MT362/462/5462 Cipher Systems

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

Administration:

- Sign-in sheet. **Please return to the lecturer after each lecture.**
- Make sure you get the Part A Notes and preliminary problem sheet.
- **Please take a clicker and use it!**
- Please form a four-person 'block' following instructions on form. Return one form per block to the lecturer; do not keep any forms.
- All handouts will be put on Moodle. The first marked problem sheet will be on Moodle by Wednesday.
- **Lectures:** Monday 5pm (ALT2), Friday 11am (McCrea 2-01), Friday 4pm (BLT2).
- **Extra lecture for MT5462:** Thursday 1pm (MFoxSem).
- **Drop-in times in McCrea LGF025:** Tuesday 3.30pm, Wednesday 11am, Thursday 11.30am.

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

§1 Introduction: Security and Kerckhoff'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 Kerckhoff'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 Kerckhoff'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

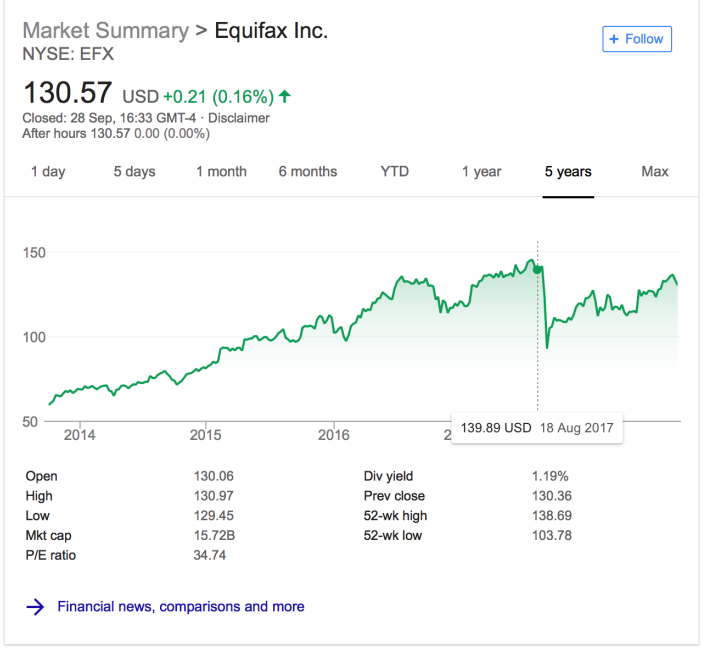
In fact they are sent a 'hash' of your password: see Part D of the course. For instance, the SHA-256 hash of the password used to encrypt this year's exam is

10419890632902139458456423619801507446386374951765933585
629283702295140878021.

Cryptography Matters!

What do the following have in common?

- Mary, Queen of Scots (1542 – 1587)
- The Equifax share price in September 2017
- Satoshi Nakamoto
- Edward Snowden?



Administration

- Sign-in sheet. **Please return to the lecturer after each lecture.**
- Please take pages 9 to 14 of the printed notes.
- Please take Problem Sheet 1. It is due in next Friday: you should be able to do the compulsory questions after today's lecture.
- There are eight problem sheets, each worth 1.25% of your exam mark.
- If you did not do so on Monday, please form a four person block. Fill out the small form. **One form per block.**
- You **must** be in a block to do the problem sheets.
- Spare copies of Monday's handouts at the front.

§2 Alphabetic Ciphers

Example 2.1

The *Caesar cipher* with key $s \in \{0, 1, \ldots, 25\}$ encrypts a word by shifting each letter s 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

Example 2.3

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

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

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

Exercise 2.4

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?

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

(A) No (B) Yes

Substitution Ciphers

Example 2.3

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

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

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

Exercise 2.4

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?

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

(A) No (B) Yes

Substitution Ciphers

Example 2.3

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

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

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

Exercise 2.4

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?

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

(A) No (B) Yes

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 `AlphabeticCiphers` 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 `AlphabeticCiphers` on Moodle to do the donkey work.

Frequency distribution of English, probability 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

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 `AlphabeticCiphers` on Moodle to do the donkey work.

Frequencies of ciphertext letters as percentages.

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

This morning we used frequency analysis to find that the plaintext in Example 2.5′, shown with ciphertext below, is

```
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

This morning we used frequency analysis to find that the plaintext in Example 2.5′, shown with ciphertext below, is

```
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

This morning we used frequency analysis to find that the plaintext in Example 2.5′, shown with ciphertext below, is

```
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

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

(A) No (B) Yes

(c) Suppose Mark can encrypt a plaintext of his choice using e_π. What is the simplest way for him to learn π?

This morning we used frequency analysis to find that the plaintext in Example 2.5′, shown with ciphertext below, is

```
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

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

(A) No (B) Yes

(c) Suppose Mark can encrypt a plaintext of his choice using e_π. What is the simplest way for him to learn π?

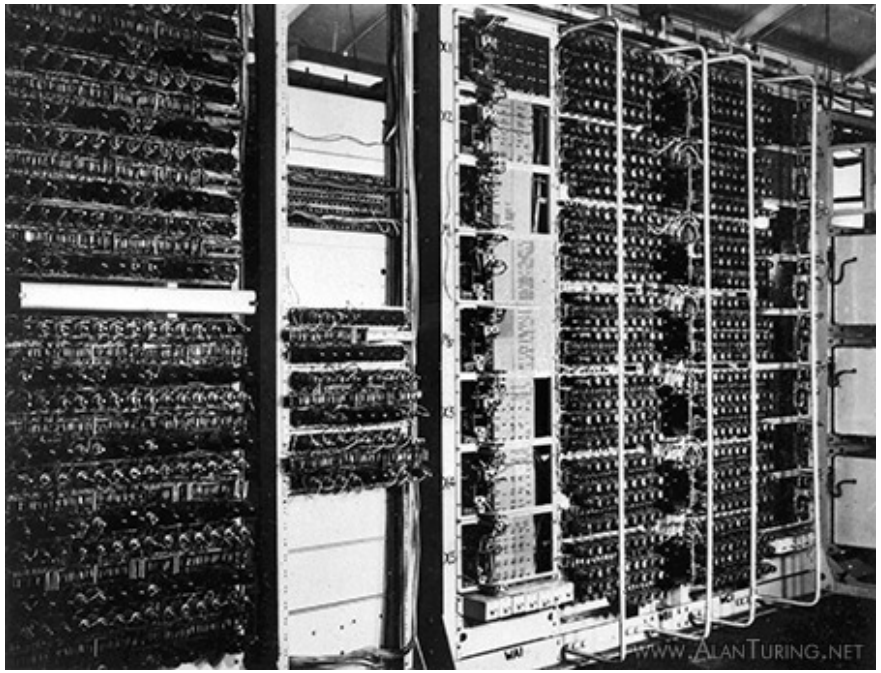
In Praise of Programming

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 τ, that is partially correct, and then improve it step-by-step by looking at the decrypt $e_\tau^{-1}(y)$ implied by this key.

Example′ 2.7

To automate this process we need a way to measure the 'Englishy-ness' of a decrypt . . . [see printed notes for details]

Exercise 2.8

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

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,

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

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,

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

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,

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

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,

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

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

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

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 $k = \texttt{emu}$, so k has length 3. Under the bijection between letters and numbers, $\texttt{emu} \longleftrightarrow (4, 12, 20)$. The table below shows that

$$e_{\texttt{emu}}(\texttt{meetatmidnightnear}) = \texttt{QQYXMNQUXRUALFHIML}.$$

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	e	m	u	e	m	u	e	m	u	e	m	u	e	m	u	e	m	u
	4	12	20	4	12	20	4	12	20	4	12	20	4	12	20	4	12	20
$x_i + k_i$	16	16	24	23	12	13	16	20	23	17	20	0	11	5	7	8	12	11
	Q	Q	Y	X	M	N	Q	U	X	R	U	A	L	F	H	I	M	L

A Weakness in the Vigenère Cipher

Exercise 2.11

(i) If you had to guess, which sample below would you say was more likely to be the ciphertext from a substitution cipher?

(A) KDDLVFUDLNELUHLYJAWLWGLWUJDULF
(B) KYBDRDDFCLVCVEDFLDUVYDKKLZCNPO
(C) KYEYAXBICDMBRFXDLCDPKFXLCILLMO

(A) (B) (C)

Each sample has 30 characters. The ten most frequent letters, with frequencies, and the total frequency of the rest are:

L	U	D	W	J	F	Y	V	N	K	the rest
7	4	4	3	2	2	1	1	1	1	3

D	V	L	K	C	Y	F	Z	U	R	the rest
6	3	3	3	3	2	2	1	1	1	5

L	X	D	C	Y	M	K	I	F	B	the rest
4	3	3	3	2	2	2	2	2	2	5

A Weakness in the Vigenère Cipher

Exercise 2.11

(i) If you had to guess, which sample below would you say was more likely to be the ciphertext from a substitution cipher?

(A) `KDDLVFUDLNELUHLYJAWLWGLWUJDULF`
(B) `KYBDRDDFCLVCVEDFLDUVYDKKLZCNPO`
(C) `KYEYAXBICDMBRFXDLCDPKFXLCILLMO`

(A) (B) (C)

Each sample has 30 characters. The ten most frequent letters, with frequencies, and the total frequency of the rest are:

L	U	D	W	J	F	Y	V	N	K	the rest
7	4	4	3	2	2	1	1	1	1	3

D	V	L	K	C	Y	F	Z	U	R	the rest
6	3	3	3	3	2	2	1	1	1	5

L	X	D	C	Y	M	K	I	F	B	the rest
4	3	3	3	2	2	2	2	2	2	5

A Weakness in the Vigenère Cipher

Exercise 2.11

(i) If you had to guess, which sample below would you say was more likely to be the ciphertext from a substitution cipher?

(A) `KDDLVFUDLNELUHLYJAWLWGLWUJDULF`
(B) `KYBDRDDFCLVCVEDFLDUVYDKKLZCNPO`
(C) `KYEYAXBICDMBRFXDLCDPKFXLCILLMO`

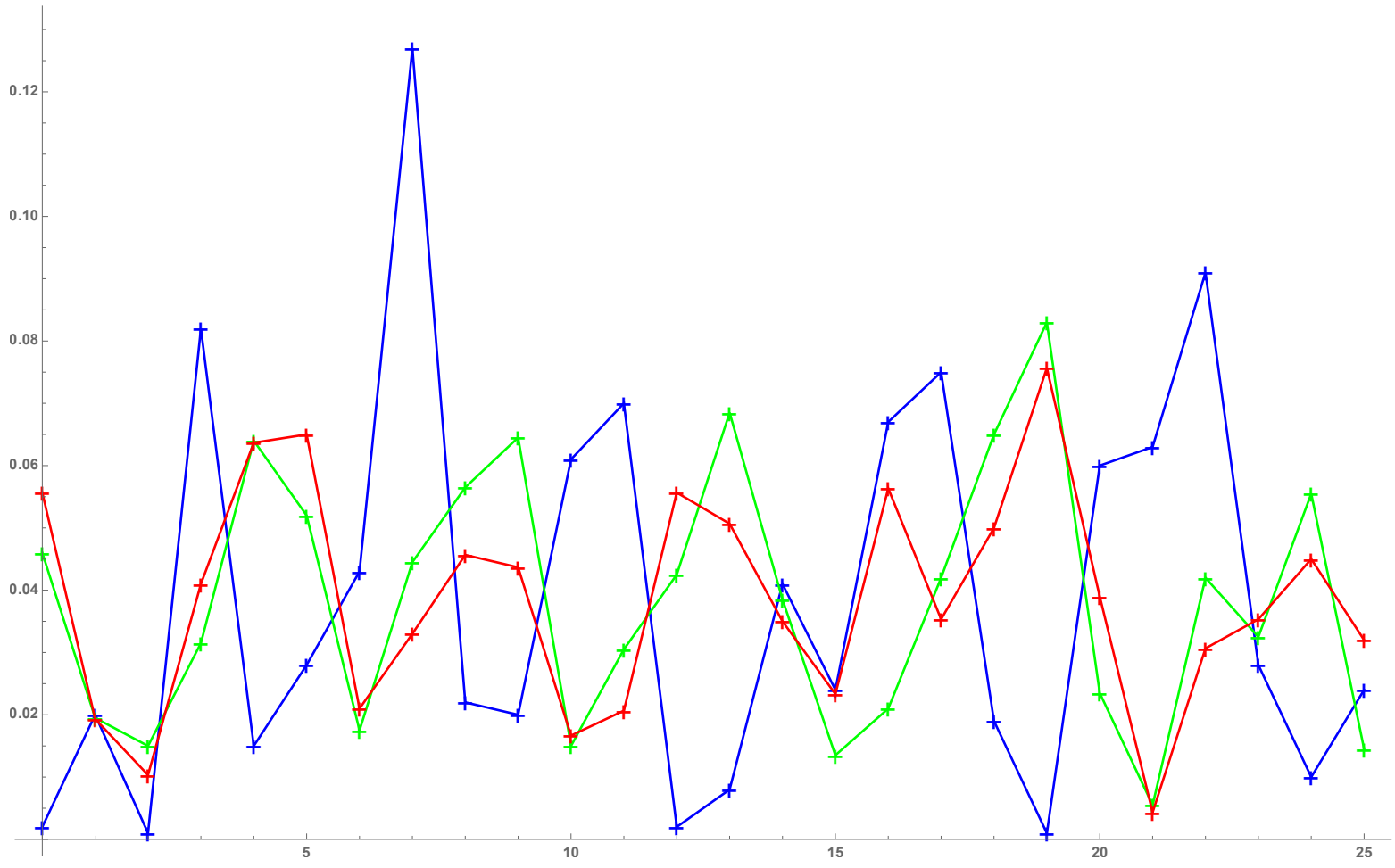
(A) (B) (C)

(ii) The samples are obtained by taking every 9th, every 3rd and every position in an English plaintext encrypted using a Vigenère cipher.

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: last Friday you saw the averaged relative frequencies for one, two and three Caesar shifts.

Averaged relative frequencies for one, two and three Caesar shifts applied to a long English text



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 $I(\texttt{QMUUFM}) = \frac{2}{15}$. What is $I(\texttt{AAABBC})$?

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

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 $I(\texttt{QMUUFM}) = \frac{2}{15}$. What is $I(\texttt{AAABBC})$?

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

There is a simple formula for $I(y)$. (An examinable proof.)

Lemma 2.14

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

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

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 $k_{\ell-1}$.

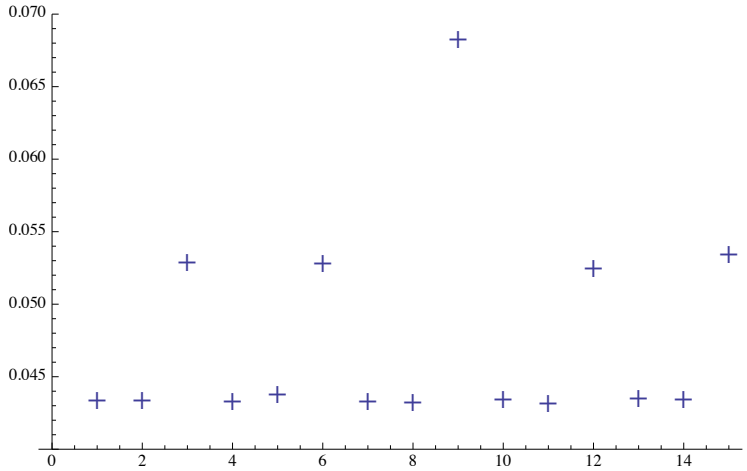
Example 2.16

The following ciphertext is the output of a Vigènre cipher:

`KYEYAXBICDMBRFXDLCDPKFXLCILLMOVRMCE ...`

(The full ciphertext is in the printed notes and the MATHEMATICA notebook `VigenereAustenExample.nb` on Moodle.)

Index of Coincidence versus *Persuasion* extract



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

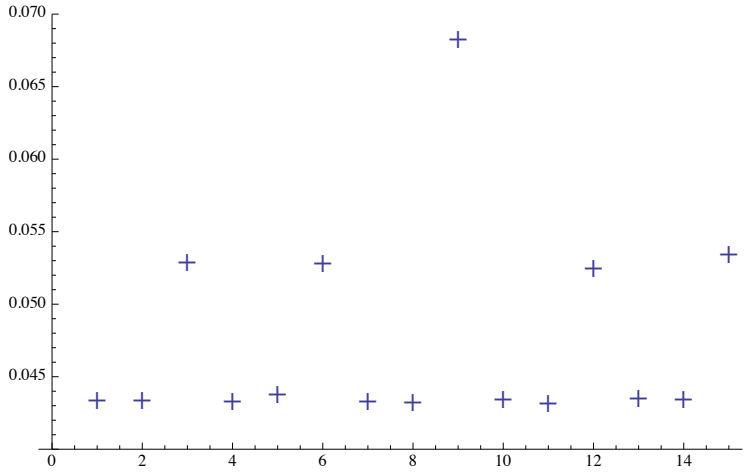
$$y_0 y_9 y_{18} \ldots = \text{`KDDLVFUDLNELUHLYJA}\ldots\text{'}$$

This is the first sample in the quiz at the start of the lecture. The frequency table (as in Example 2.5) begins

W	L	S	K
11.0	10.6	7.4	7.1

Assuming ‘W‘ $\longleftrightarrow$ 22 is the encryption of ‘e‘ $\longleftrightarrow$ 4, the shift in the Caesar cipher is 18 $\longleftrightarrow$ ‘s‘, so we guess the first letter of the key is ‘s’. The MATHEMATICA notebooks shows this finds all the key.

Index of Coincidence versus *Persuasion* extract



Exercise 2.17

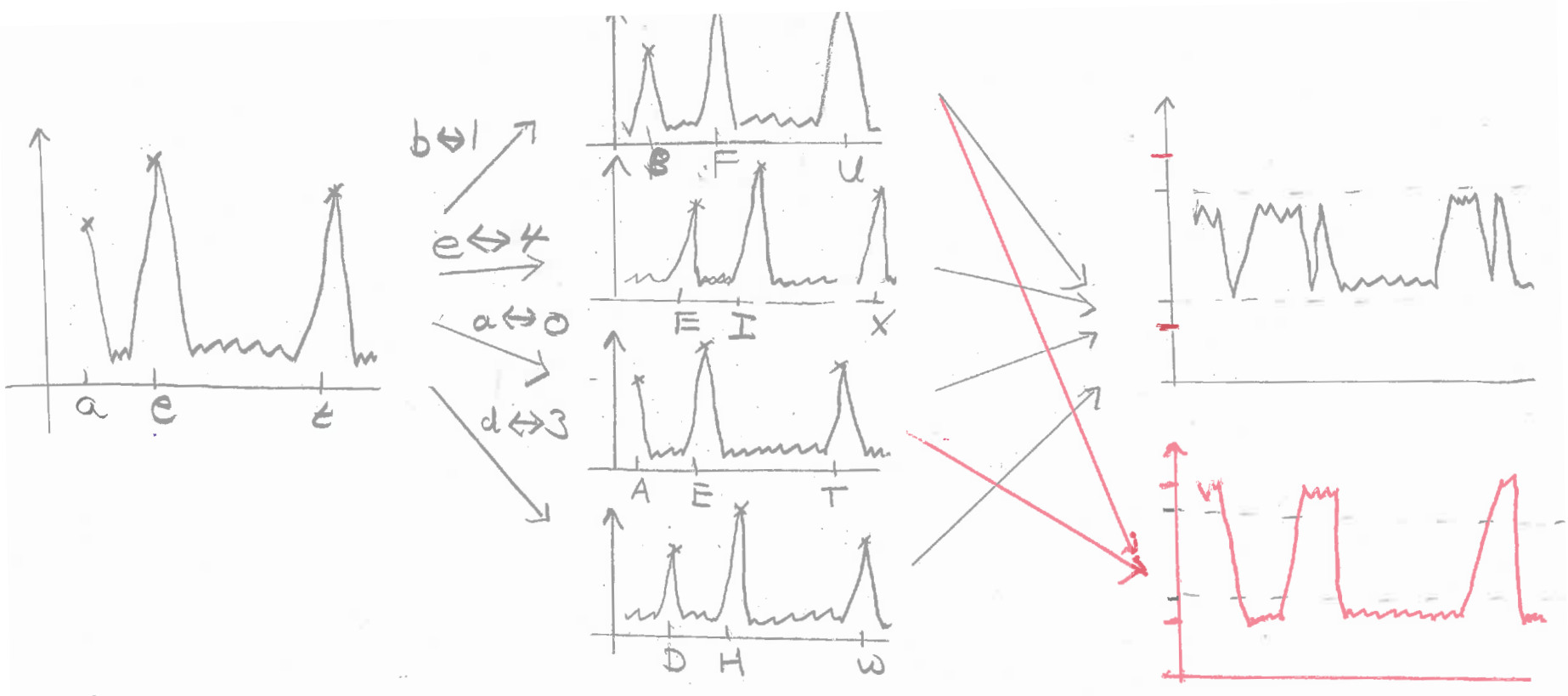
Explain why there are smaller peaks at 3, 6, 12 and 15 in the plot of Indices of Coincidence above.

The next slides have the graphs drawn in lectures for the similar case when the key has length 4 and a quiz on the Vigenère Cipher.

Vigenère Cipher with Key 'bead' of Length 4

To simplify the graphs, we imagine that English has common letters 'a' 'e' 't' and all other letters are rare. On the far right:

- Black: full ciphertext: see all 4 shifts
- Red: split ciphertext taking every other position: see 2 shifts



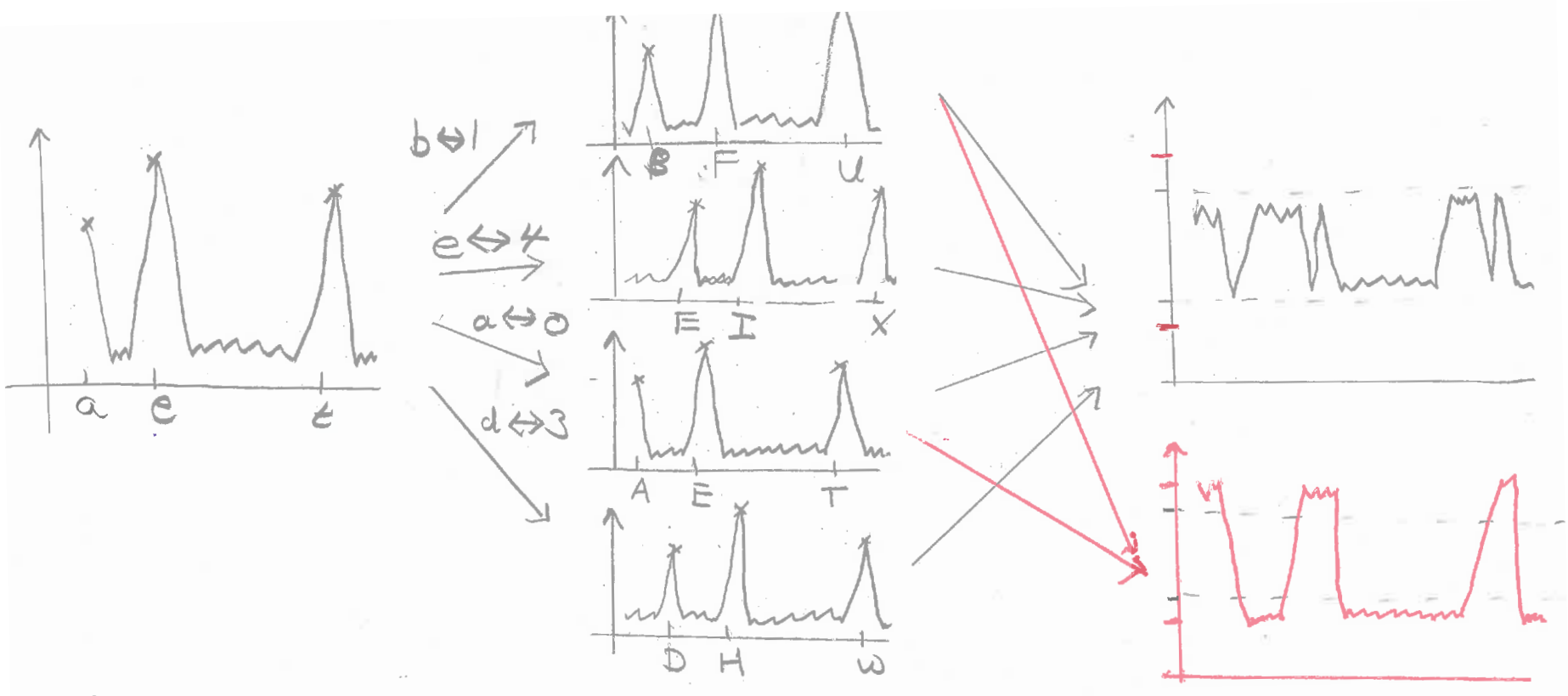
Suppose we split the ciphertext taking every third position. What will the frequency graph look more like?

(A) black (B) red

Vigenère Cipher with Key 'bead' of Length 4

To simplify the graphs, we imagine that English has common letters 'a' 'e' 't' and all other letters are rare. On the far right:

- Black: full ciphertext: see all 4 shifts
- Red: split ciphertext taking every other position: see 2 shifts



Suppose we split the ciphertext taking every third position. What will the frequency graph look more like?

(A) black (B) red

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

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

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

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

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

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

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

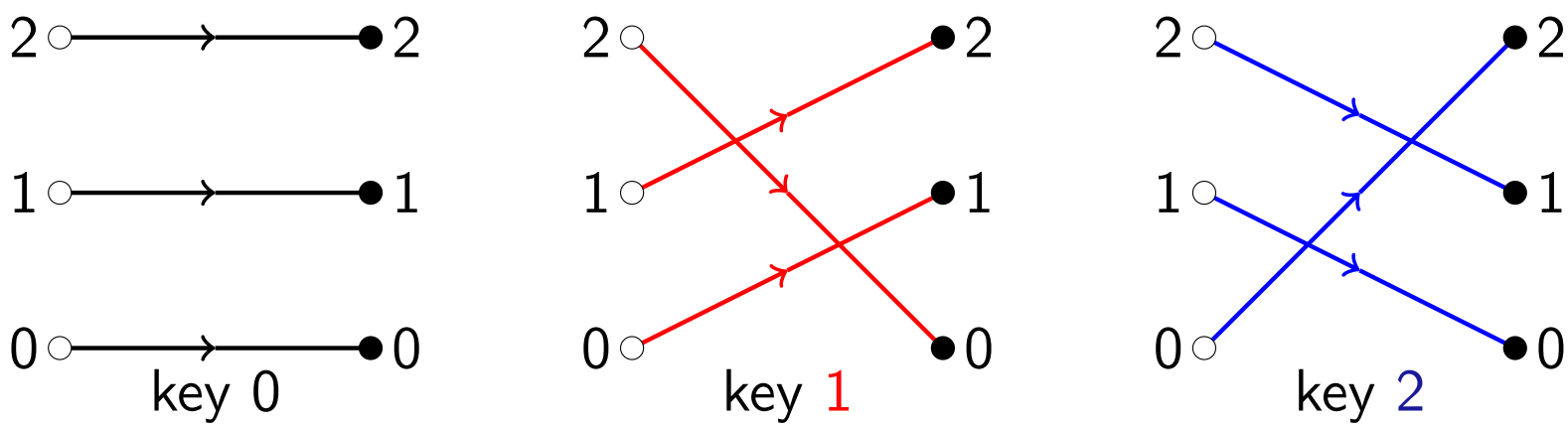
Problem Sheet 1

- 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 wish, you can then submit your answer to Q3 on Monday for full credit.
- If you have problems with `AlphabeticCiphers.nb`, or any other notebook in the course, please:
  - Quit MATHEMATICA
  - Download a fresh copy of the notebook from Moodle.
    Rename `AlphabeticCiphers.nb.txt` to `AlphabeticCiphers.nb` if necessary.
    This is a Moodle bug affecting Safari on Mac OS X and maybe other browsers.
  - Restart MATHEMATICA
  - Load the fresh copy of `AlphabeticCiphers.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.
- Following the steps above may help with Question 5 about the Vigenère Cipher. If you are confused on (e) see Exercise 2.17 and the quiz just before this slide. Slides are on Moodle.

