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 pass everything left and right, and then to the back, even if you the person you are passing to already has a copy.**
- Please form a four-person cell following instructions on form. One form per cell please.
- All handouts will be put on Moodle. The first marked problem sheet will be on Moodle by Wednesday.
- **Lectures:** Monday 4pm (MFLEC), Friday 11am (MC219), Friday 4pm (MC219).
- **Extra lecture for MT5462:** Thursday 1pm (MC336).
- **Drop-in times in McCrea 240:** Tuesday 3.30pm, Wednesday 10am, Thursday noon

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

§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

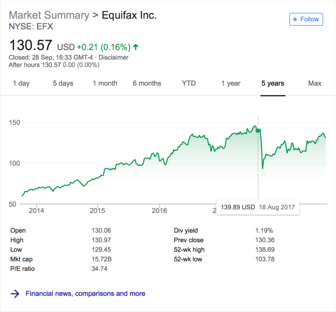
In fact they are sent a 'hash' of your password: see Part D of the course. For instance, the SHA-256 hash of my password is

102400913194339582209408270833988384182939554709307757685269621393941480523360.

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?


Market Summary > Equifax Inc.
NYSE: EFX

+ Follow

130.57 USD +0.21 (0.16%)↑

Closed: 28 Sep, 16:33 GMT-4 · Disclaimer
After hours 130.57 0.00 (0.00%)

1 day | 5 days | 1 month | 6 months | YTD | 1 year | 5 years | Max

Open	130.06	Div yield	1.19%
High	130.97	Prev close	130.36
Low	129.45	52-wk high	138.69
Mkt cap	15.72B	52-wk low	103.78
P/E ratio	34.74		

→ Financial news, comparisons and more

Administration

- Sign-in sheet. **Please return to the lecturer after each lecture.**
- Please take the first marked problem sheet and the next installment of the Part A notes. **Pass everything left and right, and then to the back, even if the person you are passing to has a copy.**
- Everyone ticked on the sign-in sheet (almost everyone) has been sent an email from me with
  - the identities of the four people in your cell
  - two cryptographic keys.

  Use the substitution cipher key to do Question 3 on Sheet 1.
  - I used College email addresses only, as many external email addresses were written illegibly.
  - Please check your email! See me this afternoon if any problems.
- 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.

Exercise 2.2

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

(b) Eve has intercepted the ciphertext `ACCB`. What is the key and what is the plaintext?

(c) Repeat (a) supposing the intercepted ciphertext is `GVTJPO`. Suppose Eve later intercepts `BUPN`. What can she conclude?

Substitution Ciphers

Example 2.3

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

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

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?

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

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.

Exercise′ 2.6

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

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

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

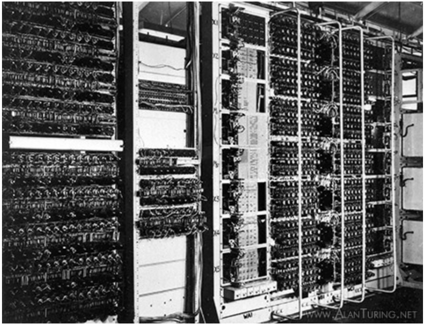
In Praise of Programming

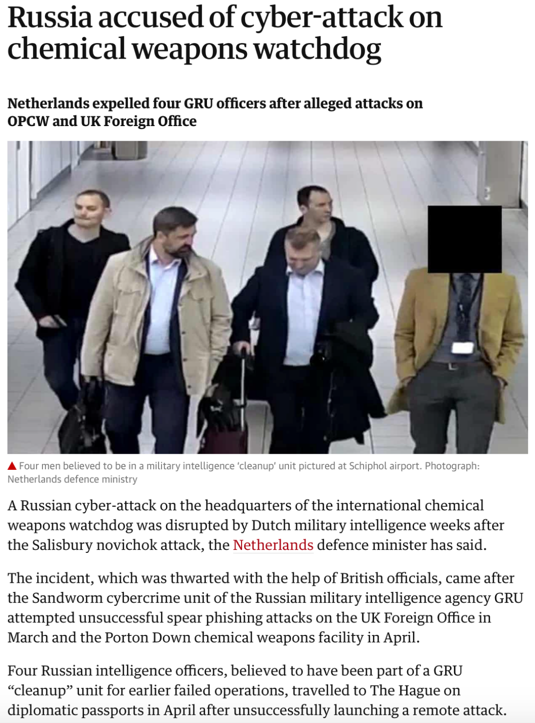
You can get MATHEMATICA for free from the College: see the top hit for Google on 'RHUL Mathematica'.

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 this morning 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 full 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 $\{0, 1, \dots, 25\}$ by

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

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

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

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

Quiz. Reminder of notation for tuples: one of these statements is false. Which one?

(A) $\{1, 2, 2\} = \{2, 1, 1\}$ is a set of size 2,
(B) $(0, 1, 0, 1, 0, 1) \in \{0, 1\}^6$ is the binary form of 21,
(C) $(1, 2, 2) = (2, 1, 1)$,
(D) If $u = (0, 1, 2, \dots, 25)$ then $u_i = i - 1$ for $i \in \{1, \dots, 26\}$.

(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. Reminder of notation for tuples: one of these statements is false. Which one?

(A) $\{1, 2, 2\} = \{2, 1, 1\}$ is a set of size 2,

(B) $(0, 1, 0, 1, 0, 1) \in \{0, 1\}^6$ is the binary form of 21,

(C) $(1, 2, 2) = (2, 1, 1)$,

(D) If $u = (0, 1, 2, \ldots, 25)$ then $u_i = i - 1$ for $i \in \{1, \ldots, 26\}$.

(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 word. Suppose that k has length ℓ. Given a plaintext x with its spaces deleted, we define its encryption by

$$e_k(x) = (x_1 + k_1, x_2 + k_2, \ldots, x_\ell + k_\ell, x_{\ell+1} + k_1, \ldots)$$

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

Vigenère Example

Example 2.10

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

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

i	1	2	3	4	5	**6**	7	8	9	10	11	12	13	14	15	16	17	18
x_i	m 12	e 4	e 4	t 19	a 0	**t** **19**	m 12	i 8	d 3	n 13	i 8	g 6	h 7	t 19	n 13	e 4	a 0	r 17
k_i	4	12	20	4	12	**20**	4	12	20	4	12	20	4	12	20	4	12	20
$x_i + k_i$	16 Q	16 Q	24 Y	23 X	12 M	**13** **N**	16 Q	20 U	23 X	17 R	20 U	0 A	11 L	5 F	7 H	8 I	12 M	11 L

A Weakness in the Vigenère Cipher

Exercise 2.11

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

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

These come from taking every 9th, every 3rd and every position in a ciphertext in Example 2.16 below; it is encrypted using a Vigenère cipher with key length 9.

(ii) Why should we expect the split ciphertext from a Vigènere cipher to have the most ‘spiky’ frequency distribution at the length of the keyword?

A Weakness in the Vigenère Cipher

Exercise 2.11

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

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

These come from taking every 9th, every 3rd and every position in a ciphertext in Example 2.16 below; it is encrypted using a Vigenère cipher with key length 9.

(ii) Why should we expect the split ciphertext from a Vigènere cipher to have the most ‘spiky’ frequency distribution at the length of the keyword?

Index of Coincidence

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 $I(\mathtt{QXNURA}) = I(\mathtt{QNRFLX}) = 0$ and check that $I(\mathtt{QMUUFM}) = \frac{2}{15}$. What is $I(\mathtt{AAABBC})$?

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

Index of Coincidence

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 $I(\mathtt{QXNURA}) = I(\mathtt{QNRFLX}) = 0$ and check that $I(\mathtt{QMUUFM}) = \frac{2}{15}$. What is $I(\mathtt{AAABBC})$?

(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 Vigère Cipher

We now have a strategy for decrypting a Vigenère ciphertext.

Attack 2.15

Given a Vigenère ciphertext, split it into groups by taking every ℓ-th letter for all small ℓ, as in Exercise 2.11. If the ciphertext is long enough, the Index of Coincidence will be greatest at the key length. Each split ciphertext is the output of a Caesar cipher; assuming the most common letter is the encryption of 'e' determines the shift.

Example 2.16

The following ciphertext is the output of a Vigènre cipher:

`KYEYAXBICDMBRFXDLCDPKFXLCILLMOVRMCE ...`

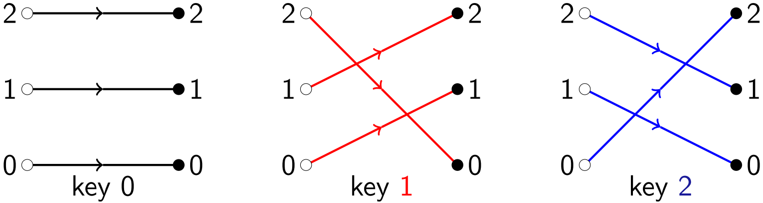
(The full ciphertext is in the printed notes, and in the MATHEMATICA notebook.) We wil decrypt this in the lecture using the Index of Coincidence to get started.

Problem Sheet 1, Question 3

- You should already have emailed a ciphertext encrypted using your substitution cipher key to the three other people in your cell.
- If you have no message to attack in (c), send the other pair an (unencrypted!) reminder. If that fails, email me and I will send you a message using their key.

§3 Cryptosystems, Attack Models 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 $k \in K$,

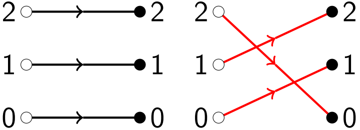
$$d_k\big(e_k(x)\big) = x \tag{$\star$}$$

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*.

