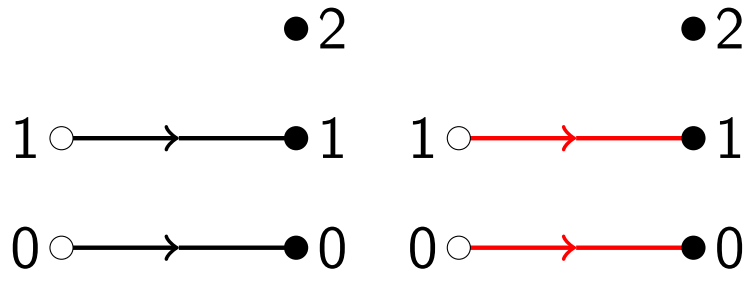
(ii)



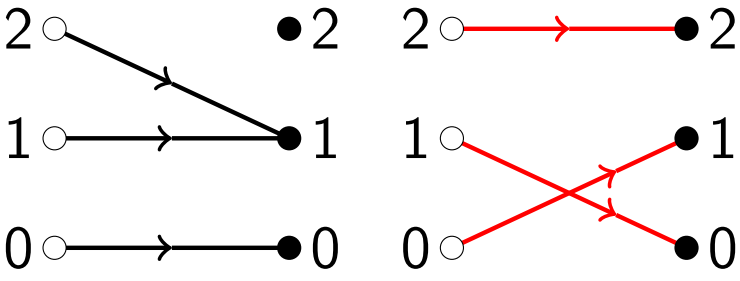
(iii)



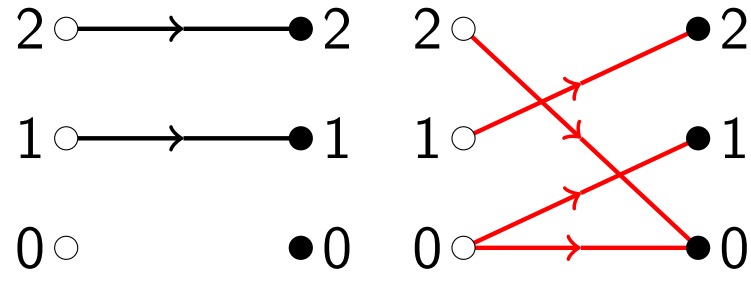
(iv)

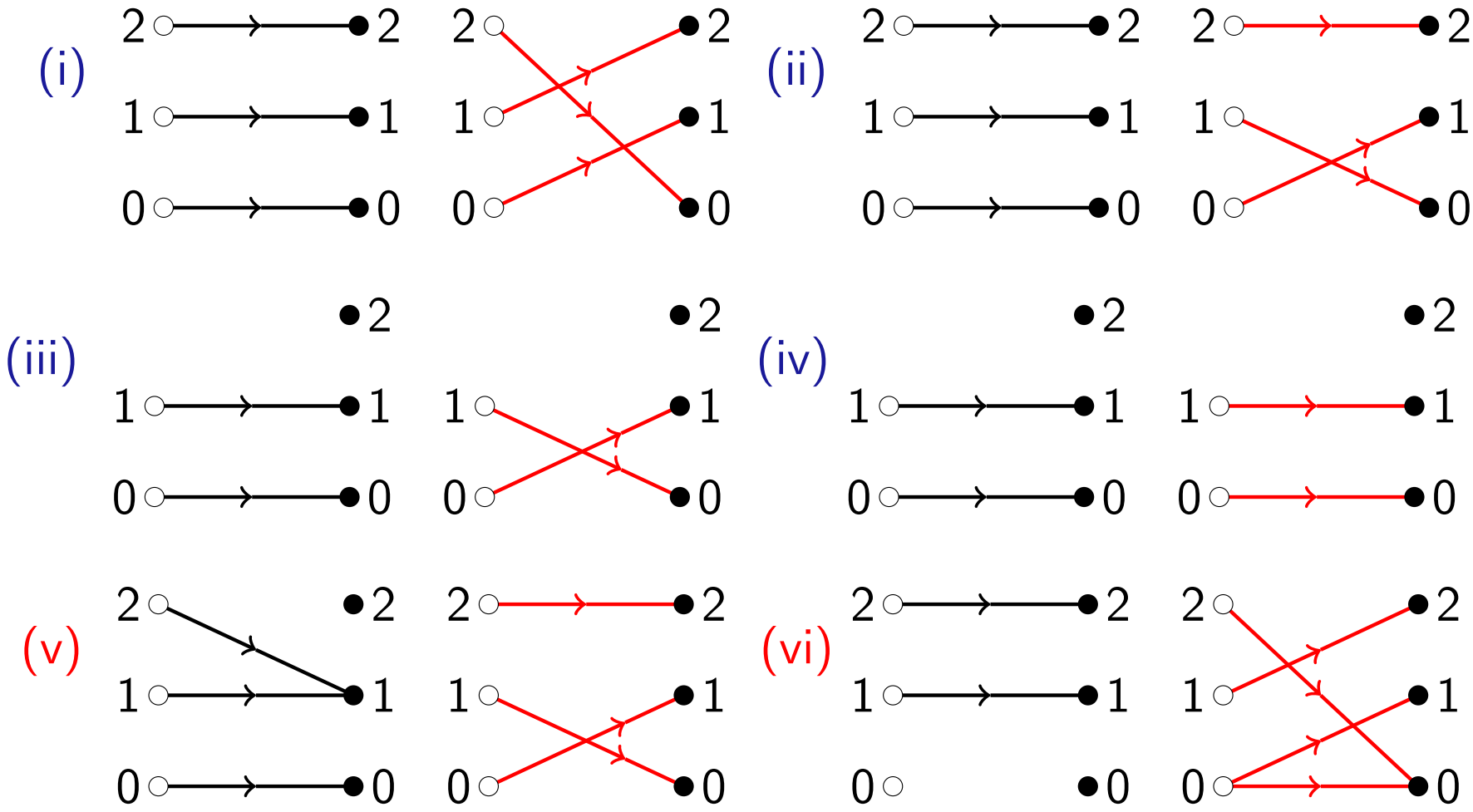


(v)



(vi)





Summary: (i), (ii), (iii) and (iv) are cryptosystems. In (iv) two keys define the same function: this is permitted. (v) is not a cryptosystem: the black encryption function is not injective, so ($\star$) does not hold. (vi) is not a cryptosystem since the black encryption function is not defined on 0. Also the red encryption function is not well-defined: what is $e_{red}(0)$? Is it 0 or is it 1?

Cryptosystems

Recall that a function $f : \mathcal{P} \to \mathcal{C}$ is *injective* if, for all $x, x' \in \mathcal{P}$, $f(x) = f(x')$ implies $x = x'$ and *surjective* if for all $y \in \mathcal{C}$ there exists $x \in \mathcal{P}$ such that $f(x) = y$.

Exercise 3.4

(i) An undergraduate writes 'For each $x \in \mathcal{P}$ there is a unique $y \in \mathcal{C}$'. Does this mean that e_k is injective?

(ii) Show that if $|\mathcal{P}| = |\mathcal{C}|$ then the encryption functions are bijections and $d_k = e_k^{-1}$ for each $k \in \mathcal{K}$.

(iii) Is there a cryptosystem with $|\mathcal{C}| < |\mathcal{P}|$?

Cryptosystems

Recall that a function $f : \mathcal{P} \to \mathcal{C}$ is *injective* if, for all $x, x' \in \mathcal{P}$, $f(x) = f(x')$ implies $x = x'$ and *surjective* if for all $y \in \mathcal{C}$ there exists $x \in \mathcal{P}$ such that $f(x) = y$.

Quiz: True or false? In any cryptosystem . . .

(a) the encryption functions $e_k : \mathcal{P} \to \mathcal{C}$ determine the decryption functions.

(A) False (B) True

(b) the decryption functions $d_k : \mathcal{C} \to \mathcal{P}$ are surjective

(A) False (B) True

(c) if $k \in \mathcal{K}$ and x, x' are distinct plaintexts then $e_k(x) \neq e_k(x')$.

(A) False (B) True

(d) if $x \in \mathcal{P}$ and k, k' are distinct keys then $e_k(x) \neq e_{k'}(x)$.

(A) False (B) True

(e) If $e_k(x) = e_{k'}(x')$ and $x \neq x'$ then $k \neq k'$.

(A) False (B) True

Cryptosystems

Recall that a function $f : \mathcal{P} \to \mathcal{C}$ is *injective* if, for all $x, x' \in \mathcal{P}$, $f(x) = f(x')$ implies $x = x'$ and *surjective* if for all $y \in \mathcal{C}$ there exists $x \in \mathcal{P}$ such that $f(x) = y$.

Quiz: True or false? In any cryptosystem . . .

(a) the encryption functions $e_k : \mathcal{P} \to \mathcal{C}$ determine the decryption functions.

(A) False (B) True

(b) the decryption functions $d_k : \mathcal{C} \to \mathcal{P}$ are surjective

(A) False (B) True

(c) if $k \in \mathcal{K}$ and x, x' are distinct plaintexts then $e_k(x) \neq e_k(x')$.

(A) False (B) True

(d) if $x \in \mathcal{P}$ and k, k' are distinct keys then $e_k(x) \neq e_{k'}(x)$.

(A) False (B) True

(e) If $e_k(x) = e_{k'}(x')$ and $x \neq x'$ then $k \neq k'$.

(A) False (B) True

Cryptosystems

Recall that a function $f : \mathcal{P} \to \mathcal{C}$ is *injective* if, for all $x, x' \in \mathcal{P}$, $f(x) = f(x')$ implies $x = x'$ and *surjective* if for all $y \in \mathcal{C}$ there exists $x \in \mathcal{P}$ such that $f(x) = y$.

Quiz: True or false? In any cryptosystem . . .

(a) the encryption functions $e_k : \mathcal{P} \to \mathcal{C}$ determine the decryption functions.

(A) False (B) True

(b) the decryption functions $d_k : \mathcal{C} \to \mathcal{P}$ are surjective

(A) False (B) True

(c) if $k \in \mathcal{K}$ and x, x' are distinct plaintexts then $e_k(x) \neq e_k(x')$.

(A) False (B) True

(d) if $x \in \mathcal{P}$ and k, k' are distinct keys then $e_k(x) \neq e_{k'}(x)$.

(A) False (B) True

(e) If $e_k(x) = e_{k'}(x')$ and $x \neq x'$ then $k \neq k'$.

(A) False (B) True

Cryptosystems

Recall that a function $f : \mathcal{P} \to \mathcal{C}$ is *injective* if, for all $x, x' \in \mathcal{P}$, $f(x) = f(x')$ implies $x = x'$ and *surjective* if for all $y \in \mathcal{C}$ there exists $x \in \mathcal{P}$ such that $f(x) = y$.

Quiz: True or false? In any cryptosystem . . .

(a) the encryption functions $e_k : \mathcal{P} \to \mathcal{C}$ determine the decryption functions.

(A) False (B) True

(b) the decryption functions $d_k : \mathcal{C} \to \mathcal{P}$ are surjective

(A) False (B) True

(c) if $k \in \mathcal{K}$ and x, x' are distinct plaintexts then $e_k(x) \neq e_k(x')$.

(A) False (B) True

(d) if $x \in \mathcal{P}$ and k, k' are distinct keys then $e_k(x) \neq e_{k'}(x)$.

(A) False (B) True

(e) If $e_k(x) = e_{k'}(x')$ and $x \neq x'$ then $k \neq k'$.

(A) False (B) True

Cryptosystems

Recall that a function $f : \mathcal{P} \to \mathcal{C}$ is *injective* if, for all $x, x' \in \mathcal{P}$, $f(x) = f(x')$ implies $x = x'$ and *surjective* if for all $y \in \mathcal{C}$ there exists $x \in \mathcal{P}$ such that $f(x) = y$.

Quiz: True or false? In any cryptosystem . . .

(a) the encryption functions $e_k : \mathcal{P} \to \mathcal{C}$ determine the decryption functions.

(A) False (B) True

(b) the decryption functions $d_k : \mathcal{C} \to \mathcal{P}$ are surjective

(A) False (B) True

(c) if $k \in \mathcal{K}$ and x, x' are distinct plaintexts then $e_k(x) \neq e_k(x')$.

(A) False (B) True

(d) if $x \in \mathcal{P}$ and k, k' are distinct keys then $e_k(x) \neq e_{k'}(x)$.

(A) False (B) True

(e) If $e_k(x) = e_{k'}(x')$ and $x \neq x'$ then $k \neq k'$.

(A) False (B) True

Cryptosystems

Recall that a function $f : \mathcal{P} \to \mathcal{C}$ is *injective* if, for all $x, x' \in \mathcal{P}$, $f(x) = f(x')$ implies $x = x'$ and *surjective* if for all $y \in \mathcal{C}$ there exists $x \in \mathcal{P}$ such that $f(x) = y$.

Quiz: True or false? In any cryptosystem . . .

(a) the encryption functions $e_k : \mathcal{P} \to \mathcal{C}$ determine the decryption functions.

(A) False (B) True

(b) the decryption functions $d_k : \mathcal{C} \to \mathcal{P}$ are surjective

(A) False (B) True

(c) if $k \in \mathcal{K}$ and x, x' are distinct plaintexts then $e_k(x) \neq e_k(x')$.

(A) False (B) True

(d) if $x \in \mathcal{P}$ and k, k' are distinct keys then $e_k(x) \neq e_{k'}(x)$.

(A) False (B) True

(e) If $e_k(x) = e_{k'}(x')$ and $x \neq x'$ then $k \neq k'$.

(A) False (B) True

Numeric one-time pad

Example 3.5 (Numeric one-time pad)

Fix $n \in \mathbb{N}$. The *numeric one-time pad* on $\{0, 1, \ldots, n-1\}$ has $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. The encryption functions are $e_k(x) = (x + k) \bmod n$. As expected from Exercise 3.4(ii), each e_k is a bijection, and the decryption functions are $d_k = e_k^{-1}$. Explicitly, $d_k(y) = (y - k) \bmod n$.

In Example 1.2 and Sheet 1 Question 2, Alice and Bob use the numeric one-time pad with $n = 100$. The key was given to them by their trusted friend Trevor, who was equally likely to pick each key.

- Suppose that Eve observes the ciphertext 80.
- The plaintext is x if and only if the key is $(80 - x) \bmod 100$.
- Since each key is equally likely then it seems reasonable to say that Eve learns nothing about the plaintext.

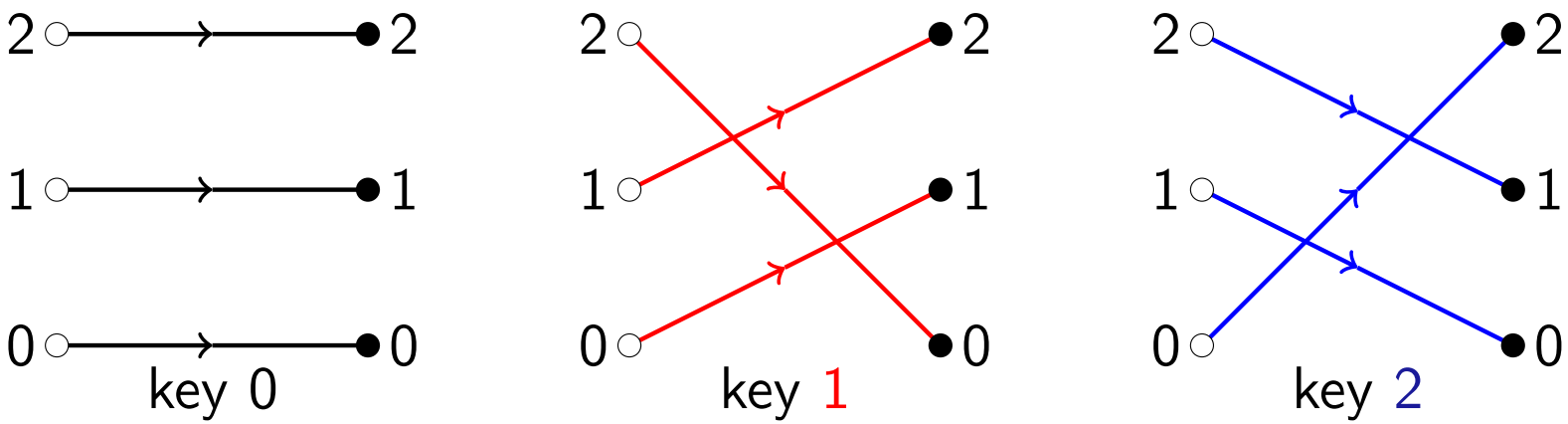
Moreover, as seen in the Group Work for Week 1, since the ciphertext is $x + k \bmod 100$, and all keys are equally likely, so are all ciphertexts.

Numeric one-time pad

Example 3.5 (Numeric one-time pad)

Fix $n \in \mathbb{N}$. The *numeric one-time pad* on $\{0, 1, \ldots, n-1\}$ has $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. The encryption functions are $e_k(x) = (x + k) \bmod n$. As expected from Exercise 3.4(ii), each e_k is a bijection, and the decryption functions are $d_k = e_k^{-1}$. Explicitly, $d_k(y) = (y - k) \bmod n$.

The diagrams before Definition 3.1 show the numeric one-time pad on $\{0, 1, 2\}$.



Probability model

Fix a cryptosystem in our usual notation. We make $\mathcal{K} \times \mathcal{P} \times \mathcal{C}$ a probability space by assuming that the plaintext $x \in \mathcal{P}$ is chosen *independently* of the key $k \in \mathcal{K}$; the ciphertext is then $e_k(x)$. Thus if p_x is the probability the plaintext is $x \in \mathcal{P}$ and r_k is the probability the key is k then the probability measure is defined by

$$p_{(k,x,y)} = \begin{cases} r_k p_x & \text{if } y = e_k(x) \\ 0 & \text{otherwise.} \end{cases}$$

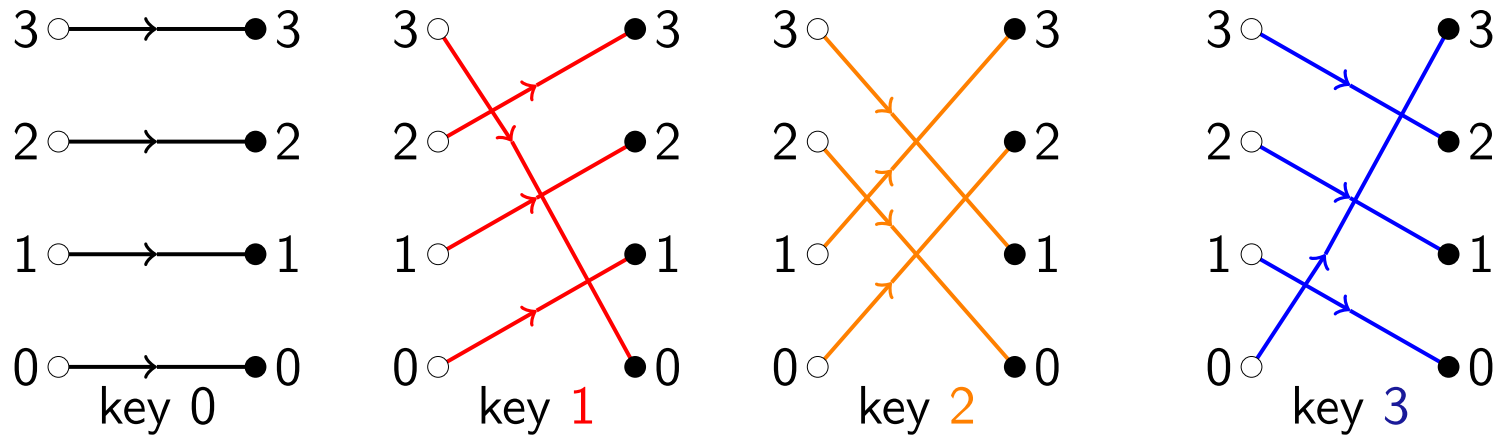
Let K, X, Y be the random variables standing for the plaintext, ciphertext and key, respectively.

Exercise 3.6

Is the assumption that the key and plaintext are independent reasonable?

Basic Quiz on Probability Model

We use the numeric one-time pad with $n = 4$ supposing that keys are equally likely and $p_0 = \frac{1}{2}, p_1 = \frac{1}{4}, p_2 = \frac{1}{6}, p_3 = \frac{1}{12}$.



(a) By assumption $r_0 = r_1 = r_2 = r_3$. What is this value?

(A) $\frac{1}{5}$ (B) $\frac{1}{4}$ (C) $\frac{1}{3}$ (D) need more information

(b) What is $\mathbb{P}[X = 2]$?

(A) $\frac{1}{2}$ (B) $\frac{1}{4}$ (C) $\frac{1}{6}$ (D) $\frac{1}{12}$

(c) What is $\mathbb{P}[K = 3]$?

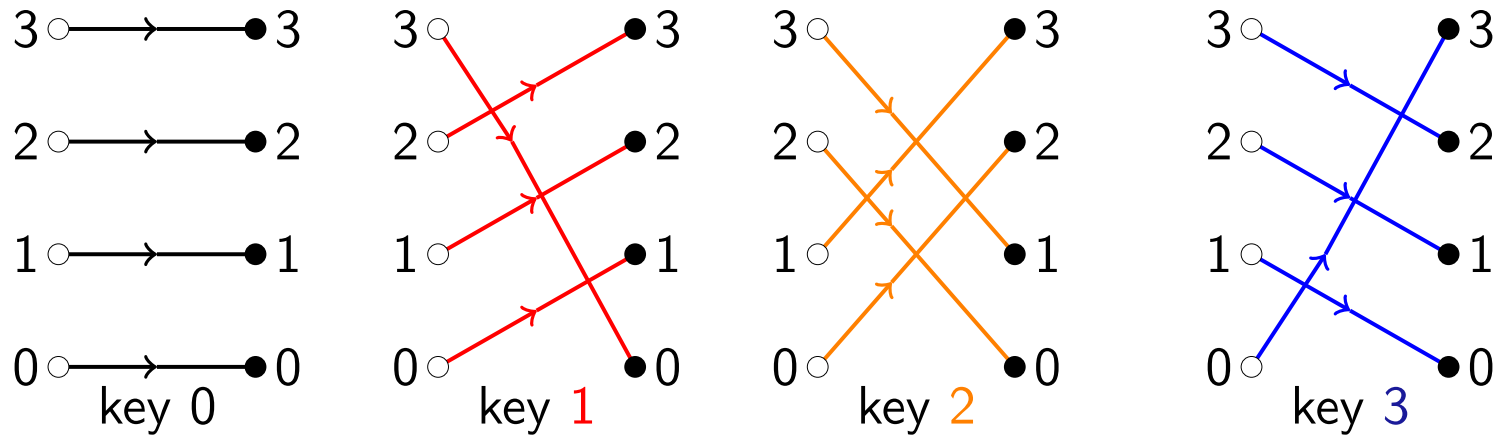
(A) $\frac{1}{5}$ (B) $\frac{1}{4}$ (C) $\frac{1}{3}$ (D) need more information

(d) What is $\mathbb{P}[X = 2 \text{ and } K = 3]$?

(A) $\frac{1}{4}$ (B) $\frac{1}{6}$ (C) $\frac{1}{12}$ (D) $\frac{1}{24}$

Basic Quiz on Probability Model

We use the numeric one-time pad with $n = 4$ supposing that keys are equally likely and $p_0 = \frac{1}{2}, p_1 = \frac{1}{4}, p_2 = \frac{1}{6}, p_3 = \frac{1}{12}$.



(a) By assumption $r_0 = r_1 = r_2 = r_3$. What is this value?

(A) $\frac{1}{5}$ (B) $\frac{1}{4}$ (C) $\frac{1}{3}$ (D) need more information

(b) What is $\mathbb{P}[X = 2]$?

(A) $\frac{1}{2}$ (B) $\frac{1}{4}$ (C) $\frac{1}{6}$ (D) $\frac{1}{12}$

(c) What is $\mathbb{P}[K = 3]$?

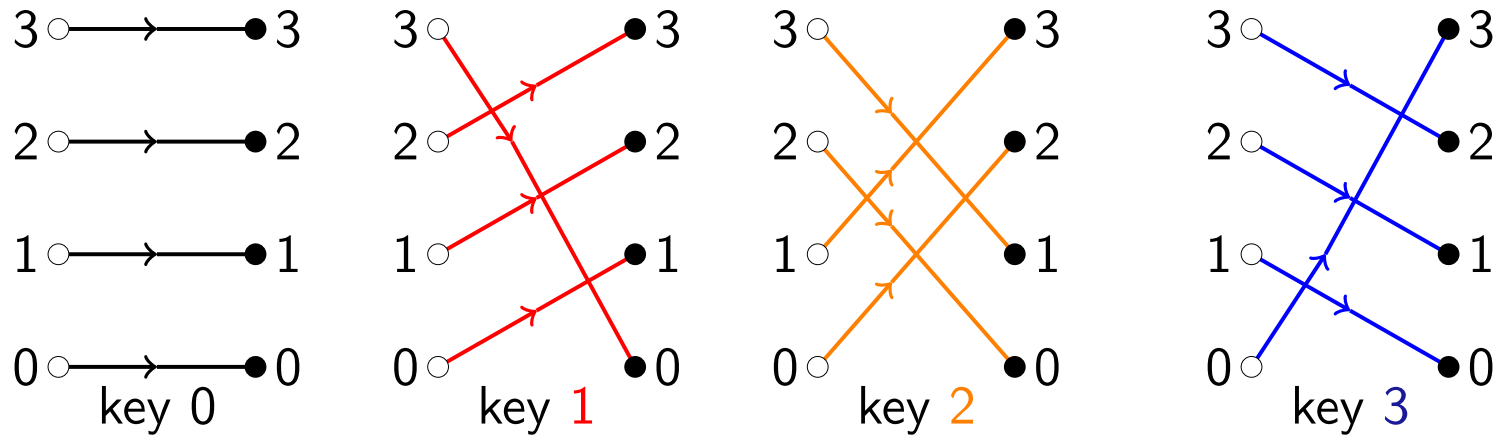
(A) $\frac{1}{5}$ (B) $\frac{1}{4}$ (C) $\frac{1}{3}$ (D) need more information

(d) What is $\mathbb{P}[X = 2 \text{ and } K = 3]$?

(A) $\frac{1}{4}$ (B) $\frac{1}{6}$ (C) $\frac{1}{12}$ (D) $\frac{1}{24}$

Basic Quiz on Probability Model

We use the numeric one-time pad with $n = 4$ supposing that keys are equally likely and $p_0 = \frac{1}{2}, p_1 = \frac{1}{4}, p_2 = \frac{1}{6}, p_3 = \frac{1}{12}$.



(a) By assumption $r_0 = r_1 = r_2 = r_3$. What is this value?

(A) $\frac{1}{5}$ (B) $\frac{1}{4}$ (C) $\frac{1}{3}$ (D) need more information

(b) What is $\mathbb{P}[X = 2]$?

(A) $\frac{1}{2}$ (B) $\frac{1}{4}$ (C) $\frac{1}{6}$ (D) $\frac{1}{12}$

(c) What is $\mathbb{P}[K = 3]$?

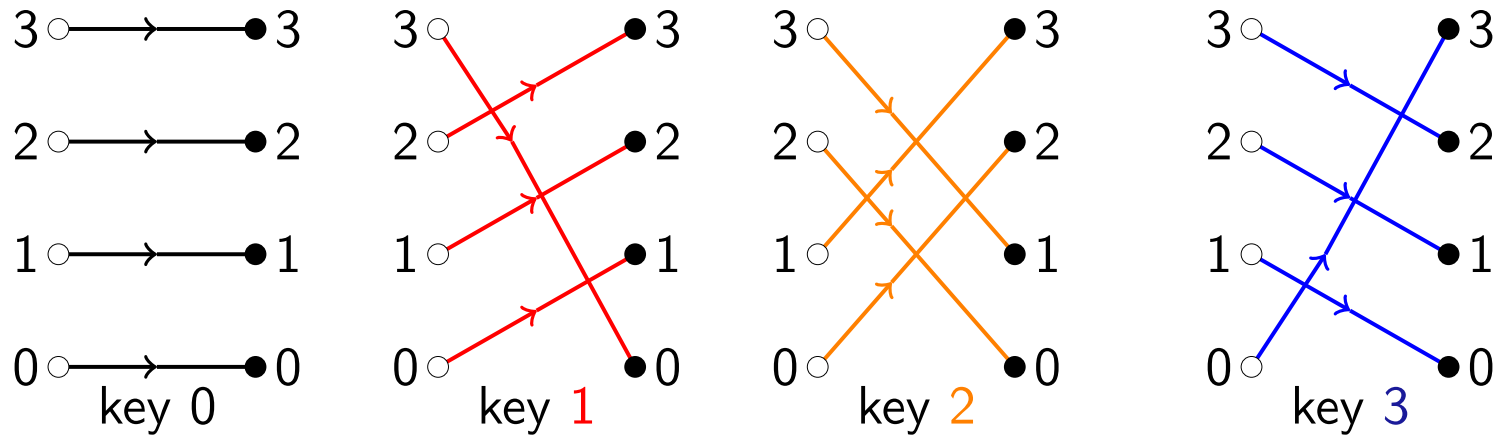
(A) $\frac{1}{5}$ (B) $\frac{1}{4}$ (C) $\frac{1}{3}$ (D) need more information

(d) What is $\mathbb{P}[X = 2 \text{ and } K = 3]$?

(A) $\frac{1}{4}$ (B) $\frac{1}{6}$ (C) $\frac{1}{12}$ (D) $\frac{1}{24}$

Basic Quiz on Probability Model

We use the numeric one-time pad with $n = 4$ supposing that keys are equally likely and $p_0 = \frac{1}{2}, p_1 = \frac{1}{4}, p_2 = \frac{1}{6}, p_3 = \frac{1}{12}$.



(a) By assumption $r_0 = r_1 = r_2 = r_3$. What is this value?

(A) $\frac{1}{5}$ (B) $\frac{1}{4}$ (C) $\frac{1}{3}$ (D) need more information

(b) What is $\mathbb{P}[X = 2]$?

(A) $\frac{1}{2}$ (B) $\frac{1}{4}$ (C) $\frac{1}{6}$ (D) $\frac{1}{12}$

(c) What is $\mathbb{P}[K = 3]$?

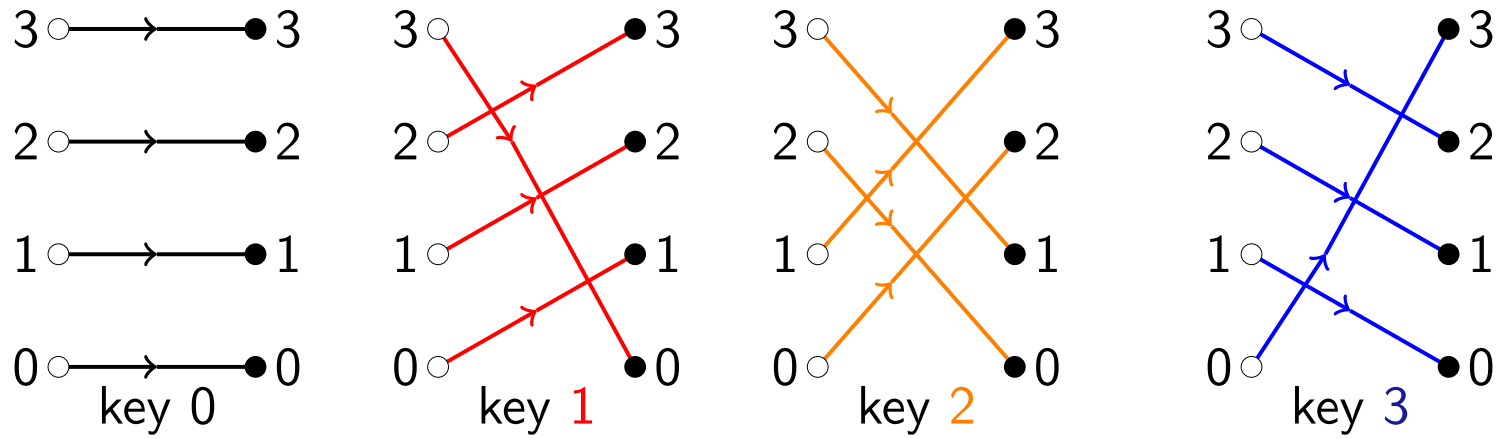
(A) $\frac{1}{5}$ (B) $\frac{1}{4}$ (C) $\frac{1}{3}$ (D) need more information

(d) What is $\mathbb{P}[X = 2 \text{ and } K = 3]$?

(A) $\frac{1}{4}$ (B) $\frac{1}{6}$ (C) $\frac{1}{12}$ (D) $\frac{1}{24}$

Basic Quiz on Probability Model

We use the numeric one-time pad with $n = 4$ supposing that keys are equally likely and $p_0 = \frac{1}{2}, p_1 = \frac{1}{4}, p_2 = \frac{1}{6}, p_3 = \frac{1}{12}$.



(a) By assumption $r_0 = r_1 = r_2 = r_3$. What is this value?

(A) $\frac{1}{5}$ (B) $\frac{1}{4}$ (C) $\frac{1}{3}$ (D) need more information

(b) What is $\mathbb{P}[X = 2]$?

(A) $\frac{1}{2}$ (B) $\frac{1}{4}$ (C) $\frac{1}{6}$ (D) $\frac{1}{12}$

(c) What is $\mathbb{P}[K = 3]$?

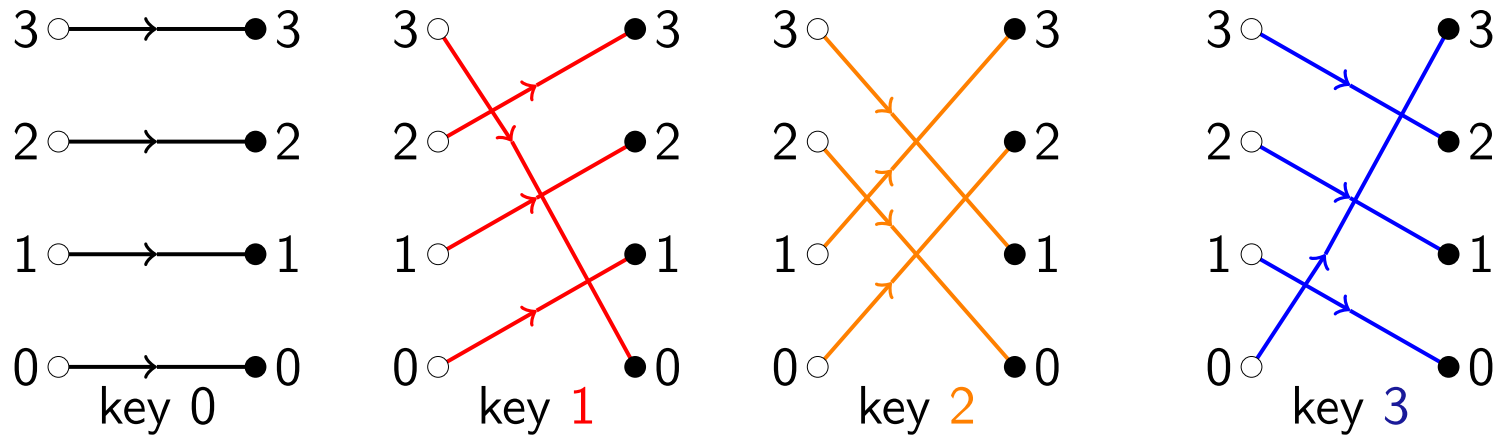
(A) $\frac{1}{5}$ (B) $\frac{1}{4}$ (C) $\frac{1}{3}$ (D) need more information

(d) What is $\mathbb{P}[X = 2 \text{ and } K = 3]$?

(A) $\frac{1}{4}$ (B) $\frac{1}{6}$ (C) $\frac{1}{12}$ (D) $\frac{1}{24}$

Basic Quiz on Probability Model

We use the numeric one-time pad with $n = 4$ supposing that keys are equally likely and $p_0 = \frac{1}{2}, p_1 = \frac{1}{4}, p_2 = \frac{1}{6}, p_3 = \frac{1}{12}$.



(e) What is $\mathbb{P}[X = 2|K = 3]$?

(A) $\frac{1}{2}$ (B) $\frac{1}{4}$ (C) $\frac{1}{6}$ (D) $\frac{1}{12}$

(f) What is $\mathbb{P}[Y = 0|X = 3]$?

(A) $\frac{1}{2}$ (B) $\frac{1}{4}$ (C) $\frac{1}{6}$ (D) $\frac{1}{12}$

(g) What is $\mathbb{P}[Y = 0]$?

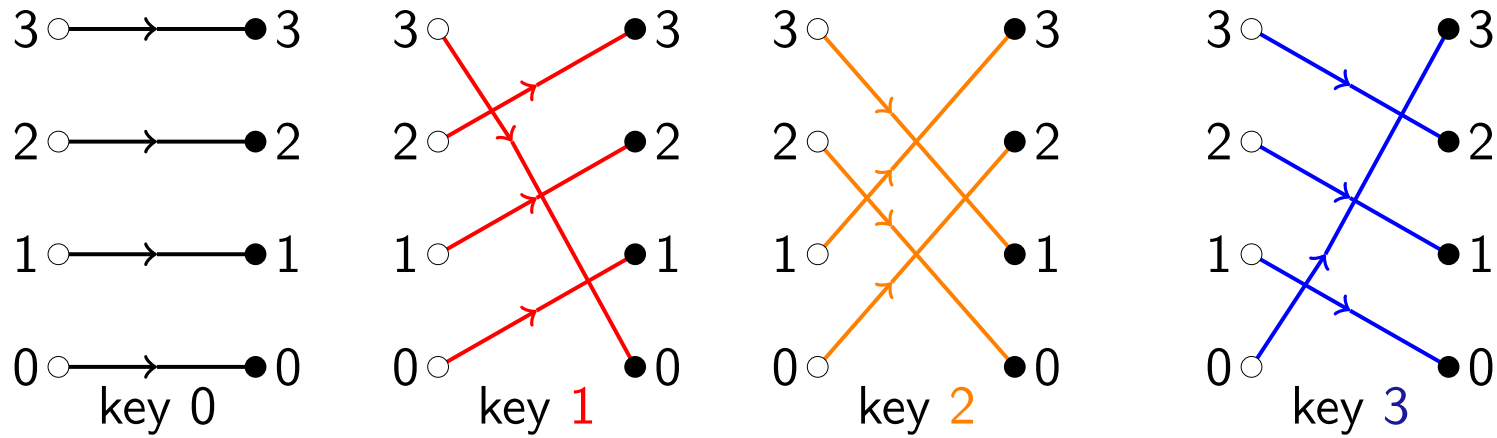
(A) $\frac{1}{2}$ (B) $\frac{1}{4}$ (C) $\frac{1}{6}$ (D) $\frac{1}{12}$

(h) What is $\mathbb{P}[X = 0 \text{ and } Y = 0]$?

(A) $\frac{1}{2}$ (B) $\frac{1}{4}$ (C) $\frac{1}{8}$ (D) $\frac{1}{16}$

Basic Quiz on Probability Model

We use the numeric one-time pad with $n = 4$ supposing that keys are equally likely and $p_0 = \frac{1}{2}, p_1 = \frac{1}{4}, p_2 = \frac{1}{6}, p_3 = \frac{1}{12}$.



(e) What is $\mathbb{P}[X = 2|K = 3]$?

(A) $\frac{1}{2}$ (B) $\frac{1}{4}$ (C) $\frac{1}{6}$ (D) $\frac{1}{12}$

(f) What is $\mathbb{P}[Y = 0|X = 3]$?

(A) $\frac{1}{2}$ (B) $\frac{1}{4}$ (C) $\frac{1}{6}$ (D) $\frac{1}{12}$

(g) What is $\mathbb{P}[Y = 0]$?

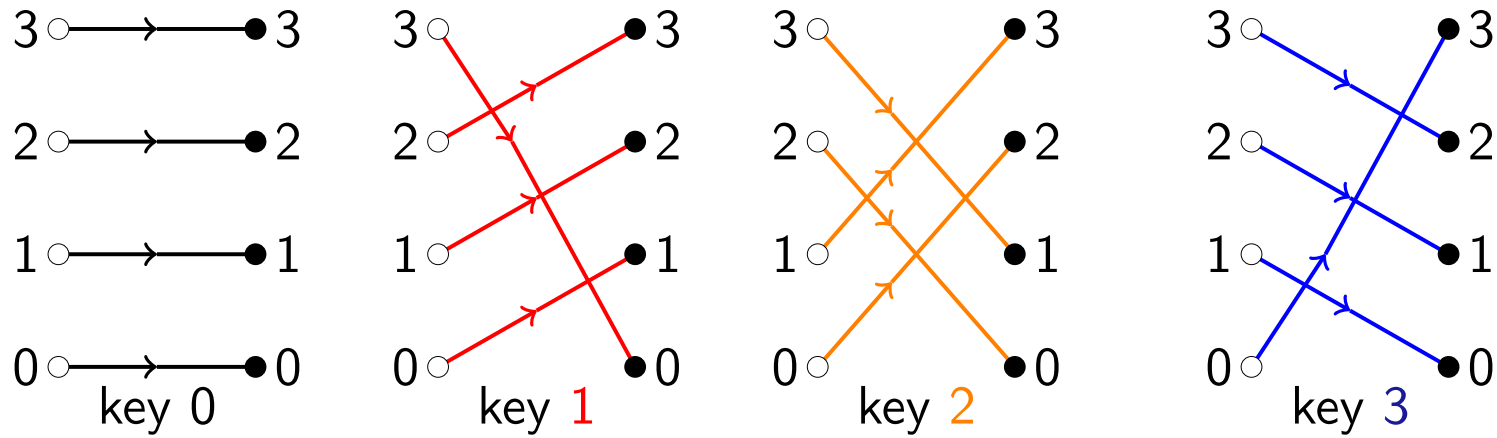
(A) $\frac{1}{2}$ (B) $\frac{1}{4}$ (C) $\frac{1}{6}$ (D) $\frac{1}{12}$

(h) What is $\mathbb{P}[X = 0 \text{ and } Y = 0]$?

(A) $\frac{1}{2}$ (B) $\frac{1}{4}$ (C) $\frac{1}{8}$ (D) $\frac{1}{16}$

Basic Quiz on Probability Model

We use the numeric one-time pad with $n = 4$ supposing that keys are equally likely and $p_0 = \frac{1}{2}, p_1 = \frac{1}{4}, p_2 = \frac{1}{6}, p_3 = \frac{1}{12}$.



(e) What is $\mathbb{P}[X = 2|K = 3]$?

(A) $\frac{1}{2}$ (B) $\frac{1}{4}$ (C) $\frac{1}{6}$ (D) $\frac{1}{12}$

(f) What is $\mathbb{P}[Y = 0|X = 3]$?

(A) $\frac{1}{2}$ (B) $\frac{1}{4}$ (C) $\frac{1}{6}$ (D) $\frac{1}{12}$

(g) What is $\mathbb{P}[Y = 0]$?

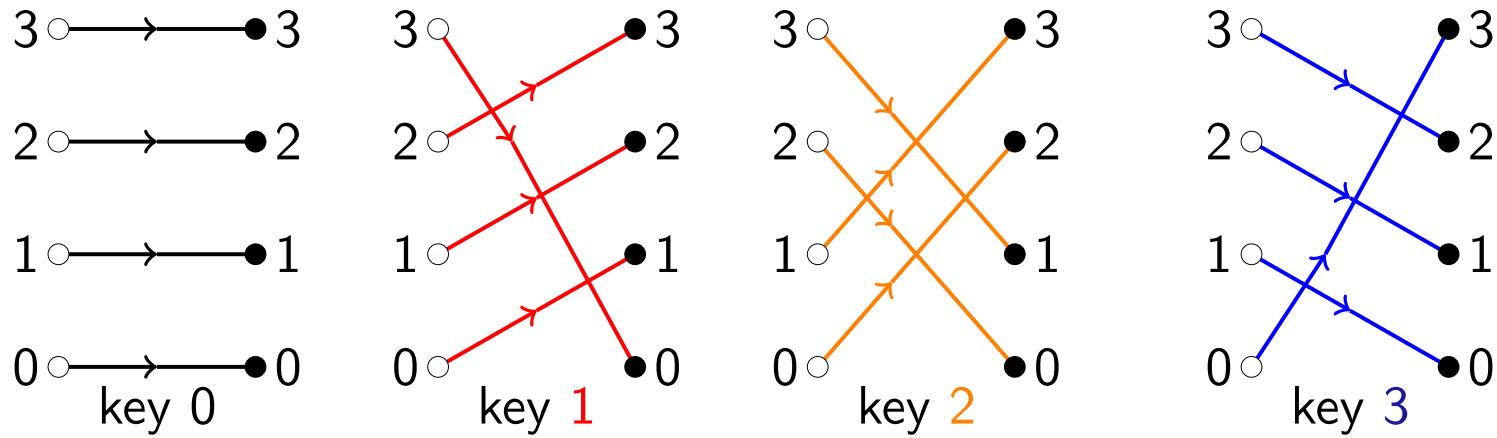
(A) $\frac{1}{2}$ (B) $\frac{1}{4}$ (C) $\frac{1}{6}$ (D) $\frac{1}{12}$

(h) What is $\mathbb{P}[X = 0 \text{ and } Y = 0]$?

(A) $\frac{1}{2}$ (B) $\frac{1}{4}$ (C) $\frac{1}{8}$ (D) $\frac{1}{16}$

Basic Quiz on Probability Model

We use the numeric one-time pad with $n = 4$ supposing that keys are equally likely and $p_0 = \frac{1}{2}, p_1 = \frac{1}{4}, p_2 = \frac{1}{6}, p_3 = \frac{1}{12}$.



(e) What is $\mathbb{P}[X = 2|K = 3]$?

(A) $\frac{1}{2}$ (B) $\frac{1}{4}$ (C) $\frac{1}{6}$ (D) $\frac{1}{12}$

(f) What is $\mathbb{P}[Y = 0|X = 3]$?

(A) $\frac{1}{2}$ (B) $\frac{1}{4}$ (C) $\frac{1}{6}$ (D) $\frac{1}{12}$

(g) What is $\mathbb{P}[Y = 0]$?

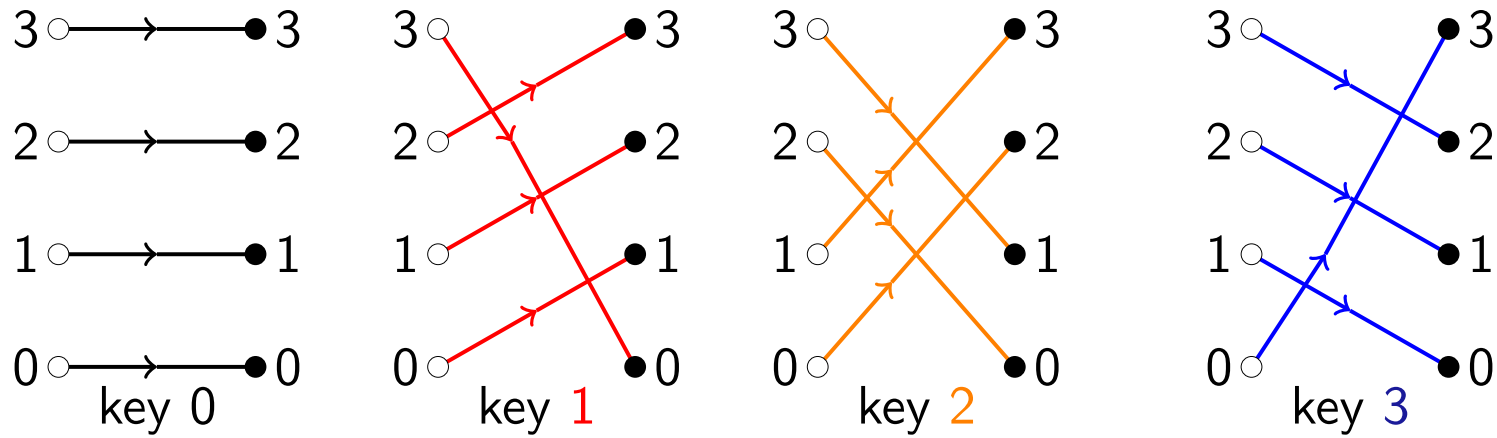
(A) $\frac{1}{2}$ (B) $\frac{1}{4}$ (C) $\frac{1}{6}$ (D) $\frac{1}{12}$

(h) What is $\mathbb{P}[X = 0 \text{ and } Y = 0]$?

(A) $\frac{1}{2}$ (B) $\frac{1}{4}$ (C) $\frac{1}{8}$ (D) $\frac{1}{16}$

Basic Quiz on Probability Model

We use the numeric one-time pad with $n = 4$ supposing that keys are equally likely and $p_0 = \frac{1}{2}, p_1 = \frac{1}{4}, p_2 = \frac{1}{6}, p_3 = \frac{1}{12}$.



(e) What is $\mathbb{P}[X = 2|K = 3]$?

(A) $\frac{1}{2}$ (B) $\frac{1}{4}$ (C) $\frac{1}{6}$ (D) $\frac{1}{12}$

(f) What is $\mathbb{P}[Y = 0|X = 3]$?

(A) $\frac{1}{2}$ (B) $\frac{1}{4}$ (C) $\frac{1}{6}$ (D) $\frac{1}{12}$

(g) What is $\mathbb{P}[Y = 0]$?

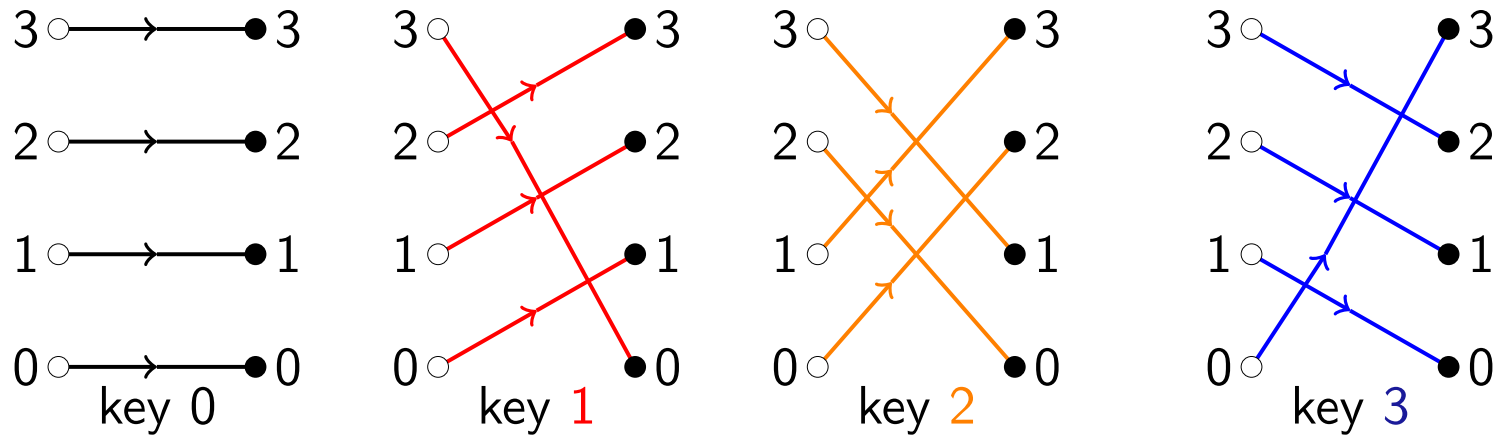
(A) $\frac{1}{2}$ (B) $\frac{1}{4}$ (C) $\frac{1}{6}$ (D) $\frac{1}{12}$

(h) What is $\mathbb{P}[X = 0 \text{ and } Y = 0]$?

(A) $\frac{1}{2}$ (B) $\frac{1}{4}$ (C) $\frac{1}{8}$ (D) $\frac{1}{16}$

Basic Quiz on Probability Model

We use the numeric one-time pad with $n = 4$ supposing that keys are equally likely and $p_0 = \frac{1}{2}, p_1 = \frac{1}{4}, p_2 = \frac{1}{6}, p_3 = \frac{1}{12}$.



Finally, decide whether each of the following probabilities is

- 'easy': you can do it in a few seconds by finding the relevant X and/or K and maybe using $\mathbb{P}[X = x, K = k] = p_x r_k$.
- 'hard': you can see you're going to have to use conditional probability and think!

(i) $\mathbb{P}[X = 2|K = 1]$? (A) Easy (B) Hard

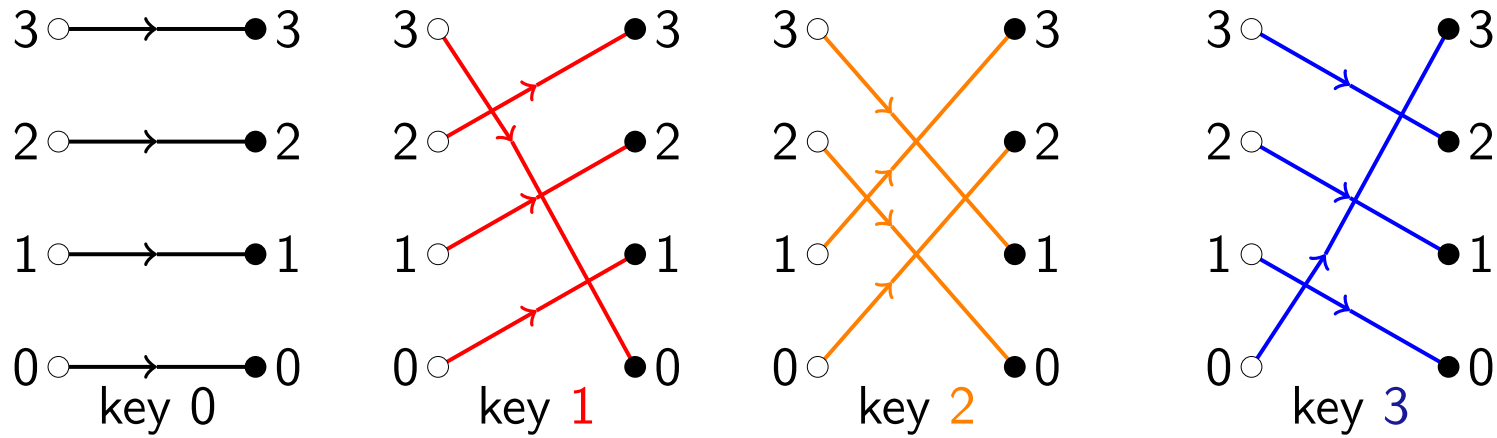
(j) $\mathbb{P}[Y = 2|X = 3]$? (A) Easy (B) Hard

(k) $\mathbb{P}[X = 3|Y = 3]$? (A) Easy (B) Hard

(l) $\mathbb{P}[K = 3|Y = 3]$? (A) Easy (B) Hard

Basic Quiz on Probability Model

We use the numeric one-time pad with $n = 4$ supposing that keys are equally likely and $p_0 = \frac{1}{2}, p_1 = \frac{1}{4}, p_2 = \frac{1}{6}, p_3 = \frac{1}{12}$.



Finally, decide whether each of the following probabilities is

- 'easy': you can do it in a few seconds by finding the relevant X and/or K and maybe using $\mathbb{P}[X = x, K = k] = p_x r_k$.
- 'hard': you can see you're going to have to use conditional probability and think!

(i) $\mathbb{P}[X = 2|K = 1]$? (A) Easy (B) Hard

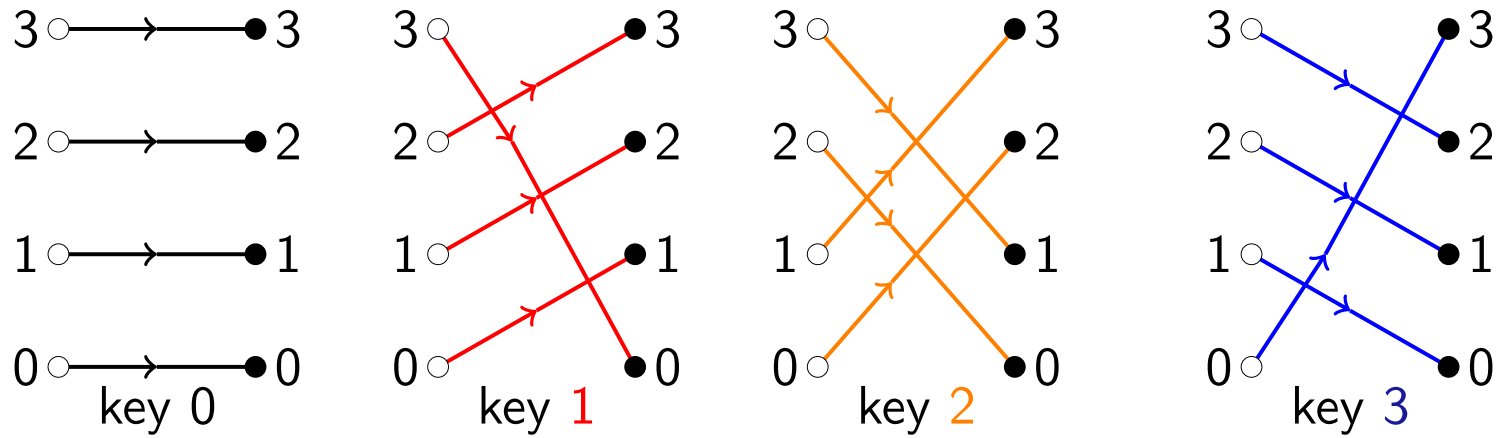
(j) $\mathbb{P}[Y = 2|X = 3]$? (A) Easy (B) Hard

(k) $\mathbb{P}[X = 3|Y = 3]$? (A) Easy (B) Hard

(l) $\mathbb{P}[K = 3|Y = 3]$? (A) Easy (B) Hard

Basic Quiz on Probability Model

We use the numeric one-time pad with $n = 4$ supposing that keys are equally likely and $p_0 = \frac{1}{2}, p_1 = \frac{1}{4}, p_2 = \frac{1}{6}, p_3 = \frac{1}{12}$.



Finally, decide whether each of the following probabilities is

- 'easy': you can do it in a few seconds by finding the relevant X and/or K and maybe using $\mathbb{P}[X = x, K = k] = p_x r_k$.
- 'hard': you can see you're going to have to use conditional probability and think!

(i) $\mathbb{P}[X = 2|K = 1]$? (A) Easy (B) Hard

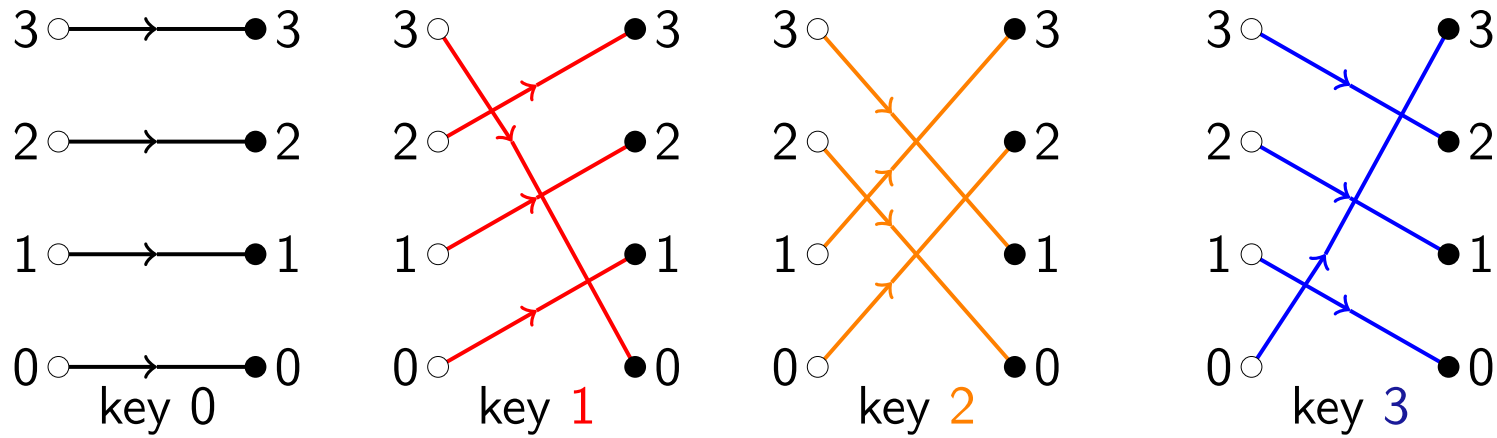
(j) $\mathbb{P}[Y = 2|X = 3]$? (A) Easy (B) Hard

(k) $\mathbb{P}[X = 3|Y = 3]$? (A) Easy (B) Hard

(l) $\mathbb{P}[K = 3|Y = 3]$? (A) Easy (B) Hard

Basic Quiz on Probability Model

We use the numeric one-time pad with $n = 4$ supposing that keys are equally likely and $p_0 = \frac{1}{2}, p_1 = \frac{1}{4}, p_2 = \frac{1}{6}, p_3 = \frac{1}{12}$.



Finally, decide whether each of the following probabilities is

- 'easy': you can do it in a few seconds by finding the relevant X and/or K and maybe using $\mathbb{P}[X = x, K = k] = p_x r_k$.
- 'hard': you can see you're going to have to use conditional probability and think!

(i) $\mathbb{P}[X = 2|K = 1]$? (A) Easy (B) Hard

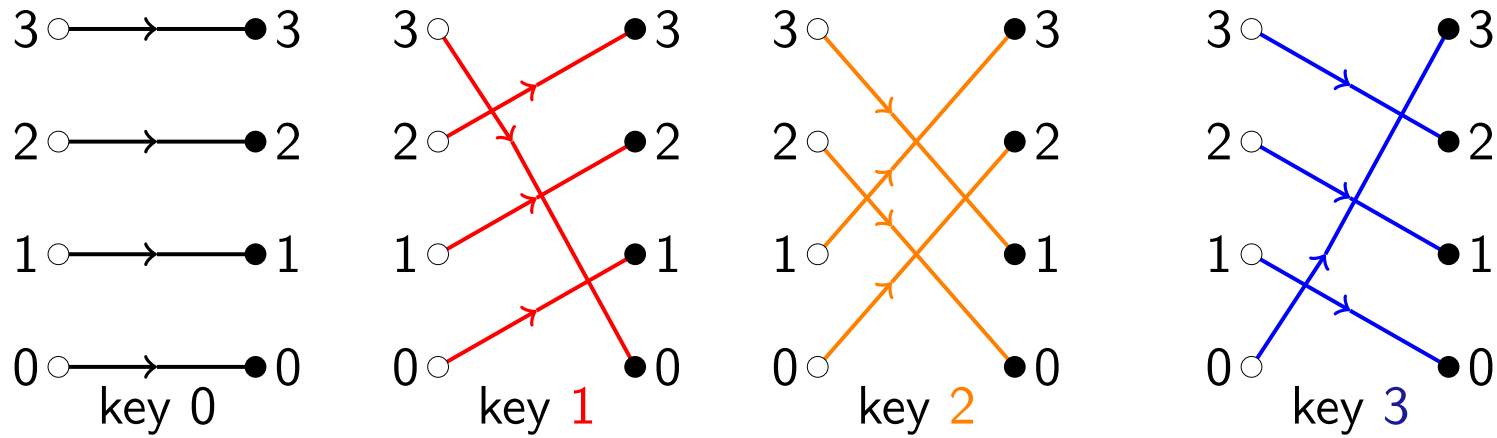
(j) $\mathbb{P}[Y = 2|X = 3]$? (A) Easy (B) Hard

(k) $\mathbb{P}[X = 3|Y = 3]$? (A) Easy (B) Hard

(l) $\mathbb{P}[K = 3|Y = 3]$? (A) Easy (B) Hard

Basic Quiz on Probability Model

We use the numeric one-time pad with $n = 4$ supposing that keys are equally likely and $p_0 = \frac{1}{2}, p_1 = \frac{1}{4}, p_2 = \frac{1}{6}, p_3 = \frac{1}{12}$.



Finally, decide whether each of the following probabilities is

- 'easy': you can do it in a few seconds by finding the relevant X and/or K and maybe using $\mathbb{P}[X = x, K = k] = p_x r_k$.
- 'hard': you can see you're going to have to use conditional probability and think!

(i) $\mathbb{P}[X = 2|K = 1]$? (A) Easy (B) Hard

(j) $\mathbb{P}[Y = 2|X = 3]$? (A) Easy (B) Hard

(k) $\mathbb{P}[X = 3|Y = 3]$? (A) Easy (B) Hard

(l) $\mathbb{P}[K = 3|Y = 3]$? (A) Easy (B) Hard

Conditional Probability: Using the Definition

We will need the formula for conditional probability:

$$\mathbb{P}[A|B] = \frac{\mathbb{P}[A \text{ and } B]}{\mathbb{P}[B]}.$$

Quiz. Let $\Omega = \{\mathrm{HH}, \mathrm{HT}, \mathrm{TH}, \mathrm{TT}\}$ be the probability space for two flips of a fair coin. What is the probability of exactly one head, given that at least one flip was a head?

(A) 2/3 (B) 1/3 (C) 1/2 (D) 1/6

Conditional Probability: Using the Definition

We will need the formula for conditional probability:

$$\mathbb{P}[A|B] = \frac{\mathbb{P}[A \text{ and } B]}{\mathbb{P}[B]}.$$

Quiz. Let $\Omega = \{\mathrm{HH}, \mathrm{HT}, \mathrm{TH}, \mathrm{TT}\}$ be the probability space for two flips of a fair coin. What is the probability of exactly one head, given that at least one flip was a head?

(A) 2/3 (B) 1/3 (C) 1/2 (D) 1/6

Conditional Probability: Using the Definition

We will need the formula for conditional probability:

$$\mathbb{P}[A|B] = \frac{\mathbb{P}[A \text{ and } B]}{\mathbb{P}[B]}.$$

Quiz. Let $\Omega = \{\mathrm{HH}, \mathrm{HT}, \mathrm{TH}, \mathrm{TT}\}$ be the probability space for two flips of a fair coin. What is the probability of exactly one head, given that at least one flip was a head?

(A) 2/3 (B) 1/3 (C) 1/2 (D) 1/6

Using the definition of conditional probability, this is proved by

$$\mathbb{P}[\{\mathrm{HT}, \mathrm{TH}\}|\{\mathrm{HH}, \mathrm{HT}, \mathrm{TH}\}] = \frac{\mathbb{P}[\{\mathrm{HT}, \mathrm{TH}\} \cap \{\mathrm{HH}, \mathrm{HT}, \mathrm{TH}\}]}{\mathbb{P}[\{\mathrm{HH}, \mathrm{HT}, \mathrm{TH}\}]}$$

$$= \frac{\mathbb{P}[\{\mathrm{HT}, \mathrm{TH}\}]}{\mathbb{P}[\{\mathrm{HH}, \mathrm{HT}, \mathrm{TH}\}]} = \frac{\frac{1}{4} + \frac{1}{4}}{\frac{1}{4} + \frac{1}{4} + \frac{1}{4}} = \frac{\frac{2}{4}}{\frac{3}{4}} = \frac{2}{3}$$

Conditional Probability: Using the Definition

We will need the formula for conditional probability:

$$\mathbb{P}[A|B] = \frac{\mathbb{P}[A \text{ and } B]}{\mathbb{P}[B]}.$$

Quiz. Let $\Omega = \{\mathrm{HH}, \mathrm{HT}, \mathrm{TH}, \mathrm{TT}\}$ be the probability space for two flips of a fair coin. What is the probability of exactly one head, given that at least one flip was a head?

(A) 2/3 (B) 1/3 (C) 1/2 (D) 1/6

Using the definition of conditional probability, this is proved by

$$\mathbb{P}[\{\mathrm{HT}, \mathrm{TH}\}|\{\mathrm{HH}, \mathrm{HT}, \mathrm{TH}\}] = \frac{\mathbb{P}[\{\mathrm{HT}, \mathrm{TH}\} \cap \{\mathrm{HH}, \mathrm{HT}, \mathrm{TH}\}]}{\mathbb{P}[\{\mathrm{HH}, \mathrm{HT}, \mathrm{TH}\}]}$$

$$= \frac{\mathbb{P}[\{\mathrm{HT}, \mathrm{TH}\}]}{\mathbb{P}[\{\mathrm{HH}, \mathrm{HT}, \mathrm{TH}\}]} = \frac{\frac{1}{4} + \frac{1}{4}}{\frac{1}{4} + \frac{1}{4} + \frac{1}{4}} = \frac{\frac{2}{4}}{\frac{3}{4}} = \frac{2}{3}$$

See the 'Treasure Island' video for a similar example, and the alternative approach by restricting the probability space. Here we would restrict to $\{\mathrm{HH}, \mathrm{HT}, \mathrm{TH}\}$ and define $\overline{p}_{\mathrm{HH}} = p_{\mathrm{HH}}/\mathbb{P}[\{\mathrm{HH}, \mathrm{HT}, \mathrm{TH}\}] = \frac{1}{4}/\frac{3}{4} = \frac{1}{3}$, and so on. Hence the quiz probability is $\overline{p}_{\mathrm{HT}} + \overline{p}_{\mathrm{TH}} = \frac{1}{3} + \frac{1}{3} = \frac{2}{3}$.

Conditional Probability: Conditioning

Just to remind you how it works, the table below shows the encryption of `notthatagain` using the Vigenére key `abc`.

i	0	1	2	3	4	5	6	7	8	9	10	11
x_i	n	o	t	t	h	a	t	a	g	a	i	n
	13	14	19	19	7	0	19	0	6	0	8	13
k_i	a	b	c	a	b	c	a	b	c	a	b	c
	0	1	2	0	1	2	0	1	2	0	1	2
$x_i + k_i$	13	15	21	19	8	2	19	1	8	0	9	15
	N	P	V	T	I	C	T	B	I	A	J	P

Given that the letters `c`, `d`, `e` appear in English with percentage probabilities, 2.8%, 4.3%, 12.7%, what percentage of ciphertext letters do you expect to be `E`?

(A) 5.4% (B) 6.6% (C) 8.5% (D) 12.7%

[*Hint:* condition on the position of the ciphertext letter modulo 3.]

Conditional Probability: Conditioning

Just to remind you how it works, the table below shows the encryption of `notthatagain` using the Vigenére key `abc`.

i	0	1	2	3	4	5	6	7	8	9	10	11
x_i	n	o	t	t	h	a	t	a	g	a	i	n
	13	14	19	19	7	0	19	0	6	0	8	13
k_i	a	b	c	a	b	c	a	b	c	a	b	c
	0	1	2	0	1	2	0	1	2	0	1	2
$x_i + k_i$	13	15	21	19	8	2	19	1	8	0	9	15
	N	P	V	T	I	C	T	B	I	A	J	P

Given that the letters `c`, `d`, `e` appear in English with percentage probabilities, 2.8%, 4.3%, 12.7%, what percentage of ciphertext letters do you expect to be `E`?

(A) 5.4% (B) 6.6% (C) 8.5% (D) 12.7%

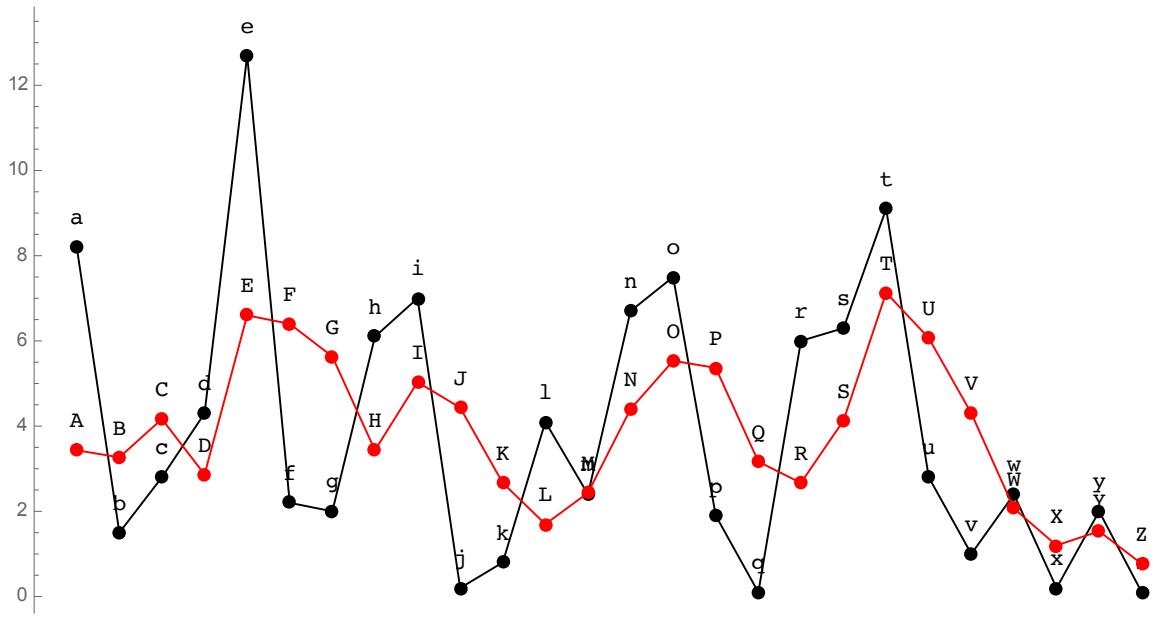
[*Hint:* condition on the position of the ciphertext letter modulo 3.]