§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 $k \in K$,

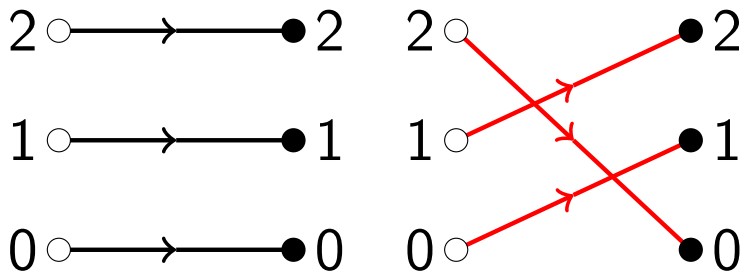
$$d_k\big(e_k(x)\big) = x \qquad (\star)$$

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*.

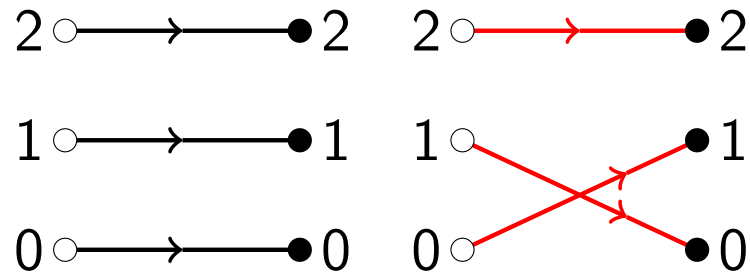
Exercise 3.2

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

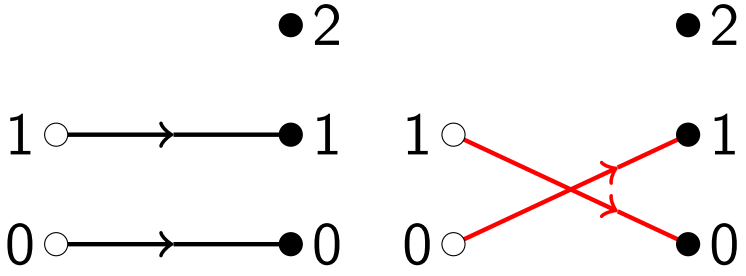
(i)



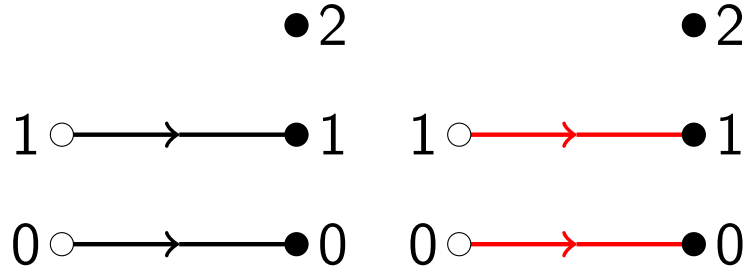
(ii)



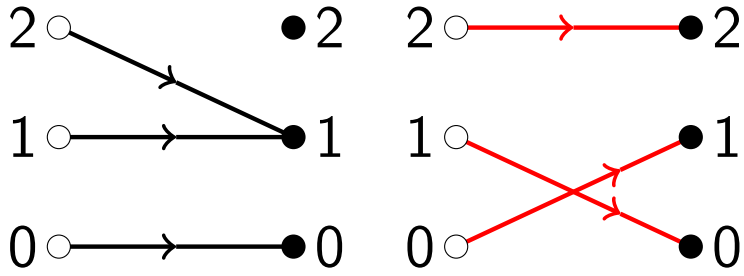
(iii)



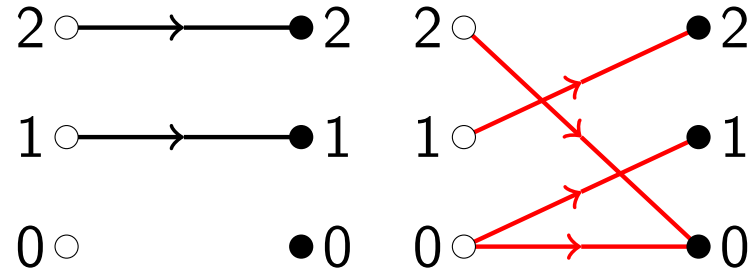
(iv)



(v)



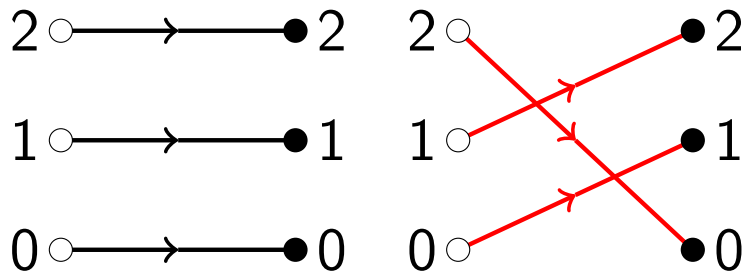
(vi)



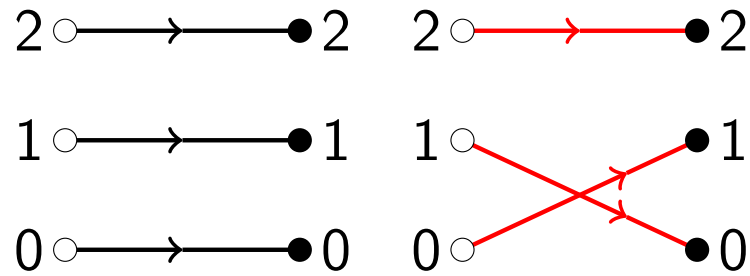
Exercise 3.2

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

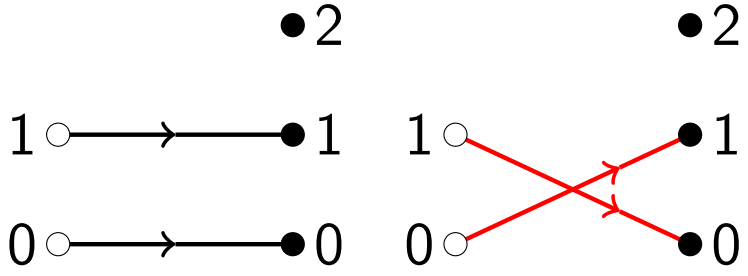
(i)



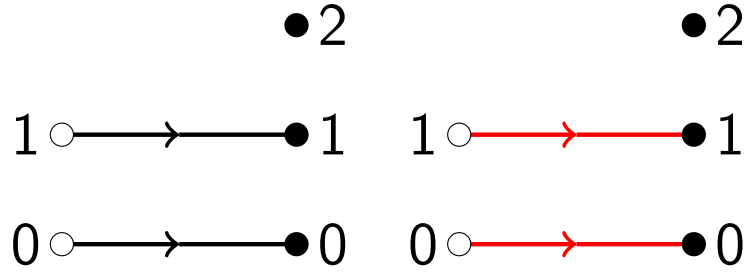
(ii)



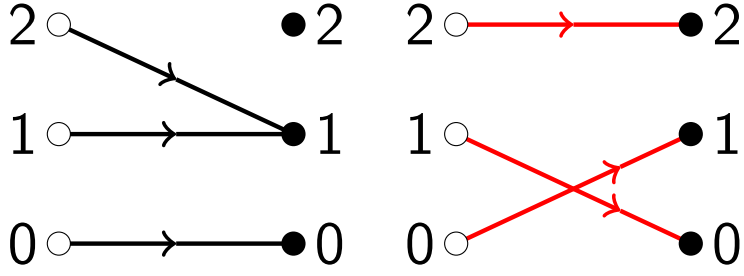
(iii)



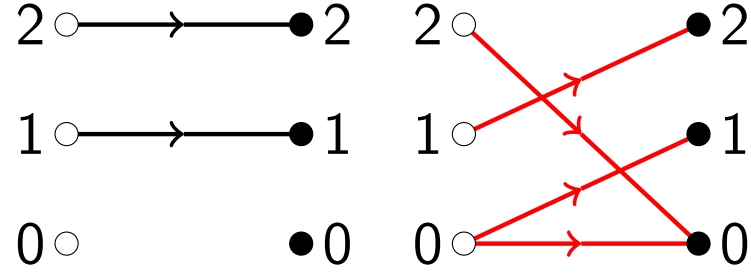
(iv)



(v)



(vi)



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 3.3

(i) Show that e_k is injective for each $k \in \mathcal{K}$.

(ii) 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?

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

(iv) 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 . . .

- the encryption functions determine the decryption functions.

  (A) False (B) True

- the decryption functions are surjective

  (A) False (B) True

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

  (A) False (B) True

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

  (A) False (B) True

Finally, true or false: a cryptosystem may have keys $k, k' \in \mathcal{K}$ such that $e_k(x) = e_{k'}(x')$ for distinct $x, x' \in \mathcal{P}$.

(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 . . .

- the encryption functions determine the decryption functions.

  (A) False (B) True

- the decryption functions are surjective

  (A) False (B) True

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

  (A) False (B) True

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

  (A) False (B) True

Finally, true or false: a cryptosystem may have keys $k, k' \in \mathcal{K}$ such that $e_k(x) = e_{k'}(x')$ for distinct $x, x' \in \mathcal{P}$.

(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 . . .

- the encryption functions determine the decryption functions.

  (A) False (B) True

- the decryption functions are surjective

  (A) False (B) True

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

  (A) False (B) True

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

  (A) False (B) True

Finally, true or false: a cryptosystem may have keys $k, k' \in \mathcal{K}$ such that $e_k(x) = e_{k'}(x')$ for distinct $x, x' \in \mathcal{P}$.

(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 . . .

- the encryption functions determine the decryption functions.

  (A) False (B) True
- the decryption functions are surjective

  (A) False (B) True
- if $k \in \mathcal{K}$ and x, x' are distinct plaintexts then $e_k(x) \neq e_k(x')$.

  (A) False (B) True
- if $x \in \mathcal{P}$ and k, k' are distinct keys then $e_k(x) \neq e_{k'}(x)$.

  (A) False (B) True

Finally, true or false: a cryptosystem may have keys $k, k' \in \mathcal{K}$ such that $e_k(x) = e_{k'}(x')$ for distinct $x, x' \in \mathcal{P}$.

(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 . . .

- the encryption functions determine the decryption functions.

  (A) False (B) True

- the decryption functions are surjective

  (A) False (B) True

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

  (A) False (B) True

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

  (A) False (B) True

Finally, true or false: a cryptosystem may have keys $k, k' \in \mathcal{K}$ such that $e_k(x) = e_{k'}(x')$ for distinct $x, x' \in \mathcal{P}$.

(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 . . .

- the encryption functions determine the decryption functions.

  (A) False (B) True

- the decryption functions are surjective

  (A) False (B) True

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

  (A) False (B) True

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

  (A) False (B) True

Finally, true or false: a cryptosystem may have keys $k, k' \in \mathcal{K}$ such that $e_k(x) = e_{k'}(x')$ for distinct $x, x' \in \mathcal{P}$.

(A) False (B) True

Numeric one-time pad

Example 3.4 (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 3.3(iii), each e_k is a bijection, and the decryption functions are $d_k = e_k^{-1}$. Explicitly, $d_k(y) = (y - k) \bmod n$.

Numeric one-time pad

Example 3.4 (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 3.3(iii), 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 $n = 100$.

- In the first lecture, Eve observed the ciphertext 80.
- The plaintext is x if and only if the key is $(80 - x) \bmod 100$.
- If each key is equally likely then it seems reasonable to say that Eve learns nothing about the plaintext.

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 3.5

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

Conditional Probability

We will need the formula for conditional probability:

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

Quiz. Is this formula intuitive to you?

(A) Yes (B) No

Conditional Probability

We will need the formula for conditional probability:

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

Quiz. Is this formula intuitive to you?

(A) Yes (B) No

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 two heads, given that at least one flip was a head?

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

Conditional Probability

We will need the formula for conditional probability:

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

Quiz. Is this formula intuitive to you?

(A) Yes (B) No

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 two heads, given that at least one flip was a head?

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

Conditional Probability

We will need the formula for conditional probability:

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

Quiz. Is this formula intuitive to you?

(A) Yes (B) No

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 two heads, given that at least one flip was a head?

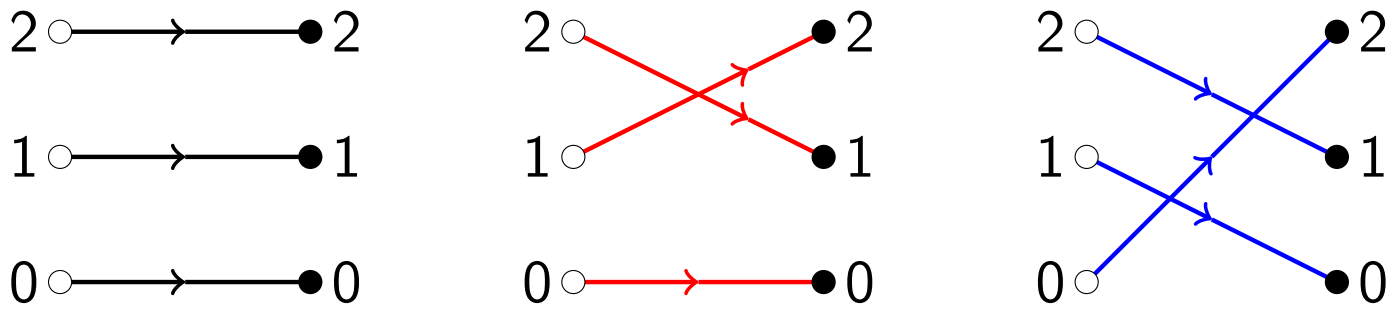
(A) 2/3 (B) 1/3 (C) 1/2 (D) 1/6

We can prove this by restricting the probability space to $B = \{\mathrm{HH}, \mathrm{HT}, \mathrm{TH}\}$ and then finding the probability, in the restricted probability space, of $A = \{\mathrm{HH}\}$.

This agrees with the definition of conditional probability.

Probability Model: Example 3.6

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) $r_{\text{black}} + r_{\text{red}}$

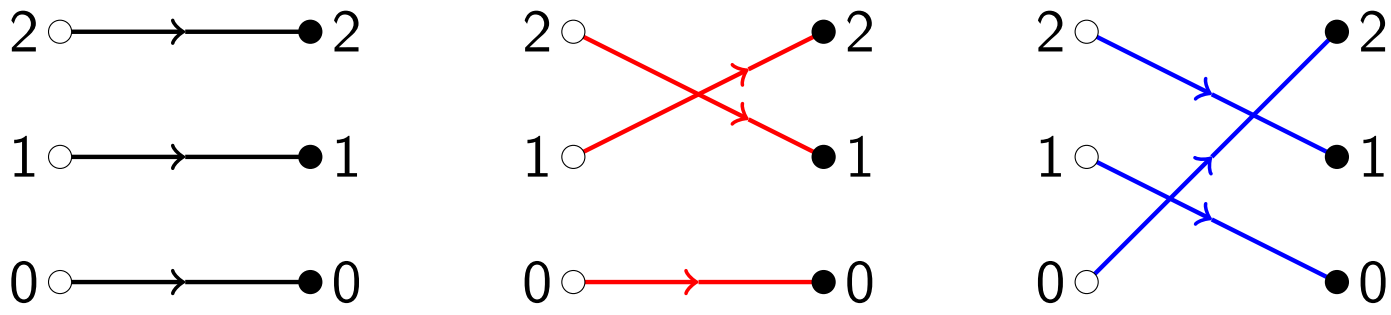
(2) Suppose that the three keys are used with equal probability $\frac{1}{3}$, and that $p_1 = 1 - q$, $p_2 = q$ so $p_0 = 0$.

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

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

Probability Model: Example 3.6

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) $r_{\text{black}} + r_{\text{red}}$

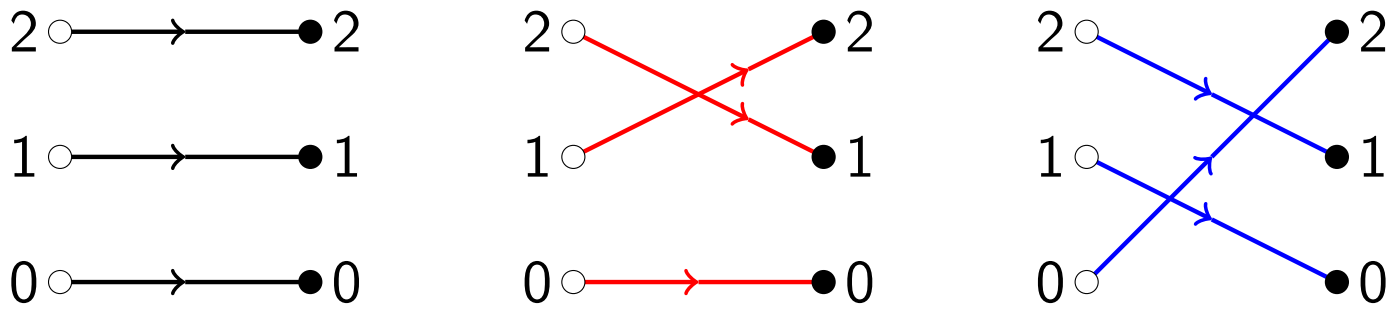
(2) Suppose that the three keys are used with equal probability $\frac{1}{3}$, and that $p_1 = 1 - q$, $p_2 = q$ so $p_0 = 0$.

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

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

Probability Model: Example 3.6

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

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

Feedback on Sheet 1

- Surname A–L: green folder
- Surname M–Y: pink folder
- The sheet was marked out of 16. There is also a 0 or 1 mark (in the box) for making a reasonable attempt: a 1 contributes 1.25% of your final exam mark.
- You can check your marks so far by emailing me `mark.wildon@rhul.ac.uk`.
- Answers and feedback on Sheet 1 are available on Moodle. You may find the 'common errors' or 'rarer errors' instructive even if you did not make them yourself.
- We will go through the hard bit of Question 5 in this lecture. The slides below will be left permanently at the end of §2.

Example 3.7

Consider the numeric one-time pad in Example 3.4, 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 3.8, the one-time pad has perfect secrecy.)

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

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

Thus the probability distribution $\mathbb{P}[K = k|Y = y]$ for k varying is a shift of the probability distribution $\mathbb{P}[X = x]$ on plaintexts. Unavoidably, Eve learns something about the key. If however each plaintext is equally likely, then Eve learns nothing.

Perfect Secrecy

Definition 3.8

Fix a cryptosystem with the usual notation and a probability distribution on the keys.

(i) Let p_x for $x \in X$ be a probability distribution on the plaintexts. 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 3.7 the one-time pad on $\mathbb{Z}_n$ has perfect secrecy when keys are used with equal probability.

Shannon's Theorem: Preliminaries

We say a cryptosystem and probability distribution on keys is *practical* if $\mathbb{P}[K = k] > 0$ 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 $e_k(x) = y$.

Exercise 3.9

Why are these reasonable assumptions to make?

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

Shannon's Theorem: Preliminaries

We say a cryptosystem and probability distribution on keys is *practical* if $\mathbb{P}[K = k] > 0$ 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 $e_k(x) = y$.

Exercise 3.9

Why are these reasonable assumptions to make?

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

Shannon's Theorem

Recall that a cryptosystem and probability distribution on keys is *practical* if $\mathbb{P}[K = k] > 0$ 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 3.10 (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 $e_k(x) = y$. Moreover each key is used with equal probability.*

Proof of Theorem 3.10

Theorem 3.10 (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 $y \in \mathcal{C}$ with $\mathbb{P}[Y = y] > 0$.

- The condition $\mathbb{P}[Y = y] > 0$ is annoying. Is there a hypothesis we could use to remove it?

Proof of Theorem 3.10

Theorem 3.10 (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 $y \in \mathcal{C}$ with $\mathbb{P}[Y = y] > 0$.
- The condition $\mathbb{P}[Y = y] > 0$ is annoying. Is there a hypothesis we could use to remove it?
- Okay, so now 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?

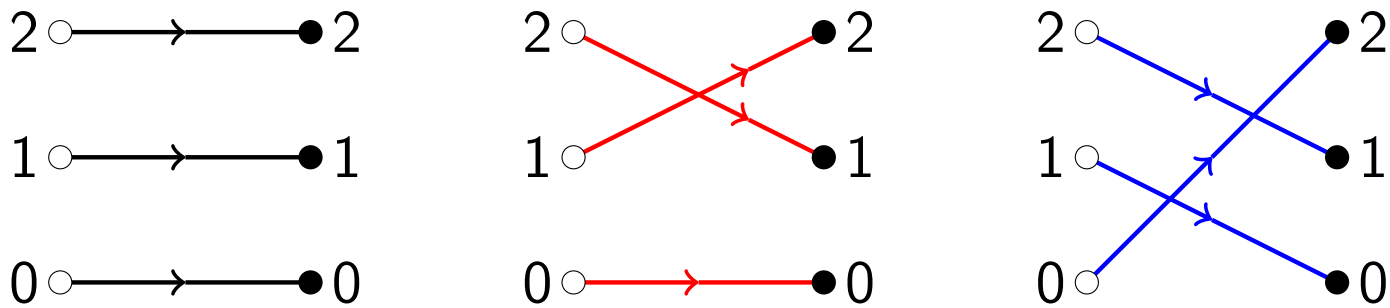
Theorem 3.10 (Shannon 1949)

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 $x \in \mathbb{P}$ and $y \in \mathcal{C}$ the events $X = x$ and $Y = y$ are independent and both have positive probability.

- In Example 3.6 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 we choose a key such that $e_k(x) = y$. Use this to prove (b).

Theorem 3.10 (Shannon 1949)

If a practical cryptosytem has perfect secrecy then

(c) $|\mathcal{K}| \geq |\mathcal{C}|$.

So far we know that for all $x \in \mathbb{P}$ and $y \in \mathcal{C}$ the events $X = x$ and $Y = y$ are independent and both have positive probability and there exists a key k such that $e_k(x) = y$.

- Hint: fix $x^\star \in \mathbb{P}$. Can the same key encrypt $x^\star$ to two different ciphertexts? So how many different keys are needed?

Theorem 3.10 (Shannon 1949)

If a practical cryptosytem has perfect secrecy then

(c) $|\mathcal{K}| \geq |\mathcal{C}|$.

So far we know that for all $x \in \mathbb{P}$ and $y \in \mathcal{C}$ the events $X = x$ and $Y = y$ are independent and both have positive probability and there exists a key k such that $e_k(x) = y$.

- Hint: fix $x^\star \in \mathbb{P}$. Can the same key encrypt $x^\star$ to two different ciphertexts? So how many different keys are needed?
- Prove (c).

Theorem 3.10 (Shannon 1949)

If a practical cryptosytem has perfect secrecy then

(c) $|\mathcal{K}| \geq |\mathcal{C}|$.

So far we know that for all $x \in \mathbb{P}$ and $y \in \mathcal{C}$ the events $X = x$ and $Y = y$ are independent and both have positive probability and there exists a key k such that $e_k(x) = y$.

- Hint: fix $x^\star \in \mathbb{P}$. Can the same key encrypt $x^\star$ to two different ciphertexts? So how many different keys are needed?
- 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 $e_k(x) = y$. Moreover each key is used with equal probability.

- Prove the uniqueness. Hint: encrypt a fixed $x^\star \in \mathbb{P}$.

Theorem 3.10 (Shannon 1949)

If a practical cryptosytem has perfect secrecy then

(c) $|\mathcal{K}| \geq |\mathcal{C}|$.

So far we know that for all $x \in \mathbb{P}$ and $y \in \mathcal{C}$ the events $X = x$ and $Y = y$ are independent and both have positive probability and there exists a key k such that $e_k(x) = y$.

- Hint: fix $x^\star \in \mathbb{P}$. Can the same key encrypt $x^\star$ to two different ciphertexts? So how many different keys are needed?
- 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 $e_k(x) = y$. Moreover each key is used with equal probability.

- Prove the uniqueness. Hint: encrypt a fixed $x^\star \in \mathbb{P}$.
- Fix $y^\star \in \mathcal{C}$. For each $x \in \mathbb{P}$, let $k_x^\star$ be the unique key such that $e_{k_x^\star}(x) = y^\star$. Are the $k_x^\star$ distinct?

Theorem 3.10 (Shannon 1949)

If a practical cryptosytem has perfect secrecy then

(c) $|\mathcal{K}| \geq |\mathcal{C}|$.

So far we know that for all $x \in \mathbb{P}$ and $y \in \mathcal{C}$ the events $X = x$ and $Y = y$ are independent and both have positive probability and there exists a key k such that $e_k(x) = y$.

- Hint: fix $x^\star \in \mathbb{P}$. Can the same key encrypt $x^\star$ to two different ciphertexts? So how many different keys are needed?
- 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 $e_k(x) = y$. Moreover each key is used with equal probability.

- Prove the uniqueness. Hint: encrypt a fixed $x^\star \in \mathbb{P}$.
- Fix $y^\star \in \mathcal{C}$. For each $x \in \mathbb{P}$, let $k_x^\star$ be the unique key such that $e_{k_x^\star}(x) = y^\star$. Are the $k_x^\star$ distinct?
- What can you say about $\mathbb{P}[K = k_x^\star]$? (Use the quiz idea: express it as a conditional probability.) Does this show (d)?