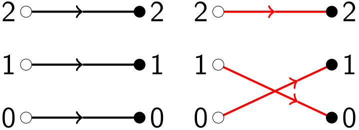
Exercise 3.2

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.

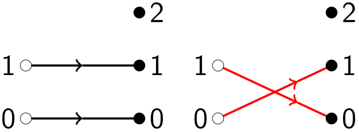
(i)



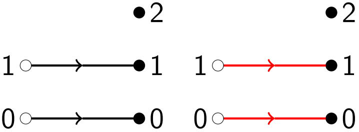
(ii)



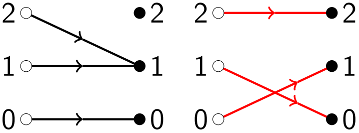
(iii)



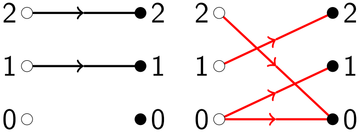
(iv)



(v)



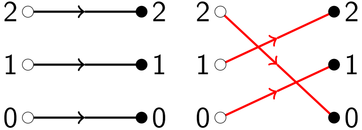
(vi)



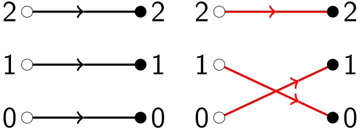
Exercise 3.2

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.

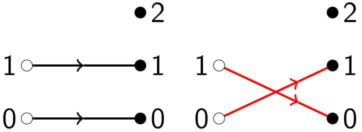
(i)



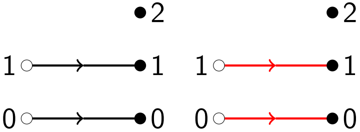
(ii)



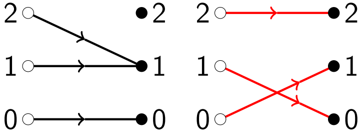
(iii)



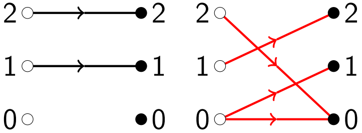
(iv)



(v)



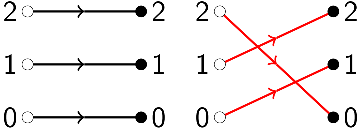
(vi)



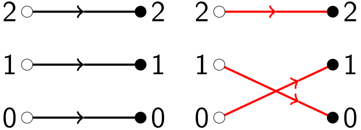
Exercise 3.2

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.

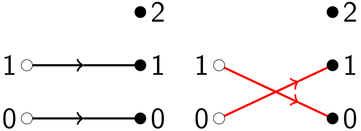
(i)



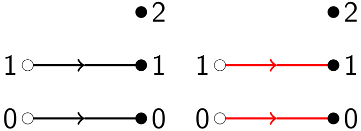
(ii)



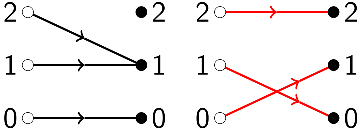
(iii)



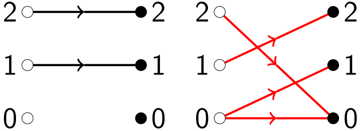
(iv)



(v)



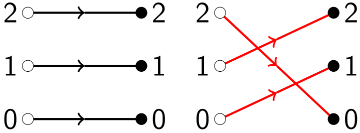
(vi)



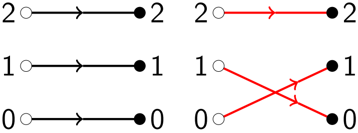
Exercise 3.2

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.

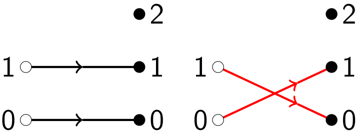
(i)



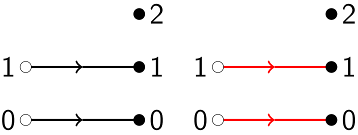
(ii)



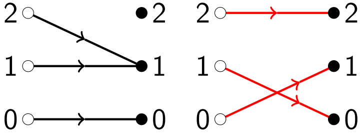
(iii)



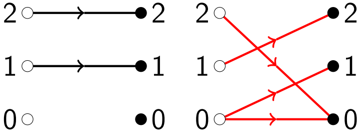
(iv)



(v)



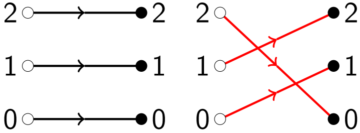
(vi)



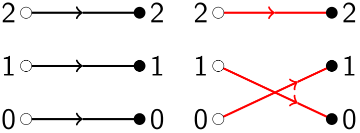
Exercise 3.2

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.

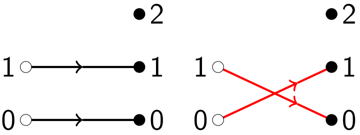
(i)



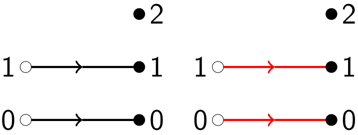
(ii)



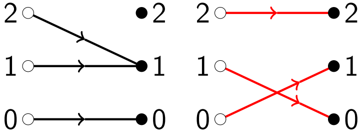
(iii)



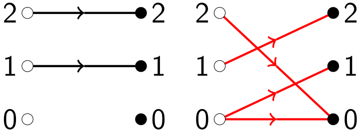
(iv)



(v)



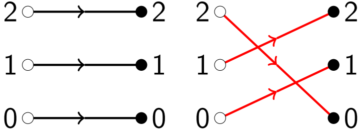
(vi)



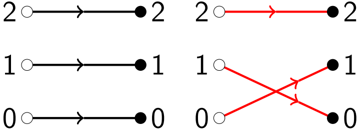
Exercise 3.2

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.

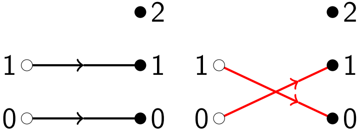
(i)



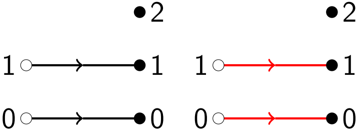
(ii)



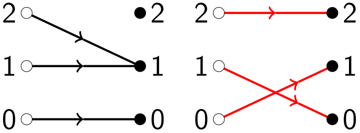
(iii)



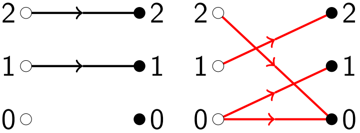
(iv)



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

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

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

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

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

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

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

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

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

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

Affine cipher

Example 3.4

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 maps are defined by $e_{(a,c)}(x) = ax + c \bmod p$. The decryption maps 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.

Exercise 3.5

Consider the affine cipher on $\mathbb{Z}_5$.

(i) Suppose that Eve observes the ciphertext 2. Does she learn anything about the plaintext?

(iii) Suppose that Mark knows that $e_{(e,c)}(1) = 2$. What does he learn about the key?

Attack Models

In each of the *attack models* below, we suppose that Alice is sending 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 $y = e_k(x)$.
- *Chosen ciphertext*. Mark may choose any $y \in \mathcal{C}$ and is given the decryption $x = d_k(y)$.

Each attack model has a generalization where the adversary observes multiple plaintexts and/or ciphertexts.

Attack Models: Remarks

Remark 3.6

(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*. Similarly we have broken the Vigenère cipher using a *known ciphertext attack* (a longer cipher text was needed).

(2) All the cryptosystems so far are broken by a *chosen plaintext attack*. By the general version of Example 3.5, the affine cipher requires two choices of plaintext, and by Question 4 on Sheet 1, the substitution cipher and the Vigenère cipher just one.

(3) Later in the course we will see modern 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*.

Probability model

Fix a cryptosystem in our usual notation. To define a probability space on $\mathcal{K} \times \mathcal{P} \times \mathcal{C}$ we assume 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 message 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 3.7

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 $\Omega = \{HH, HT, TH, TT\}$ 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?

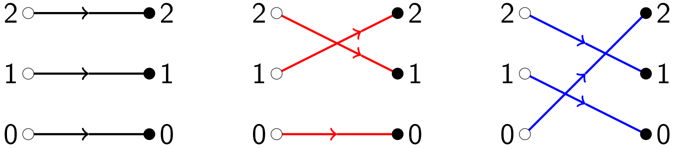
(A) Yes (B) No

Quiz. Let $\Omega = \{HH, HT, TH, TT\}$ 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

Probability Model: Example 3.8

(a) The cryptosystem below uses three keys from the affine cipher on $\mathbb{Z}_3$. It is used again in Question 1 on Sheet 2.



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

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

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

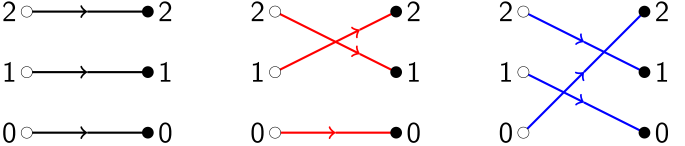
(2) Suppose that the three keys are used with equal probability $\frac{1}{3}$, and that $p_1 = 1 - q$, $p_2 = q$ so $p_0 = 0$.

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

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

Probability Model: Example 3.8

(a) The cryptosystem below uses three keys from the affine cipher on $\mathbb{Z}_3$. It is used again in Question 1 on Sheet 2.



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

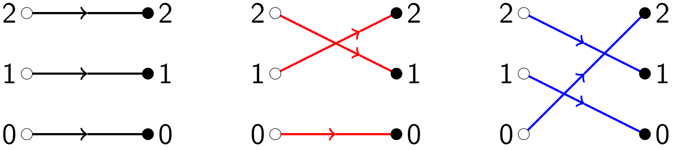
(2) Suppose that the three keys are used with equal probability $\frac{1}{3}$, and that $p_1 = 1 - q$, $p_2 = q$ so $p_0 = 0$.