Conditional Probability: Conditioning

Thus the probability of E is the average probability of c, d, e,

$$\frac{2.8\% + 4.3\% + 12.7\%}{3} = 6.6\%.$$

The graph below shows this average for all ciphertext letters (red line), compared with English probability distribution (black line).



For instance, the frequency of E is 6.6%. See Example 2.11 and later for how we use this with the IOC to guess the key length.

Question: why are F, and G *more* frequent in a typical ciphertext than f and g are in a typical plaintext?

Conditional Probability: a Girl called Alice

This is an optional challenge, generalizing a problem set in the Guardian:

`https://www.theguardian.com/science/2019/nov/18/can-you-solve-it-the-two-child-problem`

Suppose that $\frac{1}{2}$ of all children are girls, and of all girls, a proportion p are called Alice.

- Imagine I tell you 'I have exactly two children and one is a girl called Alice'. What is the probability I have two girls?

(A) $\frac{1}{3}$ (B) $\frac{1}{3}p$ (C) $\frac{2+p}{4+p}$ (D) $\frac{2-p}{4-p}$

Conditional Probability: a Girl called Alice

This is an optional challenge, generalizing a problem set in the Guardian:

`https://www.theguardian.com/science/2019/nov/18/can-you-solve-it-the-two-child-problem`

Suppose that $\frac{1}{2}$ of all children are girls, and of all girls, a proportion p are called Alice.

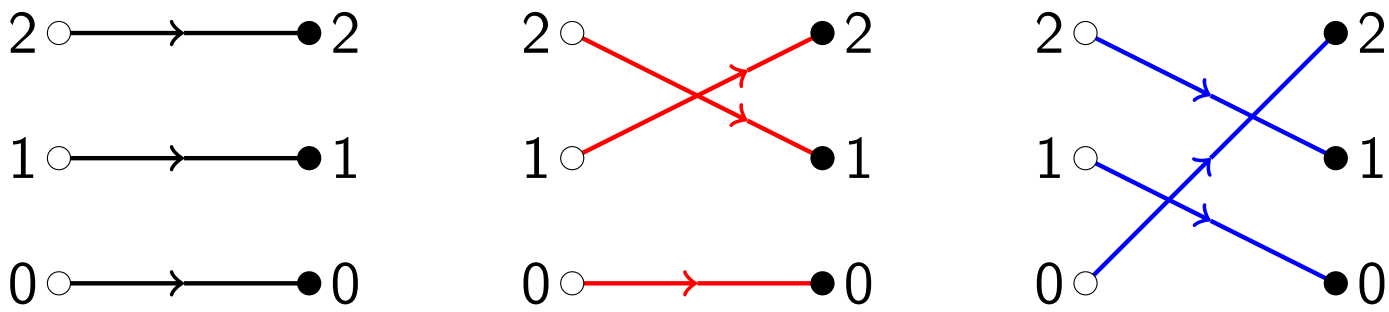
- Imagine I tell you 'I have exactly two children and one is a girl called Alice'. What is the probability I have two girls?

(A) $\frac{1}{3}$ (B) $\frac{1}{3}p$ (C) $\frac{2+p}{4+p}$ (D) $\frac{2-p}{4-p}$

To think about: Is it intuitive that if p is very small then the probability is nearly $\frac{1}{2}$, and if p is nearly 1 (so all girls are called Alice) then the probability is nearly $\frac{1}{3}$?

Probability Model: Example 3.7

Consider the cryptosystem below.



Let $P[K = \text{black}] = r_{\text{black}}$, $P[K = \text{red}] = r_{\text{red}}$, $\mathbb{P}[K = \text{blue}] = r_{\text{blue}}$.

(1) What is $\mathbb{P}[Y = 1|X = 2]$?

(A) r_{red} (B) r_{blue} (C) $r_{\text{red}} + r_{\text{blue}}$ (D) $r_{\text{black}} + r_{\text{red}}$

(2) Suppose that the three keys are used with equal probability $\frac{1}{3}$, and that $p_1 = 1 - q$, $p_2 = q$ so $p_0 = 0$.

What is $\mathbb{P}[Y = 1]$? [*Hint:* condition on the plaintext.]

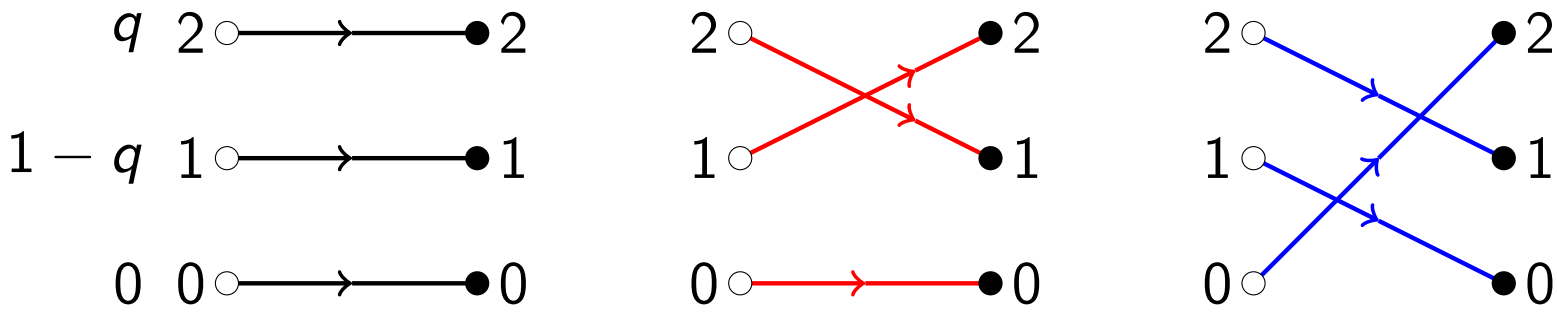
(A) $\frac{1+q}{3}$ (B) $\frac{1-q}{3}$ (C) $\frac{1+2q}{3}$ (D) $\frac{1}{3}$

What is $\mathbb{P}[X = 2|Y = 1]$?

(A) $\frac{2}{3}$ (B) $\frac{2}{3}q$ (C) $\frac{2q}{1+q}$ (D) $\frac{q}{1+q}$

Probability Model: Example 3.7

Consider the cryptosystem below.



Let $P[K = \text{black}] = r_{\text{black}}$, $P[K = \text{red}] = r_{\text{red}}$, $\mathbb{P}[K = \text{blue}] = r_{\text{blue}}$.

(1) What is $\mathbb{P}[Y = 1|X = 2]$?

(A) r_{red} (B) r_{blue} (C) $r_{\text{red}} + r_{\text{blue}}$ (D) $r_{\text{black}} + r_{\text{red}}$

(2) Suppose that the three keys are used with equal probability $\frac{1}{3}$, and that $p_1 = 1 - q$, $p_2 = q$ so $p_0 = 0$.

What is $\mathbb{P}[Y = 1]$? [*Hint:* condition on the plaintext.]

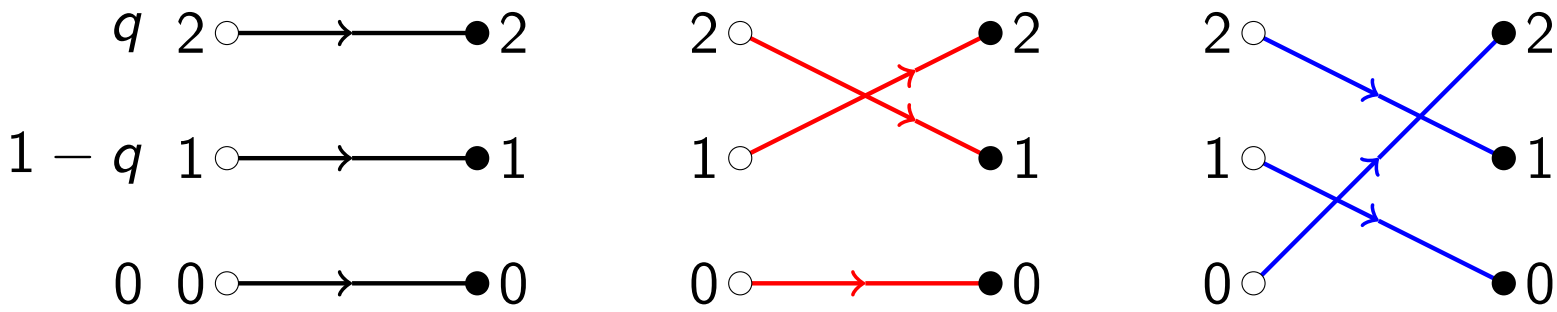
(A) $\frac{1+q}{3}$ (B) $\frac{1-q}{3}$ (C) $\frac{1+2q}{3}$ (D) $\frac{1}{3}$

What is $\mathbb{P}[X = 2|Y = 1]$?

(A) $\frac{2}{3}$ (B) $\frac{2}{3}q$ (C) $\frac{2q}{1+q}$ (D) $\frac{q}{1+q}$

Probability Model: Example 3.7

Consider the cryptosystem below.



Let $P[K = \text{black}] = r_{\text{black}}$, $P[K = \text{red}] = r_{\text{red}}$, $\mathbb{P}[K = \text{blue}] = r_{\text{blue}}$.

(1) What is $\mathbb{P}[Y = 1|X = 2]$?

(A) r_{red} (B) r_{blue} (C) $r_{\text{red}} + r_{\text{blue}}$ (D) $r_{\text{black}} + r_{\text{red}}$

(2) Suppose that the three keys are used with equal probability $\frac{1}{3}$, and that $p_1 = 1 - q$, $p_2 = q$ so $p_0 = 0$.

What is $\mathbb{P}[Y = 1]$? [*Hint:* condition on the plaintext.]

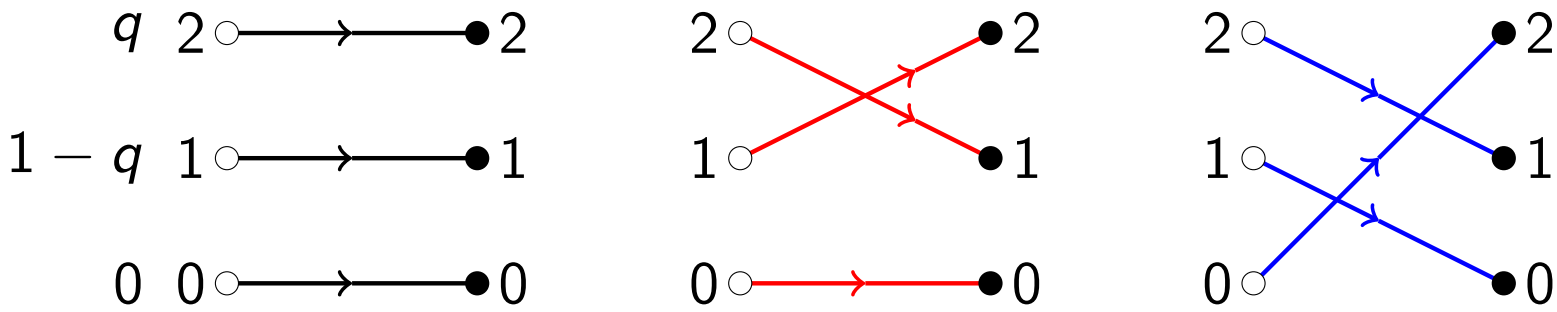
(A) $\frac{1+q}{3}$ (B) $\frac{1-q}{3}$ (C) $\frac{1+2q}{3}$ (D) $\frac{1}{3}$

What is $\mathbb{P}[X = 2|Y = 1]$?

(A) $\frac{2}{3}$ (B) $\frac{2}{3}q$ (C) $\frac{2q}{1+q}$ (D) $\frac{q}{1+q}$

Probability Model: Example 3.7

Consider the cryptosystem below.



Let $P[K = \text{black}] = r_{\text{black}}$, $P[K = \text{red}] = r_{\text{red}}$, $\mathbb{P}[K = \text{blue}] = r_{\text{blue}}$.

(1) What is $\mathbb{P}[Y = 1|X = 2]$?

(A) r_{red} (B) r_{blue} (C) $r_{\text{red}} + r_{\text{blue}}$ (D) $r_{\text{black}} + r_{\text{red}}$

(2) Suppose that the three keys are used with equal probability $\frac{1}{3}$, and that $p_1 = 1 - q$, $p_2 = q$ so $p_0 = 0$.

What is $\mathbb{P}[Y = 1]$? [*Hint:* condition on the plaintext.]

(A) $\frac{1+q}{3}$ (B) $\frac{1-q}{3}$ (C) $\frac{1+2q}{3}$ (D) $\frac{1}{3}$

What is $\mathbb{P}[X = 2|Y = 1]$?

(A) $\frac{2}{3}$ (B) $\frac{2}{3}q$ (C) $\frac{2q}{1+q}$ (D) $\frac{q}{1+q}$

Warm-up for Quiz on Probability Model

In Example 3.7 we saw the key calculation using conditional probability (or Bayes' Theorem if you prefer):

$$\mathbb{P}[X = x|Y = y] = \frac{\mathbb{P}[Y = y|X = x]\mathbb{P}[X = x]}{\mathbb{P}[Y = y]} \text{ [Corrected]}$$

Here, and in general, $\mathbb{P}[Y = y|X = x] = \sum_{k\in\mathcal{K}\,:\,e_k(x)=y} \mathbb{P}[K = k]$ is a sum of key probabilities: we saw $\mathbb{P}[Y = 1|X = 2] = r_{\text{red}} + r_{\text{blue}}$.

Bluffers' guide:

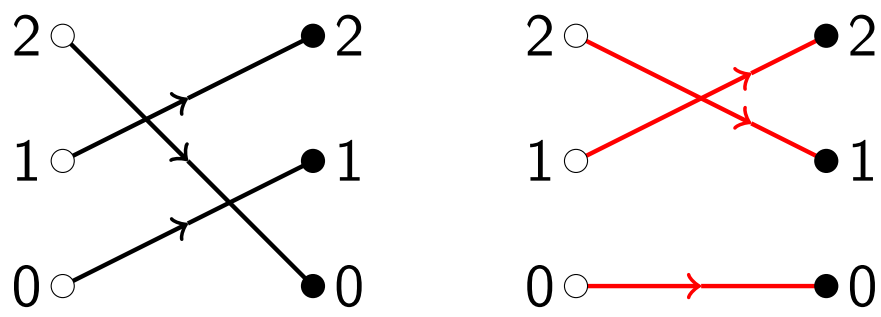
- if you see $\mathbb{P}[Y = y|X = x]$ think '**nice**: key probability';
- if you see $\mathbb{P}[X = x|Y = y]$ think '**nasty**, turn it around'

Curious fact:

- $\mathbb{P}[X = x|Y = y]$ is what we most care about: think 'What can I infer about the plaintext, **given** I've seen a ciphertext y'
- $\mathbb{P}[Y = y|X = x]$ is the thing that is most easy to compute.

Quiz on Probability Model for Cryptosystems

In the cryptosystem below, the red key is used with probability r.
In symbols: $\mathbb{P}[K = \textit{red}] = r$.



Suppose the plaintexts are sent with probabilities p_0, p_1 and p_2.

- What is the probability distribution of Y, conditioned on $X = 0$? Equivalently, what is

$$(\mathbb{P}[Y = 0|X = 0], \mathbb{P}[Y = 1|X = 0], \mathbb{P}[Y = 2|X = 0])?$$

(A) $(r, 1-r, 0)$ (B) $(p_0 r, p_0(1-r), 0)$ (C) $(p_0 r, 1-p_0 r, 0)$ (D) $(p_0, 1-p_0, 0)$

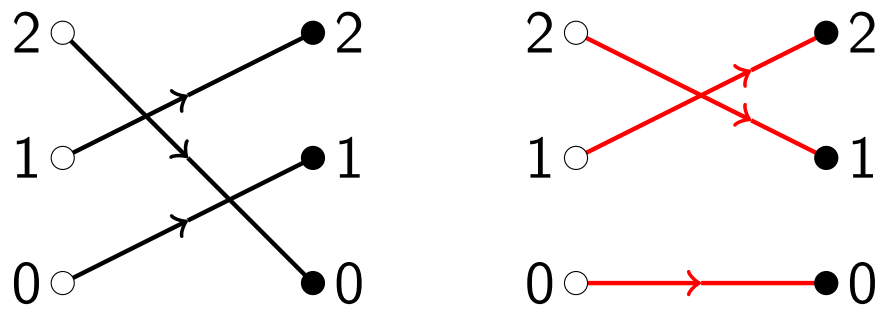
- Which expression below is equal to $\mathbb{P}[Y = 0]$?

(A) $\mathbb{P}[Y = 0|X = 0] + \mathbb{P}[Y = 0|X = 1] + \mathbb{P}[Y = 0|X = 2]$
(B) $\mathbb{P}[Y = 0|X = 0]p_0 + \mathbb{P}[Y = 0|X = 1]p_1 + \mathbb{P}[Y = 0|X = 2]p_2$

(A) (B)

Quiz on Probability Model for Cryptosystems

In the cryptosystem below, the red key is used with probability r.
In symbols: $\mathbb{P}[K = \textit{red}] = r$.



Suppose the plaintexts are sent with probabilities p_0, p_1 and p_2.

- What is the probability distribution of Y, conditioned on $X = 0$? Equivalently, what is

$$(\mathbb{P}[Y = 0|X = 0], \mathbb{P}[Y = 1|X = 0], \mathbb{P}[Y = 2|X = 0])?$$

(A) $(r, 1-r, 0)$ (B) $(p_0 r, p_0(1-r), 0)$ (C) $(p_0 r, 1-p_0 r, 0)$ (D) $(p_0, 1-p_0, 0)$

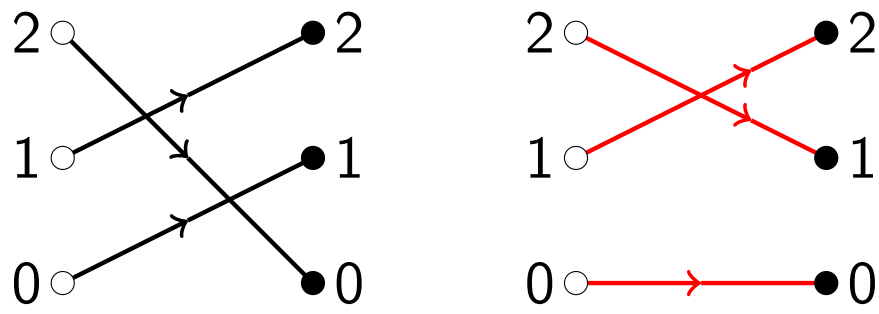
- Which expression below is equal to $\mathbb{P}[Y = 0]$?

(A) $\mathbb{P}[Y = 0|X = 0] + \mathbb{P}[Y = 0|X = 1] + \mathbb{P}[Y = 0|X = 2]$
(B) $\mathbb{P}[Y = 0|X = 0]p_0 + \mathbb{P}[Y = 0|X = 1]p_1 + \mathbb{P}[Y = 0|X = 2]p_2$

(A) (B)

Quiz on Probability Model for Cryptosystems

In the cryptosystem below, the red key is used with probability r.
In symbols: $\mathbb{P}[K = \textit{red}] = r$.



Suppose the plaintexts are sent with probabilities p_0, p_1 and p_2.

- What is the probability distribution of Y, conditioned on $X = 0$? Equivalently, what is

$$(\mathbb{P}[Y = 0|X = 0], \mathbb{P}[Y = 1|X = 0], \mathbb{P}[Y = 2|X = 0])?$$

(A) $(r, 1-r, 0)$ (B) $(p_0 r, p_0(1-r), 0)$ (C) $(p_0 r, 1-p_0 r, 0)$ (D) $(p_0, 1-p_0, 0)$

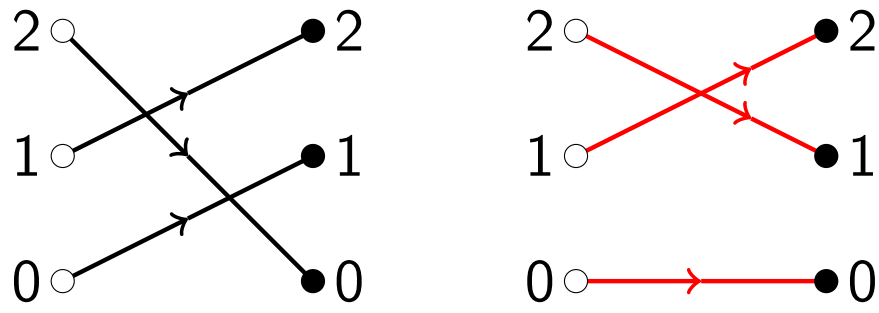
- Which expression below is equal to $\mathbb{P}[Y = 0]$?

(A) $\mathbb{P}[Y = 0|X = 0] + \mathbb{P}[Y = 0|X = 1] + \mathbb{P}[Y = 0|X = 2]$
(B) $\mathbb{P}[Y = 0|X = 0]p_0 + \mathbb{P}[Y = 0|X = 1]p_1 + \mathbb{P}[Y = 0|X = 2]p_2$

(A) (B)

Quiz on Probability Model for Cryptosystems [ctd]

In the cryptosystem below, the red key is used with probability r.
In symbols: $\mathbb{P}[K = \textit{red}] = r$.



Suppose the plaintexts are sent with probabilities p_0, p_1 and p_2.

- What is $\mathbb{P}[Y = 0]$?

  (A) $p_0 r$ (B) $p_2(1-r)$ (C) $p_0 r + p_2(1-r)$ (D) $p_0 r + p_2$

- What is $\mathbb{P}[X = 0 | Y = 0]$?

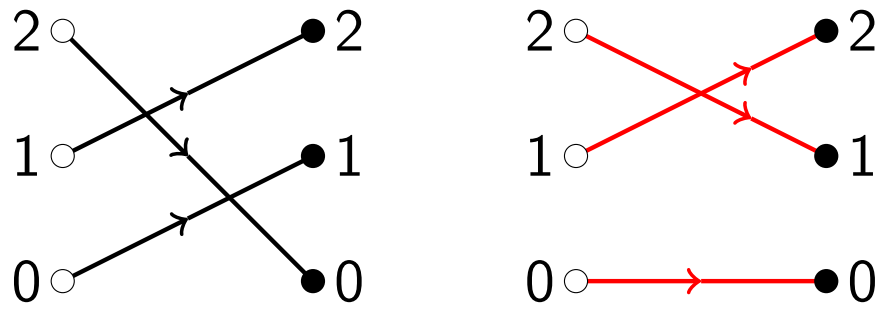
  (A) $p_0 r$ (B) $\frac{p_0 r}{p_0 r + p_2(1-r)}$ (C) $\frac{p_0 r}{p_2(1-r)}$ (D) other

- What is $\mathbb{P}[X = 1 | Y = 1]$?

  (A) 0 (B) r (C) $1-r$ (D) 1

Quiz on Probability Model for Cryptosystems [ctd]

In the cryptosystem below, the red key is used with probability r.
In symbols: $\mathbb{P}[K = \textit{red}] = r$.



Suppose the plaintexts are sent with probabilities p_0, p_1 and p_2.

- What is $\mathbb{P}[Y = 0]$?

  (A) $p_0 r$ (B) $p_2(1-r)$ (C) $p_0 r + p_2(1-r)$ (D) $p_0 r + p_2$

- What is $\mathbb{P}[X = 0 | Y = 0]$?

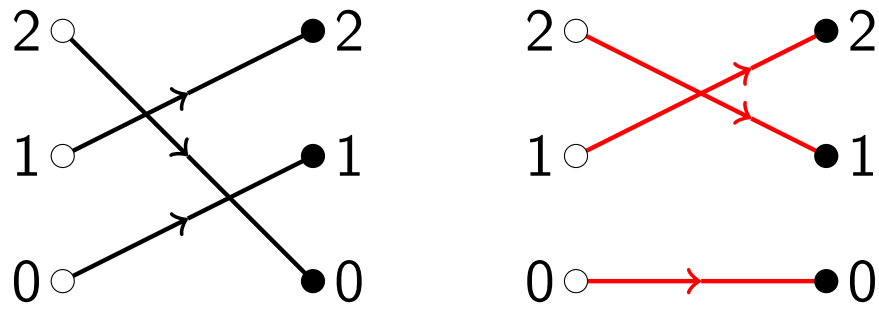
  (A) $p_0 r$ (B) $\frac{p_0 r}{p_0 r + p_2(1-r)}$ (C) $\frac{p_0 r}{p_2(1-r)}$ (D) other

- What is $\mathbb{P}[X = 1 | Y = 1]$?

  (A) 0 (B) r (C) $1-r$ (D) 1

Quiz on Probability Model for Cryptosystems [ctd]

In the cryptosystem below, the red key is used with probability r.
In symbols: $\mathbb{P}[K = \textit{red}] = r$.



Suppose the plaintexts are sent with probabilities p_0, p_1 and p_2.

- What is $\mathbb{P}[Y = 0]$?

  (A) $p_0 r$ (B) $p_2(1-r)$ (C) $p_0 r + p_2(1-r)$ (D) $p_0 r + p_2$

- What is $\mathbb{P}[X = 0 | Y = 0]$?

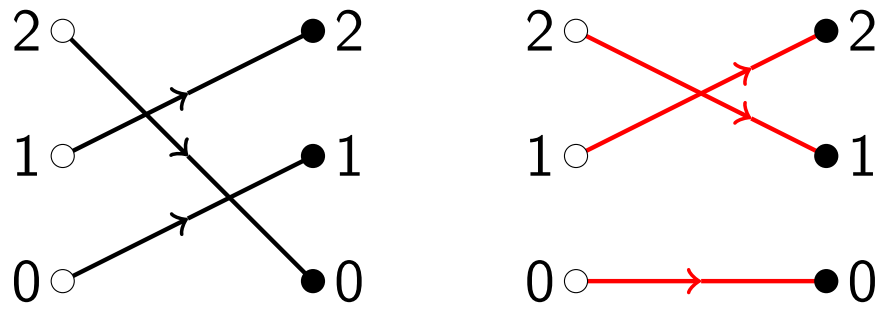
  (A) $p_0 r$ (B) $\frac{p_0 r}{p_0 r + p_2(1-r)}$ (C) $\frac{p_0 r}{p_2(1-r)}$ (D) other

- What is $\mathbb{P}[X = 1 | Y = 1]$?

  (A) 0 (B) r (C) $1-r$ (D) 1

Quiz on Probability Model for Cryptosystems [ctd]

In the cryptosystem below, the red key is used with probability r.
In symbols: $\mathbb{P}[K = \textit{red}] = r$.



Suppose the plaintexts are sent with probabilities p_0, p_1 and p_2.

- What is $\mathbb{P}[Y = 0]$?

  (A) $p_0 r$ (B) $p_2(1-r)$ (C) $p_0 r + p_2(1-r)$ (D) $p_0 r + p_2$

- What is $\mathbb{P}[X = 0 | Y = 0]$?

  (A) $p_0 r$ (B) $\frac{p_0 r}{p_0 r + p_2(1-r)}$ (C) $\frac{p_0 r}{p_2(1-r)}$ (D) other

- What is $\mathbb{P}[X = 1 | Y = 1]$?

  (A) 0 (B) r (C) $1-r$ (D) 1

Quiz on Probability Model: Purple Spots Disease

People may have Purple Spots Disease. In its first 14 days, the disease is completely symptomless. Fortunately there is a test.

- If you have Purple Spots Disease, the test is always positive.
- If you don't have it, there is a tiny $\frac{1}{1000}$ chance of a false positive.

Let

- D be the event 'I have Purple Spots Disease',
- T be the event 'My test was positive'.

Suppose that the proportion of the population having Purple Spots Disease is p.

(a) Which probability do you care about more?
(A) $\mathbb{P}[D|T]$ (B) $\mathbb{P}[T|D]$

(b) Which probability is easier to compute?
(A) $\mathbb{P}[D|T]$ (B) $\mathbb{P}[T|D]$

Quiz on Probability Model: Purple Spots Disease

People may have Purple Spots Disease. In its first 14 days, the disease is completely symptomless. Fortunately there is a test.

- If you have Purple Spots Disease, the test is always positive.
- If you don't have it, there is a tiny $\frac{1}{1000}$ chance of a false positive.

Let

- D be the event 'I have Purple Spots Disease',
- T be the event 'My test was positive'.

Suppose that the proportion of the population having Purple Spots Disease is p.

(a) Which probability do you care about more?
(A) $\mathbb{P}[D|T]$ (B) $\mathbb{P}[T|D]$

(b) Which probability is easier to compute?
(A) $\mathbb{P}[D|T]$ (B) $\mathbb{P}[T|D]$

Quiz on Probability Model: Purple Spots Disease

People may have Purple Spots Disease. In its first 14 days, the disease is completely symptomless. Fortunately there is a test.

- If you have Purple Spots Disease, the test is always positive.
- If you don't have it, there is a tiny $\frac{1}{1000}$ chance of a false positive.

Let

- D be the event 'I have Purple Spots Disease',
- T be the event 'My test was positive'.

Suppose that the proportion of the population having Purple Spots Disease is p.

(a) Which probability do you care about more?
(A) $\mathbb{P}[D|T]$ (B) $\mathbb{P}[T|D]$

(b) Which probability is easier to compute?
(A) $\mathbb{P}[D|T]$ (B) $\mathbb{P}[T|D]$

Indeed, $\mathbb{P}[T|D] = 1$: the test always works if you have the disease. But you really want to know 'what's the chance I have the disease, given the bad news from my test', and this is $\mathbb{P}[D|T]$.

Quiz on Probability Model: Purple Spots Disease [ctd]

Recall that

- If you have Purple Spots Disease, the test is always positive.
- If you don't have it, there is a tiny $\frac{1}{1000}$ chance of a false positive.

We defined D to be the event 'I have PSD', and T to be the event 'My test was positive'. Suppose that the proportion of the population having PSD is p.

(c) What is $\mathbb{P}[T|\text{not } D]$?

(A) $\frac{1}{1000}$ (B) $\frac{p}{1000}$ (C) p (D) $1-p$

(d) What is $\mathbb{P}[T]$?

(A) p (B) $\frac{1}{1000}$ (C) $\frac{1}{1000}+\frac{999}{1000}p$ (D) $\frac{1}{1000}+\frac{p}{1000}$

(e) What is $\mathbb{P}[D|T]$?

(A) p (B) $\frac{1000p}{1+999p}$ (C) $\frac{999p}{1+1000p}$ (D) $\frac{999p}{1000}$

Quiz on Probability Model: Purple Spots Disease [ctd]

Recall that

- If you have Purple Spots Disease, the test is always positive.
- If you don't have it, there is a tiny $\frac{1}{1000}$ chance of a false positive.

We defined D to be the event 'I have PSD', and T to be the event 'My test was positive'. Suppose that the proportion of the population having PSD is p.

(c) What is $\mathbb{P}[T|\text{not } D]$?

(A) $\frac{1}{1000}$ (B) $\frac{p}{1000}$ (C) p (D) $1-p$

(d) What is $\mathbb{P}[T]$?

(A) p (B) $\frac{1}{1000}$ (C) $\frac{1}{1000}+\frac{999}{1000}p$ (D) $\frac{1}{1000}+\frac{p}{1000}$

(e) What is $\mathbb{P}[D|T]$?

(A) p (B) $\frac{1000p}{1+999p}$ (C) $\frac{999p}{1+1000p}$ (D) $\frac{999p}{1000}$

Quiz on Probability Model: Purple Spots Disease [ctd]

Recall that

- If you have Purple Spots Disease, the test is always positive.
- If you don't have it, there is a tiny $\frac{1}{1000}$ chance of a false positive.

We defined D to be the event 'I have PSD', and T to be the event 'My test was positive'. Suppose that the proportion of the population having PSD is p.

(c) What is $\mathbb{P}[T|\text{not } D]$?

(A) $\frac{1}{1000}$ (B) $\frac{p}{1000}$ (C) p (D) $1-p$

(d) What is $\mathbb{P}[T]$?

(A) p (B) $\frac{1}{1000}$ (C) $\frac{1}{1000}+\frac{999}{1000}p$ (D) $\frac{1}{1000}+\frac{p}{1000}$

(e) What is $\mathbb{P}[D|T]$?

(A) p (B) $\frac{1000p}{1+999p}$ (C) $\frac{999p}{1+1000p}$ (D) $\frac{999p}{1000}$

Quiz on Probability Model: Purple Spots Disease [ctd]

Recall that

- If you have Purple Spots Disease, the test is always positive.
- If you don't have it, there is a tiny $\frac{1}{1000}$ chance of a false positive.

We defined D to be the event 'I have PSD', and T to be the event 'My test was positive'. Suppose that the proportion of the population having PSD is p.

(c) What is $\mathbb{P}[T|\text{not } D]$?

(A) $\frac{1}{1000}$ (B) $\frac{p}{1000}$ (C) p (D) $1-p$

(d) What is $\mathbb{P}[T]$?

(A) p (B) $\frac{1}{1000}$ (C) $\frac{1}{1000}+\frac{999}{1000}p$ (D) $\frac{1}{1000}+\frac{p}{1000}$

(e) What is $\mathbb{P}[D|T]$?

(A) p (B) $\frac{1000p}{1+999p}$ (C) $\frac{999p}{1+1000p}$ (D) $\frac{999p}{1000}$

Note that (c) was given: it's the false positive rate; (d) and (e) can be done using the 'switch it round' trick (equivalently Bayes, equivalently the definition of conditional probability),

$$\mathbb{P}[D|T]=\frac{\mathbb{P}[D\cap T]}{\mathbb{P}[T]}=\frac{\mathbb{P}[T|D]\mathbb{P}[D]}{\mathbb{P}[T]}=\frac{1\times p}{\frac{1}{1000}+\frac{999}{1000}p}=\frac{1000p}{1+999p}$$

Quiz on Probability Model: Purple Spots Disease [ctd]

Recall that

- If you have Purple Spots Disease, the test is always positive.
- If you don't have it, there is a tiny $\frac{1}{1000}$ chance of a false positive.

We defined D to be the event 'I have PSD', and T to be the event 'My test was positive'. Suppose that the proportion of the population having PSD is p.

(c) What is $\mathbb{P}[T|\text{not } D]$?

(A) $\frac{1}{1000}$ (B) $\frac{p}{1000}$ (C) p (D) $1-p$

(d) What is $\mathbb{P}[T]$?

(A) p (B) $\frac{1}{1000}$ (C) $\frac{1}{1000}+\frac{999}{1000}p$ (D) $\frac{1}{1000}+\frac{p}{1000}$

(e) What is $\mathbb{P}[D|T]$?

(A) p (B) $\frac{1000p}{1+999p}$ (C) $\frac{999p}{1+1000p}$ (D) $\frac{999p}{1000}$

(f) Suppose that $p=\frac{1}{2000}$. What, very nearly, is $\mathbb{P}[D|T]$?

(A) $\frac{1}{1000}$ (B) $\frac{1}{3}$ (C) $\frac{1}{2}$ (D) 1

(g) Is it a good idea to roll out mass testing?

(A) No (B) Yes

Quiz on Probability Model: Purple Spots Disease [ctd]

Recall that

- If you have Purple Spots Disease, the test is always positive.
- If you don't have it, there is a tiny $\frac{1}{1000}$ chance of a false positive.

We defined D to be the event 'I have PSD', and T to be the event 'My test was positive'. Suppose that the proportion of the population having PSD is p.

(c) What is $\mathbb{P}[T|\text{not } D]$?

(A) $\frac{1}{1000}$ (B) $\frac{p}{1000}$ (C) p (D) $1-p$

(d) What is $\mathbb{P}[T]$?

(A) p (B) $\frac{1}{1000}$ (C) $\frac{1}{1000}+\frac{999}{1000}p$ (D) $\frac{1}{1000}+\frac{p}{1000}$

(e) What is $\mathbb{P}[D|T]$?

(A) p (B) $\frac{1000p}{1+999p}$ (C) $\frac{999p}{1+1000p}$ (D) $\frac{999p}{1000}$

(f) Suppose that $p=\frac{1}{2000}$. What, very nearly, is $\mathbb{P}[D|T]$?

(A) $\frac{1}{1000}$ (B) $\frac{1}{3}$ (C) $\frac{1}{2}$ (D) 1

(g) Is it a good idea to roll out mass testing?

(A) No (B) Yes

Quiz on Probability Model: Purple Spots Disease [ctd]

Recall that

- If you have Purple Spots Disease, the test is always positive.
- If you don't have it, there is a tiny $\frac{1}{1000}$ chance of a false positive.

We defined D to be the event 'I have PSD', and T to be the event 'My test was positive'. Suppose that the proportion of the population having PSD is p.

(c) What is $\mathbb{P}[T|\text{not } D]$?

(A) $\frac{1}{1000}$ (B) $\frac{p}{1000}$ (C) p (D) $1-p$

(d) What is $\mathbb{P}[T]$?

(A) p (B) $\frac{1}{1000}$ (C) $\frac{1}{1000}+\frac{999}{1000}p$ (D) $\frac{1}{1000}+\frac{p}{1000}$

(e) What is $\mathbb{P}[D|T]$?

(A) p (B) $\frac{1000p}{1+999p}$ (C) $\frac{999p}{1+1000p}$ (D) $\frac{999p}{1000}$

(f) Suppose that $p=\frac{1}{2000}$. What, very nearly, is $\mathbb{P}[D|T]$?

(A) $\frac{1}{1000}$ (B) $\frac{1}{3}$ (C) $\frac{1}{2}$ (D) 1

(g) Is it a good idea to roll out mass testing?

(A) No (B) Yes

Indeed no, when about $\frac{2}{3}$ of all tests will give the wrong result!

Quiz on Probability Model: Purple Spots Disease [ctd]

Recall that

- If you have Purple Spots Disease, the test is always positive.
- If you don't have it, there is a tiny $\frac{1}{1000}$ chance of a false positive.

We defined D to be the event 'I have PSD', and T to be the event 'My test was positive'. Suppose that the proportion of the population having PSD is p.

(c) What is $\mathbb{P}[T|\text{not } D]$?

(A) $\frac{1}{1000}$ (B) $\frac{p}{1000}$ (C) p (D) $1-p$

(d) What is $\mathbb{P}[T]$?

(A) p (B) $\frac{1}{1000}$ (C) $\frac{1}{1000}+\frac{999}{1000}p$ (D) $\frac{1}{1000}+\frac{p}{1000}$

(e) What is $\mathbb{P}[D|T]$?

(A) p (B) $\frac{1000p}{1+999p}$ (C) $\frac{999p}{1+1000p}$ (D) $\frac{999p}{1000}$

(f) Suppose that $p=\frac{1}{2000}$. What, very nearly, is $\mathbb{P}[D|T]$?

(A) $\frac{1}{1000}$ (B) $\frac{1}{3}$ (C) $\frac{1}{2}$ (D) 1

(g) Is it a good idea to roll out mass testing?

(A) No (B) Yes

(h) What's the connection with the probability model?

Example 3.8

Consider the numeric one-time pad in Example 3.5, Assume that keys are chosen with equal probability $\frac{1}{n}$. Suppose that Eve observes the ciphertext y.

(a) By Question 1 on Problem Sheet 2, $\mathbb{P}[X = x | Y = y] = p_x$ for all $x, y \in \mathbb{Z}_n$. This is a precise statement that Eve learns nothing about the plaintext from observing y. (In the sense of Definition 3.11, the one-time pad has perfect secrecy.)

(b) As $\mathbb{P}[K = k | Y = y] = \mathbb{P}[X = y - k \bmod n | Y = y]$, (a) implies

$$\mathbb{P}[K = k | Y = y] = p_{y-k \bmod n}.$$

Thus the probability distribution $\mathbb{P}[K = k | Y = y]$ for k varying is a reflected shift of the probability distribution $\mathbb{P}[X = x]$ on plaintexts. So, unavoidably, Eve learns something about the key.

This was seen in the setting of Example 1.2 (Alice sent Bob his exam mark using the numeric one-time pad with $n = 100$) in the groupwork for Week 1, and in Question 1 on Problem Sheet 1.)

Shannon's Theorem: Preliminaries

In practice, the user of a cryptosystem needs to know how to choose the keys.

Definition 3.9

We define a *practical cryptosystem* to be a cryptosystem together with a probability distribution on the keys such that

(1) $\mathbb{P}[K = k] > 0$ for all $k \in \mathcal{K}$

(2) for all $y \in \mathcal{C}$ there exists $x \in \mathcal{P}$ and $k \in \mathcal{K}$ such that $e_k(x) = y$.

Exercise 3.10

(a) Why are the two conditions in Definition 3.9 reasonable?

(b) Show that in a practical cryptosystem, if every plaintext may be sent, then $\mathbb{P}[Y = y] > 0$ for all $y \in \mathcal{C}$.

Unlike the definition of perfect secrecy, which goes back to Shannon's 1949 paper, Definition 3.9 is not a standard definition in cryptography. You will be reminded of it when it is required.

Definition of Perfect Secrecy

Definition 3.11

Fix a practical cryptosystem.

(i) Let p_x for $x \in X$ be a probability distribution on the plaintexts such that $\mathbb{P}[Y = y] > 0$ for all $y \in \mathcal{C}$. The cryptosystem has *perfect secrecy for the distribution* p_x if

$$\mathbb{P}[X = x | Y = y] = p_x$$

for all $x \in \mathcal{P}$ and all $y \in \mathcal{C}$ such that $\mathbb{P}[Y = y] > 0$.

(ii) The cryptosystem has *perfect secrecy* if it has perfect secrecy for every probability distribution on the plaintexts.

- By Example 3.8(a) the numeric one-time pad on $\mathbb{Z}_n$ has perfect secrecy when keys are used with equal probability.

Definition of Perfect Secrecy

Definition 3.11

Fix a practical cryptosystem.

(i) Let p_x for $x \in X$ be a probability distribution on the plaintexts such that $\mathbb{P}[Y = y] > 0$ for all $y \in \mathcal{C}$. The cryptosystem has *perfect secrecy for the distribution* p_x if

$$\mathbb{P}[X = x | Y = y] = p_x$$

for all $x \in \mathcal{P}$ and all $y \in \mathcal{C}$ such that $\mathbb{P}[Y = y] > 0$.

(ii) The cryptosystem has *perfect secrecy* if it has perfect secrecy for every probability distribution on the plaintexts.

- In Example 3.7 we saw a cryptosystem where if the three keys are used with equal probability, and $p_0 = 0$, $p_1 = 1 - q$, $p_2 = q$ then $\mathbb{P}[X = 2 | Y = 1] = 2p_2/(1 + p_2)$. Hence

$$\begin{aligned} \mathbb{P}[X = 2 | Y = 1] = p_2 &\iff \frac{2p_2}{1 + p_2} = p_2 \\ &\iff p_2 = 0 \text{ or } p_2 = 1. \end{aligned}$$

This probabilistic cryptosystem does not have perfect secrecy.

Shannon's Theorem

Recall that a practical cryptosystem is a cryptosystem together with a probability distribution on keys such that $\mathbb{P}[K = k] > 0$ for all $k \in \mathcal{K}$ and for all $y \in \mathcal{C}$ there exists $x \in \mathcal{P}$ and $k \in \mathcal{K}$ such that $e_k(x) = y$.

Theorem 3.12 (Shannon 1949)

If a practical cryptosytem has perfect secrecy then

(a) *For all $x \in \mathcal{P}$ and $y \in \mathcal{C}$ the events $X = x$ and $Y = y$ are independent and $\mathbb{P}[Y = y|X = x] = \mathbb{P}[Y = y] > 0$.*

(b) *For all $x \in \mathcal{P}$ and all $y \in \mathcal{C}$ there exists a key k such that $e_k(x) = y$.*

(c) $|\mathcal{K}| \geq |\mathcal{C}|$.

(d) *Suppose $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$. For all $x \in \mathcal{P}$ and all $y \in \mathcal{C}$ there exists a unique key $k \in \mathcal{K}$ such that $e_k(x) = y$. Each key has equal probability and each ciphertext is equally likely.*

Quantifiers Matter!

Quiz: let $P(k, x, y)$ be a mathematical statement depending on quantities k, x and y. Which are logically equivalent?

(Q) $\forall y \exists x \exists k \; P(k, x, y)$

(R) $\forall y \forall x \exists k \; P(k, x, y)$

(S) $\forall x \forall y \exists k \; P(k, x, y)$

(A) Q and R (B) R and S (C) Q and S (D) none

Quantifiers Matter!

Quiz: let $P(k, x, y)$ be a mathematical statement depending on quantities k, x and y. Which are logically equivalent?

(Q) $\forall y \exists x \exists k \; P(k, x, y)$

(R) $\forall y \forall x \exists k \; P(k, x, y)$

(S) $\forall x \forall y \exists k \; P(k, x, y)$

(A) Q and R (B) R and S (C) Q and S (D) none

In Theorem 3.12 we assume a practical cryptosystem. Property (2) in the definition of practical cryptosystem is

(2) for all $y \in \mathcal{C}$ there exists $x \in \mathcal{P}$ and $k \in \mathcal{K}$ such that $e_k(x) = y$.

Conclusion (b) in Theorem 3.12 is

(b) For all $x \in \mathcal{P}$ and all $y \in \mathcal{C}$ there exists a key k such that $e_k(x) = y$.

Exercise 3.13

How does the conclusion (b) in Theorem 3.12 differ from property (2) in the definition of a practical cryptosystem?

Proof of Theorem 3.12

Theorem 3.12 (Shannon 1949)

If a practical cryptosytem has perfect secrecy then

(a) *For all $x \in \mathcal{P}$ and $y \in \mathcal{C}$ the events $X = x$ and $Y = y$ are independent and $\mathbb{P}[Y = y|X = x] = \mathbb{P}[Y = y] > 0$.*

Proof.

- By hypothesis the cryptosystem has perfect secrecy.
- So **we** can choose any probability distribution p_x on the plaintexts and writing out what perfect secrecy means, get

$$\mathbb{P}[X = x|Y = y] = p_x$$

  for all $x \in \mathbb{P}$ and $y \in \mathcal{C}$.
- We should be careful only to condition on events that have positive probability. Why do we know that $\mathbb{P}[Y = y] > 0$?
- Okay, so after this check, we know that $\mathbb{P}[X = x|Y = y] = p_x = \mathbb{P}[X = x]$ for all x and y. Is this close to independence?

Theorem 3.12 (Shannon 1949)

If a practical cryptosytem has perfect secrecy then

(b) *For all $x \in \mathcal{P}$ and all $y \in \mathcal{C}$ there exists a key k such that $e_k(x) = y$.*

So far we know that for all $x \in \mathcal{P}$ and $y \in \mathcal{C}$ the events $X = x$ and $Y = y$ are independent and both have positive probability.

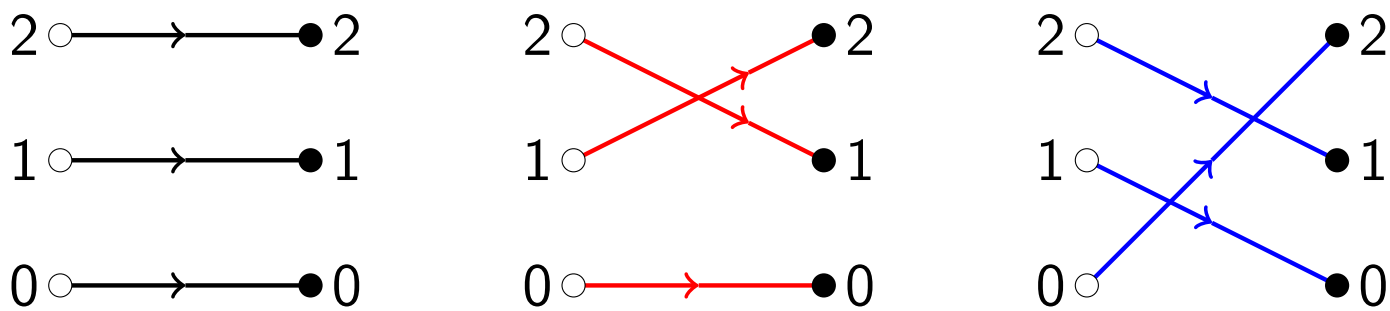
Theorem 3.12 (Shannon 1949)

If a practical cryptosytem has perfect secrecy then

(b) *For all $x \in \mathcal{P}$ and all $y \in \mathcal{C}$ there exists a key k such that $e_k(x) = y$.*

So far we know that for all $x \in \mathcal{P}$ and $y \in \mathcal{C}$ the events $X = x$ and $Y = y$ are independent and both have positive probability.

- In Example 3.7 we saw probabilities such as $\mathbb{P}[Y = y|X = x]$. Here is a reminder of the first quiz question:



Let $P[K = \text{black}] = r_{\text{black}}$, $P[K = \text{red}] = r_{\text{red}}$, $\mathbb{P}[K = \text{blue}] = r_{\text{blue}}$.

(1) What is $\mathbb{P}[Y = 1|X = 2]$?

(A) r_{red} (B) r_{blue} (C) $r_{\text{red}} + r_{\text{blue}}$ (D) $r_{\text{black}} + r_{\text{red}}$

- So $\mathbb{P}[Y = y|X = x]$ is the probability that k is the set $\mathcal{E}_{xy}$ of keys such that $e_k(x) = y$. Use this to prove (b).

Theorem 3.12 (Shannon 1949)

If a practical cryptosytem has perfect secrecy then

(c) $|\mathcal{K}| \geq |\mathcal{C}|$.

We have just shown that for all $x \in \mathcal{P}$ and $y \in \mathcal{C}$, the set $\mathcal{E}_{xy} = \{k \in \mathcal{K} : e_k(x) = y\}$ is non-empty.

- Hint: fix $x \in \mathcal{P}$. Can the same key encrypt x to two different ciphertexts? So how many different keys are needed to get every ciphertext?

Theorem 3.12 (Shannon 1949)

If a practical cryptosytem has perfect secrecy then

(c) $|\mathcal{K}| \geq |\mathcal{C}|$.

We have just shown that for all $x \in \mathcal{P}$ and $y \in \mathcal{C}$, the set $\mathcal{E}_{xy} = \{k \in \mathcal{K} : e_k(x) = y\}$ is non-empty.

- Hint: fix $x \in \mathcal{P}$. Can the same key encrypt x to two different ciphertexts? So how many different keys are needed to get every ciphertext?
- Prove (c).

Theorem 3.12 (Shannon 1949)

If a practical cryptosytem has perfect secrecy then

(c) $|\mathcal{K}| \geq |\mathcal{C}|$.

We have just shown that for all $x \in \mathcal{P}$ and $y \in \mathcal{C}$, the set $\mathcal{E}_{xy} = \{k \in \mathcal{K} : e_k(x) = y\}$ is non-empty.

- Hint: fix $x \in \mathcal{P}$. Can the same key encrypt x to two different ciphertexts? So how many different keys are needed to get every ciphertext?
- Prove (c).

(d) Suppose $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$. For all $x \in \mathcal{P}$ and all $y \in \mathcal{C}$ there exists a unique key $k \in \mathcal{K}$ such that $e_k(x) = y$. Each key has equal probability and each ciphertext is equally likely.

- Prove the uniqueness. Hint: as in (c), fix $x \in \mathcal{P}$ and then use $\mathcal{K} = \bigcup_{y \in \mathcal{C}} \mathcal{E}_{xy}$. Why is the union disjoint?

Theorem 3.12 (Shannon 1949)

If a practical cryptosytem has perfect secrecy then

(c) $|\mathcal{K}| \geq |\mathcal{C}|$.

We have just shown that for all $x \in \mathcal{P}$ and $y \in \mathcal{C}$, the set $\mathcal{E}_{xy} = \{k \in \mathcal{K} : e_k(x) = y\}$ is non-empty.

- Hint: fix $x \in \mathcal{P}$. Can the same key encrypt x to two different ciphertexts? So how many different keys are needed to get every ciphertext?
- Prove (c).

(d) Suppose $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$. For all $x \in \mathcal{P}$ and all $y \in \mathcal{C}$ there exists a unique key $k \in \mathcal{K}$ such that $e_k(x) = y$. Each key has equal probability and each ciphertext is equally likely.

- Prove the uniqueness.
- Fix $y^\star \in \mathcal{C}$. For each $x \in \mathcal{P}$, let $k_x^\star$ be the unique key with $e_{k_x^\star}(x) = y^\star$. Are the $k_x^\star$ distinct? Is every key some $k_x^\star$?

Theorem 3.12 (Shannon 1949)

If a practical cryptosytem has perfect secrecy then

(c) $|\mathcal{K}| \geq |\mathcal{C}|$.

We have just shown that for all $x \in \mathcal{P}$ and $y \in \mathcal{C}$, the set $\mathcal{E}_{xy} = \{k \in \mathcal{K} : e_k(x) = y\}$ is non-empty.

- Hint: fix $x \in \mathcal{P}$. Can the same key encrypt x to two different ciphertexts? So how many different keys are needed to get every ciphertext?
- Prove (c).

(d) Suppose $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$. For all $x \in \mathcal{P}$ and all $y \in \mathcal{C}$ there exists a unique key $k \in \mathcal{K}$ such that $e_k(x) = y$. Each key has equal probability and each ciphertext is equally likely.

- Prove the uniqueness.
- Fix $y^\star \in \mathcal{C}$. For each $x \in \mathcal{P}$, let $k_x^\star$ be the unique key with $e_{k_x^\star}(x) = y^\star$. Are the $k_x^\star$ distinct? Is every key some $k_x^\star$?
- What can you say about $\mathbb{P}[K = k_x^\star]$? [*Hint:* it is $\mathbb{P}[Y = y^\star | X = x^\star]$. We saw in (b) that, by independence, this probability is $\mathbb{P}[Y = y^\star]$, not depending on $x^\star$.]) Hence prove (d).

Thinking about Shannon's Theorem

Some good questions to ask about a theorem, or a proof of a theorem, are 'What examples of it have I seen?', 'Did we use all the hypotheses?', 'Does the converse hold?'. These are explored on Problem Sheet 2. In particular, the optional Question 7(b) asks you to show the converse result stated below.

Proposition 3.14 (Converse to Theorem 3.12(d))

Suppose that $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$, that each key is used with equal probability, and for all $x \in \mathcal{P}$ and $y \in \mathcal{C}$, there exists a unique $k \in \mathcal{K}$ such that $e_k(x) = y$. Then the cryptosystem has perfect secrecy and each ciphertext is equally likely.

In Example 3.5 (also seen in the Group Work for Week 1), we saw a special case of this proposition. As an *exercise*, check that the hypothesis of this proposition hold in this example.

Rather than prove it in the limited 'live time' for the course, we will instead use the Week 3 Group Work to explore what it means in practice.

Example 3.15: Latin Squares

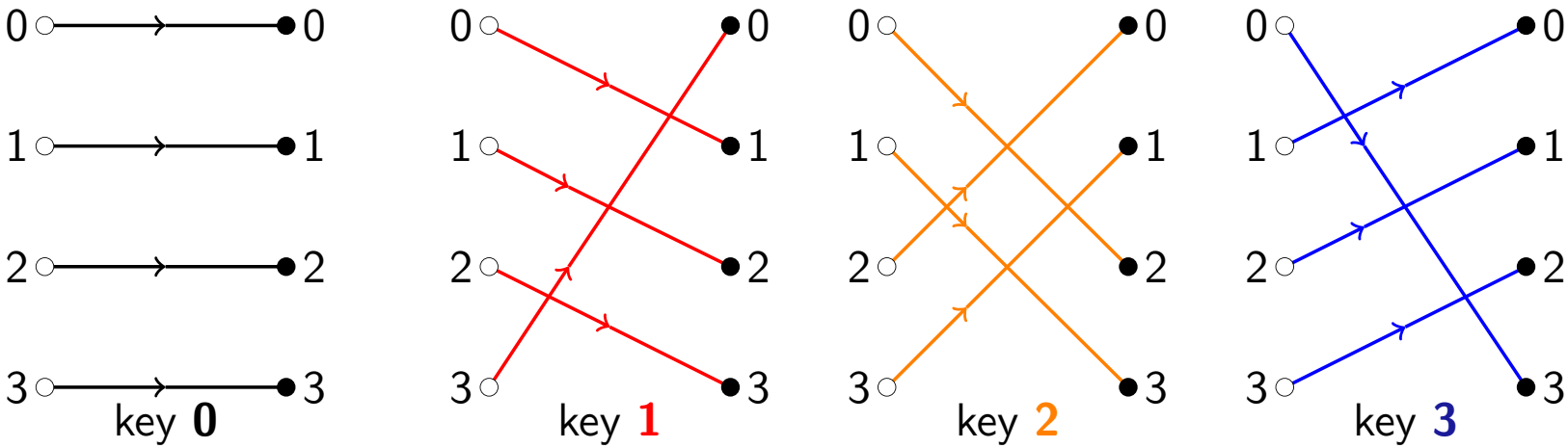
Consider a cryptosystem with perfect secrecy in which $\mathcal{P} = |\mathcal{C}| = |\mathcal{K}| = \{0, 1, \ldots, n-1\}$. By (c) in Theorem 3.12, for each $x, y \in \{0, 1, \ldots, n-1\}$, there exists a unique $k \in \{0, 1, \ldots, n-1\}$ such that $e_k(x) = y$. Therefore the cryptosystem is determined by the $n \times n$ matrix M where

$$M_{xy} = k \Longleftrightarrow e_k(x) = y.$$

Example 3.15: Latin Squares

Consider a cryptosystem with perfect secrecy in which $\mathcal{P} = |\mathcal{C}| = |\mathcal{K}| = \{0, 1, \ldots, n-1\}$. By (c) in Theorem 3.12, for each $x, y \in \{0, 1, \ldots, n-1\}$, there exists a unique $k \in \{0, 1, \ldots, n-1\}$ such that $e_k(x) = y$. Therefore the cryptosystem is determined by the $n \times n$ matrix M where

$$M_{xy} = k \iff e_k(x) = y.$$



has matrix

$$\begin{pmatrix} \mathbf{0} & \mathbf{1} & \mathbf{2} & \mathbf{3} \\ \mathbf{3} & \mathbf{0} & \mathbf{1} & \mathbf{2} \\ \mathbf{2} & \mathbf{3} & \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{0} \end{pmatrix}$$

Cheat Sheet for Cryptosystem Probability Calculations

(a) $\mathbb{P}[Y = y|X = x]$: this is the probability that the key encrypts x to y. It depends only on the keys. Do not use Bayes' Law.

(b) $\mathbb{P}[Y = y] = \sum_{x \in \mathcal{P}} \mathbb{P}[Y = y|X = x]p_x$, find using (a).

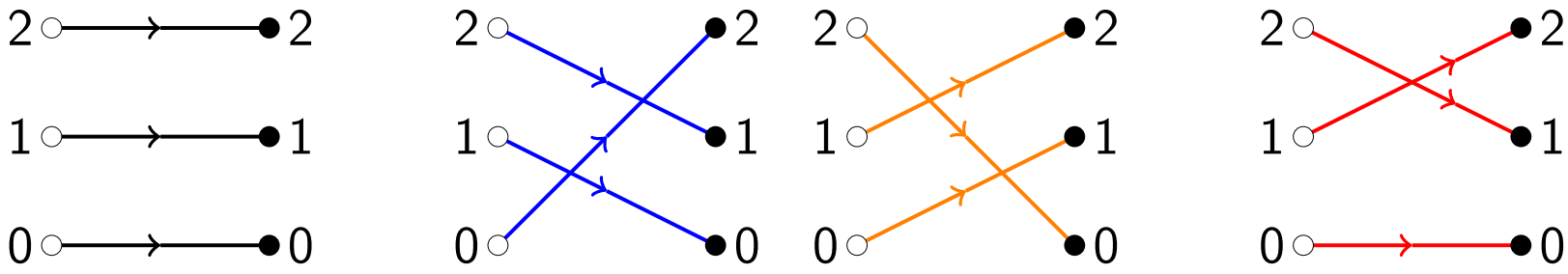
(c) $\mathbb{P}[X = x|Y = y] = \dfrac{\mathbb{P}[Y = y|X = x]p_x}{\mathbb{P}[Y = y]}$, use (a) and (b).

Here (c) is what the lecturer has often called the 'turn it around' rule. You might also recognise it as a version of Bayes' Law.

Of course I would rather you understood things at a deeper level, but here is the three step programme you need to follow to compute any $\mathbb{P}[X = x|Y = y]$. Please try it out on the end-of-section quiz.

Final Quiz on §3

Consider the cryptosystem below in which the keys have probabilities $\frac{1-r}{3}$ for black, blue and orange, and r for red.



As usual let X be the random plaintext, Y the random ciphertext and K the random key.

(a) What is $\mathbb{P}[e_K(1) = 2]$?

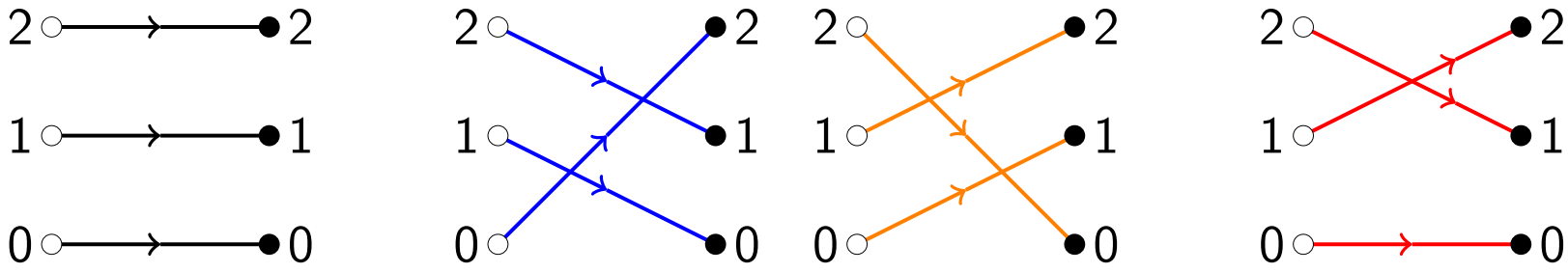
(A) $\frac{1-r}{3}$ (B) $\frac{1+2r}{3}$ (C) $\frac{1-r}{3}p_1$ (D) $\frac{1+2r}{3}p_1$

(b) What is $\mathbb{P}[X = 1 \text{ and } Y = 2]$?

(A) $\frac{1-r}{3}$ (B) $\frac{1+2r}{3}$ (C) $\frac{1-r}{3}p_1$ (D) $\frac{1+2r}{3}p_1$

Final Quiz on §3

Consider the cryptosystem below in which the keys have probabilities $\frac{1-r}{3}$ for black, blue and orange, and r for red.



As usual let X be the random plaintext, Y the random ciphertext and K the random key.

(a) What is $\mathbb{P}[e_K(1) = 2]$?

(A) $\frac{1-r}{3}$ (B) $\frac{1+2r}{3}$ (C) $\frac{1-r}{3}p_1$ (D) $\frac{1+2r}{3}p_1$

(b) What is $\mathbb{P}[X = 1 \text{ and } Y = 2]$?

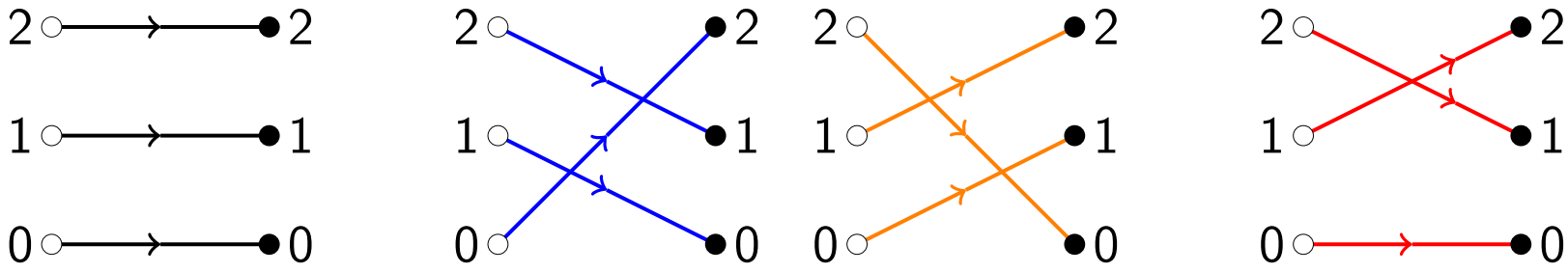
(A) $\frac{1-r}{3}$ (B) $\frac{1+2r}{3}$ (C) $\frac{1-r}{3}p_1$ (D) $\frac{1+2r}{3}p_1$

(c) What is $\mathbb{P}[Y = 2|X = 1]$?

(A) $\frac{1-r}{3}$ (B) $\frac{1+2r}{3}$ (C) $\frac{1-r}{3}p_1$ (D) $\frac{1+2r}{3}p_1$

Final Quiz on §3

Consider the cryptosystem below in which the keys have probabilities $\frac{1-r}{3}$ for black, blue and orange, and r for red.



As usual let X be the random plaintext, Y the random ciphertext and K the random key.

(a) What is $\mathbb{P}[e_K(1) = 2]$?

(A) $\frac{1-r}{3}$ (B) $\frac{1+2r}{3}$ (C) $\frac{1-r}{3}p_1$ (D) $\frac{1+2r}{3}p_1$

(b) What is $\mathbb{P}[X = 1 \text{ and } Y = 2]$?

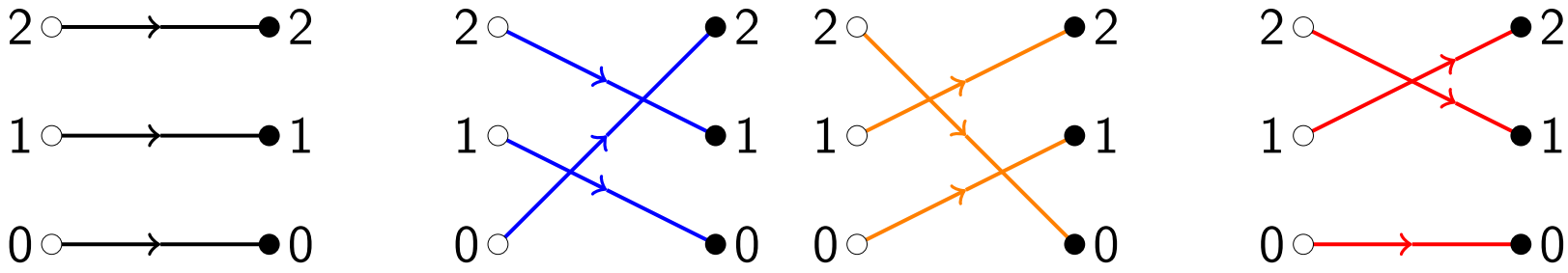
(A) $\frac{1-r}{3}$ (B) $\frac{1+2r}{3}$ (C) $\frac{1-r}{3}p_1$ (D) $\frac{1+2r}{3}p_1$

(c) What is $\mathbb{P}[Y = 2|X = 1]$?

(A) $\frac{1-r}{3}$ (B) $\frac{1+2r}{3}$ (C) $\frac{1-r}{3}p_1$ (D) $\frac{1+2r}{3}p_1$

Final Quiz on §3

Consider the cryptosystem below in which the keys have probabilities $\frac{1-r}{3}$ for black, blue and orange, and r for red.



As usual let X be the random plaintext, Y the random ciphertext and K the random key.

(a) What is $\mathbb{P}[e_K(1) = 2]$?

(A) $\frac{1-r}{3}$ (B) $\frac{1+2r}{3}$ (C) $\frac{1-r}{3}p_1$ (D) $\frac{1+2r}{3}p_1$

(b) What is $\mathbb{P}[X = 1 \text{ and } Y = 2]$?

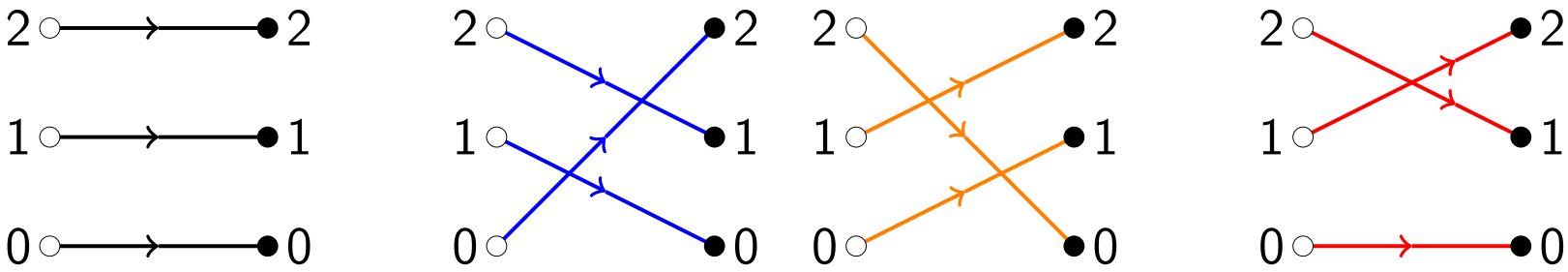
(A) $\frac{1-r}{3}$ (B) $\frac{1+2r}{3}$ (C) $\frac{1-r}{3}p_1$ (D) $\frac{1+2r}{3}p_1$

(c) What is $\mathbb{P}[Y = 2|X = 1]$?

(A) $\frac{1-r}{3}$ (B) $\frac{1+2r}{3}$ (C) $\frac{1-r}{3}p_1$ (D) $\frac{1+2r}{3}p_1$

Final Quiz on §3

Consider the cryptosystem below in which the keys have probabilities $\frac{1-r}{3}$ for black, blue and orange, and r for red.



(d) What is $\mathbb{P}[Y = 2]$?

(A) $\frac{1-r}{3}$ (B) $\frac{1-r}{3} + rp_1$ (C) $\frac{1-r}{3}(p_1 + p_2)$ (D) other

(e) What is $\mathbb{P}[X = 1 | Y = 2]$?

(A) p_1 (B) $\dfrac{(1+2r)p_1}{1-r+3rp_1}$ (C) $\dfrac{2rp_1}{1-r+3rp_1}$ (D) other

(f) Take $r = 0$. Does the cryptosystem have perfect secrecy?

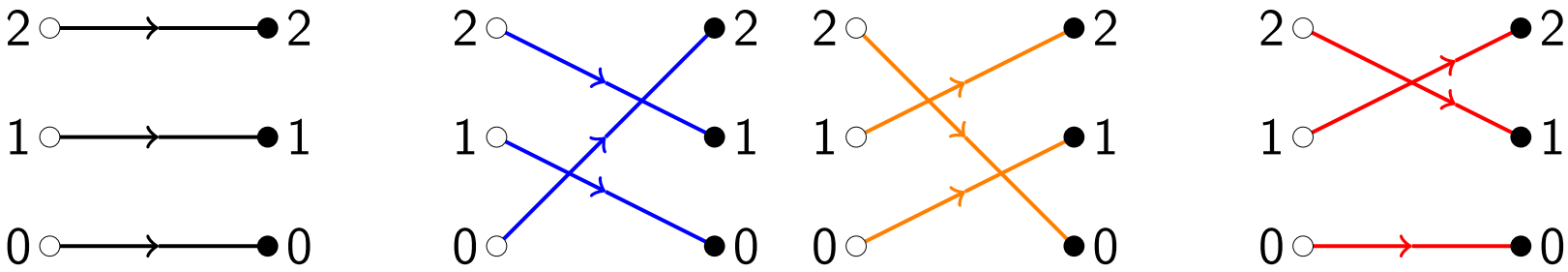
(A) No (B) Yes

(g) Take $r = \frac{1}{2}$. Does the cryptosystem have perfect secrecy?

(A) No (B) Yes

Final Quiz on §3

Consider the cryptosystem below in which the keys have probabilities $\frac{1-r}{3}$ for black, blue and orange, and r for red.



(d) What is $\mathbb{P}[Y = 2]$?

(A) $\frac{1-r}{3}$ (B) $\frac{1-r}{3} + rp_1$ (C) $\frac{1-r}{3}(p_1 + p_2)$ (D) other

(e) What is $\mathbb{P}[X = 1 | Y = 2]$?