Latin Squares

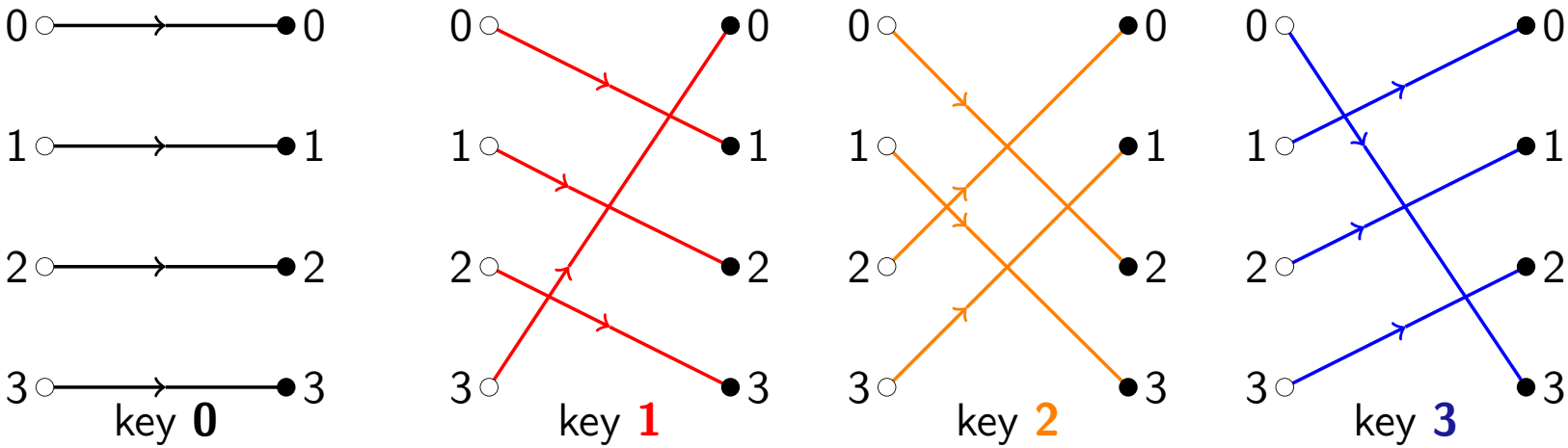
Consider a cryptosystem with perfect secrecy in which $\mathcal{P} = |\mathcal{C}| = |\mathcal{K}| = \{0, 1, \ldots, n-1\}$. By (c) in Theorem 3.10, for each $x, y \in \{0, 1, \ldots, n-1\}$, there exists a unique $k \in \{0, 1, \ldots, n-1\}$ such that $e_k(x) = y$. Therefore the cryptosystem is determined by the $n \times n$ matrix M where

$$M_{xy} = k \Longleftrightarrow e_k(x) = y.$$

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 3.10, 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

$$M_{xy} = k \iff e_k(x) = y.$$

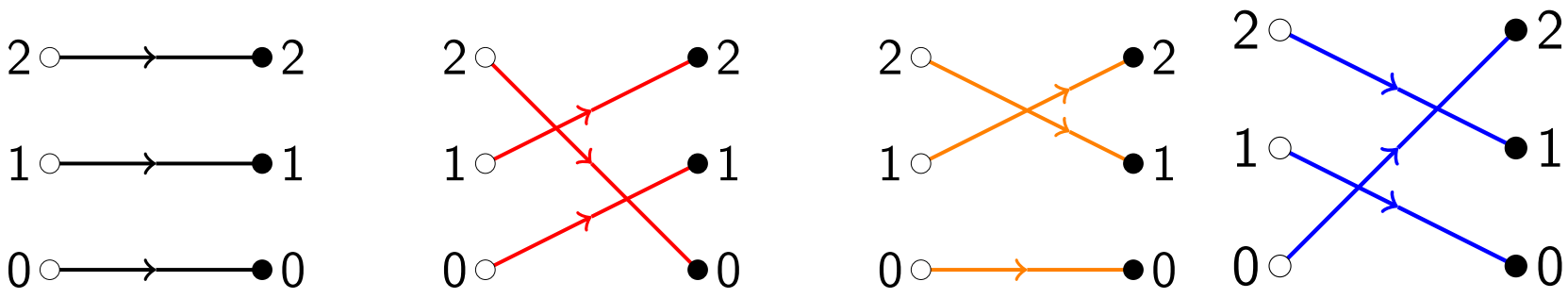


has matrix

$$\begin{pmatrix} \mathbf{0} & \mathbf{1} & \mathbf{2} & \mathbf{3} \\ \mathbf{3} & \mathbf{0} & \mathbf{1} & \mathbf{2} \\ \mathbf{2} & \mathbf{3} & \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{0} \end{pmatrix}$$

Final Quiz on §3

Consider the cryptosystem below in which the keys have probabilities $\frac{1}{2}$ (black), $\frac{1}{3}$ (red), $\frac{1}{8}$ (orange), $\frac{1}{24}$ (blue)



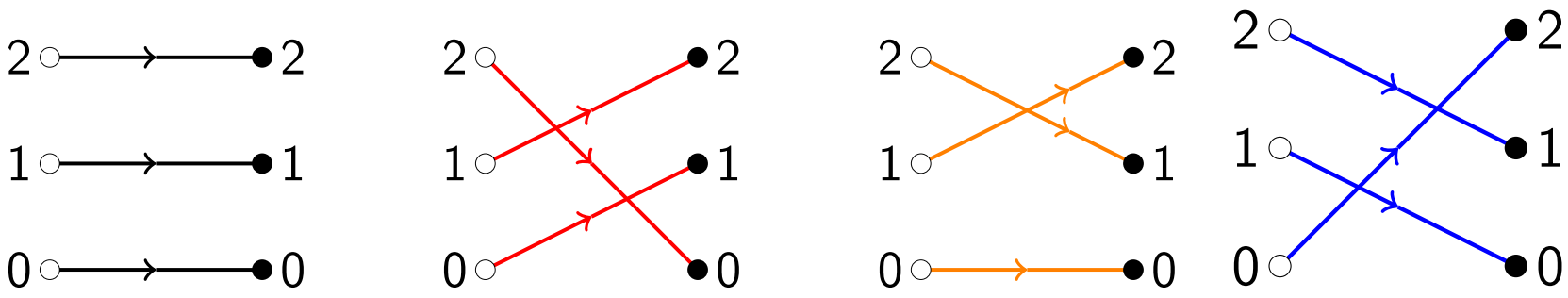
As usual let X be the random plaintext, Y the random ciphertext and K the random key.

(a) What is $\mathbb{P}[e_K(1) = 2]$?

(A) $\frac{8}{24}$ (B) $\frac{11}{24}$ (C) $\frac{12}{24}$ (D) $\frac{13}{24}$

Final Quiz on §3

Consider the cryptosystem below in which the keys have probabilities $\frac{1}{2}$ (black), $\frac{1}{3}$ (red), $\frac{1}{8}$ (orange), $\frac{1}{24}$ (blue)



As usual let X be the random plaintext, Y the random ciphertext and K the random key.

(a) What is $\mathbb{P}[e_K(1) = 2]$?

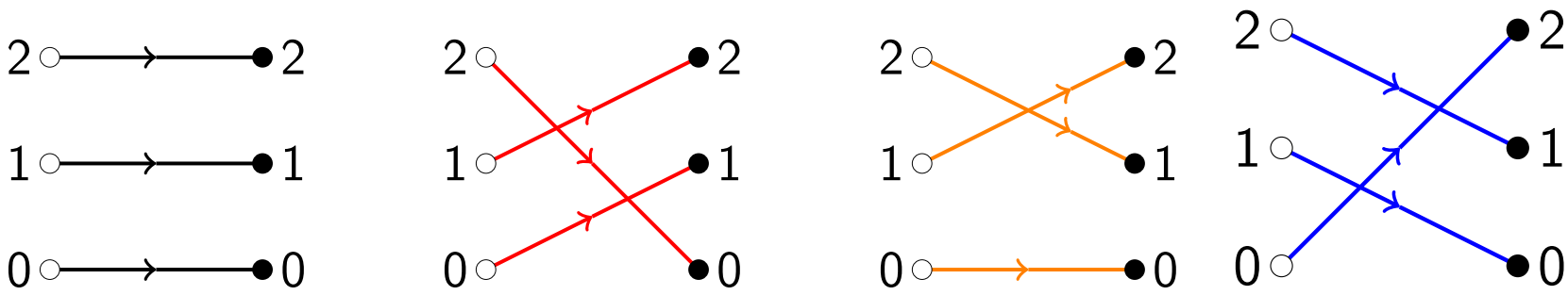
(A) $\frac{8}{24}$ (B) $\frac{11}{24}$ (C) $\frac{12}{24}$ (D) $\frac{13}{24}$

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

(A) $\frac{11}{24}$ (B) $\frac{11}{24}p_1$ (C) $\frac{13}{24}p_1$ (D) can't say

Final Quiz on §3

Consider the cryptosystem below in which the keys have probabilities $\frac{1}{2}$ (black), $\frac{1}{3}$ (red), $\frac{1}{8}$ (orange), $\frac{1}{24}$ (blue)



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) $\frac{8}{24}$ (B) $\frac{11}{24}$ (C) $\frac{12}{24}$ (D) $\frac{13}{24}$

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

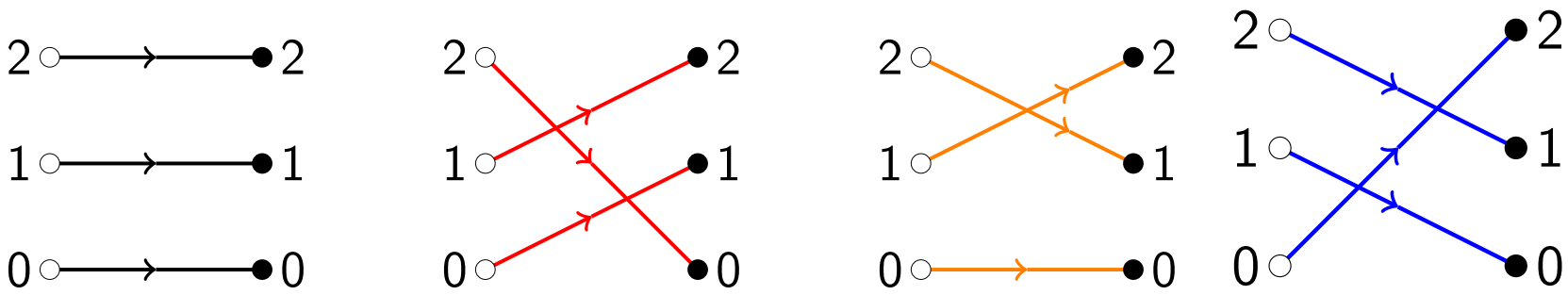
(A) $\frac{11}{24}$ (B) $\frac{11}{24}p_1$ (C) $\frac{13}{24}p_1$ (D) can't say

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

(A) $\frac{11}{24}$ (B) $\frac{11}{24}p_1$ (C) $\frac{13}{24}p_1$ (D) can't say

Final Quiz on §3

Consider the cryptosystem below in which the keys have probabilities $\frac{1}{2}$ (black), $\frac{1}{3}$ (red), $\frac{1}{8}$ (orange), $\frac{1}{24}$ (blue)



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) $\frac{8}{24}$ (B) $\frac{11}{24}$ (C) $\frac{12}{24}$ (D) $\frac{13}{24}$

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

(A) $\frac{11}{24}$ (B) $\frac{11}{24}p_1$ (C) $\frac{13}{24}p_1$ (D) can't say

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

(A) $\frac{11}{24}$ (B) $\frac{11}{24}p_1$ (C) $\frac{13}{24}p_1$ (D) can't say

§4 Attack Models

Eve observes a ciphertext. What is more useful for her: to learn the plaintext or to learn the key?

(A) Plaintext (B) Key

Example 4.2 (Affine cipher)

Let p be prime. The *affine cipher* on $\mathbb{Z}_p$ has $\mathcal{P} = \mathcal{C} = \mathbb{Z}_p$ and

$$\mathcal{K} = \{(a, c) : a \in \mathbb{Z}_p, c \in \mathbb{Z}_p, a \neq 0\}.$$

The encryption functions are defined by $e_{(a,c)}(x) = ax + c \bmod p$. The decryption functions are defined by $d_{(a,c)}(x) = b(x - c) \bmod p$, where $b \in \mathbb{Z}_p$ is the unique element such that $ab = 1 \bmod p$. With these definitions, the affine cipher is a cryptosystem.

For example, in the affine cipher on $\mathbb{Z}_{11}$, $e_{(7,2)}(5) = 4$ since $7 \times 5 + 2 \equiv 4 \bmod 11$ and, as expected, $d_{(7,2)}(4) = 5$ since $8 \times (4 - 2) \equiv 5 \bmod 11$.

§4 Attack Models

Eve observes a ciphertext. What is more useful for her: to learn the plaintext or to learn the key?

(A) Plaintext (B) Key

Example 4.2 (Affine cipher)

Let p be prime. The *affine cipher* on $\mathbb{Z}_p$ has $\mathcal{P} = \mathcal{C} = \mathbb{Z}_p$ and

$$\mathcal{K} = \{(a, c) : a \in \mathbb{Z}_p, c \in \mathbb{Z}_p, a \neq 0\}.$$

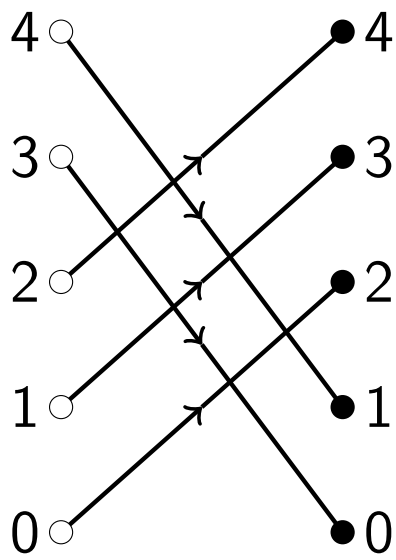
The encryption functions are defined by $e_{(a,c)}(x) = ax + c \bmod p$. The decryption functions are defined by $d_{(a,c)}(x) = b(x - c) \bmod p$, where $b \in \mathbb{Z}_p$ is the unique element such that $ab = 1 \bmod p$. With these definitions, the affine cipher is a cryptosystem.

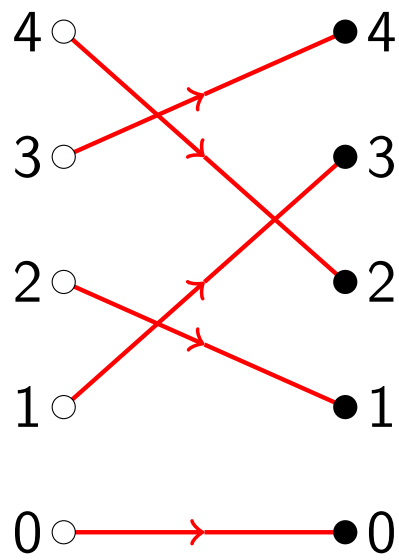
For example, in the affine cipher on $\mathbb{Z}_{11}$, $e_{(7,2)}(5) = 4$ since $7 \times 5 + 2 \equiv 4 \bmod 11$ and, as expected, $d_{(7,2)}(4) = 5$ since $8 \times (4 - 2) \equiv 5 \bmod 11$.

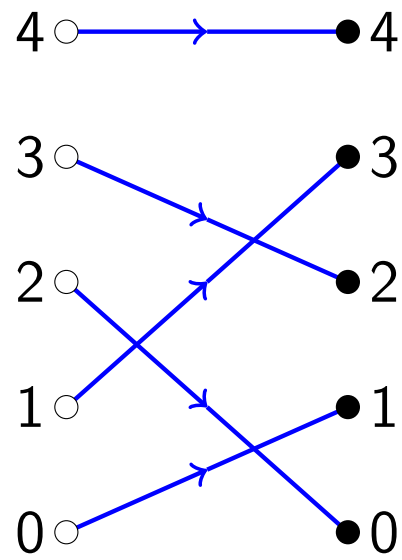
Affine Cipher

Exercise 4.3

The diagrams below show three encryption functions from the affine cipher when $p = 5$. Find the keys.







Quiz: the blue key is

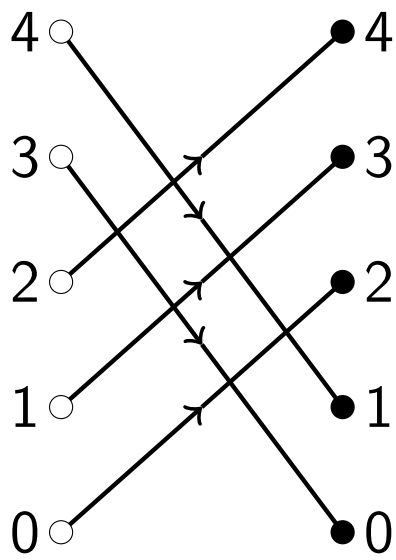
(A) $(0, 1)$ (B) $(2, 1)$ (C) $(3, 1)$ (D) $(2, -4)$

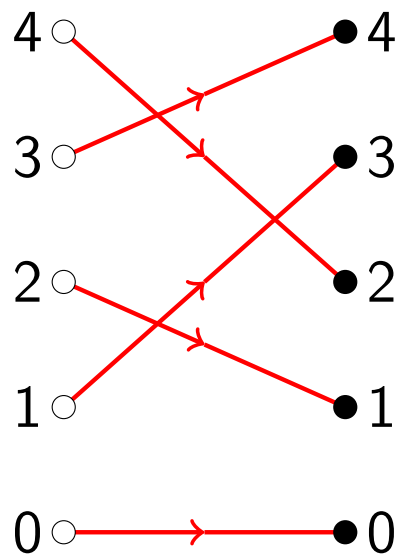
In Question 1 on Problem Sheet 3 you are asked to show that the affine cipher has perfect secrecy.

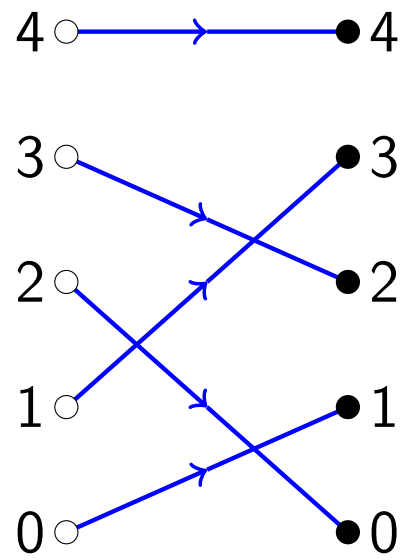
Affine Cipher

Exercise 4.3

The diagrams below show three encryption functions from the affine cipher when $p = 5$. Find the keys.







Quiz: 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.

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?

(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 that $e_{(a,c)}(2) = m \in \mathbb{Z}_5$. What 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?

(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 that $e_{(a,c)}(2) = m \in \mathbb{Z}_5$. What 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?

(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 that $e_{(a,c)}(2) = m \in \mathbb{Z}_5$. What 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?

(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 that $e_{(a,c)}(2) = m \in \mathbb{Z}_5$. What 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 choices of plaintext, and by Question 4 on Sheet 1, the substitution cipher and the Vigenère cipher just one. *Exercise:* How many does the numeric one-time pad require?

(3) Later in the course 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

$$e_k(x) = (x_1 + k_1, x_2 + k_2, \ldots, x_n + k_n)$$

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. Thus the one-time pad is the Vigenère cipher when the key has the same length as the plaintext. 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

Attacks on the One-time Pad

Example 4.7

The spy-master Alice and her agent Bob have agreed to use the one-time pad, with a randomly chosen key, for emergency messages. Following Kerckhoff's Principle, all this is known to Eve. Eve does not know that their key is $k = \texttt{atcldqezyomuua}$.

- Alice sends $e_k(\texttt{leaveinstantly}) = \texttt{lxcghyrrroznfy}$ to Bob.

Bob calculates

$$\texttt{lxcghyrrroznfy} - \texttt{atcldqezyomuua} = \texttt{leaveinstantly}.$$

Eve cannot guess the plaintext x: for example

$$\begin{aligned} x = \texttt{gototheairport} &\iff k = y - \texttt{gototheairport} \\ &\quad = \texttt{fjjsornrjxkzof} \\ x = \texttt{meetmeonbridge} &\iff k = y - \texttt{meetmeonbridge} \\ &\quad = \texttt{ztynvudeqxrkzu} \end{aligned}$$

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 sends $e_k(\texttt{goingeasttrain}) = \texttt{ghkyjuerrhducn}$ to Alice.

Eve now has ciphertexts

$$k + \texttt{leaveinstantly} = \texttt{lxcghyrrroznfy}$$
$$k + \texttt{goingeasttrain} = \texttt{ghkyjuerrhducn}.$$

She subtracts them to obtain $\Delta = \texttt{fqsiyenaahwtdl}$. Note that Δ does not depend on k.

The string Δ has the unusual property that there is an English message x' (Bob's reply) such that $\Delta + x'$ is another English message (Alice's message). 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.

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.

Exercises on One-time Pad

The previous example shows that the one-time pad is broken by a known ciphertext attack with *two* known ciphertexts.

Exercise 4.8

Show that the one-time pad is easily broken by a chosen plaintext attack.

Exercise 4.9

Does the one-time pad have perfect secrecy? (*Hint*: compare with Example 3.7.)

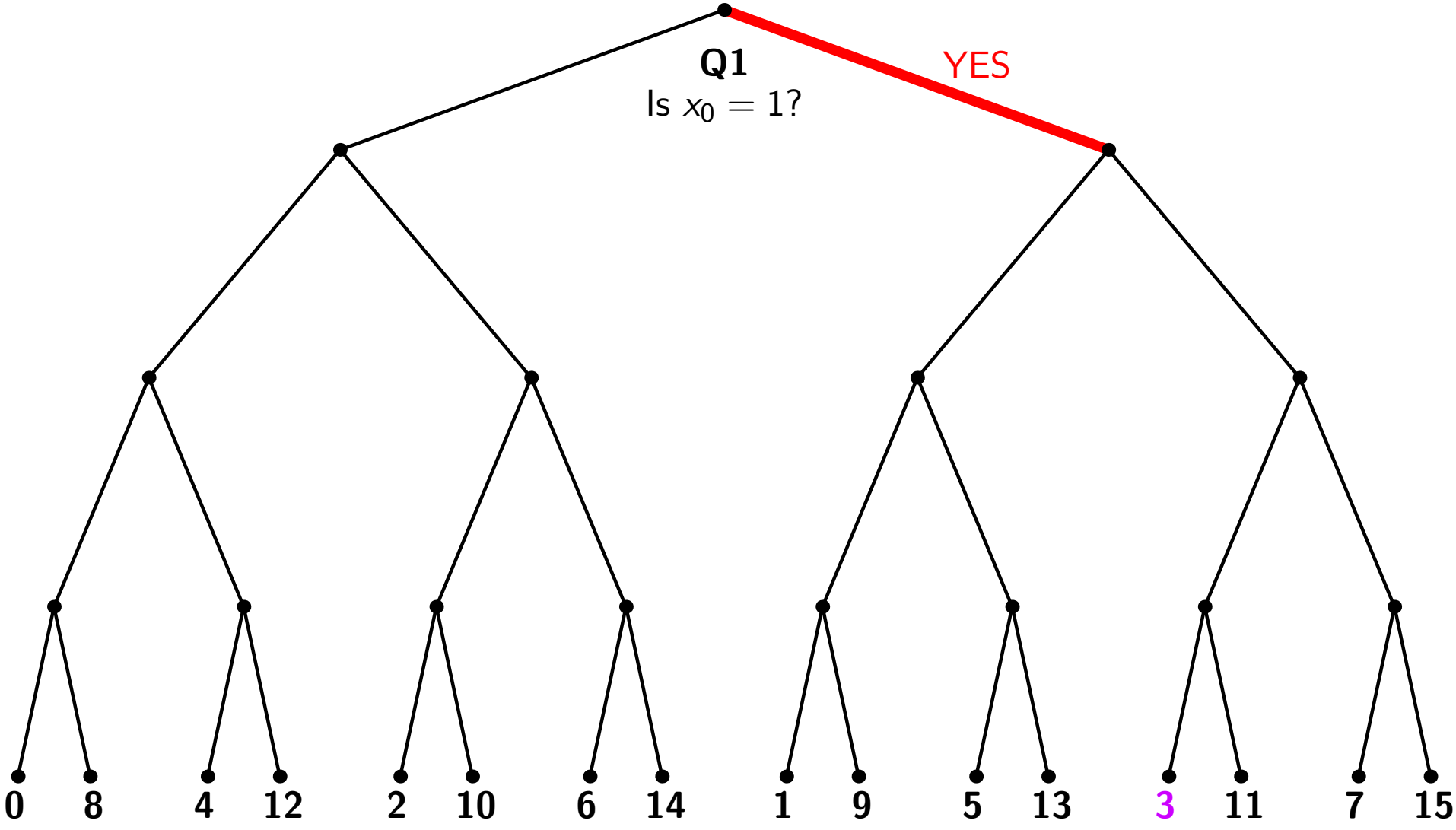
§5 Key Uncertainty and Entropy

Suppose Bob picks $x \in \{0, 1, \ldots, 15\}$. How many yes/no questions does Alice need to guess x? Question 2 on the Preliminary Problem Sheet gives one simple strategy: 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 $x_3 = 1$?'.

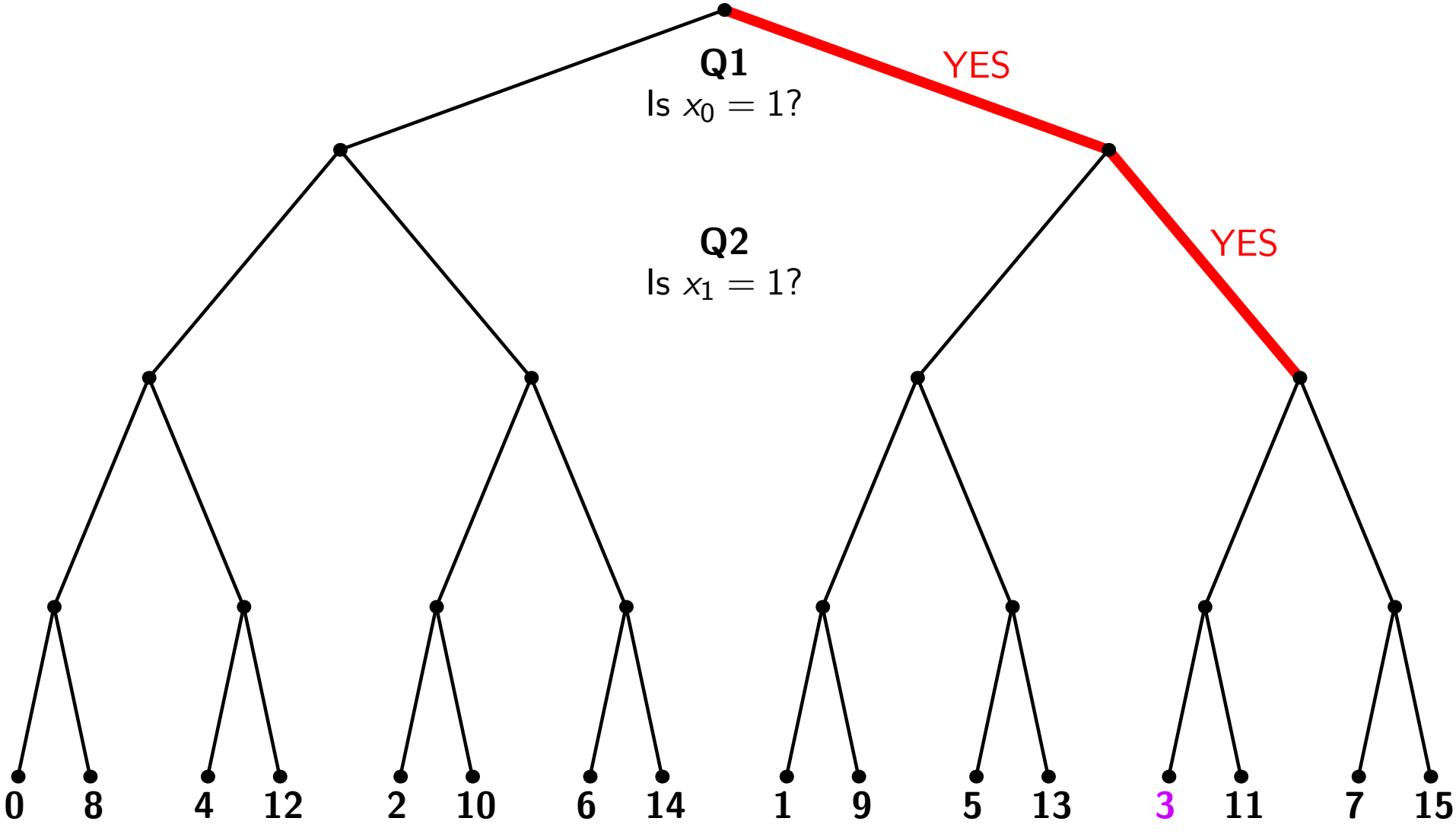
Exercise 5.1

Explain why no questioning strategy can guarantee to use fewer than four questions.