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

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

Probability Model: Example 3.8

(a) The cryptosystem below uses three keys from the affine cipher on $\mathbb{Z}_3$. It is used again in Question 1 on Sheet 2.



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

Administration

- Please take pages 17 to 20 of the printed notes.
- Please take Problem Sheet 2.
- Please hand in answers to Problem Sheet 1 at the end of this lecture.

Probability Model: Example 3.8 [continued]

(b) In the Caesar cipher on $\{0, 1, 2\}$, shown before Definition 3.1, there are three keys. Suppose keys are chosen with equal probability $\frac{1}{3}$ and, as usual the probability distribution **on plaintexts is p_0, p_1, p_2 [omitted!]**.

Will check that $\mathbb{P}[X = x | Y = y] = p_x$ for all x, $y \in \{0, 1, 2\}$. Knowing the ciphertext tells Eve nothing new about the plaintext. **Follow up:** break (b) by a chosen plaintext attack.

(c) In Exercise 3.2(i), $\mathcal{P} = \mathcal{C} = \{0, 1, 2\}$. Suppose the two keys are used with equal probability $\frac{1}{2}$. We have $\mathbb{P}[Y = 1] = \frac{p_0+p_1}{2}$ and

$$\mathbb{P}[X = 0 | Y = 1] = \frac{p_0}{p_0 + p_1},$$

$$\mathbb{P}[X = 1 | Y = 1] = \frac{p_1}{p_0 + p_1}$$

$$\mathbb{P}[X = 2 | Y = 1] = 0.$$

These probabilities are usually not the same as p_0, p_1, p_2. So (c) is broken by a known ciphertext attack.

Perfect secrecy

Definition 3.9

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

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

By Example 3.8(a), the Caesar cipher on $\{0, 1, 2\}$ has perfect secrecy when keys are used with equal probability. If instead $\mathbb{P}[K = 0] = \mathbb{P}[K = 1] = \frac{1}{2}$ and $\mathbb{P}[K = 2] = 0$ we get the cryptosystem in Exercise 3.2(i), which we saw in Example 3.8(c) does not have perfect secrecy.

Shannon's Theorem

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

Theorem 3.10 (Shannon 1949)

Suppose a cryptosystem (in our usual notation) has perfect secrecy, **that** $\mathbb{P}[K = k] > 0$ **for each** $k \in \mathcal{K}$ **[correction!]**, *and that for all* $y \in \mathcal{C}$ *there exists* $x \in \mathcal{P}$ *and* $k \in \mathcal{K}$ *such that* $e_k(x) = y$.

(a) *For all* $x \in \mathcal{P}$ *and all* $y \in \mathcal{C}$ *there exists a key* k *such that* $e_k(x) = y$.

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

(c) *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.*

Shannon's Theorem

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

Theorem 3.10 (Shannon 1949)

Suppose a cryptosystem (in our usual notation) has perfect secrecy, **that** $\mathbb{P}[K = k] > 0$ **for each** $k \in \mathcal{K}$ **[correction!]**, *and that for all* $y \in \mathcal{C}$ *there exists* $x \in \mathcal{P}$ *and* $k \in \mathcal{K}$ *such that* $e_k(x) = y$.

(a) *For all* $x \in \mathcal{P}$ *and all* $y \in \mathcal{C}$ *there exists a key* k *such that* $e_k(x) = y$.

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

(c) *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.*

Theorem 3.10 (Shannon 1949)

Suppose a cryptosystem (in our usual notation) has perfect secrecy, **that** $\mathbb{P}[K = k] > 0$ **for each** $k \in \mathcal{K}$ **[correction!]**, *and that for all* $y \in \mathcal{C}$ *there exists* $x \in \mathcal{P}$ *and* $k \in \mathcal{K}$ *such that* $e_k(x) = y$.

(a) *For all* $x \in \mathcal{P}$ *and all* $y \in \mathcal{C}$ *there exists a key* k *such that* $e_k(x) = y$.

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

(c) *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.*

For $x \in \mathcal{P}$ and $y \in \mathcal{C}$ we defined

$$\mathcal{K}_{xy} = \{k \in \mathcal{K} : e_k(x) = y\}.$$

In Monday we proved (a), that each $\mathcal{K}_{xy}$ is non-empty and also that $\mathbb{P}[k \in \mathcal{K}_{xy}] = \mathbb{P}[Y = y] > 0$. Then (b) followed from

$$|\mathcal{K}| = \sum_{y \in \mathcal{C}} |K_{xy}| \geq \sum_{y \in \mathcal{C}} 1 = |C|.$$

Latin Squares

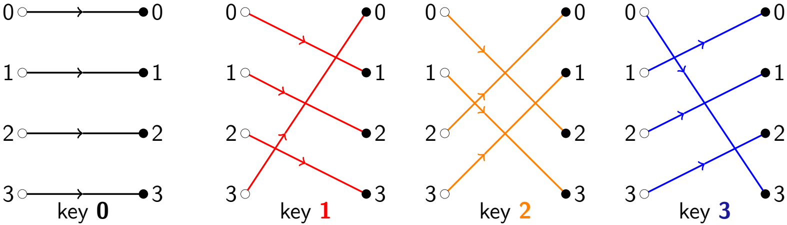
Consider a cryptosystem with perfect secrecy in which $\mathcal{P} = |\mathcal{C}| = |\mathcal{K}| = \{0, 1, \ldots, n-1\}$. By (c) in Theorem 3.10, for each $x, y \in \{0, 1, \ldots, n-1\}$, there exists a unique $k \in \{0, 1, \ldots, n-1\}$ such that $e_k(x) = y$. Therefore the cryptosystem is determined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

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

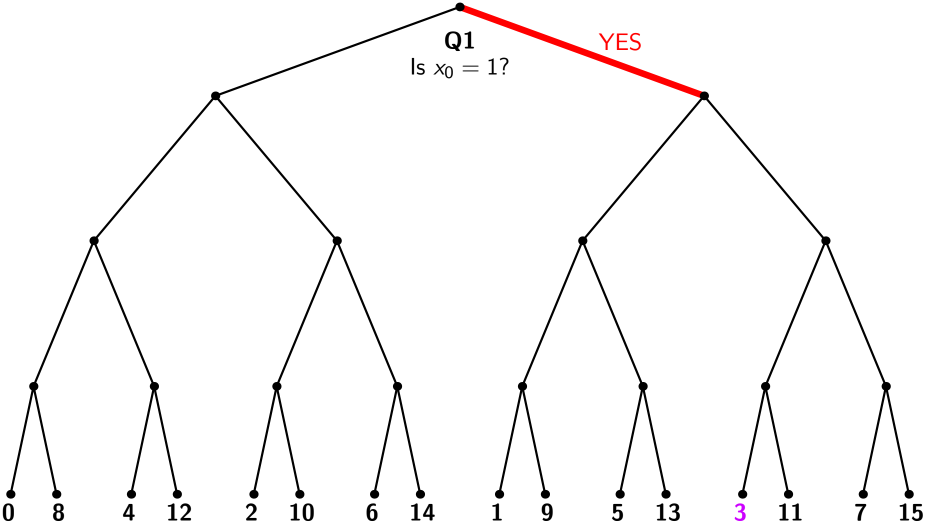
§4 Entropy and Key Uncertainty

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 $x_3 = 1$?'.

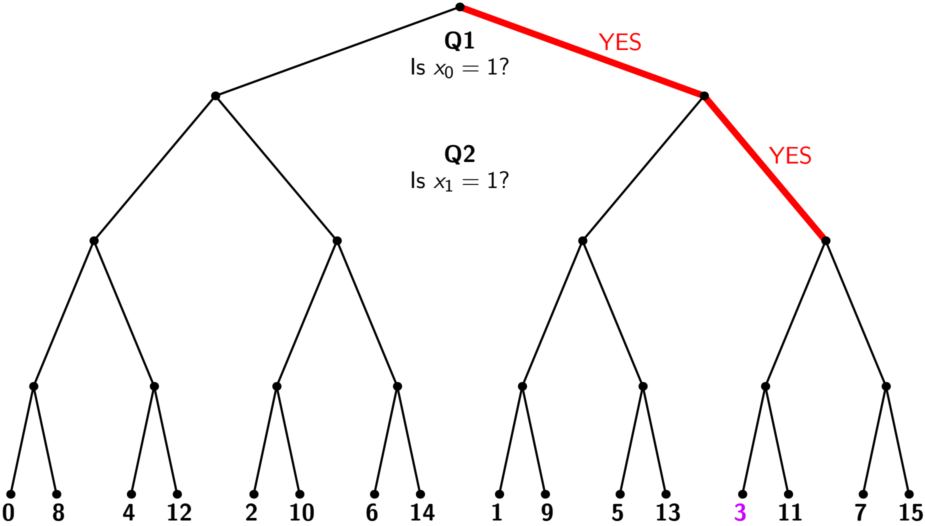
Exercise 4.1

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

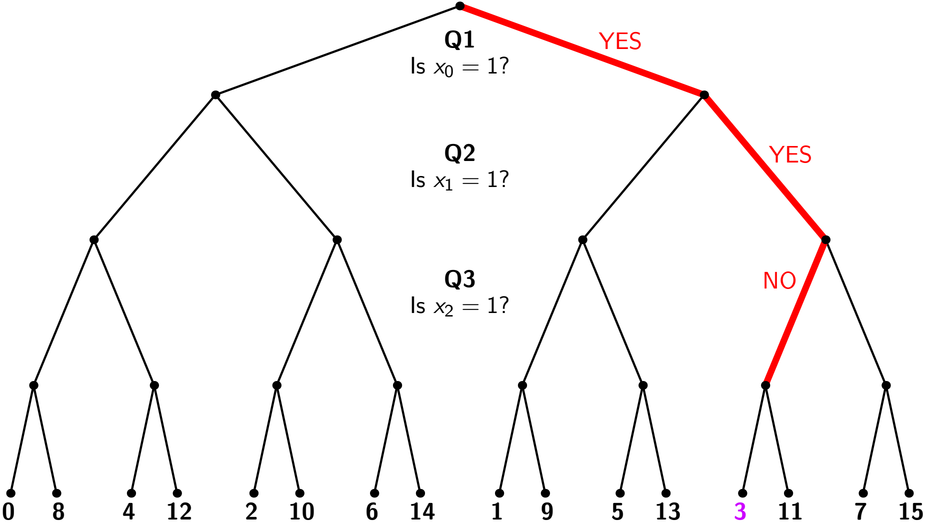
4 Yes/No Questions for 4 Bits of Information