(A) p_1 (B) $\dfrac{(1+2r)p_1}{1-r+3rp_1}$ (C) $\dfrac{2rp_1}{1-r+3rp_1}$ (D) other

(f) Take $r = 0$. Does the cryptosystem have perfect secrecy?

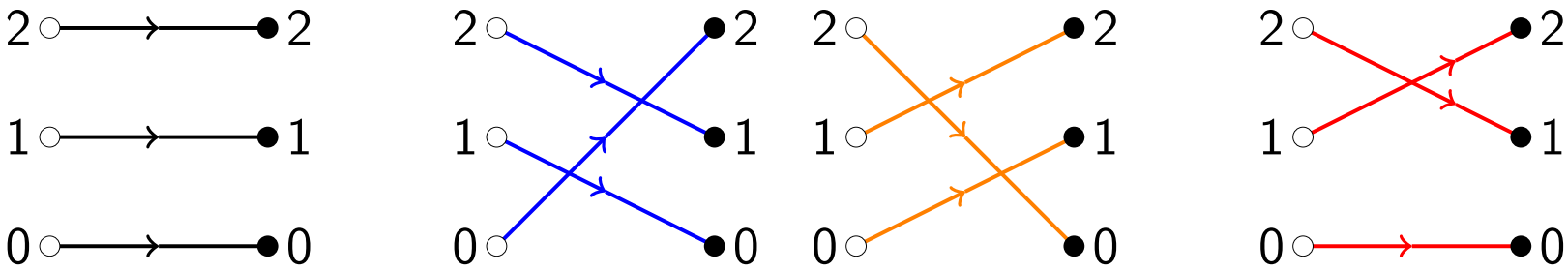
(A) No (B) Yes

(g) Take $r = \frac{1}{2}$. Does the cryptosystem have perfect secrecy?

(A) No (B) Yes

Final Quiz on §3

Consider the cryptosystem below in which the keys have probabilities $\frac{1-r}{3}$ for black, blue and orange, and r for red.



(d) What is $\mathbb{P}[Y = 2]$?

(A) $\frac{1-r}{3}$ (B) $\frac{1-r}{3} + rp_1$ (C) $\frac{1-r}{3}(p_1 + p_2)$ (D) other

(e) What is $\mathbb{P}[X = 1 | Y = 2]$?

(A) p_1 (B) $\dfrac{(1+2r)p_1}{1-r+3rp_1}$ (C) $\dfrac{2rp_1}{1-r+3rp_1}$ (D) other

(f) Take $r = 0$. Does the cryptosystem have perfect secrecy?

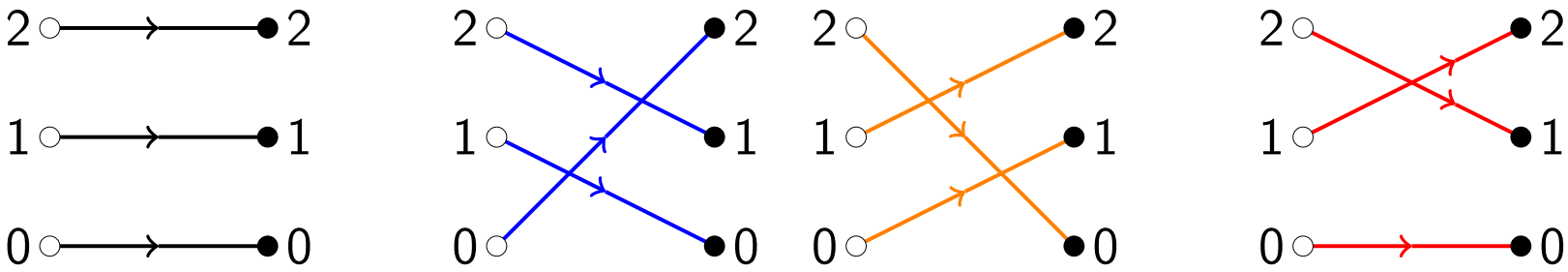
(A) No (B) Yes

(g) Take $r = \frac{1}{2}$. Does the cryptosystem have perfect secrecy?

(A) No (B) Yes

Final Quiz on §3

Consider the cryptosystem below in which the keys have probabilities $\frac{1-r}{3}$ for black, blue and orange, and r for red.



(d) What is $\mathbb{P}[Y = 2]$?

(A) $\frac{1-r}{3}$ (B) $\frac{1-r}{3} + rp_1$ (C) $\frac{1-r}{3}(p_1 + p_2)$ (D) other

(e) What is $\mathbb{P}[X = 1 | Y = 2]$?

(A) p_1 (B) $\dfrac{(1+2r)p_1}{1-r+3rp_1}$ (C) $\dfrac{2rp_1}{1-r+3rp_1}$ (D) other

(f) Take $r = 0$. Does the cryptosystem have perfect secrecy?

(A) No (B) Yes

(g) Take $r = \frac{1}{2}$. Does the cryptosystem have perfect secrecy?

(A) No (B) Yes

§4 Attack Models

Exercise 4.1

Eve observes a ciphertext. What is more useful for her: to learn the plaintext or to learn the key?

(A) Plaintext (B) Key

§4 Attack Models

Exercise 4.1

Eve observes a ciphertext. What is more useful for her: to learn the plaintext or to learn the key?

(A) Plaintext (B) Key

Reason. Because knowing the key, she can find the plaintext by decrypting, and she can also decrypt any other ciphertexts sent using the same key.

Motivating Question

Question. What can an attacker learn about the plaintext and key from an observed ciphertext? Can the key still be unknown when an attacker knows both a plaintext *and* its ciphertext?

Interpreting 'unknown' to mean 'not completely known', you have already seen an example showing that the answer to the second question is:

(A) No (B) Yes

Motivating Question

Question. What can an attacker learn about the plaintext and key from an observed ciphertext? Can the key still be unknown when an attacker knows both a plaintext *and* its ciphertext?

Interpreting 'unknown' to mean 'not completely known', you have already seen an example showing that the answer to the second question is:

(A) No (B) Yes

Reason. In Example 2.5 we successfully decrypted a ciphertext from a substitution cipher using frequency analysis. After this, both the plaintext and ciphertext were known. Since the 2 letters q, z were not in the plaintext, and the 2 letters A and E were not in the ciphertext, *either*

- $\pi(\mathtt{q}) = \mathtt{A}$ and $\pi(\mathtt{z}) = \mathtt{E}$ *or*
- $\pi(\mathtt{q}) = \mathtt{E}$ and $\pi(\mathtt{z}) = \mathtt{A}$

but we do not know which case holds. The key is not completely

Affine Cipher

Example 4.2 (Affine cipher)

Let q be prime. Let $\mathbb{Z}_q = \{0, 1, \ldots, q-1\}$. The *affine cipher* on $\mathbb{Z}_q$ has $\mathcal{P} = \mathcal{C} = \mathbb{Z}_q$ and

$$\mathcal{K} = \{(a, c) : a \in \mathbb{Z}_q, c \in \mathbb{Z}_q, a \neq 0\}.$$

The encryption functions are defined by $e_{(a,c)}(x) = ax + c \bmod q$. The decryption functions are defined by $d_{(a,c)}(y) = b(y - c) \bmod q$, where $b \in \mathbb{Z}_q$ is the unique element such that $ab \equiv 1 \bmod q$. *Exercise:* prove this formula for $d_{(a,c)}$.

With these definitions, the affine cipher is a cryptosystem.

For example, in the affine cipher on $\mathbb{Z}_{11}$, $e_{(9,2)}(5) = 3$ since $9 \times 5 + 2 \equiv 3 \bmod 11$ and, as expected, $d_{(9,2)}(3) = 5$ since $9 \times 5 \equiv 1 \bmod 11$ (see below) and $5 \times (3 - 2) \equiv 5 \bmod 11$.

To find b, the multiplicative inverse of a in $\mathbb{Z}_q$, you can either do an exhaustive search, or run Euclid's algorithm to find b and s such that $ab + qs = 1$; then $ab \equiv 1 \bmod p$: see the slide after Exercise 4.3.

Quiz on Affine Cipher

Take $q = 13$

- What is $e_{(3,4)}(4)$?

  (A) 2 (B) 3 (C) 5 (D) 16

- Mark the Mole knows that $e_k(12) = 0$. One possible key is $(1, 1)$. What is the unique possible key of the form $(2, c)$?

  (A) $(2, 0)$ (B) $(2, 1)$ (C) $(2, 2)$ (D) $(2, 4)$

- What is the multiplicative inverse of 3 modulo 13? [*Hint:* there are only 12 possibilities, so you could just try them all.]

  (A) 3 (B) 4 (C) 9 (D) 0.333 . . .

- What is $d_{(3,4)}(8)$?

  (A) 4 (B) 8 (C) 10 (D) 12

Quiz on Affine Cipher

Take $q = 13$

- What is $e_{(3,4)}(4)$?

  (A) 2 (B) 3 (C) 5 (D) 16

- Mark the Mole knows that $e_k(12) = 0$. One possible key is $(1, 1)$. What is the unique possible key of the form $(2, c)$?

  (A) $(2, 0)$ (B) $(2, 1)$ (C) $(2, 2)$ (D) $(2, 4)$

- What is the multiplicative inverse of 3 modulo 13? [*Hint:* there are only 12 possibilities, so you could just try them all.]

  (A) 3 (B) 4 (C) 9 (D) 0.333 . . .

- What is $d_{(3,4)}(8)$?

  (A) 4 (B) 8 (C) 10 (D) 12

Quiz on Affine Cipher

Take $q = 13$

- What is $e_{(3,4)}(4)$?

  (A) 2 (B) 3 (C) 5 (D) 16

- Mark the Mole knows that $e_k(12) = 0$. One possible key is $(1, 1)$. What is the unique possible key of the form $(2, c)$?

  (A) $(2, 0)$ (B) $(2, 1)$ (C) $(2, 2)$ (D) $(2, 4)$

- What is the multiplicative inverse of 3 modulo 13? [*Hint:* there are only 12 possibilities, so you could just try them all.]

  (A) 3 (B) 4 (C) 9 (D) 0.333 . . .

- What is $d_{(3,4)}(8)$?

  (A) 4 (B) 8 (C) 10 (D) 12

Quiz on Affine Cipher

Take $q = 13$

- What is $e_{(3,4)}(4)$?

  (A) 2 (B) 3 (C) 5 (D) 16

  Mark the Mole knows that $e_k(12) = 0$. Possible keys include $(1, 1)$ and $(2, 2)$. How many are there in total?

  (A) 2 (B) 12 (C) 13 (D) not enough information

- What is the multiplicative inverse of 3 modulo 13? [*Hint:* there are only 12 possibilities, so you could just try them all.]

  (A) 3 (B) 4 (C) 9 (D) 0.333 . . .

- What is $d_{(3,4)}(8)$?

  (A) 4 (B) 8 (C) 10 (D) 12

Quiz on Affine Cipher

Take $q = 13$

- What is $e_{(3,4)}(4)$?

  (A) 2 (B) 3 (C) 5 (D) 16

  Mark the Mole knows that $e_k(12) = 0$. Possible keys include $(1, 1)$ and $(2, 2)$. How many are there in total?

  (A) 2 (B) 12 (C) 13 (D) not enough information

  Thus even knowing a plaintext/ciphertext pair does not determine the key.

- What is the multiplicative inverse of 3 modulo 13? [*Hint:* there are only 12 possibilities, so you could just try them all.]

  (A) 3 (B) 4 (C) 9 (D) 0.333 . . .

- What is $d_{(3,4)}(8)$?

  (A) 4 (B) 8 (C) 10 (D) 12

Quiz on Affine Cipher

Take $q = 13$

- What is $e_{(3,4)}(4)$?

  (A) 2 (B) 3 (C) 5 (D) 16

  Mark the Mole knows that $e_k(12) = 0$. Possible keys include $(1, 1)$ and $(2, 2)$. How many are there in total?

  (A) 2 (B) 12 (C) 13 (D) not enough information

  Thus even knowing a plaintext/ciphertext pair does not determine the key.

- What is the multiplicative inverse of 3 modulo 13? [*Hint:* there are only 12 possibilities, so you could just try them all.]

  (A) 3 (B) 4 (C) 9 (D) 0.333 . . .

  Since $3 \times 4 = 12 \equiv -1 \bmod 13$, and so $3 \times (-4) \equiv 1 \bmod 13$, the inverse is $-4 \equiv 9 \bmod 13$. It's okay to write $1/3$ as long as you understand that it means 9 in this context, but $0.333\ldots$ is just wrong.

- What is $d_{(3,4)}(8)$?

  (A) 4 (B) 8 (C) 10 (D) 12

Quiz on Affine Cipher

Take $q = 13$

- What is $e_{(3,4)}(4)$?

  (A) 2 (B) 3 (C) 5 (D) 16

  Mark the Mole knows that $e_k(12) = 0$. Possible keys include $(1, 1)$ and $(2, 2)$. How many are there in total?

  (A) 2 (B) 12 (C) 13 (D) not enough information

  Thus even knowing a plaintext/ciphertext pair does not determine the key.

- What is the multiplicative inverse of 3 modulo 13? [*Hint:* there are only 12 possibilities, so you could just try them all.]

  (A) 3 (B) 4 (C) 9 (D) 0.333 . . .

  Since $3 \times 4 = 12 \equiv -1 \bmod 13$, and so $3 \times (-4) \equiv 1 \bmod 13$, the inverse is $-4 \equiv 9 \bmod 13$. It's okay to write $1/3$ as long as you understand that it means 9 in this context, but $0.333\ldots$ is just wrong.

- What is $d_{(3,4)}(8)$?

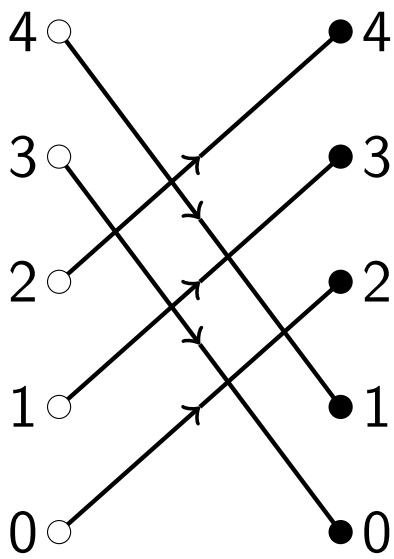
  (A) 4 (B) 8 (C) 10 (D) 12

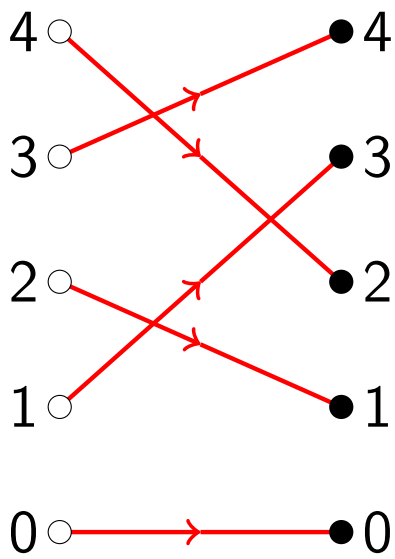
  $d_{(a,c)}(y) = b(y - c) \bmod q$ gives $9 \times (8 - 4) \equiv 10 \bmod 13$.

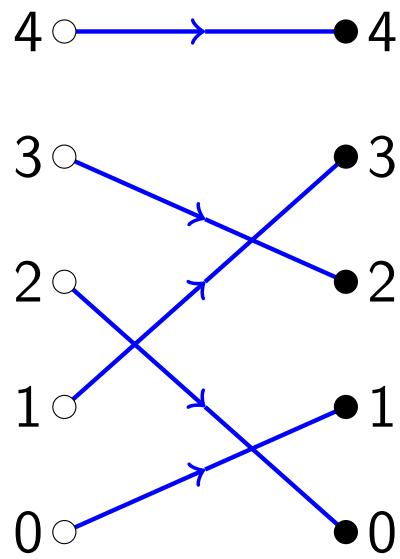
Affine Cipher

Exercise 4.3

The diagrams below show three encryption functions from the affine cipher when $q = 5$. Find the keys.







Quiz: the red key is

(A) $(0, 3)$ (B) $(1, 3)$ (C) $(3, 1)$ (D) $(3, 0)$

and the blue key is

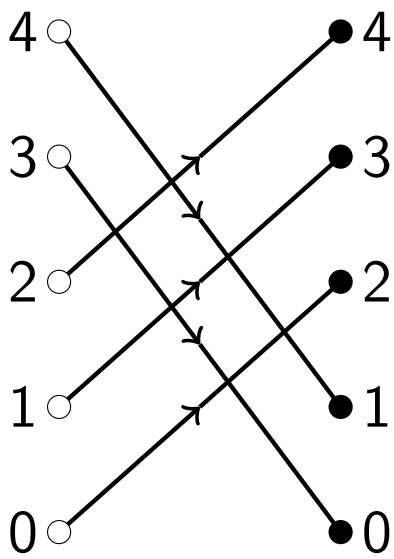
(A) $(0, 1)$ (B) $(2, 1)$ (C) $(3, 1)$ (D) $(2, -4)$

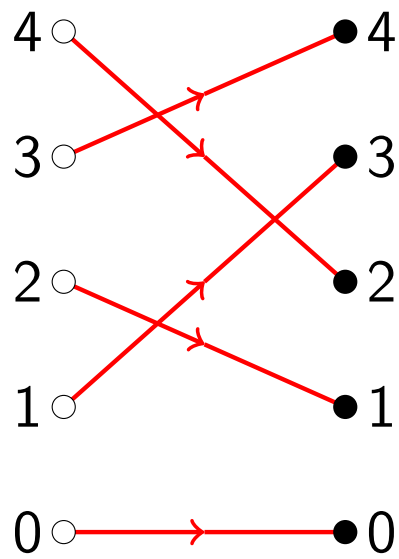
In Question 1 on Problem Sheet 3 you are asked to show that the affine cipher has perfect secrecy.

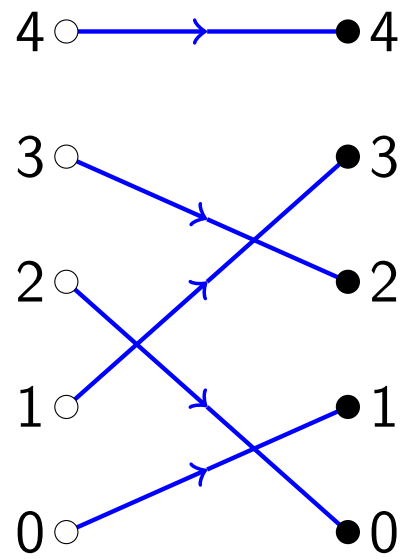
Affine Cipher

Exercise 4.3

The diagrams below show three encryption functions from the affine cipher when $q = 5$. Find the keys.







Quiz: the red key is

(A) $(0, 3)$ (B) $(1, 3)$ (C) $(3, 1)$ (D) $(3, 0)$

and the blue key is

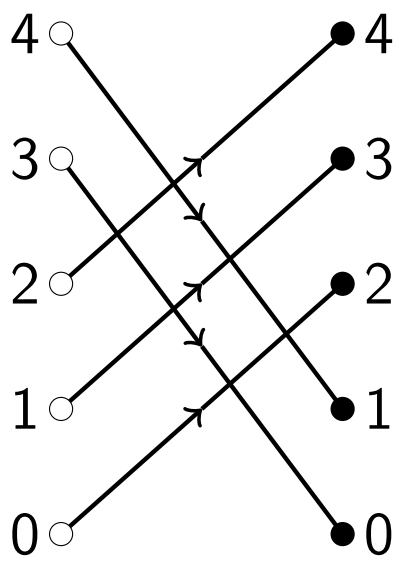
(A) $(0, 1)$ (B) $(2, 1)$ (C) $(3, 1)$ (D) $(2, -4)$

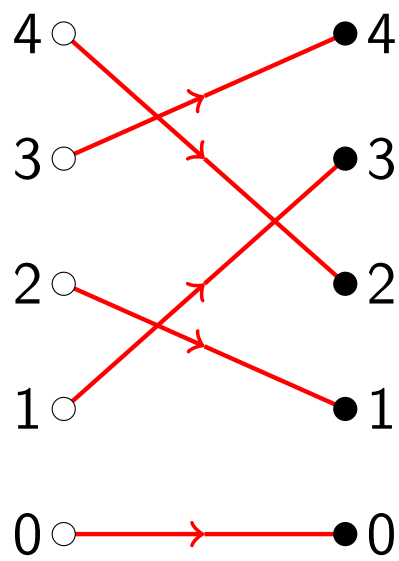
In Question 1 on Problem Sheet 3 you are asked to show that the affine cipher has perfect secrecy.

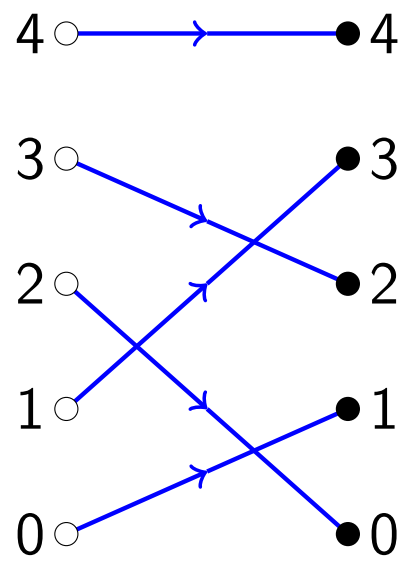
Affine Cipher

Exercise 4.3

The diagrams below show three encryption functions from the affine cipher when $q = 5$. Find the keys.







Quiz: the red key is

(A) $(0, 3)$ (B) $(1, 3)$ (C) $(3, 1)$ (D) $(3, 0)$

and the blue key is

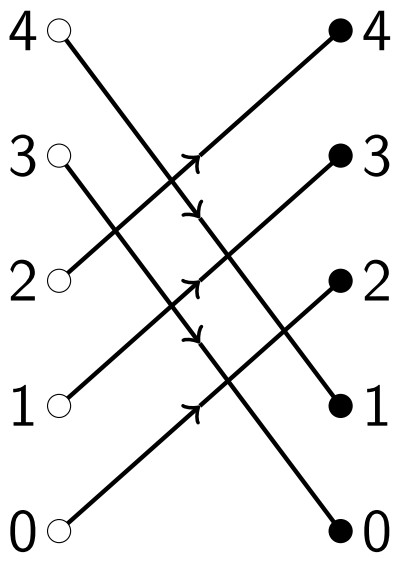
(A) $(0, 1)$ (B) $(2, 1)$ (C) $(3, 1)$ (D) $(2, -4)$

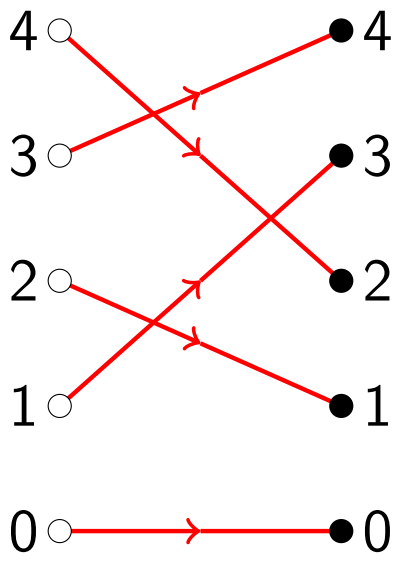
In Question 1 on Problem Sheet 3 you are asked to show that the affine cipher has perfect secrecy.

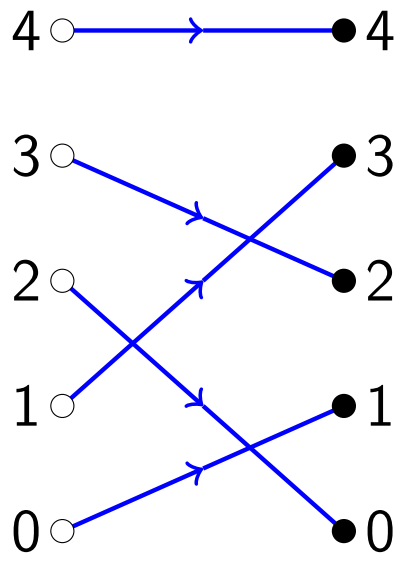
Affine Cipher

Exercise 4.3

The diagrams below show three encryption functions from the affine cipher when $q = 5$. Find the keys.







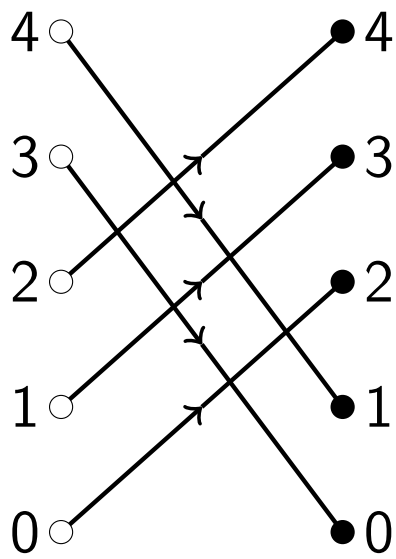
Quiz: How many keys are there in the affine cipher on $\mathbb{Z}_5$?

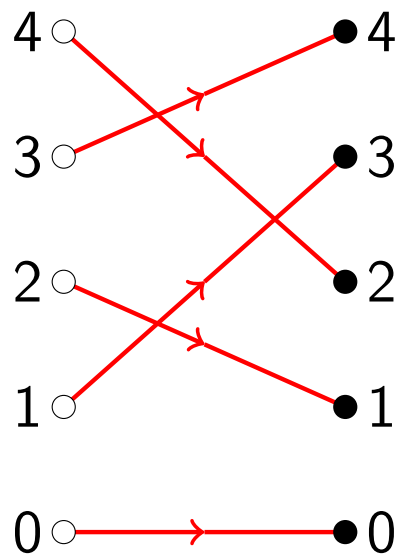
(A) 4 (B) 5 (C) 20 (D) not enough information

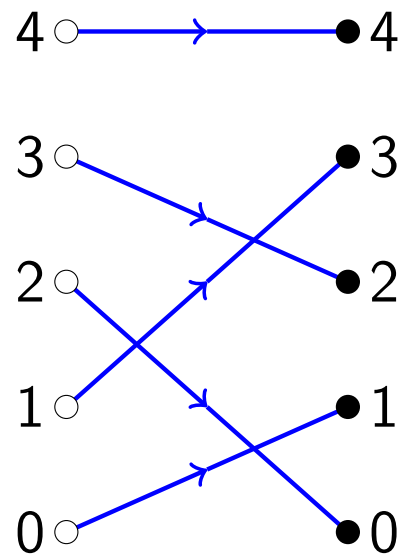
Affine Cipher

Exercise 4.3

The diagrams below show three encryption functions from the affine cipher when $q = 5$. Find the keys.







Quiz: How many keys are there in the affine cipher on $\mathbb{Z}_5$?

(A) 4 (B) 5 (C) 20 (D) not enough information

Since the keys are all (a, c) where $a, c \in \mathbb{Z}_5$ and $a \neq 0$. There are four choices for a then 5 independent choices for c, so $4 \times 5 = 20$ keys. We saw earlier that there are 4 keys (a, c) such that $e_{(a,c)}(2) = 0$.

Inverses in Modular Arithmetic

There is an efficient way to compute modular inverses when q is large using Euclid's Algorithm. This is useful for the affine cipher, and essential for the RSA Cryptosystem which we'll see in Part D of the course on Public Key Cryptography.

- For instance, in $\mathbb{Z}_{61}$, to find 7^{-1}, we run Euclid's Algorithm getting $61 = 8 \times 7 + 5$, $7 = 1 \times 5 + 2$ and $5 = 2 \times 2 + 1$, ending with the expected highest common factor of 1. Hence, working back

$$\begin{aligned} 1 &= 5 - 2 \times 2 = 5 - 2 \times (7 - 5) = 3 \times 5 - 2 \times 7 \\ &= 3 \times (61 - 8 \times 7) - 2 \times 7 = 3 \times 61 - 26 \times 7. \end{aligned}$$

  and so $7^{-1} = -26 \equiv 35 \bmod 61$.

(a) Use Euclid's Algorithm to find b and s such that $17b + 257s = 1$.

Inverses in Modular Arithmetic

There is an efficient way to compute modular inverses when q is large using Euclid's Algorithm. This is useful for the affine cipher, and essential for the RSA Cryptosystem which we'll see in Part D of the course on Public Key Cryptography.

- For instance, in $\mathbb{Z}_{61}$, to find 7^{-1}, we run Euclid's Algorithm getting $61 = 8 \times 7 + 5$, $7 = 1 \times 5 + 2$ and $5 = 2 \times 2 + 1$, ending with the expected highest common factor of 1. Hence, working back

$$1 = 5 - 2 \times 2 = 5 - 2 \times (7 - 5) = 3 \times 5 - 2 \times 7$$
$$= 3 \times (61 - 8 \times 7) - 2 \times 7 = 3 \times 61 - 26 \times 7.$$

  and so $7^{-1} = -26 \equiv 35 \bmod 61$.

(a) Use Euclid's Algorithm to find b and s such that $17b + 257s = 1$.

We have $257 = 15 \times 17 + 2$ and $17 = 8 \times 2 + 1$, hence

$1 = 17 - 8 \times 2 = 17 - 8 \times (257 - 15 \times 17) = 121 \times 17 - 8 \times 257.$

So $b = 121$ and $s = 8$.

Quiz on Inverses in Modular Arithmetic and Affine Cipher

(b) Which formula below defines the inverse function to $e_{(17,1)}$ in the affine cipher on $\mathbb{Z}_{257}$?

(A) $17y + 1$ (B) $121y - 1$ (C) $121y + 240$ (D) $121y + 136$

(c) True or false: the decryption function $d_{(17,1)}$ is equal to an encryption function in the affine cipher on $\mathbb{Z}_{257}$?

(A) False (B) True

(d) (Optional.) Bob thinks that he can improve on the affine cipher on $\mathbb{Z}_p$ by encrypting twice, using two different keys (a, c) and (a', c'), so the encryption function for his double key is $e_{(a,c),(a',c')}(x) = a'(ax + c) + c'$. Is Bob's 'composed' cryptosystem better than the original affine cipher?

(A) No (B) Yes

Quiz on Inverses in Modular Arithmetic and Affine Cipher

(b) Which formula below defines the inverse function to $e_{(17,1)}$ in the affine cipher on $\mathbb{Z}_{257}$?

(A) $17y + 1$ (B) $121y - 1$ (C) $121y + 240$ (D) $121y + 136$

(c) True or false: the decryption function $d_{(17,1)}$ is equal to an encryption function in the affine cipher on $\mathbb{Z}_{257}$?

(A) False (B) True

(d) (Optional.) Bob thinks that he can improve on the affine cipher on $\mathbb{Z}_p$ by encrypting twice, using two different keys (a, c) and (a', c'), so the encryption function for his double key is $e_{(a,c),(a',c')}(x) = a'(ax + c) + c'$. Is Bob's 'composed' cryptosystem better than the original affine cipher?

(A) No (B) Yes

Quiz on Inverses in Modular Arithmetic and Affine Cipher

(b) Which formula below defines the inverse function to $e_{(17,1)}$ in the affine cipher on $\mathbb{Z}_{257}$?

(A) $17y+1$ (B) $121y-1$ (C) $121y+240$ (D) $121y+136$

(c) True or false: the decryption function $d_{(17,1)}$ is equal to an encryption function in the affine cipher on $\mathbb{Z}_{257}$?

(A) False (B) True

It is $e_{(121,136)}$ by the previous part.

(d) (Optional.) Bob thinks that he can improve on the affine cipher on $\mathbb{Z}_p$ by encrypting twice, using two different keys (a, c) and (a', c'), so the encryption function for his double key is $e_{(a,c),(a',c')}(x) = a'(ax+c)+c'$. Is Bob's 'composed' cryptosystem better than the original affine cipher?

(A) No (B) Yes

Quiz on Inverses in Modular Arithmetic and Affine Cipher

(b) Which formula below defines the inverse function to $e_{(17,1)}$ in the affine cipher on $\mathbb{Z}_{257}$?

(A) $17y+1$ (B) $121y-1$ (C) $121y+240$ (D) $121y+136$

(c) True or false: the decryption function $d_{(17,1)}$ is equal to an encryption function in the affine cipher on $\mathbb{Z}_{257}$?

(A) False (B) True

It is $e_{(121,136)}$ by the previous part.

(d) (Optional.) Bob thinks that he can improve on the affine cipher on $\mathbb{Z}_p$ by encrypting twice, using two different keys (a,c) and (a',c'), so the encryption function for his double key is $e_{(a,c),(a',c')}(x) = a'(ax+c)+c'$. Is Bob's 'composed' cryptosystem better than the original affine cipher?

(A) No (B) Yes

Because

$$a'(ax+c)+c' = a'ax+(a'c+c') = e_{(a'a \bmod p,\, a'c+c' \bmod p)}$$

so the new encryption function is the same as an encryption function in the affine cipher.

Quiz on Inverses in Modular Arithmetic and Affine Cipher

(b) Which formula below defines the inverse function to $e_{(17,1)}$ in the affine cipher on $\mathbb{Z}_{257}$?

(A) $17y+1$ (B) $121y-1$ (C) $121y+240$ (D) $121y+136$

(c) True or false: the decryption function $d_{(17,1)}$ is equal to an encryption function in the affine cipher on $\mathbb{Z}_{257}$?

(A) False (B) True

It is $e_{(121,136)}$ by the previous part.

(d) (Optional.) Bob thinks that he can improve on the affine cipher on $\mathbb{Z}_p$ by encrypting twice, using two different keys (a,c) and (a',c'), so the encryption function for his double key is $e_{(a,c),(a',c')}(x) = a'(ax+c)+c'$. Is Bob's 'composed' cryptosystem better than the original affine cipher?

(A) No (B) Yes

If you have done or are doing a group theory course, you might notice that the encryption functions in the affine cipher form a group. For instance, the identity is $e_{(1,0)}$. Inverses were seen in (c) and closure in (d).

Attacks on the Affine Cipher

Exercise 4.4

Consider the affine cipher on $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.

(i) Suppose that Eve observes the ciphertext 2. Does she learn anything about the key? (Assume she has no knowledge about the plaintexts, so all plaintexts are equally likely.)

(A) No (B) Yes

(ii) Suppose that Mark knows that $e_{(a,c)}(1) = 2$. How many possible keys are there?

(A) 3 (B) 4 (C) 5 (D) 20

(iii) Mark later learns m such that $e_{(a,c)}(2) = m \in \mathbb{Z}_5$. What in terms of m is the key?

(A) $(2, 0)$

(B) $(m - 4, -m + 4)$

(C) $(m - 4 \bmod 5, -m + 4 \bmod 5)$

(D) $(m - 2 \bmod 5, -m + 4 \bmod 5)$

(A) (B) (C) (D)

Attacks on the Affine Cipher

Exercise 4.4

Consider the affine cipher on $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.

(i) Suppose that Eve observes the ciphertext 2. Does she learn anything about the key? (Assume she has no knowledge about the plaintexts, so all plaintexts are equally likely.)

(A) No (B) Yes

(ii) Suppose that Mark knows that $e_{(a,c)}(1) = 2$. How many possible keys are there?

(A) 3 (B) 4 (C) 5 (D) 20

(iii) Mark later learns m such that $e_{(a,c)}(2) = m \in \mathbb{Z}_5$. What in terms of m is the key?

(A) $(2, 0)$

(B) $(m - 4, -m + 4)$

(C) $(m - 4 \bmod 5, -m + 4 \bmod 5)$

(D) $(m - 2 \bmod 5, -m + 4 \bmod 5)$

(A) (B) (C) (D)

Attacks on the Affine Cipher

Exercise 4.4

Consider the affine cipher on $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.

(i) Suppose that Eve observes the ciphertext 2. Does she learn anything about the key? (Assume she has no knowledge about the plaintexts, so all plaintexts are equally likely.)

(A) No (B) Yes

(ii) Suppose that Mark knows that $e_{(a,c)}(1) = 2$. How many possible keys are there?

(A) 3 (B) 4 (C) 5 (D) 20

(iii) Mark later learns m such that $e_{(a,c)}(2) = m \in \mathbb{Z}_5$. What in terms of m is the key?

(A) $(2, 0)$

(B) $(m - 4, -m + 4)$

(C) $(m - 4 \bmod 5, -m + 4 \bmod 5)$

(D) $(m - 2 \bmod 5, -m + 4 \bmod 5)$

(A) (B) (C) (D)

Attacks on the Affine Cipher

Exercise 4.4

Consider the affine cipher on $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.

(i) Suppose that Eve observes the ciphertext 2. Does she learn anything about the key? (Assume she has no knowledge about the plaintexts, so all plaintexts are equally likely.)

(A) No (B) Yes

(ii) Suppose that Mark knows that $e_{(a,c)}(1) = 2$. How many possible keys are there?

(A) 3 (B) 4 (C) 5 (D) 20

(iii) Mark later learns m such that $e_{(a,c)}(2) = m \in \mathbb{Z}_5$. What in terms of m is the key?

(A) $(2, 0)$

(B) $(m - 4, -m + 4)$

(C) $(m - 4 \bmod 5, -m + 4 \bmod 5)$

(D) $(m - 2 \bmod 5, -m + 4 \bmod 5)$

(A) (B) (C) (D)

Attack Models

In each of the *attack models* below, we suppose that Alice sends ciphertexts to Bob encrypted using the key $k \in \mathcal{K}$. The aim of the adversary (Eve or Mark) is to determine all or part of k.

- *Known ciphertext*. Eve knows $e_k(x) \in \mathcal{C}$.
- *Known plaintext and ciphertext*. Mark knows $x \in \mathcal{P}$ and $e_k(x) \in \mathcal{C}$.
- *Chosen plaintext*. Mark may choose any $x \in \mathcal{P}$ and is given the encryption $e_k(x)$.
- *Chosen ciphertext*. Mark may choose any $y \in \mathcal{C}$ and is given the decryption $d_k(y)$.

Each attack model has a generalization where the adversary observes or chooses multiple plaintexts and/or ciphertexts.

Attack Models: Remarks

Remark 4.5

(1) In Example 2.5 we saw that (almost all) of the key in a substitution cipher can be deduced from a sufficiently long ciphertext. So the substitution cipher is broken by a *known ciphertext attack*.

(2) All the cryptosystems so far are broken by a *chosen plaintext attack*. By the general version of Example 4.4, the affine cipher requires two chosen plaintexts; by Question 4 on Sheet 2, the substitution cipher and the Vigenère cipher just one.

Exercise: How many chosen plaintexts are needed to break the numeric one-time pad?

(A) 1 (B) 2 (C) 4 (D) depends on key

How many known plaintext/ciphertext pairs are need to break the numeric one-time pad?

(A) 1 (B) 2 (C) 4 (D) depends on key

Attack Models: Remarks

Remark 4.5

(1) In Example 2.5 we saw that (almost all) of the key in a substitution cipher can be deduced from a sufficiently long ciphertext. So the substitution cipher is broken by a *known ciphertext attack*.

(2) All the cryptosystems so far are broken by a *chosen plaintext attack*. By the general version of Example 4.4, the affine cipher requires two chosen plaintexts; by Question 4 on Sheet 2, the substitution cipher and the Vigenère cipher just one.

Exercise: How many chosen plaintexts are needed to break the numeric one-time pad?

(A) 1 (B) 2 (C) 4 (D) depends on key

How many known plaintext/ciphertext pairs are need to break the numeric one-time pad?

(A) 1 (B) 2 (C) 4 (D) depends on key

Attack Models: Remarks

Remark 4.5

(1) In Example 2.5 we saw that (almost all) of the key in a substitution cipher can be deduced from a sufficiently long ciphertext. So the substitution cipher is broken by a *known ciphertext attack*.

(2) All the cryptosystems so far are broken by a *chosen plaintext attack*. By the general version of Example 4.4, the affine cipher requires two chosen plaintexts; by Question 4 on Sheet 2, the substitution cipher and the Vigenère cipher just one.

Exercise: How many chosen plaintexts are needed to break the numeric one-time pad?

(A) 1 (B) 2 (C) 4 (D) depends on key

How many known plaintext/ciphertext pairs are need to break the numeric one-time pad?

(A) 1 (B) 2 (C) 4 (D) depends on key

Attack Models: Remarks

Remark 4.5

(1) In Example 2.5 we saw that (almost all) of the key in a substitution cipher can be deduced from a sufficiently long ciphertext. So the substitution cipher is broken by a *known ciphertext attack*.

(2) All the cryptosystems so far are broken by a *chosen plaintext attack*. By the general version of Example 4.4, the affine cipher requires two chosen plaintexts; by Question 4 on Sheet 2, the substitution cipher and the Vigenère cipher just one.

Exercise: How many chosen plaintexts are needed to break the numeric one-time pad?

(A) 1 (B) 2 (C) 4 (D) depends on key

(3) In Parts B and C we will see modern stream and block ciphers where it is believed to be computationally hard to find the key even allowing *unlimited* choices of plaintexts in a *chosen plaintext attack*.

One-time Pad

Fix $n \in \mathbb{N}$. The *one-time pad* is a cryptosystem with plaintexts, ciphertexts and keyspace $\mathcal{A}^n$. You can think of $\mathcal{A}^n$ as all strings of length n. The encryption functions are defined by

$$e_k(x) = (x_0 + k_0, x_1 + k_1, \ldots, x_{n-1} + k_{n-1})$$

where, as in the Vigenère cipher (see Example 2.10), $x_i + k_i$ is computed by converting x_i and k_i to numbers and adding modulo 26. (Note, as before, we number positions from 0.) Thus the one-time pad is the Vigenère cipher when the key has the same length as the plaintext.

To make the cryptosystem practical (see Definition 3.9) we assume that each key is used with the same probability.

Example 4.6

Suppose that $n = 8$. Of the 26^8 keys, suppose (by a $1/26^8$ chance) `zyxwvuts` is chosen. Then

$$e_{\texttt{zyxwvuts}}(\texttt{goodwork}) = \texttt{fmlzrikc}.$$

Example 4.6

Suppose that $n = 8$. Of the 26^8 keys, suppose (by a $1/26^8$ chance) `zyxwvuts` is chosen. Then

$$e_{\texttt{zyxwvuts}}(\texttt{goodwork}) = \texttt{fmlzrikc}.$$

i	1	2	3	4	5	6	7	8
x_i	g	o	o	d	w	o	r	k
	6	14	14	3	22	14	17	10
k_i	z	y	x	v	w	u	t	s
	25	24	23	22	21	20	19	18
$x_i + k_i$	5	12	11	25	17	8	10	2
	f	m	l	z	r	i	k	c

The following proposition is a corollary of Proposition 3.14.

Proposition 4.7

The one-time pad has perfect secrecy.

By the proposition, the one-time pad is secure against a known ciphertext attack with *one* ciphertext.

Reminder of Proposition 3.14

Proposition 3.14 (Converse to Theorem 3.12(d))

Suppose that $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$, that each key is used with equal probability, and for all $x \in \mathcal{P}$ and $y \in \mathcal{C}$, there exists a unique $k \in \mathcal{K}$ such that $e_k(x) = y$. Then the cryptosystem has perfect secrecy and each ciphertext is equally likely.

In the one-time pad, for all $x \in \mathcal{A}^n$ and $y \in \mathcal{A}^n$ there exists a unique $k \in \mathcal{A}^n$ such that $e_k(x) = y$, namely $k = y - x$; here subtraction is done by converting to numbers and then working modulo 26. Therefore Proposition 3.14 applies.

Reminder of Proposition 3.14

Proposition 3.14 (Converse to Theorem 3.12(d))

Suppose that $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$, that each key is used with equal probability, and for all $x \in \mathcal{P}$ and $y \in \mathcal{C}$, there exists a unique $k \in \mathcal{K}$ such that $e_k(x) = y$. Then the cryptosystem has perfect secrecy and each ciphertext is equally likely.

In the one-time pad, for all $x \in \mathcal{A}^n$ and $y \in \mathcal{A}^n$ there exists a unique $k \in \mathcal{A}^n$ such that $e_k(x) = y$, namely $k = y - x$; here subtraction is done by converting to numbers and then working modulo 26. Therefore Proposition 3.14 applies.

Suppose Eve observes the ciphertext `abcdeabcde`. (The special structure is chosen just to make the examples here a bit easier to see by hand.) She can infer the plaintext has length 10, but since this is part of the definition of the keyspace, she already knows this by Kerckhoffs's assumption. She learns nothing more. For instance

- $x = \texttt{university} \iff k = \texttt{abcdeabcde} - \texttt{university} = \texttt{gouiajjukg}$
- $x = \texttt{governance} \iff k = \texttt{abcdeabcde} - \texttt{governance} = \texttt{unhznnbpba}$
- $x = \texttt{ridiculous} \iff k = \texttt{abcdeabcde} - \texttt{ridiculous} = \texttt{jtzvcggojm}$

and so on.

Attacks on the One-time Pad

Example 4.8

The spy-master Alice and her agent Bob have agreed to use the one-time pad. Following Kerckhoffs's Principle, all this is known to Eve. Eve does not know that their key is $k = \texttt{atcldqezyomuua}$.

- Alice's plaintext is $x = \texttt{leaveinstantly}$. She sends $e_k(x) = \texttt{lxcghyrrroznfy}$ to Bob.

Bob calculates

$$\texttt{lxcghyrrroznfy} - \texttt{atcldqezyomuua} = \texttt{leaveinstantly}.$$

Eve cannot guess the plaintext x: for example

$$\begin{aligned} x = \texttt{gototheairport} &\iff k = y - \texttt{gototheairport} \\ &\qquad = \texttt{fjjsornrjxkzof} \\ x = \texttt{meetmeonbridge} &\iff k = y - \texttt{meetmeonbridge} \\ &\qquad = \texttt{ztynvudeqxrkzu} \end{aligned}$$

For each guessed plaintext there is a unique possible key. Since keys are equiprobable, this proves that a single known ciphertext attack reveals no information about the plaintext.

Reuse of One-time Pad Considered Harmful

Bob now makes a fatal mistake, and re-uses the key k in his reply.

- Bob's plaintext is $x' = \texttt{goingeasttrain}$. He sends $e_k(x') = \texttt{ghkyjuerrhducn}$ to Alice.

Eve now has ciphertexts

$$k + \texttt{leaveinstantly} = \texttt{lxcghyrrroznfy}$$
$$k + \texttt{goingeasttrain} = \texttt{ghkyjuerrhducn}.$$

She subtracts them, working modulo 26 in each position, to obtain $\Delta = \texttt{fqsiyenaahwtdl}$. Note that Δ does not depend on k. (You can use the MATHEMATICA notebook `AlphabetCiphers` to do this.)

The string Δ has the unusual property that there is an English message x' (Bob's plaintext) such that $\Delta + x'$ is another English message (Alice's plaintext). This property is so rare that Eve and her computer can fairly easily deduce x' and $\Delta + x'$, and, from either of these, the key k.

Simplified Model for the Δ Attack

To make this point without the distracting complexity of English getting in the way, consider Example 1.2. In Question 1(d) on Problem Sheet 1:

- x is Bob's mark
- x' is Alice's mark
- k is the key (given to them secretly by Trevor)

Eve observes the ciphertexts

- $y = x + k \bmod 100$ (Bob's mark, encrypted) *and*
- $y' = x' + k \bmod 100$ (Alice's mark, encrypted)

She computes $\Delta = y - y' = x - x' \bmod 100$. Note $\Delta = 0$ if and only if Alice and Bob got the same mark. So Eve learns this much. (Many people wrongly claimed in their answers that Eve could learn nothing.)

The number Δ has the property that there is an exam mark x' such that $\Delta + x'$ is another exam mark. To complete the analogy, we arrange things so that this property is unusual. (Click on.)

Simplified Model for the Δ Attack

Eve observes the ciphertexts

- $y = x + k \bmod 100$ (Bob's mark, encrypted) *and*
- $y' = x' + k \bmod 100$ (Alice's mark, encrypted)

She computes $\Delta = y - y' = x - x' \bmod 100$. Note $\Delta = 0$ if and only if Alice and Bob got the same mark. So Eve learns this much.

The number Δ has the property that there is an exam mark x' such that $\Delta + x'$ is another exam mark. To complete the analogy, we arrange things so that this property is unusual.

Suppose that, perhaps because of 'stepped marking' and Eve's belief about Alice and Bob's likely marks, that she is sure

- $x, x' \in \{42, 45, 48, 52, 55, 58, 62, 65, 68, 72, 75, 78, 82, 85, 88\} = \mathcal{X}$

This set is analogous to the set of reasonable English messages. Suppose that $y = 12$ and $y' = 76$.

- What is Δ?

  (A) -64 (B) 64 (C) 34 (D) 36

- What is the strongest claim that Eve can deduce?

  (A) $x \in \mathcal{X}$ and $x \leq 52$ (B) $x = 42$ (C) $x \in \{42, 52\}$ (D) $x \in \{42, 45, 52\}$

Simplified Model for the Δ Attack

Eve observes the ciphertexts

- $y = x + k \bmod 100$ (Bob's mark, encrypted) *and*
- $y' = x' + k \bmod 100$ (Alice's mark, encrypted)

She computes $\Delta = y - y' = x - x' \bmod 100$. Note $\Delta = 0$ if and only if Alice and Bob got the same mark. So Eve learns this much.

The number Δ has the property that there is an exam mark x' such that $\Delta + x'$ is another exam mark. To complete the analogy, we arrange things so that this property is unusual.

Suppose that, perhaps because of 'stepped marking' and Eve's belief about Alice and Bob's likely marks, that she is sure

- $x, x' \in \{42, 45, 48, 52, 55, 58, 62, 65, 68, 72, 75, 78, 82, 85, 88\} = \mathcal{X}$

This set is analogous to the set of reasonable English messages. Suppose that $y = 12$ and $y' = 76$.

- What is Δ?

  (A) -64 (B) 64 (C) 34 (D) 36

- What is the strongest claim that Eve can deduce?

  (A) $x \in \mathcal{X}$ and $x \leq 52$ (B) $x = 42$ (C) $x \in \{42, 52\}$ (D) $x \in \{42, 45, 52\}$

Simplified Model for the Δ Attack

Eve observes the ciphertexts

- $y = x + k \bmod 100$ (Bob's mark, encrypted) *and*
- $y' = x' + k \bmod 100$ (Alice's mark, encrypted)

She computes $\Delta = y - y' = x - x' \bmod 100$. Note $\Delta = 0$ if and only if Alice and Bob got the same mark. So Eve learns this much.

The number Δ has the property that there is an exam mark x' such that $\Delta + x'$ is another exam mark. To complete the analogy, we arrange things so that this property is unusual.

Suppose that, perhaps because of 'stepped marking' and Eve's belief about Alice and Bob's likely marks, that she is sure

- $x, x' \in \{42, 45, 48, 52, 55, 58, 62, 65, 68, 72, 75, 78, 82, 85, 88\} = \mathcal{X}$

This set is analogous to the set of reasonable English messages. Suppose that $y = 12$ and $y' = 76$.

- What is Δ?

  (A) -64 (B) 64 (C) 34 (D) 36

- What is the strongest claim that Eve can deduce?

  (A) $x \in \mathcal{X}$ and $x \leq 52$ (B) $x = 42$ (C) $x \in \{42, 52\}$ (D) $x \in \{42, 45, 52\}$

Attack on Δ

Going back the alphabetic one-time pad, recall that $\Delta = \texttt{fqsiyenaahwtdl} = x - x'$ where x and x' are plaintexts.

The Haskell code online at `https://repl.it/@mwildon/OneTimePad2` tries all strings x' looking for a string x' such that x' looks 'Englishy' and so does $x = \Delta + x'$. The measure of 'Englishy' is the same trigram log-likelihood statistic used in the hill-climb attack on substitution ciphers (Example 2.7). The score of the pair (x, x') is the sum of the scores for x and x'.

- The output below shows that, considering the first five characters of Δ, the second most highly scored pair (x, x') is (`leave`, `going`).

```
*OneTimePad2> printList $ trigramGuess 0 4 eveDifference
(-19.75127610007881,"hesar","coast")
(-20.711633652210836,"leave","going")
(-21.41072740992255,"slave","nving")
(-22.25680387860219,"ghave","bring")
(-22.91429239440494,"houtc","cycle")
```

Attack on Δ

Going back the alphabetic one-time pad, recall that $\Delta = \texttt{fqsiyenaahwtdl} = x - x'$ where x and x' are plaintexts.

The Haskell code online at `https://repl.it/@mwildon/OneTimePad2` tries all strings x' looking for a string x' such that x' looks 'Englishy' and so does $x = \Delta + x'$. The measure of 'Englishy' is the same trigram log-likelihood statistic used in the hill-climb attack on substitution ciphers (Example 2.7). The score of the pair (x, x') is the sum of the scores for x and x'.

- Considering the next four characters, the correct pair (`inst`, `east`) is the 4th choice.

```
*OneTimePad2> printList $ trigramGuess 5 8 eveDifference
(-12.380742455780556,"mate","inte")
(-13.10527108712355,"seed","ored")
(-13.352281132485166,"oren","keen")
(-13.734263689647308,"inst","east")
(-13.805063759279664,"orep","keep")
```

Attack on Δ

Going back the alphabetic one-time pad, recall that $\Delta = \texttt{fqsiyenaahwtdl} = x - x'$ where x and x' are plaintexts.

The Haskell code online at `https://repl.it/@mwildon/OneTimePad2` tries all strings x' looking for a string x' such that x' looks 'Englishy' and so does $x = \Delta + x'$. The measure of 'Englishy' is the same trigram log-likelihood statistic used in the hill-climb attack on substitution ciphers (Example 2.7). The score of the pair (x, x') is the sum of the scores for x and x'.

- Considering the final five characters, the correct pair (`antly`, `train`) is the 7th choice.

```
*OneTimePad2> printList $ trigramGuess 9 13 eveDifference
(-21.881306681100888,"intly","brain")
(-22.069398992763965,"weere","pilot")
(-22.49826573571906,"apart","tthoi")
(-22.71310960413667,"celle","visit")
(-22.730882942814812,"hherh","allow")
(-22.775187228327354,"spare","lthot")
(-22.805037001211357,"antly","train")
(-23.48981205658887,"hello","aisid")
```

Attack on Δ

Going back the alphabetic one-time pad, recall that $\Delta = \texttt{fqsiyenaahwtdl} = x - x'$ where x and x' are plaintexts.

The Haskell code online at `https://repl.it/@mwildon/OneTimePad2` tries all strings x' looking for a string x' such that x' looks 'Englishy' and so does $x = \Delta + x'$. The measure of 'Englishy' is the same trigram log-likelihood statistic used in the hill-climb attack on substitution ciphers (Example 2.7). The score of the pair (x, x') is the sum of the scores for x and x'.

- Considering the final five characters, the correct pair (`antly`, `train`) is the 7th choice.

```
*OneTimePad2> printList $ trigramGuess 9 13 eveDifference
(-21.881306681100888,"intly","brain")
(-22.069398992763965,"weere","pilot")
(-22.49826573571906,"apart","tthoi")
(-22.71310960413667,"celle","visit")
(-22.730882942814812,"hherh","allow")
(-22.775187228327354,"spare","lthot")
(-22.805037001211357,"antly","train")
(-23.48981205658887,"hello","aisid")
```

One has to experiment to find to split at 5 and then 4 characters, but still, this shows that x and x' can be found quite easily from Δ.

Venona Decrypts

The Venona project collected Soviet messages encrypted using one-time pads. Between 1942 and 1945 many pads were produced using duplicated keys. This re-use was detected by NSA cryptographers.

Venona decrypts were important evidence (although not usable in court) against Klaus Fuchs and Ethel and Julius Rosenberg.

Other Attacks on One-time-pad

The previous example shows that the one-time pad is broken by a known ciphertext attack with *two* known ciphertexts.

- Can the one-time pad be broken (i.e. the key k found) using a single chosen plaintext attack? Assume you know the length n, so your chosen plaintext should be a string in $\mathcal{A}^n$.

  (A) No (B) Yes

- Can the one-time pad be broken by a single chosen ciphertext attack?

  (A) No (B) Yes

- Is the one-time pad broken by a single known plaintext / ciphertext pair?

  (A) No (B) Yes

Other Attacks on One-time-pad

The previous example shows that the one-time pad is broken by a known ciphertext attack with *two* known ciphertexts.

- Can the one-time pad be broken (i.e. the key k found) using a single chosen plaintext attack? Assume you know the length n, so your chosen plaintext should be a string in $\mathcal{A}^n$.

  (A) No (B) Yes

  Just encrypt $\mathtt{aa}\ldots\mathtt{a} \in \mathcal{A}^n$ to get k.

- Can the one-time pad be broken by a single chosen ciphertext attack?

  (A) No (B) Yes

- Is the one-time pad broken by a single known plaintext / ciphertext pair?

  (A) No (B) Yes

Other Attacks on One-time-pad

The previous example shows that the one-time pad is broken by a known ciphertext attack with *two* known ciphertexts.

- Can the one-time pad be broken (i.e. the key k found) using a single chosen plaintext attack? Assume you know the length n, so your chosen plaintext should be a string in $\mathcal{A}^n$.

  (A) No (B) Yes

  Just encrypt $\mathtt{aa}\ldots\mathtt{a} \in \mathcal{A}^n$ to get k.

- Can the one-time pad be broken by a single chosen ciphertext attack?

  (A) No (B) Yes

  Decrypt $\mathtt{aa}\ldots\mathtt{a} \in \mathcal{A}^n$ to get $-k$.

- Is the one-time pad broken by a single known plaintext / ciphertext pair?

  (A) No (B) Yes

Other Attacks on One-time-pad

The previous example shows that the one-time pad is broken by a known ciphertext attack with *two* known ciphertexts.

- Can the one-time pad be broken (i.e. the key k found) using a single chosen plaintext attack? Assume you know the length n, so your chosen plaintext should be a string in $\mathcal{A}^n$.

  (A) No (B) Yes

  Just encrypt $\mathtt{aa}\ldots\mathtt{a} \in \mathcal{A}^n$ to get k.

- Can the one-time pad be broken by a single chosen ciphertext attack?

  (A) No (B) Yes

  Decrypt $\mathtt{aa}\ldots\mathtt{a} \in \mathcal{A}^n$ to get $-k$.

- Is the one-time pad broken by a single known plaintext / ciphertext pair?

  (A) No (B) Yes

  We've seen that given x and $y = e_k(x) = x + k$, its easy to find the key from $k = y - x$.

These all show that one-time pad is strong only when it is used just once, and only by the intended Alice and Bob.

§5 Key Uncertainty and Entropy

Suppose Bob picks $x \in \{0, 1, \ldots, 15\}$. How many yes/no questions does Alice need to guess x? Please **do not** click on until you have thought hard about this, and maybe even played the game with someone.

§5 Key Uncertainty and Entropy

Suppose Bob picks $x \in \{0, 1, \ldots, 15\}$. How many yes/no questions does Alice need to guess x? Please **do not** click on until you have thought hard about this, and maybe even played the game with someone.

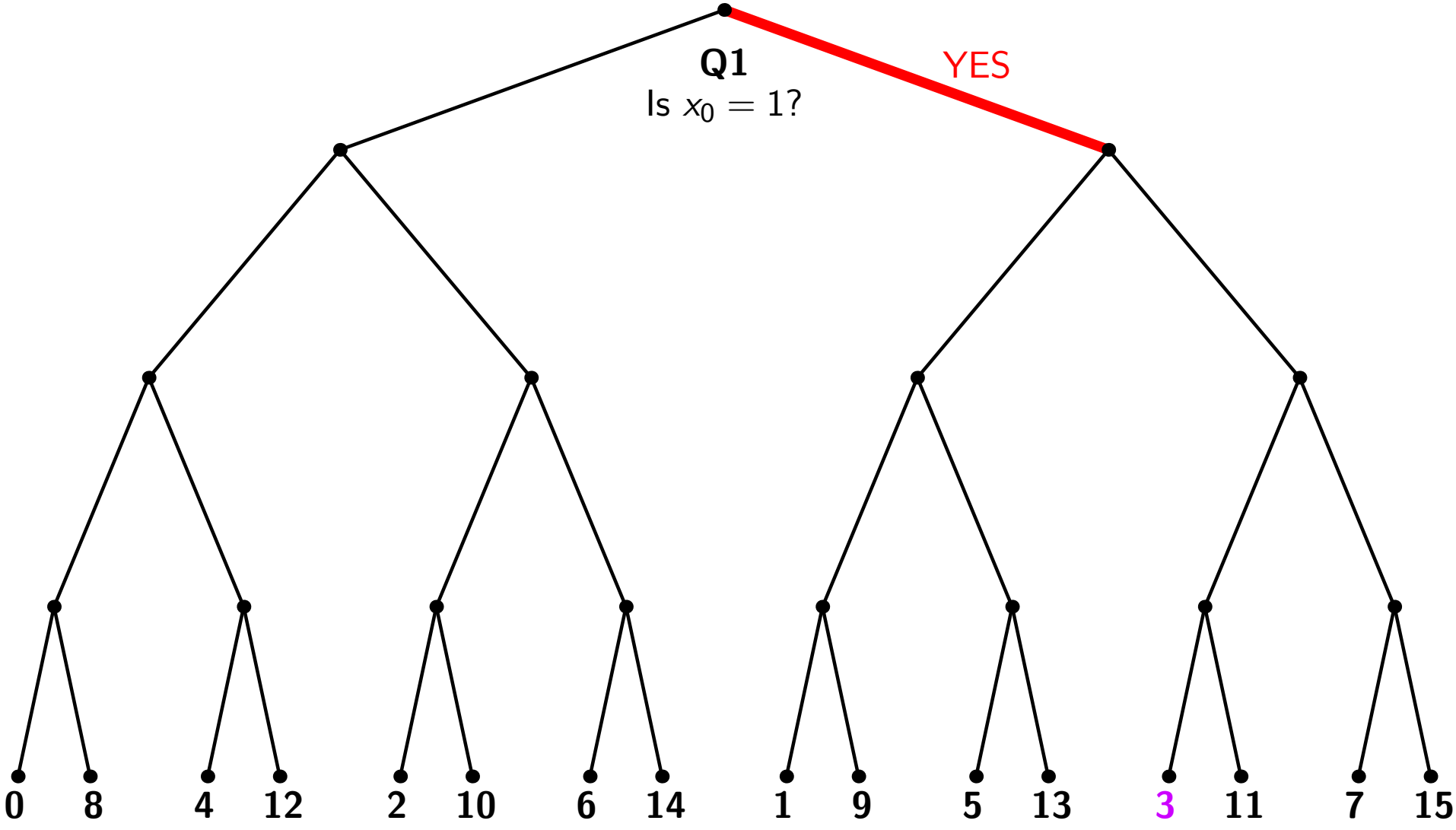
One easy strategy is to ask Bob to write x in binary as $x_3x_2x_1x_0$; then Alice asks about each bit in turn: 'Is $x_0 = 1$?', 'Is $x_1 = 1$?', 'Is $x_2 = 1$?', 'Is $x_3 = 1$?'.

0	0000	4	0100	8	1000	12	1100
1	0001	5	0101	9	1001	13	1101
2	0010	6	0110	10	1010	14	1110
3	0011	7	0111	11	1011	15	1111

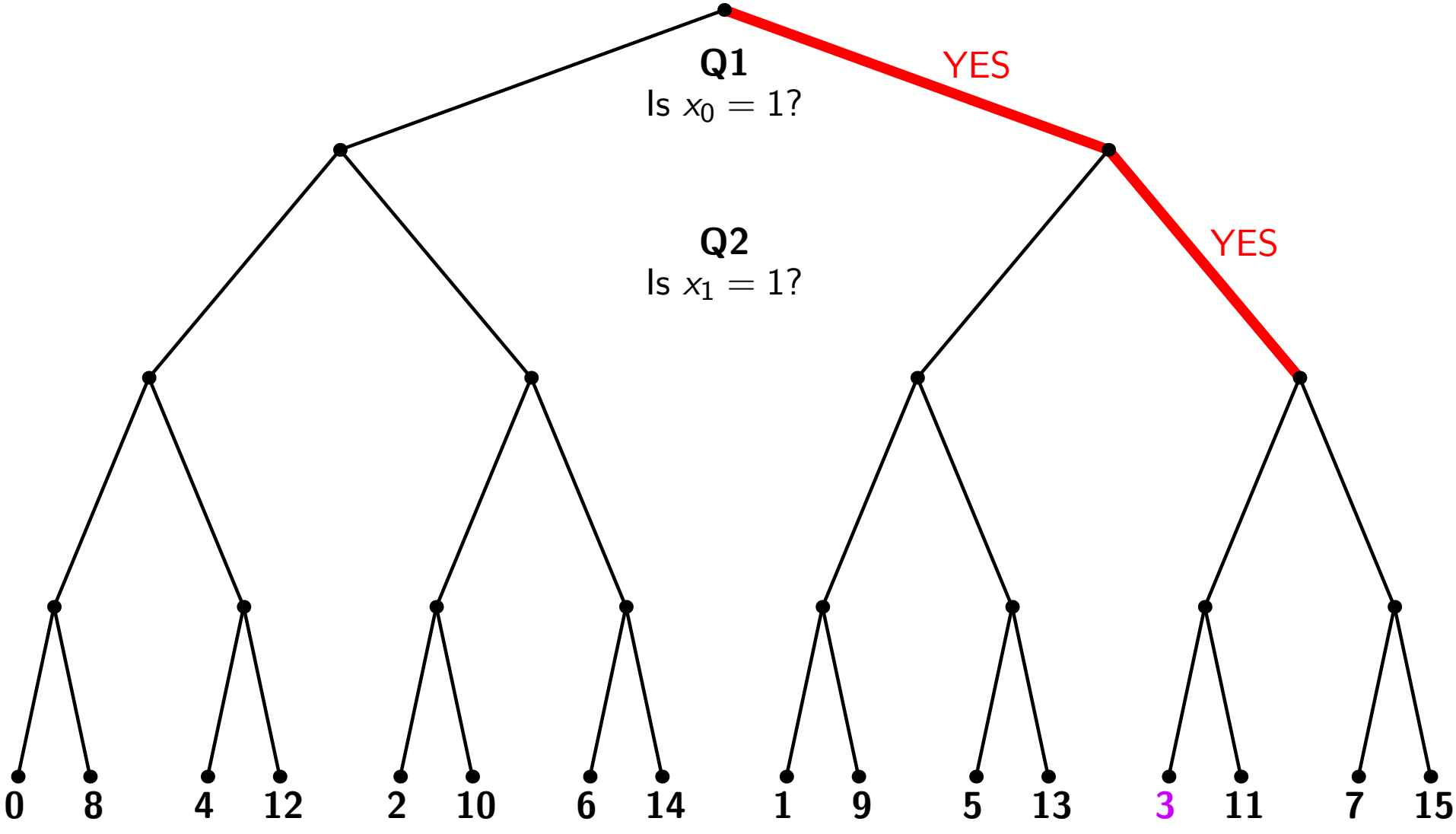
Exercise 5.1

Explain why no questioning strategy can guarantee to use fewer than four questions.