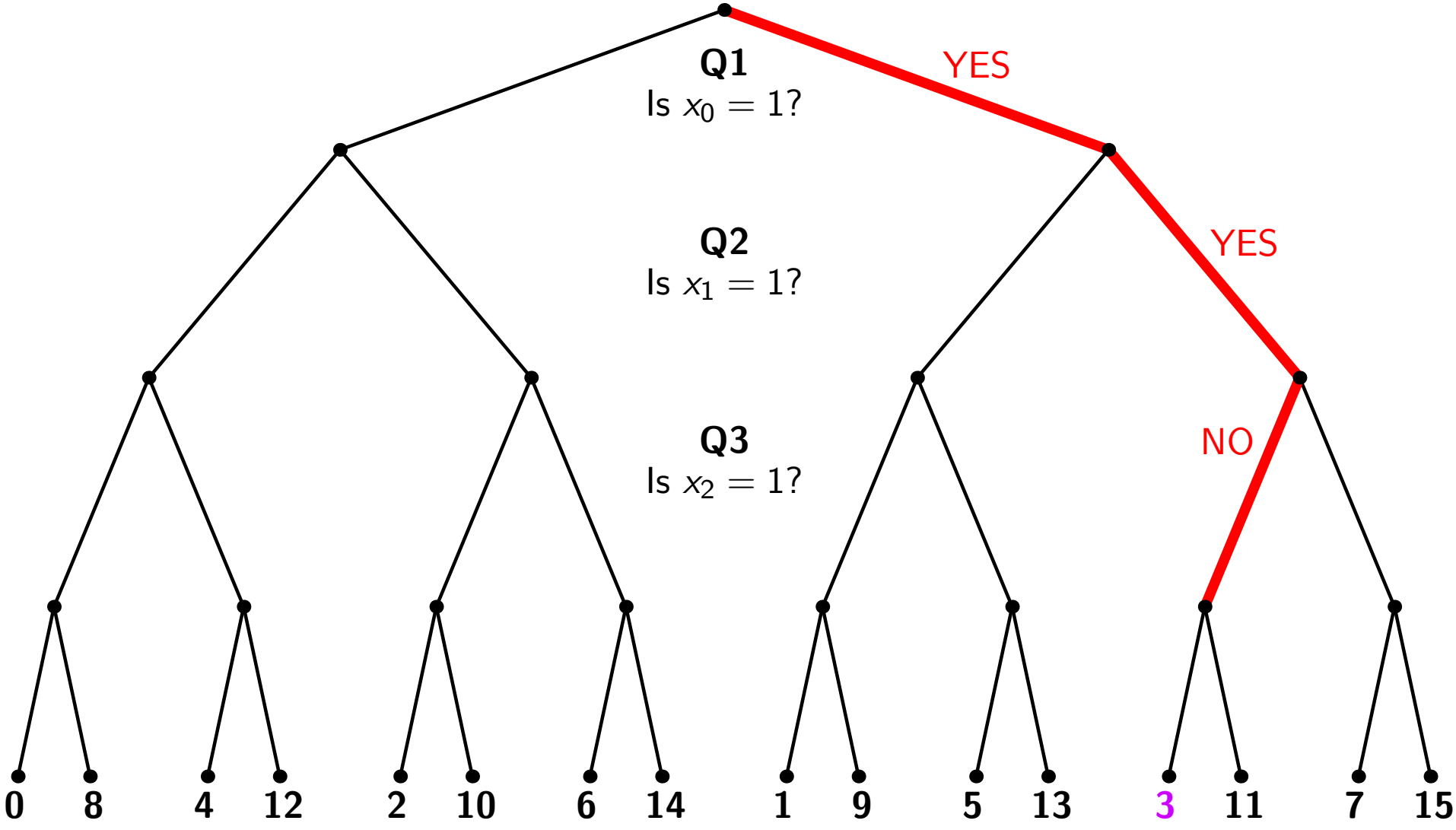
4 Yes/No Questions for 4 Bits of Information



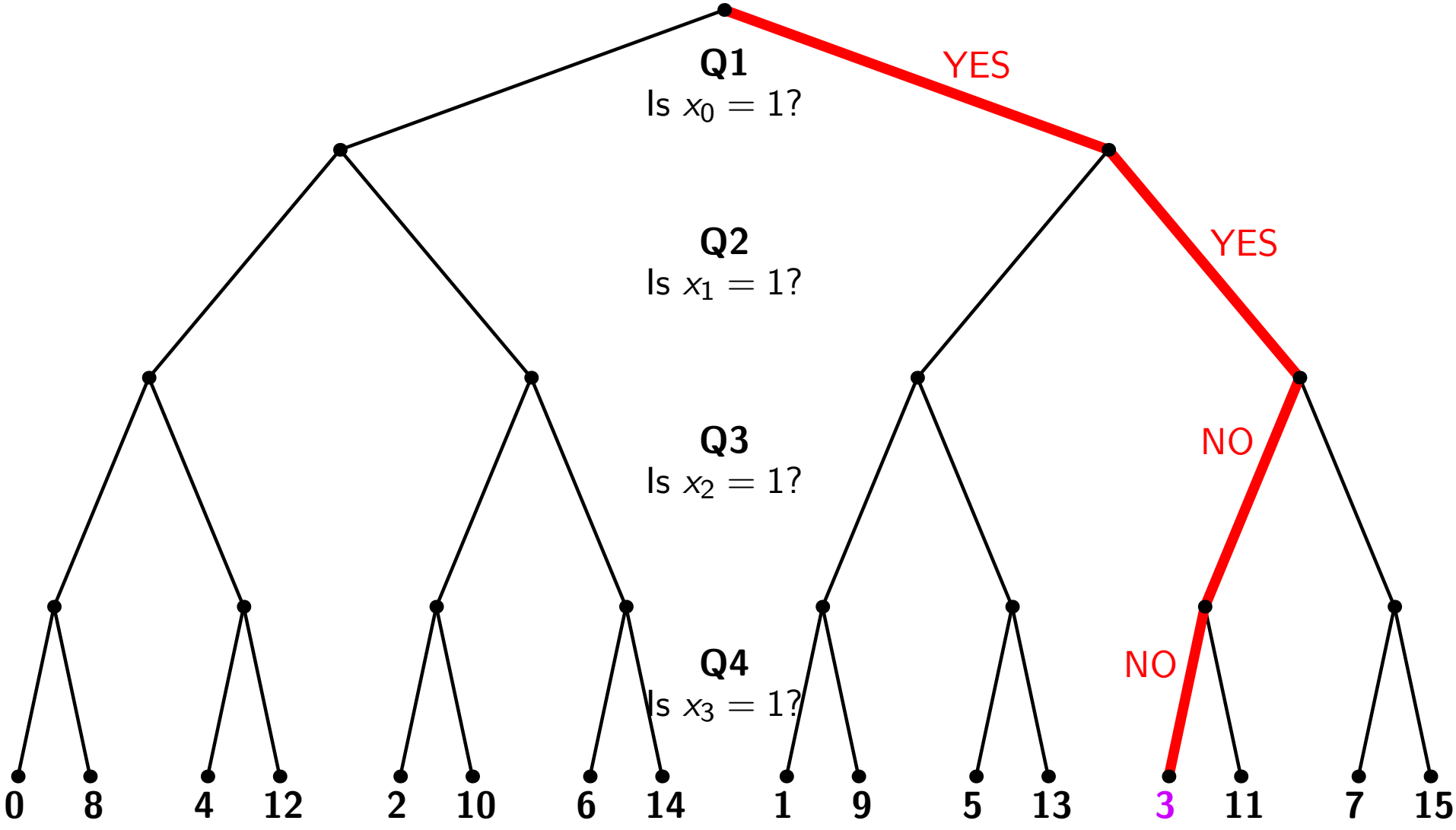
4 Yes/No Questions for 4 Bits of Information



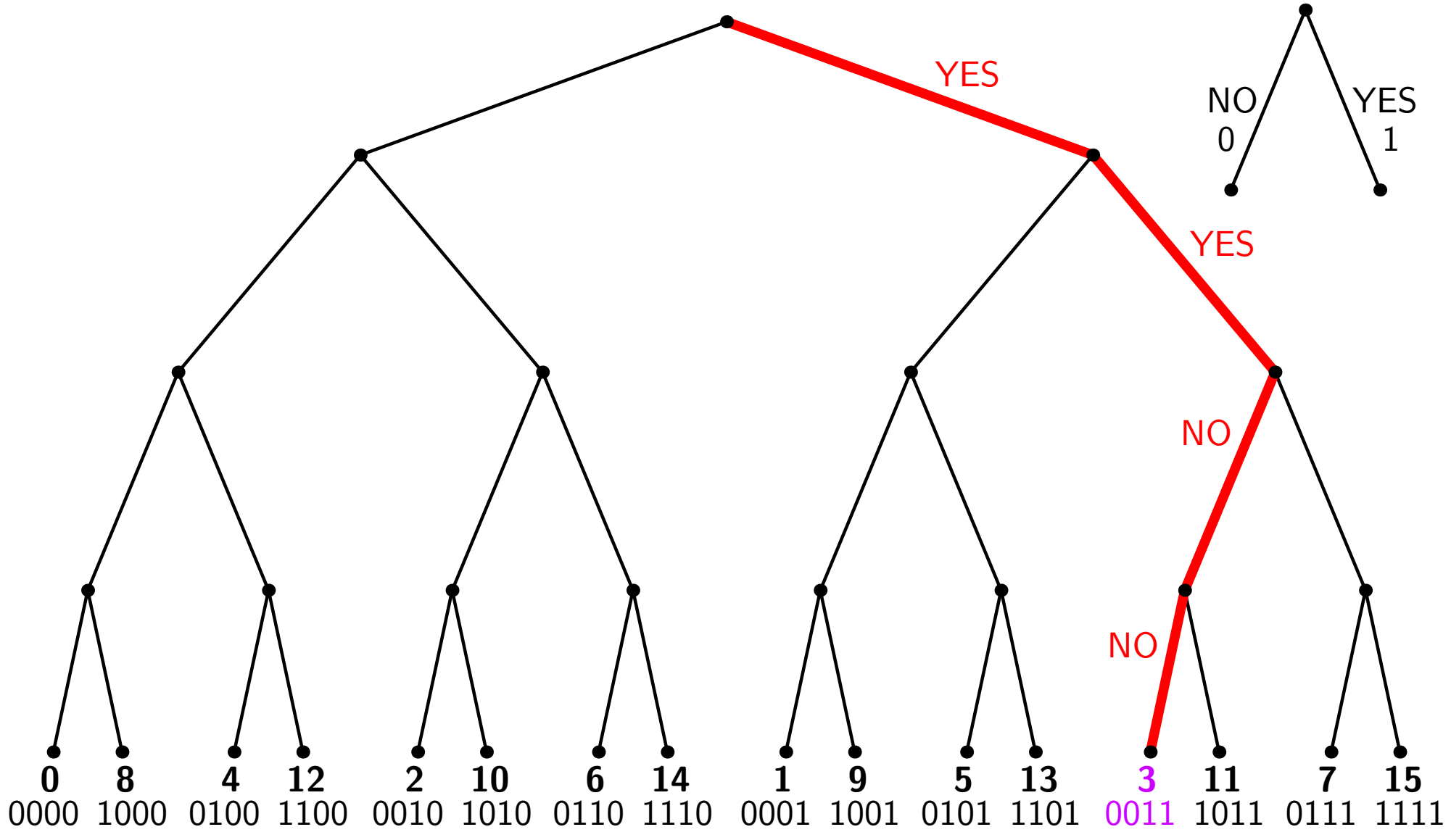
4 Yes/No Questions for 4 Bits of Information



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) $p_0 = p_1 = p_2 = p_3 = \frac{1}{4}$.

(b) $p_0 = \frac{1}{2}$, $p_1 = \frac{1}{4}$, $p_2 = \frac{1}{4}$, $p_3 = 0$.

(c) $p_0 = \frac{1}{2}$, $p_1 = \frac{1}{4}$, $p_2 = \frac{1}{8}$, $p_3 = \frac{1}{8}$.

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) $p_0 = p_1 = p_2 = p_3 = \frac{1}{4}$.

(b) $p_0 = \frac{1}{2}$, $p_1 = \frac{1}{4}$, $p_2 = \frac{1}{4}$, $p_3 = 0$.

(c) $p_0 = \frac{1}{2}$, $p_1 = \frac{1}{4}$, $p_2 = \frac{1}{8}$, $p_3 = \frac{1}{8}$.

(d) $p_0 = 1$, $p_1 = p_2 = p_3 = 0$.

Administration

- Please take Problem Sheet 3.
- Please take final installment of Part A printed notes.
- **M.Sc.** students: please take a corrected copy of pages 11/12 of the M.Sc. printed notes. My apologies for the many off-by-one errors. The notes are updated on Moodle.
- Please hand in answers to Problem Sheet 2 end of next lecture.

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

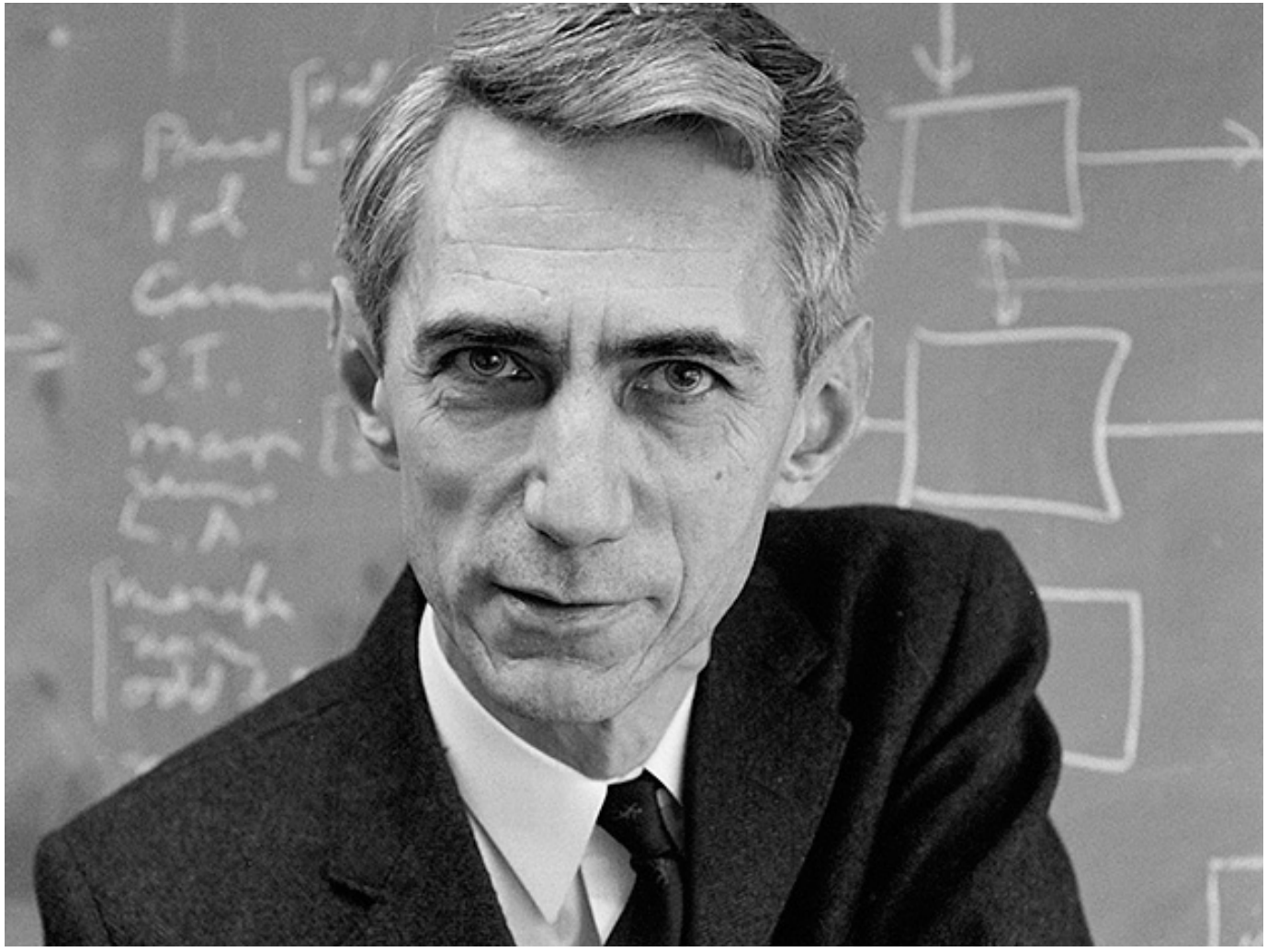
$$H(p) = -\sum_{x \in \mathcal{X}} p_x \log_2 p_x.$$

(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, $\log_2 2^n = n$ for each $n \in \mathbb{Z}$. If $p_x = 0$ then $-0 \log_2 0$ should be interpreted as $\lim_{p \to 0} -p \log_2 p = 0$.

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) $p_0 = p_1 = p_2 = p_3 = \frac{1}{4}$

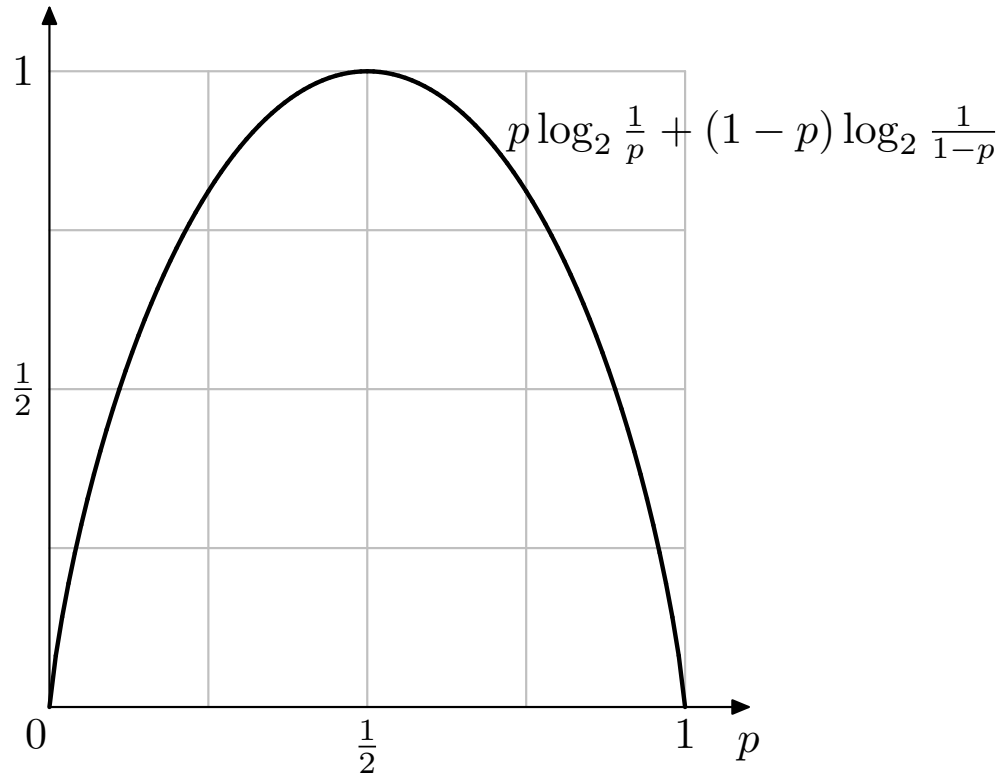
(b) $p_0 = \frac{1}{2}$, $p_1 = \frac{1}{4}$, $p_2 = \frac{1}{4}$, $p_3 = 0$

(c) $p_0 = \frac{1}{2}$, $p_1 = \frac{1}{4}$, $p_2 = \frac{1}{8}$, $p_3 = \frac{1}{8}$

(d) $p_0 = 1$, $p_1 = p_2 = p_3 = 0$

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.



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 cryptosystem in Exercise 3.2(iii). 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 $\mathbb{P}[Y = 1] = pr + (1-p)(1-r)$ and hence find $H(Y)$ when $r = 0, \frac{1}{4}, \frac{1}{2}$. Is it surprising that usually $H(Y) > H(X)$?

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.

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

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 5.8 (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 5.9

Let K and X be random variables. If K and X are independent then $H(K, X) = H(K) + H(X)$.

Lemma 5.10

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 $H\big(f(Z)\big) = H(Z)$.

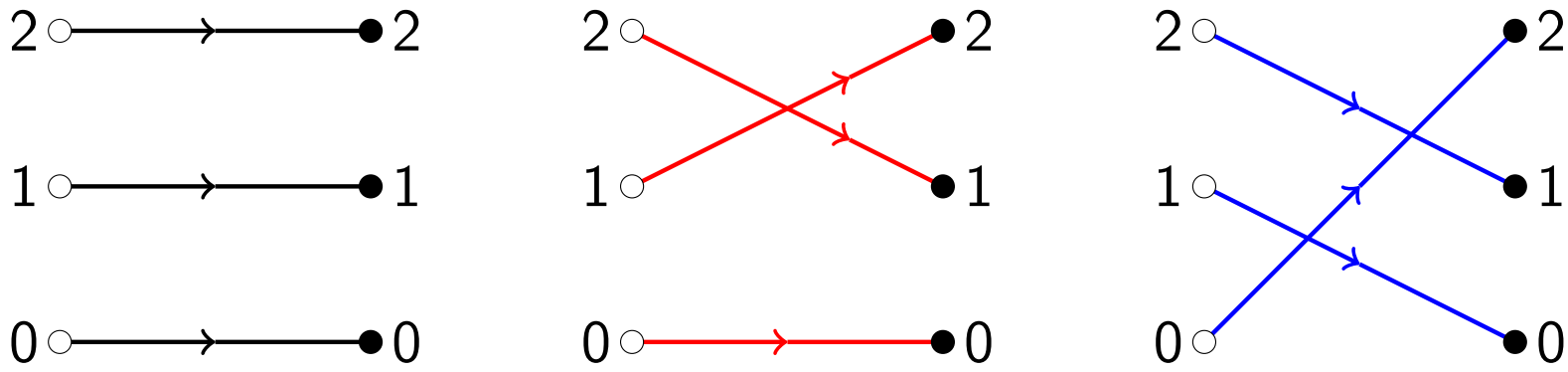
Theorem 5.11 (Shannon, 1949)

Take a cryptosystem in our usual notation. Then

$$H(K|Y) = H(K) + H(X) - H(Y).$$

Feedback on Sheet 2

Q1. The cryptosystem shown below uses three keys from the affine cipher on $\mathbb{Z}_3$, each with probability $\frac{1}{3}$. Suppose that plaintext 1 is sent with probability p and plaintext 2 is sent with probability $1-p$, so plaintext 0 is never sent.



(a) Recall that $e_{(a,c)}(x) = ax + c$. **[Sorry, this should be** $e_{(a,c)}(x) = ax + c$ **mod** 3.] Which keys (a, c) are used in this cryptosystem?

(b) Find $\mathbb{P}[Y = 1|X = 1]$. Express $\mathbb{P}[Y = 1]$, $\mathbb{P}[X = 1|Y = 1]$ in terms of p.

(c) When does the cryptosystem have perfect secrecy with respect to the probability distribution $p_0 = 0$, $p_1 = p$, $p_2 = 1 - p$ on plaintexts?

Q2. Alice and Bob communicate using the numeric one-time pad cryptosystem from Example 3.4, in which $\mathcal{K} = \mathcal{P} = \mathcal{C} = \{0, 1, \ldots, n-1\}$ and the encryption functions are defined by $e_k(x) = (x + k) \bmod n$. Each key $k \in \mathcal{K}$ is chosen with equal probability. Let p_x be the probability that $x \in \mathcal{P}$ is Alice's message.

(a) Show that if $x \in \mathcal{P}$ and $p_x > 0$ then $\mathbb{P}[Y_n = y | X_n = x] = \frac{1}{n}$ for all $y \in \mathcal{C}$.

(b) Find $\mathbb{P}[Y_n = y]$ for each $y \in \mathcal{C}$.

(c) Hence show that $\mathbb{P}[X_n = x | Y_n = y] = p_x$ for all $x \in \mathcal{P}$ with $p_x > 0$.

(d) What is $\mathbb{P}[X_n = x | Y_n = y]$ if $p_x = 0$? Deduce from this and (c) that the numeric one-time pad has perfect secrecy.

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).

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 ‘$\mathtt{abcdefgh}$’, ‘$\mathtt{goodwork}$’ $\in \mathcal{P}$ 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 3.200. We shall suppose his estimate is also good for plaintexts in $\mathcal{A}^n$.

The One-Time Pad

Example 5.12 (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 Exercise 4.9 all ciphertexts are equally likely, so

$$H(Y_n) = (\log_2 26)n.$$

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, $H(K|(X_n, Y_n))$, $H(X_n|Y_n)$ are

(A) 0 (B) 1 (C) $n(\log_2 26 - R)$ (D) $n \log_2 26$

(A) 0 (B) 1 (C) $n(\log_2 26 - R)$ (D) $n \log_2 26$

One-Time-Pad Quiz

Let $R = 3.2$ be the per character redundancy of English.

In the one-time pad of length n, $H(K|(X_n, Y_n))$, $H(X_n|Y_n)$ are

(A) 0 (B) 1 (C) $n(\log_2 26 - R)$ (D) $n \log_2 26$

(A) 0 (B) 1 (C) $n(\log_2 26 - R)$ (D) $n \log_2 26$

One-Time-Pad Quiz

Let $R = 3.2$ be the per character redundancy of English.

In the one-time pad of length n, $H(K|(X_n, Y_n))$, $H(X_n|Y_n)$ are

(A) 0 (B) 1 (C) $n(\log_2 26 - R)$ (D) $n \log_2 26$

(A) 0 (B) 1 (C) $n(\log_2 26 - R)$ (D) $n \log_2 26$

Unicity Distance

In Example 5.12 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

$$H(K|Y_n) = H(K) - Rn. \qquad (\star\star)$$

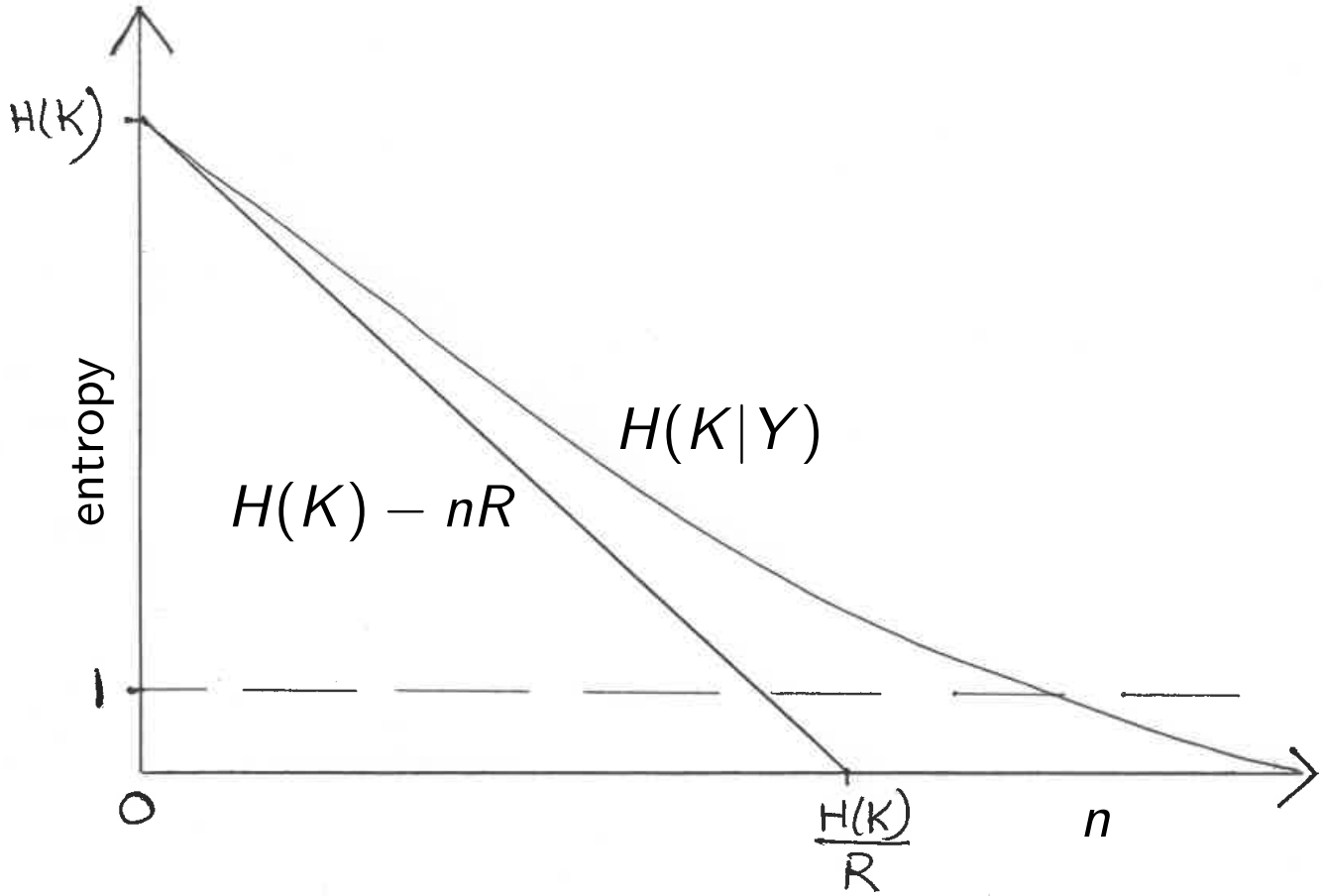
In the non-examinable extras for this part we give Shannon's argument that $(\star\star)$ should be a good approximation for $H(K|Y_n)$ in any cryptosystem where $\mathcal{P} = \mathcal{C} = \mathcal{A}^n$, and the messages are English texts. It works best when $\mathcal{K}$ is large and n is small.

Exercise 5.13

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 5.14

The quantity $H(K)/R$ is the *unicity* distance of the cryptosystem.