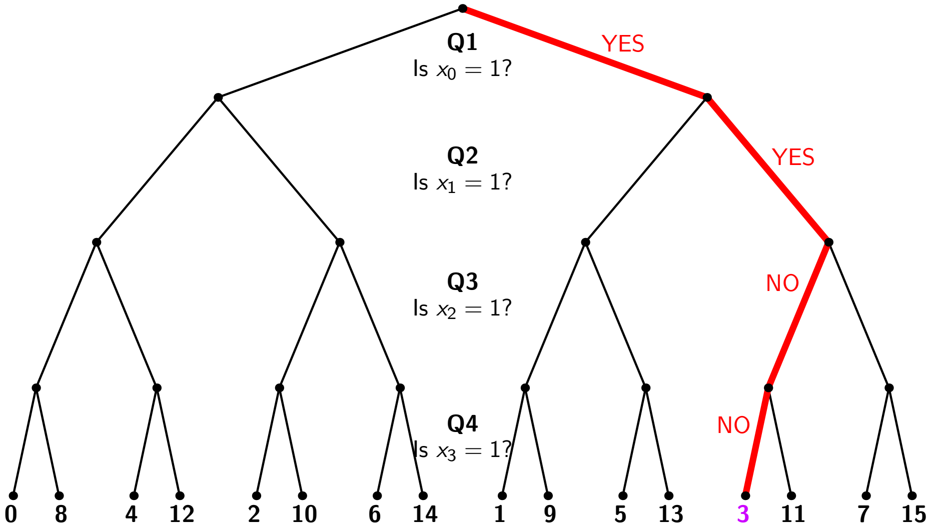
4 Yes/No Questions for 4 Bits of Information



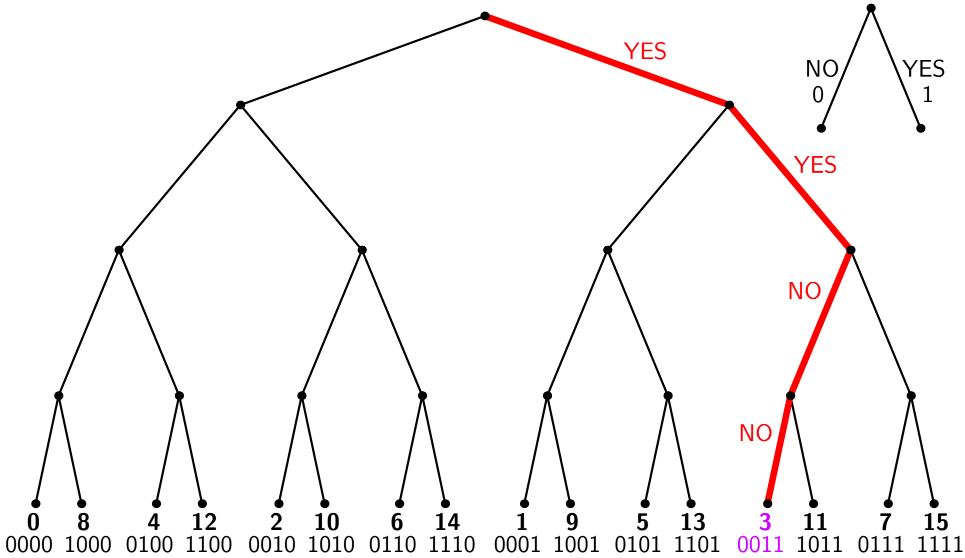
4 Yes/No Questions for 4 Bits of Information



4 Yes/No Questions for 4 Bits of Information



4 Yes/No Questions for 4 Bits of Information



Guessing games

Example 4.2

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 4.2

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

Definition of Entropy

Definition 4.3

Let $\mathcal{X}$ be a finite set.

(i) The *entropy* of a probability distribution p_x on $\mathcal{X}$ is

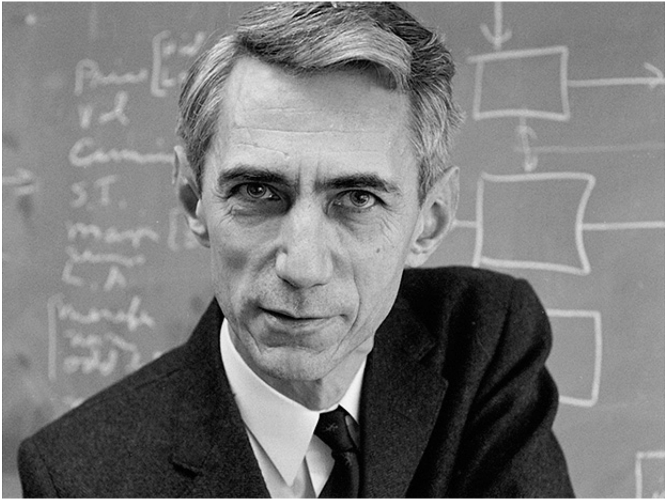
$$H(p) = -\sum_{x \in \mathcal{X}} p_x \log_2 p_x.$$

(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 4.4

(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.

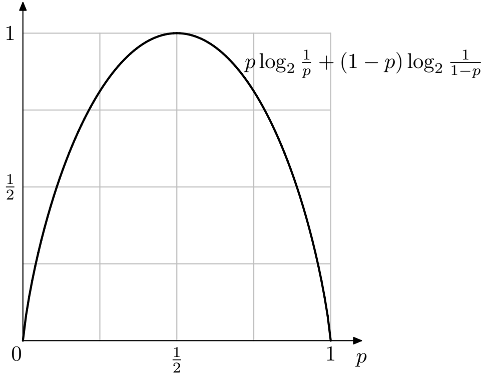
(ii) Show that if p is the probability distribution in Exercise 4.2(b) then

$$H(p) = \tfrac{1}{2} \log_2 2 + \tfrac{1}{4} \log_2 4 + \tfrac{1}{4} \log_2 4 + 0 = \tfrac{3}{2}.$$

Show that in all three cases, $H(p)$ is the average number of questions, using the strategy found in this exercise.

Example 4.5

(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 4.5 [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 $\mathbb{P}[K = \mathrm{red}] = r$, and so $\mathbb{P}[K = \mathrm{black}] = 1 - r$. [**Correction: in lecture I wrote $\mathbb{P}[K = \mathrm{black}] = r$ and $\mathbb{P}[K = \mathrm{red}] = 1 - r$. Please swap. The rest is then correct.**] 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

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

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

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

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 value, not the values themselves.

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 value, 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 4.6

Let K and Y be random variables each 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

$$H(K|Y) = \sum_{y \in \mathcal{C}} \mathbb{P}[Y = y] H(K|Y = y).$$

Definition 4.6

Let K and Y be random variables each 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 4.7

Consider the Caesar cryptosystem in which all 26 keys are equally likely. What is $H(K)$? What are $H(K|Y = \texttt{ACCB})$ and $H(K|Y = \texttt{NCYP})$?

Definition 4.6

Let K and Y be random variables each 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 4.8 (Chaining Rule)

Let K and Y be random variables. Then

$$H(K, Y) = H(K|Y) + H(Y).$$

Sigma Notation Quiz

(1) True or false?

$$\sum_{x \in \{1,2,3\}} x = \sum_{x=1}^{3} x.$$

(A) False (B) True

(2) Calculate the following sums expressed in Sigma notation:

$$\sum_{x \in \{1,2,3\}} x$$

(A) 5 (B) 6 (C) 7 (D) $x + 6$

$$\sum_{x \in \{1,2,3\}} \sum_{y \in \{1,2\}} xy$$

(A) 12 (B) 14 (C) 18 (D) 24

$$\sum_{x \in \{1,2,3\}} \sum_{y \in \{1,2\}} x$$

(A) 12 (B) 14 (C) 18 (D) 24

Sigma Notation Quiz

(1) True or false?

$$\sum_{x \in \{1,2,3\}} x = \sum_{x=1}^{3} x.$$

(A) False (B) True

(2) Calculate the following sums expressed in Sigma notation:

$$\sum_{x \in \{1,2,3\}} x$$

(A) 5 (B) 6 (C) 7 (D) $x + 6$

$$\sum_{x \in \{1,2,3\}} \sum_{y \in \{1,2\}} xy$$

(A) 12 (B) 14 (C) 18 (D) 24

$$\sum_{x \in \{1,2,3\}} \sum_{y \in \{1,2\}} x$$

(A) 12 (B) 14 (C) 18 (D) 24

Sigma Notation Quiz

(1) True or false?