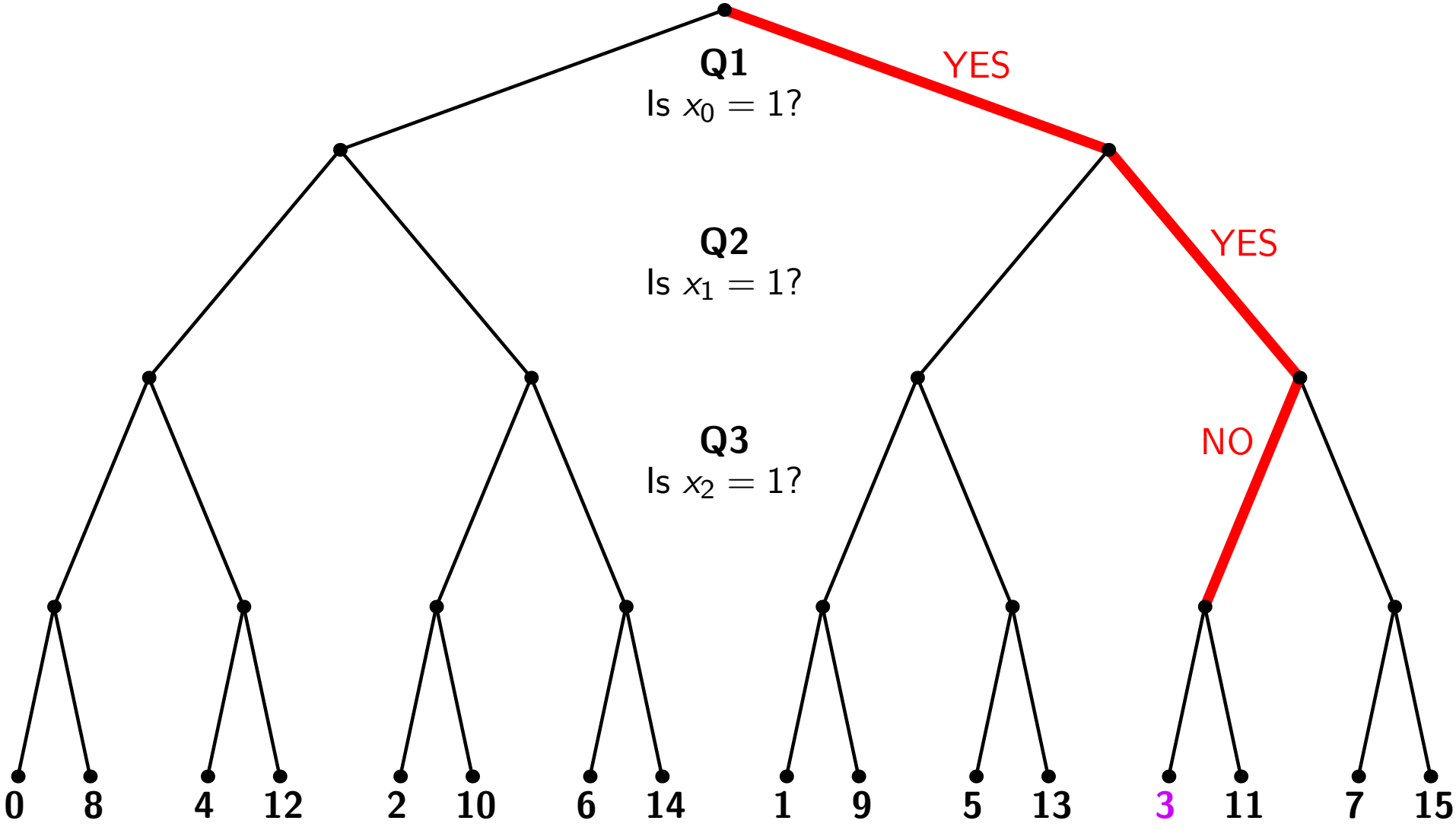
4 Yes/No Questions for 4 Bits of Information



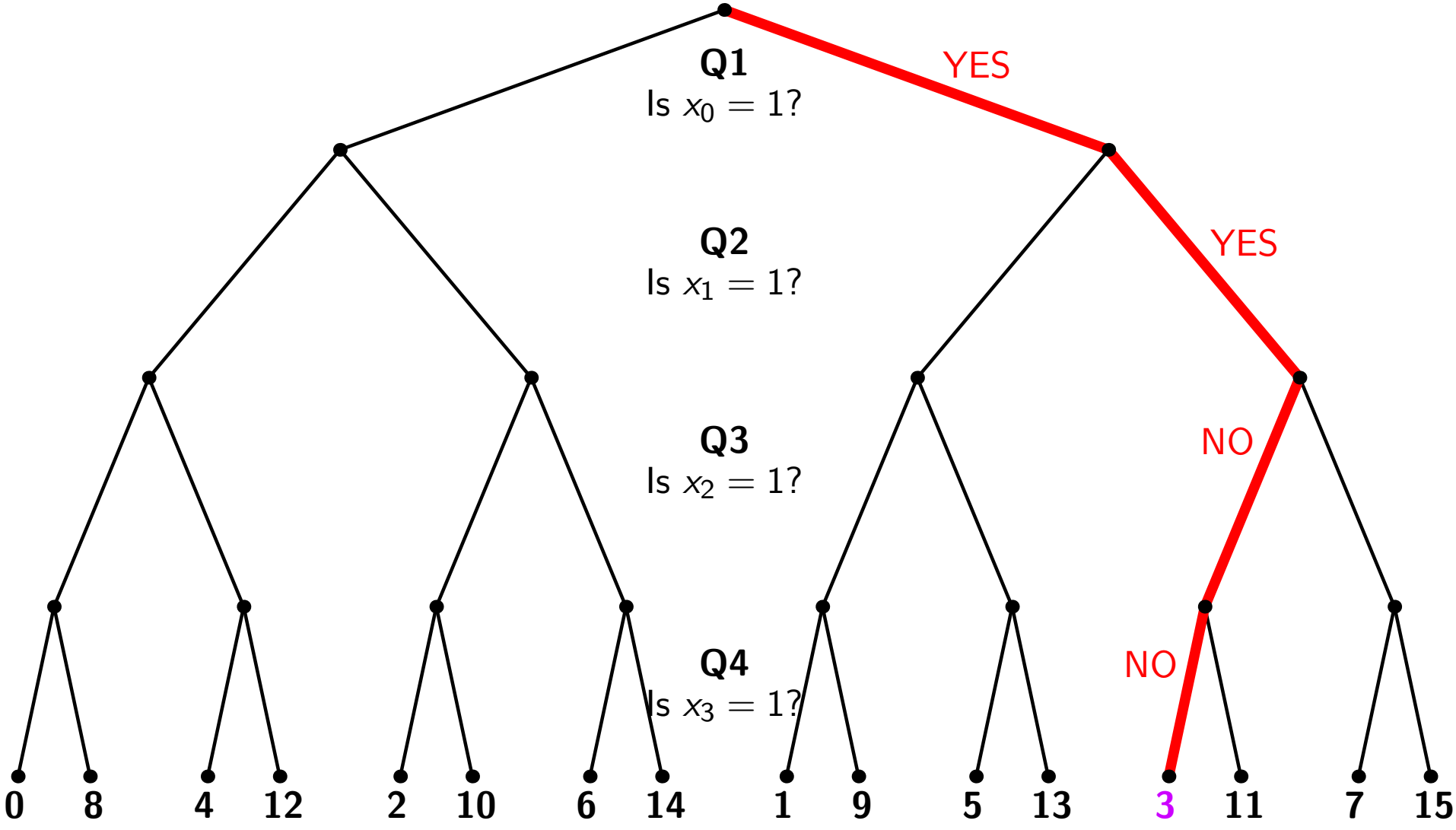
4 Yes/No Questions for 4 Bits of Information



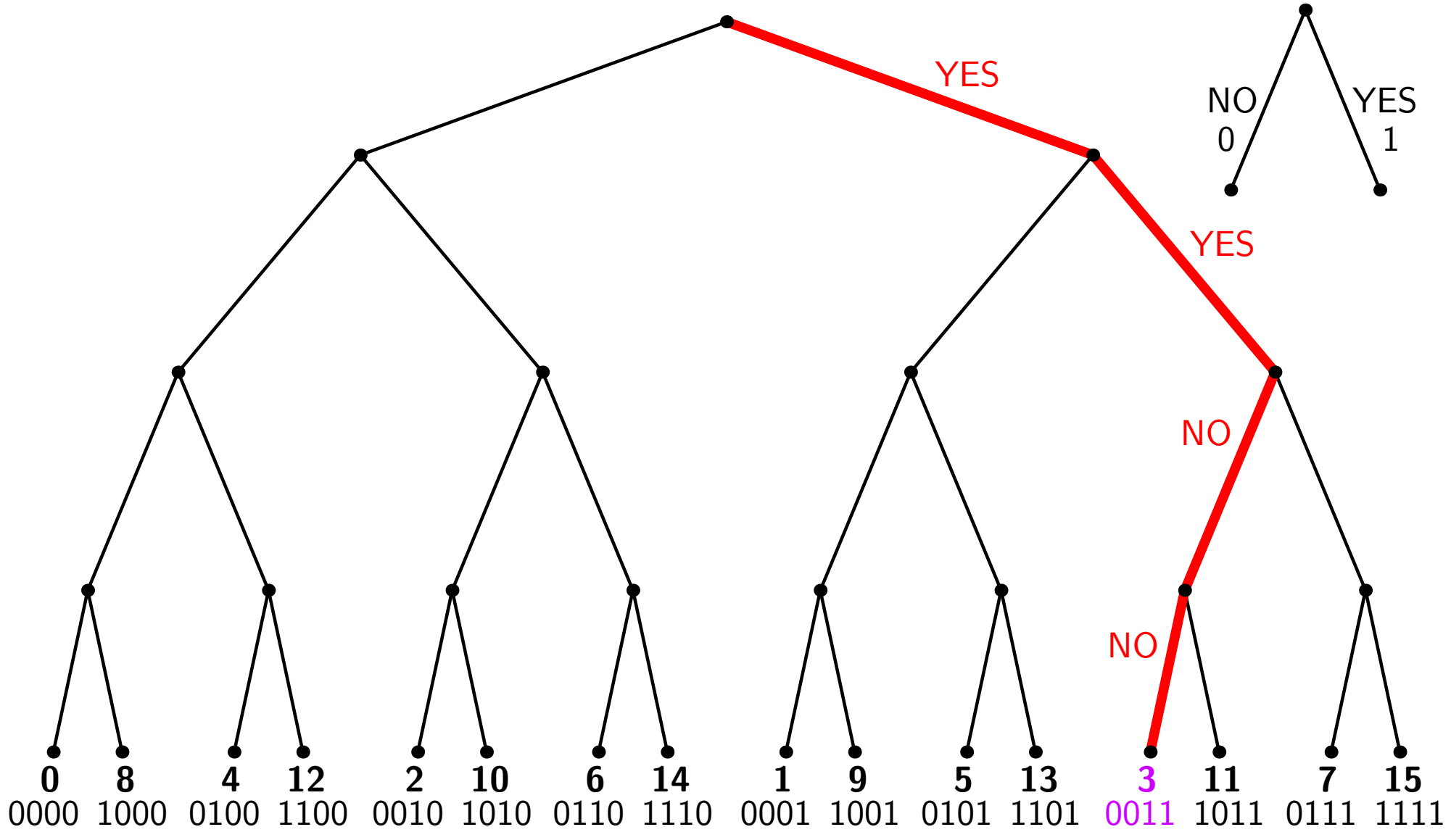
4 Yes/No Questions for 4 Bits of Information



4 Yes/No Questions for 4 Bits of Information



4 Yes/No Questions for 4 Bits of Information



Guessing Games

Example 5.2

We consider the simpler game where Bob's number is in $\{0, 1, 2, 3\}$. Let p_x be the probability that Bob chooses x. (Alice knows Bob very well, so she knows these probabilities.) For each case below, how many questions does Alice need on average, if she chooses the best possible strategy?

(a) $p_0 = p_1 = p_2 = p_3 = \frac{1}{4}$.
(A) $\frac{3}{2}$ (B) 2 (C) 3 (D) depends on Bob

(b) $p_0 = \frac{1}{2}$, $p_1 = \frac{1}{4}$, $p_2 = \frac{1}{4}$, $p_3 = 0$.
(A) 1 (B) $\frac{3}{2}$ (C) 2 (D) 3

(c) $p_0 = \frac{1}{2}$, $p_1 = \frac{1}{4}$, $p_2 = \frac{1}{8}$, $p_3 = \frac{1}{8}$.
(A) 1 (B) $\frac{3}{2}$ (C) $\frac{7}{4}$ (D) 2

Guessing Games

Example 5.2

We consider the simpler game where Bob's number is in $\{0, 1, 2, 3\}$. Let p_x be the probability that Bob chooses x. (Alice knows Bob very well, so she knows these probabilities.) For each case below, how many questions does Alice need on average, if she chooses the best possible strategy?

(a) $p_0 = p_1 = p_2 = p_3 = \frac{1}{4}$.

(A) $\frac{3}{2}$ (B) 2 (C) 3 (D) depends on Bob

This is just the previous exercise.

(b) $p_0 = \frac{1}{2}$, $p_1 = \frac{1}{4}$, $p_2 = \frac{1}{4}$, $p_3 = 0$.

(A) 1 (B) $\frac{3}{2}$ (C) 2 (D) 3

(c) $p_0 = \frac{1}{2}$, $p_1 = \frac{1}{4}$, $p_2 = \frac{1}{8}$, $p_3 = \frac{1}{8}$.

(A) 1 (B) $\frac{3}{2}$ (C) $\frac{7}{4}$ (D) 2

Guessing Games

Example 5.2

We consider the simpler game where Bob's number is in $\{0, 1, 2, 3\}$. Let p_x be the probability that Bob chooses x. (Alice knows Bob very well, so she knows these probabilities.) For each case below, how many questions does Alice need on average, if she chooses the best possible strategy?

(a) $p_0 = p_1 = p_2 = p_3 = \frac{1}{4}$.

(A) $\frac{3}{2}$ (B) 2 (C) 3 (D) depends on Bob

This is just the previous exercise.

(b) $p_0 = \frac{1}{2}$, $p_1 = \frac{1}{4}$, $p_2 = \frac{1}{4}$, $p_3 = 0$.

(A) 1 (B) $\frac{3}{2}$ (C) 2 (D) 3

Alice asks: is your number 0? If yes, done. If not, one more question does it. Average is $\frac{1}{2}1 + \frac{1}{2}2 = \frac{3}{2}$.

(c) $p_0 = \frac{1}{2}$, $p_1 = \frac{1}{4}$, $p_2 = \frac{1}{8}$, $p_3 = \frac{1}{8}$.

(A) 1 (B) $\frac{3}{2}$ (C) $\frac{7}{4}$ (D) 2

Guessing Games

Example 5.2

We consider the simpler game where Bob's number is in $\{0, 1, 2, 3\}$. Let p_x be the probability that Bob chooses x. (Alice knows Bob very well, so she knows these probabilities.) For each case below, how many questions does Alice need on average, if she chooses the best possible strategy?

(a) $p_0 = p_1 = p_2 = p_3 = \frac{1}{4}$.

(A) $\frac{3}{2}$ (B) 2 (C) 3 (D) depends on Bob

This is just the previous exercise.

(b) $p_0 = \frac{1}{2}$, $p_1 = \frac{1}{4}$, $p_2 = \frac{1}{4}$, $p_3 = 0$.

(A) 1 (B) $\frac{3}{2}$ (C) 2 (D) 3

Alice asks: is your number 0? If yes, done. If not, one more question does it. Average is $\frac{1}{2}1 + \frac{1}{2}2 = \frac{3}{2}$.

(c) $p_0 = \frac{1}{2}$, $p_1 = \frac{1}{4}$, $p_2 = \frac{1}{8}$, $p_3 = \frac{1}{8}$.

(A) 1 (B) $\frac{3}{2}$ (C) $\frac{7}{4}$ (D) 2

See video. [*Hint:* modify the previous strategy.]

Guessing Games

Example 5.2

We consider the simpler game where Bob's number is in $\{0, 1, 2, 3\}$. Let p_x be the probability that Bob chooses x. (Alice knows Bob very well, so she knows these probabilities.) For each case below, how many questions does Alice need on average, if she chooses the best possible strategy?

(d) $p_2 = 1, p_0 = p_1 = p_3 = 0$

(A) 0 (B) 1 (C) 2 (D) undefined

Guessing Games

Example 5.2

We consider the simpler game where Bob's number is in $\{0, 1, 2, 3\}$. Let p_x be the probability that Bob chooses x. (Alice knows Bob very well, so she knows these probabilities.) For each case below, how many questions does Alice need on average, if she chooses the best possible strategy?

(d) $p_2 = 1, p_0 = p_1 = p_3 = 0$

(A) 0 (B) 1 (C) 2 (D) undefined

You *know* Bob's number is 0. So no questions are needed. You don't have to ask a question to announce the number! (Compare the previous examples if you doubt this.)

Definition of Entropy

Definition 5.3

Let $\mathcal{X}$ be a finite set.

(i) The *entropy* of a probability distribution p_x on $\mathcal{X}$ is

$$H(p) = -\sum_{x \in \mathcal{X}} p_x \log_2 p_x.$$

(ii) The *entropy* of a random variable X taking values in $\mathcal{X}$ is the entropy of the probability distribution $p_x = \mathbb{P}[X = x]$.

Note that $\log_2$ means logarithm to the base 2, so $\log_2 \frac{1}{2} = -1, \log_2 1 = 0$, $\log_2 2 = 1$, $\log_2 4 = 2$, and generally, $\log_2 2^r = r$ for each $r \in \mathbb{Z}$. If $p_x = 0$ then $-0 \log_2 0$ should be interpreted as $\lim_{p \to 0} -p \log_2 p = 0$.

Quiz: For $r \in \mathbb{N}$, what is $-\frac{1}{2^r} \log_2 \frac{1}{2^r}$?

(A) $\frac{1}{2^r}$ (B) $-\frac{r}{2^r}$ (C) $\frac{r}{2^r}$ (D) r

What is $\log_2 24 - \log_2 9 + \log_2 6$?

(A) 3 (B) $3 + \log_2 3$ (C) 4 (D) $4 - \log_2 3$

Definition of Entropy

Definition 5.3

Let $\mathcal{X}$ be a finite set.

(i) The *entropy* of a probability distribution p_x on $\mathcal{X}$ is

$$H(p) = -\sum_{x \in \mathcal{X}} p_x \log_2 p_x.$$

(ii) The *entropy* of a random variable X taking values in $\mathcal{X}$ is the entropy of the probability distribution $p_x = \mathbb{P}[X = x]$.

Note that $\log_2$ means logarithm to the base 2, so $\log_2 \frac{1}{2} = -1, \log_2 1 = 0$, $\log_2 2 = 1$, $\log_2 4 = 2$, and generally, $\log_2 2^r = r$ for each $r \in \mathbb{Z}$. If $p_x = 0$ then $-0 \log_2 0$ should be interpreted as $\lim_{p \to 0} -p \log_2 p = 0$.

Quiz: For $r \in \mathbb{N}$, what is $-\frac{1}{2^r} \log_2 \frac{1}{2^r}$?

(A) $\frac{1}{2^r}$ (B) -$\frac{r}{2^r}$ (C) $\frac{r}{2^r}$ (D) r

What is $\log_2 24 - \log_2 9 + \log_2 6$?

(A) 3 (B) $3 + \log_2 3$ (C) 4 (D) $4 - \log_2 3$

Definition of Entropy

Definition 5.3

Let $\mathcal{X}$ be a finite set.

(i) The *entropy* of a probability distribution p_x on $\mathcal{X}$ is

$$H(p) = -\sum_{x \in \mathcal{X}} p_x \log_2 p_x.$$

(ii) The *entropy* of a random variable X taking values in $\mathcal{X}$ is the entropy of the probability distribution $p_x = \mathbb{P}[X = x]$.

Note that $\log_2$ means logarithm to the base 2, so $\log_2 \frac{1}{2} = -1, \log_2 1 = 0$, $\log_2 2 = 1$, $\log_2 4 = 2$, and generally, $\log_2 2^r = r$ for each $r \in \mathbb{Z}$. If $p_x = 0$ then $-0 \log_2 0$ should be interpreted as $\lim_{p \to 0} -p \log_2 p = 0$.

Quiz: For $r \in \mathbb{N}$, what is $-\frac{1}{2^r} \log_2 \frac{1}{2^r}$?

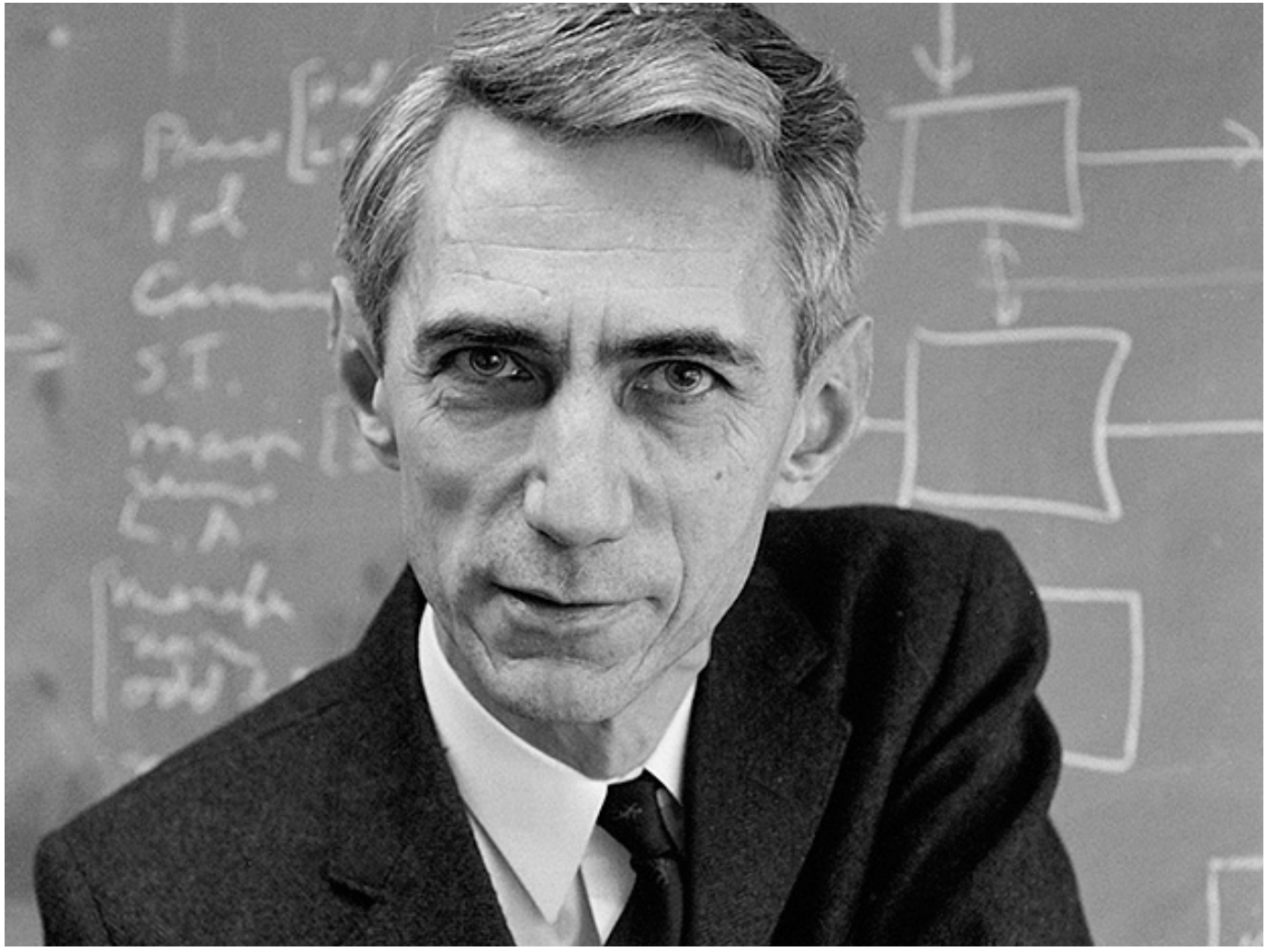
(A) $\frac{1}{2^r}$ (B) -$\frac{r}{2^r}$ (C) $\frac{r}{2^r}$ (D) r

What is $\log_2 24 - \log_2 9 + \log_2 6$?

(A) 3 (B) $3 + \log_2 3$ (C) 4 (D) $4 - \log_2 3$

Claude Shannon (1916 — 2001)

Communication theory of secrecy systems, Bell System Technical Journal (1949) **28**, 656–715.



Entropy and Guessing Games

Exercise 5.4

(i) Show that $H(p) = \sum_{x \in \mathcal{X}} p_x \log_2 \frac{1}{p_x}$, where if $p_x = 0$ then $0 \log_2 \frac{1}{0}$ is interpreted as 0.

(ii) Show that if p is the probability distribution in Exercise 5.2(b) then

$$H(p) = \tfrac{1}{2} \log_2 2 + \tfrac{1}{4} \log_2 4 + \tfrac{1}{4} \log_2 4 + 0 = \tfrac{3}{2}.$$

Show that in all three cases, $H(p)$ is the average number of questions, using the strategy found in this exercise.

(a) $p_0 = p_1 = p_2 = p_3 = \frac{1}{4}$; $H(p) = 2$

(b) $p_0 = \frac{1}{2}$, $p_1 = \frac{1}{4}$, $p_2 = \frac{1}{4}$, $p_3 = 0$; $H(p) = \frac{3}{2}$

(c) $p_0 = \frac{1}{2}$, $p_1 = \frac{1}{4}$, $p_2 = \frac{1}{8}$, $p_3 = \frac{1}{8}$; $H(p) = \frac{7}{4}$

(d) $p_0 = 1$, $p_1 = p_2 = p_3 = 0$; $H(p) = 0$

Entropy Quiz

(a) Bob chooses a random number K in $\{0, 1, 2, 3, 4\}$. If $\mathbb{P}[K = k] = 1/5$ for each k, what is $H(K)$?

(A) 2 (B) $\log_2 5 \approx 2.322$ (C) 3 (D) 4

(b) Now Bob chooses X in the same set, but with probabilities $\frac{1}{2}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}$. What is $H(X)$?

(A) 2 (B) $\log_2 5 \approx 2.322$ (C) 3 (D) 4

How many questions on average do you need to guess X?

(A) 2 (B) $\log_2 5 \approx 2.322$ (C) 3 (D) 4

Would your answer change if Bob's probabilities change to $\frac{1}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{2}$?

(A) No (B) Yes

A random variable has entropy h if and only if you can learn its value by asking about h well-chosen yes/no questions.

Entropy Quiz

(a) Bob chooses a random number K in $\{0, 1, 2, 3, 4\}$. If $\mathbb{P}[K = k] = 1/5$ for each k, what is $H(K)$?

(A) 2 (B) $\log_2 5 \approx 2.322$ (C) 3 (D) 4

(b) Now Bob chooses X in the same set, but with probabilities $\frac{1}{2}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}$. What is $H(X)$?

(A) 2 (B) $\log_2 5 \approx 2.322$ (C) 3 (D) 4

How many questions on average do you need to guess X?

(A) 2 (B) $\log_2 5 \approx 2.322$ (C) 3 (D) 4

Would your answer change if Bob's probabilities change to $\frac{1}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{2}$?

(A) No (B) Yes

A random variable has entropy h if and only if you can learn its value by asking about h well-chosen yes/no questions.

Entropy Quiz

(a) Bob chooses a random number K in $\{0, 1, 2, 3, 4\}$. If $\mathbb{P}[K = k] = 1/5$ for each k, what is $H(K)$?

(A) 2 (B) $\log_2 5 \approx 2.322$ (C) 3 (D) 4

(b) Now Bob chooses X in the same set, but with probabilities $\frac{1}{2}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}$. What is $H(X)$?

(A) 2 (B) $\log_2 5 \approx 2.322$ (C) 3 (D) 4

How many questions on average do you need to guess X?

(A) 2 (B) $\log_2 5 \approx 2.322$ (C) 3 (D) 4

Would your answer change if Bob's probabilities change to $\frac{1}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{2}$?

(A) No (B) Yes

A random variable has entropy h if and only if you can learn its value by asking about h well-chosen yes/no questions.

Entropy Quiz

(a) Bob chooses a random number K in $\{0, 1, 2, 3, 4\}$. If $\mathbb{P}[K = k] = 1/5$ for each k, what is $H(K)$?

(A) 2 (B) $\log_2 5 \approx 2.322$ (C) 3 (D) 4

(b) Now Bob chooses X in the same set, but with probabilities $\frac{1}{2}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}$. What is $H(X)$?

(A) 2 (B) $\log_2 5 \approx 2.322$ (C) 3 (D) 4

How many questions on average do you need to guess X?

(A) 2 (B) $\log_2 5 \approx 2.322$ (C) 3 (D) 4

Would your answer change if Bob's probabilities change to $\frac{1}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{2}$?

(A) No (B) Yes

A random variable has entropy h if and only if you can learn its value by asking about h well-chosen yes/no questions.

Entropy Quiz

(a) Bob chooses a random number K in $\{0, 1, 2, 3, 4\}$. If $\mathbb{P}[K = k] = 1/5$ for each k, what is $H(K)$?

(A) 2 (B) $\log_2 5 \approx 2.322$ (C) 3 (D) 4

(b) Now Bob chooses X in the same set, but with probabilities $\frac{1}{2}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}$. What is $H(X)$?

(A) 2 (B) $\log_2 5 \approx 2.322$ (C) 3 (D) 4

How many questions on average do you need to guess X?

(A) 2 (B) $\log_2 5 \approx 2.322$ (C) 3 (D) 4

Would your answer change if Bob's probabilities change to $\frac{1}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{2}$?

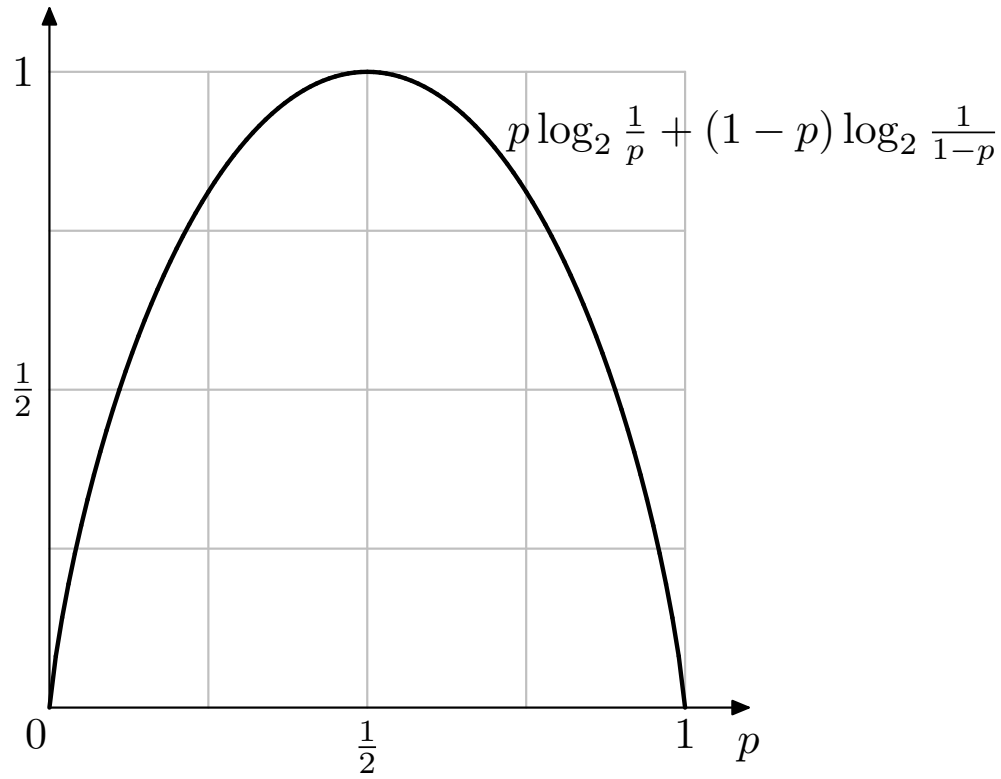
(A) No (B) Yes

No, since the entropy of a random variable depends only on the probability it takes each of its values, not the values themselves.

A random variable has entropy h if and only if you can learn its value by asking about h well-chosen yes/no questions.

Example 5.5

(1) Suppose the random variable X takes two different values, with probabilities p and $1-p$. Then $H(X) = p\log_2 \frac{1}{p} + (1-p)\log_2 \frac{1}{1-p}$, as shown in the graph below. (Using $-\log_2 q = \log_2 \frac{1}{q}$ to remove two minus signs.)



Thus the entropy of a single 'yes/no' random variable takes values between 0 and 1, with a maximum at 1 when the outcomes are equally probable.

Example 5.5 [continued]

(2) Suppose a cryptographic key K is equally likely to be any element of the keyspace $\mathcal{K}$. If $|\mathcal{K}| = n$ then $H(K) = \frac{1}{n}\log_2 n + \cdots + \frac{1}{n}\log_2 n = \log_2 n$. **This is often useful.**

(3) Consider the numeric one-time pad on $\{0, 1\}$ from Example 3.5. Suppose that $\mathbb{P}[X = 0] = p$, and so $\mathbb{P}[X = 1] = 1 - p$, and that $\mathbb{P}[K = \text{red}] = r$, and so $\mathbb{P}[K = \text{black}] = 1 - r$. As in (1) we have

$$H(X) = p\log_2 \frac{1}{p} + (1-p)\log_2 \frac{1}{1-p}.$$

Exercise: show that $\mathbb{P}[Y = 0] = p(1-r) + (1-p)r$ and $\mathbb{P}[Y = 1] = (1-p)(1-r) + pr$ and hence find $H(Y)$ when $r = 0, \frac{1}{4}, \frac{1}{2}$ and 1. Is it surprising that usually $H(Y) > H(X)$?

Definition 5.6

Let K and Y be random variables taking values in finite sets $\mathcal{K}$ and $\mathcal{C}$, respectively.The *joint entropy* of K and Y is defined by

$$H(K,Y) = -\sum_{k\in\mathcal{K}}\sum_{y\in\mathcal{C}} \mathbb{P}[K=k \text{ and } Y=y]\log_2 \mathbb{P}[K=k \text{ and } Y=y].$$

The *conditional entropy of K given that $Y=y$* is defined by

$$H(K|Y=y) = -\sum_{k\in\mathcal{K}} \mathbb{P}[K=k|Y=y]\log_2 \mathbb{P}[X=k|Y=y].$$

The *conditional entropy of K given Y* is defined by

$$H(K|Y) = \sum_{y\in\mathcal{C}} \mathbb{P}[Y=y]H(K|Y=y).$$

Example 5.7

Consider the Caesar cryptosystem in which all 26 keys are equally likely and the plaintext is a random English word. By Example 5.5, $H(K) = \log_2 26 \approx 4.7$. True or false: $H(K|Y=\texttt{ACCB}) = 0$?

(A) False (B) True

What is $H(K|Y=\texttt{NCYP})$?

(A) 0 (B) 1 (C) $\log_2 3$ (D) can't say

Definition 5.6

Let K and Y be random variables taking values in finite sets $\mathcal{K}$ and $\mathcal{C}$, respectively.The *joint entropy* of K and Y is defined by

$$H(K,Y) = -\sum_{k\in\mathcal{K}}\sum_{y\in\mathcal{C}} \mathbb{P}[K=k \text{ and } Y=y]\log_2 \mathbb{P}[K=k \text{ and } Y=y].$$

The *conditional entropy of K given that $Y=y$* is defined by

$$H(K|Y=y) = -\sum_{k\in\mathcal{K}} \mathbb{P}[K=k|Y=y]\log_2 \mathbb{P}[X=k|Y=y].$$

The *conditional entropy of K given Y* is defined by

$$H(K|Y) = \sum_{y\in\mathcal{C}} \mathbb{P}[Y=y]H(K|Y=y).$$

Example 5.7

Consider the Caesar cryptosystem in which all 26 keys are equally likely and the plaintext is a random English word. By Example 5.5, $H(K) = \log_2 26 \approx 4.7$. True or false: $H(K|Y=\texttt{ACCB}) = 0$?

(A) False (B) True

What is $H(K|Y=\texttt{NCYP})$?

(A) 0 (B) 1 (C) $\log_2 3$ (D) can't say

Definition 5.6

Let K and Y be random variables taking values in finite sets $\mathcal{K}$ and $\mathcal{C}$, respectively.The *joint entropy* of K and Y is defined by

$$H(K,Y) = -\sum_{k\in\mathcal{K}}\sum_{y\in\mathcal{C}} \mathbb{P}[K=k \text{ and } Y=y]\log_2 \mathbb{P}[K=k \text{ and } Y=y].$$

The *conditional entropy of K given that $Y=y$* is defined by

$$H(K|Y=y) = -\sum_{k\in\mathcal{K}} \mathbb{P}[K=k|Y=y]\log_2 \mathbb{P}[X=k|Y=y].$$

The *conditional entropy of K given Y* is defined by

$$H(K|Y) = \sum_{y\in\mathcal{C}} \mathbb{P}[Y=y]H(K|Y=y).$$

Example 5.7

Consider the Caesar cryptosystem in which all 26 keys are equally likely and the plaintext is a random English word. By Example 5.5, $H(K) = \log_2 26 \approx 4.7$. True or false: $H(K|Y=\texttt{ACCB}) = 0$?

(A) False (B) True

What is $H(K|Y=\texttt{NCYP})$? English shifts are `lawn` and `pear`.

(A) 0 (B) 1 (C) $\log_2 3$ (D) can't say

Definition 5.6

Let K and Y be random variables taking values in finite sets $\mathcal{K}$ and $\mathcal{C}$, respectively.The *joint entropy* of K and Y is defined by

$$H(K,Y) = -\sum_{k\in\mathcal{K}}\sum_{y\in\mathcal{C}} \mathbb{P}[K=k \text{ and } Y=y]\log_2 \mathbb{P}[K=k \text{ and } Y=y].$$

The *conditional entropy of K given that $Y=y$* is defined by

$$H(K|Y=y) = -\sum_{k\in\mathcal{K}} \mathbb{P}[K=k|Y=y]\log_2 \mathbb{P}[X=k|Y=y].$$

The *conditional entropy of K given Y* is defined by

$$H(K|Y) = \sum_{y\in\mathcal{C}} \mathbb{P}[Y=y]H(K|Y=y).$$

Example 5.7

Consider the Caesar cryptosystem in which all 26 keys are equally likely and the plaintext is a random English word. By Example 5.5, $H(K) = \log_2 26 \approx 4.7$. True or false: $H(K|Y=\texttt{ACCB}) = 0$?

(A) False (B) True

What is $H(K|Y=\texttt{NCYP})$? English shifts are `lawn` and `pear`.

(A) 0 (B) 1 (C) $\log_2 3$ (D) can't say

Example 5.8: Motivation for Chaining Rule

Fix $r \in \mathbb{N}_0$. Suppose that Bob chooses a secret key K according to the probability distribution $(\frac{1}{2}, \frac{1}{2^{r+1}}, \ldots, \frac{1}{2^{r+1}})$ on $\{0, 1, \ldots, m\}$. Here m is determined by r.

- For instance, if $r = 2$ then because the sum of the probabilities is 1, we have

$$1 = \frac{1}{2} + \overbrace{\frac{1}{2^3} + \cdots + \frac{1}{2^3}}^{m} = \frac{1}{2} + m \times \frac{1}{2^3}$$

which implies $m = 4$.

(a) Using that the sum of probabilities is 1, what, in terms of r, is the maximum possible number m that the Picker might have chosen?

(b) Show that $H(K) = 1 + r/2$.

(c) Suppose that Alice begins by asking 'Is your key 0?'. Let A be the answer. If $A =$ 'No' how many questions are needed to guess K? Show that $H(K|A = \text{'No'}) = r$. How many questions are needed if $A =$ 'Yes'? What is $H(K|A = \text{'Yes'})$?

Example 5.8: Motivation for Chaining Rule

Fix $r \in \mathbb{N}_0$. Suppose that Bob chooses a secret key K according to the probability distribution $(\frac{1}{2}, \frac{1}{2^{r+1}}, \ldots, \frac{1}{2^{r+1}})$ on $\{0, 1, \ldots, m\}$. Here m is determined by r.

(b) Show that $H(K) = 1 + r/2$.

(c) Suppose that Alice begins by asking 'Is your key 0?'. Let A be the answer. If $A =$ 'No' how many questions are needed to guess K? Show that $H(K|A = \text{'No'}) = r$. How many questions are needed if $A =$ 'Yes'? What is $H(K|A = \text{'Yes'})$?

(d) Is it possible to have $H(K|A = \text{'No'}) > H(K)$? (If so, then after learning $A =$ 'No' you are *more uncertain* about K than you were at the start.)

(e) By the definition of conditional entropy

$$H(X|A) = \mathbb{P}[A = \text{'No'}]H(X|A = \text{'No'}) + P[A = \text{'Yes'}]H(X|A = \text{'Yes'})$$

Compute $H(X|A)$ using (c).

(f) Show that $H(K|A) + H(A) = H(K, A)$. [*Hint:* $H(K, A) = H(K)$, since if you know K you certainly know A, so there is no extra information in the pair (K, A).]

Definition 5.6

Let K and Y be random variables taking values in finite sets $\mathcal{K}$ and $\mathcal{C}$, respectively.The *joint entropy* of K and Y is defined by

$$H(K,Y) = -\sum_{k\in\mathcal{K}}\sum_{y\in\mathcal{C}} \mathbb{P}[K=k \text{ and } Y=y]\log_2 \mathbb{P}[K=k \text{ and } Y=y].$$

The *conditional entropy of K given that $Y=y$* is defined by

$$H(K|Y=y) = -\sum_{k\in\mathcal{K}} \mathbb{P}[K=k|Y=y]\log_2 \mathbb{P}[X=k|Y=y].$$

The *conditional entropy of K given Y* is defined by

$$H(K|Y) = \sum_{y\in\mathcal{C}} \mathbb{P}[Y=y]H(K|Y=y).$$

Lemma 5.9 (Chaining Rule)

Let K and Y be random variables taking values in sets $\mathcal{K}$ and $\mathcal{C}$, respectively. Then

$$H(K,Y) = H(K|Y) + H(Y).$$

Shannon's Theorem on Key Uncertainty

Lemma 5.10

Let K and X be random variables. If K and X are independent then $H(K, X) = H(K) + H(X)$.

Lemma 5.11

Let Z be a random variable taking values in a set $\mathcal{Z}$. Let $f : \mathcal{Z} \to \mathcal{W}$ be a function. If f is injective then $H\big(f(Z)\big) = H(Z)$.

Theorem 5.12 (Shannon, 1949)

Take a cryptosystem in our usual notation. Then

$$H(K|Y) = H(K) + H(X) - H(Y).$$

Per-Character Information/Redundancy of English

Let $\mathcal{A} = \{\mathtt{a}, \mathtt{b}, \ldots, \mathtt{z}\}$ be the alphabet. We take $\mathcal{P} = \mathcal{C} = \mathcal{A}^n$: you can think of this as the set of all strings of length n. To indicate that plaintexts and ciphertexts have length n, we write $X^{(n)}$ and $Y^{(n)}$ rather than X and Y.

We suppose only those strings that make good sense in English have non-zero probability. So if $n = 8$ then '$\mathtt{abcdefgh}$' $\in \mathcal{P}$ and '$\mathtt{goodwork}$' $\in \mathcal{P}$ but

$$\mathbb{P}[X^{(8)} = \text{'}\mathtt{abcdefgh}\text{'}] = 0$$

whereas

$$\mathbb{P}[X^{(8)} = \text{'}\mathtt{goodwork}\text{'}] > 0.$$

Shannon estimated that the per-character redundancy of English plaintexts, with spaces, is about 3.2 bits.

Quiz: what is the entropy in a string in $\mathcal{A}^n$ if all strings are equally likely?

(A) $\log_2 26$ (B) $n \log_2 26$ (C) $3.2n$ (D) $(\log_2 26 - 3.2)n$

According to Shannon's estimate, what is the entropy in an English plaintext $X^{(n)}$ of length n?

(A) $\log_2 26$ (B) $n \log_2 26$ (C) $3.2n$ (D) $(\log_2 26 - 3.2)n$

Per-Character Information/Redundancy of English

Let $\mathcal{A} = \{\mathtt{a}, \mathtt{b}, \ldots, \mathtt{z}\}$ be the alphabet. We take $\mathcal{P} = \mathcal{C} = \mathcal{A}^n$: you can think of this as the set of all strings of length n. To indicate that plaintexts and ciphertexts have length n, we write $X^{(n)}$ and $Y^{(n)}$ rather than X and Y.

We suppose only those strings that make good sense in English have non-zero probability. So if $n = 8$ then '$\mathtt{abcdefgh}$' $\in \mathcal{P}$ and '$\mathtt{goodwork}$' $\in \mathcal{P}$ but

$$\mathbb{P}[X^{(8)} = \text{'}\mathtt{abcdefgh}\text{'}] = 0$$

whereas

$$\mathbb{P}[X^{(8)} = \text{'}\mathtt{goodwork}\text{'}] > 0.$$

Shannon estimated that the per-character redundancy of English plaintexts, with spaces, is about 3.2 bits.

Quiz: what is the entropy in a string in $\mathcal{A}^n$ if all strings are equally likely?

(A) $\log_2 26$ (B) $n \log_2 26$ (C) $3.2n$ (D) $(\log_2 26 - 3.2)n$

According to Shannon's estimate, what is the entropy in an English plaintext $X^{(n)}$ of length n?

(A) $\log_2 26$ (B) $n \log_2 26$ (C) $3.2n$ (D) $(\log_2 26 - 3.2)n$

Per-Character Information/Redundancy of English

Let $\mathcal{A} = \{\mathtt{a}, \mathtt{b}, \ldots, \mathtt{z}\}$ be the alphabet. We take $\mathcal{P} = \mathcal{C} = \mathcal{A}^n$: you can think of this as the set of all strings of length n. To indicate that plaintexts and ciphertexts have length n, we write $X^{(n)}$ and $Y^{(n)}$ rather than X and Y.

We suppose only those strings that make good sense in English have non-zero probability. So if $n = 8$ then '$\mathtt{abcdefgh}$' $\in \mathcal{P}$ and '$\mathtt{goodwork}$' $\in \mathcal{P}$ but

$$\mathbb{P}[X^{(8)} = \text{'}\mathtt{abcdefgh}\text{'}] = 0$$

whereas

$$\mathbb{P}[X^{(8)} = \text{'}\mathtt{goodwork}\text{'}] > 0.$$

Shannon estimated that the per-character redundancy of English plaintexts, with spaces, is about 3.2 bits.

Quiz: what is the entropy in a string in $\mathcal{A}^n$ if all strings are equally likely?

(A) $\log_2 26$ (B) $n \log_2 26$ (C) $3.2n$ (D) $(\log_2 26 - 3.2)n$

According to Shannon's estimate, what is the entropy in an English plaintext $X^{(n)}$ of length n?

(A) $\log_2 26$ (B) $n \log_2 26$ (C) $3.2n$ (D) $(\log_2 26 - 3.2)n$

The One-Time Pad

Let $X^{(n)}$, $Y^{(n)}$ and $K^{(n)}$ be the plaintext, ciphertext and key in the one-time pad with plaintext, ciphertext and key all of length n.

Example 5.13 (One-time-pad)

Suppose that all keys in $\mathcal{A}^n$ are equally likely. Then $H(K) = (\log_2 26)n$ by Example 5.5(2). By Proposition 4.7 the one-time has perfect secrecy. Hence by Theorem 3.12, all ciphertexts are equally likely. Therefore

$$H(Y^{(n)}) = (\log_2 26)n.$$

We saw above that $H(X^{(n)}) \approx (\log_2 26 - R)n$. Therefore by Shannon's formula,

$$H(K|Y^{(n)}) = H(K)+H(X^{(n)})-H(Y^{(n)}) = (\log_2 26-R)n = H(X^{(n)}).$$

Thus if Eve knows something about the probability distribution of plaintexts then she learns something about the key. In fact, her uncertainty about the key is precisely her uncertainty about the plaintext.

One-Time Pad Quiz

Let $R = 3.2$ be the per character redundancy of English.

In the one-time pad of length n,

- $H(K|Y^{(n)})$ is

  (A) 0 (B) 1 (C) $n(\log_2 26 - R)$ (D) $n \log_2 26$

- $H(K|(X^{(n)}, Y^{(n)}))$ is

  (A) 0 (B) 1 (C) $n(\log_2 26 - R)$ (D) $n \log_2 26$

- $H(X^{(n)}|Y^{(n)})$ is

  (A) 0 (B) 1 (C) $n(\log_2 26 - R)$ (D) $n \log_2 26$

For discussion please see video: 'One-time Pad Quiz'. *Hint:* use that the one-time pad has perfect secrecy, and so Shannon's Theorem, Theorem 3.12 applies. For instance, in the third question, you could use that $X^{(n)}$ and $Y^{(n)}$ are independent by Theorem 3.12(a).

One-Time Pad Quiz

Let $R = 3.2$ be the per character redundancy of English.

In the one-time pad of length n,

- $H(K|Y^{(n)})$ is

  (A) 0 (B) 1 (C) $n(\log_2 26 - R)$ (D) $n \log_2 26$

- $H(K|(X^{(n)}, Y^{(n)}))$ is

  (A) 0 (B) 1 (C) $n(\log_2 26 - R)$ (D) $n \log_2 26$

- $H(X^{(n)}|Y^{(n)})$ is

  (A) 0 (B) 1 (C) $n(\log_2 26 - R)$ (D) $n \log_2 26$

For discussion please see video: 'One-time Pad Quiz'. *Hint:* use that the one-time pad has perfect secrecy, and so Shannon's Theorem, Theorem 3.12 applies. For instance, in the third question, you could use that $X^{(n)}$ and $Y^{(n)}$ are independent by Theorem 3.12(a).

One-Time Pad Quiz

Let $R = 3.2$ be the per character redundancy of English.

In the one-time pad of length n,

- $H(K|Y^{(n)})$ is

  (A) 0 (B) 1 (C) $n(\log_2 26 - R)$ (D) $n \log_2 26$

- $H(K|(X^{(n)}, Y^{(n)}))$ is

  (A) 0 (B) 1 (C) $n(\log_2 26 - R)$ (D) $n \log_2 26$

- $H(X^{(n)}|Y^{(n)})$ is

  (A) 0 (B) 1 (C) $n(\log_2 26 - R)$ (D) $n \log_2 26$

For discussion please see video: 'One-time Pad Quiz'. *Hint:* use that the one-time pad has perfect secrecy, and so Shannon's Theorem, Theorem 3.12 applies. For instance, in the third question, you could use that $X^{(n)}$ and $Y^{(n)}$ are independent by Theorem 3.12(a).

One-Time Pad Quiz

Let $R = 3.2$ be the per character redundancy of English.

In the one-time pad of length n,

- $H(K|Y^{(n)})$ is

  (A) 0 (B) 1 (C) $n(\log_2 26 - R)$ (D) $n \log_2 26$

- $H(K|(X^{(n)}, Y^{(n)}))$ is

  (A) 0 (B) 1 (C) $n(\log_2 26 - R)$ (D) $n \log_2 26$

- $H(X^{(n)}|Y^{(n)})$ is

  (A) 0 (B) 1 (C) $n(\log_2 26 - R)$ (D) $n \log_2 26$

For discussion please see video: 'One-time Pad Quiz'. *Hint:* use that the one-time pad has perfect secrecy, and so Shannon's Theorem, Theorem 3.12 applies. For instance, in the third question, you could use that $X^{(n)}$ and $Y^{(n)}$ are independent by Theorem 3.12(a).

Unicity Distance

In Example 5.13 we proved that for the one-time pad $H(K|Y^{(n)}) = (\log_2 26 - R)n$ and that $H(K) = (\log_2 26)n$. Therefore

$$H(K|Y^{(n)}) = H(K) - Rn. \qquad (\star\star)$$

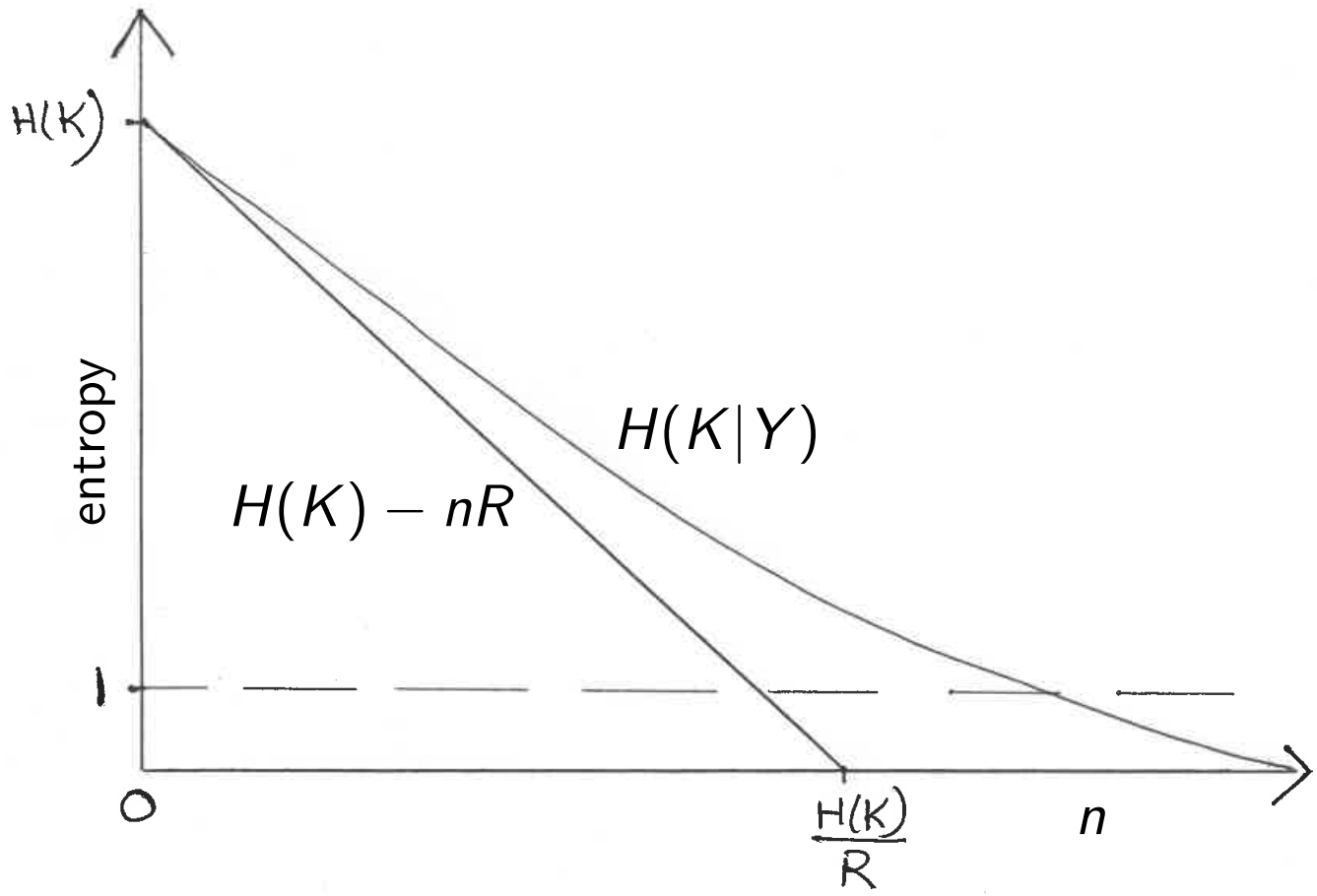
In the non-examinable extras for this part we give Shannon's argument that $(\star\star)$ should be a good approximation for $H(K|Y^{(n)})$ in any cryptosystem where $\mathcal{P} = \mathcal{C} = \mathcal{A}^n$, and the messages are English texts. It works best when $\mathcal{K}$ is large and n is small.

Exercise 5.14

What is the largest length of ciphertext n for which $(\star\star)$ could hold with equality?

Expected behaviour of $H(K|Y^{(n)})$

The graph below shows the expected behaviour of $H(K|Y^{(n)})$.



Definition 5.15

The quantity $H(K)/R$ is the *unicity* distance of the cryptosystem.

Unicity Distance for Substitution Cipher

Exercise 5.16

In the substitution cipher attack in Example 2.5 we saw that the ciphertext $y^{(280)}$ of length 280 determined the key π except for $\pi(\mathtt{k})$, $\pi(\mathtt{q})$, $\pi(\mathtt{z})$. By Exercise 2.6(a) $\pi(\mathtt{k})$, $\pi(\mathtt{q})$, $\pi(\mathtt{z})$ are the three letters, namely `A`, `E`, `N`, which never appear in the ciphertext. Assuming equally likely keys, what is $H(K|Y^{(280)} = y^{(280)})$?

(A) 0 (B) $\log_2 3$ (C) $\log_2 6$ (D) 6

What is $H(K)$?

(A) $\log_2 26$ (B) $\log_2 26!$ (C) $26 \log_2 26$ (D) depends on the key

Unicity Distance for Substitution Cipher

Exercise 5.16

In the substitution cipher attack in Example 2.5 we saw that the ciphertext $y^{(280)}$ of length 280 determined the key π except for $\pi(\mathtt{k})$, $\pi(\mathtt{q})$, $\pi(\mathtt{z})$. By Exercise 2.6(a) $\pi(\mathtt{k})$, $\pi(\mathtt{q})$, $\pi(\mathtt{z})$ are the three letters, namely `A`, `E`, `N`, which never appear in the ciphertext. Assuming equally likely keys, what is $H(K|Y^{(280)} = y^{(280)})$?

(A) 0 (B) $\log_2 3$ (C) $\log_2 6$ (D) 6

What is $H(K)$?

(A) $\log_2 26$ (B) $\log_2 26!$ (C) $26 \log_2 26$ (D) depends on the key

Unicity Distance for Substitution Cipher

Exercise 5.16

In the substitution cipher attack in Example 2.5 we saw that the ciphertext $y^{(280)}$ of length 280 determined the key π except for $\pi(\mathtt{k})$, $\pi(\mathtt{q})$, $\pi(\mathtt{z})$. By Exercise 2.6(a) $\pi(\mathtt{k})$, $\pi(\mathtt{q})$, $\pi(\mathtt{z})$ are the three letters, namely `A`, `E`, `N`, which never appear in the ciphertext. Assuming equally likely keys, what is $H(K|Y^{(280)} = y^{(280)})$?

(A) 0 (B) $\log_2 3$ (C) $\log_2 6$ (D) 6

What is $H(K)$?

(A) $\log_2 26$ (B) $\log_2 26!$ (C) $26 \log_2 26$ (D) depends on the key

Example 5.17

The first 28 characters of the ciphertext in Example 2.5 are `KQX WJZRUHXZKUY GTOXSKPIX GW`. A computer search using a dictionary of about 70000 words gives 6 possible decryptions of the first 24 letters. These include '`imo purgatorial hedonics`', '`iwo purgatorial hedonism`' and '`the fundamental objectiv`'. Taking 25 letters,

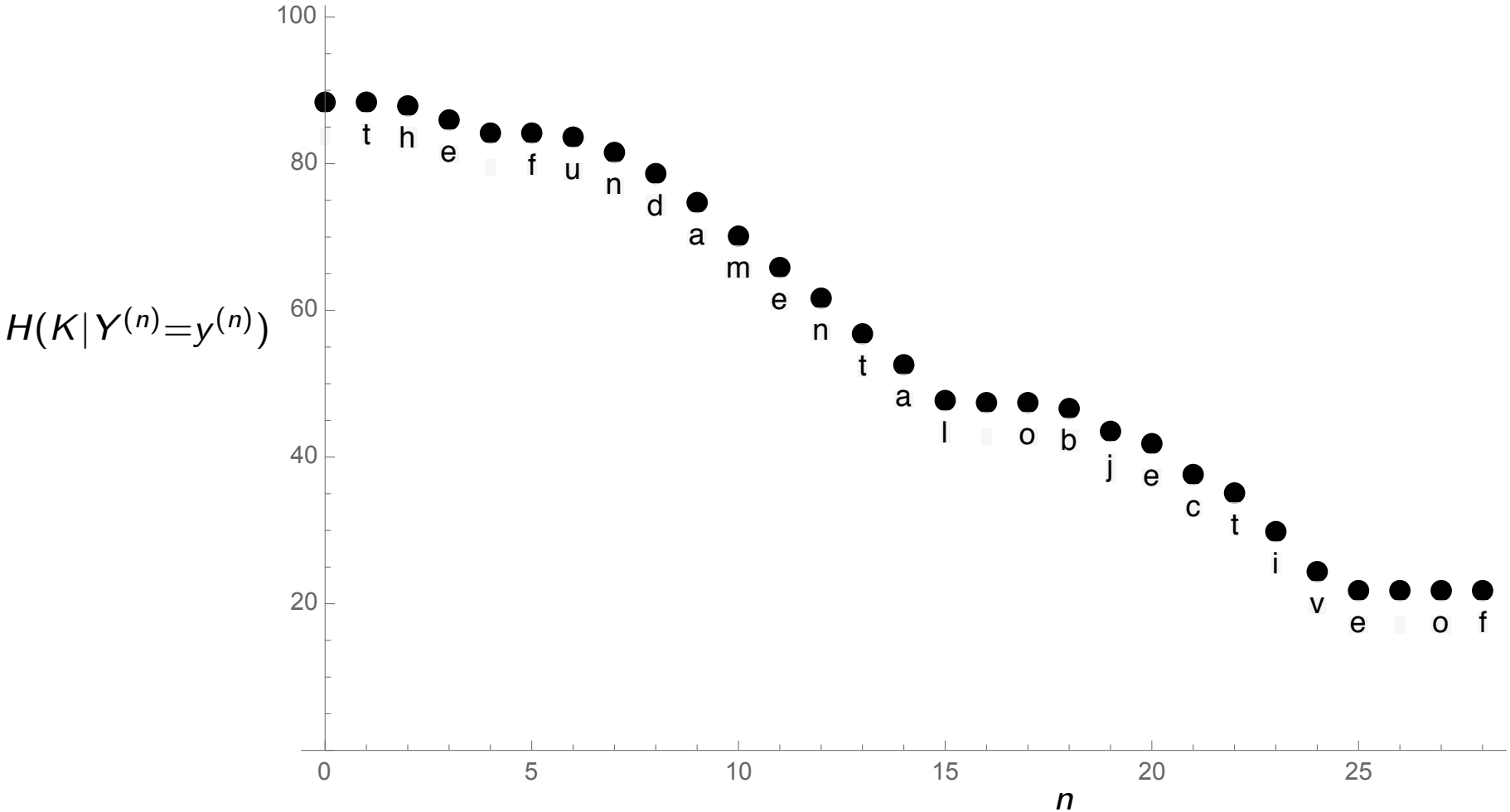
'`the fundamental objective`'

is the only decryption consistent with the dictionary. This is in excellent agreement with Shannon's argument.

Since 10 characters do not appear in the first 28 letters of ciphertext, the argument in Exercise 5.16 shows that $H(K|Y^{(28)} = y^{(28)}) = \log_2 10! = 21.791$. Nothing new about the key is learned after letter 25, so this is the value of the final 4 points in the graph of $H(K|Y^{(n)} = y^{(n)})$ for $1 \leq n \leq 28$.

See the printed notes for full details, including the simplifying assumption that all English phrases whose words have the right lengths are equally likely.

$H(K|Y^{(n)})$ for Ciphertext Y from Substitution Cipher



The remaining slides are on the optional extras for Part A.

Outline of Shannon's Argument for $H(K|Y^{(n)}) \approx H(K) - Rn$

- Fix $n \in \mathbb{N}$. As a simplified model for English messages of length n, we suppose that a proportion c of the strings of length n are *common*. The rest are *rare*.
- All common strings of length n are equally likely as messages. Rare strings are never sent.
  - What value, in terms of the per-character redundancy R of English, should we pick for c?

    (A) $\frac{1}{2^{n \log_2 26}}$ (B) $\frac{1}{2^{n(\log_2 26 - R)}}$ (C) $\frac{1}{2^{nR}}$ (D) $\frac{1}{Rn}$
- As a simplified model of a cryptosystem encrypting English messages, we take $\mathcal{P} = \mathcal{C} = \mathcal{A}^n$ and fix a keyspace $\mathcal{K}$. (This can be any set you like, for instance a subset of $\mathbb{N}$.)
- For each $k \in \mathcal{K}$ choose a random bijection $e_k : \mathcal{P} \to \mathcal{C}$. These are part of the definition of the cryptoscheme, so known to everyone by Kerckhoffs's Assumption.
- As usual, we suppose all keys are equally likely.

Outline of Shannon's Argument for $H(K|Y^{(n)}) \approx H(K) - Rn$

- Fix $n \in \mathbb{N}$. As a simplified model for English messages of length n, we suppose that a proportion c of the strings of length n are *common*. The rest are *rare*.
- All common strings of length n are equally likely as messages. Rare strings are never sent.
  - What value, in terms of the per-character redundancy R of English, should we pick for c?

    (A) $\frac{1}{2^{n \log_2 26}}$ (B) $\frac{1}{2^{n(\log_2 26 - R)}}$ (C) $\frac{1}{2^{nR}}$ (D) $\frac{1}{Rn}$
- As a simplified model of a cryptosystem encrypting English messages, we take $\mathcal{P} = \mathcal{C} = \mathcal{A}^n$ and fix a keyspace $\mathcal{K}$. (This can be any set you like, for instance a subset of $\mathbb{N}$.)
- For each $k \in \mathcal{K}$ choose a random bijection $e_k : \mathcal{P} \to \mathcal{C}$. These are part of the definition of the cryptoscheme, so known to everyone by Kerckhoffs's Assumption.
- As usual, we suppose all keys are equally likely.

Outline of Shannon's Argument for $H(K|Y^{(n)}) \approx H(K) - Rn$

- Suppose you observe a ciphertext y.
  - What is the probability that y is an encryption of a common plaintext?

    (A) 0 (B) c (C) 1 (D) $\frac{1}{26^{n \log_2 26}}$
- Define a function $g : \mathcal{C} \to \mathbb{Z}$ so that $g(y)$ is the number of keys that encrypt some common plaintext to the ciphertext y.
  - Which of the sets below is the smallest set that must contain the range of g?

    (A) $\mathbb{N}_0$ (B) $\mathbb{N}$ (C) $\{0, 1, \ldots, |\mathcal{K}|\}$ (D) $\{1, \ldots, |\mathcal{K}|\}$
- Let y be a ciphertext observed after a user encrypts the common $x \in \mathcal{P}$ with the key k.
  - If $K^\star$ is a key, chosen uniformly at random but not equal to k, what is the probability that $d_{K^\star}(y)$ is common?

    (A) 0 (B) c (C) $\frac{1}{26^{n \log_2 26}}$ (D) 1
  - True or false: since the chance that after decrypting y by a random key we get a common plaintext is c, and there are $|\mathcal{K}|$ keys, $g(Y)$ is distributed as $\mathrm{Bin}(|\mathcal{K}|, c)$.

    (A) False (B) True

Outline of Shannon's Argument for $H(K|Y^{(n)}) \approx H(K) - Rn$

- Suppose you observe a ciphertext y.
  - What is the probability that y is an encryption of a common plaintext?

    (A) 0 (B) c (C) 1 (D) $\frac{1}{26^{n \log_2 26}}$
- Define a function $g : \mathcal{C} \to \mathbb{Z}$ so that $g(y)$ is the number of keys that encrypt some common plaintext to the ciphertext y.
  - Which of the sets below is the smallest set that must contain the range of g?

    (A) $\mathbb{N}_0$ (B) $\mathbb{N}$ (C) $\{0, 1, \ldots, |\mathcal{K}|\}$ (D) $\{1, \ldots, |\mathcal{K}|\}$
- Let y be a ciphertext observed after a user encrypts the common $x \in \mathcal{P}$ with the key k.
  - If $K^\star$ is a key, chosen uniformly at random but not equal to k, what is the probability that $d_{K^\star}(y)$ is common?

    (A) 0 (B) c (C) $\frac{1}{26^{n \log_2 26}}$ (D) 1
  - True or false: since the chance that after decrypting y by a random key we get a common plaintext is c, and there are $|\mathcal{K}|$ keys, $g(Y)$ is distributed as $\mathrm{Bin}(|\mathcal{K}|, c)$.

    (A) False (B) True

Outline of Shannon's Argument for $H(K|Y^{(n)}) \approx H(K) - Rn$

- Suppose you observe a ciphertext y.
  - What is the probability that y is an encryption of a common plaintext?

    (A) 0 (B) c (C) 1 (D) $\frac{1}{26^{n \log_2 26}}$
- Define a function $g : \mathcal{C} \to \mathbb{Z}$ so that $g(y)$ is the number of keys that encrypt some common plaintext to the ciphertext y.
  - Which of the sets below is the smallest set that must contain the range of g?

    (A) $\mathbb{N}_0$ (B) $\mathbb{N}$ (C) $\{0, 1, \ldots, |\mathcal{K}|\}$ (D) $\{1, \ldots, |\mathcal{K}|\}$
- Let y be a ciphertext observed after a user encrypts the common $x \in \mathcal{P}$ with the key k.
  - If $K^\star$ is a key, chosen uniformly at random but not equal to k, what is the probability that $d_{K^\star}(y)$ is common?

    (A) 0 (B) c (C) $\frac{1}{26^{n \log_2 26}}$ (D) 1
  - True or false: since the chance that after decrypting y by a random key we get a common plaintext is c, and there are $|\mathcal{K}|$ keys, $g(Y)$ is distributed as $\mathrm{Bin}(|\mathcal{K}|, c)$.

    (A) False (B) True

Outline of Shannon's Argument for $H(K|Y^{(n)}) \approx H(K) - Rn$

- Suppose you observe a ciphertext y.
  - What is the probability that y is an encryption of a common plaintext?

    (A) 0 (B) c (C) 1 (D) $\frac{1}{26^{n \log_2 26}}$
- Define a function $g : \mathcal{C} \to \mathbb{Z}$ so that $g(y)$ is the number of keys that encrypt some common plaintext to the ciphertext y.
  - Which of the sets below is the smallest set that must contain the range of g?

    (A) $\mathbb{N}_0$ (B) $\mathbb{N}$ (C) $\{0, 1, \ldots, |\mathcal{K}|\}$ (D) $\{1, \ldots, |\mathcal{K}|\}$
- Let y be a ciphertext observed after a user encrypts the common $x \in \mathcal{P}$ with the key k.
  - If $K^\star$ is a key, chosen uniformly at random but not equal to k, what is the probability that $d_{K^\star}(y)$ is common?

    (A) 0 (B) c (C) $\frac{1}{26^{n \log_2 26}}$ (D) 1
  - True or false: since the chance that after decrypting y by a random key we get a common plaintext is c, and there are $|\mathcal{K}|$ keys, $g(Y)$ is distributed as $\mathrm{Bin}(|\mathcal{K}|, c)$.

    (A) False (B) True

Outline of Shannon's Argument for $H(K|Y^{(n)}) \approx H(K) - Rn$

- Suppose you observe a ciphertext y.
  - What is the probability that y is an encryption of a common plaintext?

    (A) 0 (B) c (C) 1 (D) $\frac{1}{26^{n \log_2 26}}$
- Define a function $g : \mathcal{C} \to \mathbb{Z}$ so that $g(y)$ is the number of keys that encrypt some common plaintext to the ciphertext y.
  - Which of the sets below is the smallest set that must contain the range of g?

    (A) $\mathbb{N}_0$ (B) $\mathbb{N}$ (C) $\{0, 1, \ldots, |\mathcal{K}|\}$ (D) $\{1, \ldots, |\mathcal{K}|\}$
- Let y be a ciphertext observed after a user encrypts the common $x \in \mathcal{P}$ with the key k.
  - If $K^\star$ is a key, chosen uniformly at random but not equal to k, what is the probability that $d_{K^\star}(y)$ is common?

    (A) 0 (B) c (C) $\frac{1}{26^{n \log_2 26}}$ (D) 1
  - True or false: since the chance that after decrypting y by a random key we get a common plaintext is c, and there are $|\mathcal{K}|$ keys, $g(Y)$ is distributed as $\mathrm{Bin}(|\mathcal{K}|, c)$.

    (A) False (B) True

  You probably already realised this. The answer (D) above shows $g(Y) \geq 1$, but a binomially distribed random variable always has a chance of being 0. Next slide shows the fallacy.

Ciphertexts with High $g(y)$ are Extra Likely: Intuition

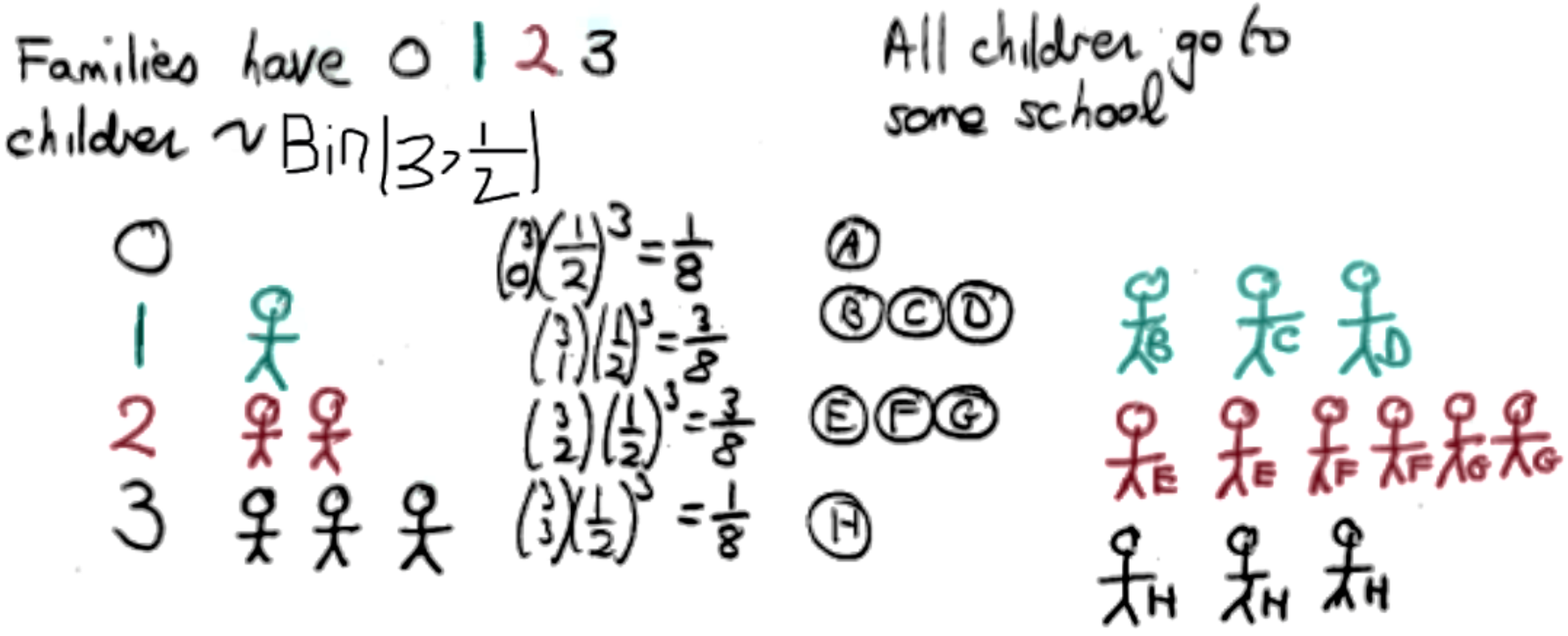
Quiz: Suppose I ask everyone here online how many siblings you have (not counting yourself). If the mean is s, then $1 + s$ is a good estimate for the average number of children in a family.

(A) False (B) True

Ciphertexts with High $g(y)$ are Extra Likely: Intuition

Quiz: Suppose I ask everyone here online how many siblings you have (not counting yourself). If the mean is s, then $1 + s$ is a good estimate for the average number of children in a family.

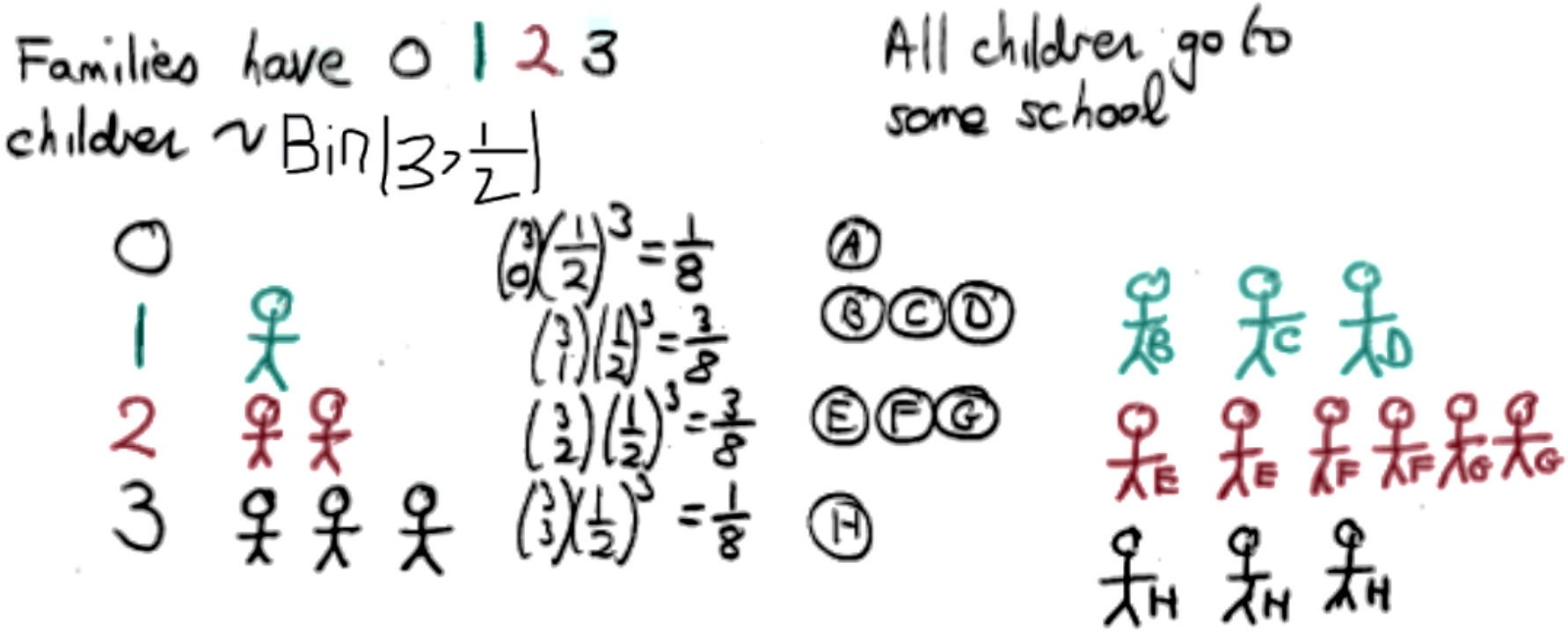
(A) False (B) True



Ciphertexts with High $g(y)$ are Extra Likely: Intuition

Quiz: Suppose I ask everyone here online how many siblings you have (not counting yourself). If the mean is s, then $1 + s$ is a good estimate for the average number of children in a family.