Unicity Distance for Substitution Cipher

Exercise 5.15

In the substitution cipher attack in Example 2.5 we saw that the ciphertext y 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 $H(K|Y_{280} = y)$?

(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 5.15

In the substitution cipher attack in Example 2.5 we saw that the ciphertext y 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 $H(K|Y_{280} = y)$?

(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 5.15

In the substitution cipher attack in Example 2.5 we saw that the ciphertext y 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 $H(K|Y_{280} = y)$?

(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 5.16

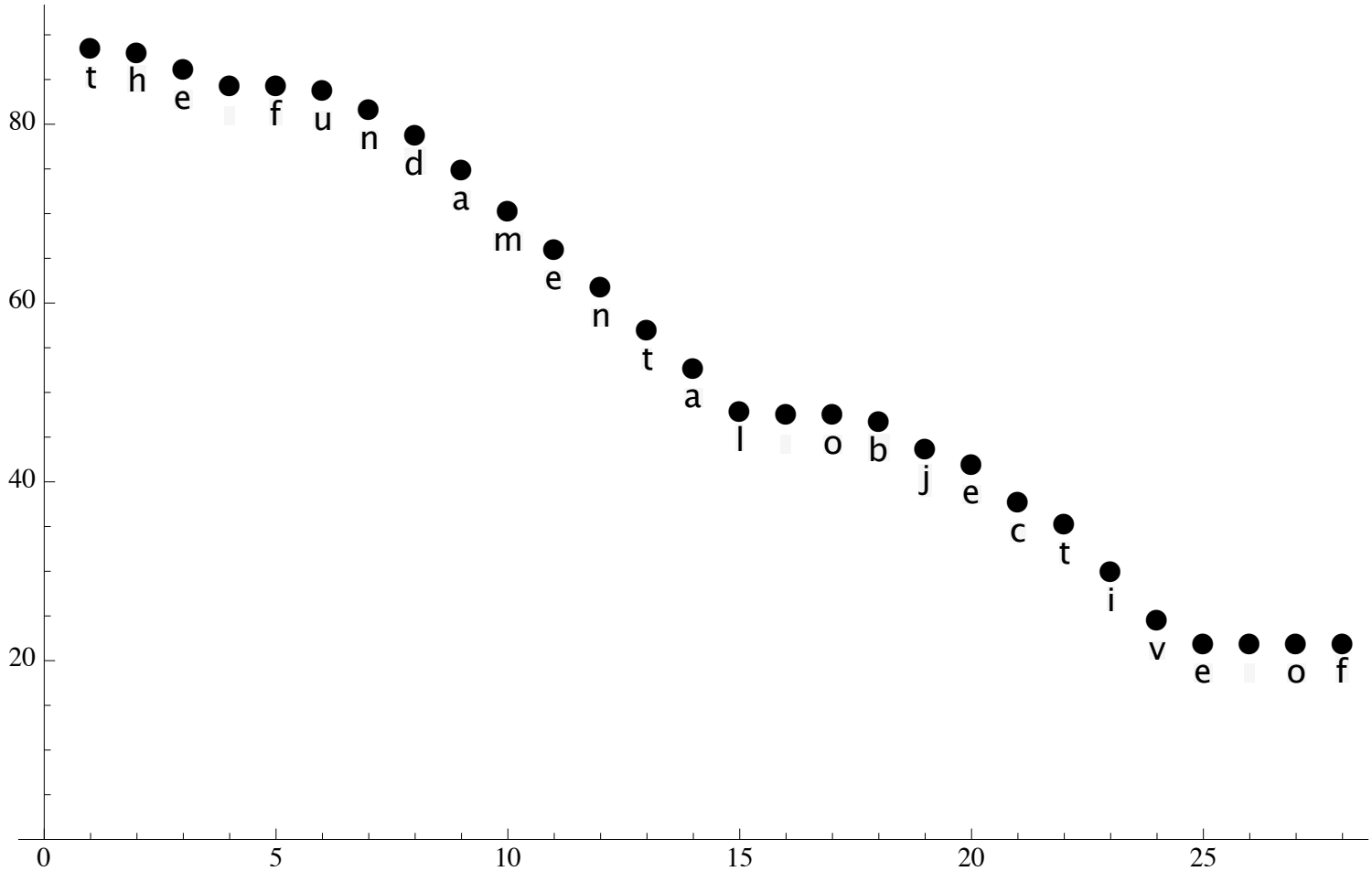
The first 28 characters of the ciphertext in Example 2.5 are `KQX WJZRUHXZKUY GTOXSKPIX GW`. A computer search using a dictionary of about 70000 words gives 6 possible decryptions of the first 24 letters. These include '`imo purgatorial hedonics`', '`iwo purgatorial hedonism`' and '`the fundamental objectiv`'. 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 5.15 shows that $H(K|Y = y_{28}) = \log_2 10! = 21.791$. Nothing new about the key is learned after letter 25, so this is the value of the final 4 points in the graph of $H(K|Y_n)$ for $1 \leq n \leq 28$.

$H(K|Y_n)$ for Ciphertext Y from Substitution Cipher



Ciphertexts with High $g(y)$ are More Likely: Intuition

Quiz: Suppose I ask everyone here 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

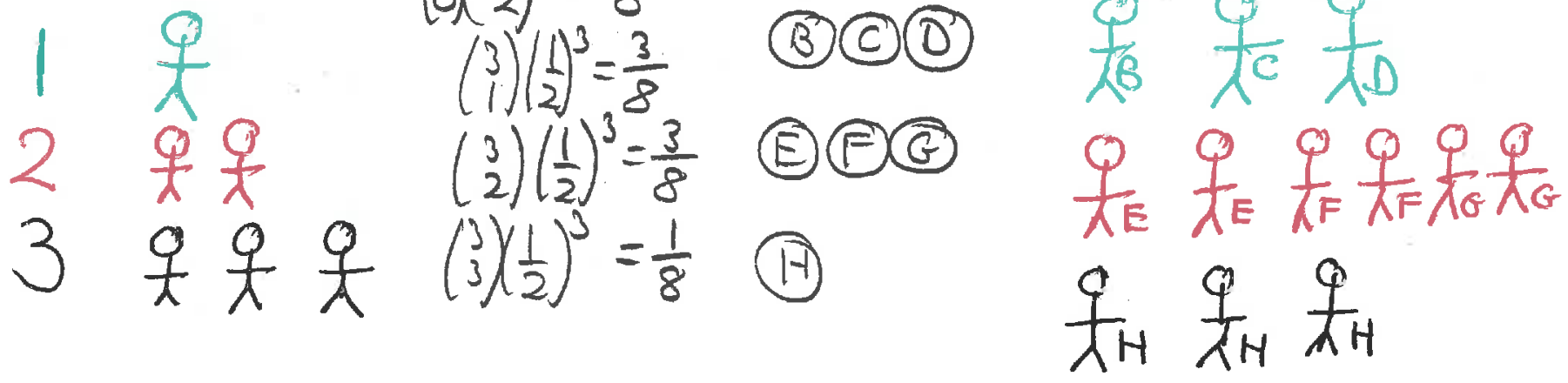
Ciphertexts with High $g(y)$ are More Likely: Intuition

Quiz: Suppose I ask everyone here 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

Families have 0 1 2 3 children $\sim$ Bin$(\frac{1}{2}, 3)$

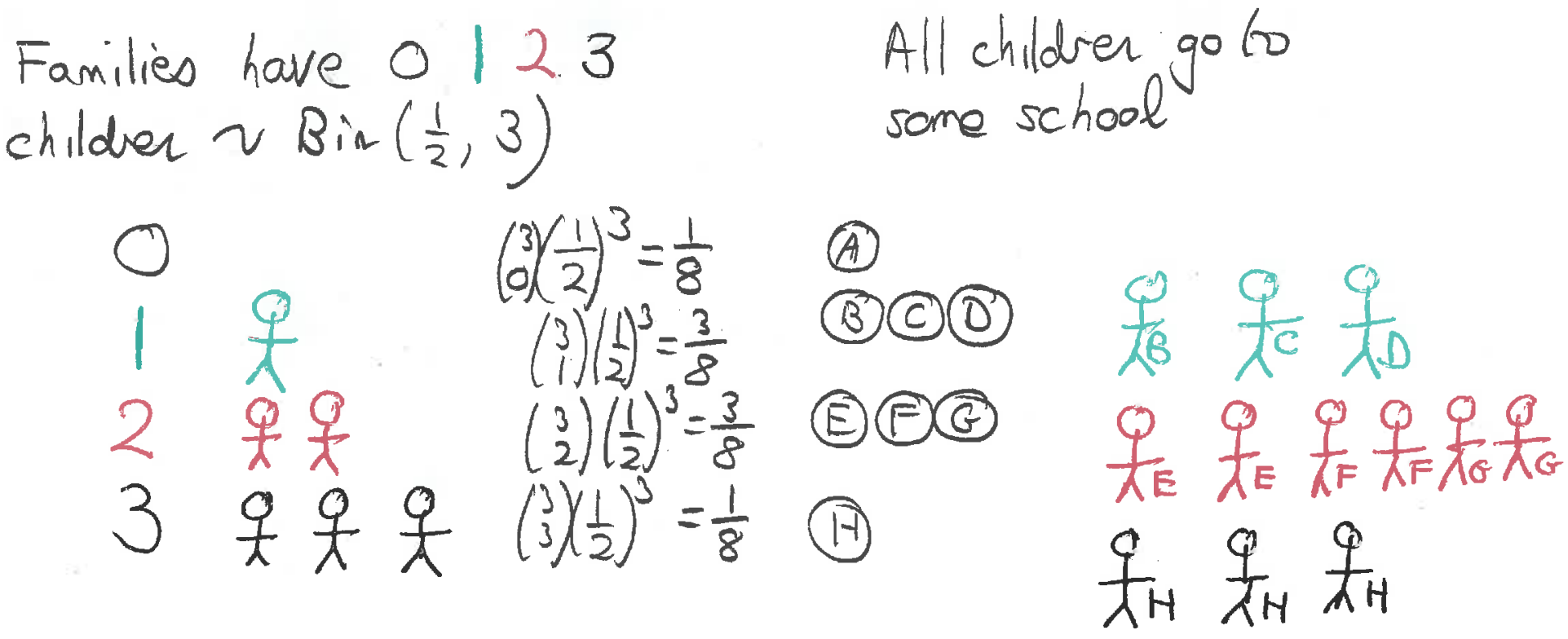
All children go to some school



Ciphertexts with High $g(y)$ are More Likely: Intuition

Quiz: Suppose I ask everyone here 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



Sampling the school, the observed probabilities are 0 (no children), 1/4 (3 green only children), 1/2 (6 red children), 1/4 (3 black children).

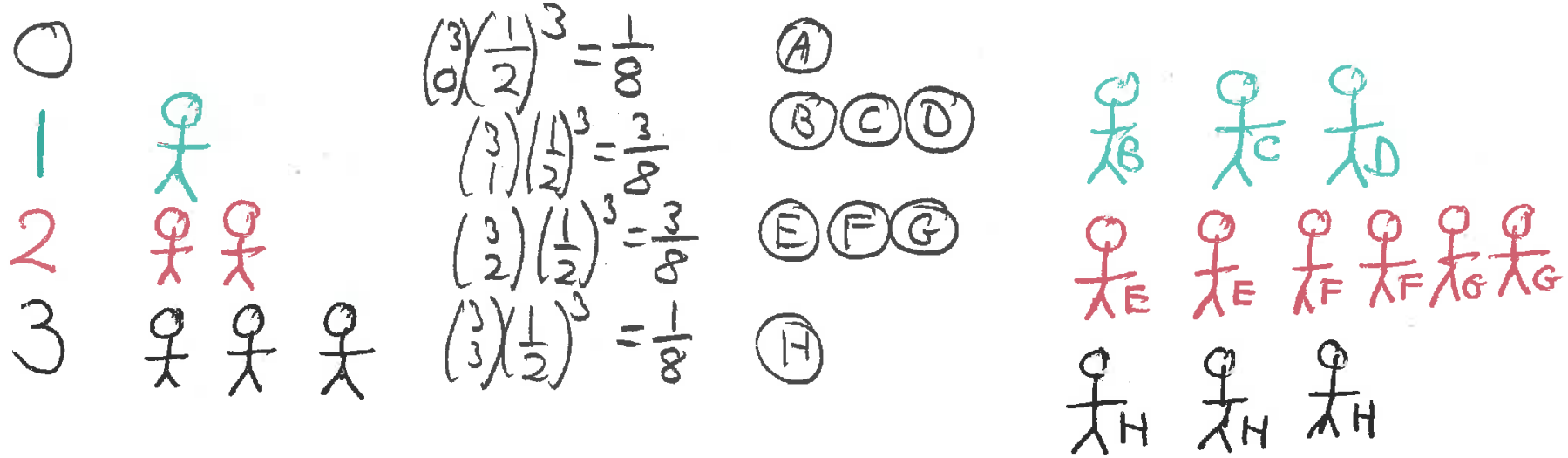
Ciphertexts with High $g(y)$ are More Likely: Intuition

Quiz: Suppose I ask everyone here 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

Families have 0 1 2 3 children $\sim$ Bin$(\frac{1}{2}, 3)$

All children go to some school



Sampling the school, the observed probabilities are 0 (no children), 1/4 (3 green only children), 1/2 (6 red children), 1/4 (3 black children). So we observe the $1 + \text{Bin}(\frac{1}{2}, 2)$ distribution.

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?

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

$$k_s = \sum_{t \in T} k_{s-t}$$

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.

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:* observe that $k' = 0011$ appears in positions 4, 5, 6, 7 of the keystream above. Find the keystream for k'.

(iv) Starting with $k = 0111$, the sequence k, $F(k)$, $F^2(k)$, $F^3(k), \ldots, F^{14}(k)$, $F^{15}(k)$ is 0111, 1111, 1110, . . . , 1011, 0111, 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.

(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:* observe that $k' = 0011$ appears in positions 4, 5, 6, 7 of the keystream above. Find the keystream for k'.

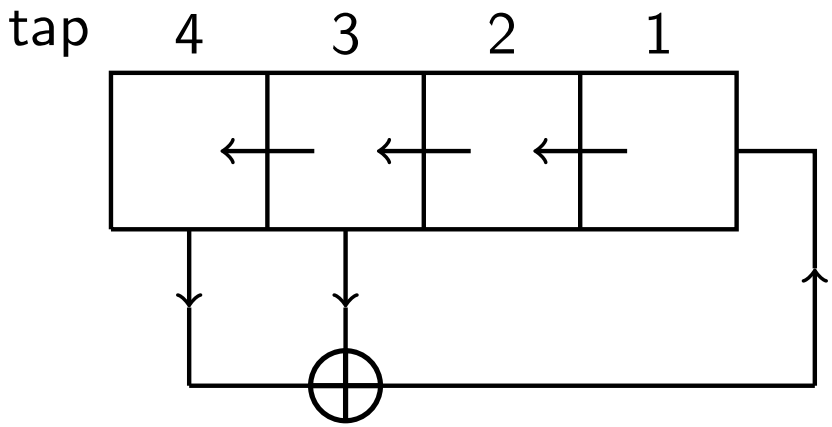
(iv) Starting with $k = 0111$, the sequence k, $F(k)$, $F^2(k)$, $F^3(k), \ldots, F^{14}(k)$, $F^{15}(k)$ is 0111, 1111, 1110, . . . , 1011, 0111, with $F^{15}(k) = k$.

(v) Quiz. Every keystream generated by F is obtained by reading the circle of 15 bits we used to solve Exercise 6.1.

(A) False (B) True

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.

Circuit Diagrams and 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

$$\begin{array}{cccccccccccccccccccc} (0, & 1, & 1, & 1, & 1, & 0, & 0, & 0, & 1, & 0, & 0, & 1, & 1, & 0, & 1, & 0, & 1, & 1, & 1, & 1 \ldots) \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{array}$$

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

Circuit Diagrams and 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

Circuit Diagrams and 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

Circuit Diagrams and 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

Circuit Diagrams and 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

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 $d_k : \mathbb{F}_2^n \to \mathbb{F}_2^n$.

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 5.2, 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

(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 5.2, 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

(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 $\mathbf{011}011\ldots$.

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.

Where is the first position in which the keystream for key 0110 repeats? (This is the period of the keystream.)

(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 $\mathbf{011}011\ldots$.

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.

Where is the first position in which the keystream for key 0110 repeats? (This is the period of the keystream.)

(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 $\mathbf{011}011\ldots$.

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.

Where is the first position in which the keystream for key 0110 repeats? (This is the period of the keystream.)

(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 with taps $\{2, 3\}$ 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? As in Example 6.3(iv), 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 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 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 $7, 7, 1, 1$ **[Correction!]** 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 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 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 ...

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 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 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 ...

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 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 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 ...

What is the period of H?

(A) 3 (B) 6 (C) 15 (D) 18

In general, (**VUP**) implies that the period of an LFSR is the lowest common multiple of the periods of its keystreams.

Periods, Polynomials and Power Series

An LFSR of width ℓ and maximum possible period $2^\ell - 1$ has a unique non-zero keystream, up to cyclic shifts. (This was seen in Example 6.3 in a case for $\ell = 4$.)

To find such LFSRs, it will be helpful to represent infinite keystreams by power series. We use z as an indeterminate. For instance, using the LFSR of width 3 with taps $\{2, 3\}$,

$$\mathbf{001}0111\mathbf{001}0111\ldots \longleftrightarrow \mathbf{z^2}+z^4+z^5+z^6+\mathbf{z^9}+z^{11}+z^{12}+z^{13}+\cdots .$$

Let $K(z)$ be the power series on the right. Since the keystream has period 7, when we multiply by $1 + z^7$ the infinite power series becomes a polynomial:

$$K(z)(1 + z^7) = z^2 + z^4 + z^5 + z^6.$$

For example, the coefficient of z^9 is zero since $k_2 = k_7 = 1$ and $1 + 1 = 0$.

Annihilating Power Series

The LFSR of width 3 with taps $\{2, 3\}$ has keystream

$$\mathbf{001}0111\mathbf{001}0111\ldots \longleftrightarrow \mathbf{z^2}+z^4+z^5+z^6+\mathbf{z^9}+z^{11}+z^{12}+z^{13}+\cdots .$$

Let $K(z)$ be the power series on the right.

Exercise 6.9

(i) Recall that the *degree* of a polynomial is its highest power of z. Which polynomial $p(z)$ of degree 3 is such that $K(z)p(z)$ is a polynomial?

(A) $1+z$ (B) $1+z^2$ (C) $1+z^2+z^3$ (D) $1+z+z^3$

(ii) Which key gives the keystream corresponding to the power series $1/(1+z^2+z^3)$? [**Correction: not** $1/(1+z+z^3)$**.**] [*Hint:* think of it as $1/(1+t)$, and expand as a geometric series. Be bold! Remember $+$ is $-$ in $\mathbb{F}_2$.]

(A) 000 (B) 100 (C) 101 (D) 111

Annihilating Power Series

The LFSR of width 3 with taps $\{2, 3\}$ has keystream

$$\mathbf{001}0111\mathbf{001}0111\ldots \longleftrightarrow \mathbf{z^2}+z^4+z^5+z^6+\mathbf{z^9}+z^{11}+z^{12}+z^{13}+\cdots .$$

Let $K(z)$ be the power series on the right.

Exercise 6.9

(i) Recall that the *degree* of a polynomial is its highest power of z. Which polynomial $p(z)$ of degree 3 is such that $K(z)p(z)$ is a polynomial?

(A) $1+z$ (B) $1+z^2$ (C) $1+z^2+z^3$ (D) $1+z+z^3$

(ii) Which key gives the keystream corresponding to the power series $1/(1+z^2+z^3)$? [**Correction: not** $1/(1+z+z^3)$**.**] [*Hint:* think of it as $1/(1+t)$, and expand as a geometric series. Be bold! Remember $+$ is $-$ in $\mathbb{F}_2$.]

(A) 000 (B) 100 (C) 101 (D) 111

Annihilating Power Series

The LFSR of width 3 with taps $\{2, 3\}$ has keystream

$$\mathbf{001}0111\mathbf{001}0111\ldots \longleftrightarrow \mathbf{z^2}+z^4+z^5+z^6+\mathbf{z^9}+z^{11}+z^{12}+z^{13}+\cdots .$$

Let $K(z)$ be the power series on the right.

Exercise 6.9

(i) Recall that the *degree* of a polynomial is its highest power of z. Which polynomial $p(z)$ of degree 3 is such that $K(z)p(z)$ is a polynomial?

(A) $1+z$ (B) $1+z^2$ (C) $1+z^2+z^3$ (D) $1+z+z^3$

(ii) Which key gives the keystream corresponding to the power series $1/(1+z^2+z^3)$? [**Correction: not** $1/(1+z+z^3)$**.**] [*Hint:* think of it as $1/(1+t)$, and expand as a geometric series. Be bold! Remember $+$ is $-$ in $\mathbb{F}_2$.]

(A) 000 (B) 100 (C) 101 (D) 111

Annihilating Power Series

The LFSR of width 3 with taps $\{2, 3\}$ has keystream

$$\mathbf{001}0111\mathbf{001}0111\ldots \longleftrightarrow \mathbf{z^2}+z^4+z^5+z^6+\mathbf{z^9}+z^{11}+z^{12}+z^{13}+\cdots .$$

Let $K(z)$ be the power series on the right.

Motivated by this exercise, we define the *feedback polynomial* of a LFSR with taps T to be

$$g_T(z) = 1 + \sum_{t \in T} z^t.$$

Definition 6.10

Let $K(z)$ be an infinite power series with coefficients in $\mathbb{F}_2$. Let $p(z)$ be a polynomial. We say that $p(z)$ *annihilates* $K(z)$ if $K(z)p(z)$ is a polynomial.

For example, we have seen that if

$$K(z) = \mathbf{z^2} + z^4 + z^5 + z^6 + \mathbf{z^7} + z^9 + x^{12} + z^{13} + \cdots$$

then $K(z)$ is annihilated by $1 + z^7$ (period!) and also by $1 + z^2 + z^3$ (taps!).

Annihilating Keystreams

Definition 6.10

Let $K(z)$ be an infinite power series with coefficients in $\mathbb{F}_2$. Let $p(z)$ be a polynomial. We say that $p(z)$ *annihilates* $K(z)$ if $K(z)p(z)$ is a polynomial.

For example, we have seen that if

$$K(z) = \mathbf{z^2} + z^4 + z^5 + z^6 + \mathbf{z}^7 + z^9 + x^{12} + z^{13} + \cdots$$

then $K(z)$ is annihilated by $1 + z^7$ (period!) and also by $1 + z^2 + z^3$ (taps!).

Lemma 6.11

Let F be an LFSR with taps T.

(a) *Let $K(z)$ be the infinite power series corresponding to a keystream of F. Then $g_T(z)$ annihilates $K(z)$.*

(b) *There is a keystream of F corresponding to the power series $1/g_T(z)$. It is annihilated only by the multiples of $g_T(z)$.*

- If you have problems with `LFSRs.nb`, or any other notebook in the course, please:
  - Quit MATHEMATICA
  - Download a fresh copy of the notebook from Moodle.
    Rename `AlphabeticCiphers.nb.txt` to `AlphabeticCiphers.nb` if necessary.
    This is a Moodle bug affecting Safari on Mac OS X and maybe other browsers.
  - Restart MATHEMATICA
  - Load the fresh copy of `AlphabeticCiphers.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.
- You can use the notebook for Questions 2 and 3 on Sheet 5. It will also help with Question 4: there is a hint in the notebook on how to do it using annihilators.

Annhilators Determine Period of LFSR

Corollary 6.12

Let F be an invertible LFSR with taps T. Let $m \in \mathbb{N}$ be least such that $g_T(z)$ divides $1 + z^m$. The period of F is m.

Annhilators Determine Period of LFSR

Corollary 6.12

Let F be an invertible LFSR with taps T. Let $m \in \mathbb{N}$ be least such that $g_T(z)$ divides $1 + z^m$. The period of F is m.

Lemma 6.13

If a polynomial $g(z)$ divides $z^d + 1$ and $z^e + 1$ then it divides $z^{\mathrm{hcf}(d,e)} + 1$.

Example 6.14

The number $2^{13} - 1 = 8191$ is a prime. The MATHEMATICA command `Factor[z^8191 + 1, Modulus -> 2]` returns

$$(1 + z)(1 + z + z^3 + z^4 + z^{13})(1 + z + z^2 + z^5 + z^{13}) \ldots .$$

The taps of the LFSR of width 13 with minimal polynomial $1 + z + z^3 + z^4 + z^{13}$ are $\{9, 10, 12, 13\}$. By Corollary 6.12, its period is the least m such that $1 + z + z^3 + z^4 + z^{13}$ divides $z^m + 1$. Will use this to show period is 8191.

§7 Pseudo-random Number Generation

We saw before Definition 6.8 that the maximum possible period of a keystream of an LFSR of width ℓ is $2^\ell - 1$. Such an LFSR has period $2^\ell - 1$. 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.)

Generating Cycles of Maximum Period LFSRs

Exercise 7.1

Let F be the LFSR of width 4 with taps $\{0, 1\}$ 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

$$(\mathbf{1}, \mathbf{1}, \mathbf{0}, \mathbf{0}, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0 \ldots).$$

Correspondingly, by the Very Useful Property,

$$F(\mathbf{1}, \mathbf{1}, \mathbf{0}, \mathbf{0}) = (1, 0, 0, 0), \ldots F^{14}(\mathbf{1}, \mathbf{1}, \mathbf{0}, \mathbf{0}) = (1, 1, 1, 0)$$

and $F^{15}(\mathbf{1}, \mathbf{1}, \mathbf{0}, \mathbf{0}) = (1, 1, 0, 0)$. By taking the first 15 positions we get the generating cycle

$$\begin{array}{c} (\mathbf{1}, \mathbf{1}, \mathbf{0}, \mathbf{0}, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \\ k_0\ k_1\ k_2\ k_3\ k_4\ k_5\ k_6\ k_7\ k_8\ k_9\ k_{10} k_{11} k_{12} k_{13} k_{14} \end{array}$$

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 t such that

$$(k_t, k_{t+1}, k_{t+2}, k_{t+3}) = (0,1,1,1).$$

(b) What is the only element of $\mathbb{F}_2^4$ *not* appearing in the keystream for $(1,1,0,0)$?

(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 t such that $(k_t, k_{t+1}, k_{t+2}) = (0,1,1)$. How many are there?

(e) Repeat (d) changing $(0,1,1)$ to $(0,0,1)$, $(0,0,0)$, $(0,1)$, $(1,1)$, $(1,0)$ and $(0,0)$. What is the pattern?

Quiz

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

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

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

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

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

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

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 and 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 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

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 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 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 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 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 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 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 statistic is $20^2/100 = 4$. If the hypothesis is true,

- we observed a random variable $Z \sim N(0,1)$ and found that $Z^2 \approx 4$;
- this event has probability between 0.01 and 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. Examples: 'this medical intervention is no better than a placebo', 'this keystream is equally likely to be 0 as 1', with a χ^2 distribution.

(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. Examples: 'this medical intervention is no better than a placebo', 'this keystream is equally likely to be 0 as 1', with a χ^2 distribution.

(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. Examples: 'this medical intervention is no better than a placebo', 'this keystream is equally likely to be 0 as 1', with a χ^2 distribution.

(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. Examples: 'this medical intervention is no better than a placebo', 'this keystream is equally likely to be 0 as 1', with a χ^2 distribution.

(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. Examples: 'this medical intervention is no better than a placebo', 'this keystream is equally likely to be 0 as 1', with a χ^2 distribution.

(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 Z is in the most extreme 10% of its range. Clearly this has probability 10%.

Quiz on Hypothesis Testing

We test a hypothesis using a statistic Z. If the hypothesis is true, Z has a known distribution. Examples: 'this medical intervention is no better than a placebo', 'this keystream is equally likely to be 0 as 1', with a χ^2 distribution.

(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 $\frac{2}{3}$ chance one will be rejected.

(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. Examples: 'this medical intervention is no better than a placebo', 'this keystream is equally likely to be 0 as 1', with a χ^2 distribution.

(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 $\frac{2}{3}$ chance one will be rejected.

(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. Examples: 'this medical intervention is no better than a placebo', 'this keystream is equally likely to be 0 as 1', with a χ^2 distribution.

(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?