$$\sum_{x\in\{1,2,3\}} x = \sum_{x=1}^{3} x.$$

(A) False [✓ (B) True]

(2) Calculate the following sums expressed in Sigma notation:

$$\sum_{x\in\{1,2,3\}} x$$

(A) 5 (B) 6 [✓ (C) 7] (D) $x + 6$

$$\sum_{x\in\{1,2,3\}} \sum_{y\in\{1,2\}} xy$$

(A) 12 (B) 14 (C) 18 (D) 24

$$\sum_{x\in\{1,2,3\}} \sum_{y\in\{1,2\}} x$$

(A) 12 (B) 14 (C) 18 (D) 24

Sigma Notation Quiz

(1) True or false?

$$\sum_{x\in\{1,2,3\}} x = \sum_{x=1}^{3} x.$$

(A) False [✓ (B) True]

(2) Calculate the following sums expressed in Sigma notation:

$$\sum_{x\in\{1,2,3\}} x$$

(A) 5 (B) 6 [✓ (C) 7] (D) $x+6$

$$\sum_{x\in\{1,2,3\}} \sum_{y\in\{1,2\}} xy$$

(A) 12 (B) 14 [✓ (C) 18] (D) 24

$$\sum_{x\in\{1,2,3\}} \sum_{y\in\{1,2\}} x$$

(A) 12 (B) 14 (C) 18 (D) 24

Sigma Notation Quiz

(1) True or false?

$$\sum_{x\in\{1,2,3\}} x = \sum_{x=1}^{3} x.$$

(A) False [✓ (B) True]

(2) Calculate the following sums expressed in Sigma notation:

$$\sum_{x\in\{1,2,3\}} x$$

(A) 5 (B) 6 [✓ (C) 7] (D) $x+6$

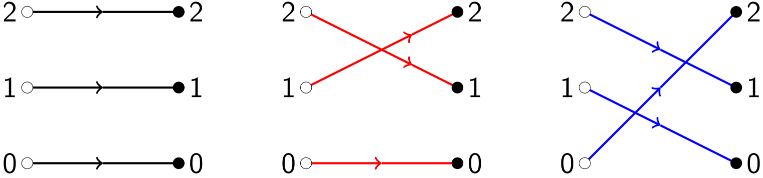
$$\sum_{x\in\{1,2,3\}} \sum_{y\in\{1,2\}} xy$$

(A) 12 (B) 14 [✓ (C) 18] (D) 24

$$\sum_{x\in\{1,2,3\}} \sum_{y\in\{1,2\}} x$$

[✓ (A) 12] (B) 14 (C) 18 (D) 24

Question 1 on Problem Sheet 2

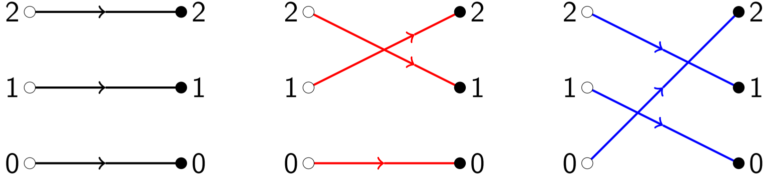


(a) Recall that $e_{(a,c)}(x) = ax + c$. Which keys (a, c) are used in this cryptosystem?

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

Question 1 on Problem Sheet 2



(a) Recall that $e_{(a,c)}(x) = ax + c$. Which keys (a, c) are used in this cryptosystem?

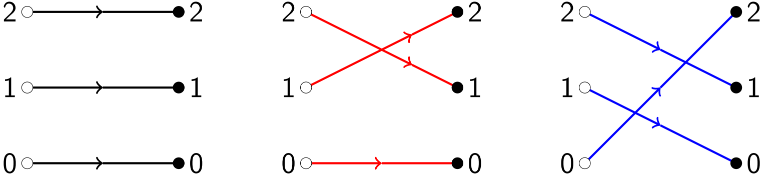
(b) Express $\mathbb{P}[Y = 1|X = 1]$, $\mathbb{P}[Y = 1]$, $\mathbb{P}[X = 1|Y = 1]$ in terms of p.

(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?

True or false: the cryptosystem has perfect secrecy with respect to the probability distribution $p_0 = 1$, $p_1 = p_2 = 0$?

(A) False (B) True

Question 1 on Problem Sheet 2



(a) Recall that $e_{(a,c)}(x) = ax + c$. Which keys (a, c) are used in this cryptosystem?

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

True or false: the cryptosystem has perfect secrecy with respect to the probability distribution $p_0 = 1$, $p_1 = p_2 = 0$?

(A) False (B) True

Shannon's Theorem on Key Uncertainty

Lemma 4.9

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

Lemma 4.10

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 4.11

Take a cryptosystem in our usual notation. Then

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

Per-Character Information/Redundancy of English

Let $\mathcal{A} = \{\mathtt{a}, \mathtt{b}, \ldots, \mathtt{z}\}$ be the alphabet. We take $\mathcal{P} = \mathcal{C} = \mathcal{A}^n$: you can think of this as the set of all strings of length n. To indicate that plaintexts and ciphertexts have length n, we write X_n and Y_n rather than X and Y.

We suppose only those strings that make good sense in English have non-zero probability. So if $n = 8$ then $`\mathtt{abcdefgh}', `\mathtt{goodwork}' \in \mathcal{P}$ but $\mathbb{P}[X_8 = `\mathtt{abcdefgh}'] = 0$ whereas $\mathbb{P}[X_8 = `\mathtt{goodwork}'] > 0$.

Shannon estimated that the per-character redundancy of English plaintexts, with spaces, is about 3.200. (See the optional extras for this part.) We shall suppose his estimate is also good for plaintexts in $\mathcal{A}^n$.

The One-Time Pad

Example 4.12 (One-time pad)

Fix $n \in \mathbb{N}$. The *one-time pad* is a cryptosystem with plaintexts, ciphertexts and keyspace $\mathcal{A}^n$. 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. For example, when $n = 8$, $e_{\texttt{zyxwvuts}}(\texttt{goodwork}) = \texttt{fmlzrikc}$.

Suppose that all keys in $\mathcal{A}^n$ are equally likely. Then all ciphertexts are equally likely, and by Example 4.5(2)

$$\begin{aligned} H(K) &= (\log_2 26)n \\ H(Y_n) &= (\log_2 26)n. \end{aligned}$$

By Shannon's formula,

$$H(K|Y_n) = H(K) + H(X_n) - H(Y_n) = (\log_2 26 - R)n = H(X_n).$$

One-Time-Pad Quiz

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

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

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) $n \log_2 26$

Re-use of One-Time-Pad Considered Harmful

Example 4.13

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 assumption, 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

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

So far Eve has learned nothing, except that Alice has sent Bob the ciphertext $y = \texttt{lxcghyrrroznfy}$. Eve cannot guess Alice's message x: for example

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

Example 4.13 [continued]

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.

Unicity Distance

In Example 4.12 [**Correction: not 4.13**] we proved that for the one-time-pad $H(K|Y_n) = (\log_2 26 - R)n$ and that $H(K) = (\log_2 26)n$. Therefore

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

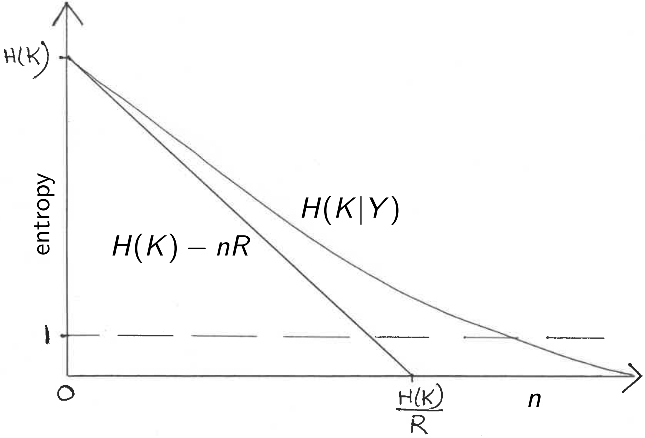
In the non-examinable extras for this part we give Shannon's argument that $(\star\star)$ should be a good approximation for $H(K|Y_n)$ in any cryptosystem where $\mathcal{P} = \mathcal{C} = \mathcal{A}^n$ and the messages are English texts.

Exercise 4.14

What is the largest length of ciphertext n for which $(\star\star)$ could hold with equality?

Expected behaviour of $H(K|Y_n)$

The graph below shows the expected behaviour of $H(K|Y_n)$.



Definition 4.15

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

Unicity Distance for Substitution Cipher

Exercise 4.16

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 $H(K|Y_{280} = y)$? What is $H(K)$?

Example 4.17

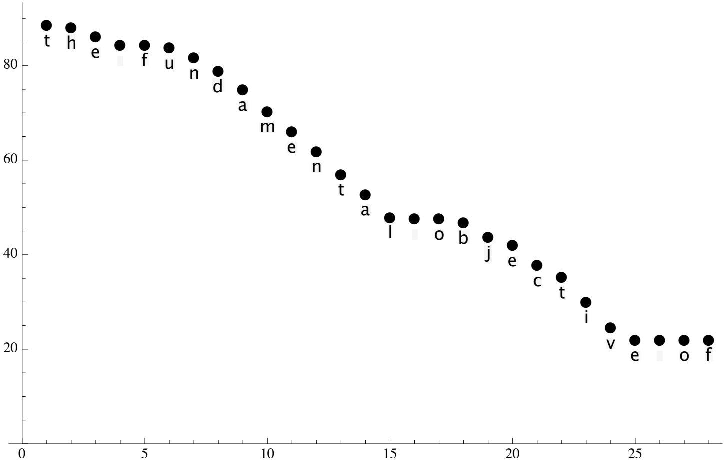
The first 28 characters of the ciphertext in Example 2.5 are `KQX WJZRUHXZKUY GTOXSKPIX GW`. A computer search using a dictionary of about 70000 words gives 6 possible decryptions of the first 24 letters. These include '`imo purgatorial hedonics`', '`iwo purgatorial hedonism`' and '`the fundamental objectiv`'. Taking 25 letters,

'`the fundamental objective`'

is the only decryption consistent with the dictionary. This is in excellent agreement with Shannon's argument.