(A) False (B) True

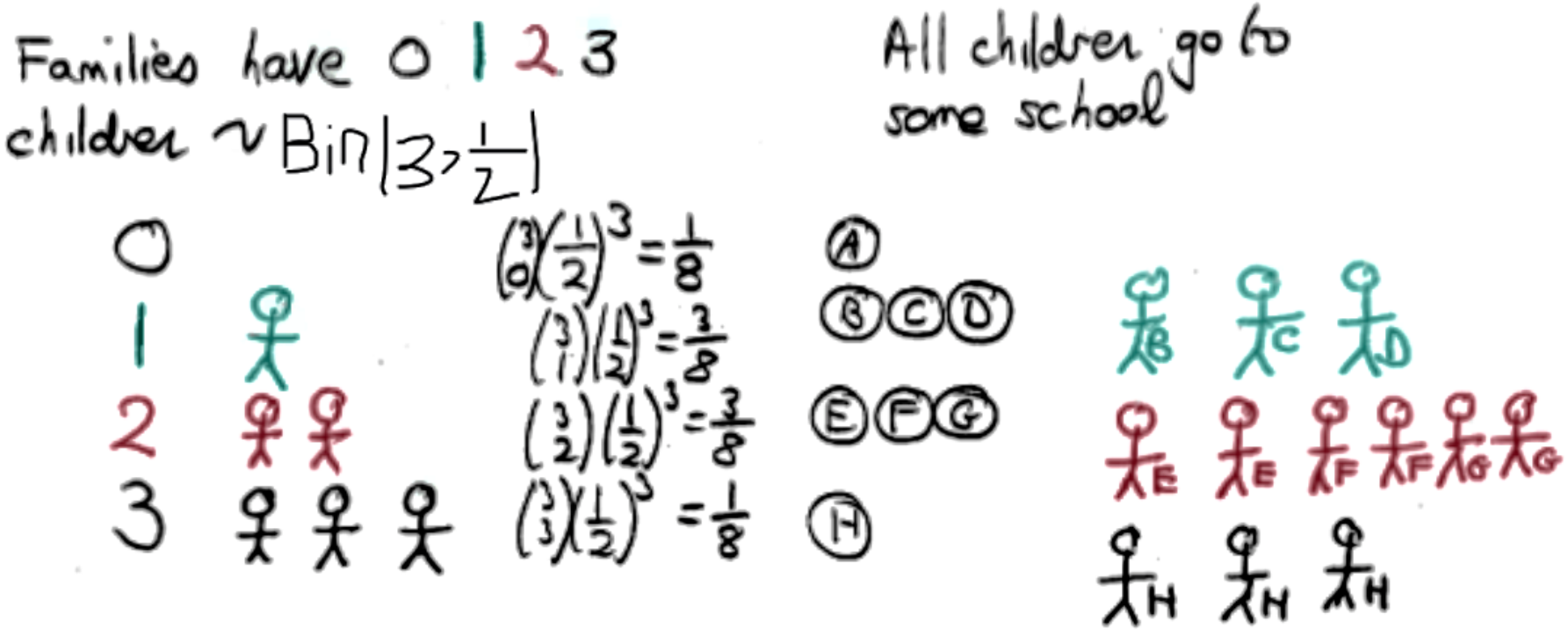


In Shannon's argument for unicity distance, $g(y)$ is the number of English plaintexts that encrypt to y by some substitution cipher key. Ciphertexts with high $g(y)$ are disproportionately likely.

Ciphertexts with High $g(y)$ are Extra Likely: Intuition

Quiz: Suppose I ask everyone here online how many siblings you have (not counting yourself). If the mean is s, then $1 + s$ is a good estimate for the average number of children in a family.

(A) False (B) True

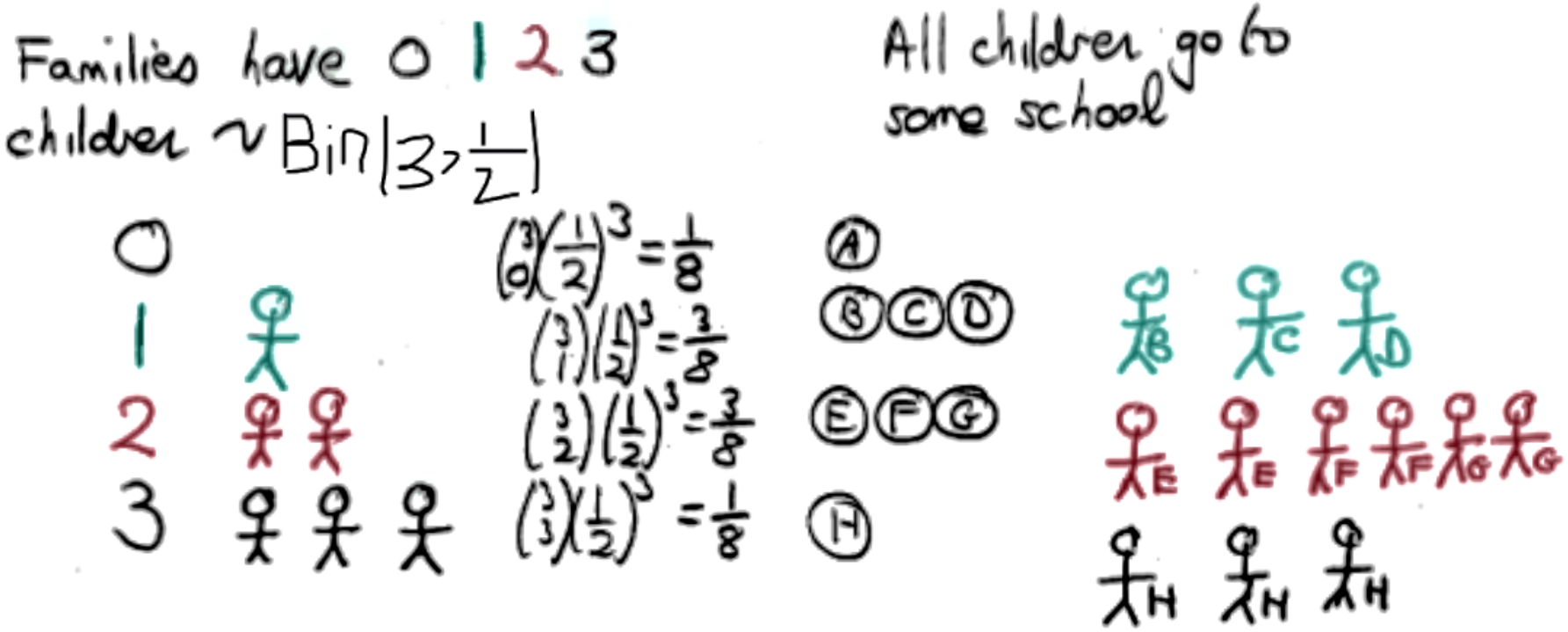


To complete the analogy: sampling $g(y)$ is a bit like sampling from the school: we never observe the childless families or the rare plaintexts.

Ciphertexts with High $g(y)$ are Extra Likely: Intuition

Quiz: Suppose I ask everyone here online how many siblings you have (not counting yourself). If the mean is s, then $1 + s$ is a good estimate for the average number of children in a family.

(A) False (B) True



In fact sampling from the school exaggerates the effect: the right-hand part of the diagram shows that the observed distribution is $1 + 3\mathrm{Bin}(2, \frac{1}{2})$ and not $\mathrm{Bin}(3, \frac{1}{2})$. For $g(y)$ we don't see the scaling (at least, not in this way), but the shift by 1 is still present.

End of Shannon's Argument for $H(K|Y^{(n)}) \approx H(K) - Rn$

- The correct argument is that since the chance that after decrypting y by a random key we get a common plaintext is c, and there are $|\mathcal{K}| - 1$ keys *other than the key k used to obtain y*,
$$g(Y) \sim 1 + \mathrm{Bin}(|\mathcal{K}| - 1, c).$$
- By the formula for conditional entropy:
$$\begin{aligned} H(K|Y) &= \sum_{y \in \mathcal{C}} H(K|Y=y)\mathbb{P}[Y=y] \\ &= \sum_{m \geq 1} \binom{|\mathcal{K}|-1}{m-1} c^{m-1}(1-c)^{|\mathcal{K}|-m} \log_2 m \\ &= \frac{1}{c|\mathcal{K}|} \sum_{m \geq 0} \binom{|\mathcal{K}|}{m} c^m (1-c)^{|\mathcal{K}|-m} m \log_2 m \end{aligned}$$
where we used $\binom{|\mathcal{K}|-1}{m-1} = \binom{|\mathcal{K}|}{m} \frac{m}{|\mathcal{K}|}$.
- Hence with high probability $H(K|Y)$ is about
$$H(K|Y) \approx \frac{1}{c|\mathcal{K}|} c|\mathcal{K}| \log_2(c|\mathcal{K}|) = \log_2 |\mathcal{K}| + \log_2 c.$$

End of Shannon's Argument for $H(K|Y^{(n)}) \approx H(K) - Rn$

- We showed that with high probability

$$H(K|Y) \approx \log_2 |\mathcal{K}| + \log_2 c.$$

- From earlier $c = \frac{1}{2^{nR}}$.
- Hence $H(K|Y) \approx \log_2 |\mathcal{K}| - Rn = H(K) - Rn$ as required.

Part B: Stream ciphers

§6 Linear Feedback Shift Registers

Computers are deterministic: given the same inputs, you always get the same answer. In this part we will see how to get sequences that 'look random' out of deterministic algorithms.

Recall that $\mathbb{F}_2$ is the finite field of size 2 with elements the *bits* (short for *bi*nary digi*ts*) 0, 1. Addition and multiplication are defined modulo 2, so

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

By definition, $\mathbb{F}_2^n$ is the set of n-tuples $(x_0, x_1, \ldots, x_{n-1})$ where each x_i is a bit 0 or 1. For brevity we may write this tuple as $x_0x_1 \ldots x_{n-1}$. As seen here, we number positions from 0 up to $n-1$. It is usual to refer to elements of $\mathbb{F}_2^n$ as *binary words* of length n.

Definition of LFSRs

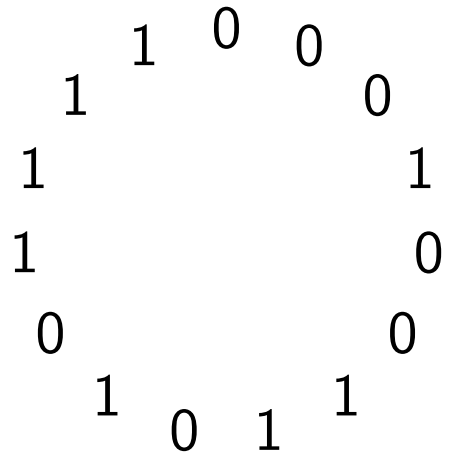
Exercise 6.1

Write down 15 bits in a circle so that, reading the cycle clockwise, every non-zero binary word of length 4 appears exactly once. How many 0s do you use? How many 1s do you use?

Definition of LFSRs

Exercise 6.1

Write down 15 bits in a circle so that, reading the cycle clockwise, every non-zero binary word of length 4 appears exactly once. How many 0s do you use? How many 1s do you use? How often does 110 appear when your circle is read clockwise? What about other words of length 3?



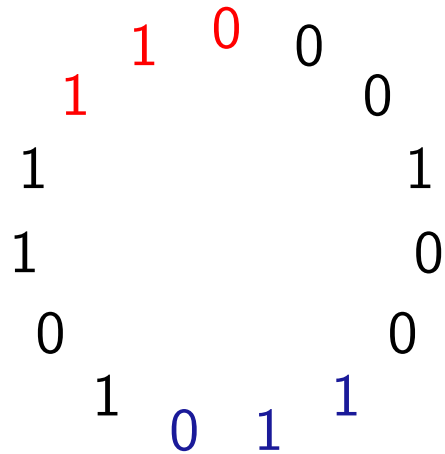
This is the unique solution, up to rotations and reflections.

- There are seven 0s and eight 1s
- 110 appears twice (click on to see highlighted), as do each of the words $001, 010, \ldots, 111$. Can you see why? We generalize this observation in Proposition 7.2. What about 000?

Definition of LFSRs

Exercise 6.1

Write down 15 bits in a circle so that, reading the cycle clockwise, every non-zero binary word of length 4 appears exactly once. How many 0s do you use? How many 1s do you use? How often does 110 appear when your circle is read clockwise? What about other words of length 3?



This is the unique solution, up to rotations and reflections.

- There are seven 0s and eight 1s
- 110 appears twice (click on to see highlighted), as do each of the words $001, 010, \ldots, 111$. Can you see why? We generalize this observation in Proposition 7.2. What about 000?

Definition of LFSRs

Exercise 6.1

Write down 15 bits in a circle so that, reading the cycle clockwise, every non-zero binary word of length 4 appears exactly once. How many 0s do you use? How many 1s do you use?

Definition 6.2

(i) Let $\ell \in \mathbb{N}$. A *linear feedback shift register* of *width* ℓ with *taps* $T \subseteq \{1, 2, \ldots, \ell\}$ is a function $F : \mathbb{F}_2^\ell \to \mathbb{F}_2^\ell$ of the form

$$F\big((x_0, x_1, \ldots, x_{\ell-2}, x_{\ell-1})\big) = (x_1, \ldots, x_{\ell-1}, \sum_{t \in T} x_{\ell-t}).$$

(ii) The function $f : \mathbb{F}_2^\ell \to \mathbb{F}_2$ defined by $f(x) = \sum_{t \in T} x_{\ell-t}$ is called the *feedback function*.

(iii) The *keystream* for $k \in \mathbb{F}_2^\ell$ is the sequence $k_0, k_1, \ldots, k_{\ell-1}, k_\ell, k_{\ell+1}, \ldots$, where for each $s \geq \ell$ we define

$$k_s = \sum_{t \in T} k_{s-t}$$

First Quiz on LFSRs

The keystream of the LFSR F of width 4 with taps $\{3, 4\}$ is defined by $k_s = k_{s-3} + k_{s-4}$ for $s \geq 4$. The keystream for key $k = (k_0, k_1, k_2, k_3) = (0, 1, 1, 0)$ starts

$$(0, 1, 1, 0, 1, 0, 1, 1, \ldots)$$
$$0\ \ 1\ \ 2\ \ 3\ \ 4\ \ 5\ \ 6\ \ 7$$

Thus $k_4 = k_0 + k_1 = 0 + 1 = 1$, $k_5 = k_1 + k_2 = 1 + 1 = 0$, and $k_7 = k_3 + k_4 = 0 + 1 = 1$.

- True or false: $k_8 = 1$?

  (A) False (B) True

- What is $k_8 k_9 k_{10} k_{11} \in \mathbb{F}_2^4$?

  (A) 1100 (B) 1110 (C) 1000 (D) 1111

- What is $k_9 k_{10} k_{11} k_{12} \in \mathbb{F}_2^4$?

  (A) 1100 (B) 1110 (C) 1000 (D) 1111

First Quiz on LFSRs

The keystream of the LFSR F of width 4 with taps $\{3, 4\}$ is defined by $k_s = k_{s-3} + k_{s-4}$ for $s \geq 4$. The keystream for key $k = (k_0, k_1, k_2, k_3) = (0, 1, 1, 0)$ starts

$$(0, 1, 1, 0, 1, 0, 1, 1, \ldots)$$
$$0\ \ 1\ \ 2\ \ 3\ \ 4\ \ 5\ \ 6\ \ 7$$

Thus $k_4 = k_0 + k_1 = 0 + 1 = 1$, $k_5 = k_1 + k_2 = 1 + 1 = 0$, and $k_7 = k_3 + k_4 = 0 + 1 = 1$.

- True or false: $k_8 = 1$?

  (A) False (B) True

- What is $k_8 k_9 k_{10} k_{11} \in \mathbb{F}_2^4$?

  (A) 1100 (B) 1110 (C) 1000 (D) 1111

- What is $k_9 k_{10} k_{11} k_{12} \in \mathbb{F}_2^4$?

  (A) 1100 (B) 1110 (C) 1000 (D) 1111

First Quiz on LFSRs

The keystream of the LFSR F of width 4 with taps $\{3, 4\}$ is defined by $k_s = k_{s-3} + k_{s-4}$ for $s \geq 4$. The keystream for key $k = (k_0, k_1, k_2, k_3) = (0, 1, 1, 0)$ starts

$$(0, 1, 1, 0, 1, 0, 1, 1, \ldots)$$
$$0\ \ 1\ \ 2\ \ 3\ \ 4\ \ 5\ \ 6\ \ 7$$

Thus $k_4 = k_0 + k_1 = 0 + 1 = 1$, $k_5 = k_1 + k_2 = 1 + 1 = 0$, and $k_7 = k_3 + k_4 = 0 + 1 = 1$.

- True or false: $k_8 = 1$?

  (A) False (B) True

- What is $k_8 k_9 k_{10} k_{11} \in \mathbb{F}_2^4$?

  (A) 1100 (B) 1110 (C) 1000 (D) 1111

- What is $k_9 k_{10} k_{11} k_{12} \in \mathbb{F}_2^4$?

  (A) 1100 (B) 1110 (C) 1000 (D) 1111

First Quiz on LFSRs

The keystream of the LFSR F of width 4 with taps $\{3, 4\}$ is defined by $k_s = k_{s-3} + k_{s-4}$ for $s \geq 4$. The keystream for key $k = (k_0, k_1, k_2, k_3) = (0, 1, 1, 0)$ starts

$$(0, 1, 1, 0, 1, 0, 1, 1, \ldots)$$
$$0\ \ 1\ \ 2\ \ 3\ \ 4\ \ 5\ \ 6\ \ 7$$

Thus $k_4 = k_0 + k_1 = 0 + 1 = 1$, $k_5 = k_1 + k_2 = 1 + 1 = 0$, and $k_7 = k_3 + k_4 = 0 + 1 = 1$.

- True or false: $k_8 = 1$?

  (A) False (B) True

- What is $k_8 k_9 k_{10} k_{11} \in \mathbb{F}_2^4$?

  (A) 1100 (B) 1110 (C) 1000 (D) 1111

- What is $k_9 k_{10} k_{11} k_{12} \in \mathbb{F}_2^4$?

  (A) 1100 (B) 1110 (C) 1000 (D) 1111

The Very Useful Property

Equivalently, $k_s = f\big((k_{s-\ell}, k_{s-\ell+1}, \ldots, k_{s-1})\big)$ and so

$$F\big((k_{s-\ell}, k_{s-\ell+1}, \ldots, k_{s-1})\big) = (k_{s-\ell+1}, \ldots, k_{s-1}, k_s).$$

Thus the LFSR function F shifts the bits in the first $\ell - 1$ positions left (forgetting the very first), and puts a new bit, defined by its feedback function, into the rightmost position. Taking all these rightmost positions gives the keystream. We call this the **Very Useful Property**:

$$F^s\big((k_0, k_1, \ldots, k_{\ell-1})\big) = (k_s, k_{s+1}, \ldots, k_{s+\ell-1}). \qquad (\textbf{VUP})$$

Here F^s is the function defined by applying F a total of s times.

See (iv) in Example 6.3, slide after the quiz, for an example.

Quiz on the Very Useful Property

Very Useful Property

$$F^s\big((k_0, k_1 \ldots, k_{\ell-1})\big) = (k_s, k_{s+1}, \ldots, k_{s+\ell-1}).$$

The keystream for the LFSR F in Example 6.3 with key 0111 is below

$$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1 \ldots)$$
$$0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9$$

True or false?

(1) $F^2(0111) = 1110$ (A) False (B) True

(2) $F^3(0111) = 1100$ (A) False (B) True

(3) $F^{11}(0111) = 1101$ (A) False (B) True

(4) $F^2(1110) = 1100$ (A) False (B) True

Quiz on the Very Useful Property

Very Useful Property

$$F^s\big((k_0, k_1 \ldots, k_{\ell-1})\big) = (k_s, k_{s+1}, \ldots, k_{s+\ell-1}).$$

The keystream for the LFSR F in Example 6.3 with key 0111 is below

$$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1 \ldots)$$
$$0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9$$

True or false?

(1) $F^2(0111) = 1110$ (A) False (B) True

(2) $F^3(0111) = 1100$ (A) False (B) True

(3) $F^{11}(0111) = 1101$ (A) False (B) True

(4) $F^2(1110) = 1100$ (A) False (B) True

Quiz on the Very Useful Property

Very Useful Property

$$F^s\big((k_0, k_1 \ldots, k_{\ell-1})\big) = (k_s, k_{s+1}, \ldots, k_{s+\ell-1}).$$

The keystream for the LFSR F in Example 6.3 with key 0111 is below

$$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1 \ldots)$$
$$0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9$$

True or false?

(1) $F^2(0111) = 1110$ (A) False (B) True

(2) $F^3(0111) = 1100$ (A) False (B) True

(3) $F^{11}(0111) = 1101$ (A) False (B) True

(4) $F^2(1110) = 1100$ (A) False (B) True

Quiz on the Very Useful Property

Very Useful Property

$$F^s\big((k_0, k_1 \ldots, k_{\ell-1})\big) = (k_s, k_{s+1}, \ldots, k_{s+\ell-1}).$$

The keystream for the LFSR F in Example 6.3 with key 0111 is below

$$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1 \ldots)$$
$$0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9$$

True or false?

(1) $F^2(0111) = 1110$ (A) False (B) True

(2) $F^3(0111) = 1100$ (A) False (B) True

(3) $F^{11}(0111) = 1101$ (A) False (B) True

(4) $F^2(1110) = 1100$ (A) False (B) True

Quiz on the Very Useful Property

Very Useful Property

$$F^s\big((k_0, k_1 \ldots, k_{\ell-1})\big) = (k_s, k_{s+1}, \ldots, k_{s+\ell-1}).$$

The keystream for the LFSR F in Example 6.3 with key 0111 is below

$$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1 \ldots)$$
$$0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9$$

True or false?

(1) $F^2(0111) = 1110$ (A) False (B) True

(2) $F^3(0111) = 1100$ (A) False (B) True

(3) $F^{11}(0111) = 1101$ (A) False (B) True

(4) $F^2(1110) = 1100$ (A) False (B) True

Example 6.3

The LFSR F of width 4 with taps $\{3, 4\}$ is defined by

$$F\big((x_0, x_1, x_2, x_3)\big) = (x_1, x_2, x_3, x_0 + x_1).$$

(i) Solving the equation $F\big((x_0, x_1, x_2, x_3)\big) = (y_0, y_1, y_2, y_3)$ shows that F has inverse

$$F^{-1}\big((y_0, y_1, y_2, y_3)\big) = (y_0 + y_3, y_0, y_1, y_2).$$

(ii) The keystream for the key $k = 0111$ is

$$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1 \ldots)$$
$$0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9$$

repeating from position 15 onwards: $k_s = k_{s+15}$ for all $s \in \mathbb{N}_0$.

(iii) *Exercise:* $k' = 0001$ appears as $k_5k_6k_7k_8$ in the keystream. Find the keystream when the LFSR is *started* with k'.

(iv) By the (**VUP**), starting with $k = 0111$, we have $k_1k_2k_3k_4 = F(k) = 1111$ and $k_2k_3k_4k_5 = F^2(k) = 1110$. Observe that $F^{14}(k) = 1011$ with $F^{15}(k) = k$.

(v) Quiz. Every keystream generated by F is obtained by reading the circle of 15 bits we used to solve Exercise 6.1. (Click on if surprised.)

(A) False (B) True

Example 6.3

The LFSR F of width 4 with taps $\{3, 4\}$ is defined by

$$F\big((x_0, x_1, x_2, x_3)\big) = (x_1, x_2, x_3, x_0 + x_1).$$

(i) Solving the equation $F\big((x_0, x_1, x_2, x_3)\big) = (y_0, y_1, y_2, y_3)$ shows that F has inverse

$$F^{-1}\big((y_0, y_1, y_2, y_3)\big) = (y_0 + y_3, y_0, y_1, y_2).$$

(ii) The keystream for the key $k = 0111$ is

$$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1 \ldots)$$
$$0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9$$

repeating from position 15 onwards: $k_s = k_{s+15}$ for all $s \in \mathbb{N}_0$.

(iii) *Exercise:* $k' = 0001$ appears as $k_5k_6k_7k_8$ in the keystream. Find the keystream when the LFSR is *started* with k'.
Use that $k'_s = k'_{s-3} + k'_{s-4}$ satisfies same recurrence as $k_s = k_{s-3} + k_{s-4}$ so you just read the keystream for k from 0001.

(iv) By the (**VUP**), starting with $k = 0111$, we have $k_1k_2k_3k_4 = F(k) = 1111$ and $k_2k_3k_4k_5 = F^2(k) = 1110$.
Observe that $F^{14}(k) = 1011$ with $F^{15}(k) = k$.

(v) Quiz. Every keystream generated by F is obtained by reading the circle of 15 bits we used to solve Exercise 6.1. (Click on if surprised.)

(A) False (B) True

Example 6.3

The LFSR F of width 4 with taps $\{3, 4\}$ is defined by

$$F\big((x_0, x_1, x_2, x_3)\big) = (x_1, x_2, x_3, x_0 + x_1).$$

(i) Solving the equation $F\big((x_0, x_1, x_2, x_3)\big) = (y_0, y_1, y_2, y_3)$ shows that F has inverse

$$F^{-1}\big((y_0, y_1, y_2, y_3)\big) = (y_0 + y_3, y_0, y_1, y_2).$$

(ii) The keystream for the key $k = 0111$ is

$$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1 \ldots)$$
$$0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9$$

repeating from position 15 onwards: $k_s = k_{s+15}$ for all $s \in \mathbb{N}_0$.

(iii) *Exercise:* $k' = 0001$ appears as $k_5k_6k_7k_8$ in the keystream. Find the keystream when the LFSR is *started* with k'.
Use that $k'_s = k'_{s-3} + k'_{s-4}$ satisfies same recurrence as $k_s = k_{s-3} + k_{s-4}$ so you just read the keystream for k from 0001.

(iv) By the (**VUP**), starting with $k = 0111$, we have $k_1k_2k_3k_4 = F(k) = 1111$ and $k_2k_3k_4k_5 = F^2(k) = 1110$.
Observe that $F^{14}(k) = 1011$ with $F^{15}(k) = k$.

(v) Quiz. Every keystream generated by F is obtained by reading the circle of 15 bits we used to solve Exercise 6.1. (Click on if surprised.)

(A) False (B) True

Example 6.3

The LFSR F of width 4 with taps $\{3, 4\}$ is defined by

$$F\big((x_0, x_1, x_2, x_3)\big) = (x_1, x_2, x_3, x_0 + x_1).$$

(i) Solving the equation $F\big((x_0, x_1, x_2, x_3)\big) = (y_0, y_1, y_2, y_3)$ shows that F has inverse

$$F^{-1}\big((y_0, y_1, y_2, y_3)\big) = (y_0 + y_3, y_0, y_1, y_2).$$

(ii) The keystream for the key $k = 0111$ is

$$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1 \ldots)$$
$$0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9$$

repeating from position 15 onwards: $k_s = k_{s+15}$ for all $s \in \mathbb{N}_0$.

(iii) *Exercise:* $k' = 0001$ appears as $k_5k_6k_7k_8$ in the keystream. Find the keystream when the LFSR is *started* with k'.
Use that $k'_s = k'_{s-3} + k'_{s-4}$ satisfies same recurrence as $k_s = k_{s-3} + k_{s-4}$ so you just read the keystream for k from 0001.

(iv) By the (**VUP**), starting with $k = 0111$, we have $k_1k_2k_3k_4 = F(k) = 1111$ and $k_2k_3k_4k_5 = F^2(k) = 1110$.
Observe that $F^{14}(k) = 1011$ with $F^{15}(k) = k$.

(v) Quiz. Every keystream generated by F is obtained by reading the circle of 15 bits we used to solve Exercise 6.1. (Click on if surprised.)

(A) False (B) True

Example 6.3

The LFSR F of width 4 with taps $\{3, 4\}$ is defined by

$$F\big((x_0, x_1, x_2, x_3)\big) = (x_1, x_2, x_3, x_0 + x_1).$$

(i) Solving the equation $F\big((x_0, x_1, x_2, x_3)\big) = (y_0, y_1, y_2, y_3)$ shows that F has inverse

$$F^{-1}\big((y_0, y_1, y_2, y_3)\big) = (y_0 + y_3, y_0, y_1, y_2).$$

(ii) The keystream for the key $k = 0111$ is

$$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1 \ldots)$$
$$0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9$$

repeating from position 15 onwards: $k_s = k_{s+15}$ for all $s \in \mathbb{N}_0$.

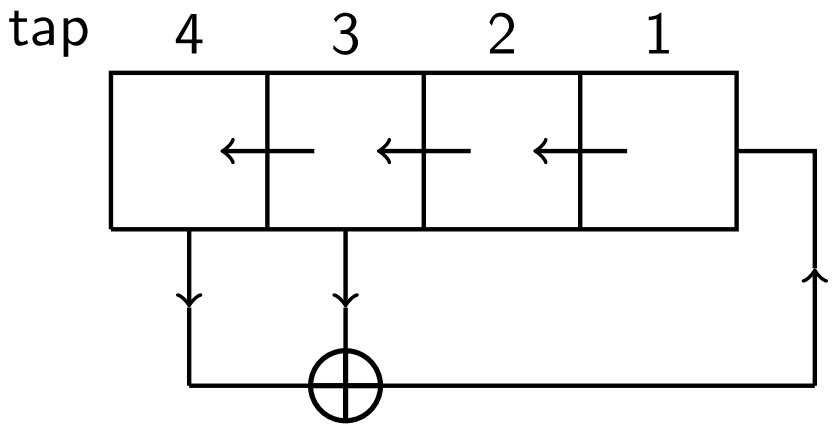
(iii) *Exercise:* $k' = 0001$ appears as $k_5k_6k_7k_8$ in the keystream. Find the keystream when the LFSR is *started* with k'.
Use that $k'_s = k'_{s-3} + k'_{s-4}$ satisfies same recurrence as $k_s = k_{s-3} + k_{s-4}$ so you just read the keystream for k from 0001.

(iv) By the (**VUP**), starting with $k = 0111$, we have $k_1k_2k_3k_4 = F(k) = 1111$ and $k_2k_3k_4k_5 = F^2(k) = 1110$.
Observe that $F^{14}(k) = 1011$ with $F^{15}(k) = k$.

(v) Quiz. Every keystream generated by F is obtained by reading the circle of 15 bits we used to solve Exercise 6.1. (Click on if surprised.)
Because 0000 . . . is also a keystream. Every other keystream *is* obtained from the circle of bits.

Circuit Diagrams

In the cryptographic literature it is conventional to represent LFSRs by circuit diagrams, such as the one below showing F. By convention $\bigoplus$ denotes addition modulo 2, implemented in electronics by the XOR gate.



The word 'register' in LFSR refers to the boxed memory units storing the bits.

Cryptosystem defined by an LFSR

Definition 6.4

Let F be an LFSR of width ℓ and let $n \in \mathbb{N}$. The *cryptosystem defined by* F has $\mathcal{P} = \mathcal{C} = \mathbb{F}_2^n$ and keyspace $\mathcal{K} = \mathbb{F}_2^\ell$. The encryption functions are defined by

$$e_k(x) = (k_0, k_1, \ldots, k_{n-1}) + (x_0, x_1, \ldots, x_{n-1})$$

for each $k \in \mathcal{K}$ and $x \in \mathcal{P}$.

Thus, like the one-time pad, the ciphertext is obtained by addition to the plaintext. But unlike the one-time pad, the key is usually much shorter than the plaintext.

Exercise 6.5

Define the decryption function $d_k : \mathbb{F}_2^n \to \mathbb{F}_2^n$.

Question 1 on Problem Sheet 5 shows how to encrypt an English message of length n by using the ASCII encoding to convert it to a word in $\mathbb{F}_2^{8n}$.

Cryptosystem defined by an LFSR

Definition 6.4

Let F be an LFSR of width ℓ and let $n \in \mathbb{N}$. The *cryptosystem defined by* F has $\mathcal{P} = \mathcal{C} = \mathbb{F}_2^n$ and keyspace $\mathcal{K} = \mathbb{F}_2^\ell$. The encryption functions are defined by

$$e_k(x) = (k_0, k_1, \ldots, k_{n-1}) + (x_0, x_1, \ldots, x_{n-1})$$

for each $k \in \mathcal{K}$ and $x \in \mathcal{P}$.

Thus, like the one-time pad, the ciphertext is obtained by addition to the plaintext. But unlike the one-time pad, the key is usually much shorter than the plaintext.

Quiz. Alice sends Bob (a hardworking student) his exam mark using the LFSR F in Example 6.2, by writing the mark in binary using 8 bits and encrypting using their key $k_0k_1k_2k_3$.

What is the binary form of 61 written using 8 bits?

(A) 00111100 (B) 00111001 (C) 00111101 (D) 01111101

Cryptosystem defined by an LFSR

Definition 6.4

Let F be an LFSR of width ℓ and let $n \in \mathbb{N}$. The *cryptosystem defined by* F has $\mathcal{P} = \mathcal{C} = \mathbb{F}_2^n$ and keyspace $\mathcal{K} = \mathbb{F}_2^\ell$. The encryption functions are defined by

$$e_k(x) = (k_0, k_1, \ldots, k_{n-1}) + (x_0, x_1, \ldots, x_{n-1})$$

for each $k \in \mathcal{K}$ and $x \in \mathcal{P}$.

Thus, like the one-time pad, the ciphertext is obtained by addition to the plaintext. But unlike the one-time pad, the key is usually much shorter than the plaintext.

Quiz. Alice sends Bob (a hardworking student) his exam mark using the LFSR F in Example 6.2, by writing the mark in binary using 8 bits and encrypting using their key $k_0k_1k_2k_3$.

What is the binary form of 61 written using 8 bits?

(A) 00111100 (B) 00111001 (C) 00111101 (D) 01111101

Cryptosystem defined by an LFSR

Definition 6.4

Let F be an LFSR of width ℓ and let $n \in \mathbb{N}$. The *cryptosystem defined by* F has $\mathcal{P} = \mathcal{C} = \mathbb{F}_2^n$ and keyspace $\mathcal{K} = \mathbb{F}_2^\ell$. The encryption functions are defined by

$$e_k(x) = (k_0, k_1, \ldots, k_{n-1}) + (x_0, x_1, \ldots, x_{n-1})$$

for each $k \in \mathcal{K}$ and $x \in \mathcal{P}$.

Thus, like the one-time pad, the ciphertext is obtained by addition to the plaintext. But unlike the one-time pad, the key is usually much shorter than the plaintext.

Quiz. Alice sends Bob (a hardworking student) his exam mark using the LFSR F in Example 6.2, by writing the mark in binary using 8 bits and encrypting using their key $k_0k_1k_2k_3$.

Eve observes the ciphertext 00100110. Writing $\star$ for an unknown bit, she can guess that $k_0k_1k_2k_3$ is certainly

(A) $0\star\star\star$ (B) $1\star\star\star$ (C) $00\star\star$ (D) $01\star\star$

Cryptosystem defined by an LFSR

Definition 6.4

Let F be an LFSR of width ℓ and let $n \in \mathbb{N}$. The *cryptosystem defined by* F has $\mathcal{P} = \mathcal{C} = \mathbb{F}_2^n$ and keyspace $\mathcal{K} = \mathbb{F}_2^\ell$. The encryption functions are defined by

$$e_k(x) = (k_0, k_1, \ldots, k_{n-1}) + (x_0, x_1, \ldots, x_{n-1})$$

for each $k \in \mathcal{K}$ and $x \in \mathcal{P}$.

Thus, like the one-time pad, the ciphertext is obtained by addition to the plaintext. But unlike the one-time pad, the key is usually much shorter than the plaintext.

Quiz. Alice sends Bob (a hardworking student) his exam mark using the LFSR F in Example 6.2, by writing the mark in binary using 8 bits and encrypting using their key $k_0k_1k_2k_3$.

Eve observes the ciphertext 00100110. Writing $\star$ for an unknown bit, she can guess that $k_0k_1k_2k_3$ is certainly

(A) $0\star\star\star$ (B) $1\star\star\star$ (C) $00\star\star$ (D) $01\star\star$

Cryptosystem defined by an LFSR

Definition 6.4

Let F be an LFSR of width ℓ and let $n \in \mathbb{N}$. The *cryptosystem defined by* F has $\mathcal{P} = \mathcal{C} = \mathbb{F}_2^n$ and keyspace $\mathcal{K} = \mathbb{F}_2^\ell$. The encryption functions are defined by

$$e_k(x) = (k_0, k_1, \ldots, k_{n-1}) + (x_0, x_1, \ldots, x_{n-1})$$

for each $k \in \mathcal{K}$ and $x \in \mathcal{P}$.

Thus, like the one-time pad, the ciphertext is obtained by addition to the plaintext. But unlike the one-time pad, the key is usually much shorter than the plaintext.

Quiz. Alice sends Bob (a hardworking student) his exam mark using the LFSR F in Example 6.2, by writing the mark in binary using 8 bits and encrypting using their key $k_0k_1k_2k_3$.

Eve observes the ciphertext 00100110. Writing $\star$ for an unknown bit, she can guess that $k_0k_1k_2k_3$ is most probably

(A) $00\star\star$ (B) $01\star\star$ (C) $10\star\star$ (D) $11\star\star$

Cryptosystem defined by an LFSR

Definition 6.4

Let F be an LFSR of width ℓ and let $n \in \mathbb{N}$. The *cryptosystem defined by* F has $\mathcal{P} = \mathcal{C} = \mathbb{F}_2^n$ and keyspace $\mathcal{K} = \mathbb{F}_2^\ell$. The encryption functions are defined by

$$e_k(x) = (k_0, k_1, \ldots, k_{n-1}) + (x_0, x_1, \ldots, x_{n-1})$$

for each $k \in \mathcal{K}$ and $x \in \mathcal{P}$.

Thus, like the one-time pad, the ciphertext is obtained by addition to the plaintext. But unlike the one-time pad, the key is usually much shorter than the plaintext.

Quiz. Alice sends Bob (a hardworking student) his exam mark using the LFSR F in Example 6.2, by writing the mark in binary using 8 bits and encrypting using their key $k_0k_1k_2k_3$.

Eve observes the ciphertext 00100110. Writing $\star$ for an unknown bit, she can guess that $k_0k_1k_2k_3$ is most probably

(A) $00\star\star$ (B) $01\star\star$ (C) $10\star\star$ (D) $11\star\star$

Invertible LFSRs and periods: motivation

Exercise 6.6

Let H be the LFSR of width 3 with taps $\{1, 2\}$. Show that H is not invertible and check that $111\mathbf{011}011\mathbf{011}011\ldots$ is a keystream of H, ending in the cycle $011011\ldots$.

This exercise and Example 6.3(i) suggest the general result: an LFSR is invertible if and only if ℓ is one of the taps.

Exercise 6.7

Let G be the LFSR of width 4 with taps $\{1, 2, 4\}$.

(a) Find the keystreams for the keys 0001 and 0010.

(b) Which words of length 4 do not appear in either keystream?

(c) Find all keystreams generated by this LFSR.

After how many positions does the keystream for key 0110 repeats? (This is the period of the keystream for 0110, and also 0001.)

(A) 3 (B) 7 (C) 14 (D) 15

True or false: $G^7 = \mathrm{id}$, the identity function.

(A) False (B) True

Invertible LFSRs and periods: motivation

Exercise 6.6

Let H be the LFSR of width 3 with taps $\{1, 2\}$. Show that H is not invertible and check that $111\mathbf{011}011\mathbf{011}011\ldots$ is a keystream of H, ending in the cycle $011011\ldots$.

This exercise and Example 6.3(i) suggest the general result: an LFSR is invertible if and only if ℓ is one of the taps.

Exercise 6.7

Let G be the LFSR of width 4 with taps $\{1, 2, 4\}$.

(a) Find the keystreams for the keys 0001 and 0010.

(b) Which words of length 4 do not appear in either keystream?

(c) Find all keystreams generated by this LFSR.

After how many positions does the keystream for key 0110 repeats? (This is the period of the keystream for 0110, and also 0001.)

(A) 3 (B) 7 (C) 14 (D) 15

True or false: $G^7 = \mathrm{id}$, the identity function.

(A) False (B) True

Invertible LFSRs and periods: motivation

Exercise 6.6

Let H be the LFSR of width 3 with taps $\{1, 2\}$. Show that H is not invertible and check that $111\mathbf{011}011\mathbf{011}011\ldots$ is a keystream of H, ending in the cycle $011011\ldots$.

This exercise and Example 6.3(i) suggest the general result: an LFSR is invertible if and only if ℓ is one of the taps.

Exercise 6.7

Let G be the LFSR of width 4 with taps $\{1, 2, 4\}$.

(a) Find the keystreams for the keys 0001 and 0010.

(b) Which words of length 4 do not appear in either keystream?

(c) Find all keystreams generated by this LFSR.

After how many positions does the keystream for key 0110 repeats? (This is the period of the keystream for 0110, and also 0001.)

(A) 3 (B) 7 (C) 14 (D) 15

True or false: $G^7 = \mathrm{id}$, the identity function.

(A) False (B) True

Invertible LFSRs and Periods

For example, the LFSR F of width 4 with taps $\{3, 4\}$ has a keystream with period 15: $k_s = k_{s+15}$ for all s.

$$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1 \ldots)$$
$$0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9$$

Fix a non-zero key $k \in \mathbb{F}_2^\ell$ and consider the binary words $F^s(k)$ for $s \in \mathbb{N}_0$. **Mini-exercise:** why are they all non-zero? We make a chain

$$k \mapsto F(k) \mapsto F^2(k) \mapsto \ldots \mapsto F^s(k) \mapsto \ldots \mapsto F^{s'}(k) \mapsto \ldots.$$

Since there are $2^\ell - 1$ non-zero binary words of length ℓ, and

$$k, F(k), \ldots, F^{2^\ell - 1}(k)$$

has 2^ℓ words, there exist r, r' with $0 \leq r < r' < 2^\ell$ such that $F^r(k) = F^{r'}(k)$. Now applying F^{-r} we get $k = F^{r'-r}(k)$. Hence, by (**VUP**),

$$k_0 k_1 \ldots k_{\ell-1} = k_{r'-r} k_{r'-r+1} \ldots k_{r'-r+\ell-1}$$

and the keystream repeats after at most $r' - r < 2^\ell$ positions.

Definition 6.8

Let F be an invertible LFSR.

(i) We define the *period* of a keystream $k_0, k_1, \ldots$ generated by F to be the least $p \in \mathbb{N}$ such that $k_{s+p} = k_s$ for all $s \in \mathbb{N}_0$.

(ii) We define the *period* of F to be the least $P \in \mathbb{N}$ such that $F^P = \mathrm{id}$, the identity function.

For example, the LFSRs F and G in Example 6.3 and Exercise 6.7 have non-zero keystreams of periods 15 (the maximum possible) and $7, 7, 1, 1$, respectively. Their periods are 15 and 7, respectively. We just saw that the period of a keystream of an LFSR of width ℓ is at most $2^\ell - 1$.

Definition 6.8

Let F be an invertible LFSR.

(i) We define the *period* of a keystream $k_0, k_1, \ldots$ generated by F to be the least $p \in \mathbb{N}$ such that $k_{s+p} = k_s$ for all $s \in \mathbb{N}_0$.

(ii) We define the *period* of F to be the least $P \in \mathbb{N}$ such that $F^P = \mathrm{id}$, the identity function.

Quiz. The minimum period an LFSR with keystreams of lengths 4 and 30 could have is

(A) 30 (B) 60 (C) 120 (D) 360

The LFSR H of width 4 with taps $\{2, 4\}$ has the keystreams

- 0 0 0 ...
- 011 011 011 ...
- 000101 000101 000101 ...
- 001111 001111 001111 ...

Observe that, as seen in Exercise 6.7 and the slide on periods, every binary word of length 4 appears exactly once in some keystream (reading the keystream until its first repeat).

What is the period of H?

(A) 3 (B) 6 (C) 15 (D) 18

Definition 6.8

Let F be an invertible LFSR.

(i) We define the *period* of a keystream $k_0, k_1, \ldots$ generated by F to be the least $p \in \mathbb{N}$ such that $k_{s+p} = k_s$ for all $s \in \mathbb{N}_0$.

(ii) We define the *period* of F to be the least $P \in \mathbb{N}$ such that $F^P = \mathrm{id}$, the identity function.

Quiz. The minimum period an LFSR with keystreams of lengths 4 and 30 could have is

(A) 30 (B) 60 (C) 120 (D) 360

The LFSR H of width 4 with taps $\{2, 4\}$ has the keystreams

- 0 0 0 ...
- 011 011 011 ...
- 000101 000101 000101 ...
- 001111 001111 001111 ...

Observe that, as seen in Exercise 6.7 and the slide on periods, every binary word of length 4 appears exactly once in some keystream (reading the keystream until its first repeat).

What is the period of H?

(A) 3 (B) 6 (C) 15 (D) 18

Definition 6.8

Let F be an invertible LFSR.

(i) We define the *period* of a keystream $k_0, k_1, \ldots$ generated by F to be the least $p \in \mathbb{N}$ such that $k_{s+p} = k_s$ for all $s \in \mathbb{N}_0$.

(ii) We define the *period* of F to be the least $P \in \mathbb{N}$ such that $F^P = \mathrm{id}$, the identity function.

Quiz. The minimum period an LFSR with keystreams of lengths 4 and 30 could have is

(A) 30 (B) 60 (C) 120 (D) 360

The LFSR H of width 4 with taps $\{2, 4\}$ has the keystreams

- 0 0 0 ...
- 011 011 011 ...
- 000101 000101 000101 ...
- 001111 001111 001111 ...

Observe that, as seen in Exercise 6.7 and the slide on periods, every binary word of length 4 appears exactly once in some keystream (reading the keystream until its first repeat).

What is the period of H?

(A) 3 (B) 6 (C) 15 (D) 18

§7 Keysteams and Randomness

We saw before Definition 6.8 that the maximum possible period of a keystream of an LFSR of width ℓ is $2^\ell - 1$. Given any non-zero $k \in \mathbb{F}_2^\ell$, the first $2^\ell - 1$ positions of the keystream for k are the *generating cycle* for k. (The term '*m-sequence*' is also used.) Thus

$$k_{2^\ell - 1 + s} = k_s \text{ for all } s \in \mathbb{N}. \qquad (\dagger)$$

Generating Cycles of Maximum Period LFSRs

Exercise 7.1

Let F be the LFSR of width 4 with taps $\{3, 4\}$ and period $15 = 2^4 - 1$ seen in Example 5.1. It has the maximum possible period for its width. The keystream for $k = (1, 1, 0, 0)$ is

$$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0 \ldots).$$

Correspondingly, by the Very Useful Property,

$$F(1, 1, 0, 0) = (1, 0, 0, 0), \ldots F^{14}(1, 1, 0, 0) = (1, 1, 1, 0)$$

and $F^{15}(1, 1, 0, 0) = (1, 1, 0, 0)$. By taking the first 15 positions we get the generating cycle

$$\begin{array}{c} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \\ k_0\ k_1\ k_2\ k_3\ k_4\ k_5\ k_6\ k_7\ k_8\ k_9\ k_{10} k_{11} k_{12} k_{13} k_{14} \end{array}$$

Exercise 7.1 [continued]

By taking the first 15 positions we get the generating cycle

$$\begin{array}{c}(1,1,0,0,0,1,0,0,1,1,0,1,0,1,1)\\ k_0\ k_1\ k_2\ k_3\ k_4\ k_5\ k_6\ k_7\ k_8\ k_9\ k_{10}k_{11}k_{12}k_{13}k_{14}\end{array}$$

(a) Find all the positions s such that

$$(k_s, k_{s+1}, k_{s+2}, k_{s+3}) = (0,1,1,1).$$

(b) What is the only element of $\mathbb{F}_2^4$ *not* appearing in the keystream for $(0,0,0,1)$?

(c) Why is the generating cycle for $(0,1,1,1)$ a cyclic shift of the generating cycle for $(1,1,0,0)$?

(d) Find all the positions s such that $(k_s, k_{s+1}, k_{s+2}) = (0,1,1)$. How many are there? [*Hint:* you do something similar in the Group Work for Week 5.]

(e) Repeat (d) changing $(0,1,1)$ to $(0,0,1)$, $(0,0,0)$ and then to $(0,1)$, $(1,1)$, $(1,0)$ and $(0,0)$. Explain the pattern.

Quiz Very Similar to Exercise 7.1 (used in Plenary Session Week 7)

The keystream for the LFSR with taps $\{0, 2, 3, 4\}$ and width 5 for the key 00001 has period 31. The first 31 positions are

$$\begin{array}{c} (0,0,0,0,1,1,0,0,1,0,0,1,1,1,1,1,0,1,1,1,0,0,0,1,0,1,0,1,1,0,1) \\ k_0\ k_1\ k_2\ k_3\ k_4\ k_5\ k_6\ k_7\ k_8\ k_9\ k_{10}\ k_{11}\ k_{12}\ k_{13}\ k_{14}\ k_{15}\ k_{16}\ k_{17}\ k_{18}\ k_{19}\ k_{20}\ k_{21}\ k_{22}\ k_{23}\ k_{24}\ k_{25}\ k_{26}\ k_{27}\ k_{28}\ k_{29}\ k_{30} \end{array}$$

- How many times does 11110 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times does 1111 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times does 111 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times does 010 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times does 100 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times does 000 appear?
  (A) 1 (B) 2 (C) 3 (D) 4

Quiz Very Similar to Exercise 7.1 (used in Plenary Session Week 7)

The keystream for the LFSR with taps $\{0, 2, 3, 4\}$ and width 5 for the key 00001 has period 31. The first 31 positions are

$$(0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$$
$$k_0\ k_1\ k_2\ k_3\ k_4\ k_5\ k_6\ k_7\ k_8\ k_9\ k_{10}\ k_{11}\ k_{12}\ k_{13}\ k_{14}\ k_{15}\ k_{16}\ k_{17}\ k_{18}\ k_{19}\ k_{20}\ k_{21}\ k_{22}\ k_{23}\ k_{24}\ k_{25}\ k_{26}\ k_{27}\ k_{28}\ k_{29}\ k_{30}$$

- How many times does 11110 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times does 1111 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times does 111 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times does 010 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times does 100 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times does 000 appear?
  (A) 1 (B) 2 (C) 3 (D) 4

Quiz Very Similar to Exercise 7.1 (used in Plenary Session Week 7)

The keystream for the LFSR with taps $\{0, 2, 3, 4\}$ and width 5 for the key 00001 has period 31. The first 31 positions are

$$(0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$$
$$k_0\ k_1\ k_2\ k_3\ k_4\ k_5\ k_6\ k_7\ k_8\ k_9\ k_{10}\ k_{11}\ k_{12}\ k_{13}\ k_{14}\ k_{15}\ k_{16}\ k_{17}\ k_{18}\ k_{19}\ k_{20}\ k_{21}\ k_{22}\ k_{23}\ k_{24}\ k_{25}\ k_{26}\ k_{27}\ k_{28}\ k_{29}\ k_{30}$$

- How many times does 11110 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times does 1111 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times does 111 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times does 010 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times does 100 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times does 000 appear?
  (A) 1 (B) 2 (C) 3 (D) 4

Quiz Very Similar to Exercise 7.1 (used in Plenary Session Week 7)

The keystream for the LFSR with taps $\{0, 2, 3, 4\}$ and width 5 for the key 00001 has period 31. The first 31 positions are

$$(0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$$
$$k_0\ k_1\ k_2\ k_3\ k_4\ k_5\ k_6\ k_7\ k_8\ k_9\ k_{10}\ k_{11}\ k_{12}\ k_{13}\ k_{14}\ k_{15}\ k_{16}\ k_{17}\ k_{18}\ k_{19}\ k_{20}\ k_{21}\ k_{22}\ k_{23}\ k_{24}\ k_{25}\ k_{26}\ k_{27}\ k_{28}\ k_{29}\ k_{30}$$

- How many times does 11110 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times does 1111 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times does 111 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times does 010 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times does 100 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times does 000 appear?
  (A) 1 (B) 2 (C) 3 (D) 4

Quiz Very Similar to Exercise 7.1 (used in Plenary Session Week 7)

The keystream for the LFSR with taps $\{0, 2, 3, 4\}$ and width 5 for the key 00001 has period 31. The first 31 positions are

$$\begin{array}{ccccccccccccccccccccccccccccc} (0, & 0, & 0, & 0, & 1, & 1, & 0, & 0, & 1, & 0, & 0, & 1, & 1, & 1, & 1, & 1, & 0, & 1, & 1, & 1, & 0, & 0, & 0, & 1, & 0, & 1, & 0, & 1, & 1, & 0, & 1) \\ k_0 & k_1 & k_2 & k_3 & k_4 & k_5 & k_6 & k_7 & k_8 & k_9 & k_{10} & k_{11} & k_{12} & k_{13} & k_{14} & k_{15} & k_{16} & k_{17} & k_{18} & k_{19} & k_{20} & k_{21} & k_{22} & k_{23} & k_{24} & k_{25} & k_{26} & k_{27} & k_{28} & k_{29} & k_{30} \end{array}$$

- How many times does 11110 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times does 1111 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times does 111 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times does 010 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times does 100 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times does 000 appear?
  (A) 1 (B) 2 (C) 3 (D) 4

Quiz Very Similar to Exercise 7.1 (used in Plenary Session Week 7)

The keystream for the LFSR with taps $\{0, 2, 3, 4\}$ and width 5 for the key 00001 has period 31. The first 31 positions are

$$(0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$$
$$k_0\ k_1\ k_2\ k_3\ k_4\ k_5\ k_6\ k_7\ k_8\ k_9\ k_{10}\ k_{11}\ k_{12}\ k_{13}\ k_{14}\ k_{15}\ k_{16}\ k_{17}\ k_{18}\ k_{19}\ k_{20}\ k_{21}\ k_{22}\ k_{23}\ k_{24}\ k_{25}\ k_{26}\ k_{27}\ k_{28}\ k_{29}\ k_{30}$$

- How many times does 11110 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times does 1111 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times does 111 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times does 010 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times does 100 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times does 000 appear?
  (A) 1 (B) 2 (C) 3 (D) 4

Quiz Very Similar to Exercise 7.1 (used in Plenary Session Week 7)

The keystream for the LFSR with taps $\{0, 2, 3, 4\}$ and width 5 for the key 00001 has period 31. The first 31 positions are

$$(0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$$
$$k_0\ k_1\ k_2\ k_3\ k_4\ k_5\ k_6\ k_7\ k_8\ k_9\ k_{10}\ k_{11}\ k_{12}\ k_{13}\ k_{14}\ k_{15}\ k_{16}\ k_{17}\ k_{18}\ k_{19}\ k_{20}\ k_{21}\ k_{22}\ k_{23}\ k_{24}\ k_{25}\ k_{26}\ k_{27}\ k_{28}\ k_{29}\ k_{30}$$

- How many times does 11110 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times does 1111 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times does 111 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times does 010 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times does 100 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times does 000 appear?
  (A) 1 (B) 2 (C) 3 (D) 4

Generalizing Example 7.1

Proposition 7.2

Let F be an invertible LFSR of width ℓ with a keystream of period $2^\ell - 1$. Let $k \in \mathbb{F}_2^\ell$ be non-zero and let $(k_0, k_1, \ldots, k_{2^\ell-2})$ be its generating cycle. We consider starting positions s within this cycle, so $0 \leq s < 2^\ell - 1$.

(a) *For each non-zero $x \in \mathbb{F}_2^\ell$ there exists a unique s such that*

$$(k_s, \ldots, k_{s+\ell-1}) = x.$$

(b) *Given any non-zero $y \in \mathbb{F}_2^m$ where $m \leq \ell$, there are precisely $2^{\ell-m}$ positions s such that $(k_s, \ldots, k_{s+m-1}) = y$.*

(c) *There are precisely $2^{\ell-m} - 1$ positions s such that $(k_s, \ldots, k_{s+m-1}) = (0, 0, \ldots, 0) \in \mathbb{F}_2^m$.*

Testing for Randomness

Exercise 7.3

Write down a sequence of 33 bits, fairly quickly, but trying to make it seem random. Count the number of zeros and the number of ones. (Do not wrap around.) Now count the number of adjacent pairs 00, 01, 10, 11. Does your sequence still seem random?

Exercise 7.4 (Monobit Test)

Let M_0 be the number of zeros and let M_1 be the number of ones in a binary sequence $B_0, B_1, \ldots, B_{n-1}$ of length n.

(a) Explain why if the bits are random we would expect that M_0 and M_1 both have the $\mathrm{Bin}(n, \frac{1}{2})$ distribution.

(b) Show that the χ^2 statistic with (a) as null hypothesis is $(M_0 - M_1)^2/n$.

(c) A sequence with $n = 100$ has 60 zeros. Does this suggest it is not truly random? [*Hint:* if $Z \sim N(0,1)$ then $\mathbb{P}[Z^2 \geq 3.841] \approx 0.05$ and $\mathbb{P}[Z^2 \geq 6.635] \approx 0.01$.]

The Hypothesis Testing Framework

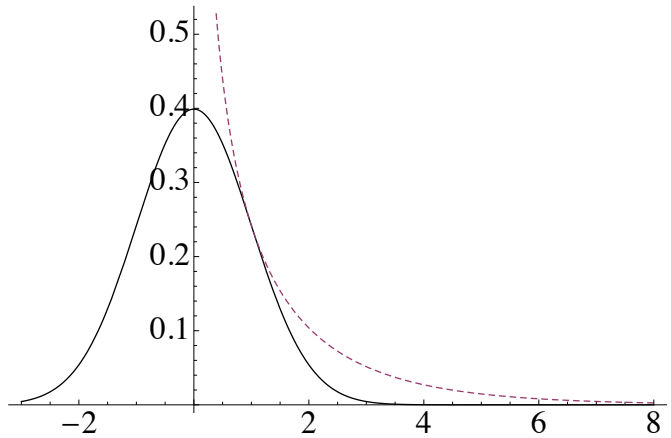
In Exercise 7.4 our null hypothesis was

- M_0 and M_1 are distributed binomially as $\mathrm{Bin}(n, \frac{1}{2})$.

We tested this using the statistic $(M_0 - M_1)^2/n$.

If the null hypothesis is true, this statistic is distributed as the χ^2 distribution, with 1 degree of freedom. (This is the square of an $N(0,1)$ random variable: mean 0, variance 1.)

(c) A sequence with $n = 100$ has 60 zeros. Does this suggest it is not random? [*Hint:* if $Z \sim N(0,1)$ then $\mathbb{P}[Z^2 \geq 3.841] \approx 0.05$ and $\mathbb{P}[Z^2 \geq 6.635] \approx 0.01$. The probability density functions for Z (solid) and Z^2 (dashed) are shown below.]



The Hypothesis Testing Framework

In Exercise 7.4 our null hypothesis was

- M_0 and M_1 are distributed binomially as $\mathrm{Bin}(n, \frac{1}{2})$.

We tested this using the statistic $(M_0 - M_1)^2/n$.

If the null hypothesis is true, this statistic is distributed as the χ^2 distribution, with 1 degree of freedom. (This is the square of an $N(0,1)$ random variable: mean 0, variance 1.)

(c) A sequence with $n = 100$ has 60 zeros. Does this suggest it is not random? [*Hint:* if $Z \sim N(0,1)$ then $\mathbb{P}[Z^2 \geq 3.841] \approx 0.05$ and $\mathbb{P}[Z^2 \geq 6.635] \approx 0.01$. The probability density functions for Z (solid) and Z^2 (dashed) are shown below.]

The statistic is $20^2/100 = 4$. **If the null hypothesis is true**,

- we observed a random variable $Z \sim N(0,1)$ and found that $Z^2 = 4$;
- the event that Z^2 is 3.891 or more has probability about 0.05
- we therefore decide the hypothesis is false.

The 'p-value' is 0.05 or 5%.

Quiz on Hypothesis Testing

We test a hypothesis using a statistic Z. If the hypothesis is true, Z has a known distribution; often this is a χ^2 distribution.
Examples: 'this medical intervention is no better than a placebo', 'this keystream is equally likely to be 0 as 1'.

(a) A p-value of 0.01 means there is only a 1% chance the hypothesis is true.

(A) False (B) True

(b) The p-value is the probability of seeing the exact value of Z.

(A) False (B) True

(c) The p-value is the probability, if the hypothesis is true, of seeing this value of Z, or something more extreme.

(A) False (B) True

(d) If the hypothesis is true then the p-value is uniformly distributed on $[0, 1]$.

(A) False (B) True

Quiz on Hypothesis Testing

We test a hypothesis using a statistic Z. If the hypothesis is true, Z has a known distribution; often this is a χ^2 distribution.
Examples: 'this medical intervention is no better than a placebo', 'this keystream is equally likely to be 0 as 1'.

(a) A p-value of 0.01 means there is only a 1% chance the hypothesis is true.

(A) False (B) True

(b) The p-value is the probability of seeing the exact value of Z.

(A) False (B) True

(c) The p-value is the probability, if the hypothesis is true, of seeing this value of Z, or something more extreme.

(A) False (B) True

(d) If the hypothesis is true then the p-value is uniformly distributed on $[0, 1]$.

(A) False (B) True

Quiz on Hypothesis Testing

We test a hypothesis using a statistic Z. If the hypothesis is true, Z has a known distribution; often this is a χ^2 distribution.
Examples: 'this medical intervention is no better than a placebo', 'this keystream is equally likely to be 0 as 1'.

(a) A p-value of 0.01 means there is only a 1% chance the hypothesis is true.

(A) False (B) True

(b) The p-value is the probability of seeing the exact value of Z.

(A) False (B) True

(c) The p-value is the probability, if the hypothesis is true, of seeing this value of Z, or something more extreme.

(A) False (B) True

(d) If the hypothesis is true then the p-value is uniformly distributed on $[0, 1]$.

(A) False (B) True

Quiz on Hypothesis Testing

We test a hypothesis using a statistic Z. If the hypothesis is true, Z has a known distribution; often this is a χ^2 distribution.
Examples: 'this medical intervention is no better than a placebo', 'this keystream is equally likely to be 0 as 1'.

(a) A p-value of 0.01 means there is only a 1% chance the hypothesis is true.

(A) False (B) True

(b) The p-value is the probability of seeing the exact value of Z.

(A) False (B) True

(c) The p-value is the probability, if the hypothesis is true, of seeing this value of Z, or something more extreme.

(A) False (B) True

(d) If the hypothesis is true then the p-value is uniformly distributed on $[0, 1]$.

(A) False (B) True

Quiz on Hypothesis Testing

We test a hypothesis using a statistic Z. If the hypothesis is true, Z has a known distribution; often this is a χ^2 distribution.
Examples: 'this medical intervention is no better than a placebo', 'this keystream is equally likely to be 0 as 1'.

(a) A p-value of 0.01 means there is only a 1% chance the hypothesis is true.

(A) False (B) True

(b) The p-value is the probability of seeing the exact value of Z.

(A) False (B) True

(c) The p-value is the probability, if the hypothesis is true, of seeing this value of Z, or something more extreme.

(A) False (B) True

(d) If the hypothesis is true then the p-value is uniformly distributed on $[0, 1]$.

(A) False (B) True

If the hypothesis is true and the statistic is z then the reported p-value is 10% if and only if $\mathbb{P}[Z \geq z] = 1/10$; clearly this has probability $1/10$.
You can replace $1/10$ with any probability p.

Quiz on Hypothesis Testing

We test a hypothesis using a statistic Z. If the hypothesis is true, Z has a known distribution; often this is a χ^2 distribution.
Examples: 'this medical intervention is no better than a placebo', 'this keystream is equally likely to be 0 as 1'.

(a) A p-value of 0.01 means there is only a 1% chance the hypothesis is true.

(A) False (B) True

(b) The p-value is the probability of seeing the exact value of Z.

(A) False (B) True

(c) The p-value is the probability, if the hypothesis is true, of seeing this value of Z, or something more extreme.

(A) False (B) True

(d) If the hypothesis is true then the p-value is uniformly distributed on $[0, 1]$.

(A) False (B) True

(e) If a lab conducts 20 experiments, on 20 different true hypotheses, then there is about a $\frac{2}{3}$ chance one will be rejected.

Quiz on Hypothesis Testing

We test a hypothesis using a statistic Z. If the hypothesis is true, Z has a known distribution; often this is a χ^2 distribution.
Examples: 'this medical intervention is no better than a placebo', 'this keystream is equally likely to be 0 as 1'.

(a) A p-value of 0.01 means there is only a 1% chance the hypothesis is true.

(A) False (B) True

(b) The p-value is the probability of seeing the exact value of Z.

(A) False (B) True

(c) The p-value is the probability, if the hypothesis is true, of seeing this value of Z, or something more extreme.

(A) False (B) True

(d) If the hypothesis is true then the p-value is uniformly distributed on $[0, 1]$.

(A) False (B) True

(e) If a lab conducts 20 experiments, on 20 different true hypotheses, then there is about a $\frac{2}{3}$ chance one will be rejected.

Quiz on Hypothesis Testing

We test a hypothesis using a statistic Z. If the hypothesis is true, Z has a known distribution; often this is a χ^2 distribution.
Examples: 'this medical intervention is no better than a placebo', 'this keystream is equally likely to be 0 as 1'.

(a) A p-value of 0.01 means there is only a 1% chance the hypothesis is true.

(A) False (B) True

(b) The p-value is the probability of seeing the exact value of Z.

(A) False (B) True

(c) The p-value is the probability, if the hypothesis is true, of seeing this value of Z, or something more extreme.

(A) False (B) True

(d) If the hypothesis is true then the p-value is uniformly distributed on $[0, 1]$.

(A) False (B) True

The p-value for the CERN Higgs Boson test is 3×10^{-7}, corresponding to 5 standard deviation off the mean in a normal distribution.

Correlation

Definition 7.5

Given $(x_0, x_1, \ldots, x_{n-1})$ and $(y_0, y_1, \ldots, y_{n-1}) \in \mathbb{F}_2^n$ define

$$c_{\text{same}} = \left|\{i : x_i = y_i\}\right|$$
$$c_{\text{diff}} = \left|\{i : x_i \neq y_i\}\right|.$$

The *correlation* between x and y is $(c_{\text{same}} - c_{\text{diff}})/n$.

Exercise 7.6

Find the correlation between a generating cycle for the LFSR of width 3 with taps $\{2, 3\}$ and each cyclic shift of itself. Would your answer change if a different key was used in the generating cycle?

Proposition 7.7

Let $(k_0, k_1, \ldots, k_{2^\ell - 2})$ be a generating cycle of an LFSR of width ℓ and maximum possible period $2^\ell - 1$. Let $1 \leq r < 2^\ell - 1$. The correlation between $(k_0, k_1, \ldots, k_{2^\ell - 2})$ and its proper cyclic shift

$$(k_r, k_{r+1}, \ldots, k_{2^\ell - 2}, k_0, \ldots, k_{r-1})$$

is $-\frac{1}{2^\ell - 1}$.

Quiz and Reminder of Proof of Proposition 7.7

Here are the key ideas. You should try to write out a proof for yourself using them and the quiz. Suppose the shift is $r \in \mathbb{N}$.

(a) Define $u_s = k_s + k_{s+r}$ for each $s \in \mathbb{N}_0$.

For example, the LFSR F of width 4 and taps $\{1, 4\}$ has a unique non-zero keystream of period 15. Taking $r = 2$ and $k = 0001$, we have

$$k_0 k_1 k_2 \ldots k_{12} k_{13} k_{14} = 000111101011001$$
$$k_2 k_3 k_4 \ldots \quad k_{14} k_0 k_1 = 011110101100100$$
$$u_0 u_1 u_2 \ldots u_{12} u_{13} u_{14} = 011001000111101$$

- True or false: $u_0 u_1 u_2 \ldots$ is the keystream of F with key 0110?
  (A) False (B) True
- The number of 0s in the generating cycle $u_0 u_1 u_2 \ldots u_{14}$ is?
  (A) 6 (B) 7 (C) 8 (D) 9
- The number of positions s in the generating cycle $k_0 k_1 k_2 \ldots k_{14}$ such that $k_s = k_{s+1}$ is?
  (A) 6 (B) 7 (C) 8 (D) 9

To complete the proof just generalize from this quiz.

Quiz and Reminder of Proof of Proposition 7.7

Here are the key ideas. You should try to write out a proof for yourself using them and the quiz. Suppose the shift is $r \in \mathbb{N}$.

(a) Define $u_s = k_s + k_{s+r}$ for each $s \in \mathbb{N}_0$.

For example, the LFSR F of width 4 and taps $\{1, 4\}$ has a unique non-zero keystream of period 15. Taking $r = 2$ and $k = 0001$, we have

$$k_0 k_1 k_2 \ldots k_{12} k_{13} k_{14} = 000111101011001$$
$$k_2 k_3 k_4 \ldots \quad k_{14} k_0 k_1 = 011110101100100$$
$$u_0 u_1 u_2 \ldots u_{12} u_{13} u_{14} = 011001000111101$$

- True or false: $u_0 u_1 u_2 \ldots$ is the keystream of F with key 0110?
  (A) False (B) True
- The number of 0s in the generating cycle $u_0 u_1 u_2 \ldots u_{14}$ is?
  (A) 6 (B) 7 (C) 8 (D) 9
- The number of positions s in the generating cycle $k_0 k_1 k_2 \ldots k_{14}$ such that $k_s = k_{s+1}$ is?
  (A) 6 (B) 7 (C) 8 (D) 9

To complete the proof just generalize from this quiz.

Quiz and Reminder of Proof of Proposition 7.7

Here are the key ideas. You should try to write out a proof for yourself using them and the quiz. Suppose the shift is $r \in \mathbb{N}$.

(a) Define $u_s = k_s + k_{s+r}$ for each $s \in \mathbb{N}_0$.

For example, the LFSR F of width 4 and taps $\{1, 4\}$ has a unique non-zero keystream of period 15. Taking $r = 2$ and $k = 0001$, we have

$$k_0 k_1 k_2 \ldots k_{12} k_{13} k_{14} = 000111101011001$$
$$k_2 k_3 k_4 \ldots \quad k_{14} k_0 k_1 = 011110101100100$$
$$u_0 u_1 u_2 \ldots u_{12} u_{13} u_{14} = 011001000111101$$

- True or false: $u_0 u_1 u_2 \ldots$ is the keystream of F with key 0110?
  (A) False (B) True
- The number of 0s in the generating cycle $u_0 u_1 u_2 \ldots u_{14}$ is?
  (A) 6 (B) 7 (C) 8 (D) 9
- The number of positions s in the generating cycle $k_0 k_1 k_2 \ldots k_{14}$ such that $k_s = k_{s+1}$ is?
  (A) 6 (B) 7 (C) 8 (D) 9

To complete the proof just generalize from this quiz.

Quiz and Reminder of Proof of Proposition 7.7

Here are the key ideas. You should try to write out a proof for yourself using them and the quiz. Suppose the shift is $r \in \mathbb{N}$.

(a) Define $u_s = k_s + k_{s+r}$ for each $s \in \mathbb{N}_0$.

For example, the LFSR F of width 4 and taps $\{1, 4\}$ has a unique non-zero keystream of period 15. Taking $r = 2$ and $k = 0001$, we have

$$k_0 k_1 k_2 \ldots k_{12} k_{13} k_{14} = 000111101011001$$
$$k_2 k_3 k_4 \ldots \quad k_{14} k_0 k_1 = 011110101100100$$
$$u_0 u_1 u_2 \ldots u_{12} u_{13} u_{14} = 011001000111101$$

- True or false: $u_0 u_1 u_2 \ldots$ is the keystream of F with key 0110?
  (A) False (B) True
- The number of 0s in the generating cycle $u_0 u_1 u_2 \ldots u_{14}$ is?
  (A) 6 (B) 7 (C) 8 (D) 9
- The number of positions s in the generating cycle $k_0 k_1 k_2 \ldots k_{14}$ such that $k_s = k_{s+1}$ is?
  (A) 6 (B) 7 (C) 8 (D) 9

To complete the proof just generalize from this quiz.