More generally we shall prove the following proposition.

Proposition 7.7

Let $(k_0, k_1, \ldots, k_{2^\ell - 2})$ be a generating cycle of a maximal period LFSR of width ℓ. The correlation between $(k_0, k_1, \ldots, k_{2^\ell - 2})$ and any proper cyclic shift of $(k_0, k_1, \ldots, k_{2^\ell - 2})$ is $-1/(2^\ell - 1)$.

§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: it is the keystream for $(1, 0, 0, 1)$. *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: it is the keystream for $(1, 0, 0, 1)$. *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: it is the keystream for $(1, 0, 0, 1)$. *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?

(A) No (A) 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:

$$
\begin{array}{rl}
k_i & 0,0,0,1,0,0,1,1,0,1,0,1,1,1,1,0,0,0,1,0 \\
k_i^\star & 1,1,1,1,0,0,0,1,0,0,1,1,0,1,0,1,1,1,1,0 \\
u_i & 1,1,1,0,0,0,1,0,0,1,1,0,1,0,1,1,1,1,0,0 \\
 & 0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9
\end{array}
$$

Unfortunately, $u_0 u_1 u_2 \ldots$ is also generated by F: it is the keystream for $(1, 0, 0, 1)$. *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?

(A) No (A) Yes

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 $\{2, 4, 5, 7\}$. This is shown in Question 4(c) on Sheet 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 7.3 [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 $(g_0,g_1,g_2,g_3)=(0,0,0,1)$ 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 7.3 [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 $(g_0,g_1,g_2,g_3)=(0,0,0,1)$ 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 7.3 [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 $(g_0,g_1,g_2,g_3)=(0,0,0,1)$ 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 7.3 [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 $(g_0,g_1,g_2,g_3)=(0,0,0,1)$ 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 7.3 [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 $(g_0,g_1,g_2,g_3) = (0,0,0,1)$ 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 $k'_0 k_1 \ldots k'_{19}$ and $u_0 u_1 \ldots u_{19}$?

(A) $\frac{3}{10}$ (B) $\frac{1}{2}$ (C) $\frac{3}{5}$ (D) $\frac{7}{10}$

Example 7.3 [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 $(g_0,g_1,g_2,g_3) = (0,0,0,1)$ 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 $k'_0 k_1 \ldots k'_{19}$ and $u_0 u_1 \ldots u_{19}$?

(A) $\frac{3}{10}$ (B) $\frac{1}{2}$ (C) $\frac{3}{5}$ (D) $\frac{7}{10}$

Example 7.3 [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 $(g_0,g_1,g_2,g_3)=(0,0,0,1)$ 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 7.3 [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 $(g_0,g_1,g_2,g_3)=(0,0,0,1)$ then, using colours to indicate which bit is used:

$$\begin{array}{ll} k_i & 0,0,0,1,0,0,1,1,0,1,0,1,1,1,1,0,0,0,1,0 \\ k'_i & 0,0,1,0,1,1,1,0,0,1,0,1,1,1,0,0,1,0,1,1 \\ g_i & 0,0,0,1,1,1,1,0,1,0,1,1,0,0,1,0,0,0,1,1 \\ u_i & 0,0,0,0,1,1,1,1,0,1,0,1,1,1,0,0,0,0,1,1 \\ & 0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9 \end{array}$$

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 $(7-13)/20=-\frac{3}{10}$.

$$\begin{array}{ll} v_i & 1,1,0,0,1,0,1,1,1,0,0,1,0,1,1,1,0,0,1,0 \\ u_i & 0,0,1,0,1,1,1,1,0,1,0,1,1,0,0,0,1,0,0,1 \end{array}$$

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

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** saw this on Thursday for the cases $m = 1$ and $m = 2$; the general case is proved using 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

$$(x_0, \ldots, x_{92}) \mapsto \big(x_1, \ldots, x_{92}, f(x, y, z)\big).$$

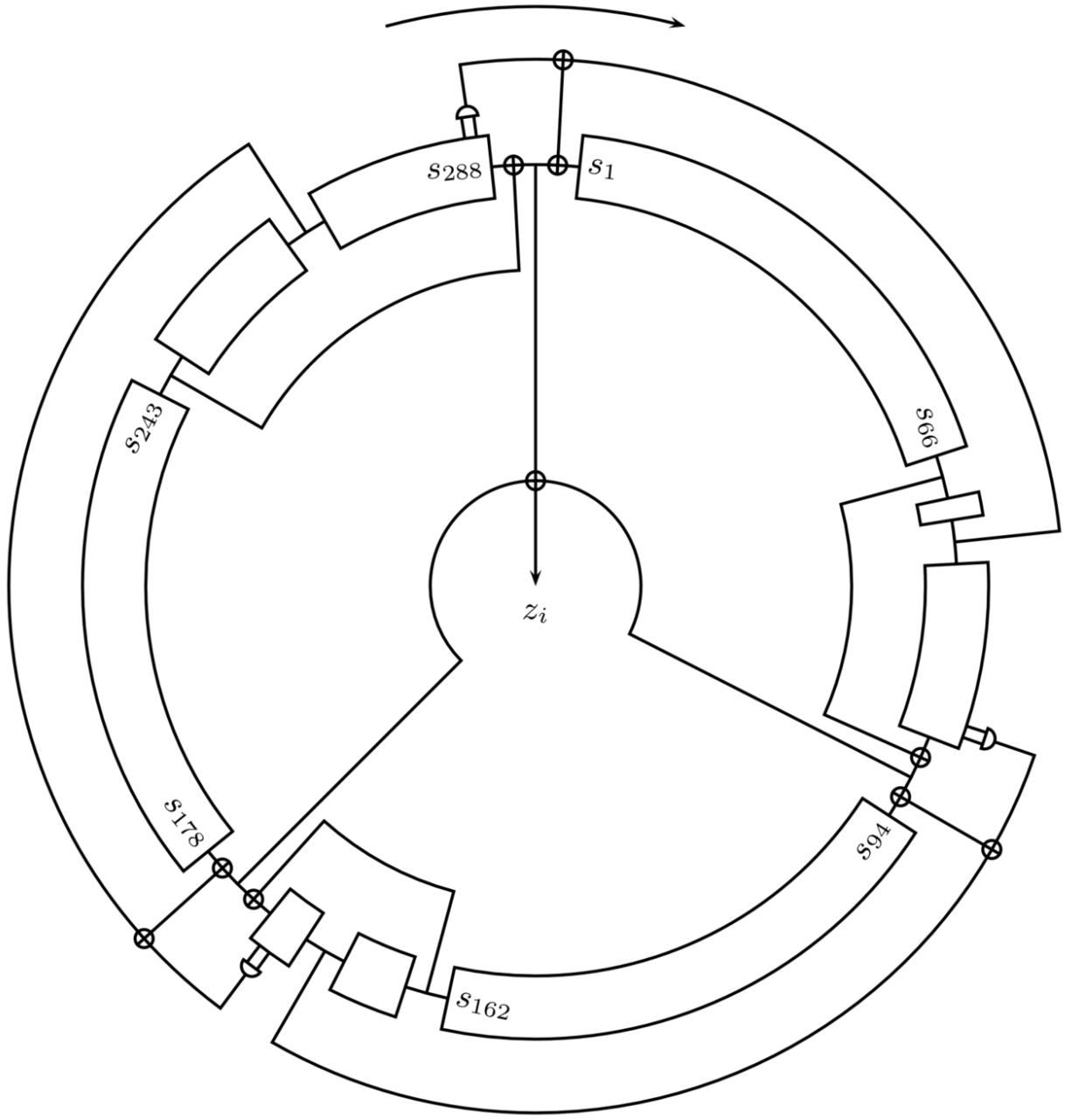
The keystream bit from each step is

$$x_0 + x_{93-66} + y_0 + y_{84-69} + z_0 + z_{111-66}.$$

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.

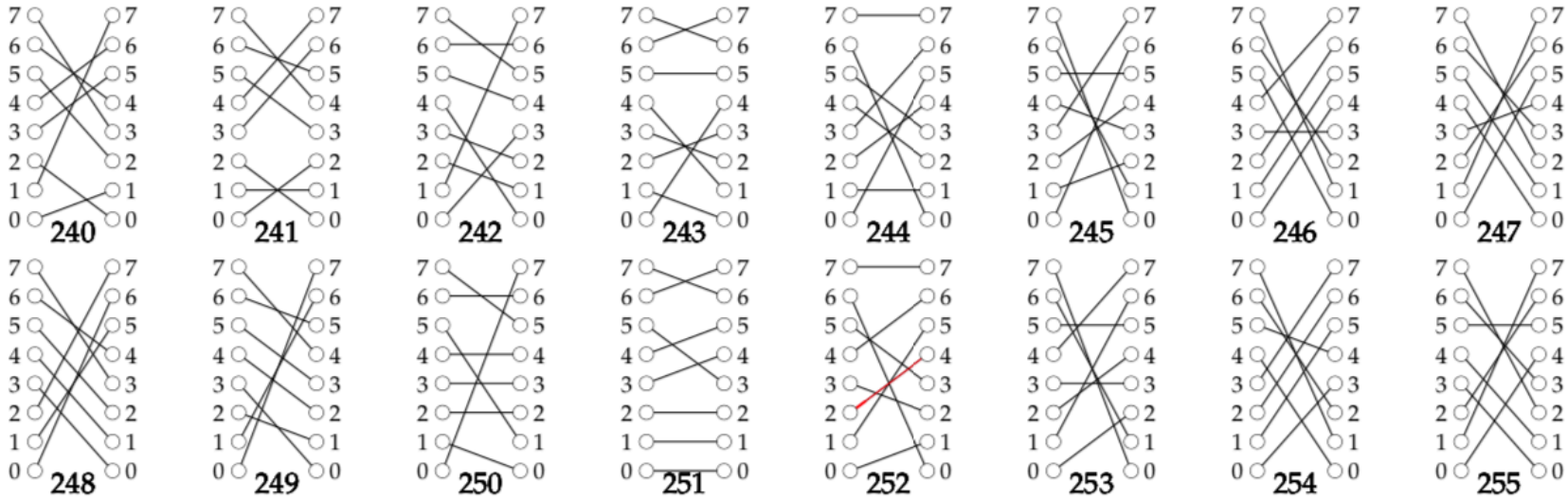
Example 9.1

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 permutations $\mathbb{F}_2^3 \to \mathbb{F}_2^3$, 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, $e_{\mathbf{252}}(2) = 4$



The other 240 permutations are posted on Moodle and will be available in the lecture. [**Please take a fresh sheet.**]

Example 8.2 [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 $8! = 40320$ permutations of $\mathbb{F}_2^3$, of which 256 were used.

Example 8.2 [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 $8! = 40320$ permutations of $\mathbb{F}_2^3$, of which 256 were used.

Example 8.2 [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 $8! = 40320$ permutations of $\mathbb{F}_2^3$, of which 256 were used.

- Correction: in the example of storing a permutation, I said AES had block size 64. I meant DES. (AES has block size 128.)
- Please see updated answers and feedback for Problem Sheet 5 on Moodle. Often more explanation was needed for full marks.

(3) (a) Let $k_0k_1k_2k_3k_4k_5k_6k_7$ be the keystream of an LFSR of width 4. (The taps could be anything.) Show that the the matrix equation

$$\begin{pmatrix} k_0 & k_1 & k_2 & k_3 \\ k_1 & k_2 & k_3 & k_4 \\ k_2 & k_3 & k_4 & k_5 \\ k_3 & k_4 & k_5 & k_6 \end{pmatrix} \begin{pmatrix} b_4 \\ b_3 \\ b_2 \\ b_1 \end{pmatrix} = \begin{pmatrix} k_4 \\ k_5 \\ k_6 \\ k_7 \end{pmatrix}$$

has a solution b_4, b_3, b_2, b_1. [*Hint:* remember that if T is the taps then $k_s = \sum_{t \in T} k_{s-t}$ for each $s \geq \ell$. Relate this to the four equations from the matrix.]

(b) Is the converse to (a) true? Justify your answer.

(c) Which of the bit sequences 00100110, 00100111, 11100001 and 0110111 is a keystream of an LFSR of width 4? (In the last you are only given $k_0k_1 \ldots k_6$.) Justify your answers. Do they change if the LFSR is required to be invertible?

Problem Sheet 5 Question 5

Let $B_0, B_1, \ldots, B_{n-1}$ be a sequence of bits, each 0 or 1 independently with probability $\frac{1}{2}$. For $b, b' \in \{0, 1\}$, let $M_{bb'}$ be the number of $i \in \{0, \ldots, n-2\}$ such that $(B_i, B_{i+1}) = (b, b')$.

(a) Show that the expected value of M_{00} is $\mathbb{E}[M_{00}] = (n-1)/4$ and find $\mathbb{E}[M_{01}], \mathbb{E}[M_{10}], \mathbb{E}[M_{11}]$.

(b) Does the sequence below pass the monobit test in Exercise 7.4?

0,1,0,1,1,0,0,1,0,1,0,1,0,1,0,1,0,0,1,1,0,0,1,1,0,0,1,0,1,0,1,1,0

What is n and what are the statistics M_{00}, M_{10}, M_{01}, M_{11} for this sequence?

(c) Perform a χ^2-test on $M_{00}, M_{01}, M_{10}, M_{11}$ to test the sequence in (b) for randomness on pairs of bits. [*Hint:* use $M_{00} + M_{01} + M_{10} + M_{11} = n$ to determine the degrees of freedom.]

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) $(1001\,1110)$

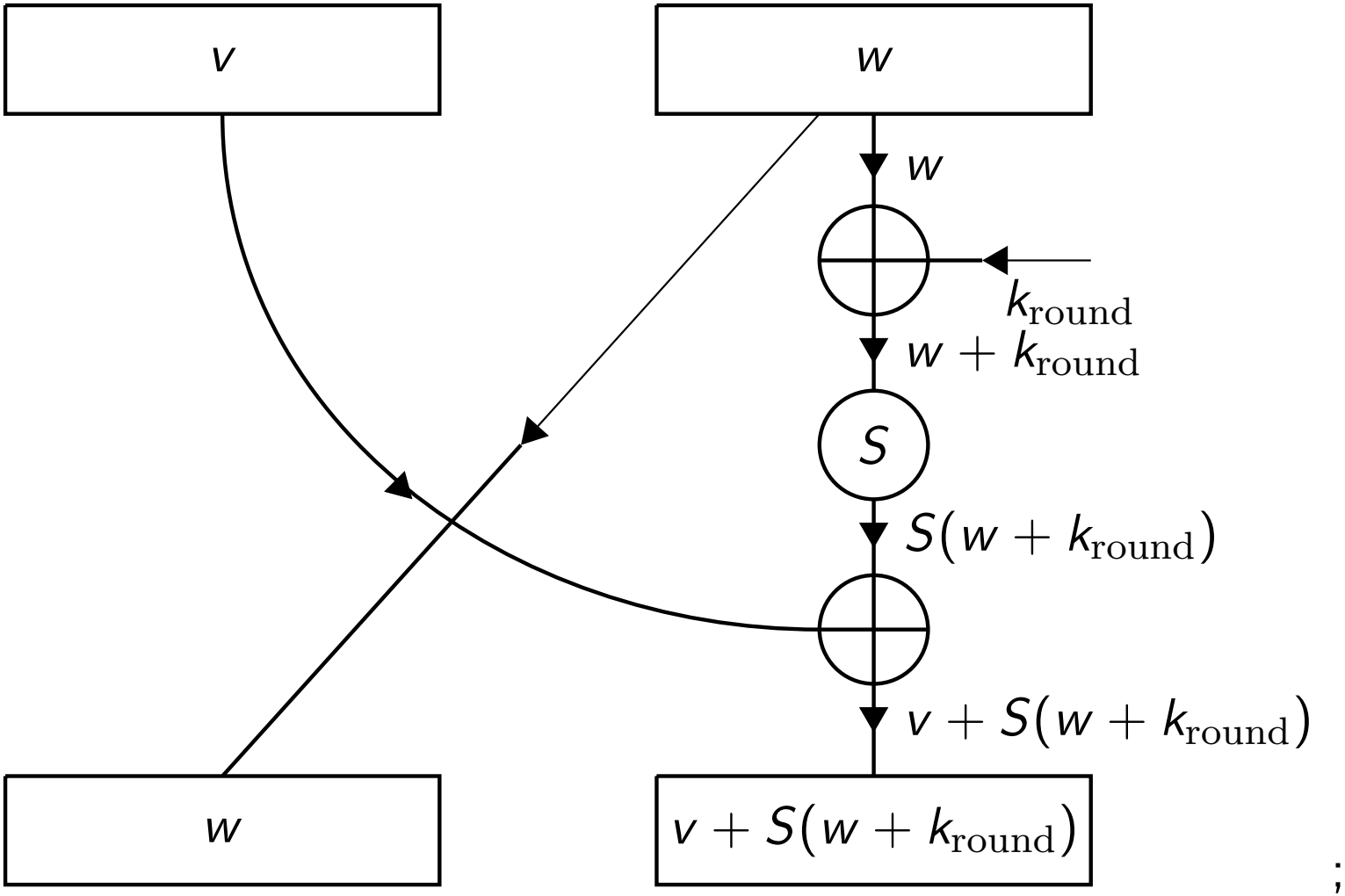
(C) $(0100\,1110)$ (D) $(1110\,1011)$

(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 $v^{(2)}$?

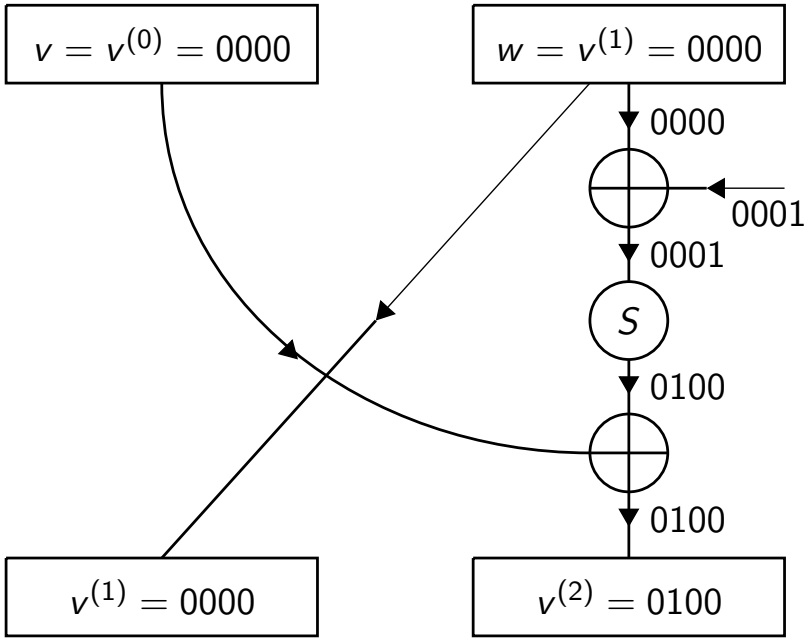
(A) k (B) $k_0 k_1 k_2 k_3$ (C) $k_4 k_5 k_6 k_7$ (D) $k_8 k_9 k_{10} k_{11}$

Exercise 9.6(a): $(v, w) \mapsto \big(w + v + S(w + k_{\text{round}})\big)$

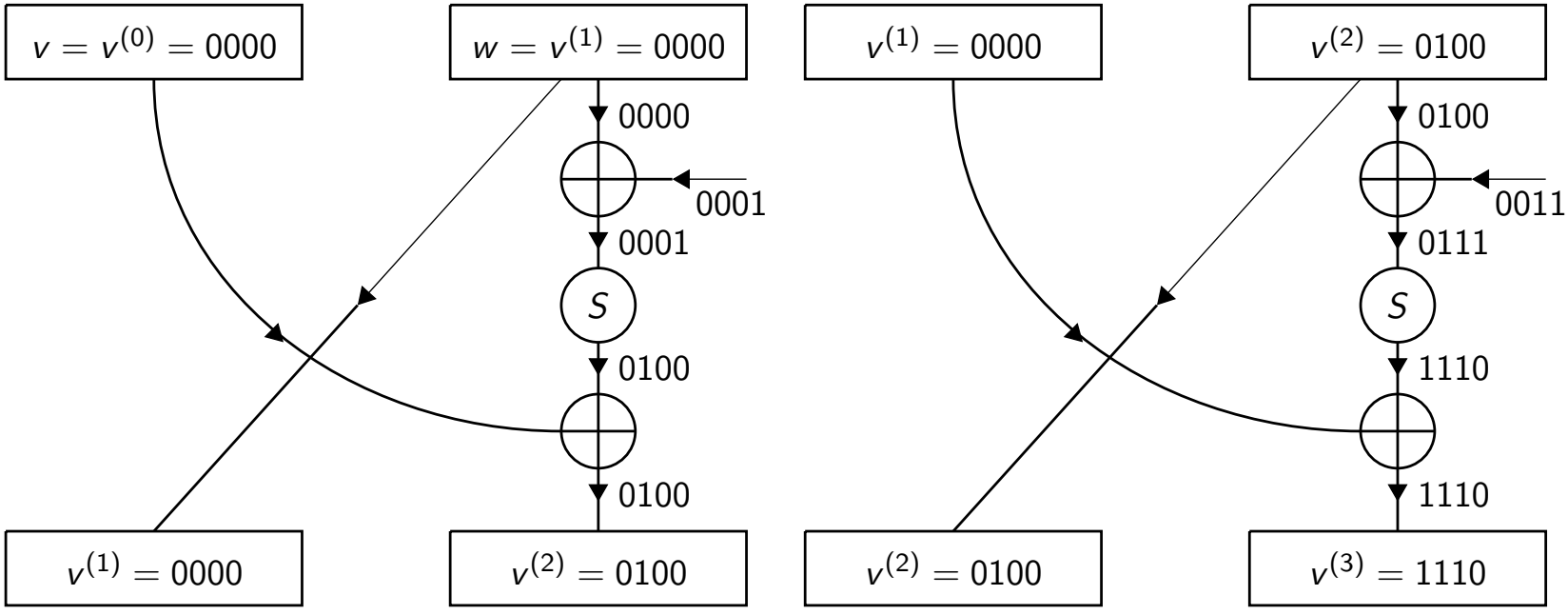


;

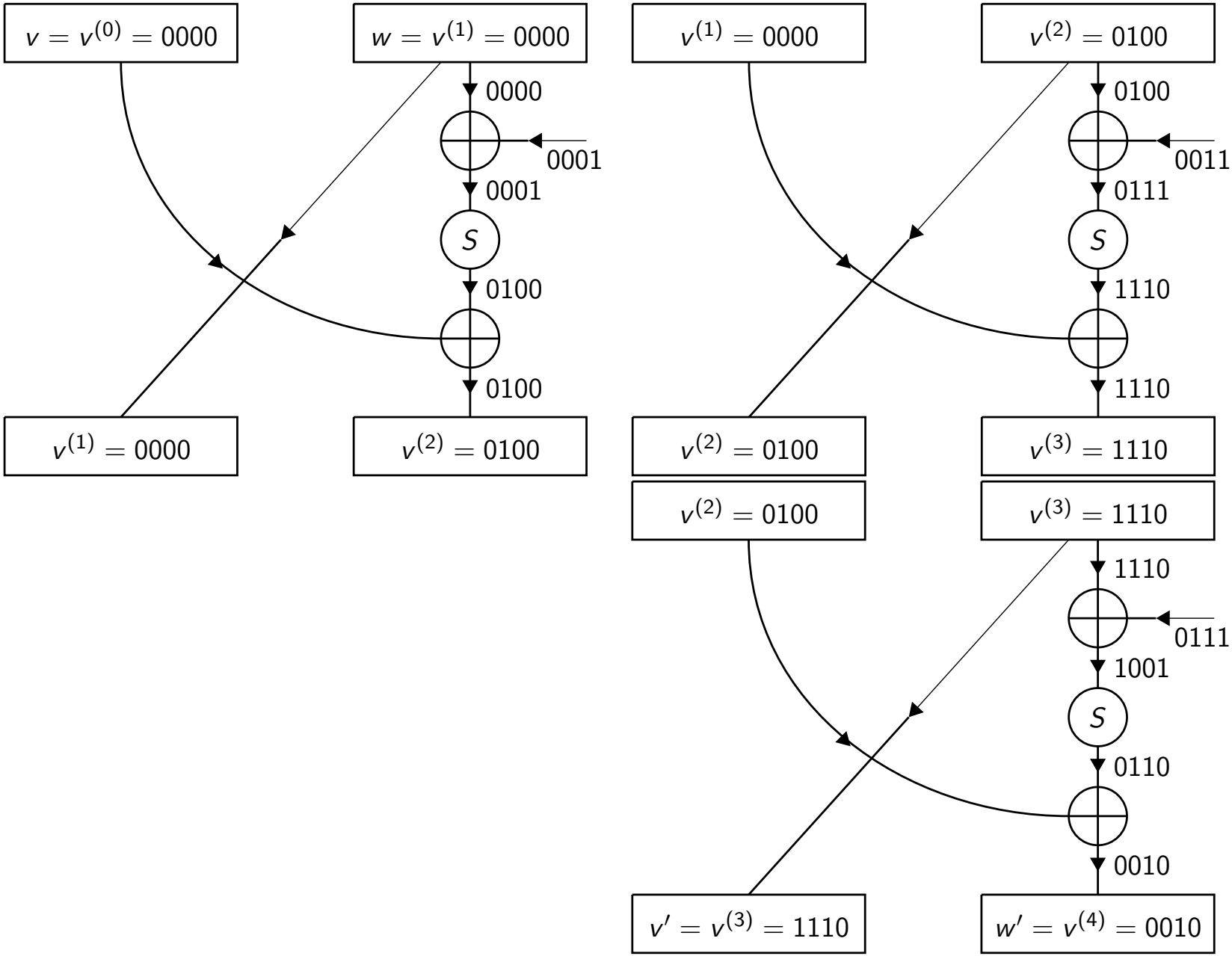
Exercise 9.6(a): $(v, w) \mapsto \big(w + v + S(w + k_{\text{round}})\big)$



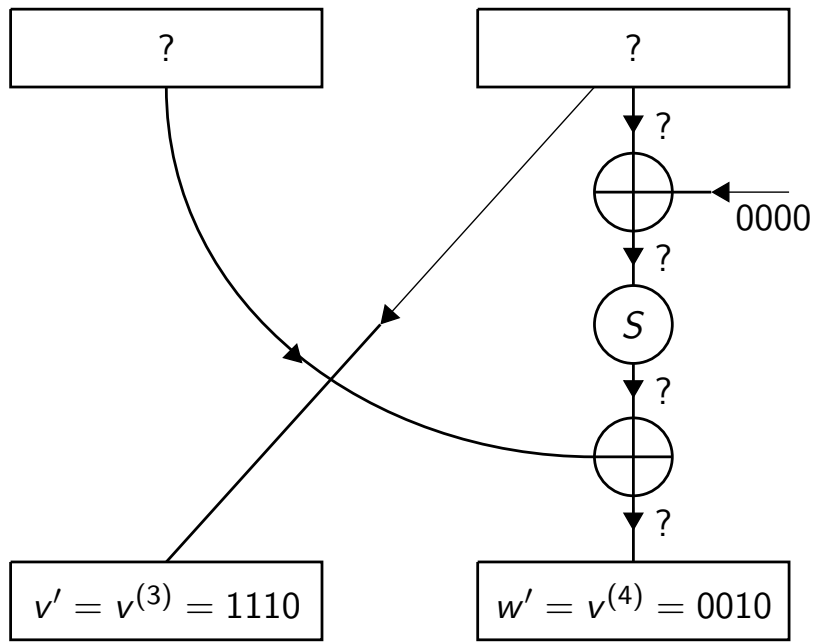
Exercise 9.6(a): $(v, w) \mapsto \big(w + v + S(w + k_{\text{round}})\big)$