Since 10 characters do not appear in the first 28 letters of ciphertext, the argument in Exercise 4.16 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

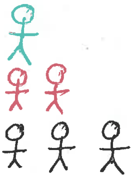
Ciphertexts with High $g(y)$ are More Likely: Intuition

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 $\sim \mathrm{Bin}(\frac{1}{2}, 3)$

All children go to some school

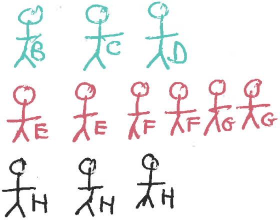


0 $\binom{3}{0}\left(\frac{1}{2}\right)^3 = \frac{1}{8}$ Ⓐ

1 $\binom{3}{1}\left(\frac{1}{2}\right)^3 = \frac{3}{8}$ Ⓑ Ⓒ Ⓓ

2 $\binom{3}{2}\left(\frac{1}{2}\right)^3 = \frac{3}{8}$ Ⓔ Ⓕ Ⓖ

3 $\binom{3}{3}\left(\frac{1}{2}\right)^3 = \frac{1}{8}$ Ⓗ



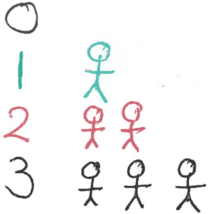
Ciphertexts with High $g(y)$ are More Likely: Intuition

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 $\sim \text{Bin}(\frac{1}{2}, 3)$

All children go to some school

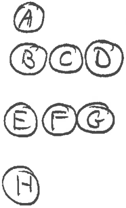


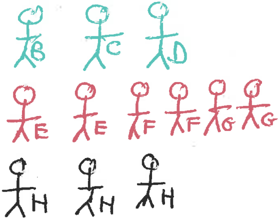
$$\binom{3}{0}\left(\frac{1}{2}\right)^3=\frac{1}{8}$$

$$\binom{3}{1}\left(\frac{1}{2}\right)^3=\frac{3}{8}$$

$$\binom{3}{2}\left(\frac{1}{2}\right)^3=\frac{3}{8}$$

$$\binom{3}{3}\left(\frac{1}{2}\right)^3=\frac{1}{8}$$





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).

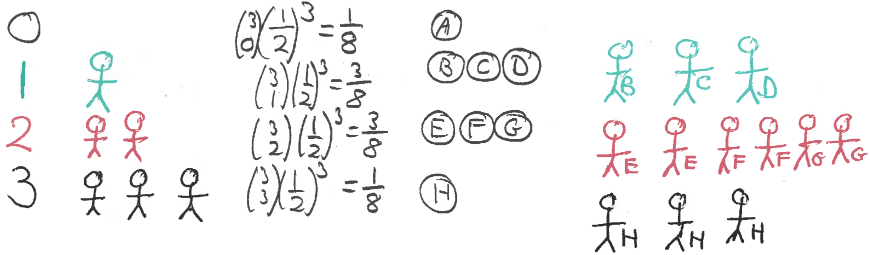
Ciphertexts with High $g(y)$ are More Likely: Intuition

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 $\sim \mathrm{Bin}(\frac{1}{2}, 3)$

All children go to some school



$\binom{3}{0}\left(\frac{1}{2}\right)^3 = \frac{1}{8}$

$\binom{3}{1}\left(\frac{1}{2}\right)^3 = \frac{3}{8}$

$\binom{3}{2}\left(\frac{1}{2}\right)^3 = \frac{3}{8}$

$\binom{3}{3}\left(\frac{1}{2}\right)^3 = \frac{1}{8}$

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 $1 + \mathrm{Bin}(\frac{1}{2}, 2)$ distribution.

Part B: Stream ciphers

§5 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 $x_0 x_1 \ldots x_{n-1}$. 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

Definition 5.1

(i) Let $\ell \in \mathbb{N}$. A *linear feedback shift register* of *width* ℓ with *taps* $T \subseteq \{0, 1, \ldots, \ell - 1\}$ is a function $F : \mathbb{F}_2^\ell \to \mathbb{F}_2^\ell$ of the form

$$F\big((x_0, x_1, \ldots, x_{\ell-2}, x_{\ell-1})\big) = (x_1, \ldots, x_{\ell-1}, \sum_{t \in T} x_t).$$

(ii) The function $f : \mathbb{F}_2^\ell \to \mathbb{F}_2$ defined by $f(x) = \sum_{t \in T} x_t$ 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

$$k_s = f\big((k_{s-\ell}, k_{s-\ell+1}, \ldots, k_{s-1})\big).$$

The Very Useful Property

Equivalently, $k_s = \sum_{t \in T} k_{s-\ell+t}$. Thus an LFSR shifts the bits in positions 1 to $\ell - 1$ left, and puts a new bit, defined by its feedback function, into the rightmost position $\ell - 1$. Taking all these rightmost positions gives the keystream. **This very useful property is expressed by**

$$F^s\big((k_0, k_1, \ldots, k_{\ell-1})\big) = (k_s, k_{s+1}, \ldots, k_{s+\ell-1}). \qquad (\star)$$

Here F^s is the function defined by applying F a total of s times.

Example 5.2

The LFSR F of width 4 with taps $\{0,1\}$ 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

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

repeating from position 15 onwards: $k_s = k_{s+15}$ for all $s \in \mathbb{N}_0$.

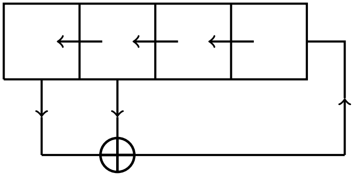
(iii) *Exercise:* observe that $k' = 0001$ appears in positions 5, 6, 7, 8 of the keystream above. Find the keystream for k'.

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

(v) *Exercise:* Is every keystream generated by F a cyclic shift of the keystream for 0111?

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 5.2 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) $F^2(0111) = 1110$ (A) False (B) True

(3) $F^4(0111) = 1000$ (A) False (B) True

(4) $F^2(1110) = 1000$ (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 5.2 with key 0111 is below

$$(\underset{0}{0}, \underset{1}{1}, \underset{2}{1}, \underset{3}{1}, \underset{4}{1}, \underset{5}{0}, \underset{6}{0}, \underset{7}{0}, \underset{8}{1}, \underset{9}{0}, \underset{0}{0}, \underset{1}{1}, \underset{2}{1}, \underset{3}{0}, \underset{4}{1}, \underset{5}{0}, \underset{6}{1}, \underset{7}{1}, \underset{8}{1}, \underset{9}{1} \ldots)$$

True or false?

(1) $F^2(0111) = 1110$ (A) False [✓ (B) True]

(2) $F^2(0111) = 1110$ (A) False (B) True

(3) $F^4(0111) = 1000$ (A) False (B) True

(4) $F^2(1110) = 1000$ (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 5.2 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) $F^2(0111) = 1110$ (A) False [✓ (B) True]

(3) $F^4(0111) = 1000$ (A) False (B) True

(4) $F^2(1110) = 1000$ (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 5.2 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) $F^2(0111) = 1110$ (A) False (B) True

(3) $F^4(0111) = 1000$ (A) False (B) True

(4) $F^2(1110) = 1000$ (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 5.2 with key 0111 is below

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

True or false?

(1) $F^2(0111) = 1110$ (A) False (B) True

(2) $F^2(0111) = 1110$ (A) False (B) True

(3) $F^4(0111) = 1000$ (A) False (B) True

(4) $F^2(1110) = 1000$ (A) False (B) True

Cryptosystem defined by an LFSR

Definition 5.3

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 5.4

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 5.3

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. She can guess that $k_0k_1k_2k_3$ is

(A) 00?? (B) 01?? (C) 10?? (D) 11??

Cryptosystem defined by an LFSR

Definition 5.3

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 $k_0 k_1 k_2 k_3$.

Eve observes the ciphertext 00100110. She can guess that $k_0 k_1 k_2 k_3$ is

(A) 00?? (B) 01?? (C) 10?? (D) 11??

Invertible LFSRs and periods: motivation

Exercise 5.5

Let H be the LFSR of width 4 with taps $\{1,2\}$. Show that H is not invertible.

This exercise and Example 5.2(i) suggest the general result: an LFSR is invertible if and only if 0 is one of the taps. The steps in a proof are indicated in Question 3 of Sheet 4.

Exercise 5.6

Let G be the LFSR of width 4 with taps $\{0,2\}$.

(a) Find the keystreams for the keys 0001 and 0011.

(b) Which words of length 4 do not appear in either keystream?

(c) Find all keystreams generated by this LFSR.

True or false: the keystream for key 0110 has period 6?

(A) False (B) True

True or false: $G^6 = \mathrm{id}$, the identity function.

(A) False (B) True

Invertible LFSRs and periods: motivation

Exercise 5.5

Let H be the LFSR of width 4 with taps $\{1, 2\}$. Show that H is not invertible.

This exercise and Example 5.2(i) suggest the general result: an LFSR is invertible if and only if 0 is one of the taps. The steps in a proof are indicated in Question 3 of Sheet 4.