Quiz and Reminder of Proof of Proposition 7.7

Here are the key ideas. You should try to write out a proof for yourself using them and the quiz. Suppose the shift is $r \in \mathbb{N}$.

(a) Define $u_s = k_s + k_{s+r}$ for each $s \in \mathbb{N}_0$.

(b) Show that u_s satisfies the same recurrence relation $k_s = \sum_{t \in T} k_{s-t}$ as the original keystream (and its shift).

(c) In the keystream for u, 'sames' where $k_s = k_{s+r}$ correspond to 0s and 'differents' where $k_s \neq k_{s+r}$ correspond to 1s.

(d) Use Proposition 7.2 and (b) to determine the number of 'sames' and 'differents'. Why is the relevant key $u_0 u_1 \ldots u_\ell$ non-zero?

§8 Non-Linear Stream Ciphers

A general stream cipher takes a key $k \in \mathbb{F}_2^\ell$, for some fixed ℓ, and outputs a sequence $u_0, u_1, u_2, \ldots$ of bits. For each $n \in \mathbb{N}$ there is a corresponding cryptosystem where, as in Definition 6.4, the encryption functions $e_k : \mathbb{F}_2^n \to \mathbb{F}_2^n$ are defined by

$$e_k(x) = (u_0, u_1, \ldots, u_{n-1}) + (x_0, x_1, \ldots, x_{n-1}).$$

Exercise 8.1

In the LFSR cryptosystem of Definition 6.4, the keystream $u_0 u_1 u_2 \ldots$ is simply $k_0 k_1 k_2, \ldots$. Show how to find the key $(k_0, \ldots, k_{\ell-1})$ using a chosen plaintext attack.

Sum of LFSRs

Example 8.2

- Let F be the LFSR of width 4 with taps $\{3, 4\}$ of period 15.

The first 20 bits in the keystreams for F with keys $k = (0, 0, 0, 1)$ and $k' = (1, 1, 1, 1)$ sum to the sequence $(u_0, u_1, \ldots, u_{19})$ below:

k_i	0,	0,	0,	1,	0,	0,	1,	1,	0,	1,	0,	1,	1,	1,	1,	0,	0,	0,	1,	0
$k_i^\star$	1,	1,	1,	1,	0,	0,	0,	1,	0,	0,	1,	1,	0,	1,	0,	1,	1,	1,	1,	0
u_i	1,	1,	1,	0,	0,	0,	1,	0,	0,	1,	1,	0,	1,	0,	1,	1,	1,	1,	0,	0
	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9

Unfortunately, $u_0 u_1 u_2 \ldots$ is also generated by F: since it starts 1110, it is the keystream for $(1, 1, 1, 0)$. *Exercise:*

(a) Explain why this should have been expected. [*Hint:* the same linearity was used to prove Proposition 7.7.]

(b) *Exercise:* which pair of keys below gives the same sequence $(u_0, u_1, \ldots, u_{19})$?

(A) $0001, 1110$ (B) $0011, 1110$ (C) $0011, 1101$ (D) $0011, 1111$

Sum of LFSRs

Example 8.2

- Let F be the LFSR of width 4 with taps $\{3, 4\}$ of period 15.

The first 20 bits in the keystreams for F with keys $k = (0, 0, 0, 1)$ and $k' = (1, 1, 1, 1)$ sum to the sequence $(u_0, u_1, \ldots, u_{19})$ below:

k_i	0,	0,	0,	1,	0,	0,	1,	1,	0,	1,	0,	1,	1,	1,	1,	0,	0,	0,	1,	0
$k_i^\star$	1,	1,	1,	1,	0,	0,	0,	1,	0,	0,	1,	1,	0,	1,	0,	1,	1,	1,	1,	0
u_i	1,	1,	1,	0,	0,	0,	1,	0,	0,	1,	1,	0,	1,	0,	1,	1,	1,	1,	0,	0
	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9

Unfortunately, $u_0 u_1 u_2 \ldots$ is also generated by F: since it starts 1110, it is the keystream for $(1, 1, 1, 0)$. *Exercise:*

(a) Explain why this should have been expected. [*Hint:* the same linearity was used to prove Proposition 7.7.]

(b) *Exercise:* which pair of keys below gives the same sequence $(u_0, u_1, \ldots, u_{19})$?

(A) $0001, 1110$ (B) $0011, 1110$ (C) $0011, 1101$ (D) $0011, 1111$

Sum of LFSRs

Example 8.2

- Let F be the LFSR of width 4 with taps $\{3, 4\}$ of period 15.

The first 20 bits in the keystreams for F with keys $k = (0, 0, 0, 1)$ and $k' = (1, 1, 1, 1)$ sum to the sequence $(u_0, u_1, \ldots, u_{19})$ below:

k_i	0,	0,	0,	1,	0,	0,	1,	1,	0,	1,	0,	1,	1,	1,	1,	0,	0,	0,	1,	0
$k_i^\star$	1,	1,	1,	1,	0,	0,	0,	1,	0,	0,	1,	1,	0,	1,	0,	1,	1,	1,	1,	0
u_i	1,	1,	1,	0,	0,	0,	1,	0,	0,	1,	1,	0,	1,	0,	1,	1,	1,	1,	0,	0
	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9

Unfortunately, $u_0 u_1 u_2 \ldots$ is also generated by F: since it starts 1110, it is the keystream for $(1, 1, 1, 0)$. *Exercise:*

(a) Explain why this should have been expected. [*Hint:* the same linearity was used to prove Proposition 7.7.]

(b) *Exercise:* can the keys k and $k^\star$ be recovered from $(u_0, u_1, \ldots, u_{19})$?

(A) No (B) Yes

Sum of LFSRs

Example 8.2

- Let F be the LFSR of width 4 with taps $\{3, 4\}$ of period 15.

The first 20 bits in the keystreams for F with keys $k = (0, 0, 0, 1)$ and $k' = (1, 1, 1, 1)$ sum to the sequence $(u_0, u_1, \ldots, u_{19})$ below:

k_i	0,	0,	0,	1,	0,	0,	1,	1,	0,	1,	0,	1,	1,	1,	1,	0,	0,	0,	1,	0
$k_i^\star$	1,	1,	1,	1,	0,	0,	0,	1,	0,	0,	1,	1,	0,	1,	0,	1,	1,	1,	1,	0
u_i	1,	1,	1,	0,	0,	0,	1,	0,	0,	1,	1,	0,	1,	0,	1,	1,	1,	1,	0,	0
	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9

Unfortunately, $u_0 u_1 u_2 \ldots$ is also generated by F: since it starts 1110, it is the keystream for $(1, 1, 1, 0)$. *Exercise:*

(a) Explain why this should have been expected. [*Hint:* the same linearity was used to prove Proposition 7.7.]

(b) *Exercise:* can the keys k and $k^\star$ be recovered from $(u_0, u_1, \ldots, u_{19})$?

(A) No (B) Yes

Sum of LFSRs

Example 8.2

- Let F be the LFSR of width 4 with taps $\{3, 4\}$ of period 15.

The first 20 bits in the keystreams for F with keys $k = (0, 0, 0, 1)$ and $k' = (1, 1, 1, 1)$ sum to the sequence $(u_0, u_1, \ldots, u_{19})$ below:

k_i	0,	0,	0,	1,	0,	0,	1,	1,	0,	1,	0,	1,	1,	1,	1,	0,	0,	0,	1,	0
$k_i^\star$	1,	1,	1,	1,	0,	0,	0,	1,	0,	0,	1,	1,	0,	1,	0,	1,	1,	1,	1,	0
u_i	1,	1,	1,	0,	0,	0,	1,	0,	0,	1,	1,	0,	1,	0,	1,	1,	1,	1,	0,	0
	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9

Unfortunately, $u_0 u_1 u_2 \ldots$ is also generated by F: since it starts 1110, it is the keystream for $(1, 1, 1, 0)$. *Exercise:*

(a) Explain why this should have been expected. [*Hint:* the same linearity was used to prove Proposition 7.7.]

(b) The attacker knows $u_0 u_1 u_2 \ldots u_{19}$ but cannot learn k and $k^\star$. Can she decrypt further ciphertexts obtained by adding the keystream to the plaintext?

(A) No (B) Yes

Sum of LFSRs

Example 8.2

- Let F be the LFSR of width 4 with taps $\{3, 4\}$ of period 15.

The first 20 bits in the keystreams for F with keys $k = (0, 0, 0, 1)$ and $k' = (1, 1, 1, 1)$ sum to the sequence $(u_0, u_1, \ldots, u_{19})$ below:

k_i	0,	0,	0,	1,	0,	0,	1,	1,	0,	1,	0,	1,	1,	1,	1,	0,	0,	0,	1,	0
$k_i^\star$	1,	1,	1,	1,	0,	0,	0,	1,	0,	0,	1,	1,	0,	1,	0,	1,	1,	1,	1,	0
u_i	1,	1,	1,	0,	0,	0,	1,	0,	0,	1,	1,	0,	1,	0,	1,	1,	1,	1,	0,	0
	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9

Unfortunately, $u_0 u_1 u_2 \ldots$ is also generated by F: since it starts 1110, it is the keystream for $(1, 1, 1, 0)$. *Exercise:*

(a) Explain why this should have been expected. [*Hint:* the same linearity was used to prove Proposition 7.7.]

(b) The attacker knows $u_0 u_1 u_2 \ldots u_{19}$ but cannot learn k and $k^\star$. Can she decrypt further ciphertexts obtained by adding the keystream to the plaintext?

(A) No (B) Yes

Sum of LFSRs

Example 8.2

- Let F be the LFSR of width 4 with taps $\{3, 4\}$ of period 15.

The first 20 bits in the keystreams for F with keys $k = (0, 0, 0, 1)$ and $k' = (1, 1, 1, 1)$ sum to the sequence $(u_0, u_1, \ldots, u_{19})$ below:

k_i	0,	0,	0,	1,	0,	0,	1,	1,	0,	1,	0,	1,	1,	1,	1,	0,	0,	0,	1,	0
$k_i^\star$	1,	1,	1,	1,	0,	0,	0,	1,	0,	0,	1,	1,	0,	1,	0,	1,	1,	1,	1,	0
u_i	1,	1,	1,	0,	0,	0,	1,	0,	0,	1,	1,	0,	1,	0,	1,	1,	1,	1,	0,	0
	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9

Unfortunately, $u_0 u_1 u_2 \ldots$ is also generated by F: since it starts 1110, it is the keystream for $(1, 1, 1, 0)$. *Exercise:*

(a) Explain why this should have been expected. [*Hint:* the same linearity was used to prove Proposition 7.7.]

(b) Reason: She doesn't need k and $k^\star$, she just needs $u_0 u_1 u_2 u_3$, since this is the key for the keystream $u_0 u_1 u_2 u_3 \ldots u_{19}$.

Example 8.2 [continued]

- Let F' be the LFSR of width 3 with taps $\{2, 3\}$ of period 7.

The first 20 bits in the keystreams for F and F' with keys $k = (0, 0, 0, 1)$ and $k' = (0, 0, 1)$ and their sum $u_0 u_1 \ldots u_{19}$ are:

k_i	0	0	0	1	0	0	1	1	0	1	0	1	1	1	1	0	0	0	1	0
k'_i	0	0	1	0	1	1	1	0	0	1	0	1	1	1	0	0	1	0	1	1
u_i	0	0	1	1	1	1	0	1	0	0	0	0	0	0	1	0	1	0	0	1
	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9

Quiz: what is the period of $u_0 u_1 u_2 \ldots$?

(A) 7 (B) 15 (C) 105 (D) need more info

Example 8.2 [continued]

- Let F' be the LFSR of width 3 with taps $\{2, 3\}$ of period 7.

The first 20 bits in the keystreams for F and F' with keys $k = (0, 0, 0, 1)$ and $k' = (0, 0, 1)$ and their sum $u_0 u_1 \ldots u_{19}$ are:

k_i	0	0	0	1	0	0	1	1	0	1	0	1	1	1	1	0	0	0	1	0
k'_i	0	0	1	0	1	1	1	0	0	1	0	1	1	1	0	0	1	0	1	1
u_i	0	0	1	1	1	1	0	1	0	0	0	0	0	0	1	0	1	0	0	1
	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9

Quiz: what is the period of $u_0 u_1 u_2 \ldots$?

(A) 7 (B) 15 (C) 105 (D) need more info

Example 8.2 [continued]

- Let F' be the LFSR of width 3 with taps $\{2, 3\}$ of period 7.

The first 20 bits in the keystreams for F and F' with keys $k = (0, 0, 0, 1)$ and $k' = (0, 0, 1)$ and their sum $u_0 u_1 \ldots u_{19}$ are:

k_i	0,	0,	0,	1,	0,	0,	1,	1,	0,	1,	0,	1,	1,	1,	1,	0,	0,	0,	1,	0
k'_i	0,	0,	1,	0,	1,	1,	1,	0,	0,	1,	0,	1,	1,	1,	0,	0,	1,	0,	1,	1
u_i	0,	0,	1,	1,	1,	1,	0,	1,	0,	0,	0,	0,	0,	0,	1,	0,	1,	0,	0,	1
	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9

Quiz: what is the period of $u_0 u_1 u_2 \ldots$?
(A) 7 (B) 15 (C) 105 (D) need more info

This is encouraging: combining the LFSRs creates a keystream with a much longer period than either individually.

The bad news is that the keystream $(u_0, u_1, u_2, \ldots)$ is generated by the LFSR of width 7 with taps $\{2, 4, 5, 7\}$. So any LFSR attack is still effective.

M.Sc. students will see the Berlekamp–Massey Algorithm in §6, that can be used to find this LFSR. We also used these keystreams as an example of annihilators in §5.

Geffe Generator

Example 8.3

A *Geffe generator* is constructed using three LFSRs F, F' and G of widths ℓ, ℓ' and m, all with maximum possible period. Following Kerckhoff's Principle, the widths and taps of these LFSRs are public knowledge.

- Let $k_0 k_1 k_2 \ldots$ and $k'_0 k'_1 k'_2 \ldots$ be keystreams for F and F'
- Let $g_0 g_1 g_2 \ldots$ be a keystream for G.

The *Geffe keystream* $(u_0, u_1, u_2, \ldots)$ is defined by

$$u_i = \begin{cases} k_i & \text{if } g_i = 0 \\ k'_i & \text{if } g_i = 1. \end{cases}$$

Example 8.3 [continued]

For example, if F and F' and their keystreams are as in Example 8.2 (so F has width 4, taps $\{3,4\}$, F' has width 3, taps $\{2,3\}$), and G is the LFSR of width 4 with taps $\{1,4\}$ and $g_0g_1g_2g_3 = 0001$, then, using colours to indicate which bit is used:

k_i	0,	0,	0,	1,	0,	0,	1,	1,	0,	1,	0,	1,	1,	1,	1,	0,	0,	0,	1,	0
k'_i	0,	0,	1,	0,	1,	1,	1,	0,	0,	1,	0,	1,	1,	1,	0,	0,	1,	0,	1,	1
g_i	0,	0,	0,	1,	1,	1,	1,	0,	1,	0,	1,	1,	0,	0,	1,	0,	0,	0,	1,	1
u_i	0,	0,	0,	0,	1,	1,	1,	1,	0,	1,	0,	1,	1,	1,	0,	0,	0,	0,	1,	1
	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9

Quiz: the period of $u_0u_1u_2\ldots$ is

(A) 15 (B) 35 (C) 105 (D) 1575

Quiz: What (up to a very small error) is $\mathbb{P}[k_i = u_i]$?

(A) 1/4 (B) 1/2 (C) 3/4 (D) 1

Quiz: For n large, what is the expected correlation between $(k_0,\ldots,k_{n-1})$ and $(u_0,\ldots,u_{n-1})$?

(A) 0 (B) 1/4 (C) 1/2 (D) 3/4

Example 8.3 [continued]

For example, if F and F' and their keystreams are as in Example 8.2 (so F has width 4, taps $\{3,4\}$, F' has width 3, taps $\{2,3\}$), and G is the LFSR of width 4 with taps $\{1,4\}$ and $g_0g_1g_2g_3 = 0001$, then, using colours to indicate which bit is used:

k_i	0,	0,	0,	1,	0,	0,	1,	1,	0,	1,	0,	1,	1,	1,	1,	0,	0,	0,	1,	0
k'_i	0,	0,	1,	0,	1,	1,	1,	0,	0,	1,	0,	1,	1,	1,	0,	0,	1,	0,	1,	1
g_i	0,	0,	0,	1,	1,	1,	1,	0,	1,	0,	1,	1,	0,	0,	1,	0,	0,	0,	1,	1
u_i	0,	0,	0,	0,	1,	1,	1,	1,	0,	1,	0,	1,	1,	1,	0,	0,	0,	0,	1,	1
	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9

Quiz: the period of $u_0u_1u_2\ldots$ is

(A) 15 (B) 35 (C) 105 (D) 1575

Quiz: What (up to a very small error) is $\mathbb{P}[k_i = u_i]$?

(A) 1/4 (B) 1/2 (C) 3/4 (D) 1

Quiz: For n large, what is the expected correlation between $(k_0,\ldots,k_{n-1})$ and $(u_0,\ldots,u_{n-1})$?

(A) 0 (B) 1/4 (C) 1/2 (D) 3/4

Example 8.3 [continued]

For example, if F and F' and their keystreams are as in Example 8.2 (so F has width 4, taps $\{3,4\}$, F' has width 3, taps $\{2,3\}$), and G is the LFSR of width 4 with taps $\{1,4\}$ and $g_0g_1g_2g_3 = 0001$, then, using colours to indicate which bit is used:

k_i	0,	0,	0,	1,	0,	0,	1,	1,	0,	1,	0,	1,	1,	1,	1,	0,	0,	0,	1,	0
k'_i	0,	0,	1,	0,	1,	1,	1,	0,	0,	1,	0,	1,	1,	1,	0,	0,	1,	0,	1,	1
g_i	0,	0,	0,	1,	1,	1,	1,	0,	1,	0,	1,	1,	0,	0,	1,	0,	0,	0,	1,	1
u_i	0,	0,	0,	0,	1,	1,	1,	1,	0,	1,	0,	1,	1,	1,	0,	0,	0,	0,	1,	1
	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9

Quiz: the period of $u_0u_1u_2\ldots$ is

(A) 15 (B) 35 (C) 105 (D) 1575

Quiz: What (up to a very small error) is $\mathbb{P}[k_i = u_i]$?

(A) 1/4 (B) 1/2 (C) 3/4 (D) 1

Quiz: For n large, what is the expected correlation between $(k_0,\ldots,k_{n-1})$ and $(u_0,\ldots,u_{n-1})$?

(A) 0 (B) 1/4 (C) 1/2 (D) 3/4

Example 8.3 [continued]

For example, if F and F' and their keystreams are as in Example 8.2 (so F has width 4, taps $\{3,4\}$, F' has width 3, taps $\{2,3\}$), and G is the LFSR of width 4 with taps $\{1,4\}$ and $g_0g_1g_2g_3 = 0001$, then, using colours to indicate which bit is used:

k_i	0,	0,	0,	1,	0,	0,	1,	1,	0,	1,	0,	1,	1,	1,	1,	0,	0,	0,	1,	0
k'_i	0,	0,	1,	0,	1,	1,	1,	0,	0,	1,	0,	1,	1,	1,	0,	0,	1,	0,	1,	1
g_i	0,	0,	0,	1,	1,	1,	1,	0,	1,	0,	1,	1,	0,	0,	1,	0,	0,	0,	1,	1
u_i	0,	0,	0,	0,	1,	1,	1,	1,	0,	1,	0,	1,	1,	1,	0,	0,	0,	0,	1,	1
	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9

Quiz: the period of $u_0u_1u_2\ldots$ is

(A) 15 (B) 35 (C) 105 (D) 1575

Quiz: What (up to a very small error) is $\mathbb{P}[k_i = u_i]$?

(A) 1/4 (B) 1/2 (C) 3/4 (D) 1

Quiz: For n large, what is the expected correlation between $(k_0,\ldots,k_{n-1})$ and $(u_0,\ldots,u_{n-1})$?

(A) 0 (B) 1/4 (C) 1/2 (D) 3/4

Example 8.3 [continued]

For example, if F and F' and their keystreams are as in Example 8.2 (so F has width 4, taps $\{3,4\}$, F' has width 3, taps $\{2,3\}$), and G is the LFSR of width 4 with taps $\{1,4\}$ and $g_0g_1g_2g_3 = 0001$, then, using colours to indicate which bit is used:

k_i	0,	0,	0,	1,	0,	0,	1,	1,	0,	1,	0,	1,	1,	1,	1,	0,	0,	0,	1,	0
k'_i	0,	0,	1,	0,	1,	1,	1,	0,	0,	1,	0,	1,	1,	1,	0,	0,	1,	0,	1,	1
g_i	0,	0,	0,	1,	1,	1,	1,	0,	1,	0,	1,	1,	0,	0,	1,	0,	0,	0,	1,	1
u_i	0,	0,	0,	0,	1,	1,	1,	1,	0,	1,	0,	1,	1,	1,	0,	0,	0,	0,	1,	1
	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9

What is the correlation in this case between $k'_0k_1 \ldots k'_{19}$ and $u_0u_1 \ldots u_{19}$?

(A) $\frac{3}{10}$ (B) $\frac{1}{2}$ (C) $\frac{3}{5}$ (D) $\frac{7}{10}$

Example 8.3 [continued]

For example, if F and F' and their keystreams are as in Example 8.2 (so F has width 4, taps $\{3,4\}$, F' has width 3, taps $\{2,3\}$), and G is the LFSR of width 4 with taps $\{1,4\}$ and $g_0g_1g_2g_3 = 0001$, then, using colours to indicate which bit is used:

k_i	0,	0,	0,	1,	0,	0,	1,	1,	0,	1,	0,	1,	1,	1,	1,	0,	0,	0,	1,	0
k'_i	0,	0,	1,	0,	1,	1,	1,	0,	0,	1,	0,	1,	1,	1,	0,	0,	1,	0,	1,	1
g_i	0,	0,	0,	1,	1,	1,	1,	0,	1,	0,	1,	1,	0,	0,	1,	0,	0,	0,	1,	1
u_i	0,	0,	0,	0,	1,	1,	1,	1,	0,	1,	0,	1,	1,	1,	0,	0,	0,	0,	1,	1
	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9

What is the correlation in this case between $k'_0k_1 \ldots k'_{19}$ and $u_0u_1 \ldots u_{19}$?

(A) $\frac{3}{10}$ (B) $\frac{1}{2}$ (C) $\frac{3}{5}$ (D) $\frac{7}{10}$

Example 8.3 [continued]

For example, if F and F' and their keystreams are as in Example 8.2 (so F has width 4, taps $\{3,4\}$, F' has width 3, taps $\{2,3\}$), and G is the LFSR of width 4 with taps $\{1,4\}$ and $g_0g_1g_2g_3 = 0001$, then, using colours to indicate which bit is used:

k_i	0,	0,	0,	1,	0,	0,	1,	1,	0,	1,	0,	1,	1,	1,	1,	0,	0,	0,	1,	0
k'_i	0,	0,	1,	0,	1,	1,	1,	0,	0,	1,	0,	1,	1,	1,	0,	0,	1,	0,	1,	1
g_i	0,	0,	0,	1,	1,	1,	1,	0,	1,	0,	1,	1,	0,	0,	1,	0,	0,	0,	1,	1
u_i	0,	0,	0,	0,	1,	1,	1,	1,	0,	1,	0,	1,	1,	1,	0,	0,	0,	0,	1,	1
	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9

What is the correlation in this case between $k'_0k_1 \ldots k'_{19}$ and $u_0u_1 \ldots u_{19}$?

(A) $\frac{3}{10}$ (B) $\frac{1}{2}$ (C) $\frac{3}{5}$ (D) $\frac{7}{10}$

So when we guess correctly, we see a correlation of $\frac{7}{10}$. The sample is small, and by chance this is more than the predicted $\frac{1}{2}$.

Example 8.3 [continued]

For example, if F and F' and their keystreams are as in Example 8.2 (so F has width 4, taps $\{3,4\}$, F' has width 3, taps $\{2,3\}$), and G is the LFSR of width 4 with taps $\{1,4\}$ and $g_0g_1g_2g_3 = 0001$, then, using colours to indicate which bit is used:

k_i	0	0	0	1	0	0	1	1	0	1	0	1	1	1	1	0	0	0	1	0
k'_i	0	0	1	0	1	1	1	0	0	1	0	1	1	1	0	0	1	0	1	1
g_i	0	0	0	1	1	1	1	0	1	0	1	1	0	0	1	0	0	0	1	1
u_i	0	0	0	0	1	1	1	1	0	1	0	1	1	1	0	0	0	0	1	1
	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9

Suppose we guess (wrongly) that

$$(k_0, k_1, k_2) = (1, 1, 0).$$

The correlation between the implied keystream $(v_0, v_1, v_2, \ldots, v_{19})$ and $(u_0, u_1, \ldots, u_{19})$ is $(7 - 13)/20 = -\frac{3}{10}$.

v_i	1	1	0	0	1	0	1	1	1	0	0	1	0	1	1	1	0	0	1	0
u_i	0	0	1	0	1	1	1	1	0	1	0	1	1	0	0	0	1	0	0	1

Correlation Attack on Geffe Generator

Attack 8.4

Suppose that n bits of the Geffe keystream are known. The attacker computes, for each candidate key $(v_0, v_1, \ldots, v_{\ell-1}) \in \mathbb{F}_2^\ell$, the correlation between $(v_0, v_1, \ldots, v_{n-1})$ and $(u_0, u_1, \ldots, u_{n-1})$. If the correlation is not nearly $\frac{1}{2}$ then the candidate key is rejected. Otherwise it is likely that $(k_0, \ldots, k_{\ell-1}) = (v_0, \ldots, v_{\ell-1})$.

Quiz: suppose that $\ell < \ell'$. Is it better to guess the key for F or the key for F'?

(A) Guess F (B) Guess F'

Correlation Attack on Geffe Generator

Attack 8.4

Suppose that n bits of the Geffe keystream are known. The attacker computes, for each candidate key $(v_0, v_1, \ldots, v_{\ell-1}) \in \mathbb{F}_2^\ell$, the correlation between $(v_0, v_1, \ldots, v_{n-1})$ and $(u_0, u_1, \ldots, u_{n-1})$. If the correlation is not nearly $\frac{1}{2}$ then the candidate key is rejected. Otherwise it is likely that $(k_0, \ldots, k_{\ell-1}) = (v_0, \ldots, v_{\ell-1})$.

Quiz: suppose that $\ell < \ell'$. Is it better to guess the key for F or the key for F'?

(A) Guess F (B) Guess F'

Correlation Attack on Geffe Generator

Attack 8.4

Suppose that n bits of the Geffe keystream are known. The attacker computes, for each candidate key $(v_0, v_1, \ldots, v_{\ell-1}) \in \mathbb{F}_2^\ell$, the correlation between $(v_0, v_1, \ldots, v_{n-1})$ and $(u_0, u_1, \ldots, u_{n-1})$. If the correlation is not nearly $\frac{1}{2}$ then the candidate key is rejected. Otherwise it is likely that $(k_0, \ldots, k_{\ell-1}) = (v_0, \ldots, v_{\ell-1})$.

Quiz: suppose that $\ell < \ell'$. Is it better to guess the key for F or the key for F'?

(A) Guess F (B) Guess F'

One can repeat Attack 8.4 to learn $(k'_0, k'_1, \ldots, k'_{\ell'-1})$. Overall this requires at most $2^\ell + 2^{\ell'}$ guesses. This is a huge improvement on the $2^{\ell+\ell'}$ guesses required by trying every possible pair of keys. (See Question 1(b) on Sheet 6 for a faster finish.)

An attack such as Attack 8.4 is said to be *sub-exhaustive* because it finds the key using fewer guesses than brute-force exhaustive search through the keyspace.

Quadratic Stream Cipher

The remaining slides are on optional extras for Part B. You are encouraged to look briefly at Trivium, just to see the first example in this course of a complete cryptosystem that is used in practice for highly confidential data.

Example 8.5

Let F be the LFSR of width 5 with taps $\{3, 5\}$ and let F' be the LFSR of width 6 with taps $\{2, 3, 5, 6\}$. These have the maximum possible periods for their widths, namely $2^5 - 1 = 31$ and $2^6 - 1 = 63$. Fix $m \in \mathbb{N}$ and for each $i \geq m$, define

$$u_s = k_s k'_s + k_{s-1} k'_{s-1} + \cdots + k_{s-(m-1)} k'_{s-(m-1)}.$$

Note that there are m products in the sum. Define $u_s = 0$ if $0 \leq s < m - 1$. The *m-quadratic stream cipher* is the cryptosystem defined using the keystream $u_0, u_1, \ldots, u_{1023}$.

Taking $m = 1$ gives a cipher like the Geffe generator: since $u_s = k_s k'_s$ we have $\mathbb{P}[u_s = k_s] = \frac{3}{4}$, giving a correlation of $\frac{1}{2}$. Attack 8.4 is effective.

Quadratic Stream Cipher

For general m, the expected correlation between keystream of the m-quadratic stream cipher $u_0 u_1 u_2 \ldots u_{1023}$ and the keystream $k_0 k_1 k_2 \ldots k_{1023}$ of the LFSR of width 5 is about $\frac{1}{2^m}$. (**M.Sc. students**: this was seen for the cases $m = 1$ and $m = 2$ in §4 and the general case follows from the Piling-Up Lemma.)

Taking $m = 5$, this makes the correlation attack ineffective because the difference between 0 correlation and the correlation of $\pm\frac{1}{2^5}$ from a correct key guess cannot be detected with 2^{10} samples.

The 5-quadratic stream cipher is therefore somewhat resistant to the chosen plaintext attack in Exercise 8.1.

Exercise 8.6

Unfortunately the m-quadratic cipher is still vulnerable because taking the sum of two adjacent bits u_i and u_{i-1} in the keystream cancels out many of the quadratic terms. Use this to find a subexhaustive attack.

Trivium

Example 8.7 (Trivium)

The building blocks are three LFSRs of widths 93, 84 and 111, with taps $\{66, 93\}$, $\{69, 84\}$ and $\{66, 111\}$. Let $x \in \mathbb{F}_2^{93}$, $y \in \mathbb{F}_2^{84}$, $z \in \mathbb{F}_2^{111}$ be the internal states. The registers are updated using the functions f, g and h, respectively, where

$$\begin{aligned} f(x, y, z) &= z_0 + z_{111-66} + z_1 z_2 + x_{24} \\ g(x, y, z) &= x_0 + x_{93-66} + x_1 x_2 + y_6 \\ h(x, y, z) &= y_0 + y_{84-69} + y_1 y_2 + z_{24} \end{aligned}$$

For instance the x-register is updated using f, so in each step

$$(x_0, \ldots, x_{92}) \mapsto \big(x_1, \ldots, x_{92}, f(x, y, z)\big).$$

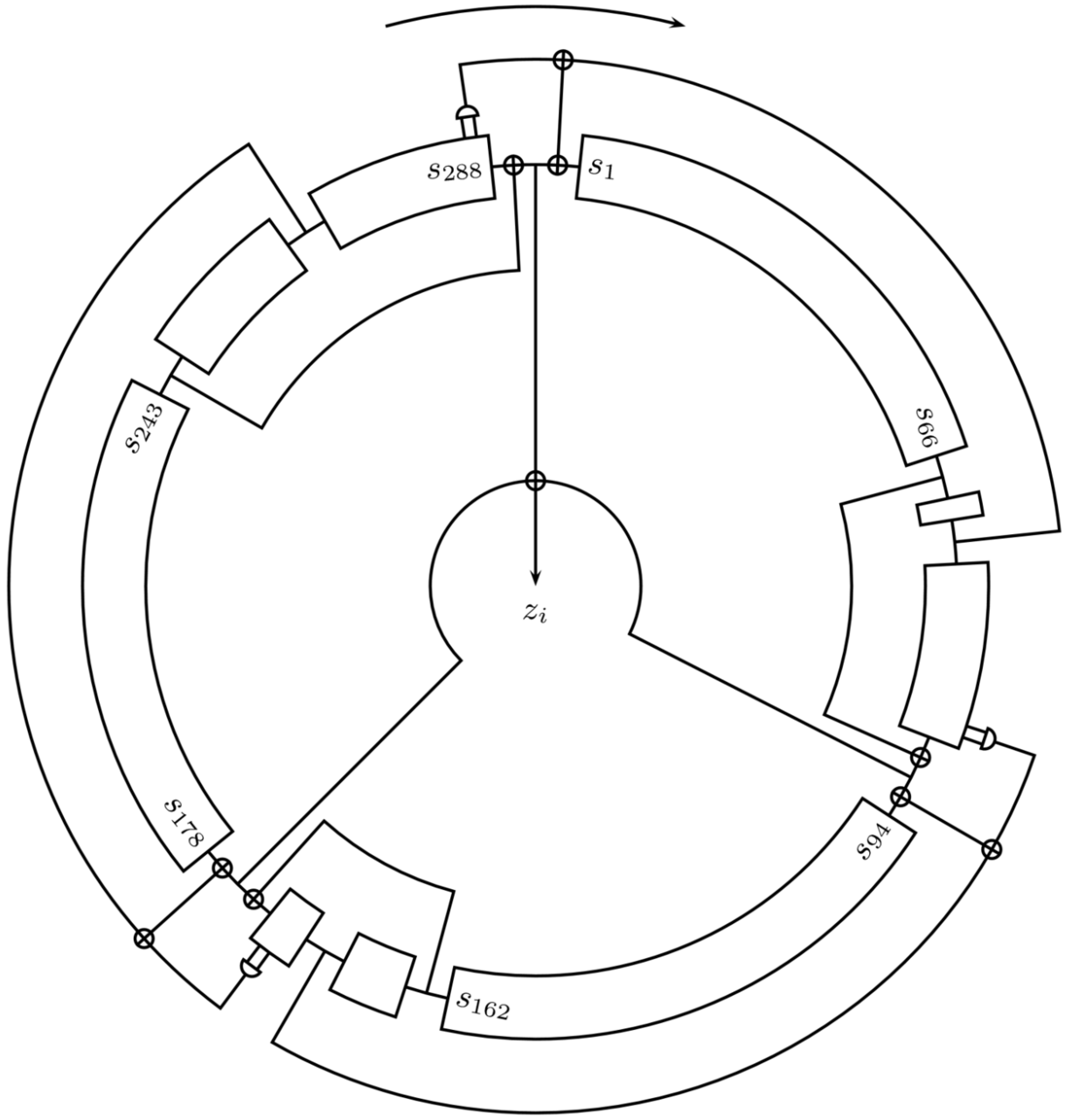
The keystream bit from each step is

$$x_0 + x_{93-66} + y_0 + y_{84-69} + z_0 + z_{111-66}.$$

Example 8.7 [continued]: Trivium Key

Rather than use a 288-bit key, TRIVIUM uses a (secret) 80-bit key put in the x-register, and a (non-secret) 80-bit initialization vector put in the y-register. The remaining positions in the internal state start as 0, except for z_0, z_1, z_2 which start as 1. (Exercise: why do this?) The first 1152 bits of the keystream are unusually biased, and so are discarded. This can be seen, for the earlier bits, using the implementation of TRIVIUM in the MATHEMATICA notebook on Moodle.

Example 8.7 [continued]: Trivium Circuit Diagram



Part C: Block ciphers

§9 Feistel Networks and DES

In a block cipher of *block size* n and *key length* ℓ, $\mathcal{P} = \mathcal{C} = \mathbb{F}_2^n$, and $\mathcal{K} = \mathbb{F}_2^\ell$. Since $\mathcal{P} = \mathcal{C}$, by Exercise 3.3(ii), each encryption function e_k for $k \in \mathcal{K}$ is bijective, and the cryptoscheme is determined by the encryption functions.

In a typical modern block cipher, $n = 128$ and $\ell = 128$. Since most messages have more than n bits, they have to be split into multiple *blocks*, each of n bits, before encryption.

Part C: Block ciphers

§9 Feistel Networks and DES

In a block cipher of *block size* n and *key length* ℓ, $\mathcal{P} = \mathcal{C} = \mathbb{F}_2^n$, and $\mathcal{K} = \mathbb{F}_2^\ell$. Since $\mathcal{P} = \mathcal{C}$, by Exercise 3.3(ii), each encryption function e_k for $k \in \mathcal{K}$ is bijective, and the cryptoscheme is determined by the encryption functions.

In a typical modern block cipher, $n = 128$ and $\ell = 128$. Since most messages have more than n bits, they have to be split into multiple *blocks*, each of n bits, before encryption.

Example 9.1

The binary one-time pad of length n is the block cipher of block size n and key length n in which $e_k(x) = x + k$ for all $k \in \mathbb{F}_2^n$.

Part C: Block ciphers

§9 Feistel Networks and DES

In a block cipher of *block size* n and *key length* ℓ, $\mathcal{P} = \mathcal{C} = \mathbb{F}_2^n$, and $\mathcal{K} = \mathbb{F}_2^\ell$. Since $\mathcal{P} = \mathcal{C}$, by Exercise 3.3(ii), each encryption function e_k for $k \in \mathcal{K}$ is bijective, and the cryptoscheme is determined by the encryption functions.

In a typical modern block cipher, $n = 128$ and $\ell = 128$. Since most messages have more than n bits, they have to be split into multiple *blocks*, each of n bits, before encryption.

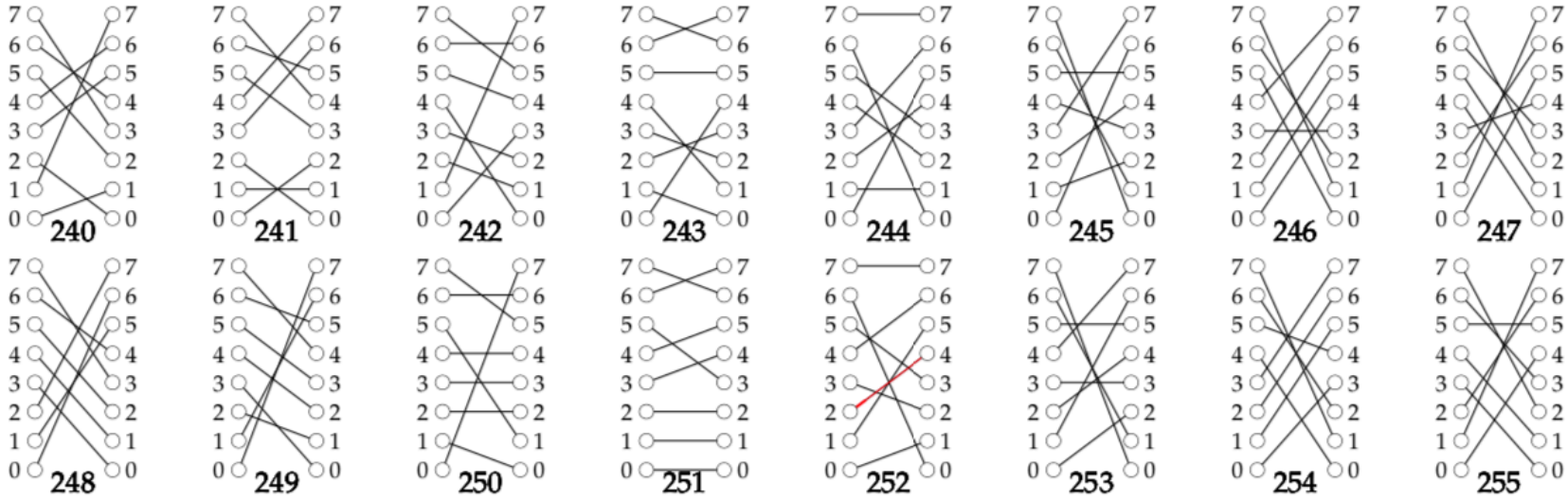
Example 9.1

The binary one-time pad of length n is the block cipher of block size n and key length n in which $e_k(x) = x + k$ for all $k \in \mathbb{F}_2^n$.

Modern block ciphers aim to be secure even against a chosen plaintext attack allowing *arbitrarily many* plaintexts. That is, even given all pairs $(x, e_k(x))$ for $x \in \mathbb{F}_2^n$, there should be no faster way to find the key k then exhausting over all possible keys in $\mathbb{F}_2^\ell$.

Finding a Key in a Haystack: Example 9.2

Take $n = 3$ so $\mathcal{P} = \mathcal{C} = \mathbb{F}_2^3$. The *toy block cipher* has $\mathcal{K} = \mathbb{F}_2^8$. The encryption functions are 256 of the bijections $\mathbb{F}_2^3 \to \mathbb{F}_2^3$, chosen according to a fairly arbitrary rule (details omitted). For example, the red edge in diagram **252** shows that $e_{11111100}(010) = 100$, or in decimal, $e_{\mathbf{252}}(2) = 4$



All 256 bijections are posted on Moodle, or use this direct link `http://www.ma.rhul.ac.uk/~uvah099/Ciphers/RandomCipherPAllP.pdf`.

Example 9.2 [continued]

Suppose Alice and Bob used the toy block cipher with their shared secret key k.

(i) By a chosen plaintext attack Mark learns that $e_k(000) = 011$ and $e_k(100) = 000$. One possible key is **254**, or 11111110 in binary. There are twelve others: find at least one of them.

(ii) By choosing two further plaintexts Mark learns that $e_k(001) = 101$ and $e_k(110) = 111$. Determine k.

(A) 6 (B) 122 (C) 170 (D) 254

(iii) Later Mark's boss Eve observes the ciphertext 100. What is $d_k(100)$?

(A) 1 (B) 3 (C) 5 (D) 7

In this case since $|\mathbb{F}_2^3| = 8$, there are $8! = 40320$ bijections of $\mathbb{F}_2^3$, of which 256 were used.

Example 9.2 [continued]

Suppose Alice and Bob used the toy block cipher with their shared secret key k.

(i) By a chosen plaintext attack Mark learns that $e_k(000) = 011$ and $e_k(100) = 000$. One possible key is **254**, or 11111110 in binary. There are twelve others: find at least one of them.

(ii) By choosing two further plaintexts Mark learns that $e_k(001) = 101$ and $e_k(110) = 111$. Determine k.

(A) 6 (B) 122 (C) 170 (D) 254

(iii) Later Mark's boss Eve observes the ciphertext 100. What is $d_k(100)$?

(A) 1 (B) 3 (C) 5 (D) 7

In this case since $|\mathbb{F}_2^3| = 8$, there are $8! = 40320$ bijections of $\mathbb{F}_2^3$, of which 256 were used.

Example 9.2 [continued]

Suppose Alice and Bob used the toy block cipher with their shared secret key k.

(i) By a chosen plaintext attack Mark learns that $e_k(000) = 011$ and $e_k(100) = 000$. One possible key is **254**, or 11111110 in binary. There are twelve others: find at least one of them.

(ii) By choosing two further plaintexts Mark learns that $e_k(001) = 101$ and $e_k(110) = 111$. Determine k.

(A) 6 (B) 122 (C) 170 (D) 254

(iii) Later Mark's boss Eve observes the ciphertext 100. What is $d_k(100)$?

(A) 1 (B) 3 (C) 5 (D) 7

In this case since $|\mathbb{F}_2^3| = 8$, there are $8! = 40320$ bijections of $\mathbb{F}_2^3$, of which 256 were used.

Feistel Networks

Definition 9.3

Let $m \in \mathbb{N}$ and let $f : \mathbb{F}_2^m \to \mathbb{F}_2^m$ be a function. Given v, $w \in \mathbb{F}_2^m$, let (v, w) denote $(v_0, \ldots, v_{m-1}, w_0, \ldots, w_{m-1}) \in \mathbb{F}_2^{2m}$. The *Feistel function* for f is the function $F : \mathbb{F}_2^{2m} \to \mathbb{F}_2^{2m}$ defined by

$$F\big((v, w)\big) = (w, v + f(w)).$$

This can be compared with an LFSR: we shift left by m bits to move w to the first position. The feedback function is $(v, w) \mapsto v + f(w)$. It is linear in v, like an LFSR, but typically non-linear in w.

Exercise 9.4

Show that, for any function $f : \mathbb{F}_2^m \to \mathbb{F}_2^m$, the Feistel function F for f is invertible. Give a formula for its inverse in terms of f.

Example 9.5 (Q-Block Cipher)

Take $m = 4$ and let

$$S\big((x_0, x_1, x_2, x_3)\big) = (x_2, x_3, x_0 + x_1x_2, x_1 + x_2x_3).$$

We define a block cipher with block size 8 and key length 12 composed of three Feistel functions. If the key is $k \in \mathbb{F}_2^{16}$ then

$$k^{(1)} = (k_0, k_1, k_2, k_3), k^{(2)} = (k_4, k_5, k_6, k_7), k^{(3)} = (k_8, k_9, k_{10}, k_{11}).$$

The Feistel function in round i is $x \mapsto S(x + k^{(i)})$. Since in each round the contents of the right register shift to the left, we can consistently denote the output of round i by $(v^{(i)}, v^{(i+1)})$. Thus the plaintext $(v, w) \in \mathbb{F}_2^{16}$ is encrypted to the cipher text $e_k\big((v, w)\big) = (v^{(3)}, v^{(4)})$ in three rounds:

$$\begin{aligned}(v, w) = (v^{(0)}, v^{(1)}) &\mapsto \big(v^{(1)}, v^{(0)} + S(v^{(1)} + k^{(1)})\big) = (v^{(1)}, v^{(2)}) \\ &\mapsto \big(v^{(2)}, v^{(1)} + S(v^{(2)} + k^{(2)})\big) = (v^{(2)}, v^{(3)}) \\ &\mapsto \big(v^{(3)}, v^{(2)} + S(v^{(3)} + k^{(3)})\big) = (v^{(3)}, v^{(4)}).\end{aligned}$$

Q-Block Cipher: Recall $(v, w) \mapsto \big(w, v + S(w + k_{\text{round}})\big)$

Exercise 9.6

(a) Suppose that $k = 0001\,0011\,0111$, shown split into the three round keys. Show that $e_k(0000\,0000) = 1110\,0010$ and $(v^{(1)}, v^{(2)}) = (0000\,0100)$. Find $(v^{(2)}, v^{(3)})$.

(A) $(0100\,1110)$ (B) $(1110\,0100)$

(C) $(0100\,1010)$ (D) $(1010\,0100)$

(A) (B) (C) (D)

(b) Let $k' = 0001\,0011\,0000$. When $(1110, 0010)$ is *decrypted*, what is $(v^{(2)}, v^{(3)})$?

(A) $(1011\,1110)$ (B) $(1001\,1110)$

(C) $(0100\,1110)$ (D) $(1110\,1011)$

(A) (B) (C) (D)

(c) Suppose Eve observes the ciphertext $(v^{(3)}, v^{(4)})$ from the Q-block cipher with key k. What does she need to know to learn $v^{(2)}$?

(A) k (B) $k_0 k_1 k_2 k_3$ (C) $k_4 k_5 k_6 k_7$ (D) $k_8 k_9 k_{10} k_{11}$

Q-Block Cipher: Recall $(v, w) \mapsto \big(w, v + S(w + k_{\text{round}})\big)$

Exercise 9.6

(a) Suppose that $k = 0001\,0011\,0111$, shown split into the three round keys. Show that $e_k(0000\,0000) = 1110\,0010$ and $(v^{(1)}, v^{(2)}) = (0000\,0100)$. Find $(v^{(2)}, v^{(3)})$.

(A) $(0100\,1110)$ (B) $(1110\,0100)$

(C) $(0100\,1010)$ (D) $(1010\,0100)$

(A) (B) (C) (D)

(b) Let $k' = 0001\,0011\,0000$. When $(1110, 0010)$ is *decrypted*, what is $(v^{(2)}, v^{(3)})$?

(A) $(1011\,1110)$ (B) $(1001\,1110)$

(C) $(0100\,1110)$ (D) $(1110\,1011)$

(A) (B) (C) (D)

(c) Suppose Eve observes the ciphertext $(v^{(3)}, v^{(4)})$ from the Q-block cipher with key k. What does she need to know to learn $v^{(2)}$?

(A) k (B) $k_0 k_1 k_2 k_3$ (C) $k_4 k_5 k_6 k_7$ (D) $k_8 k_9 k_{10} k_{11}$

Q-Block Cipher: Recall $(v, w) \mapsto \big(w, v + S(w + k_{\text{round}})\big)$

Exercise 9.6

(a) Suppose that $k = 0001\,0011\,0111$, shown split into the three round keys. Show that $e_k(0000\,0000) = 1110\,0010$ and $(v^{(1)}, v^{(2)}) = (0000\,0100)$. Find $(v^{(2)}, v^{(3)})$.

(A) $(0100\,1110)$ (B) $(1110\,0100)$

(C) $(0100\,1010)$ (D) $(1010\,0100)$

(A) (B) (C) (D)

(b) Let $k' = 0001\,0011\,0000$. When $(1110, 0010)$ is *decrypted*, what is $(v^{(2)}, v^{(3)})$?

(A) $(1011\,1110)$ (B) $(1001\,1110)$

(C) $(0100\,1110)$ (D) $(1110\,1011)$

(A) (B) (C) (D)

(c) Suppose Eve observes the ciphertext $(v^{(3)}, v^{(4)})$ from the Q-block cipher with key k. What does she need to know to learn $v^{(2)}$?

(A) k (B) $k_0 k_1 k_2 k_3$ (C) $k_4 k_5 k_6 k_7$ (D) $k_8 k_9 k_{10} k_{11}$

Q-Block Cipher: Recall $(v, w) \mapsto \big(w, v + S(w + k_{\text{round}})\big)$

Exercise 9.6

(a) Suppose that $k = 0001\,0011\,0111$, shown split into the three round keys. Show that $e_k(0000\,0000) = 1110\,0010$ and $(v^{(1)}, v^{(2)}) = (0000\,0100)$. Find $(v^{(2)}, v^{(3)})$.

(A) $(0100\,1110)$ (B) $(1110\,0100)$

(C) $(0100\,1010)$ (D) $(1010\,0100)$

(A) (B) (C) (D)

(b) Let $k' = 0001\,0011\,0000$. When $(1110, 0010)$ is *decrypted*, what is $(v^{(2)}, v^{(3)})$?

(A) $(1011\,1110)$ (B) $(1001\,1110)$

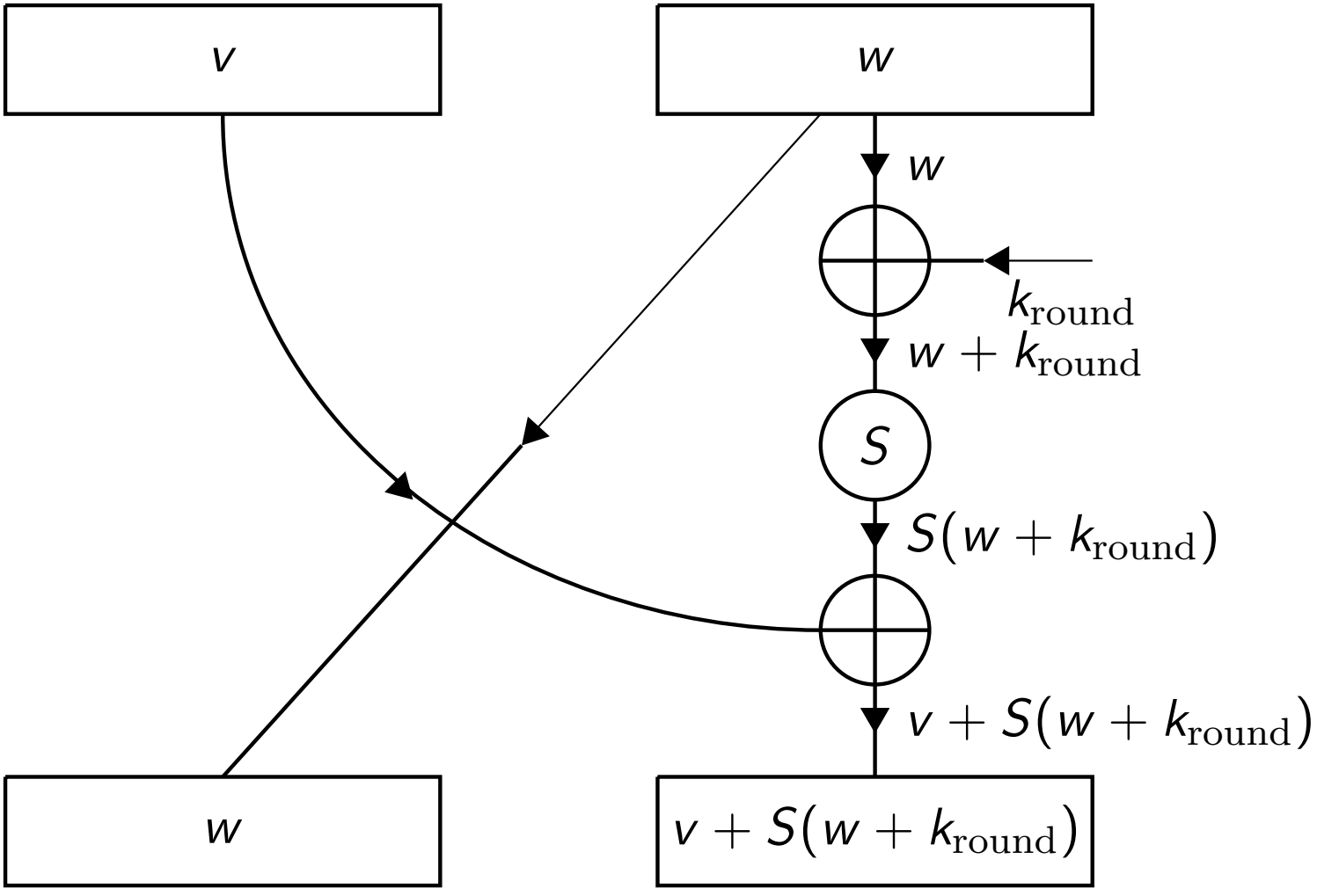
(C) $(0100\,1110)$ (D) $(1110\,1011)$

(A) (B) (C) (D)

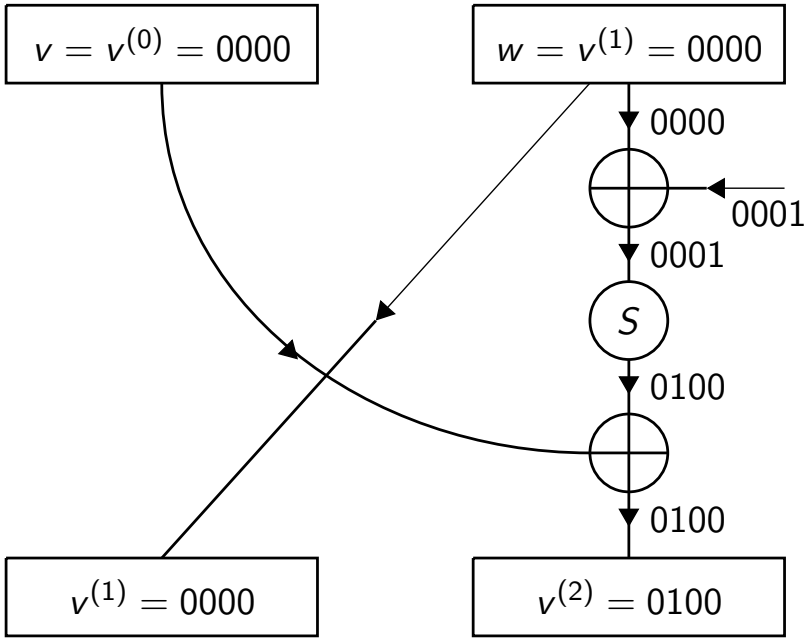
(c) Suppose Eve observes the ciphertext $(v^{(3)}, v^{(4)})$ from the Q-block cipher with key k. What does she need to know to learn $v^{(2)}$?

(A) k (B) $k_0 k_1 k_2 k_3$ (C) $k_4 k_5 k_6 k_7$ (D) $k_8 k_9 k_{10} k_{11}$

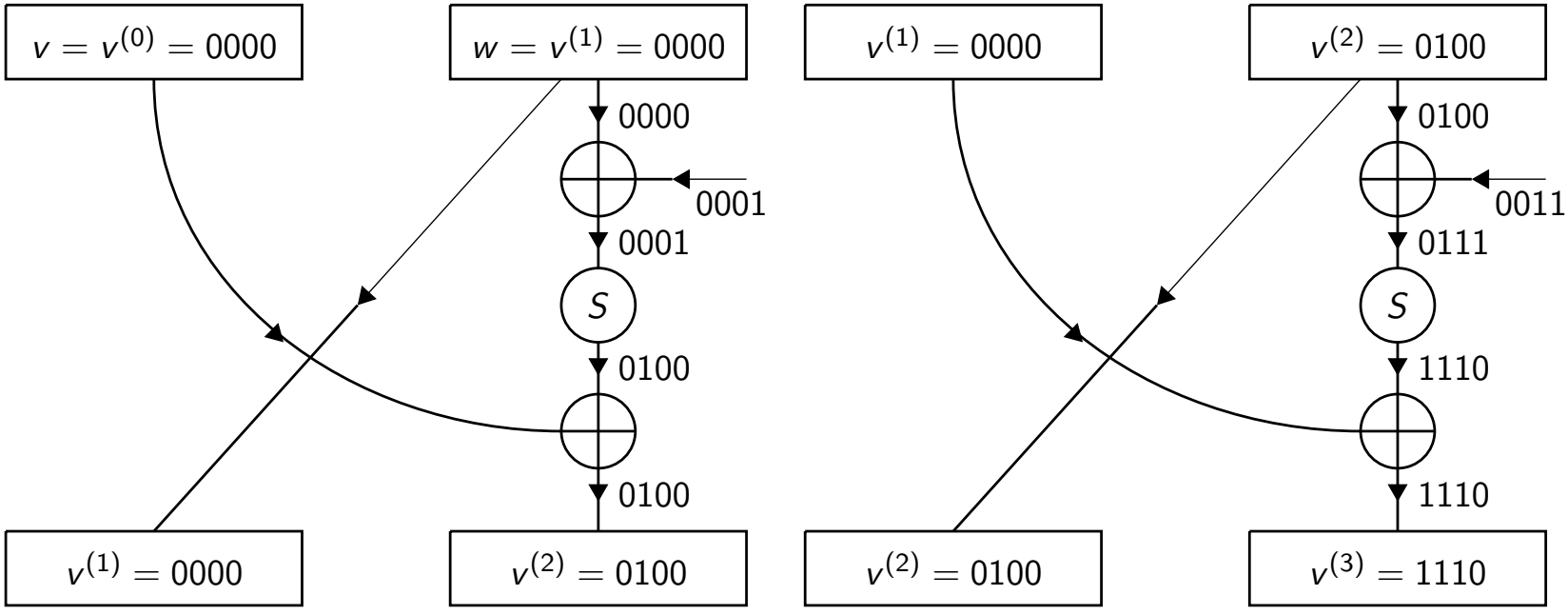
Exercise 9.6(a): $(v, w) \mapsto (w + v + S(w + k_{\text{round}}))$



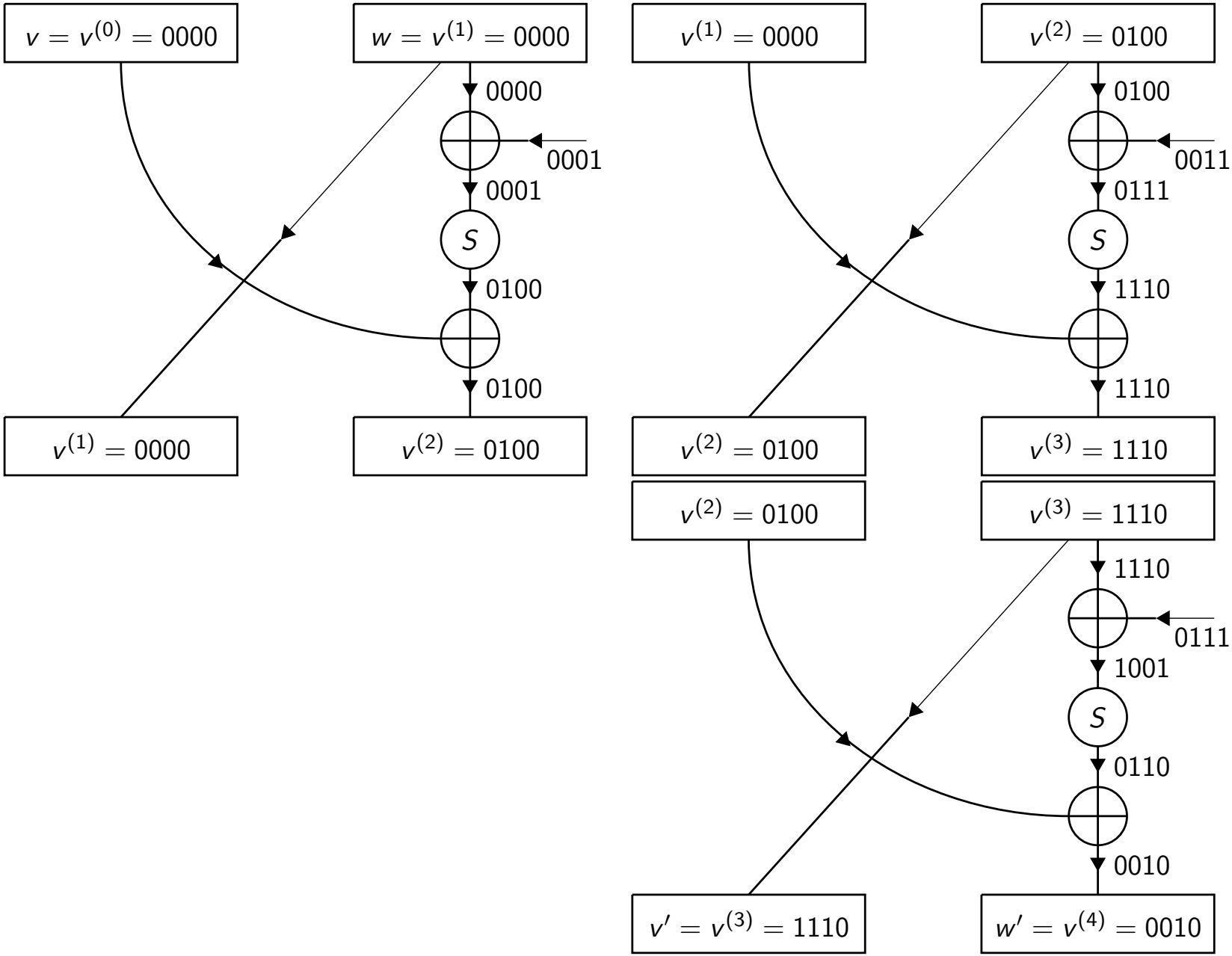
Exercise 9.6(a): $(v, w) \mapsto \big(w + v + S(w + k_{\text{round}})\big)$



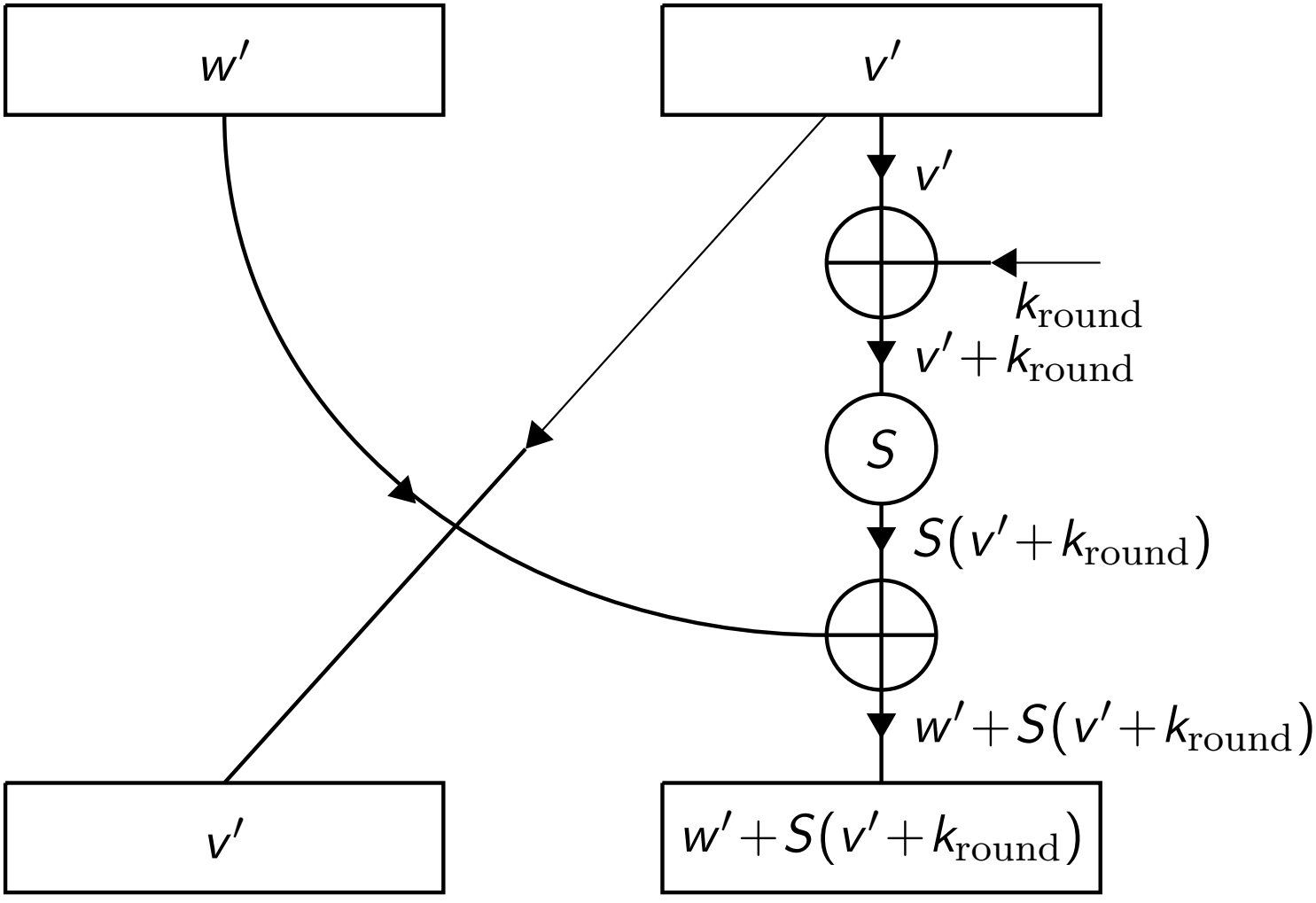
Exercise 9.6(a): $(v, w) \mapsto \big(w + v + S(w + k_{\text{round}})\big)$



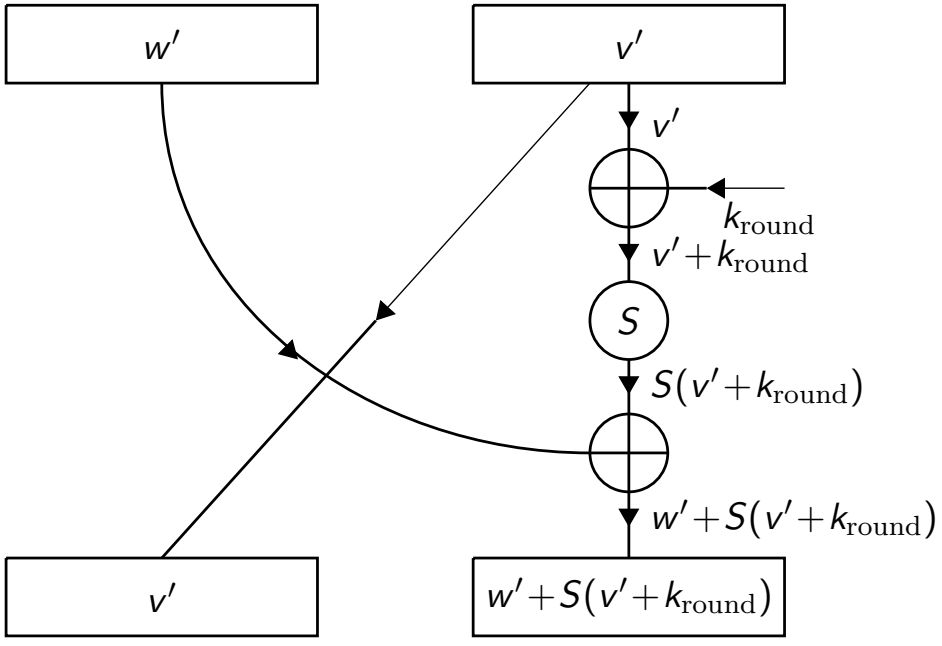
Exercise 9.6(a): $(v, w) \mapsto \big(w + v + S(w + k_{\text{round}})\big)$

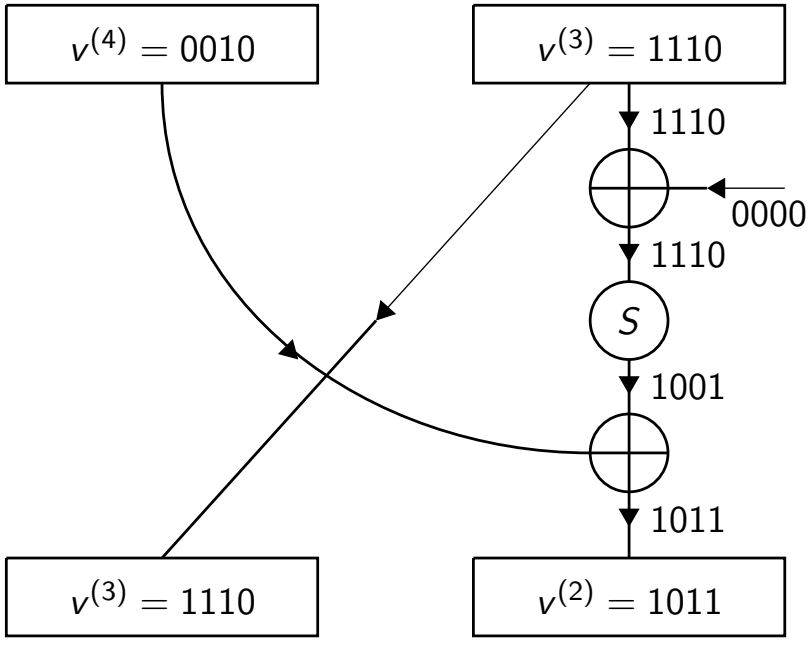


Exercise 9.6(b) flip: $(w', v') \mapsto \big(v', w' + S(v' + k_{\text{round}})\big)$

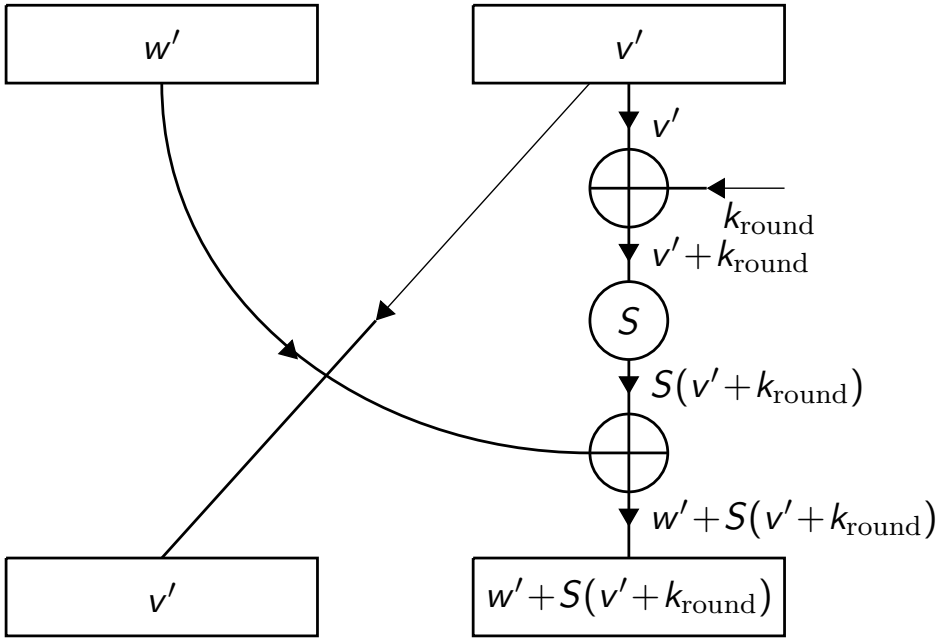


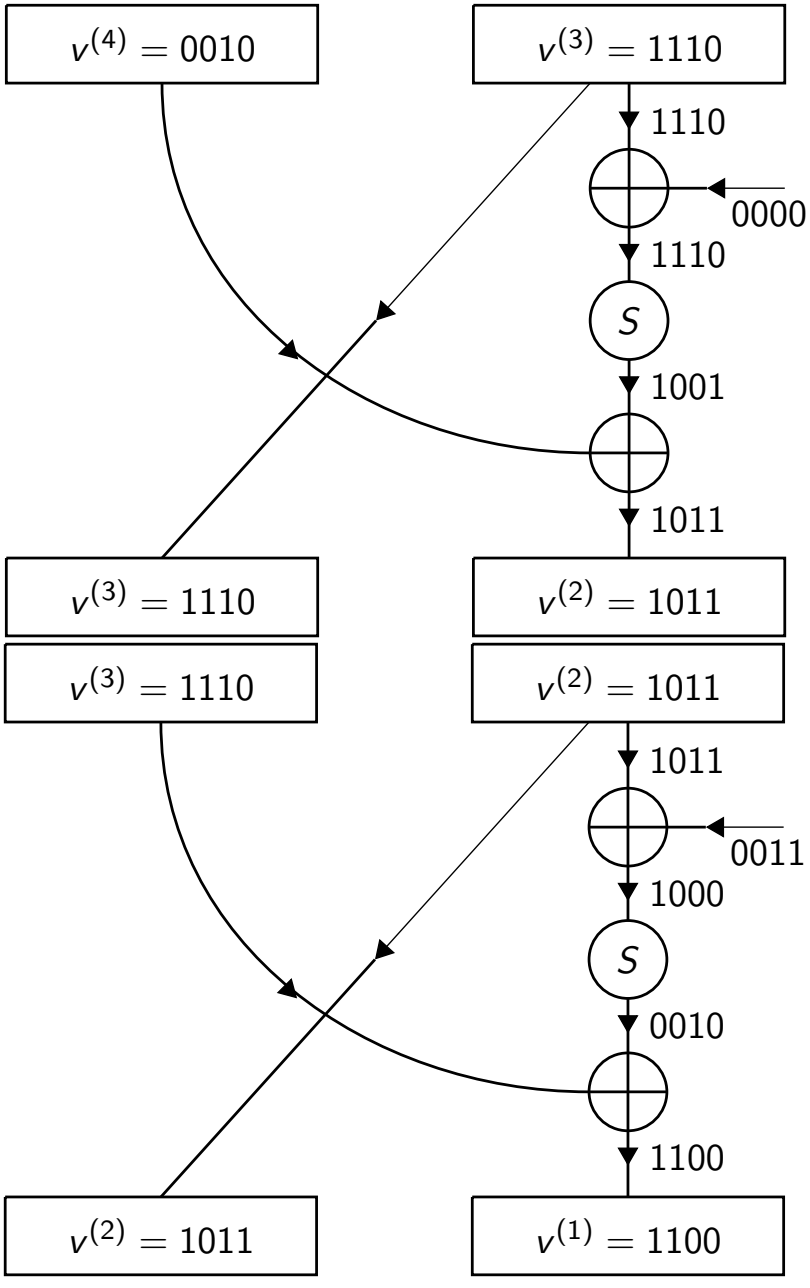
Exercise 9.6(b) flip: $(w', v') \mapsto \big(v', w' + S(v' + k_{\text{round}})\big)$





Exercise 9.6(b) flip: $(w', v') \mapsto \big(v', w' + S(v' + k_{\text{round}})\big)$





DES (Data Encryption Standard 1975)

DES is a Feistel block cipher of block size 64. The key length is 56, so the keyspace is $\mathbb{F}_2^{56}$. Each round key is in $\mathbb{F}_2^{48}$. There are 16 rounds. (Details of how the 16 round keys are derived from the key are omitted.)