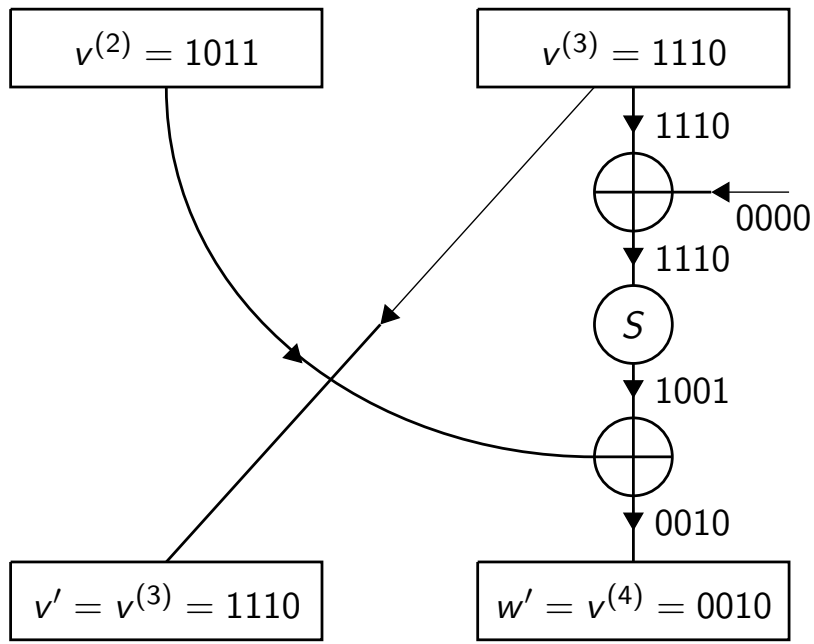
Exercise 9.6(a): $(v, w) \mapsto \big(w + v + S(w + k_{\text{round}})\big)$



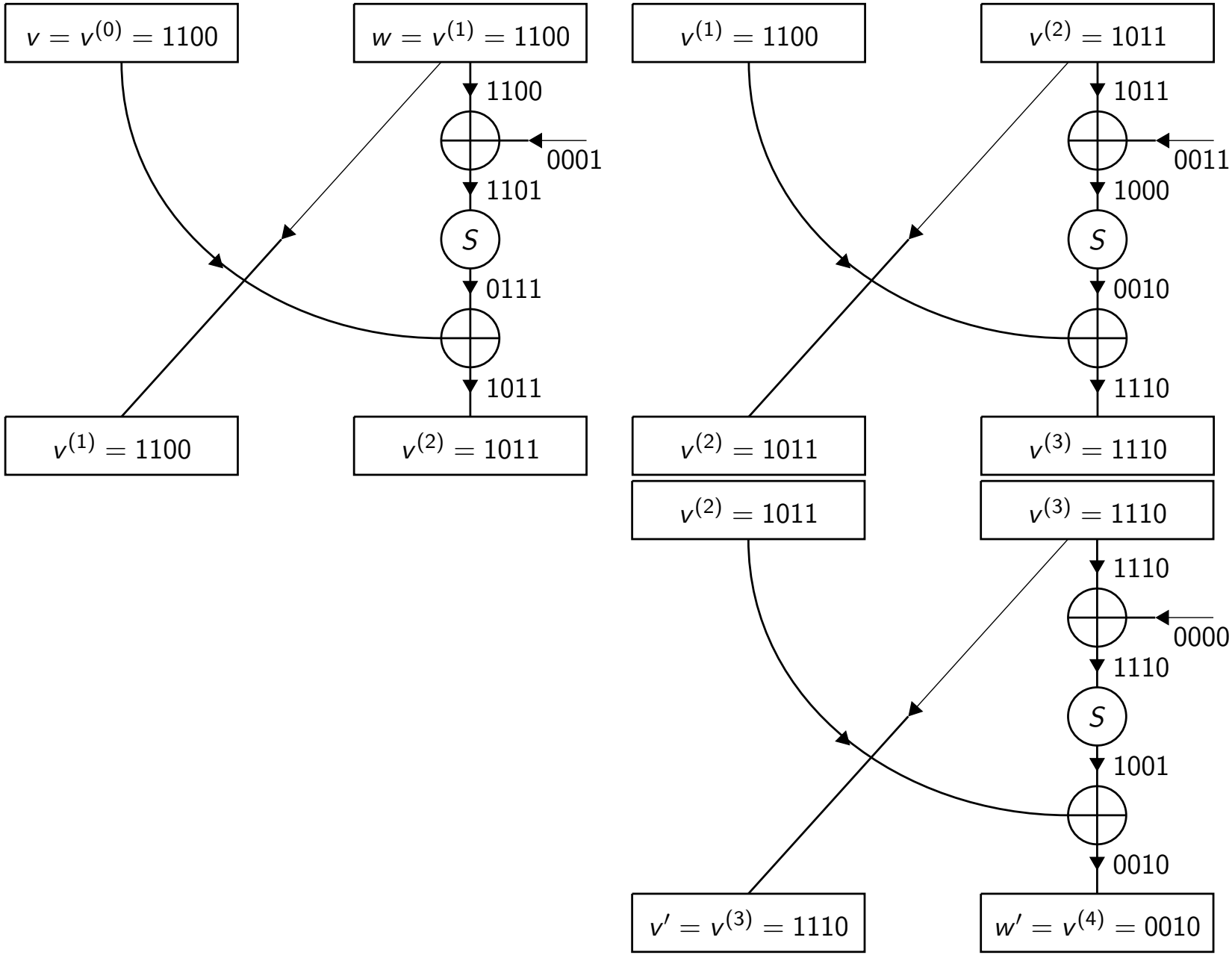
Exercise 9.6(b): $(v', w') \mapsto \left(w' + S(v' + k_{\text{round}}), v'\right)$



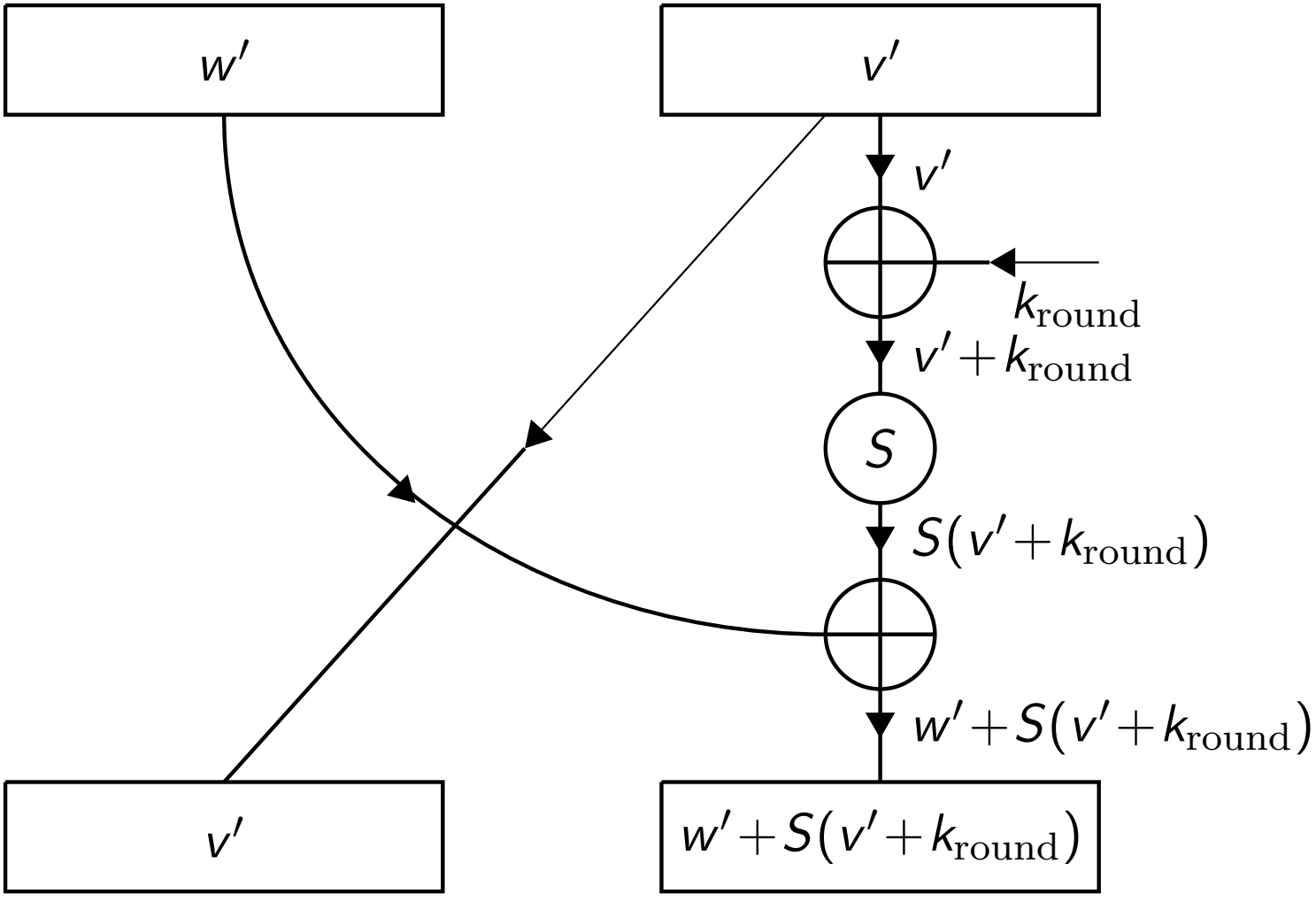
Exercise 9.6(b): $(v', w') \mapsto \left(w' + S(v' + k_{\text{round}}), v'\right)$



Exercise 9.6(b): $(v', w') \mapsto \left(w' + S(v' + k_{\text{round}}), v'\right)$

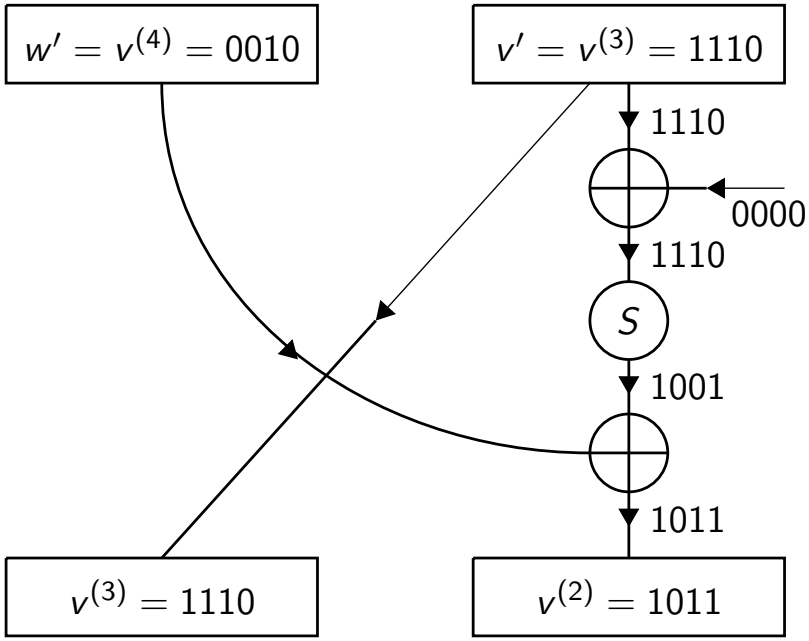


Exercise 9.6(b) flip: $(w', v') \mapsto \big(v', w' + S(v' + k_{\text{round}})\big)$

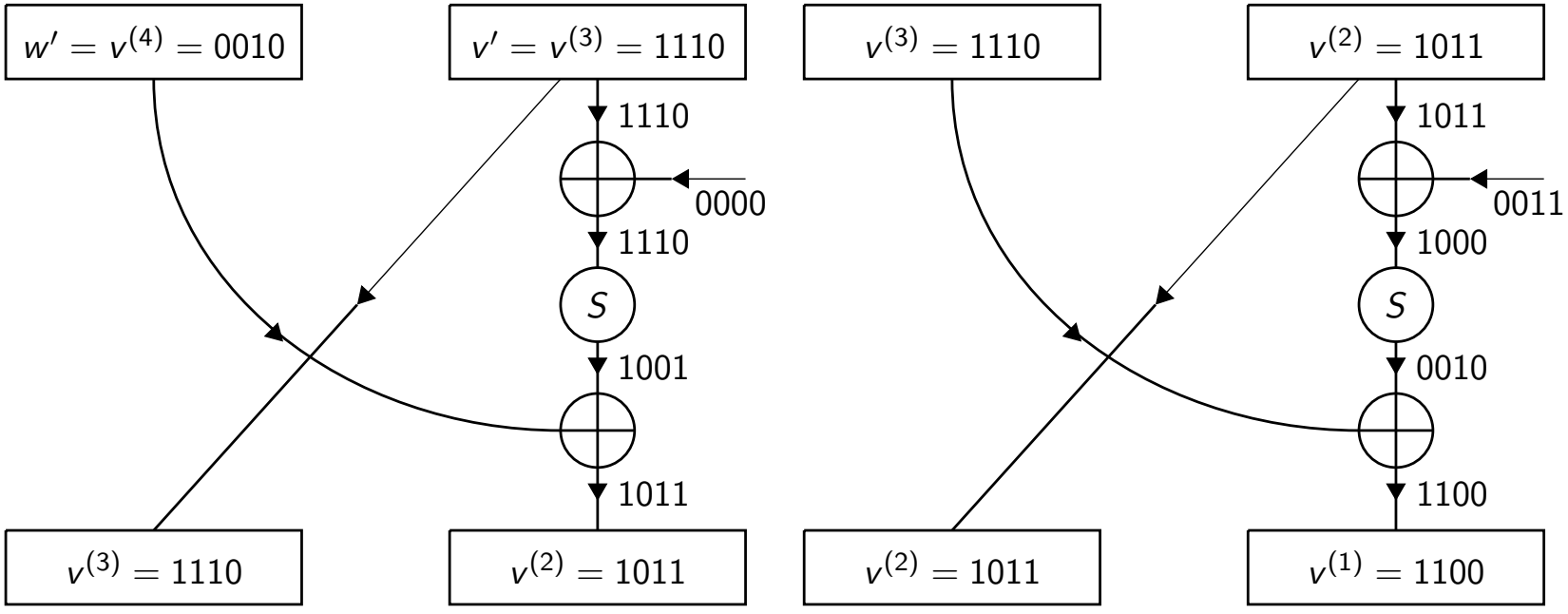


;

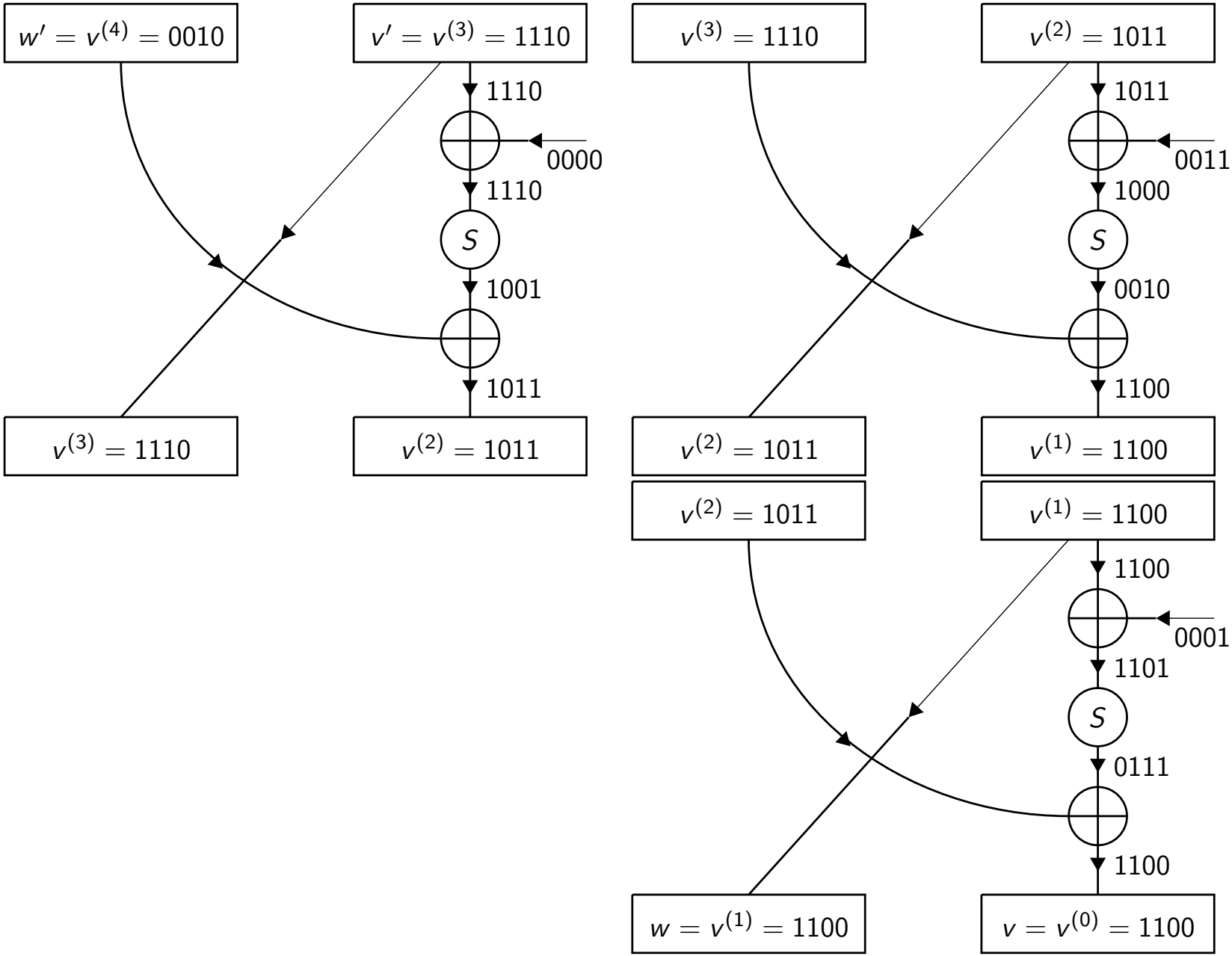
Exercise 9.6(b) flip: $(w', v') \mapsto \big(v', w' + S(v' + k_{\text{round}})\big)$



Exercise 9.6(b) flip: $(w', v') \mapsto \left(v', w' + S(v' + k_{\text{round}})\right)$



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 permutation (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* 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 may choose any 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 unknown

$$(k, k') \in \mathbb{F}_2^{56} \times \mathbb{F}_2^{56}.$$

Meet-in-the-Middle Attack on 2DES

In a chosen plaintext attack on 2DES we may choose any 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 unknown

$$(k, k') \in \mathbb{F}_2^{56} \times \mathbb{F}_2^{56}.$$

We defined

$$E = \{\big(k_\star, e_{k_\star}(x)\big) : k_\star \in \mathbb{F}_2^{56}\}$$
$$D = \{\big(k'_\star, d_{k'_\star}(z)\big) : k'_\star \in \mathbb{F}_2^{56}\}.$$

Assume that k and k' are chosen independently. Given a random $y \in \mathbb{F}_2^{64}$, what, approximately, is the probability that $(k_\star, y) \in E$, for some key $k_\star$?

(A) $\frac{1}{256}$ (B) $\frac{1}{128}$ (C) $\frac{1}{8}$ (D) 1

Meet-in-the-Middle Attack on 2DES

In a chosen plaintext attack on 2DES we may choose any 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 unknown

$$(k, k') \in \mathbb{F}_2^{56} \times \mathbb{F}_2^{56}.$$

We defined

$$E = \{\big(k_\star, e_{k_\star}(x)\big) : k_\star \in \mathbb{F}_2^{56}\}$$
$$D = \{\big(k'_\star, d_{k'_\star}(z)\big) : k'_\star \in \mathbb{F}_2^{56}\}.$$

Assume that k and k' are chosen independently. Given a random $y \in \mathbb{F}_2^{64}$, what, approximately, is the probability that $(k_\star, y) \in E$, for some key $k_\star$?

(A) $\frac{1}{256}$ (B) $\frac{1}{128}$ (C) $\frac{1}{8}$ (D) 1

What approximately is the probability that $(k_\star, y) \in E$, for some key $k_\star$ and $(k'_\star, y) \in D$ for some key $k'_\star$?

(A) $\frac{1}{2^{32}}$ (B) $\frac{1}{2^{16}}$ (C) $\frac{1}{2^8}$ (D) $\frac{1}{2^4}$

Meet-in-the-Middle Attack on 2DES

In a chosen plaintext attack on 2DES we may choose any 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 unknown

$$(k, k') \in \mathbb{F}_2^{56} \times \mathbb{F}_2^{56}.$$

We defined

$$E = \{\big(k_\star, e_{k_\star}(x)\big) : k_\star \in \mathbb{F}_2^{56}\}$$
$$D = \{\big(k'_\star, d_{k'_\star}(z)\big) : k'_\star \in \mathbb{F}_2^{56}\}.$$

Assume that k and k' are chosen independently. Given a random $y \in \mathbb{F}_2^{64}$, what, approximately, is the probability that $(k_\star, y) \in E$, for some key $k_\star$?

(A) $\frac{1}{256}$ (B) $\frac{1}{128}$ (C) $\frac{1}{8}$ (D) 1

What approximately is the probability that $(k_\star, y) \in E$, for some key $k_\star$ and $(k'_\star, y) \in D$ for some key $k'_\star$?

(A) $\frac{1}{2^{32}}$ (B) $\frac{1}{2^{16}}$ (C) $\frac{1}{2^8}$ (D) $\frac{1}{2^4}$

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 may choose any 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 unknown

$$(k, k') \in \mathbb{F}_2^{56} \times \mathbb{F}_2^{56}.$$

We defined

$$E = \{\big(k_\star, e_{k_\star}(x)\big) : k_\star \in \mathbb{F}_2^{56}\}$$
$$D = \{\big(k'_\star, d_{k'_\star}(z)\big) : k'_\star \in \mathbb{F}_2^{56}\}.$$

Assume that k and k' are chosen independently. Given a random $y \in \mathbb{F}_2^{64}$, what, approximately, is the probability that $(k_\star, y) \in E$, for some key $k_\star$?

(A) $\frac{1}{256}$ (B) $\frac{1}{128}$ (C) $\frac{1}{8}$ (D) 1

What approximately is the probability that $(k_\star, y) \in E$, for some key $k_\star$ and $(k'_\star, y) \in D$ for some key $k'_\star$?

(A) $\frac{1}{2^{32}}$ (B) $\frac{1}{2^{16}}$ (C) $\frac{1}{2^8}$ (D) $\frac{1}{2^4}$

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:

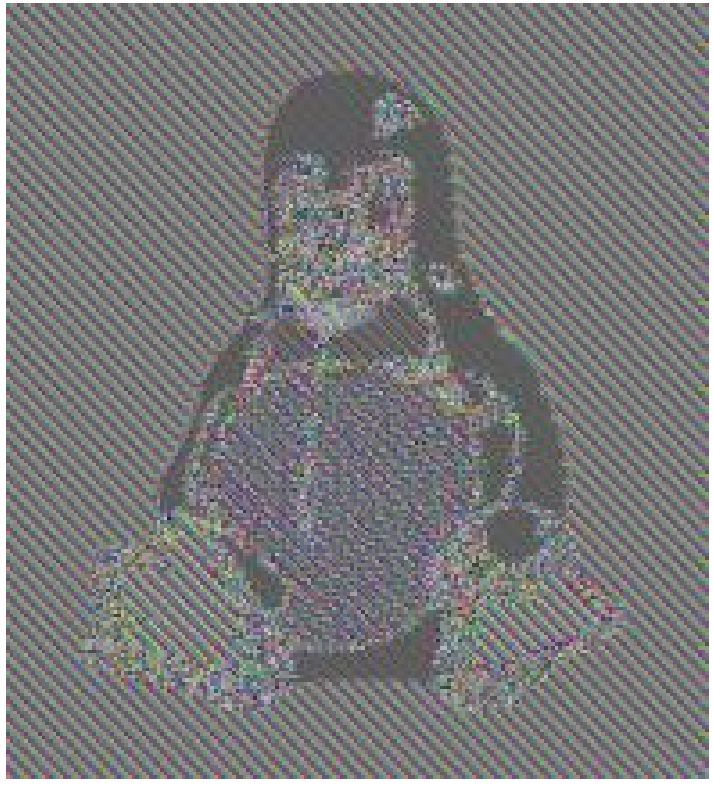
$$\begin{aligned} x^{(1)} &\mapsto e_k(x^{(1)}) \\ x^{(2)} &\mapsto e_k(x^{(2)}) \\ &\vdots \\ x^{(m)} &\mapsto e_k(x^{(m)}) \end{aligned}$$

- 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.

§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 2 on Problem Sheet 3. We have unknown plaintexts x, $x' \in \mathbb{F}_2^n$, an unknown key $k_{\text{otp}} \in \mathbb{F}_2^n$, and known ciphertexts $x + k_{\text{otp}}$ and $x' + k_{\text{otp}}$. Adding the known ciphertexts gives $x + x'$, independent of k_{otp}.

§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 2 on Problem Sheet 3. We have unknown plaintexts x, $x' \in \mathbb{F}_2^n$, an unknown key $k_{\text{otp}} \in \mathbb{F}_2^n$, and known ciphertexts $x + k_{\text{otp}}$ and $x' + k_{\text{otp}}$. Adding the known ciphertexts gives $x + x'$, independent of k_{otp}.

Thus if x and x' differ by Δ then so do their encryptions $x + k_{\text{otp}}$ and $x' + k_{\text{otp}}$. In symbols:

$$x + x' = \Delta \implies (x + k_{\text{otp}}) + (x' + k_{\text{otp}}) = \Delta.$$

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 2 on Problem Sheet 3. We have unknown plaintexts x, $x' \in \mathbb{F}_2^n$, an unknown key $k_{\text{otp}} \in \mathbb{F}_2^n$, and known ciphertexts $x + k_{\text{otp}}$ and $x' + k_{\text{otp}}$. Adding the known ciphertexts gives $x + x'$, independent of k_{otp}.

Thus if x and x' differ by Δ then so do their encryptions $x + k_{\text{otp}}$ and $x' + k_{\text{otp}}$. In symbols:

$$x + x' = \Delta \implies (x + k_{\text{otp}}) + (x' + k_{\text{otp}}) = \Delta.$$

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 2 on Problem Sheet 3. We have unknown plaintexts x, $x' \in \mathbb{F}_2^n$, an unknown key $k_{\text{otp}} \in \mathbb{F}_2^n$, and known ciphertexts $x + k_{\text{otp}}$ and $x' + k_{\text{otp}}$. Adding the known ciphertexts gives $x + x'$, independent of k_{otp}.

Thus if x and x' differ by Δ then so do their encryptions $x + k_{\text{otp}}$ and $x' + k_{\text{otp}}$. In symbols:

$$x + x' = \Delta \implies (x + k_{\text{otp}}) + (x' + k_{\text{otp}}) = \Delta.$$

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 $(x + k_{\text{otp}}) - (x' + k_{\text{otp}}) = \Delta$

(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 2 on Problem Sheet 3. We have unknown plaintexts x, $x' \in \mathbb{F}_2^n$, an unknown key $k_{\text{otp}} \in \mathbb{F}_2^n$, and known ciphertexts $x + k_{\text{otp}}$ and $x' + k_{\text{otp}}$. Adding the known ciphertexts gives $x + x'$, independent of k_{otp}.

Thus if x and x' differ by Δ then so do their encryptions $x + k_{\text{otp}}$ and $x' + k_{\text{otp}}$. In symbols:

$$x + x' = \Delta \implies (x + k_{\text{otp}}) + (x' + k_{\text{otp}}) = \Delta.$$

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 $(x + k_{\text{otp}}) - (x' + k_{\text{otp}}) = \Delta$

(B) It's the same: we're working in $\mathbb{F}_2$

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* **[Correction.]**

$$\big(v+\mathbf{0000}, w+\mathbf{1000}\big) \mapsto \big(w, v+S(w+k^{(1)})\big)++(\mathbf{1000}, \mathbf{0010}).$$

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* **[Correction.]**

$$\big(v+\mathbf{0000}, w+\mathbf{1000}\big) \mapsto \big(w, v+S(w+k^{(1)})\big)++(\mathbf{1000}, \mathbf{0010}).$$

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.

Corrections

- At the end of the proof of Lemma 10.1, I wrote

$$\big(w + \mathbf{1000}, S(v + k^{(1)})\big) + (\mathbf{1000}, \mathbf{0010})$$

  putting in the difference twice. This should have been

$$\big(w, S(v + k^{(1)})\big) + (\mathbf{1000}, \mathbf{0010}).$$

- **M.Sc.** Question 5 on Sheet 7: the taps are $\{1, 4\}$ not $\{0, 3\}$. (Last year's convention, sorry.)