Exercise 5.6

Let G be the LFSR of width 4 with taps $\{0, 2\}$.

(a) Find the keystreams for the keys 0001 and 0011.

(b) Which words of length 4 do not appear in either keystream?

(c) Find all keystreams generated by this LFSR.

True or false: the keystream for key 0110 has period 6?

(A) False (B) True

True or false: $G^6 = \mathrm{id}$, the identity function.

(A) False (B) True

Invertible LFSRs and periods: motivation

Exercise 5.5

Let H be the LFSR of width 4 with taps $\{1,2\}$. Show that H is not invertible.

This exercise and Example 5.2(i) suggest the general result: an LFSR is invertible if and only if 0 is one of the taps. The steps in a proof are indicated in Question 3 of Sheet 4.

Exercise 5.6

Let G be the LFSR of width 4 with taps $\{0,2\}$.

(a) Find the keystreams for the keys 0001 and 0011.

(b) Which words of length 4 do not appear in either keystream?

(c) Find all keystreams generated by this LFSR.

True or false: the keystream for key 0110 has period 6?

(A) False (B) True

True or false: $G^6 = \mathrm{id}$, the identity function.

(A) False (B) True

Invertible LFSRs and periods

Lemma 5.7

Let F be an invertible LFSR of width ℓ.

(i) *Let $k \in \mathbb{F}_2^\ell$. There exists $m \leq 2^\ell - 1$ such that $F^m(k) = k$.*

(ii) *There exists $m \in \mathbb{N}$ such that $F^m = \mathrm{id}$, the identity function.*

By this lemma the following definitions are well-defined.

Definition 5.8

(i) We define the *period* of a keystream $k_0, k_1, \ldots$ generated by an invertible LFSR to be the least m such that $k_{s+m} = k_s$ for all $s \in \mathbb{N}_0$.

(ii) We define the *period* of an invertible LFSR F to be the least m such that $F^m = \mathrm{id}$, the identity function.

For example, the LFSRs F and G in Example 5.2 and Exercise 5.6 have periods 15 and 6, respectively. By Lemma 5.7, the period of a keystream of an LFSR of width ℓ is at most $2^\ell - 1$.

Invertible LFSRs and periods

Lemma 5.7

Let F be an invertible LFSR of width ℓ.

(i) *Let $k \in \mathbb{F}_2^\ell$. There exists $m \leq 2^\ell - 1$ such that $F^m(k) = k$.*

(ii) *There exists $m \in \mathbb{N}$ such that $F^m = \mathrm{id}$, the identity function.*

By this lemma the following definitions are well-defined.

Definition 5.8

(i) We define the *period* of a keystream $k_0, k_1, \ldots$ generated by an invertible LFSR to be the least m such that $k_{s+m} = k_s$ for all $s \in \mathbb{N}_0$.

(ii) We define the *period* of an invertible LFSR F to be the least m such that $F^m = \mathrm{id}$, 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

Invertible LFSRs and periods

Lemma 5.7

Let F be an invertible LFSR of width ℓ.

(i) *Let $k \in \mathbb{F}_2^\ell$. There exists $m \leq 2^\ell - 1$ such that $F^m(k) = k$.*

(ii) *There exists $m \in \mathbb{N}$ such that $F^m = \mathrm{id}$, the identity function.*

By this lemma the following definitions are well-defined.

Definition 5.8

(i) We define the *period* of a keystream $k_0, k_1, \ldots$ generated by an invertible LFSR to be the least m such that $k_{s+m} = k_s$ for all $s \in \mathbb{N}_0$.

(ii) We define the *period* of an invertible LFSR F to be the least m such that $F^m = \mathrm{id}$, 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

Matrix representation of an LFSR

LFSRs are linear functions: if F is an LFSR of width ℓ then $F(x+x') = F(x) + F(x')$ for all x, $x' \in \mathbb{F}_2^\ell$. We can therefore represent an LFSR by a matrix.

Proposition 5.9

Let F be an LFSR of width ℓ and taps $T \subseteq \{0, 1, \ldots, \ell - 1\}$. The matrix (acting on row vectors) representing F is

$$\begin{pmatrix}
0 & 0 & 0 & \ldots & 0 & [0 \in T] \\
1 & 0 & 0 & \ldots & 0 & [1 \in T] \\
0 & 1 & 0 & \ldots & 0 & [2 \in T] \\
\vdots & \vdots & \ddots & \vdots & \vdots & \\
0 & 0 & 0 & \ldots & 0 & [\ell - 2 \in T] \\
0 & 0 & 0 & \ldots & 1 & [\ell - 1 \in T]
\end{pmatrix}$$

where

$$[t \in T] = \begin{cases} 1 & \textit{if } t \in T \\ 0 & \textit{otherwise.} \end{cases}$$

Matrix representation of an LFSR

LFSRs are linear functions: if F is an LFSR of width ℓ then $F(x+x') = F(x) + F(x')$ for all x, $x' \in \mathbb{F}_2^\ell$. We can therefore represent an LFSR by a matrix.

Quiz. The matrix representing the LFSR in Example 5.2 is

$$M = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

$$\mathbf{v}(0) = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \mathbf{v}(1) = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \mathbf{v}(2) = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \mathbf{v}(3) = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

What is $M\mathbf{v}(0)$?

(A) $\mathbf{v}(1)$ (B) $\mathbf{v}(2)$ (C) $\mathbf{v}(3)$ (D) $\mathbf{v}(0) + \mathbf{v}(1)$

What is $M\mathbf{v}(3)$?

(A) $\mathbf{v}(1)$ (B) $\mathbf{v}(2)$ (C) $\mathbf{v}(3)$ (D) $\mathbf{v}(0) + \mathbf{v}(1)$

Matrix representation of an LFSR

LFSRs are linear functions: if F is an LFSR of width ℓ then $F(x+x') = F(x) + F(x')$ for all $x, x' \in \mathbb{F}_2^\ell$. We can therefore represent an LFSR by a matrix.

Quiz. The matrix representing the LFSR in Example 5.2 is

$$M = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

$$\mathbf{v}(0) = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \mathbf{v}(1) = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \mathbf{v}(2) = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \mathbf{v}(3) = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

What is $M\mathbf{v}(0)$?

(A) $\mathbf{v}(1)$ (B) $\mathbf{v}(2)$ (C) $\mathbf{v}(3)$ (D) $\mathbf{v}(0) + \mathbf{v}(1)$

What is $M\mathbf{v}(3)$?

(A) $\mathbf{v}(1)$ (B) $\mathbf{v}(2)$ (C) $\mathbf{v}(3)$ (D) $\mathbf{v}(0) + \mathbf{v}(1)$

Matrix representation of an LFSR

LFSRs are linear functions: if F is an LFSR of width ℓ then $F(x+x') = F(x) + F(x')$ for all x, $x' \in \mathbb{F}_2^\ell$. We can therefore represent an LFSR by a matrix.

Quiz. The matrix representing the LFSR in Example 5.2 is

$$M = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

$$\mathbf{v}(0) = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \mathbf{v}(1) = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \mathbf{v}(2) = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \mathbf{v}(3) = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

What is $M\mathbf{v}(0)$?

(A) $\mathbf{v}(1)$ (B) $\mathbf{v}(2)$ (C) $\mathbf{v}(3)$ (D) $\mathbf{v}(0) + \mathbf{v}(1)$

What is $M\mathbf{v}(3)$?

(A) $\mathbf{v}(1)$ (B) $\mathbf{v}(2)$ (C) $\mathbf{v}(3)$ (D) $\mathbf{v}(0) + \mathbf{v}(1)$

Matrix Representing an LFSR

Proposition 5.9

Let F be an LFSR of width ℓ and taps $T \subseteq \{0, 1, \ldots, \ell - 1\}$. The matrix (acting on row vectors) representing F is

$$\begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & [0 \in T] \\ 1 & 0 & 0 & \ldots & 0 & [1 \in T] \\ 0 & 1 & 0 & \ldots & 0 & [2 \in T] \\ \vdots & \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & 0 & \ldots & 0 & [\ell - 2 \in T] \\ 0 & 0 & 0 & \ldots & 1 & [\ell - 1 \in T] \end{pmatrix}$$

where

$$[t \in T] = \begin{cases} 1 & \textit{if } t \in T \\ 0 & \textit{otherwise.} \end{cases}$$

Linear Algebra for LFSR

Lemma 5.10

Let F be an LFSR of width ℓ with taps T representing by the matrix M. Define $g(X) = X^\ell + \sum_{t \in T} X^t$.

(a) *If $t < \ell$ then $M^t \mathbf{v}(0) = \mathbf{v}(t)$;*

(b) $\sum_{t \in T} M^t \mathbf{v}(0) = M^\ell \mathbf{v}(0)$,

(c) $g(M)\mathbf{v} = 0$ *for all column vectors* $\mathbf{v}$,

(d) $g(X)$ *is the minimal polynomial of* M.

Linear Algebra for LFSR

Lemma 5.10

Let F be an LFSR of width ℓ with taps T representing by the matrix M. Define $g(X) = X^\ell + \sum_{t \in T} X^t$.

(a) *If $t < \ell$ then $M^t\mathbf{v}(0) = \mathbf{v}(t)$;*

(b) $\sum_{t \in T} M^t\mathbf{v}(0) = M^\ell\mathbf{v}(0)$,

(c) $g(M)\mathbf{v} = 0$ *for all column vectors* $\mathbf{v}$,

(d) $g(X)$ *is the minimal polynomial of M.*

Motivated by the lemma we define the *minimal polynomial* of an LFSR F of width ℓ with taps T to be $g_F(X) = X^\ell + \sum_{t \in T} X^t$.