Each Feistel Network is defined using a function $\mathbb{F}_2^{32} \to \mathbb{F}_2^{32}$:

(a) Expand $w \in \mathbb{F}_2^{32}$ by a linear function (details omitted) to $w' \in \mathbb{F}_2^{48}$.

(b) Add the 48-bit round key to get $w' + k^{(i)}$.

(c) Let $w' + k^{(i)} = (y^{(1)}, \ldots, y^{(8)})$ where $y^{(i)} \in \mathbb{F}_2^6$. Let $z = \left(S_1(y^{(1)}), \ldots, S_8(y^{(8)})\right) \in \mathbb{F}_2^{32}$. *Confusion*: obscure relationship between plaintext and ciphertext on nearby bits.

(d) Apply a bijection (details omitted) of the positions of z. *Diffusion*: turn short range confusion into long range confusion.

Note that (a) and (d) are linear, and (b) is a conventional key addition in $\mathbb{F}_2^{48}$. So the *S-boxes* $S_i : \mathbb{F}_2^6 \to \mathbb{F}_2^4$ in (c) are the only source of non-linearity.

DES *S*-boxes

שורה	מס' עמודה															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	S_1															
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	3	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	13	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
	S_2															
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
	S_3															
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
	S_4															
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

	S_5															
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
	S_6															
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
	S_7															
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
	S_8															
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

DES attacks

The small keyspace $\mathbb{F}_2^{56}$ makes DES insecure.

- 1997: 140 days, distributed search on internet
- 1998: 9 days 'DES cracker' (special purpose) \$250000
- 2017: 6 days 'COPACOBANA' (35 FPGA's) \$10000

Roughly how many keys does COPACOBANA test in each second?

(A) 2^{32} (B) 2^{36} (C) 2^{37} (D) 2^{40}

Hint: $\log_2(6 \times 24 \times 60 \times 60) \approx 19$.

Exercise 9.7

Suppose we apply DES twice, first with key $k \in \mathbb{F}_2^{56}$ then with $k' \in \mathbb{F}_2^{56}$. So the keyspace is $\mathbb{F}_2^{56} \times \mathbb{F}_2^{56}$ and for $(k, k') \in \mathbb{F}_2^{56} \times \mathbb{F}_2^{56}$,

$$e_{(k,k')}(x) = e'_k\big(e_k(x)\big) \in \mathbb{F}_2^{64}.$$

(a) Roughly how long would a brute force exhaustive search over $\mathbb{F}_2^{56} \times \mathbb{F}_2^{56}$ take? (Assume you own a COPACOBANA.)

(A) 12 days (B) 36 days (C) 10^6 years (D) 10^{15} years

(b) Does this mean 2DES is secure?

(A) False (B) True

DES attacks

The small keyspace $\mathbb{F}_2^{56}$ makes DES insecure.

- 1997: 140 days, distributed search on internet
- 1998: 9 days 'DES cracker' (special purpose) \$250000
- 2017: 6 days 'COPACOBANA' (35 FPGA's) \$10000

Roughly how many keys does COPACOBANA test in each second?

(A) 2^{32} (B) 2^{36} (C) 2^{37} (D) 2^{40}

Hint: $\log_2(6 \times 24 \times 60 \times 60) \approx 19$.

Exercise 9.7

Suppose we apply DES twice, first with key $k \in \mathbb{F}_2^{56}$ then with $k' \in \mathbb{F}_2^{56}$. So the keyspace is $\mathbb{F}_2^{56} \times \mathbb{F}_2^{56}$ and for $(k, k') \in \mathbb{F}_2^{56} \times \mathbb{F}_2^{56}$,

$$e_{(k,k')}(x) = e'_k\big(e_k(x)\big) \in \mathbb{F}_2^{64}.$$

(a) Roughly how long would a brute force exhaustive search over $\mathbb{F}_2^{56} \times \mathbb{F}_2^{56}$ take? (Assume you own a COPACOBANA.)

(A) 12 days (B) 36 days (C) 10^6 years (D) 10^{15} years

(b) Does this mean 2DES is secure?

(A) False (B) True

DES attacks

The small keyspace $\mathbb{F}_2^{56}$ makes DES insecure.

- 1997: 140 days, distributed search on internet
- 1998: 9 days 'DES cracker' (special purpose) \$250000
- 2017: 6 days 'COPACOBANA' (35 FPGA's) \$10000

Roughly how many keys does COPACOBANA test in each second?

(A) 2^{32} (B) 2^{36} (C) 2^{37} (D) 2^{40}

Hint: $\log_2(6 \times 24 \times 60 \times 60) \approx 19$.

Exercise 9.7

Suppose we apply DES twice, first with key $k \in \mathbb{F}_2^{56}$ then with $k' \in \mathbb{F}_2^{56}$. So the keyspace is $\mathbb{F}_2^{56} \times \mathbb{F}_2^{56}$ and for $(k, k') \in \mathbb{F}_2^{56} \times \mathbb{F}_2^{56}$,

$$e_{(k,k')}(x) = e'_k\big(e_k(x)\big) \in \mathbb{F}_2^{64}.$$

(a) Roughly how long would a brute force exhaustive search over $\mathbb{F}_2^{56} \times \mathbb{F}_2^{56}$ take? (Assume you own a COPACOBANA.)

(A) 12 days (B) 36 days (C) 10^6 years (D) 10^{15} years

(b) Does this mean 2DES is secure?

(A) False (B) True

DES attacks

The small keyspace $\mathbb{F}_2^{56}$ makes DES insecure.

- 1997: 140 days, distributed search on internet
- 1998: 9 days 'DES cracker' (special purpose) \$250000
- 2017: 6 days 'COPACOBANA' (35 FPGA's) \$10000

Roughly how many keys does COPACOBANA test in each second?

(A) 2^{32} (B) 2^{36} (C) 2^{37} (D) 2^{40}

Hint: $\log_2(6 \times 24 \times 60 \times 60) \approx 19$.

Exercise 9.7

Suppose we apply DES twice, first with key $k \in \mathbb{F}_2^{56}$ then with $k' \in \mathbb{F}_2^{56}$. So the keyspace is $\mathbb{F}_2^{56} \times \mathbb{F}_2^{56}$ and for $(k, k') \in \mathbb{F}_2^{56} \times \mathbb{F}_2^{56}$,

$$e_{(k,k')}(x) = e'_k\big(e_k(x)\big) \in \mathbb{F}_2^{64}.$$

(a) Roughly how long would a brute force exhaustive search over $\mathbb{F}_2^{56} \times \mathbb{F}_2^{56}$ take? (Assume you own a COPACOBANA.)

(A) 12 days (B) 36 days (C) 10^6 years (D) 10^{15} years

(b) Does this mean 2DES is secure?

(A) False (B) True

DES attacks

The small keyspace $\mathbb{F}_2^{56}$ makes DES insecure.

- 1997: 140 days, distributed search on internet
- 1998: 9 days 'DES cracker' (special purpose) \$250000
- 2017: 6 days 'COPACOBANA' (35 FPGA's) \$10000

Roughly how many keys does COPACOBANA test in each second?

(A) 2^{32} (B) 2^{36} (C) 2^{37} (D) 2^{40}

Hint: $\log_2(6 \times 24 \times 60 \times 60) \approx 19$.

Exercise 9.7

Suppose we apply DES twice, first with key $k \in \mathbb{F}_2^{56}$ then with $k' \in \mathbb{F}_2^{56}$. So the keyspace is $\mathbb{F}_2^{56} \times \mathbb{F}_2^{56}$ and for $(k, k') \in \mathbb{F}_2^{56} \times \mathbb{F}_2^{56}$,

$$e_{(k,k')}(x) = e'_k\big(e_k(x)\big) \in \mathbb{F}_2^{64}.$$

(a) Roughly how long would a brute force exhaustive search over $\mathbb{F}_2^{56} \times \mathbb{F}_2^{56}$ take? (Assume you own a COPACOBANA.)

(A) 12 days (B) 36 days (C) 10^6 years (D) 10^{15} years

(b) Does this mean 2DES is secure?

(A) False (B) True

Meet-in-the-Middle Attack on 2DES

In a chosen plaintext attack on 2DES we **choose** a plaintext $x \in \mathbb{F}_2^{64}$ and get its encryption $z = e_{k'}\big(e_k(x)\big) \in \mathbb{F}_2^{64}$, by an unknown 2DES key

$$(k, k') \in \mathbb{F}_2^{56} \times \mathbb{F}_2^{56}.$$

Meet-in-the-Middle Attack on 2DES

In a chosen plaintext attack on 2DES we **choose** a plaintext $x \in \mathbb{F}_2^{64}$ and get its encryption $z = e_{k'}\big(e_k(x)\big) \in \mathbb{F}_2^{64}$, by an unknown 2DES key

$$(k, k') \in \mathbb{F}_2^{56} \times \mathbb{F}_2^{56}.$$

We define

$$E = \{\big(k_\star, e_{k_\star}(x)\big) : k_\star \in \mathbb{F}_2^{56}\}$$
$$D = \{\big(k'_\star, d_{k'_\star}(z)\big) : k'_\star \in \mathbb{F}_2^{56}\}.$$

Using the sets E and D, the attacker computes for each $y \in \mathbb{F}_2^{64}$

$$\mathcal{K}_y = \big\{(k_\star, k'_\star) : k_\star \in \mathbb{F}_2^{56}, k'_\star \in \mathbb{F}_2^{56}, e_{k_\star}(x) = y = d_{k'_\star}(z)\big\}.$$

- The correct key (k, k') is in one of the sets $\mathcal{K}_y$. Which y?
  (A) $e_{(k,k')}(x)$ (B) $e_k(x)$ (C) z (D) $e_k(z)$
- What is another way to write y?
  (A) $d_{(k,k')}(z)$ (B) $d_{k'}(z)$ (C) x (D) $d_{k'}(x)$
- There may be many non-empty sets $\mathcal{K}_y$. Can the attacker know just from E and D which set $\mathcal{K}_y$ contains (k, k')?
  (A) No (B) Yes

Meet-in-the-Middle Attack on 2DES

In a chosen plaintext attack on 2DES we **choose** a plaintext $x \in \mathbb{F}_2^{64}$ and get its encryption $z = e_{k'}\big(e_k(x)\big) \in \mathbb{F}_2^{64}$, by an unknown 2DES key

$$(k, k') \in \mathbb{F}_2^{56} \times \mathbb{F}_2^{56}.$$

We define

$$E = \{\big(k_\star, e_{k_\star}(x)\big) : k_\star \in \mathbb{F}_2^{56}\}$$
$$D = \{\big(k'_\star, d_{k'_\star}(z)\big) : k'_\star \in \mathbb{F}_2^{56}\}.$$

Using the sets E and D, the attacker computes for each $y \in \mathbb{F}_2^{64}$

$$\mathcal{K}_y = \big\{(k_\star, k'_\star) : k_\star \in \mathbb{F}_2^{56}, k'_\star \in \mathbb{F}_2^{56}, e_{k_\star}(x) = y = d_{k'_\star}(z)\big\}.$$

- The correct key (k, k') is in one of the sets $\mathcal{K}_y$. Which y?
  (A) $e_{(k,k')}(x)$ (B) $e_k(x)$ (C) z (D) $e_k(z)$
- What is another way to write y?
  (A) $d_{(k,k')}(z)$ (B) $d_{k'}(z)$ (C) x (D) $d_{k'}(x)$
- There may be many non-empty sets $\mathcal{K}_y$. Can the attacker know just from E and D which set $\mathcal{K}_y$ contains (k, k')?
  (A) No (B) Yes

Meet-in-the-Middle Attack on 2DES

In a chosen plaintext attack on 2DES we **choose** a plaintext $x \in \mathbb{F}_2^{64}$ and get its encryption $z = e_{k'}\big(e_k(x)\big) \in \mathbb{F}_2^{64}$, by an unknown 2DES key

$$(k, k') \in \mathbb{F}_2^{56} \times \mathbb{F}_2^{56}.$$

We define

$$E = \{\big(k_\star, e_{k_\star}(x)\big) : k_\star \in \mathbb{F}_2^{56}\}$$
$$D = \{\big(k'_\star, d_{k'_\star}(z)\big) : k'_\star \in \mathbb{F}_2^{56}\}.$$

Using the sets E and D, the attacker computes for each $y \in \mathbb{F}_2^{64}$

$$\mathcal{K}_y = \big\{(k_\star, k'_\star) : k_\star \in \mathbb{F}_2^{56}, k'_\star \in \mathbb{F}_2^{56}, e_{k_\star}(x) = y = d_{k'_\star}(z)\big\}.$$

- The correct key (k, k') is in one of the sets $\mathcal{K}_y$. Which y?
  (A) $e_{(k,k')}(x)$ (B) $e_k(x)$ (C) z (D) $e_k(z)$
- What is another way to write y?
  (A) $d_{(k,k')}(z)$ (B) $d_{k'}(z)$ (C) x (D) $d_{k'}(x)$
- There may be many non-empty sets $\mathcal{K}_y$. Can the attacker know just from E and D which set $\mathcal{K}_y$ contains (k, k')?
  (A) No (B) Yes

Meet-in-the-Middle Attack on 2DES

In a chosen plaintext attack on 2DES we **choose** a plaintext $x \in \mathbb{F}_2^{64}$ and get its encryption $z = e_{k'}\big(e_k(x)\big) \in \mathbb{F}_2^{64}$, by an unknown 2DES key

$$(k, k') \in \mathbb{F}_2^{56} \times \mathbb{F}_2^{56}.$$

We define

$$E = \{\big(k_\star, e_{k_\star}(x)\big) : k_\star \in \mathbb{F}_2^{56}\}$$
$$D = \{\big(k'_\star, d_{k'_\star}(z)\big) : k'_\star \in \mathbb{F}_2^{56}\}.$$

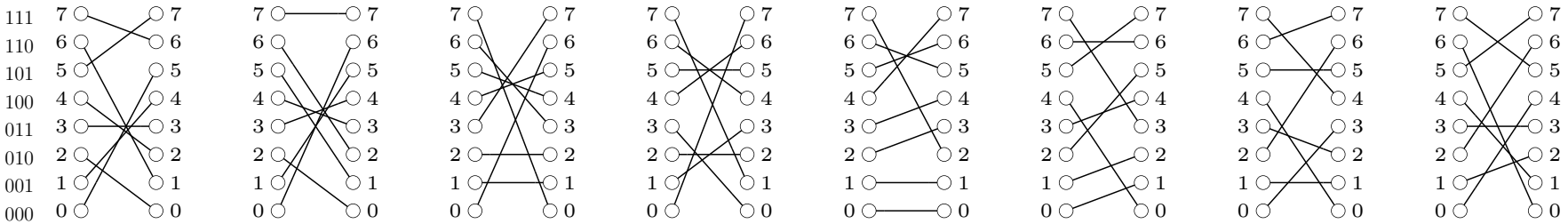
Using the sets E and D, the attacker computes for each $y \in \mathbb{F}_2^{64}$

$$\mathcal{K}_y = \big\{(k_\star, k'_\star) : k_\star \in \mathbb{F}_2^{56}, k'_\star \in \mathbb{F}_2^{56}, e_{k_\star}(x) = y = d_{k'_\star}(z)\big\}.$$

- The correct key (k, k') is in one of the sets $\mathcal{K}_y$. Which y?
  (A) $e_{(k,k')}(x)$ (B) $e_k(x)$ (C) z (D) $e_k(z)$
- What is another way to write y?
  (A) $d_{(k,k')}(z)$ (B) $d_{k'}(z)$ (C) x (D) $d_{k'}(x)$
- There may be many non-empty sets $\mathcal{K}_y$. Can the attacker know just from E and D which set $\mathcal{K}_y$ contains (k, k')?
  (A) No (B) Yes

Same Idea in Group Work Week 9

In the Group Work in Week 9, we saw the cut-down version using 8 keys from the Toy Block Cipher.



The secret key was $(6, 7)$ and we choose $x = 011$, so $z = e_{(6,7)}(011) = e_7\big(e_6(011)\big) = 110$. In this setup the sets $\mathcal{K}_y$ are

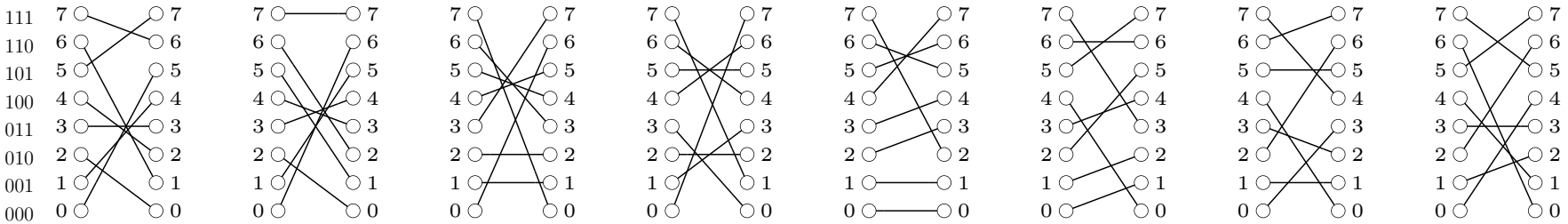
$$\mathcal{K}_y = \left\{(k_\star, k'_\star) : \begin{matrix} k_\star \in \{0,1,\ldots,7\}, k'_\star \in \{0,1,\ldots,7\} \\ e_{k_\star}(x) = y = d_{k'_\star}(z) \end{matrix} \right\}.$$

If you already understand why the correct key is in the set $\mathcal{K}_y$ where $y = e_6(011) = d_7(110)$ you can skip this quiz.

- What is $e_6(011)$?
  (A) 0 (B) 1 (C) 2 (D) 3
- What is $d_7(110)$?
  (A) 0 (B) 1 (C) 2 (D) 3
- Which set $\mathcal{K}_y$ contains the key?
  (A) 0 (B) 1 (C) 2 (D) 3

Same Idea in Group Work Week 9

In the Group Work in Week 9, we saw the cut-down version using 8 keys from the Toy Block Cipher.



The secret key was $(6, 7)$ and we choose $x = 011$, so $z = e_{(6,7)}(011) = e_7\big(e_6(011)\big) = 110$. In this setup the sets $\mathcal{K}_y$ are

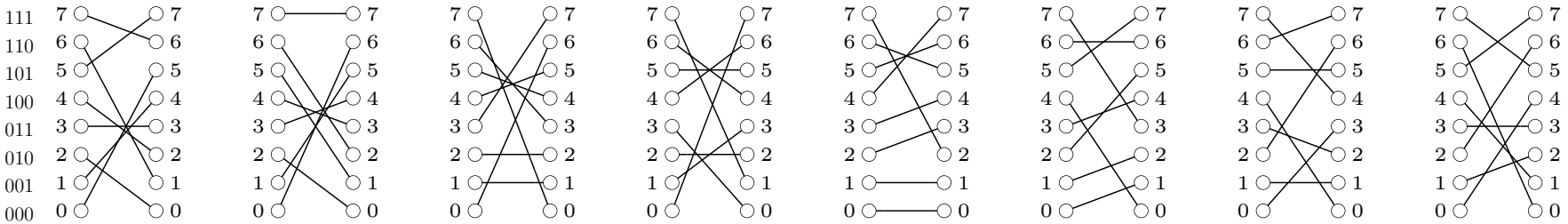
$$\mathcal{K}_y = \left\{(k_\star, k'_\star) : \begin{matrix} k_\star \in \{0,1,\ldots,7\}, k'_\star \in \{0,1,\ldots,7\} \\ e_{k_\star}(x) = y = d_{k'_\star}(z) \end{matrix} \right\}.$$

If you already understand why the correct key is in the set $\mathcal{K}_y$ where $y = e_6(011) = d_7(110)$ you can skip this quiz.

- What is $e_6(011)$?
  (A) 0 (B) 1 (C) 2 (D) 3
- What is $d_7(110)$?
  (A) 0 (B) 1 (C) 2 (D) 3
- Which set $\mathcal{K}_y$ contains the key?
  (A) 0 (B) 1 (C) 2 (D) 3

Same Idea in Group Work Week 9

In the Group Work in Week 9, we saw the cut-down version using 8 keys from the Toy Block Cipher.



The secret key was $(6, 7)$ and we choose $x = 011$, so $z = e_{(6,7)}(011) = e_7\big(e_6(011)\big) = 110$. In this setup the sets $\mathcal{K}_y$ are

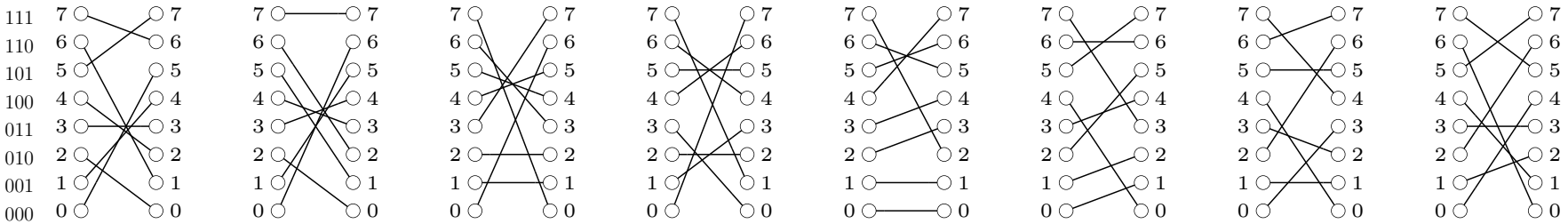
$$\mathcal{K}_y = \left\{ (k_\star, k'_\star) : \begin{matrix} k_\star \in \{0,1,\ldots,7\}, k'_\star \in \{0,1,\ldots,7\} \\ e_{k_\star}(x) = y = d_{k'_\star}(z) \end{matrix} \right\}.$$

If you already understand why the correct key is in the set $\mathcal{K}_y$ where $y = e_6(011) = d_7(110)$ you can skip this quiz.

- What is $e_6(011)$?
  (A) 0 (B) 1 (C) 2 (D) 3
- What is $d_7(110)$?
  (A) 0 (B) 1 (C) 2 (D) 3
- Which set $\mathcal{K}_y$ contains the key?
  (A) 0 (B) 1 (C) 2 (D) 3

Same Idea in Group Work Week 9

In the Group Work in Week 9, we saw the cut-down version using 8 keys from the Toy Block Cipher.



The secret key was $(6, 7)$ and we choose $x = 011$, so $z = e_{(6,7)}(011) = e_7\big(e_6(011)\big) = 110$. In this setup the sets $\mathcal{K}_y$ are

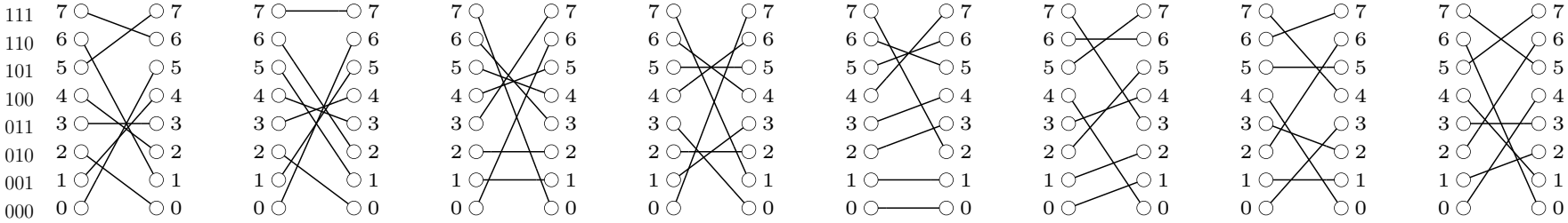
$$\mathcal{K}_y = \left\{ (k_\star, k'_\star) : \begin{matrix} k_\star \in \{0,1,\ldots,7\}, k'_\star \in \{0,1,\ldots,7\} \\ e_{k_\star}(x) = y = d_{k'_\star}(z) \end{matrix} \right\}.$$

If you already understand why the correct key is in the set $\mathcal{K}_y$ where $y = e_6(011) = d_7(110)$ you can skip this quiz.

- What is $e_6(011)$?
  (A) 0 (B) 1 (C) 2 (D) 3
- What is $d_7(110)$?
  (A) 0 (B) 1 (C) 2 (D) 3
- Which set $\mathcal{K}_y$ contains the key?
  (A) 0 (B) 1 (C) 2 (D) 3

Same Idea in Group Work Week 9

In the Group Work in Week 9, we saw the cut-down version using 8 keys from the Toy Block Cipher.



The secret key was $(6, 7)$ and we choose $x = 011$, so $z = e_{(6,7)}(011) = e_7\big(e_6(011)\big) = 110$. In this setup the sets $\mathcal{K}_y$ are

$$\mathcal{K}_y = \left\{(k_\star, k'_\star) : \begin{matrix} k_\star \in \{0,1,\ldots,7\}, k'_\star \in \{0,1,\ldots,7\} \\ e_{k_\star}(x) = y = d_{k'_\star}(z) \end{matrix} \right\}.$$

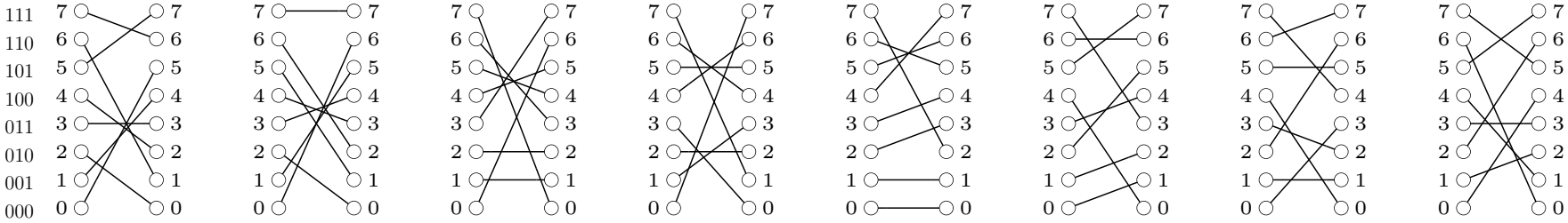
- What is the set $\mathcal{K}_2$?

  (A) $\{(6,7)\}$ (B) $\{(6,6)\}$ (C) $\{(6,6),(6,7)\}$ (D) $\{(6,6),(6,7),(0,6)\}$
- What is the set $\mathcal{K}_0$?

  (A) $\{(3,1)\}$ (B) $\{(3,2)\}$ (C) $\{(3,1),(3,2)\}$ (D) $\{(3,1),(3,2),(0,2))\}$

Same Idea in Group Work Week 9

In the Group Work in Week 9, we saw the cut-down version using 8 keys from the Toy Block Cipher.



The secret key was $(6, 7)$ and we choose $x = 011$, so $z = e_{(6,7)}(011) = e_7\big(e_6(011)\big) = 110$. In this setup the sets $\mathcal{K}_y$ are

$$\mathcal{K}_y = \left\{(k_\star, k'_\star) : \begin{matrix} k_\star \in \{0,1,\ldots,7\}, k'_\star \in \{0,1,\ldots,7\} \\ e_{k_\star}(x) = y = d_{k'_\star}(z) \end{matrix} \right\}.$$

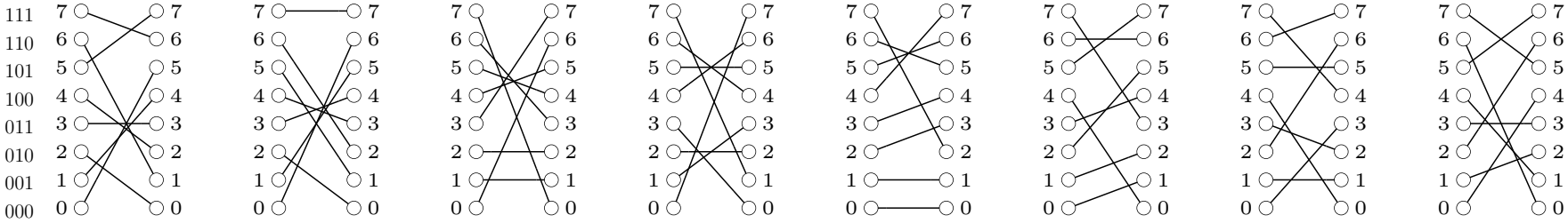
- What is the set $\mathcal{K}_2$?

  (A) $\{(6,7)\}$ (B) $\{(6,6)\}$ (C) $\{(6,6),(6,7)\}$ (D) $\{(6,6),(6,7),(0,6)\}$
- What is the set $\mathcal{K}_0$?

  (A) $\{(3,1)\}$ (B) $\{(3,2)\}$ (C) $\{(3,1),(3,2)\}$ (D) $\{(3,1),(3,2),(0,2)\}$

Same Idea in Group Work Week 9

In the Group Work in Week 9, we saw the cut-down version using 8 keys from the Toy Block Cipher.



The secret key was $(6, 7)$ and we choose $x = 011$, so $z = e_{(6,7)}(011) = e_7\big(e_6(011)\big) = 110$. In this setup the sets $\mathcal{K}_y$ are

$$\mathcal{K}_y = \left\{(k_\star, k'_\star) : \begin{matrix} k_\star \in \{0,1,\ldots,7\}, k'_\star \in \{0,1,\ldots,7\} \\ e_{k_\star}(x) = y = d_{k'_\star}(z) \end{matrix} \right\}.$$

- What is the set $\mathcal{K}_2$?

  (A) $\{(6,7)\}$ (B) $\{(6,6)\}$ (C) $\{(6,6),(6,7)\}$ (D) $\{(6,6),(6,7),(0,6)\}$
- What is the set $\mathcal{K}_0$?

  (A) $\{(3,1)\}$ (B) $\{(3,2)\}$ (C) $\{(3,1),(3,2)\}$ (D) $\{(3,1),(3,2),(0,2)\}$

Meet-in-the-Middle Attack on 2DES

In a chosen plaintext attack on 2DES we **choose** a plaintext $x \in \mathbb{F}_2^{64}$ and get its encryption $z = e_{k'}\left(e_k(x)\right) \in \mathbb{F}_2^{64}$, by an unknown $(k, k') \in \mathbb{F}_2^{56} \times \mathbb{F}_2^{56}$. We defined

$$E = \{\left(k_\star, e_{k_\star}(x)\right) : k_\star \in \mathbb{F}_2^{56}\}$$
$$D = \{\left(k'_\star, d_{k'_\star}(z)\right) : k'_\star \in \mathbb{F}_2^{56}\}.$$

and $\mathcal{K}_y = \left\{(k_\star, k'_\star) : k_\star \in \mathbb{F}_2^{56}, k'_\star \in \mathbb{F}_2^{56}, e_{k_\star}(x) = y = d_{k'_\star}(z)\right\}$ and saw that the key (k, k') is in $\mathcal{K}_y$ where $y = e_k(x) = d_{k'}(z)$.

Model DES as a random cipher, so the encryption function are independent bijections $\mathbb{F}_2^{64} \to \mathbb{F}_2^{64}$. Fix $y_\star \in \mathbb{F}_2^{64}$.

- Given $k_\star \in \mathbb{F}_2^{56}$ what is the probability that $(k_\star, y_\star) \in E$?
  (A) $\frac{1}{2^{128}}$ (B) $\frac{1}{2^{64}}$ (C) $\frac{1}{2^{56}}$ (D) $\frac{1}{2^8}$
- Given $k_\star \in \mathbb{F}_2^{56}$ and $k'_\star \in \mathbb{F}_2^{56}$, what is the probability that $(k_\star, y_\star) \in E$ and $(k'_\star, y_\star) \in D$?
  (A) $\frac{1}{2^{128}}$ (B) $\frac{1}{2^{64}}$ (C) $\frac{1}{2^{56}}$ (D) $\frac{1}{2^8}$
- What is the expected size of the set $\mathcal{K}_{y_\star}$?
  (A) $\frac{1}{2^{16}}$ (B) $\frac{1}{2^8}$ (C) 1 (D) 2^8

Meet-in-the-Middle Attack on 2DES

In a chosen plaintext attack on 2DES we **choose** a plaintext $x \in \mathbb{F}_2^{64}$ and get its encryption $z = e_{k'}\left(e_k(x)\right) \in \mathbb{F}_2^{64}$, by an unknown $(k, k') \in \mathbb{F}_2^{56} \times \mathbb{F}_2^{56}$. We defined

$$E = \{\left(k_\star, e_{k_\star}(x)\right) : k_\star \in \mathbb{F}_2^{56}\}$$
$$D = \{\left(k'_\star, d_{k'_\star}(z)\right) : k'_\star \in \mathbb{F}_2^{56}\}.$$

and $\mathcal{K}_y = \left\{(k_\star, k'_\star) : k_\star \in \mathbb{F}_2^{56}, k'_\star \in \mathbb{F}_2^{56}, e_{k_\star}(x) = y = d_{k'_\star}(z)\right\}$ and saw that the key (k, k') is in $\mathcal{K}_y$ where $y = e_k(x) = d_{k'}(z)$.

Model DES as a random cipher, so the encryption function are independent bijections $\mathbb{F}_2^{64} \to \mathbb{F}_2^{64}$. Fix $y_\star \in \mathbb{F}_2^{64}$.

- Given $k_\star \in \mathbb{F}_2^{56}$ what is the probability that $(k_\star, y_\star) \in E$?
  (A) $\frac{1}{2^{128}}$ (B) $\frac{1}{2^{64}}$ (C) $\frac{1}{2^{56}}$ (D) $\frac{1}{2^8}$
- Given $k_\star \in \mathbb{F}_2^{56}$ and $k'_\star \in \mathbb{F}_2^{56}$, what is the probability that $(k_\star, y_\star) \in E$ and $(k'_\star, y_\star) \in D$?
  (A) $\frac{1}{2^{128}}$ (B) $\frac{1}{2^{64}}$ (C) $\frac{1}{2^{56}}$ (D) $\frac{1}{2^8}$
- What is the expected size of the set $\mathcal{K}_{y_\star}$?
  (A) $\frac{1}{2^{16}}$ (B) $\frac{1}{2^8}$ (C) 1 (D) 2^8

Meet-in-the-Middle Attack on 2DES

In a chosen plaintext attack on 2DES we **choose** a plaintext $x \in \mathbb{F}_2^{64}$ and get its encryption $z = e_{k'}\big(e_k(x)\big) \in \mathbb{F}_2^{64}$, by an unknown $(k, k') \in \mathbb{F}_2^{56} \times \mathbb{F}_2^{56}$. We defined

$$E = \{\big(k_\star, e_{k_\star}(x)\big) : k_\star \in \mathbb{F}_2^{56}\}$$
$$D = \{\big(k'_\star, d_{k'_\star}(z)\big) : k'_\star \in \mathbb{F}_2^{56}\}.$$

and $\mathcal{K}_y = \big\{(k_\star, k'_\star) : k_\star \in \mathbb{F}_2^{56}, k'_\star \in \mathbb{F}_2^{56}, e_{k_\star}(x) = y = d_{k'_\star}(z)\big\}$ and saw that the key (k, k') is in $\mathcal{K}_y$ where $y = e_k(x) = d_{k'}(z)$.

Model DES as a random cipher, so the encryption function are independent bijections $\mathbb{F}_2^{64} \to \mathbb{F}_2^{64}$. Fix $y_\star \in \mathbb{F}_2^{64}$.

- Given $k_\star \in \mathbb{F}_2^{56}$ what is the probability that $(k_\star, y_\star) \in E$?
  (A) $\frac{1}{2^{128}}$ (B) $\frac{1}{2^{64}}$ (C) $\frac{1}{2^{56}}$ (D) $\frac{1}{2^8}$
- Given $k_\star \in \mathbb{F}_2^{56}$ and $k'_\star \in \mathbb{F}_2^{56}$, what is the probability that $(k_\star, y_\star) \in E$ and $(k'_\star, y_\star) \in D$?
  (A) $\frac{1}{2^{128}}$ (B) $\frac{1}{2^{64}}$ (C) $\frac{1}{2^{56}}$ (D) $\frac{1}{2^8}$
- What is the expected size of the set $\mathcal{K}_{y_\star}$?
  (A) $\frac{1}{2^{16}}$ (B) $\frac{1}{2^8}$ (C) 1 (D) 2^8

Meet-in-the-Middle Attack on 2DES

In a chosen plaintext attack on 2DES we **choose** a plaintext $x \in \mathbb{F}_2^{64}$ and get its encryption $z = e_{k'}\big(e_k(x)\big) \in \mathbb{F}_2^{64}$, by an unknown $(k, k') \in \mathbb{F}_2^{56} \times \mathbb{F}_2^{56}$. We defined

$$E = \{\big(k_\star, e_{k_\star}(x)\big) : k_\star \in \mathbb{F}_2^{56}\}$$
$$D = \{\big(k'_\star, d_{k'_\star}(z)\big) : k'_\star \in \mathbb{F}_2^{56}\}.$$

and $\mathcal{K}_y = \big\{(k_\star, k'_\star) : k_\star \in \mathbb{F}_2^{56}, k'_\star \in \mathbb{F}_2^{56}, e_{k_\star}(x) = y = d_{k'_\star}(z)\big\}$ and saw that the key (k, k') is in $\mathcal{K}_y$ where $y = e_k(x) = d_{k'}(z)$.

Model DES as a random cipher, so the encryption function are independent bijections $\mathbb{F}_2^{64} \to \mathbb{F}_2^{64}$. Fix $y_\star \in \mathbb{F}_2^{64}$.

- Given $k_\star \in \mathbb{F}_2^{56}$ what is the probability that $(k_\star, y_\star) \in E$?
  (A) $\frac{1}{2^{128}}$ (B) $\frac{1}{2^{64}}$ (C) $\frac{1}{2^{56}}$ (D) $\frac{1}{2^8}$
- Given $k_\star \in \mathbb{F}_2^{56}$ and $k'_\star \in \mathbb{F}_2^{56}$, what is the probability that $(k_\star, y_\star) \in E$ and $(k'_\star, y_\star) \in D$?
  (A) $\frac{1}{2^{128}}$ (B) $\frac{1}{2^{64}}$ (C) $\frac{1}{2^{56}}$ (D) $\frac{1}{2^8}$
- What is the expected size of the set $\mathcal{K}_{y_\star}$?
  (A) $\frac{1}{2^{16}}$ (B) $\frac{1}{2^8}$ (C) 1 (D) 2^8

Meet-in-the-Middle Attack on 2DES

In a chosen plaintext attack on 2DES we **choose** a plaintext $x \in \mathbb{F}_2^{64}$ and get its encryption $z = e_{k'}\big(e_k(x)\big) \in \mathbb{F}_2^{64}$, by an unknown $(k, k') \in \mathbb{F}_2^{56} \times \mathbb{F}_2^{56}$. We defined

$$E = \{\big(k_\star, e_{k_\star}(x)\big) : k_\star \in \mathbb{F}_2^{56}\}$$
$$D = \{\big(k'_\star, d_{k'_\star}(z)\big) : k'_\star \in \mathbb{F}_2^{56}\}.$$

and $\mathcal{K}_y = \big\{(k_\star, k'_\star) : k_\star \in \mathbb{F}_2^{56}, k'_\star \in \mathbb{F}_2^{56}, e_{k_\star}(x) = y = d_{k'_\star}(z)\big\}$ and saw that the key (k, k') is in $\mathcal{K}_y$ where $y = e_k(x) = d_{k'}(z)$.

Model DES as a random cipher, so the encryption function are independent bijections $\mathbb{F}_2^{64} \to \mathbb{F}_2^{64}$. Fix $y_\star \in \mathbb{F}_2^{64}$.

- What is the expected size of the set $\mathcal{K}_{y_\star}$?
  (A) $\frac{1}{2^{16}}$ (B) $\frac{1}{2^8}$ (C) 1 (D) 2^8
- What is the expected total size of the sets $\mathcal{K}_y$; in other words, what is $\sum_{y_\star \in \mathbb{F}_2^{64}} |\mathcal{K}_{y_\star}|$?
  (A) 2^{48} (B) 2^{56} (C) 2^{64} (D) 2^{72}
- How many DES encryptions / decryptions in total to find key? [*Hint:* check the possible keys by encrypting another plaintext.]
  (A) 2^{57} (B) $2^{57} + 2^{48}$ (C) $2^{57} + 2^{49}$ (D) 2^{112}

Meet-in-the-Middle Attack on 2DES

In a chosen plaintext attack on 2DES we **choose** a plaintext $x \in \mathbb{F}_2^{64}$ and get its encryption $z = e_{k'}\big(e_k(x)\big) \in \mathbb{F}_2^{64}$, by an unknown $(k, k') \in \mathbb{F}_2^{56} \times \mathbb{F}_2^{56}$. We defined

$$E = \{\big(k_\star, e_{k_\star}(x)\big) : k_\star \in \mathbb{F}_2^{56}\}$$
$$D = \{\big(k'_\star, d_{k'_\star}(z)\big) : k'_\star \in \mathbb{F}_2^{56}\}.$$

and $\mathcal{K}_y = \big\{(k_\star, k'_\star) : k_\star \in \mathbb{F}_2^{56}, k'_\star \in \mathbb{F}_2^{56}, e_{k_\star}(x) = y = d_{k'_\star}(z)\big\}$ and saw that the key (k, k') is in $\mathcal{K}_y$ where $y = e_k(x) = d_{k'}(z)$.

Model DES as a random cipher, so the encryption function are independent bijections $\mathbb{F}_2^{64} \to \mathbb{F}_2^{64}$. Fix $y_\star \in \mathbb{F}_2^{64}$.

- What is the expected size of the set $\mathcal{K}_{y_\star}$?
  (A) $\frac{1}{2^{16}}$ (B) $\frac{1}{2^8}$ (C) 1 (D) 2^8
- What is the expected total size of the sets $\mathcal{K}_y$; in other words, what is $\sum_{y_\star \in \mathbb{F}_2^{64}} |\mathcal{K}_{y_\star}|$?
  (A) 2^{48} (B) 2^{56} (C) 2^{64} (D) 2^{72}
- How many DES encryptions / decryptions in total to find key? [*Hint:* check the possible keys by encrypting another plaintext.]
  (A) 2^{57} (B) $2^{57} + 2^{48}$ (C) $2^{57} + 2^{49}$ (D) 2^{112}

Meet-in-the-Middle Attack on 2DES

In a chosen plaintext attack on 2DES we **choose** a plaintext $x \in \mathbb{F}_2^{64}$ and get its encryption $z = e_{k'}\big(e_k(x)\big) \in \mathbb{F}_2^{64}$, by an unknown $(k, k') \in \mathbb{F}_2^{56} \times \mathbb{F}_2^{56}$. We defined

$$E = \{\big(k_\star, e_{k_\star}(x)\big) : k_\star \in \mathbb{F}_2^{56}\}$$
$$D = \{\big(k'_\star, d_{k'_\star}(z)\big) : k'_\star \in \mathbb{F}_2^{56}\}.$$

and $\mathcal{K}_y = \big\{(k_\star, k'_\star) : k_\star \in \mathbb{F}_2^{56}, k'_\star \in \mathbb{F}_2^{56}, e_{k_\star}(x) = y = d_{k'_\star}(z)\big\}$ and saw that the key (k, k') is in $\mathcal{K}_y$ where $y = e_k(x) = d_{k'}(z)$.

Model DES as a random cipher, so the encryption function are independent bijections $\mathbb{F}_2^{64} \to \mathbb{F}_2^{64}$. Fix $y_\star \in \mathbb{F}_2^{64}$.

- What is the expected size of the set $\mathcal{K}_{y_\star}$?
  (A) $\frac{1}{2^{16}}$ (B) $\frac{1}{2^8}$ (C) 1 (D) 2^8
- What is the expected total size of the sets $\mathcal{K}_y$; in other words, what is $\sum_{y_\star \in \mathbb{F}_2^{64}} |\mathcal{K}_{y_\star}|$?
  (A) 2^{48} (B) 2^{56} (C) 2^{64} (D) 2^{72}
- How many DES encryptions / decryptions in total to find key? [*Hint:* check the possible keys by encrypting another plaintext.]
  (A) 2^{57} (B) $2^{57} + 2^{48}$ (C) $2^{57} + 2^{49}$ (D) 2^{112}

Modes of Operation

A block cipher with block size n encrypts plaintexts $x \in \mathbb{F}_2^n$. If x is longer it has to be split into blocks $x^{(1)}, \ldots, x^{(m)} \in \mathbb{F}_2^n$:

$$x = (x^{(1)}, \ldots, x^{(m)}).$$

Fix a key $k \in \mathcal{K}$: this is only key used.

- Electronic Codebook Mode:

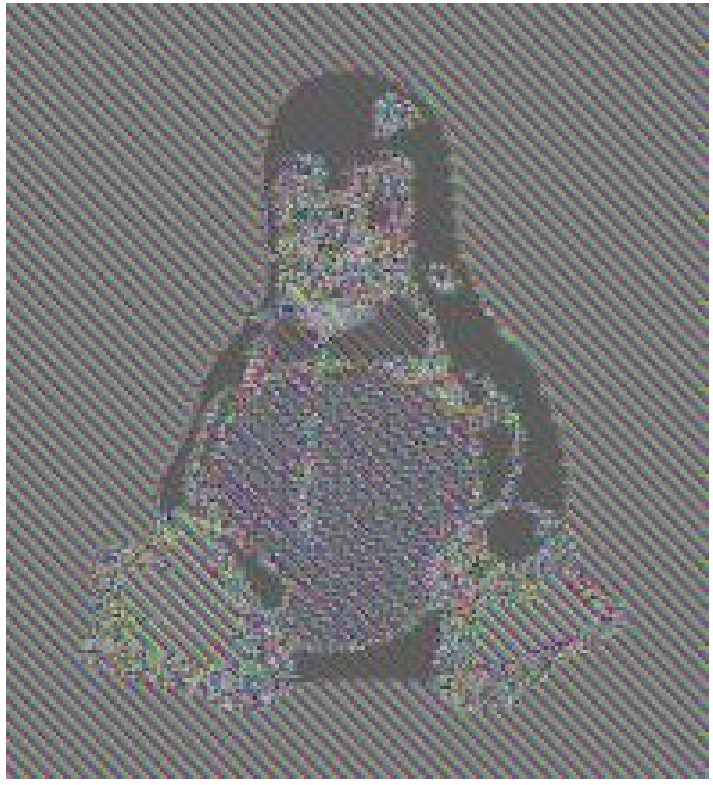
$$\begin{aligned} x^{(1)} &\mapsto e_k(x^{(1)}) \\ x^{(2)} &\mapsto e_k(x^{(2)}) \\ &\vdots \\ x^{(m)} &\mapsto e_k(x^{(m)}) \end{aligned}$$

- Cipher Block Chaining:

$$\begin{aligned} x^{(1)} &\mapsto e_k(x^{(1)}) = y^{(1)} \\ x^{(2)} &\mapsto e_k(y^{(1)} + x^{(2)}) = y^{(2)} \\ &\vdots \\ x^{(m)} &\mapsto e_k(y^{(m-1)} + x^{(m)}) = y^{(m)} \end{aligned}$$

Same In Implies Same Out

If $x^{(i)} = x^{(j)}$ then, in Electronic Codebook Mode, the ciphertext blocks $e_k(x^{(i)}$ and $e_k(x^{(j)})$ are equal. This is a weakness of the mode of operation, not of the underlying block cipher.



Cipher Block Chaining (and the many other modes of operation you are not expected to know about) avoid this problem.

Grace Murray Hopper, Cryptanalyst and US Navy Officer

§10 Differential Cryptanalysis and AES

Differential cryptanalysis was known to the designers of DES in 1974 and was considered when designing the DES S-boxes. They kept it secret, at the request of the NSA. It was rediscovered in the late 1980s.

One important idea is seen in the attack on the reused one-time pad in Question 4 on Problem Sheet 3. We have unknown plaintexts x, $x' \in \mathbb{F}_2^n$, an unknown key $k \in \mathbb{F}_2^n$, and known ciphertexts $x + k$ and $x' + k$. Adding the known ciphertexts gives $x + x'$, independent of k.

§10 Differential Cryptanalysis and AES

Differential cryptanalysis was known to the designers of DES in 1974 and was considered when designing the DES S-boxes. They kept it secret, at the request of the NSA. It was rediscovered in the late 1980s.

One important idea is seen in the attack on the reused one-time pad in Question 4 on Problem Sheet 3. We have unknown plaintexts x, $x' \in \mathbb{F}_2^n$, an unknown key $k \in \mathbb{F}_2^n$, and known ciphertexts $x + k$ and $x' + k$. Adding the known ciphertexts gives $x + x'$, independent of k.

Thus if x and x' differ by Δ then so do their encryptions $x + k$ and $x' + k$. In symbols:

$$x + x' = \Delta \implies (x + k) + (x' + k) = \Delta.$$

This shows the one-time-pad is weak to differences.

§10 Differential Cryptanalysis and AES

Differential cryptanalysis was known to the designers of DES in 1974 and was considered when designing the DES S-boxes. They kept it secret, at the request of the NSA. It was rediscovered in the late 1980s.

One important idea is seen in the attack on the reused one-time pad in Question 4 on Problem Sheet 3. We have unknown plaintexts x, $x' \in \mathbb{F}_2^n$, an unknown key $k \in \mathbb{F}_2^n$, and known ciphertexts $x + k$ and $x' + k$. Adding the known ciphertexts gives $x + x'$, independent of k.

Thus if x and x' differ by Δ then so do their encryptions $x + k$ and $x' + k$. In symbols:

$$x + x' = \Delta \implies (x + k) + (x' + k) = \Delta.$$

This shows the one-time-pad is weak to differences.

Quiz: If this is a difference attack, where are all the minus signs?

§10 Differential Cryptanalysis and AES

Differential cryptanalysis was known to the designers of DES in 1974 and was considered when designing the DES S-boxes. They kept it secret, at the request of the NSA. It was rediscovered in the late 1980s.

One important idea is seen in the attack on the reused one-time pad in Question 4 on Problem Sheet 3. We have unknown plaintexts x, $x' \in \mathbb{F}_2^n$, an unknown key $k \in \mathbb{F}_2^n$, and known ciphertexts $x + k$ and $x' + k$. Adding the known ciphertexts gives $x + x'$, independent of k.

Thus if x and x' differ by Δ then so do their encryptions $x + k$ and $x' + k$. In symbols:

$$x + x' = \Delta \implies (x + k) + (x' + k) = \Delta.$$

This shows the one-time-pad is weak to differences.

Quiz: If this is a difference attack, where are all the minus signs?

(A) It should be $x - x' = \Delta$ and $(x + k) - (x' + k) = \Delta$

(B) It's the same: we're working in $\mathbb{F}_2$

§10 Differential Cryptanalysis and AES

Differential cryptanalysis was known to the designers of DES in 1974 and was considered when designing the DES S-boxes. They kept it secret, at the request of the NSA. It was rediscovered in the late 1980s.

One important idea is seen in the attack on the reused one-time pad in Question 4 on Problem Sheet 3. We have unknown plaintexts x, $x' \in \mathbb{F}_2^n$, an unknown key $k \in \mathbb{F}_2^n$, and known ciphertexts $x + k$ and $x' + k$. Adding the known ciphertexts gives $x + x'$, independent of k.

Thus if x and x' differ by Δ then so do their encryptions $x + k$ and $x' + k$. In symbols:

$$x + x' = \Delta \implies (x + k) + (x' + k) = \Delta.$$

This shows the one-time-pad is weak to differences.

Quiz: If this is a difference attack, where are all the minus signs?

(A) It should be $x - x' = \Delta$ and $(x + k) - (x' + k) = \Delta$

(B) It's the same: we're working in $\mathbb{F}_2$

Example 10.2: Difference Attack on the Q-Block Cipher

Recall that we may write elements as $\mathbb{F}_2^8$ as pairs (v, w) where $v \in \mathbb{F}_2^4$ and $w \in \mathbb{F}_2^4$. In round 1 of the Q-block cipher (see Example 9.5), the Feistel network sends (v, w) to $\big(w, v + S(w + k^{(1)})\big)$ where

$$S\big((x_0, x_1, x_2, x_3)\big) = (x_2, x_3, x_0 + x_1x_2, x_1 + x_2x_3).$$

Lemma 10.1

(i) *For any* $w \in \mathbb{F}_2^4$ *we have* $S(w + \mathbf{1000}) = S(w) + \mathbf{0010}$.

(ii) *For any* $(v, w) \in \mathbb{F}_2^8$ *and any round key* $k^{(1)} \in \mathbb{F}_2^4$, *round* 1 *of the* Q*-block cipher is*

$$\big(v + \mathbf{0000}, w + \mathbf{1000}\big) \mapsto \big(w, v + S(w + k^{(1)})\big) + (\mathbf{1000}, \mathbf{0010}).$$

Example 10.2: Difference Attack on the Q-Block Cipher

Recall that we may write elements as $\mathbb{F}_2^8$ as pairs (v, w) where $v \in \mathbb{F}_2^4$ and $w \in \mathbb{F}_2^4$. In round 1 of the Q-block cipher (see Example 9.5), the Feistel network sends (v, w) to $\big(w, v + S(w + k^{(1)})\big)$ where

$$S\big((x_0, x_1, x_2, x_3)\big) = (x_2, x_3, x_0 + x_1x_2, x_1 + x_2x_3).$$

Lemma 10.1

(i) *For any* $w \in \mathbb{F}_2^4$ *we have* $S(w + \mathbf{1000}) = S(w) + \mathbf{0010}$.

(ii) *For any* $(v, w) \in \mathbb{F}_2^8$ *and any round key* $k^{(1)} \in \mathbb{F}_2^4$, *round* 1 *of the* Q*-block cipher is*

$$\big(v + \mathbf{0000}, w + \mathbf{1000}\big) \mapsto \big(w, v + S(w + k^{(1)})\big) + (\mathbf{1000}, \mathbf{0010}).$$

Thus the first round of the Q-block cipher encrypts plaintexts differing by $\mathbf{0000\,1000}$ to intermediate ciphertexts differing by $\mathbf{1000\,0010}$. *This 'deterministic' behaviour is just like the one-time pad.* This makes the Q-block cipher vulnerable to a difference attack using chosen plaintexts and ciphertexts.

Attack on the Q-Block Cipher [continued]

Let $x \in \mathbb{F}_2^8$ and let $\boldsymbol{\Delta} = \mathbf{0000\,1000} \in \mathbb{F}_2^8$. The diagram below shows the encryption of x and $x_\Delta = x + \boldsymbol{\Delta}$ over the three rounds of the Q-block cipher using the key $k = (k^{(1)}, k^{(2)}, k^{(3)})$, split into three round keys:

$$x \xrightarrow{k^{(1)}} y \xrightarrow{k^{(2)},\ k^{(3)}} z$$

$$\boldsymbol{\Delta} = \mathbf{0000\,1000} \qquad \boldsymbol{\Delta}' = \mathbf{1000\,0010} \qquad \boldsymbol{\Gamma}$$

$$x_\Delta \xrightarrow{k^{(1)}} y_\Delta \xrightarrow{k^{(2)},\ k^{(3)}} z_\Delta$$

The middle differences are $\boldsymbol{\Delta} = x + x_\Delta$ and $\boldsymbol{\Delta}' = y + y_\Delta$. We know $\boldsymbol{\Delta}'$ by Lemma 10.1(ii).

Attack on the Q-Block Cipher [continued]

Let $x \in \mathbb{F}_2^8$ and let $\boldsymbol{\Delta} = \mathbf{0000\,1000} \in \mathbb{F}_2^8$. The diagram below shows the encryption of x and $x_\Delta = x + \boldsymbol{\Delta}$ over the three rounds of the Q-block cipher using the key $k = (k^{(1)}, k^{(2)}, k^{(3)})$, split into three round keys:

$$x \xrightarrow{k^{(1)}} y \xrightarrow{k^{(2)},\ k^{(3)}} z$$

$$\boldsymbol{\Delta} = \mathbf{0000\,1000} \qquad \boldsymbol{\Delta}' = \mathbf{1000\,0010} \qquad \boldsymbol{\Gamma}$$

$$x_\Delta \xrightarrow{k^{(1)}} y_\Delta \xrightarrow{k^{(2)},\ k^{(3)}} z_\Delta$$

The middle differences are $\boldsymbol{\Delta} = x + x_\Delta$ and $\boldsymbol{\Delta}' = y + y_\Delta$. We know $\boldsymbol{\Delta}'$ by Lemma 10.1(ii).

We attack by guessing $k^{(2)}_{\text{guess}}$ and $k^{(3)}_{\text{guess}}$. We use these guesses to decrypt the ciphertexts z and z_Δ **over two rounds**, obtaining the intermediate ciphertexts w and w_Δ. On a correct guess $k^{(2)}_{\text{guess}} = k^{(2)}$ and $k^{(3)}_{\text{guess}} = k^{(3)}$ and then $w = y$ and $w_\Delta = y_\Delta$ and $w + w_\Delta = \boldsymbol{\Delta}'$.

Attack on the Q-Block Cipher [continued]

To see this in practice, take $k = 0001\,0011\,0111$ and $x = 0000\,0000$. (For this example, we have chosen k, but from the attacker's perspective, it is unknown.) By Exercise 5.6(i), $z = 1110\,0010$; a similar calculation gives $z_\Delta = 1101\,1100$.

(1) If we guess that $k^{(2)} = 0011$, $k^{(3)} = 0000$ then $w = 1100\,1011$, as can be read from $(v^{(1)}, v^{(2)})$ in Example 5.6(ii), and $w_\Delta = 1111\,1011$. Hence $\boldsymbol{\Delta}_\star = \mathbf{0011\,0000}$ and we know this guess is wrong.

(2) If we guess that $k^{(2)} = 0001$, $k^{(3)} = 1111$ then $w = 0000\,0110$ and $w_\Delta = 1000\,0100$. Hence $\boldsymbol{\Delta}_\star = \mathbf{1000\,0010}$ and we do not know that the guess is wrong. (This example was chosen so that also $w_0 w_1 w_2 w_3 = x_4 x_5 x_6 x_7$, as required by the Feistel function.)

Attack on the Q-Block Cipher [continued]

To see this in practice, take $k = 0001\,0011\,0111$ and $x = 0000\,0000$. (For this example, we have chosen k, but from the attacker's perspective, it is unknown.) By Exercise 5.6(i), $z = 1110\,0010$; a similar calculation gives $z_\Delta = 1101\,1100$.

(1) If we guess that $k^{(2)} = 0011$, $k^{(3)} = 0000$ then $w = 1100\,1011$, as can be read from $(v^{(1)}, v^{(2)})$ in Example 5.6(ii), and $w_\Delta = 1111\,1011$. Hence $\boldsymbol{\Delta}_\star = \mathbf{0011\,0000}$ and we know this guess is wrong.

(2) If we guess that $k^{(2)} = 0001$, $k^{(3)} = 1111$ then $w = 0000\,0110$ and $w_\Delta = 1000\,0100$. Hence $\boldsymbol{\Delta}_\star = \mathbf{1000\,0010}$ and we do not know that the guess is wrong. (This example was chosen so that also $w_0 w_1 w_2 w_3 = x_4 x_5 x_6 x_7$, as required by the Feistel function.)

Exercise 10.3

Assume that the difference attack shows the key is one of 16 possible $(k_\star^{(2)}, k_\star^{(3)})$. Show that it is subexhaustive: that is, it requires less computing than trying all $2^{12} = 4096$ keys.

Advanced Encryption Standard (2002): AES

AES is the winner of an open competition to design a successor to DES. Its block size is 128 and its key length is 128 (with variants allowing 192 and 256). It is not a Feistel cipher, but it is still built out of multiple rounds, like DES. It is the most widely used block cipher. No-one has found a subexhaustive attack on AES, despite the huge incentive.

The remaining material below is 'extra', and included for interest only.

Building Blocks of AES: Affine Transformations

Example 10.4

The *affine block cipher* of block size n has keyspace all pairs (A, b), where A is an invertible $n \times n$ matrix with entries in $\mathbb{F}_2$ and $b \in \mathbb{F}_2^n$. The encryption functions $e_{(A,b)} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ are the *affine transformations* defined by

$$e_{(A,b)}(x) = xA + b.$$

- True or false: $e_{(A,b)}$ is good for 'diffusion', i.e. making sure that every bit of the ciphertext depends on the key.
  (A) False (B) True
- True or false: $e_{(A,b)}$ is good for 'confusion', i.e. making sure the ciphertext depends in a non-linear way on the plaintext.
  (A) False (B) True

Building Blocks of AES: Affine Transformations

Example 10.4

The *affine block cipher* of block size n has keyspace all pairs (A, b), where A is an invertible $n \times n$ matrix with entries in $\mathbb{F}_2$ and $b \in \mathbb{F}_2^n$. The encryption functions $e_{(A,b)} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ are the *affine transformations* defined by

$$e_{(A,b)}(x) = xA + b.$$

- True or false: $e_{(A,b)}$ is good for 'diffusion', i.e. making sure that every bit of the ciphertext depends on the key.
  (A) False (B) True
- True or false: $e_{(A,b)}$ is good for 'confusion', i.e. making sure the ciphertext depends in a non-linear way on the plaintext.
  (A) False (B) True

Building Blocks of AES: Affine Transformations

Example 10.4

The *affine block cipher* of block size n has keyspace all pairs (A, b), where A is an invertible $n \times n$ matrix with entries in $\mathbb{F}_2$ and $b \in \mathbb{F}_2^n$. The encryption functions $e_{(A,b)} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ are the *affine transformations* defined by

$$e_{(A,b)}(x) = xA + b.$$

- True or false: $e_{(A,b)}$ is good for 'diffusion', i.e. making sure that every bit of the ciphertext depends on the key.
  (A) False (B) True
- True or false: $e_{(A,b)}$ is good for 'confusion', i.e. making sure the ciphertext depends in a non-linear way on the plaintext.
  (A) False (B) True

In fact $e_{(A,b)}$ is the composition of a linear function, namely $x \mapsto xA$ with a translation, so is almost no use for 'confusion'.

Building Blocks of AES: Pseudo-inversion

Definition 10.5

Let z be an indeterminate, as used for polynomials and power series in Part B. Define

$$\mathbb{F}_{2^8} = \{x_0 + x_1 z + \cdots + x_7 z^7 : x_0, x_1, \ldots, x_7 \in \mathbb{F}_2\}.$$

Elements of $\mathbb{F}_2^8$ are added and multiplied like polynomials in z, but whenever you see a power z^d where $d \geq 8$, eliminate it using the rule $z^8 = 1 + z + z^3 + z^4$.

Definition 10.6

Define $p : \mathbb{F}_{2^8} \to \mathbb{F}_{2^8}$ by

$$p(\beta) = \begin{cases} \beta^{-1} & \text{if } \beta \neq 0 \\ 0 & \text{if } \beta = 0. \end{cases}.$$

Let $P : \mathbb{F}_2^8 \to \mathbb{F}_2^8$ be the corresponding function defined by identifying $\mathbb{F}_2^8$ with $\mathbb{F}_{2^8}$

$$(x_0, x_1, \ldots, x_7) \longleftrightarrow x_0 + x_1 z + x_2 z^2 + \cdots + x_7 z^7.$$

Working with Pseudo-inversion: $z^8 = 1 + z + z^3 + z^4$

Example 10.7

Writing elements of $\mathbb{F}_2^8$ as words of length 8 (with a small space for readability):

(1) $1000\,0000 \longleftrightarrow 1 \in \mathbb{F}_{2^8}$ and $1^{-1} = 1$, so $p(1) = 1$ and $P(1000\,0000) = 10000000$;

(2) $0100\,0000 \longleftrightarrow z \in \mathbb{F}_{2^8}$ and $z^{-1} = 1 + z^2 + z^3 + z^7$ was seen above, so $p(z) = 1 + z^2 + z^3 + z^7$ and

$$P(0100\,0000) = 10110001.$$

(3) *Exercise:* Find $p(z^2)$ and hence show

$$P(0010\,0000) = 1101\,0011.$$

Advanced Encryption Standard (AES)

There are 10 rounds in AES. In each round, the input $x \in \mathbb{F}_2^{128}$ is split into $128/8 = 16$ subblocks each in $\mathbb{F}_2^8$.

- The round key in $\mathbb{F}_2^{128}$ is added (AddRoundKey).
- The pseudo inverse function $P : \mathbb{F}_2^8 \to \mathbb{F}_2^8$ is applied to each subblock *followed* by an affine transformation $\mathbb{F}_2^8 \to \mathbb{F}_2^8$, of the type in Example 10.4. This gives confusion and diffusion *within each subblock*. (SubBytes.)
- Diffusion across all 128 bits comes from a row bijection of the 16 subblocks, organized into a 4×4 grid

$$\begin{matrix} q(0) & q(4) & q(8) & q(12) \\ q(1) & q(5) & q(9) & q(13) \\ q(2) & q(6) & q(10) & q(14) \\ q(3) & q(7) & q(11) & q(15) \end{matrix} \longrightarrow \begin{matrix} q(0) & q(4) & q(8) & q(12) \\ q(13) & q(1) & q(5) & q(9) \\ q(10) & q(14) & q(2) & q(6) \\ q(7) & q(11) & q(15) & q(3) \end{matrix}$$

  and a further mixing of each column by the affine block cipher (ShiftRows and MixColumns)

There are no known sub-exhaustive attacks on AES. It is the most commonly used block cipher.

Differences through Pseudo-inverse

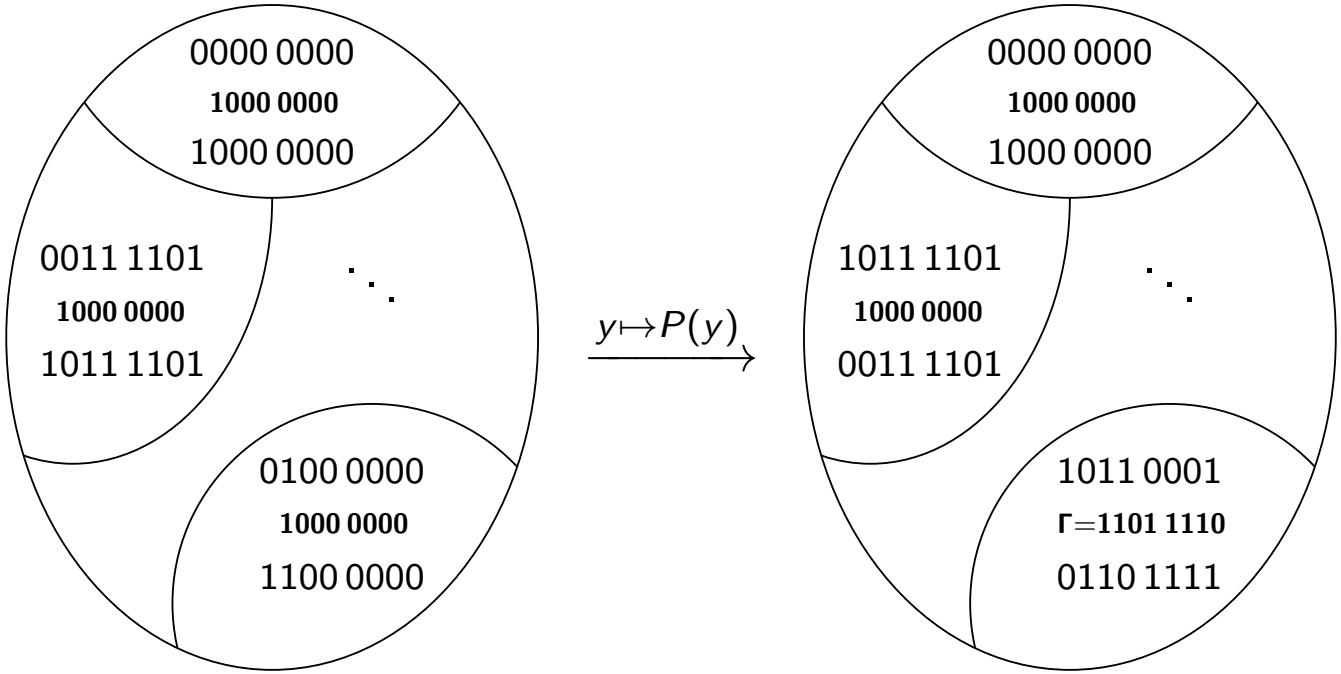
Lemma 10.8

Let $\gamma \in \mathbb{F}_2^8$ be non-zero. Then

$$\left\{\beta \in \mathbb{F}_{2^8} : p(\beta) + p(\beta + 1) = \gamma\right\}$$

has size 0 or 2, except when $\gamma = 1$, when it is $\{0, 1, \zeta, 1 + \zeta\}$ where $\zeta = z^2 + z^3 + z^4 + z^5 + z^7$.

The analogous result holds for $P : \mathbb{F}_2^8 \to \mathbb{F}_2^8$.