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*

$$\big(v+\mathbf{0000}, w+\mathbf{1000}\big) \mapsto \big(w, v+S(w+k^{(1)})\big)+(\mathbf{1000}, \mathbf{0010}).$$

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Meet our alumni mathematicians...

Sophie Christiansen CBE

(MSci Mathematics 2011)

Sportswoman, software developer and disability campaigner, winner of eight Gold medals, a Silver medal and a Bronze medal at Athens 2004, Beijing 2008, London 2012, and Rio 2016 Paralympic equestrian events, Sophie has brought a gold post box to the campus.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Meet our alumni mathematicians...

Bobby Seagull

(BSc Economics and Mathematics 2007)

Mathematician, school teacher and author, UK library champion, University Challenge team captain and host of Monkman & Seagull's Genius Guide to Britain, Bobby seeks to demystify maths in everyday life and creates puzzles for fun.

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 $k^{(2)} = 0011$, $k^{(3)} = 1111$ then $w = 1011\,0110$ and $w_\Delta = 0011\,0100$. Hence $\boldsymbol{\Delta}_\star = \mathbf{1000\,0010}$ and we do not know (yet) that the guess is wrong.

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 $k^{(2)} = 0011$, $k^{(3)} = 1111$ then $w = 1011\,0110$ and $w_\Delta = 0011\,0100$. Hence $\boldsymbol{\Delta}_\star = \mathbf{1000\,0010}$ and we do not know (yet) that the guess is wrong.

Exercise 10.2

Assume that the difference attack shows the key is one of 16 possible $(k^{(2)}_{\text{guess}}, k^{(3)}_{\text{guess}})$. Show that it is subexhaustive: that is, it requires less computing than trying all $2^{12} = 4096$ keys.

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

$$e_{(A,b)}(x) = xA + b.$$

We will define the decryption functions in lectures. By Question 4 on Problem Sheet 8, the key in the affine block cipher can be deduced by a known plaintext attack using $n + 1$ chosen plaintexts.

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 **[correction]** $z^8 = 1 + z + z^3 + z^4$.

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 permutation of the 16 subblocks, organized into a 4×4 grid

$$\begin{array}{cccc} q(0) & q(4) & q(8) & q(12) \\ q(1) & q(5) & q(9) & q(13) \\ q(2) & q(6) & q(10) & q(14) \\ q(3) & q(7) & q(11) & q(15) \end{array} \longrightarrow \begin{array}{cccc} q(0) & q(4) & q(8) & q(12) \\ q(13) & q(1) & q(5) & q(9) \\ q(10) & q(14) & q(2) & q(6) \\ q(7) & q(11) & q(15) & q(3) \end{array}$$

  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

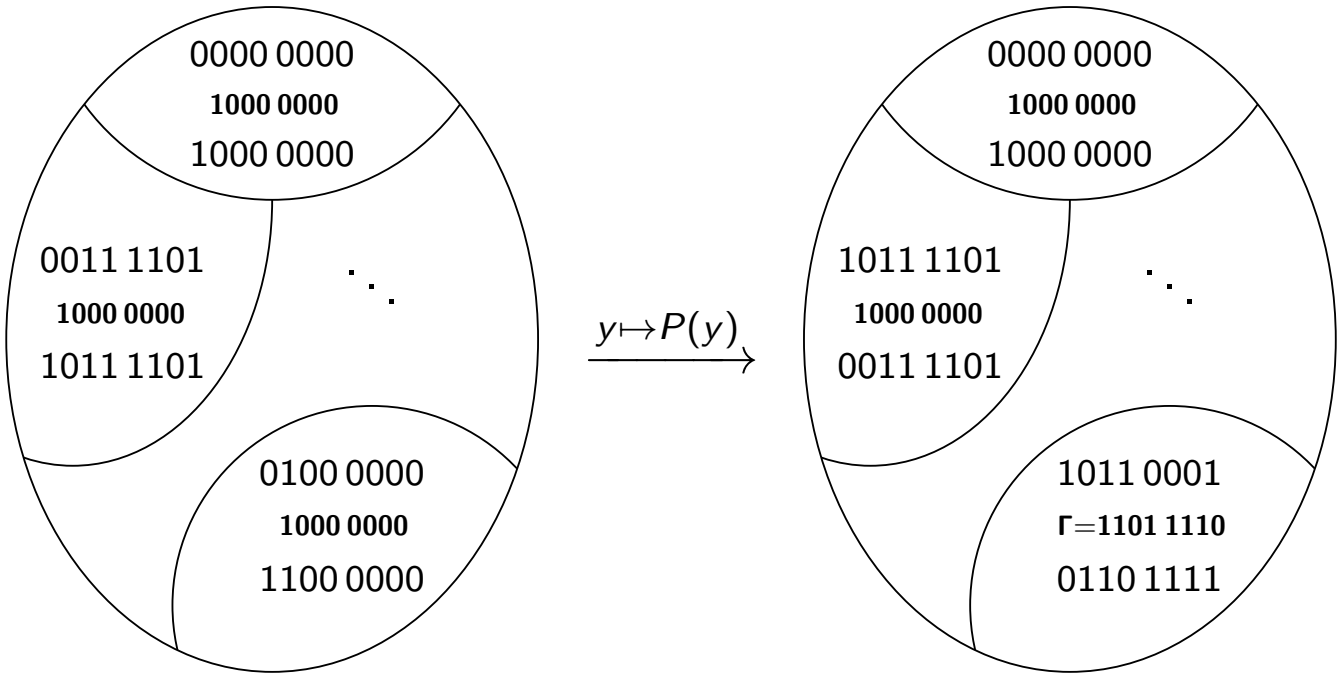
Lemma 10.8

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.

Grace Murray Hopper, American Cryptanalyst

Problem Sheet 8

- Please take the Part D handout
- Answers and feedback to Problem Sheet 7 are on Moodle
- Problem Sheet 8: the deadline is Monday 9th

Part D: Public Key Cryptography and Digital Signatures

§11 Introduction to Public Key Cryptography

We begin with a way that Alice and Bob can establish a shared secret key, communicating only over the insecure channel on page 4.

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. They agree a prime p such that $p > 2^{128}$. Then

(1) Alice chooses a secret $a \in \mathbb{N}$ with $1 \leq a < p$. Bob chooses a secret $b \in \mathbb{N}$ with $1 \leq b < p$.

(2) Alice sends Bob $2^a \bmod p$. Bob sends Alice $2^b \bmod p$.

(3) Alice computes $(2^b)^a \bmod p$ and Bob computes $(2^a)^b \bmod p$.

(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 10.1 [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 10.1 [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 10.1 [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 cryptosystems, 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, $c^{p-1} \equiv 1 \bmod c$ 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 10.1, 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 Question 3 on 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 $g^{ab} \bmod p$.

Exponentiation as a one-way function

A primitive root modulo 131 is $g = 2$.

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), working modulo 131. For example $2^{46} \equiv 5 \bmod 131$ so the discrete log of 5 is 46.

(a) What is the discrete log of 16?

(A) 1 (B) 2 (C) 4 (D) 130

(b) What is the discrete log of 125?

(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 the discrete log of 130? [Hint: $130^2 \equiv (-1)^2 \equiv 1$.]

(A) 1 (B) 65 (C) 66 (D) 130

(e) The discrete log of 49 is 62. So the discrete log of 7 is 31?

(A) False (B) True

Exponentiation as a one-way function

A primitive root modulo 131 is $g = 2$.

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), working modulo 131. For example $2^{46} \equiv 5 \bmod 131$ so the discrete log of 5 is 46.

(a) What is the discrete log of 16?

(A) 1 (B) 2 (C) 4 (D) 130

(b) What is the discrete log of 125?

(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 the discrete log of 130? [Hint: $130^2 \equiv (-1)^2 \equiv 1$.]

(A) 1 (B) 65 (C) 66 (D) 130

(e) The discrete log of 49 is 62. So the discrete log of 7 is 31?

(A) False (B) True

Exponentiation as a one-way function

A primitive root modulo 131 is $g = 2$.

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), working modulo 131. For example $2^{46} \equiv 5 \bmod 131$ so the discrete log of 5 is 46.

(a) What is the discrete log of 16?

(A) 1 (B) 2 (C) 4 (D) 130

(b) What is the discrete log of 125?

(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 the discrete log of 130? [Hint: $130^2 \equiv (-1)^2 \equiv 1$.]

(A) 1 (B) 65 (C) 66 (D) 130

(e) The discrete log of 49 is 62. So the discrete log of 7 is 31?

(A) False (B) True

Exponentiation as a one-way function

A primitive root modulo 131 is $g = 2$.

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), working modulo 131. For example $2^{46} \equiv 5 \bmod 131$ so the discrete log of 5 is 46.

(a) What is the discrete log of 16?

(A) 1 (B) 2 (C) 4 (D) 130

(b) What is the discrete log of 125?

(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 the discrete log of 130? [Hint: $130^2 \equiv (-1)^2 \equiv 1$.]

(A) 1 (B) 65 (C) 66 (D) 130

(e) The discrete log of 49 is 62. So the discrete log of 7 is 31?

(A) False (B) True

Exponentiation as a one-way function

A primitive root modulo 131 is $g = 2$.

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), working modulo 131. For example $2^{46} \equiv 5 \bmod 131$ so the discrete log of 5 is 46.

(a) What is the discrete log of 16?

(A) 1 (B) 2 (C) 4 (D) 130

(b) What is the discrete log of 125?

(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 the discrete log of 130? [Hint: $130^2 \equiv (-1)^2 \equiv 1$.]

(A) 1 (B) 65 (C) 66 (D) 130

(e) The discrete log of 49 is 62. So the discrete log of 7 is 31?

(A) False (B) True

Exponentiation as a one-way function

A primitive root modulo 131 is $g = 2$.

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), working modulo 131. For example $2^{46} \equiv 5 \bmod 131$ so the discrete log of 5 is 46.

(a) What is the discrete log of 16?

(A) 1 (B) 2 (C) 4 (D) 130

(b) What is the discrete log of 125?

(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 the discrete log of 130? [Hint: $130^2 \equiv (-1)^2 \equiv 1$.]

(A) 1 (B) 65 (C) 66 (D) 130

(e) The discrete log of 49 is 62. So the discrete log of 7 is 31?

(A) False (B) True

Exponentiation as a one-way function

A primitive root modulo 131 is $g = 2$.

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), working modulo 131. For example $2^{46} \equiv 5 \bmod 131$ so the discrete log of 5 is 46.

(e) The discrete log of 49 is 62. So the discrete log of 7 is 31?

(A) False (B) True

Explanation: there are two square roots of 49, namely 7 and $-7 \equiv 124 \bmod 131$. Calculating shows that $2^{31} \equiv 124 \equiv -7 \bmod 131$. To get 7 we use (d), that $2^{65} \equiv 1 \bmod 131$: so adding discrete logs,

$$\operatorname{dlog} 7 = \operatorname{dlog}(-7 \times -1) = \operatorname{dlog}(-7) + \operatorname{dlog}(-1) = 31 + 65 = 96.$$

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.

It is not known whether one-way functions exist. Their existence implies P $\neq$ NP: very roughly, if P = NP then any problem whose solution is quick to check, such as Sudoku, is also quick to solve.

Diffie–Hellman key exchange is secure only if, given g and g^x it is hard to find x. (This is called the Discrete Log Problem.) Equivalently, the function

$$f : \{0, \ldots, p-2\} \to \{1, \ldots, p-1\}$$

defined by $f(x) = g^x \bmod p$, is one-way.

ElGamal Cryptosystem and Further Comments

Diffie–Hellman can be turned into the ElGamal cryptosystem: see Question 2 on Sheet 9.

- 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. But it is more likely that the Discrete Log Problem is easy than that AES has a sub-exhaustive attack.

For these reasons block ciphers and stream ciphers are still widely used.

Inverting exponentiation mod 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 mod 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.

Equality and Diversity Survey

The Mathematics and ISG Equality and Diversity Committee wants to hear from you!

All students in the Mathematics Department and ISG are warmly encouraged to complete this survey. Go to:

- https://rhul.onlinesurveys.ac.uk/athena-swan-student-survey-mathematics-2019
- tinyurl.com/vof7lso
- use QR code below, or read your email for the link

The survey is linked to the Athena SWAN scheme. Its purpose is to promote gender equality in higher education for staff and students. Your responses will inform our Athena SWAN actions.

Athena SWAN GENDER CHARTER

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 (n, 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), [**typo in printed notes:** c **should be** a] can decrypt.

Quiz on RSA

True or false?

- Alice's encryption exponent c 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 c 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 c 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 c 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 c 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 c 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 c 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 c 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

The Key Distribution Problem

One problem with RSA is that Bob somehow has to learn Alice's public key. If Alice has no better way to email 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.

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 (the US standard body) now recommend that n should have 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 $(187, 89)$. 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 Sheet 9. (If your block has broken down, you can instead email the lecturer your public key and get a message to decrypt.)

(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.

Let p and q be primes of size about 2^{1024}. Let $n = pq$.

(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 $\{1, \ldots, p-1\} \to \{1, \ldots, p-1\}$ 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) 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 $x \mapsto x^a$ mod n is invertible.

(A) False (B) True

(f) Suppose $x \mapsto x^a$ mod n is invertible. Given a and n it is fast to compute its inverse.

(A) False (B) True

Let p and q be primes of size about 2^{1024}. Let $n = pq$.

(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 $\{1, \ldots, p-1\} \to \{1, \ldots, p-1\}$ 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) 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 $x \mapsto x^a$ mod n is invertible.

(A) False (B) True

(f) Suppose $x \mapsto x^a$ mod n is invertible. Given a and n it is fast to compute its inverse.

(A) False (B) True

Let p and q be primes of size about 2^{1024}. Let $n = pq$.

(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 $\{1, \ldots, p-1\} \to \{1, \ldots, p-1\}$ 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) 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 $x \mapsto x^a$ mod n is invertible.

(A) False (B) True

(f) Suppose $x \mapsto x^a$ mod n is invertible. Given a and n it is fast to compute its inverse.

(A) False (B) True

Let p and q be primes of size about 2^{1024}. Let $n = pq$.

(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 $\{1, \ldots, p-1\} \to \{1, \ldots, p-1\}$ 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) 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 $x \mapsto x^a$ mod n is invertible.

(A) False (B) True

(f) Suppose $x \mapsto x^a$ mod n is invertible. Given a and n it is fast to compute its inverse.

(A) False (B) True

Let p and q be primes of size about 2^{1024}. Let $n = pq$.

(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 $\{1, \ldots, p-1\} \to \{1, \ldots, p-1\}$ 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) 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 $x \mapsto x^a$ mod n is invertible.

(A) False (B) True

(f) Suppose $x \mapsto x^a$ mod n is invertible. Given a and n it is fast to compute its inverse.

(A) False (B) True

Let p and q be primes of size about 2^{1024}. Let $n = pq$.

(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 $\{1, \ldots, p-1\} \to \{1, \ldots, p-1\}$ 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) 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 $x \mapsto x^a$ mod n is invertible.

(A) False (B) True

(f) Suppose $x \mapsto x^a$ mod n is invertible. Given a and n it is fast to compute its inverse.

(A) False (B) True

Let p and q be primes of size about 2^{1024}. Let $n = pq$.

(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 $\{1, \ldots, p-1\} \to \{1, \ldots, p-1\}$ 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) 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 $x \mapsto x^a$ mod n is invertible.

(A) False (B) True

(f) Suppose $x \mapsto x^a$ mod n is invertible. Given a and n it is fast to compute its inverse.

(A) False (B) True

RSA as an Illegal Munition

§12 Digital Signatures and Hash Functions

Suppose Alice and Bob have the RSA keys:

	public	private
Alice	(m, a)	(m, r)
Bob	(n, b)	(n, s)

Suppose Alice wants to tell Bob his 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)	(m, r)
Bob	(n, b)	(n, s)

Suppose Alice wants to tell Bob his 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)	(m, r)
Bob	(n, b)	(n, 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

$$e_A(x) = x^a \bmod m \quad d_A(x) = x^r \bmod m$$
$$e_B(x) = x^b \bmod n \quad d_B(x) = x^s \bmod n.$$

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?

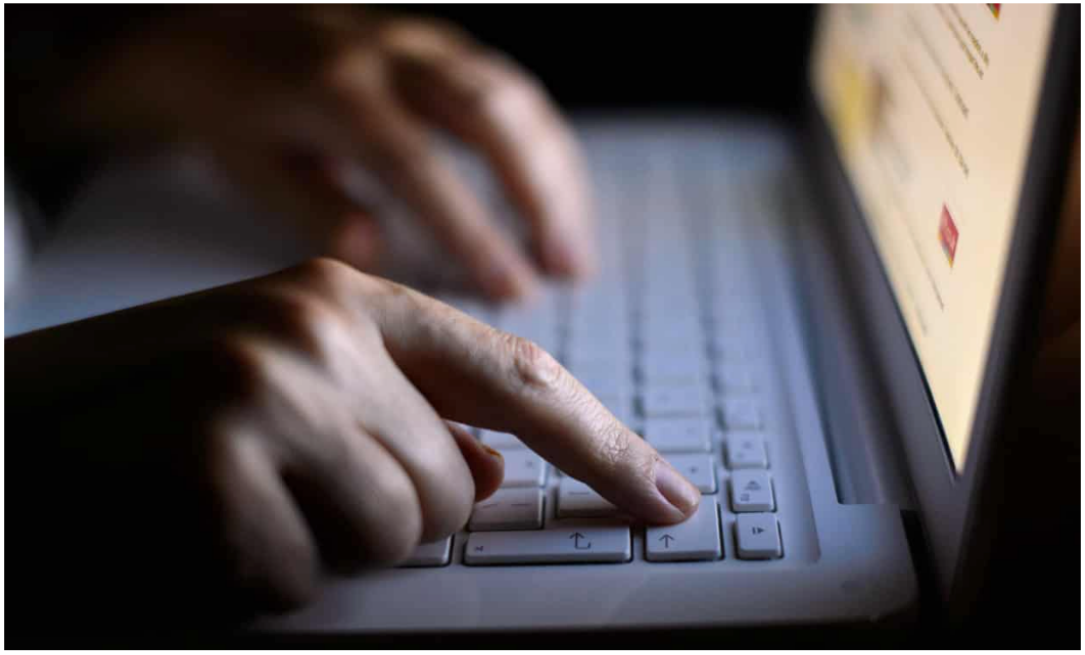
(c) Can Malcolm read z?

(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 Bob's RSA functions are

$$e_B(x) = x^b \bmod n \quad d_B(x) = x^s \bmod n.$$

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.

Equality and Diversity Survey

The Mathematics and ISG Equality and Diversity Committee wants to hear from you!

All students in the Mathematics Department and ISG are warmly encouraged to complete this survey. Go to:

- https://rhul.onlinesurveys.ac.uk/athena-swan-student-survey-mathematics-2019
- tinyurl.com/vof7lso
- use QR code below, or read your email for the link

The survey is linked to the Athena SWAN scheme. Its purpose is to promote gender equality in higher education for staff and students. Your responses will inform our Athena SWAN actions.

Athena SWAN GENDER CHARTER

Course Questionnaires

Please complete the online questionnaire for MT362/462/5462.

There are fewer questions than in the old version so your comments are particularly welcome.

- Did you find the quizzes useful?
- Was the pace too fast, too slow or about right?
- Were the problem sheets too hard, too easy, or about right?

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 $x' \in \mathbb{N}$ such that $x' \neq x$ and $h(x') = h(x)$. (*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 x' with $h(x') = v$ then he can replace x with x' 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 $x' \in \mathbb{N}_0$ will have $h(x') = v$?

  (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 x' such that $h(x') = v$?

  (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 x'?

Preimage resistance: Example 12.3

Malcolm has intercepted a signed message (x, v) from Alice. If he can find x' with $h(x') = v$ then he can replace x with x' 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 $x' \in \mathbb{N}_0$ will have $h(x') = v$?

  (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 x' such that $h(x') = v$?

  (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 x'?

Preimage resistance: Example 12.3

Malcolm has intercepted a signed message (x, v) from Alice. If he can find x' with $h(x') = v$ then he can replace x with x' 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 $x' \in \mathbb{N}_0$ will have $h(x') = v$?

  (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 x' such that $h(x') = v$?

  (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 x'?

Preimage resistance: Example 12.3

Malcolm has intercepted a signed message (x, v) from Alice. If he can find x' with $h(x') = v$ then he can replace x with x' 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 $x' \in \mathbb{N}_0$ will have $h(x') = v$?

  (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 x' such that $h(x') = v$?

  (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 x'? Answer: geometric with parameter $1/2^r$.

Birthday Paradox

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 $h(x) = h(x')$?

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) $\frac{1}{2^m}$ (C) $\frac{1}{2^{m+1}}$ (D) $\frac{1}{2^{2m}}$

- 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) $R(R-1)$

Birthday Paradox

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 $h(x) = h(x')$?

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) $\frac{1}{2^m}$ (C) $\frac{1}{2^{m+1}}$ (D) $\frac{1}{2^{2m}}$

- 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) $R(R-1)$

Birthday Paradox

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 $h(x) = h(x')$?

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) $\frac{1}{2^m}$ (C) $\frac{1}{2^{m+1}}$ (D) $\frac{1}{2^{2m}}$

- 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) $R(R-1)$

Birthday Paradox

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 $h(x) = h(x')$?

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) $\frac{1}{2^m}$ (C) $\frac{1}{2^{m+1}}$ (D) $\frac{1}{2^{2m}}$

- 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) $R(R-1)$

Lemma 12.5

If there are B possible birthdays then in a room of $\sqrt{2 \ln 2}\sqrt{B}$ people, the probability is about $\frac{1}{2}$ that two people have the same birthday.

Birthday Paradox

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 $h(x) = h(x')$?

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) $\frac{1}{2^m}$ (C) $\frac{1}{2^{m+1}}$ (D) $\frac{1}{2^{2m}}$

- 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) $R(R-1)$

Lemma 12.5 (If you don't celebrate your birthday)

If a hash function has values in $\mathbb{F}_2^r$ then if we hash $\sqrt{2 \ln 2}\sqrt{2^r}$ different numbers, the probability is about $\frac{1}{2}$ that two numbers have the same hash.

Hash Functions In Practice

A block cipher of length r can be used as a hash function. Chop the message x (maybe already encrypted) into blocks $x^{(1)}$, $x^{(2)}$, $\ldots$, $x^{(\ell)}$, such that each $x^{(i)} < 2^r$. Replacing each $x^{(i)}$ with its r bit binary form, we use the block cipher in CBC mode to get

$$\begin{aligned} y^{(1)} &= e_k(x^{(1)}) \\ y^{(2)} &= e_k(y^{(1)} + x^{(2)}), \\ &\vdots \\ y^{(\ell)} &= e_k(y^{(\ell-1)} + x^{(\ell)}) \end{aligned}$$

The final ciphertext $y^{(\ell))} \in \mathbb{F}_2^r$ 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 chosen key k be secret?

(A) No (B) Yes

Hash Functions In Practice

A block cipher of length r can be used as a hash function. Chop the message x (maybe already encrypted) into blocks $x^{(1)}$, $x^{(2)}$, ..., $x^{(\ell)}$, such that each $x^{(i)} < 2^r$. Replacing each $x^{(i)}$ with its r bit binary form, we use the block cipher in CBC mode to get

$$\begin{aligned} y^{(1)} &= e_k(x^{(1)}) \\ y^{(2)} &= e_k(y^{(1)} + x^{(2)}), \\ &\vdots \\ y^{(\ell)} &= e_k(y^{(\ell-1)} + x^{(\ell)}) \end{aligned}$$

The final ciphertext $y^{(\ell))} \in \mathbb{F}_2^r$ 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 chosen key k be secret?

  (A) No (B) Yes

  If Bob receives (x, v), then, as usual, he computed $e_A(v)$. He then needs to know k so that he can repeat the calculation above and verify that $h(x) = e_A(v)$. (The secret part is d_A.)

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?

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.

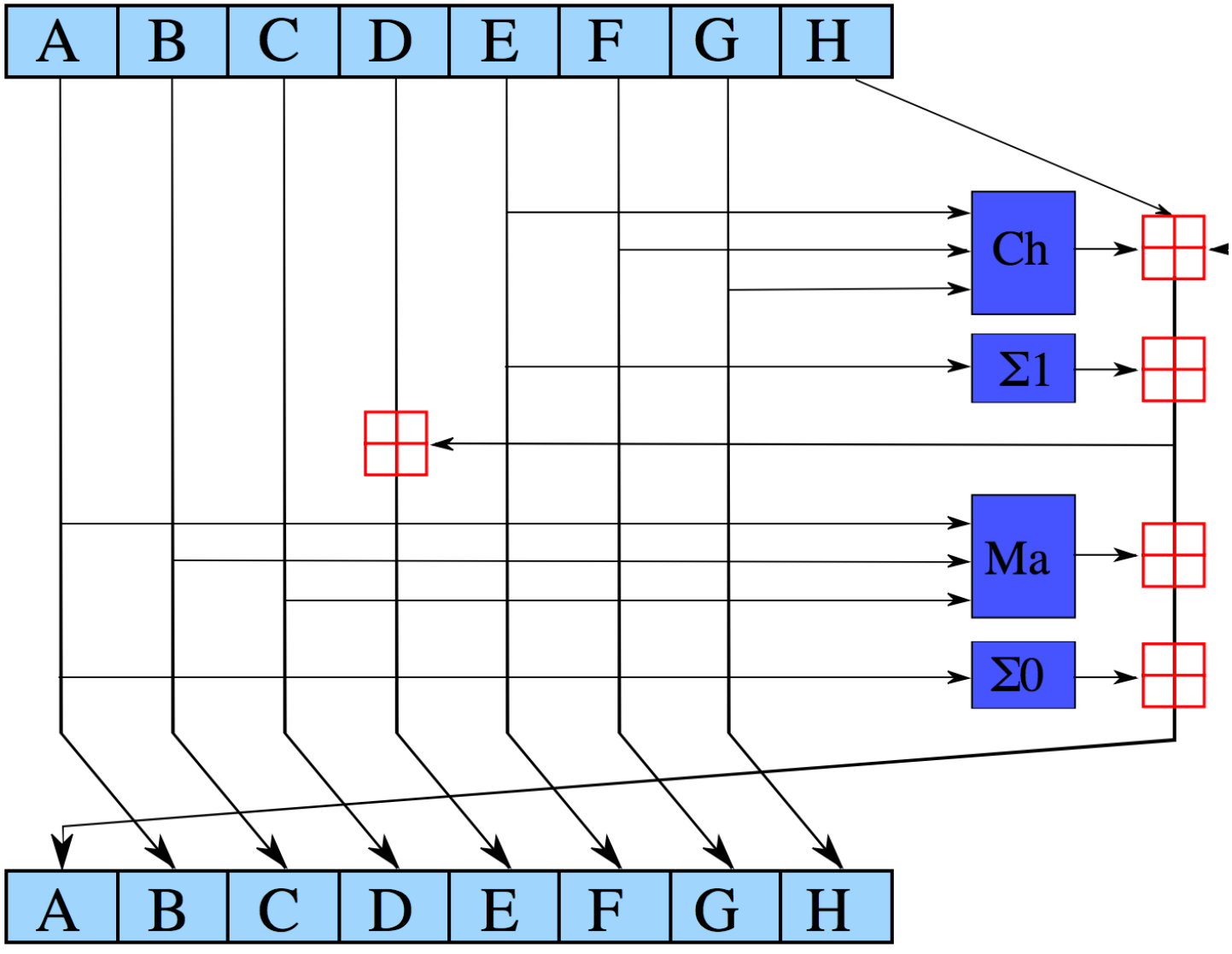
The best attack can break (b) when the number of rounds is reduced to 57, and (c) reducing the rounds further to 46.

A draft of this year's MT362 exam is available from 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 on the Preliminary Problem Sheet.

Wiring Diagram for SHA256



Hashing Passwords

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)

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 last year the bitcoin traded at \$3245.00; the year before in December it was at a near record high of \$15879.79. This year it is at \$7415.64. 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.