AES Resists the Difference Attacks

Let $\mathbf{\Delta} = 1000\,0000$, corresponding to $1 \in \mathbb{F}_{2^8}$. The left diagram shows $\mathbb{F}_2^8$ partitioned into pairs $\{x, x_\Delta\}$ with $x + x_\Delta = \mathbf{\Delta}$. The *output difference* $P(x) + P(x_\Delta)$ can be any of 127 elements $\mathbf{\Gamma} \in \mathbb{F}_2^8$. Unless $\mathbf{\Gamma} = \mathbf{1000\,0000}$, the pair $\{x, x_\Delta\}$ for output difference $\mathbf{\Gamma}$ is unique (as in the bottom-right of the diagram). Exceptionally, when $\mathbf{\Gamma} = \mathbf{1000\,0000}$, there are two possible pairs (shown in the top-left of the diagram).

Exercise 10.9

Explain why the output difference cannot be $\mathbf{0000\,0000}$.

Suppose we encrypt two plaintexts x, $x_\Delta \in \mathbb{F}_2^{128}$ differing by $\mathbf{\Delta}$ using one round of AES. In the first step of the first round, an unknown round key k_{round} is added, to give $x + k_{\text{round}}$ and $x_\Delta + k_{\text{round}}$. The difference is still Δ. But by Lemma 10.8, there are 127 (almost) equally likely output differences $\mathbf{\Gamma}$. The difference attack is ineffective.

Part D: Public Key Cryptography and Digital Signatures

§11 Introduction to Public Key Cryptography

Throughout this course we have supposed that Alice sends Bob a plaintext encrypted using some key k to a ciphertext $e_k(x) = y$ and Bob decrypts. Eve the eavesdropper observes y.

Suppose that Eve has no way (even using many years of computing time) to decrypt y getting the plaintext x. True or false?

- Bob has to know something about k that Eve does not.
  (A) False (B) True
- Alice has to know something about k that Eve does not.
  (A) False (B) True

Part D: Public Key Cryptography and Digital Signatures

§11 Introduction to Public Key Cryptography

Throughout this course we have supposed that Alice sends Bob a plaintext encrypted using some key k to a ciphertext $e_k(x) = y$ and Bob decrypts. Eve the eavesdropper observes y.

Suppose that Eve has no way (even using many years of computing time) to decrypt y getting the plaintext x. True or false?

- Bob has to know something about k that Eve does not.
  (A) False (B) True
- Alice has to know something about k that Eve does not.
  (A) False (B) True

Part D: Public Key Cryptography and Digital Signatures

§11 Introduction to Public Key Cryptography

Throughout this course we have supposed that Alice sends Bob a plaintext encrypted using some key k to a ciphertext $e_k(x) = y$ and Bob decrypts. Eve the eavesdropper observes y.

Suppose that Eve has no way (even using many years of computing time) to decrypt y getting the plaintext x. True or false?

- Bob has to know something about k that Eve does not.
  (A) False (B) True
- Alice has to know something about k that Eve does not.
  (A) False (B) True

In this part we will see why the second answer is 'False'.

- In the RSA cryposystem, Alice can encrypt a message to Bob using only Bob's public key. This is known to Eve (and everyone else). Only Bob can decrypt.
- Diffie–Hellman key exchange is even more remarkable: **both** Alice and Bob get a shared secret key (which they can use in AES or any other strong cipher), which Eve cannot determine, even though Eve observes all the messages they send.

Diffie–Hellman Key Exchange

Everything in red is private. Everything not in red is known to the whole world — this includes the eavesdropper Eve.

Example 11.1

Alice and Bob need a 128-bit key for use in AES.

(0) Alice (say) chooses a prime $p > 2^{128}$.

(1) Alice chooses a secret $a \in \mathbb{N}$ with $1 \leq a < p$ and sends Bob $2^a \bmod p$.

(2) Bob chooses a secret $b \in \mathbb{N}$ with $1 \leq b < p$ and sends Alice $2^b \bmod p$.

(3) Alice computes $(2^b \bmod p)^a \bmod p$ and Bob computes $(2^a \bmod p)^b \bmod p$.

(4) Now Alice and Bob both know $2^{ab} \bmod p$. They each write $2^{ab} \bmod p$ in binary and take the final 128 bits to get an AES key.

Example 11.1 [continued]

After (2), the eavesdropper Eve knows p, $2^a \bmod p$ and $2^b \bmod p$. It is believed that it is hard for her to use this information to find $2^{ab} \bmod p$. The difficulty can be seen even in small examples.

Exercise 11.2

Let $p = 11$. As Eve you know that Alice has sent Bob 6. Do you have any better way to find a such that $2^a = 6$ than trying each possibility?

m	0	1	2	3	4	5	6	7	8	9
$2^m \bmod 11$	1	2								

m	10	11	12	13	14	15	16	17	18	19
$2^m \bmod 11$										

Example 11.1 [continued]

After (2), the eavesdropper Eve knows p, $2^a \bmod p$ and $2^b \bmod p$. It is believed that it is hard for her to use this information to find $2^{ab} \bmod p$. The difficulty can be seen even in small examples.

Exercise 11.2

Let $p = 11$. As Eve you know that Alice has sent Bob 6. Do you have any better way to find a such that $2^a = 6$ than trying each possibility?

m	0	1	2	3	4	5	6	7	8	9
$2^m \bmod 11$	1	2	4	8	5	10	9	7	3	6
m	10	11	12	13	14	15	16	17	18	19
$2^m \bmod 11$	1	2	4	8	5	10	9	7	3	6

Example 11.1 [continued]

After (2), the eavesdropper Eve knows p, $2^a \bmod p$ and $2^b \bmod p$. It is believed that it is hard for her to use this information to find $2^{ab} \bmod p$. The difficulty can be seen even in small examples.

Exercise 11.2

Let $p = 11$. As Eve you know that Alice has sent Bob 6. Do you have any better way to find a such that $2^a = 6$ than trying each possibility?

m	0	1	2	3	4	5	6	7	8	9
$2^m \bmod 11$	1	2	4	8	5	10	9	7	3	6
m	10	11	12	13	14	15	16	17	18	19
$2^m \bmod 11$	1	2	4	8	5	10	9	7	3	6

After (4) Alice and Bob can communicate using the AES cryptosystem, which has no known sub-exhaustive attacks.
So remarkably, Alice and Bob can communicate securely *without exchanging any private key material*.

Integers Modulo a Prime

- By Fermat's Little Theorem, $c^{p-1} \equiv 1 \bmod p$ for any c not divisible by p.
- If $c^m \not\equiv 1 \bmod p$ for $m < p-1$ then c is said to be a *primitive root* modulo p and, working modulo p,

$$\{1, c, c^2, \ldots, c^{p-2}\} = \{1, 2, \ldots, p-1\}$$

  Primitive roots always exist: often one can take 2.
- Equivalently: $\mathbb{Z}_p^\times$ is cyclic of order $p-1$.
- For instance 2 is a primitive root modulo 11 but 5 is not, because $5 \equiv 2^4 \bmod 11$, so $5^5 \equiv 2^{10} \equiv 1 \bmod 11$.

Diffie–Hellman Key Exchange

This is nothing more than Example 11.1, modified to avoid some potential weaknesses, and implemented efficiently.

- The prime p is chosen so that $p-1$ has at least one large prime factor. (This is true of most primes. There are fast ways to decide if a number is prime.)
- Rather than use 2, Alice and Bob use a primitive root modulo p, so every element of $\{1,\ldots,p-1\}$ is congruent to a power of g. (The base is public.)
- Alice and Bob compute $g^a \bmod p$ and $g^b \bmod p$ by repeated squaring. See Problem Sheet 8 for the idea. For example $2^{21} \bmod 177$ is computed as follows:
  - $2^2 \equiv 4 \bmod 199$
  - $2^4 \equiv 4^2 = 16 \bmod 199$
  - $2^8 \equiv 16^2 = 256 \equiv 57 \bmod 199$
  - $2^{16} \equiv 57^2 = 3249 \equiv 65 \bmod 199$

  Now use $2^{21} = 2^{16+4+1} \equiv 65 \times 16 \times 2 = 2080 \equiv 90 \bmod 199$.
- The shared key is now $g^{ab} \bmod p$.

Discrete Logarithms (See also Group Work Week 10)

A primitive root modulo 131 is $g = 2$. So $2^{130} = 1 \bmod 131$ (this is Fermat's Little Theorem) and

$\{1, 2, \ldots, 130\} = \{1 \bmod 130, 2 \bmod 130, 2^2 \bmod 130, \ldots, 2^{130} \bmod 130\}$.

m	0	1	2	3	4	5	6	7	8	9	...
$2^m \bmod 131$	1	2	4	8	16	32	64	128	125	119	...

If $2^m = y \bmod 131$ where $0 \leq m \leq 129$ then we say that m is the *discrete log* of y (with respect to 2), modulo 131. For example $2^{46} \equiv 5 \bmod 131$ so the discrete log of 5 is 46: write $\operatorname{dlog} 46 = 5$.

(a) What is the discrete log of 16?

(A) 1 (B) 2 (C) 4 (D) 130

(b) What is the discrete log of 125? [*Hint:* $125 = 5^3$.]

(A) 8 (B) 48 (C) 92 (D) 138

(c) What is the discrete log of 80?

(A) 46 (B) 50 (C) 54 (D) 184

(d) What is $\operatorname{dlog} -1$? [*Hint:* $2^{130} \equiv 1 \bmod 131$.]

(A) 1 (B) 65 (C) 66 (D) 130

(e) What is $\operatorname{dlog} 11$?

(A) 50 (B) 54 (C) 56 (D) need a computer

Discrete Logarithms (See also Group Work Week 10)

A primitive root modulo 131 is $g = 2$. So $2^{130} = 1 \bmod 131$ (this is Fermat's Little Theorem) and

$\{1, 2, \ldots, 130\} = \{1 \bmod 130, 2 \bmod 130, 2^2 \bmod 130, \ldots, 2^{130} \bmod 130\}$.

m	0	1	2	3	4	5	6	7	8	9	...
$2^m \bmod 131$	1	2	4	8	16	32	64	128	125	119	...

If $2^m = y \bmod 131$ where $0 \leq m \leq 129$ then we say that m is the *discrete log* of y (with respect to 2), modulo 131. For example $2^{46} \equiv 5 \bmod 131$ so the discrete log of 5 is 46: write $\operatorname{dlog} 46 = 5$.

(a) What is the discrete log of 16?

(A) 1 (B) 2 (C) 4 (D) 130

(b) What is the discrete log of 125? [*Hint:* $125 = 5^3$.]

(A) 8 (B) 48 (C) 92 (D) 138

(c) What is the discrete log of 80?

(A) 46 (B) 50 (C) 54 (D) 184

(d) What is $\operatorname{dlog} -1$? [*Hint:* $2^{130} \equiv 1 \bmod 131$.]

(A) 1 (B) 65 (C) 66 (D) 130

(e) What is $\operatorname{dlog} 11$?

(A) 50 (B) 54 (C) 56 (D) need a computer

Discrete Logarithms (See also Group Work Week 10)

A primitive root modulo 131 is $g = 2$. So $2^{130} = 1 \bmod 131$ (this is Fermat's Little Theorem) and

$\{1, 2, \ldots, 130\} = \{1 \bmod 130, 2 \bmod 130, 2^2 \bmod 130, \ldots, 2^{130} \bmod 130\}$.

m	0	1	2	3	4	5	6	7	8	9	...
$2^m \bmod 131$	1	2	4	8	16	32	64	128	125	119	...

If $2^m = y \bmod 131$ where $0 \leq m \leq 129$ then we say that m is the *discrete log* of y (with respect to 2), modulo 131. For example $2^{46} \equiv 5 \bmod 131$ so the discrete log of 5 is 46: write $\operatorname{dlog} 46 = 5$.

(a) What is the discrete log of 16?

(A) 1 (B) 2 (C) 4 (D) 130

(b) What is the discrete log of 125? [*Hint:* $125 = 5^3$.]

(A) 8 (B) 48 (C) 92 (D) 138

(c) What is the discrete log of 80?

(A) 46 (B) 50 (C) 54 (D) 184

(d) What is $\operatorname{dlog} -1$? [*Hint:* $2^{130} \equiv 1 \bmod 131$.]

(A) 1 (B) 65 (C) 66 (D) 130

(e) What is $\operatorname{dlog} 11$?

(A) 50 (B) 54 (C) 56 (D) need a computer

Discrete Logarithms (See also Group Work Week 10)

A primitive root modulo 131 is $g = 2$. So $2^{130} = 1 \bmod 131$ (this is Fermat's Little Theorem) and

$\{1, 2, \ldots, 130\} = \{1 \bmod 130, 2 \bmod 130, 2^2 \bmod 130, \ldots, 2^{130} \bmod 130\}$.

m	0	1	2	3	4	5	6	7	8	9	...
$2^m \bmod 131$	1	2	4	8	16	32	64	128	125	119	...

If $2^m = y \bmod 131$ where $0 \leq m \leq 129$ then we say that m is the *discrete log* of y (with respect to 2), modulo 131. For example $2^{46} \equiv 5 \bmod 131$ so the discrete log of 5 is 46: write $\operatorname{dlog} 46 = 5$.

(a) What is the discrete log of 16?

(A) 1 (B) 2 (C) 4 (D) 130

(b) What is the discrete log of 125? [*Hint:* $125 = 5^3$.]

(A) 8 (B) 48 (C) 92 (D) 138

(c) What is the discrete log of 80?

(A) 46 (B) 50 (C) 54 (D) 184

(d) What is $\operatorname{dlog} -1$? [*Hint:* $2^{130} \equiv 1 \bmod 131$.]

(A) 1 (B) 65 (C) 66 (D) 130

(e) What is $\operatorname{dlog} 11$?

(A) 50 (B) 54 (C) 56 (D) need a computer

Discrete Logarithms (See also Group Work Week 10)

A primitive root modulo 131 is $g = 2$. So $2^{130} = 1 \bmod 131$ (this is Fermat's Little Theorem) and

$\{1, 2, \ldots, 130\} = \{1 \bmod 130, 2 \bmod 130, 2^2 \bmod 130, \ldots, 2^{130} \bmod 130\}$.

m	0	1	2	3	4	5	6	7	8	9	...
$2^m \bmod 131$	1	2	4	8	16	32	64	128	125	119	...

If $2^m = y \bmod 131$ where $0 \leq m \leq 129$ then we say that m is the *discrete log* of y (with respect to 2), modulo 131. For example $2^{46} \equiv 5 \bmod 131$ so the discrete log of 5 is 46: write $\operatorname{dlog} 46 = 5$.

(a) What is the discrete log of 16?

(A) 1 (B) 2 (C) 4 (D) 130

(b) What is the discrete log of 125? [*Hint:* $125 = 5^3$.]

(A) 8 (B) 48 (C) 92 (D) 138

(c) What is the discrete log of 80?

(A) 46 (B) 50 (C) 54 (D) 184

(d) What is $\operatorname{dlog} -1$? [*Hint:* $2^{130} \equiv 1 \bmod 131$.]

(A) 1 (B) 65 (C) 66 (D) 130

(e) What is $\operatorname{dlog} 11$?

(A) 50 (B) 54 (C) 56 (D) need a computer

Discrete Logarithms (See also Group Work Week 10)

A primitive root modulo 131 is $g = 2$. So $2^{130} = 1 \bmod 131$ (this is Fermat's Little Theorem) and

$\{1, 2, \ldots, 130\} = \{1 \bmod 130, 2 \bmod 130, 2^2 \bmod 130, \ldots, 2^{130} \bmod 130\}$.

m	0	1	2	3	4	5	6	7	8	9	...
$2^m \bmod 131$	1	2	4	8	16	32	64	128	125	119	...

If $2^m = y \bmod 131$ where $0 \leq m \leq 129$ then we say that m is the *discrete log* of y (with respect to 2), modulo 131. For example $2^{46} \equiv 5 \bmod 131$ so the discrete log of 5 is 46: write $\operatorname{dlog} 46 = 5$.

(a) What is the discrete log of 16?

(A) 1 (B) 2 (C) 4 (D) 130

(b) What is the discrete log of 125? [*Hint:* $125 = 5^3$.]

(A) 8 (B) 48 (C) 92 (D) 138

(c) What is the discrete log of 80?

(A) 46 (B) 50 (C) 54 (D) 184

(d) What is $\operatorname{dlog} -1$? [*Hint:* $2^{130} \equiv 1 \bmod 131$.]

(A) 1 (B) 65 (C) 66 (D) 130

(e) What is $\operatorname{dlog} 11$? (D) is also fine: finding discrete logs is hard!

(A) 50 (B) 54 (C) 56 (D) need a computer

Discrete Logarithm Problem and One-way Functions

- Diffie–Hellman key exchange is secure only if given g, p and $g^m \bmod p$ it is hard to find m;

Equivalently, given p, g and y it is hard to find $\operatorname{dlog}_g y$. This is called the *Discrete Logarithm Problem*.

The function

$$f : \{0, \ldots, p-2\} \to \{1, \ldots, p-1\}$$

defined by $f(m) = g^m \bmod p$ is bijective. Its inverse is $h : \{1, \ldots, p-1\} \to \{0, \ldots, p-2\}$ defined by $h(y) = \operatorname{dlog}_g y$. It is hard to find discrete logarithms if and only if f is one-way.

For instance, let $p = 1\,000\,003$.

- Asked to show that $5^{65537} \equiv 730\,930 \bmod p$ you could do it using a pocket calculator and repeated squaring. [*Hint:* $65537 = 2^{16} + 1$, so 16 squarings will find $5^{65536} \bmod p$.]
  - Computing that $f(65537) = 730\,930$ is easy.
- But given $y = 730\,930$ and asked to find m such that $5^m \equiv 730\,930 \bmod p$ you are somewhat stuck.
  - Computing that $h(730\,930) = 65537$ is hard.

Sudoku Analogy for One-way Functions

A *one-way function* is a bijective function that is fast to compute, but whose inverse is hard to compute. It is beyond the scope of this course to make this more precise. This analogy may be useful.

- Given the starting Sudoku grid on the left, it will probably take you a while to find the unique solution on the right.
- But given the solution on the right, you can verify in a few seconds that it is a Latin square (as in Example 3.15) and has the same entries as the left grid.

						6	8	
				7	3			9
3		9					4	5
4	9							
8		3		5		9		2
							3	6
9	6					3		8
7			6	8				
	2	8						

1	7	2	5	4	9	6	8	3
6	4	5	8	7	3	2	1	9
3	8	9	2	6	1	7	4	5
4	9	6	3	2	7	8	5	1
8	1	3	4	5	6	9	7	2
2	5	7	1	9	8	4	3	6
9	6	4	7	1	5	3	2	8
7	3	1	6	8	2	5	9	4
5	2	8	9	3	4	1	6	7

This shows Sudoku is in the class NP, of problems whose solution can be checked in polynomial time. P = NP if and only problems whose solution can be checked quickly can also be solved quickly.

ElGamal Cryptosystem and Further Comments

Diffie–Hellman can be turned into the ElGamal cryptosystem: see Question 6 on Sheet 8.

- ElGamal avoids the drawback of Diffie–Hellman that either Alice and Bob both have to be online at the same time, or one must wait for the other to respond before they can exchange messages.
- It is faster to use Diffie–Hellmann to agree a secret key, and then switch to a a block cipher such as DES or AES using this key.
- Diffie–Hellman is secure only if the Discrete Log Problem is hard. This is widely believed to be true (for classical computers). But it is more likely that the Discrete Log Problem is easy, or that someone will make a quantum computer big enough to solve practical instances of it, than that AES has a sub-exhaustive attack.

For these reasons block ciphers and stream ciphers are still widely used.

Inverting Exponentiation Modulo p

In the RSA cryptosystem, we use modular exponentiation as the encryption map. We therefore need to know when it is invertible.

Lemma 11.3

If p is prime and $\mathrm{hcf}(a, p-1) = 1$ then the inverse of $x \mapsto x^a$ mod p is $y \mapsto y^r$ mod p, where $ar \equiv 1$ mod $p-1$.

For example, if $p = 29$ then $x \mapsto x^7$ is not invertible, and $x \mapsto x^3$ is invertible, with inverse $y \mapsto y^{19}$. This works, since after doing both maps, in either order, we send x to x^{57}; by Fermat's Little Theorem, $x^{57} = x^{28\times 2+1} = (x^{28})^2 x \equiv x$ mod 29.

Given p and a, one can use Euclid's algorithm to find s, $t \in \mathbb{Z}$ such that $as + (p-1)t = 1$. Then $as = 1 - pt$ so $as \equiv 1$ mod $p-1$, and we take $r \equiv s$ mod $p-1$.

This proves Lemma 11.3, and shows that it is fast to find r. Thus we cannot use $x \mapsto x^a$ mod p as a secure encryption function.

Inverting Exponentiation Modulo n

Fact 11.4

Let p and q be distinct primes. Let $n = pq$. If

$$\mathrm{hcf}\big(a, (p-1)(q-1)\big) = 1$$

then $x \mapsto x^a$ mod n is invertible with inverse $y \mapsto y^r$ mod n, where $ar \equiv 1$ mod $(p-1)(q-1)$.

Example 11.5

Let $p = 11$, $q = 17$, so $n = pq = 187$ and $(p-1)(q-1) = 160$. Let $a = 9$. Adapting the proof for Lemma 11.3, we use Euclid's Algorithm to solve $9s + 160t = 1$, getting $s = -71$ and $t = 4$. Since $-71 \equiv 89$ mod 160, the inverse of $x \mapsto x^9$ mod 187 is $y \mapsto y^{89}$ mod 187.

Thus given a, p and q it is easy to find r as in Fact 11.4. But it is believed to be hard to find r given only a and n. This makes $x \mapsto x^a$ mod n suitable for use in a cryptosystem.

RSA Cryptosystem

Let $n = pq$ be the product of distinct primes p and q. In the RSA Cryptosystem, with *RSA modulus* n,

$$\mathcal{P} = \mathcal{C} = \{0, 1, \ldots, n-1\}$$

and

$$\mathcal{K} = \big\{(p, q, a) : a \in \{1, \ldots, n-1\}, \operatorname{hcf}\big(a, (p-1)(q-1)\big) = 1\big\}.$$

The *public key* corresponding to (p, q, a) is (n, a) and the *private key* corresponding to (p, q, a) is (p, q, r), where $ar \equiv 1 \bmod (p-1)(q-1)$. (Note that a is part of the public key, so unlike Diffie–Hellman, it is public.) The encryption function for (p, q, a) is

$$x \mapsto x^a \bmod n$$

and the decryption function is

$$y \mapsto y^r \bmod n.$$

Note that anyone knowing the public key can encrypt, but only someone knowing the private key, or the entire key (p, q, a), can decrypt (or so it is widely believed).

Quiz on RSA

True or false?

- Alice's encryption exponent a is public knowledge.
  (A) False (B) True
- Alice's decryption exponent r is public knowledge.
  (A) False (B) True
- If Malcolm can learn r then he decrypt.
  (A) False (B) True
- If Malcolm can learn r then he can factor n.
  (A) False (B) True

Suppose Alice's RSA modulus n is $13 \times 17 = 221$ and her encryption exponent is 8.

- If Bob's plaintext is 2, what number will he send to Alice?
  (A) 2 (B) 35 (C) 223 (D) 256
- Suppose Bob mistakenly uses the (invalid) plaintext 223. What will Alice decode his ciphertext $223^8 \bmod 221$ as?
  (A) 2 (B) 35 (C) 223 (D) 256

Quiz on RSA

True or false?

- Alice's encryption exponent a is public knowledge.
  (A) False (B) True
- Alice's decryption exponent r is public knowledge.
  (A) False (B) True
- If Malcolm can learn r then he decrypt.
  (A) False (B) True
- If Malcolm can learn r then he can factor n.
  (A) False (B) True

Suppose Alice's RSA modulus n is $13 \times 17 = 221$ and her encryption exponent is 8.

- If Bob's plaintext is 2, what number will he send to Alice?
  (A) 2 (B) 35 (C) 223 (D) 256
- Suppose Bob mistakenly uses the (invalid) plaintext 223. What will Alice decode his ciphertext $223^8 \bmod 221$ as?
  (A) 2 (B) 35 (C) 223 (D) 256

Quiz on RSA

True or false?

- Alice's encryption exponent a is public knowledge.
  (A) False (B) True
- Alice's decryption exponent r is public knowledge.
  (A) False (B) True
- If Malcolm can learn r then he decrypt.
  (A) False (B) True
- If Malcolm can learn r then he can factor n.
  (A) False (B) True

Suppose Alice's RSA modulus n is $13 \times 17 = 221$ and her encryption exponent is 8.

- If Bob's plaintext is 2, what number will he send to Alice?
  (A) 2 (B) 35 (C) 223 (D) 256
- Suppose Bob mistakenly uses the (invalid) plaintext 223. What will Alice decode his ciphertext $223^8 \bmod 221$ as?
  (A) 2 (B) 35 (C) 223 (D) 256

Quiz on RSA

True or false?

- Alice's encryption exponent a is public knowledge.
  (A) False (B) True
- Alice's decryption exponent r is public knowledge.
  (A) False (B) True
- If Malcolm can learn r then he decrypt.
  (A) False (B) True
- If Malcolm can learn r then he can factor n.
  (A) False (B) True

Suppose Alice's RSA modulus n is $13 \times 17 = 221$ and her encryption exponent is 8.

- If Bob's plaintext is 2, what number will he send to Alice?
  (A) 2 (B) 35 (C) 223 (D) 256
- Suppose Bob mistakenly uses the (invalid) plaintext 223. What will Alice decode his ciphertext $223^8 \bmod 221$ as?
  (A) 2 (B) 35 (C) 223 (D) 256

Quiz on RSA

True or false?

- Alice's encryption exponent a is public knowledge.
  (A) False (B) True
- Alice's decryption exponent r is public knowledge.
  (A) False (B) True
- If Malcolm can learn r then he decrypt.
  (A) False (B) True
- If Malcolm can learn r then he can factor n. (In Part D extras.)
  (A) False (B) True

Suppose Alice's RSA modulus n is $13 \times 17 = 221$ and her encryption exponent is 8.

- If Bob's plaintext is 2, what number will he send to Alice?
  (A) 2 (B) 35 (C) 223 (D) 256
- Suppose Bob mistakenly uses the (invalid) plaintext 223. What will Alice decode his ciphertext 223^8 mod 221 as?
  (A) 2 (B) 35 (C) 223 (D) 256

Quiz on RSA

True or false?

- Alice's encryption exponent a is public knowledge.
  (A) False (B) True
- Alice's decryption exponent r is public knowledge.
  (A) False (B) True
- If Malcolm can learn r then he decrypt.
  (A) False (B) True
- If Malcolm can learn r then he can factor n. (In Part D extras.)
  (A) False (B) True

Suppose Alice's RSA modulus n is $13 \times 17 = 221$ and her encryption exponent is 8.

- If Bob's plaintext is 2, what number will he send to Alice?
  (A) 2 (B) 35 (C) 223 (D) 256
- Suppose Bob mistakenly uses the (invalid) plaintext 223. What will Alice decode his ciphertext 223^8 mod 221 as?
  (A) 2 (B) 35 (C) 223 (D) 256

Quiz on RSA

True or false?

- Alice's encryption exponent a is public knowledge.
  (A) False (B) True
- Alice's decryption exponent r is public knowledge.
  (A) False (B) True
- If Malcolm can learn r then he decrypt.
  (A) False (B) True
- If Malcolm can learn r then he can factor n. (In Part D extras.)
  (A) False (B) True

Suppose Alice's RSA modulus n is $13 \times 17 = 221$ and her encryption exponent is 8.

- If Bob's plaintext is 2, what number will he send to Alice?
  (A) 2 (B) 35 (C) 223 (D) 256
- Suppose Bob mistakenly uses the (invalid) plaintext 223. What will Alice decode his ciphertext 223^8 mod 221 as?
  (A) 2 (B) 35 (C) 223 (D) 256

Quiz on RSA

True or false?

- Alice's encryption exponent a is public knowledge.
  (A) False (B) True
- Alice's decryption exponent r is public knowledge.
  (A) False (B) True
- If Malcolm can learn r then he decrypt.
  (A) False (B) True
- If Malcolm can learn r then he can factor n. (In Part D extras.)
  (A) False (B) True

Suppose Alice's RSA modulus n is $13 \times 17 = 221$ and her encryption exponent is 8.

- If Bob's plaintext is 2, what number will he send to Alice?
  (A) 2 (B) 35 (C) 223 (D) 256
- Suppose Bob mistakenly uses the (invalid) plaintext 223. What will Alice decode his ciphertext 223^8 mod 221 as?
  (A) 2 (B) 35 (C) 223 (D) 256

Key Distribution and Other Traps

One problem with RSA is that Bob somehow has to learn Alice's public key. If Alice emails her public key to Bob, there is a man-in-the-middle attack, in which Malcolm tricks Bob into encrypting with his public key instead. See video! There are several other traps for the unwary.

- Suppose Alice is expecting a 'Yes', 'No' message from Bob, and Eve the eavesdropper knows this. Alice receives an RSA ciphertext from Bob and decrypts it, using her private key, to read 'Yes'. Can Eve learn Bob's message?

  (A) No (B) Yes

  What if Alice and Bob instead used AES with a shared secret key. Can Eve learn Bob's message?

  (A) No (B) Yes

Key Distribution and Other Traps

One problem with RSA is that Bob somehow has to learn Alice's public key. If Alice emails her public key to Bob, there is a man-in-the-middle attack, in which Malcolm tricks Bob into encrypting with his public key instead. See video! There are several other traps for the unwary.

- Suppose Alice is expecting a 'Yes', 'No' message from Bob, and Eve the eavesdropper knows this. Alice receives an RSA ciphertext from Bob and decrypts it, using her private key, to read 'Yes'. Can Eve learn Bob's message?

  (A) No (B) Yes

  What if Alice and Bob instead used AES with a shared secret key. Can Eve learn Bob's message?

  (A) No (B) Yes

Key Distribution and Other Traps

One problem with RSA is that Bob somehow has to learn Alice's public key. If Alice emails her public key to Bob, there is a man-in-the-middle attack, in which Malcolm tricks Bob into encrypting with his public key instead. See video! There are several other traps for the unwary.

- Suppose Alice is expecting a 'Yes', 'No' message from Bob, and Eve the eavesdropper knows this. Alice receives an RSA ciphertext from Bob and decrypts it, using her private key, to read 'Yes'. Can Eve learn Bob's message?

  (A) No (B) Yes

  What if Alice and Bob instead used AES with a shared secret key. Can Eve learn Bob's message?

  (A) No (B) Yes

Key Distribution and Other Traps

One problem with RSA is that Bob somehow has to learn Alice's public key. If Alice emails her public key to Bob, there is a man-in-the-middle attack, in which Malcolm tricks Bob into encrypting with his public key instead. See video! There are several other traps for the unwary.

- Suppose Alice is expecting a 'Yes', 'No' message from Bob, and Eve the eavesdropper knows this. Alice receives an RSA ciphertext from Bob and decrypts it, using her private key, to read 'Yes'. Can Eve learn Bob's message?

  (A) No (B) Yes

  What if Alice and Bob instead used AES with a shared secret key. Can Eve learn Bob's message?

  (A) No (B) Yes

Why? Anyone can encrypt an RSA message to Alice, so Eve can encrypt 'Yes' and 'No' and see which one agrees with Bob's ciphertext. She cannot do this with AES, as she does not know the key. To avoid this problem, Bob should 'pad' his message with some random numbers, sending 'Yes13242394239423 . . . '.

Key Distribution and Other Traps

One problem with RSA is that Bob somehow has to learn Alice's public key. If Alice emails her public key to Bob, there is a man-in-the-middle attack, in which Malcolm tricks Bob into encrypting with his public key instead. See video! There are several other traps for the unwary.

- Suppose Alice is expecting a 'Yes', 'No' message from Bob, and Eve the eavesdropper knows this. Alice receives an RSA ciphertext from Bob and decrypts it, using her private key, to read 'Yes'. Can Eve learn Bob's message?

  (A) No (B) Yes

  What if Alice and Bob instead used AES with a shared secret key. Can Eve learn Bob's message?

  (A) No (B) Yes

No-one has found a mathematical attack on RSA other than factorizing n. The best known algorithm (the Number Field Sieve) was used to factorize a 768 bit n in 2010. This took about 1500 computer years, in 2010 technology.

NIST (US standards body) now recommend that n has 2048 bits.

RSA in Practice

Example 11.6

(1) For a small example, take p and q as in Example 11.5. If Alice's public key is $(187, 9)$ then her private key is $(11, 17, 89)$. If Bob's message is 10 then he sends 109 to Alice, since $10^9 \equiv 109 \bmod 187$. Alice decrypts to 10 by computing $109^{89} \bmod 187$.

(2) The MATHEMATICA notebook `PKC.nb` available from Moodle can be used when p and q are large. It has some 'helper functions' for encrypting and decrypting strings.

Please use it for Question 3 on Problem Sheet 8. (If you do not get a message from your partner then instead email the lecturer your public key for a substitute.)

(3) RSA is much slower than block ciphers such as AES. In practice RSA is often used to encrypt a key for AES or another block cipher. This is how HTTPS (padlock in your address bar) and Pretty Good Privacy work.

Quiz on Diffie–Hellman and RSA

Let p be a prime of size about 2^{1024}.

(a) Given g and a it is fast to compute g^a mod p.

(A) False (B) True

(b) Given g and g^a mod p, with a known to be in $\{1, \ldots, p-2\}$, it is fast to compute a.

(A) False (B) True

(c) The function $\{1, \ldots, p-1\} \to \{1, \ldots, p-1\}$ mod p defined by $x \mapsto x^2$ is invertible.

(A) False (B) True

(d) If $\mathrm{hcf}(a, p-1) = 1$ then the function $\{1, \ldots, p-1\} \to \{1, \ldots, p-1\}$ defined by $x \mapsto x^a$ mod p is invertible, and it is fast to compute its inverse.

(A) False (B) True

(e) Let g be a primitive root modulo p. The function $\{0, \ldots, p-2\} \to \{1, \ldots, p-1\}$ defined by $m \mapsto g^m$ mod p is invertible and it is fast to compute its inverse.

(A) False (B) True

Quiz on Diffie–Hellman and RSA

Let p be a prime of size about 2^{1024}.

(a) Given g and a it is fast to compute g^a mod p.

(A) False (B) True

(b) Given g and g^a mod p, with a known to be in $\{1, \ldots, p-2\}$, it is fast to compute a.

(A) False (B) True

(c) The function $\{1, \ldots, p-1\} \to \{1, \ldots, p-1\}$ mod p defined by $x \mapsto x^2$ is invertible.

(A) False (B) True

(d) If $\mathrm{hcf}(a, p-1) = 1$ then the function $\{1, \ldots, p-1\} \to \{1, \ldots, p-1\}$ defined by $x \mapsto x^a$ mod p is invertible, and it is fast to compute its inverse.

(A) False (B) True

(e) Let g be a primitive root modulo p. The function $\{0, \ldots, p-2\} \to \{1, \ldots, p-1\}$ defined by $m \mapsto g^m$ mod p is invertible and it is fast to compute its inverse.

(A) False (B) True

Quiz on Diffie–Hellman and RSA

Let p be a prime of size about 2^{1024}.

(a) Given g and a it is fast to compute g^a mod p.

(A) False (B) True

(b) Given g and g^a mod p, with a known to be in $\{1, \ldots, p-2\}$, it is fast to compute a.

(A) False (B) True

(c) The function $\{1, \ldots, p-1\} \to \{1, \ldots, p-1\}$ mod p defined by $x \mapsto x^2$ is invertible.

(A) False (B) True

(d) If $\mathrm{hcf}(a, p-1) = 1$ then the function $\{1, \ldots, p-1\} \to \{1, \ldots, p-1\}$ defined by $x \mapsto x^a$ mod p is invertible, and it is fast to compute its inverse.

(A) False (B) True

(e) Let g be a primitive root modulo p. The function $\{0, \ldots, p-2\} \to \{1, \ldots, p-1\}$ defined by $m \mapsto g^m$ mod p is invertible and it is fast to compute its inverse.

(A) False (B) True

Quiz on Diffie–Hellman and RSA

Let p be a prime of size about 2^{1024}.

(a) Given g and a it is fast to compute g^a mod p.

(A) False (B) True

(b) Given g and g^a mod p, with a known to be in $\{1, \ldots, p-2\}$, it is fast to compute a.

(A) False (B) True

(c) The function $\{1, \ldots, p-1\} \to \{1, \ldots, p-1\}$ mod p defined by $x \mapsto x^2$ is invertible.

(A) False (B) True

(d) If $\mathrm{hcf}(a, p-1) = 1$ then the function $\{1, \ldots, p-1\} \to \{1, \ldots, p-1\}$ defined by $x \mapsto x^a$ mod p is invertible, and it is fast to compute its inverse.

(A) False (B) True

(e) Let g be a primitive root modulo p. The function $\{0, \ldots, p-2\} \to \{1, \ldots, p-1\}$ defined by $m \mapsto g^m$ mod p is invertible and it is fast to compute its inverse.

(A) False (B) True

Quiz on Diffie–Hellman and RSA

Let p be a prime of size about 2^{1024}.

(a) Given g and a it is fast to compute g^a mod p.

(A) False (B) True

(b) Given g and g^a mod p, with a known to be in $\{1, \ldots, p-2\}$, it is fast to compute a.

(A) False (B) True

(c) The function $\{1, \ldots, p-1\} \to \{1, \ldots, p-1\}$ mod p defined by $x \mapsto x^2$ is invertible.

(A) False (B) True

(d) If $\mathrm{hcf}(a, p-1) = 1$ then the function $\{1, \ldots, p-1\} \to \{1, \ldots, p-1\}$ defined by $x \mapsto x^a$ mod p is invertible, and it is fast to compute its inverse.

(A) False (B) True

(e) Let g be a primitive root modulo p. The function $\{0, \ldots, p-2\} \to \{1, \ldots, p-1\}$ defined by $m \mapsto g^m$ mod p is invertible and it is fast to compute its inverse.

(A) False (B) True

Quiz on Diffie–Hellman and RSA

Let p be a prime of size about 2^{1024}.

(a) Given g and a it is fast to compute g^a mod p.

(A) False (B) True

(b) Given g and g^a mod p, with a known to be in $\{1, \ldots, p-2\}$, it is fast to compute a.

(A) False (B) True

(c) The function $\{1, \ldots, p-1\} \to \{1, \ldots, p-1\}$ mod p defined by $x \mapsto x^2$ is invertible.

(A) False (B) True

(d) If $\mathrm{hcf}(a, p-1) = 1$ then the function $\{1, \ldots, p-1\} \to \{1, \ldots, p-1\}$ defined by $x \mapsto x^a$ mod p is invertible, and it is fast to compute its inverse.

(A) False (B) True

(e) Let g be a primitive root modulo p. The function $\{0, \ldots, p-2\} \to \{1, \ldots, p-1\}$ defined by $m \mapsto g^m$ mod p is invertible and it is fast to compute its inverse.

(A) False (B) True

Quiz on Diffie–Hellman and RSA [continued]

Let p and q be primes of size about 2^{1024} and let $n = pq$.

(f) If $\mathrm{hcf}\big(a, (p-1)(q-1)\big) = 1$ then the function $\{1, \ldots, n-1\} \to \{1, \ldots, n-1\}$ defined by $x \mapsto x^a \bmod n$ is invertible.

(A) False (B) True

(g) Suppose $x \mapsto x^a \bmod n$ is invertible. Given a and n it is fast to compute its inverse.

(A) False (B) True

(h) Let $x \mapsto x^a \bmod n$ be the encryption function in RSA. The decryption function is $y \mapsto y^r \bmod n$ where $ar \equiv 1 \bmod (p-1)(q-1)$.

(A) False (B) True

(i) Let (n, a) be an RSA public key with private key (p, q, r). Knowing (n, a) and the decryption exponent r in the private key, it is possible to find p and q.

(A) False (B) True

For (i) see the optional extras in §11 of the Part D Notes, in particular Example 11.7.

Quiz on Diffie–Hellman and RSA [continued]

Let p and q be primes of size about 2^{1024} and let $n = pq$.

(f) If $\mathrm{hcf}\big(a, (p-1)(q-1)\big) = 1$ then the function $\{1, \ldots, n-1\} \to \{1, \ldots, n-1\}$ defined by $x \mapsto x^a \bmod n$ is invertible.

(A) False (B) True

(g) Suppose $x \mapsto x^a \bmod n$ is invertible. Given a and n it is fast to compute its inverse.

(A) False (B) True

(h) Let $x \mapsto x^a \bmod n$ be the encryption function in RSA. The decryption function is $y \mapsto y^r \bmod n$ where $ar \equiv 1 \bmod (p-1)(q-1)$.

(A) False (B) True

(i) Let (n, a) be an RSA public key with private key (p, q, r). Knowing (n, a) and the decryption exponent r in the private key, it is possible to find p and q.

(A) False (B) True

For (i) see the optional extras in §11 of the Part D Notes, in particular Example 11.7.

Quiz on Diffie–Hellman and RSA [continued]

Let p and q be primes of size about 2^{1024} and let $n = pq$.

(f) If $\mathrm{hcf}\big(a, (p-1)(q-1)\big) = 1$ then the function $\{1, \ldots, n-1\} \to \{1, \ldots, n-1\}$ defined by $x \mapsto x^a \bmod n$ is invertible.

(A) False (B) True

(g) Suppose $x \mapsto x^a \bmod n$ is invertible. Given a and n it is fast to compute its inverse.

(A) False (B) True

(h) Let $x \mapsto x^a \bmod n$ be the encryption function in RSA. The decryption function is $y \mapsto y^r \bmod n$ where $ar \equiv 1 \bmod (p-1)(q-1)$.

(A) False (B) True

(i) Let (n, a) be an RSA public key with private key (p, q, r). Knowing (n, a) and the decryption exponent r in the private key, it is possible to find p and q.

(A) False (B) True

For (i) see the optional extras in §11 of the Part D Notes, in particular Example 11.7.

Quiz on Diffie–Hellman and RSA [continued]

Let p and q be primes of size about 2^{1024} and let $n = pq$.

(f) If $\mathrm{hcf}\big(a, (p-1)(q-1)\big) = 1$ then the function $\{1, \ldots, n-1\} \to \{1, \ldots, n-1\}$ defined by $x \mapsto x^a \bmod n$ is invertible.

(A) False (B) True

(g) Suppose $x \mapsto x^a \bmod n$ is invertible. Given a and n it is fast to compute its inverse.

(A) False (B) True

(h) Let $x \mapsto x^a \bmod n$ be the encryption function in RSA. The decryption function is $y \mapsto y^r \bmod n$ where $ar \equiv 1 \bmod (p-1)(q-1)$.

(A) False (B) True

(i) Let (n, a) be an RSA public key with private key (p, q, r). Knowing (n, a) and the decryption exponent r in the private key, it is possible to find p and q.

(A) False (B) True

For (i) see the optional extras in §11 of the Part D Notes, in particular Example 11.7.

Quiz on Diffie–Hellman and RSA [continued]

Let p and q be primes of size about 2^{1024} and let $n = pq$.

(f) If $\mathrm{hcf}\big(a, (p-1)(q-1)\big) = 1$ then the function $\{1, \ldots, n-1\} \to \{1, \ldots, n-1\}$ defined by $x \mapsto x^a \bmod n$ is invertible.

(A) False (B) True

(g) Suppose $x \mapsto x^a \bmod n$ is invertible. Given a and n it is fast to compute its inverse.

(A) False (B) True

(h) Let $x \mapsto x^a \bmod n$ be the encryption function in RSA. The decryption function is $y \mapsto y^r \bmod n$ where $ar \equiv 1 \bmod (p-1)(q-1)$.

(A) False (B) True

(i) Let (n, a) be an RSA public key with private key (p, q, r). Knowing (n, a) and the decryption exponent r in the private key, it is possible to find p and q.

(A) False (B) True

For (i) see the optional extras in §11 of the Part D Notes, in particular Example 11.7.

RSA as an Illegal Munition

§12 Digital Signatures and Hash Functions

Suppose Alice and Bob have the RSA keys:

	public	private
Alice	(m, a)	(p, q, r)
Bob	(n, b)	$(?, ?, s)$

Suppose Alice wants to tell Bob her bank details in a message x. She looks up his public key (n, b) and sends him $e_B(x) = x^b \bmod n$. (Assume that $x < n$.)

Malcolm cannot decrypt $x^b \bmod n$, because he does not know s. But if he has control of the channel, he can replace $x^b \bmod n$ with another $x'^b \bmod n$, of his choice.

§12 Digital Signatures and Hash Functions

Suppose Alice and Bob have the RSA keys:

	public	private
Alice	(m, a)	(p, q, r)
Bob	(n, b)	$(?, ?, s)$

Suppose Alice wants to tell Bob her bank details in a message x. She looks up his public key (n, b) and sends him $e_B(x) = x^b \bmod n$. (Assume that $x < n$.)

Malcolm cannot decrypt $x^b \bmod n$, because he does not know s. But if he has control of the channel, he can replace $x^b \bmod n$ with another $x'^b \bmod n$, of his choice.

This requires Malcolm to know Bob's public key. So the attack is specific to public key cryptosystems such as RSA. If the key k is secret, only Alice and Bob know the encryption function e_k.

How can Bob be confident that a message signed 'Alice' is from Alice, and not from Malcolm pretending to Alice?

Motivation for Hash Functions

RSA keys	public	private
Alice	(m, a)	(p, q, r)
Bob	(n, b)	$(?, ?, s)$

Alice and Bob's encryption and decryption functions are

$$e_A(x) = x^a \bmod m \quad d_A(x) = x^r \bmod m$$
$$e_B(x) = x^b \bmod n \quad d_B(x) = x^s \bmod n.$$

Motivation for Hash Functions

Alice and Bob's encryption and decryption functions are

$$e_A(x) = x^a \bmod m \quad d_A(x) = x^r \bmod m$$
$$e_B(x) = x^b \bmod n \quad d_B(x) = x^s \bmod n.$$

Motivation for Hash Functions

Alice and Bob's encryption and decryption functions are

$$e_A(x) = x^a \bmod m \quad d_A(x) = x^r \bmod m$$
$$e_B(x) = x^b \bmod n \quad d_B(x) = x^s \bmod n.$$

Example 12.1

Bob is expecting a message from Alice. He receives z, and computes $d_B(z) = z^s \bmod n$, but gets garbage. Thinking that Alice has somehow confused the keys, he computes $e_A(z) = z^a \bmod m$, and gets the ASCII encoding of

'Dear Bob, my account number is 40081234, best wishes, Alice'.

(a) How did Alice compute z?

(b) Should Bob believe z was sent by Alice?

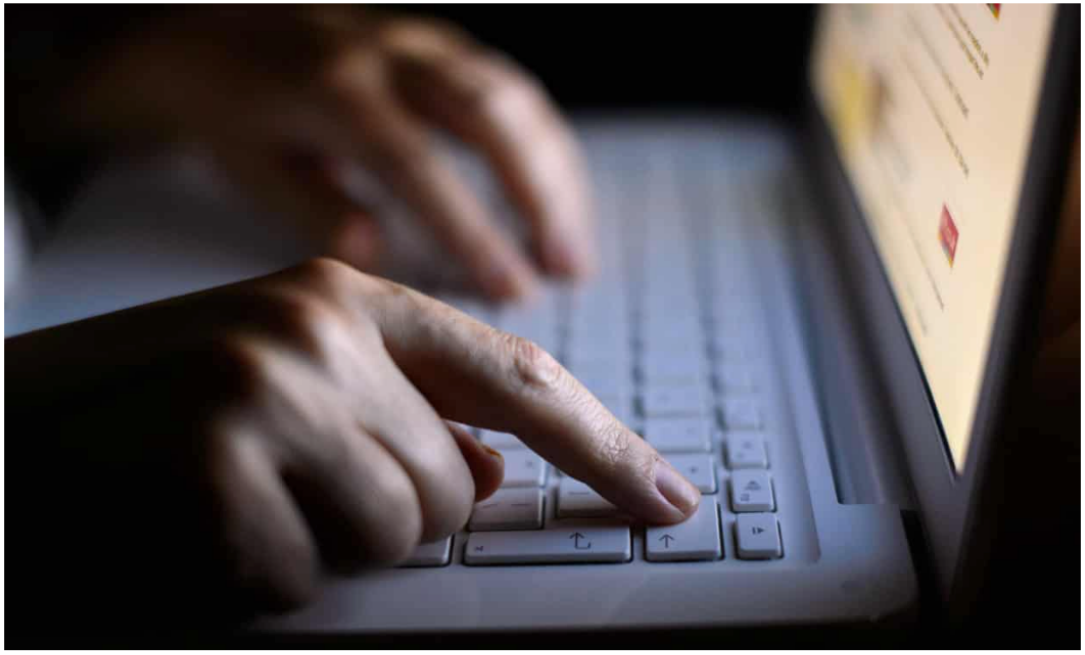
(c) Can Malcolm read z?

(d) How can Alice avoid the problem in (c)? (Assume that $m < n$.)

Guardian, October 2017

‘We lost £120,000 in an email scam but the banks won’t help get it back’

In another example of a growing menace, the Scotts thought they were sending money to their solicitor’s bank account. Little did they know it went to a fraudster



▲ Never trust an email containing bank account or payment details. Photograph: Dominic Lipinski/PA

It is the worst case of email intercept fraud that Money has ever featured. An Essex couple have lost £120,000 after sending the money to what they thought was their solicitor’s bank account, but which instead went to an account in Kent that was systematically emptied of £20,000 in cash every day for the next six days.

Signed Messages using RSA

Recall that Alice's RSA functions are

$$e_A(x) = x^a \bmod m \quad d_A(x) = x^r \bmod m.$$

Let $x \in \mathbb{N}_0$ be Alice's message. If Alice's RSA modulus m is about 2^{2048} then the message x is a legitimate ciphertext only if $x < 2^{2048}$. This may seem big, but, using the 8-bit ASCII coding, it means only $2048/8 = 2^8 = 256$ characters can be sent.

Alice can get round this by splitting the message into blocks, but computing $d_A(x^{(i)})$ for each block $x^{(i)} \in \{1, \ldots, n-1\}$ is slow. It is better to send x, and then append $d_A\big(h(x)\big)$ where $h(x) \in \{0, 1, \ldots, n-1\}$ is a hash of x.

Hash Functions

Definition 12.2

(i) A *hash function* of length r is a function $h : \mathbb{N}_0 \to \mathbb{F}_2^r$. The value $h(x)$ is the *hash* of the message $x \in \mathbb{N}_0$.

(ii) Let (m, a) be Alice's public key in the RSA cryptosystem where $m > 2^r$. To *sign* a message x, Alice computes $h(x) \in \mathbb{F}_2^r$ and, reading $h(x)$ as a number written in binary, computes $d_A\big(h(x)\big)$. The pair $\big(x, d_A(h(x))\big)$ is a *signed message of x from Alice*.

Bob (or anyone else) *verifies* that a pair (x, v) is a valid signed message from Alice by checking that $h(x) = e_A(v)$.

Hash Functions

Definition 12.2

(i) A *hash function* of length r is a function $h : \mathbb{N}_0 \to \mathbb{F}_2^r$. The value $h(x)$ is the *hash* of the message $x \in \mathbb{N}_0$.

(ii) Let (m, a) be Alice's public key in the RSA cryptosystem where $m > 2^r$. To *sign* a message x, Alice computes $h(x) \in \mathbb{F}_2^r$ and, reading $h(x)$ as a number written in binary, computes $d_A\big(h(x)\big)$. The pair $\big(x, d_A(h(x))\big)$ is a *signed message of x from Alice*.

Bob (or anyone else) *verifies* that a pair (x, v) is a valid signed message from Alice by checking that $h(x) = e_A(v)$.

A cryptographically useful hash function satisfies:

(a) It is fast to compute $h(x)$.

(b) Given a message $x \in \mathbb{N}_0$, and its hash $h(x)$, it is hard to find $y \in \mathbb{N}_0$ such that $y \neq x$ and $h(y) = h(x)$. (*Preimage resistance.*)

(c) It is hard to find a pair (x, x') with $x \neq x'$ such that $h(x) = h(x')$. (*Collision resistance.*)

Preimage Resistance: Example 12.3

Malcolm has intercepted a signed message (x, v) from Alice. If he can find y with $h(y) = v$ then he can replace x with y and Bob will still verify Alice's signature.

Assume hash values are distributed uniformly at random in $\mathbb{F}_2^r$.

- Given a hash value $v \in \mathbb{F}_2^r$, what is the probability that a random $y \in \mathbb{N}_0$ will have $h(y) = v$?
  (A) $\frac{1}{2^{2r}}$ (B) $\frac{1}{2^r}$ (C) $\frac{1}{2^{r/2}}$ (D) $\frac{1}{2}$
- How many hashes does Malcolm need to compute on average to find y such that $h(y) = v$?
  (A) $2^{r/2}$ (B) 2^{r-1} (C) 2^r (D) 2^{2r}
- What is the distribution of the number of hashes Malcolm computes before finding a suitable y?

Preimage Resistance: Example 12.3

Malcolm has intercepted a signed message (x, v) from Alice. If he can find y with $h(y) = v$ then he can replace x with y and Bob will still verify Alice's signature.

Assume hash values are distributed uniformly at random in $\mathbb{F}_2^r$.

- Given a hash value $v \in \mathbb{F}_2^r$, what is the probability that a random $y \in \mathbb{N}_0$ will have $h(y) = v$?

  (A) $\frac{1}{2^{2r}}$ (B) $\frac{1}{2^r}$ (C) $\frac{1}{2^{r/2}}$ (D) $\frac{1}{2}$

- How many hashes does Malcolm need to compute on average to find y such that $h(y) = v$?

  (A) $2^{r/2}$ (B) 2^{r-1} (C) 2^r (D) 2^{2r}

- What is the distribution of the number of hashes Malcolm computes before finding a suitable y?

Preimage Resistance: Example 12.3

Malcolm has intercepted a signed message (x, v) from Alice. If he can find y with $h(y) = v$ then he can replace x with y and Bob will still verify Alice's signature.

Assume hash values are distributed uniformly at random in $\mathbb{F}_2^r$.

- Given a hash value $v \in \mathbb{F}_2^r$, what is the probability that a random $y \in \mathbb{N}_0$ will have $h(y) = v$?

  (A) $\frac{1}{2^{2r}}$ (B) $\frac{1}{2^r}$ (C) $\frac{1}{2^{r/2}}$ (D) $\frac{1}{2}$

- How many hashes does Malcolm need to compute on average to find y such that $h(y) = v$?

  (A) $2^{r/2}$ (B) 2^{r-1} (C) 2^r (D) 2^{2r}

- What is the distribution of the number of hashes Malcolm computes before finding a suitable y?

Preimage Resistance: Example 12.3

Malcolm has intercepted a signed message (x, v) from Alice. If he can find y with $h(y) = v$ then he can replace x with y and Bob will still verify Alice's signature.

Assume hash values are distributed uniformly at random in $\mathbb{F}_2^r$.

- Given a hash value $v \in \mathbb{F}_2^r$, what is the probability that a random $y \in \mathbb{N}_0$ will have $h(y) = v$?
  (A) $\frac{1}{2^{2r}}$ (B) $\frac{1}{2^r}$ (C) $\frac{1}{2^{r/2}}$ (D) $\frac{1}{2}$
- How many hashes does Malcolm need to compute on average to find y such that $h(y) = v$?
  (A) $2^{r/2}$ (B) 2^{r-1} (C) 2^r (D) 2^{2r}
- What is the distribution of the number of hashes Malcolm computes before finding a suitable y? Answer: geometric with parameter $1/2^r$.

Therefore 'hard to find' in (b) means 'takes about 2^r hashes'.

(b) Given a message $x \in \mathbb{N}_0$, and its hash $h(x)$, it is hard to find $y \in \mathbb{N}_0$ such that $y \neq x$ and $h(y) = h(x)$. (*Preimage resistance.*)

Birthday Paradox

Assume hash values are distributed uniformly at random in $\mathbb{F}_2^r$.

- Given a pair $(x, x') \in \mathbb{N}_0$, what is the probability that $h(x) = h(x')$?

  (A) 0 (B) $\frac{1}{2^r}$ (C) $\frac{1}{2^{r+1}}$ (D) $\frac{1}{2^{2r}}$

- Suppose we hash R distinct numbers, $x^{(1)}, \ldots, x^{(R)}$. How many (unordered) pairs $\{x, x'\}$ with $x \neq x'$ can be made?

  (A) R (B) $\frac{R(R-1)}{2}$ (C) $\frac{R(R+1)}{2}$ (D) $R(R-1)$

- How many numbers do we have to hash before the expected number of collisions $h(x) = h(x')$ is at least 1?

  (A) About 2^r (B) About $2^{r/2}$ (C) About 2^{r-1} (D) Depends on h

Exercise 12.4

Let $h : \mathbb{N}_0 \to \mathbb{F}_2^r$ be a good hash function. On average, how many hashes does an attacker need to calculate to find $x, x' \in \mathbb{N}_0$ with $x \neq x'$ and $h(x) = h(x')$?

Birthday Paradox

Assume hash values are distributed uniformly at random in $\mathbb{F}_2^r$.

- Given a pair $(x, x') \in \mathbb{N}_0$, what is the probability that $h(x) = h(x')$?

  (A) 0 (B) $\frac{1}{2^r}$ (C) $\frac{1}{2^{r+1}}$ (D) $\frac{1}{2^{2r}}$

- Suppose we hash R distinct numbers, $x^{(1)}, \ldots, x^{(R)}$. How many (unordered) pairs $\{x, x'\}$ with $x \neq x'$ can be made?

  (A) R (B) $\frac{R(R-1)}{2}$ (C) $\frac{R(R+1)}{2}$ (D) $R(R-1)$

- How many numbers do we have to hash before the expected number of collisions $h(x) = h(x')$ is at least 1?

  (A) About 2^r (B) About $2^{r/2}$ (C) About 2^{r-1} (D) Depends on h

Exercise 12.4

Let $h : \mathbb{N}_0 \to \mathbb{F}_2^r$ be a good hash function. On average, how many hashes does an attacker need to calculate to find $x, x' \in \mathbb{N}_0$ with $x \neq x'$ and $h(x) = h(x')$?

Birthday Paradox

Assume hash values are distributed uniformly at random in $\mathbb{F}_2^r$.

- Given a pair $(x, x') \in \mathbb{N}_0$, what is the probability that $h(x) = h(x')$?

  (A) 0 (B) $\frac{1}{2^r}$ (C) $\frac{1}{2^{r+1}}$ (D) $\frac{1}{2^{2r}}$

- Suppose we hash R distinct numbers, $x^{(1)}, \ldots, x^{(R)}$. How many (unordered) pairs $\{x, x'\}$ with $x \neq x'$ can be made?

  (A) R (B) $\frac{R(R-1)}{2}$ (C) $\frac{R(R+1)}{2}$ (D) $R(R-1)$

- How many numbers do we have to hash before the expected number of collisions $h(x) = h(x')$ is at least 1?

  (A) About 2^r (B) About $2^{r/2}$ (C) About 2^{r-1} (D) Depends on h

Exercise 12.4

Let $h : \mathbb{N}_0 \to \mathbb{F}_2^r$ be a good hash function. On average, how many hashes does an attacker need to calculate to find $x, x' \in \mathbb{N}_0$ with $x \neq x'$ and $h(x) = h(x')$?

Birthday Paradox

Assume hash values are distributed uniformly at random in $\mathbb{F}_2^r$.

- Given a pair $(x, x') \in \mathbb{N}_0$, what is the probability that $h(x) = h(x')$?

  (A) 0 (B) $\frac{1}{2^r}$ (C) $\frac{1}{2^{r+1}}$ (D) $\frac{1}{2^{2r}}$

- Suppose we hash R distinct numbers, $x^{(1)}, \ldots, x^{(R)}$. How many (unordered) pairs $\{x, x'\}$ with $x \neq x'$ can be made?

  (A) R (B) $\frac{R(R-1)}{2}$ (C) $\frac{R(R+1)}{2}$ (D) $R(R-1)$

- How many numbers do we have to hash before the expected number of collisions $h(x) = h(x')$ is at least 1?

  (A) About 2^r (B) About $2^{r/2}$ (C) About 2^{r-1} (D) Depends on h

Exercise 12.4

Let $h : \mathbb{N}_0 \to \mathbb{F}_2^r$ be a good hash function. On average, how many hashes does an attacker need to calculate to find $x, x' \in \mathbb{N}_0$ with $x \neq x'$ and $h(x) = h(x')$?

Summary of Hash Functions

We can now make precise what 'hard' means in our requirements for a good hash function $h : \mathbb{N}_0 \to \mathbb{F}_2^r$

(a) It is fast to compute $h(x)$.

(b) Given a message $x \in \mathbb{N}_0$, and its hash $h(x)$, it is hard to find $y \in \mathbb{N}_0$ such that $y \neq x$ and $h(y) = h(x)$. (*Preimage resistance.*)

- By Example 12.3, 'hard' means that the attacker must compute about 2^r hashes to find y.

(c) It is hard to find a pair (x, x') with $x \neq x'$ such that $h(x) = h(x')$. (*Collision resistance.*)

- By Exercise 12.4, 'hard' means that the attacker must compute about $2^{r/2}$ hashes to find x'.

Hash Functions In Practice

A block cipher with keyspace $\mathbb{F}_2^\ell$ and block size n can be used as a hash function. Fix an initialisation state $z^{(0)} \in \mathbb{F}_2^n$. Chop the message x (assumed converted to binary) into binary words $x^{(1)}$, $x^{(2)}$, ..., $x^{(t)} \in \mathbb{F}_2^\ell$. Then use the block cipher with *keys* $x^{(i)}$, starting with $z^{(0)} \in \mathbb{F}_2^\ell$ as follows:

$$\begin{aligned} z^{(1)} &= z^{(0)} + e_{x^{(1)}}(z^{(0)}) \\ z^{(2)} &= z^{(1)} + e_{x^{(2)}}(z^{(1)}) \\ &\vdots \\ z^{(t)} &= z^{(t-1)} + e_{x^{(t)}}(z^{(t-1)}) \end{aligned}$$

The final state $z^{(t)} \in \mathbb{F}_2^r$ depends on the entire message x in a complicated way, so is a good choice for $h(x)$. Using RSA, Alice sends the signed message $\big(x, d_A\big(h(x)\big)\big)$.

- Should the initialization vector $z^{(0)}$ be secret?

(A) No (B) Yes

Hash Functions In Practice

A block cipher with keyspace $\mathbb{F}_2^\ell$ and block size n can be used as a hash function. Fix an initialisation state $z^{(0)} \in \mathbb{F}_2^n$. Chop the message x (assumed converted to binary) into binary words $x^{(1)}$, $x^{(2)}$, ..., $x^{(t)} \in \mathbb{F}_2^\ell$. Then use the block cipher with *keys* $x^{(i)}$, starting with $z^{(0)} \in \mathbb{F}_2^\ell$ as follows:

$$\begin{aligned} z^{(1)} &= z^{(0)} + e_{x^{(1)}}(z^{(0)}) \\ z^{(2)} &= z^{(1)} + e_{x^{(2)}}(z^{(1)}) \\ &\vdots \\ z^{(t)} &= z^{(t-1)} + e_{x^{(t)}}(z^{(t-1)}) \end{aligned}$$

The final state $z^{(t)} \in \mathbb{F}_2^r$ depends on the entire message x in a complicated way, so is a good choice for $h(x)$. Using RSA, Alice sends the signed message $\big(x, d_A\big(h(x)\big)\big)$.

- Should the initialization vector $z^{(0)}$ be secret?

(A) No (B) Yes

No, since a receiver of the message x needs to know $z^{(0)}$ in order to verify the hash.

Block Ciphers as Hash Functions

Recall that to hash a message x (in binary) we chop x into binary words $x^{(1)}, x^{(2)}, \ldots, x^{(\ell)} \in \mathbb{F}_2^\ell$, such that each $x^{(i)} < 2^r$ and then use the block cipher with *keys* $x^{(i)}$, starting with $z^{(0)} \in \mathbb{F}_2^\ell$ as follows:

$$\begin{aligned} z^{(1)} &= z^{(0)} + e_{x^{(1)}}(z^{(0)}) \\ z^{(2)} &= z^{(1)} + e_{x^{(2)}}(z^{(1)}) \\ &\vdots \\ z^{(t)} &= z^{(t-1)} + e_{x^{(t)}}(z^{(t-1)}) \end{aligned}$$

to get the hash value $z^{(t)} \in \mathbb{F}_2^r$.

Exercise 12.5

Suppose that we use AES (with 128-bit keys) to hash a message $x \in \mathbb{F}_2^{128}$, using the initialisation state $z^{(0)} = 0 \ldots 0 \in \mathbb{F}_2^{128}$. Then only one step is needed above and the hash value is $h(x) = e_x(0 \ldots 0)$. An adversary therefore knows the plaintext $0 \ldots 0$ and its encryption using x as the key. Why is it hard for her to find x?

Coin-flips by Email

Example 12.6

Alice flips a coin and records the result. Bob guesses heads or tails and Alice informs him whether he is correct. If the two can communicate only by email, how can Bob be sure that Alice does not falsely claim that the flip is the opposite of Bob's guess?

This was demonstrated in an early Q&A session: see the answer posted to the Moodle Forum.

SHA-256

Example 12.7 (SHA-256)

SHA-256 is the most commonly used hash function today. It has length 256. There is an internal state of 256 bits, divided into 8 blocks of 32 bits.

The blocks are combined with each other by multiplying bits in the same positions (this is 'logical and'), addition in $\mathbb{F}_2^{32}$, cyclic shifts (like an LFSR), and addition modulo 2^{32}, over 64 rounds.

The best attack can break (b) when the number of rounds is reduced to 57, and (c) reducing the rounds further to 46.

SHA-256

Example 12.7 (SHA-256)

SHA-256 is the most commonly used hash function today. It has length 256. There is an internal state of 256 bits, divided into 8 blocks of 32 bits.

The blocks are combined with each other by multiplying bits in the same positions (this is 'logical and'), addition in $\mathbb{F}_2^{32}$, cyclic shifts (like an LFSR), and addition modulo 2^{32}, over 64 rounds.

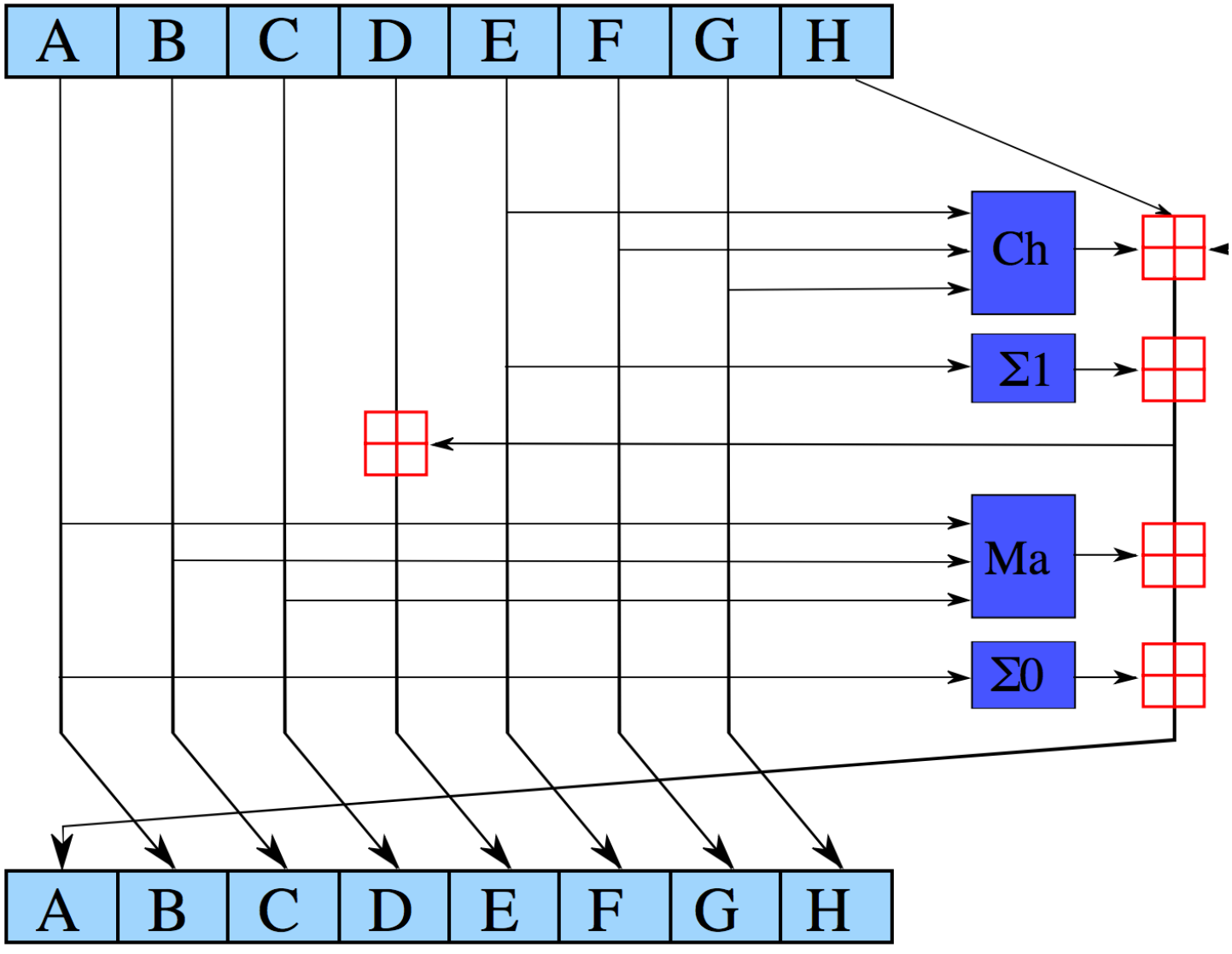
The best attack can break (b) when the number of rounds is reduced to 57, and (c) reducing the rounds further to 46.

A draft of the questions in this year's MT362 exam will be posted to Moodle. It has been encrypted using AES in ECB mode: the key is the first 128 bits of the **SHA-512** hash of the lecturer's password. The SHA-256 hash of this password is

`170972f840215582a876e057f7b22ff662d77e94526df8e1f57c854ccd29c6c5`

Here each of the 64 digits is a hexadecimal digit representing 4 bits. The decimal form is in the Part A Slides.

Wiring Diagram for SHA256



Hashing Passwords — Optional

When you create an account online, you typically choose a username, let us say 'Alice' and a password, say 'alicepassword'. A well run website will not store your password. Instead, oversimplifying slightly, your password is converted to a number x and the SHA-256 hash $h(x)$ is stored. By (b), it is hard for anyone to find another word whose hash is also $h(x)$.

Provided your password is hard to guess, your account is secure, and you have avoided telling the webmaster your password.

Exercise 12.8

As described, it will be obvious to a hacker who has access to the password database when two users have the same password. Moreover, if you use the same password on two different sites, the same hash will be stored on both. How can this be avoided?

Example 12.9 (Bitcoin Blockchain — Optional)

The bitcoin blockchain is a distributed record of all transactions involving bitcoins. When Alice transfers a bitcoin b to Bob, she appends a message x to his bitcoin, saying 'I Alice give Bob the bitcoin b', and signs this message, by appending $d_a(h(x))$.

Signing the message ensures that only Alice can transfer Alice's bitcoins. But as described so far, Alice can double-spend: a few minutes later she can sign another message $\big(x', d_a(h(x'))\big)$ where x' says 'I Alice give Charlie the bitcoin b'.

To avoid this, transactions are *validated*. To validate a list of transactions

$$\big(b^{(1)}, x^{(1)}, d_{a^{(1)}}(h(x^{(1)}))\big), \big(b^{(2)}, x^{(2)}, d_{a^{(2)}}(h(x^{(2)}))\big), \ldots$$

a *miner* searches for $c \in \mathbb{N}$ such that, when this list is converted to a number, its hash, by two iterations of SHA-256, has a large number of initial zeros.

Example 12.9 [continued]

When Bob receives $\big(b, x', d_a(h(x'))\big)$, he looks to see if there is a block already containing a transaction involving b. When Bob finds $(b, x, d_a(h(x)))$ as part of a block with the laboriously computed c, Bob knows Alice has cheated.

Vast numbers of hashes must be computed to grow the blockchain. Miners are incentivized to do this: the reward for growing the blockchain is given in bitcoins.

This time in 2019 the bitcoin traded at \$7415.64; in 2018 it was at \$3245.00, in 2017 it was at a (then) near record high of \$15879.79. This year it is \$19,145.10. The reward for growing the blockchain is 12.5 bitcoins. (This gradually decreases; there will never be more than 21×10^6 bitcoins in circulation.) Most transactions therefore involve small fractions of a bitcoin. A typical block verifies about 2500 separate transactions.

Miners are further incentivized by transaction fees, again paid in bitcoins, attached to each transaction. These will become more important as the per block reward gets smaller.