Corollary 5.11

The period of an invertible LFSR F is the least m such that $g_F(X)$ divides $X^m + 1$.

LFSRs of Maximum Possible Period

Lemma 5.12

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

Example 5.13

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

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

Hence will show that the LFSR of width 13 with taps $\{0, 1, 3, 4\}$ has period 8191.

§6 Pseudo-random Number Generation

By Lemma 5.7(i) 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 6.1

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

$$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0 \ldots).$$

Correspondingly, by the Very Useful Property,

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

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

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

Exercise 6.1 [continued]

By taking the first 15 positions we get the generating cycle

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

(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 $(1, 1, 0, 0)$? [Printed notes have $(0, 0, 0, 1)$: same answer.]

(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

$$(0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$$

$k_0\ k_1\ k_2\ k_3\ k_4\ k_5\ k_6\ k_7\ k_8\ k_9\ k_{10}\ k_{11}\ k_{12}\ k_{13}\ k_{14}\ k_{15}\ k_{16}\ k_{17}\ k_{18}\ k_{19}\ k_{20}\ k_{21}\ k_{22}\ k_{23}\ k_{24}\ k_{25}\ k_{26}\ k_{27}\ k_{28}\ k_{29}\ k_{30}\ k_{31}$

- 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 111 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times 010 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times 100 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times 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} k_{31}

- 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 111 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times 010 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times 100 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times 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

$$(0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$$

$$k_0\ k_1\ k_2\ k_3\ k_4\ k_5\ k_6\ k_7\ k_8\ k_9\ k_{10}\ k_{11}\ k_{12}\ k_{13}\ k_{14}\ k_{15}\ k_{16}\ k_{17}\ k_{18}\ k_{19}\ k_{20}\ k_{21}\ k_{22}\ k_{23}\ k_{24}\ k_{25}\ k_{26}\ k_{27}\ k_{28}\ k_{29}\ k_{30}\ k_{31}$$

- 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 111 appear?
  (A) 1   (B) 2   (C) 3   (D) 4
- How many times 010 appear?
  (A) 1   (B) 2   (C) 3   (D) 4
- How many times 100 appear?
  (A) 1   (B) 2   (C) 3   (D) 4
- How many times 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} k_{31}

- 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 111 appear?
  (A) 1 (B) 2 (C) 3 [✓ (D) 4]
- How many times 010 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times 100 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times 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} k_{31}

- 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 111 appear?
  (A) 1 (B) 2 (C) 3 [✓ (D) 4]
- How many times 010 appear?
  (A) 1 (B) 2 (C) 3 [✓ (D) 4]
- How many times 100 appear?
  (A) 1 (B) 2 (C) 3 (D) 4
- How many times 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} k_{31}

- 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 111 appear?
  (A) 1 (B) 2 (C) 3 [✓ (D) 4]
- How many times 010 appear?
  (A) 1 (B) 2 (C) 3 [✓ (D) 4]
- How many times 100 appear?
  (A) 1 (B) 2 (C) 3 [✓ (D) 4]
- How many times 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} k_{31}

- 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 111 appear?
  (A) 1 (B) 2 (C) 3 [✓ (D) 4]
- How many times 010 appear?
  (A) 1 (B) 2 (C) 3 [✓ (D) 4]
- How many times 100 appear?
  (A) 1 (B) 2 (C) 3 [✓ (D) 4]
- How many times 000 appear?
  (A) 1 (B) 2 [✓ (C) 3] (D) 4

Generalizing Example 6.1

Proposition 6.2

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 t within this cycle, so $0 \le t < 2^\ell - 1$.

(a) *For each non-zero $x \in \mathbb{F}_2^\ell$ there exists a unique t such that*

$$(k_t, \ldots, k_{t+\ell-1}) = x.$$

(b) *Given any non-zero $y \in \mathbb{F}_2^m$ where $m \le \ell$, there are precisely $2^{\ell-m}$ positions t such that $(k_t, \ldots, t_{t+m-1}) = y$.*

(c) *There are precisely $2^{\ell-m} - 1$ positions t such that $(k_t, \ldots, k_{t+m-1}) = (0, 0, \ldots, 0) \in \mathbb{F}_2^m$.*

Testing for Randomness

Exercise 6.3

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 6.4

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 $\mathbb{P}[Z^2 \geq 6.635] \approx 0.01$.]

Sample Bias

Quiz: Suppose I ask you 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

Sample Bias

Quiz: Suppose I ask you 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 $\sim \text{Bin}\left(\frac{1}{2}, 3\right)$

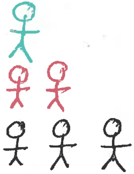
All children go to some school

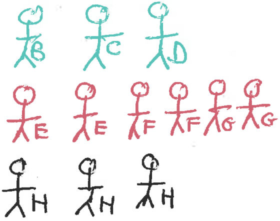
0 $\binom{3}{0}\left(\frac{1}{2}\right)^3 = \frac{1}{8}$ A

1 $\binom{3}{1}\left(\frac{1}{2}\right)^3 = \frac{3}{8}$ B C D

2 $\binom{3}{2}\left(\frac{1}{2}\right)^3 = \frac{3}{8}$ E F G

3 $\binom{3}{3}\left(\frac{1}{2}\right)^3 = \frac{1}{8}$ H





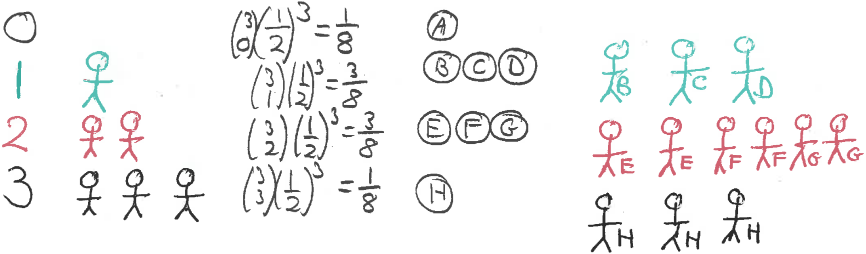
Sample Bias

Quiz: Suppose I ask you 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 $\sim \text{Bin}(\frac{1}{2}, 3)$

All children go to some school



$$\binom{3}{0}\left(\frac{1}{2}\right)^3 = \frac{1}{8}$$

$$\binom{3}{1}\left(\frac{1}{2}\right)^3 = \frac{3}{8}$$

$$\binom{3}{2}\left(\frac{1}{2}\right)^3 = \frac{3}{8}$$

$$\binom{3}{3}\left(\frac{1}{2}\right)^3 = \frac{1}{8}$$

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).

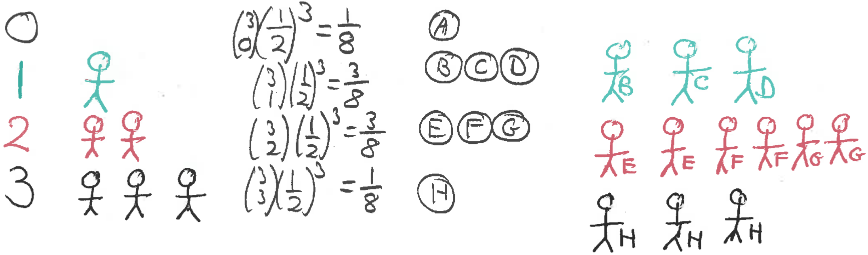
Sample Bias

Quiz: Suppose I ask you 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 $\sim \mathrm{Bin}(\frac{1}{2}, 3)$

All children go to some school



$$\binom{3}{0}\left(\frac{1}{2}\right)^3 = \frac{1}{8}$$

$$\binom{3}{1}\left(\frac{1}{2}\right)^3 = \frac{3}{8}$$

$$\binom{3}{2}\left(\frac{1}{2}\right)^3 = \frac{3}{8}$$

$$\binom{3}{3}\left(\frac{1}{2}\right)^3 = \frac{1}{8}$$

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 $1 + \mathrm{Bin}(2, \frac{1}{2})$ distribution.

Correlation

Definition 6.5

Given $(x_0, x_1, \ldots, x_{n-1})$ and $(y_0, y_1, \ldots, y_{n-1}) \in \mathbb{F}_2^n$ define

$$\begin{aligned} c_{\mathrm{same}} &= \bigl|\{i : x_i = y_i\}\bigr| \\ c_{\mathrm{diff}} &= \bigl|\{i : x_i \neq y_i\}\bigr|. \end{aligned}$$

The *correlation* between x and y is $(c_{\mathrm{same}} - c_{\mathrm{diff}})/n$.

Exercise 6.6

Find the correlation between a generating cycle for the LFSR of width 3 with taps $\{0, 1\}$ 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 6.7

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 $-1/(2^\ell - 1)$.

§7 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 5.3, the encryption functions $e_k : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ are defined by

$$e_k(x) = (u_0, u_1, \ldots, u_{n-1}) + (x_0, x_1, \ldots, x_{n-1}).$$

Exercise 7.1

In the LFSR cryptosystem of Definition 5.3, the sequence $u_0, u_1, u_2, \ldots$ is simply the keystream $k_0, k_1, k_2, \ldots$. Show how to find the key $(k_0, \ldots, k_{\ell-1})$ using a chosen plaintext attack.

Sum of LFSRs

Example 7.2

- Let F be the LFSR of width 4 with taps $\{0,3\}$ of period 15.

The first 20 bits in the keystreams for F with keys $k = (1,0,0,0)$ and $k^\star = (0,0,0,1)$ sum to the sequence $(u_0, u_1, \ldots, u_{19})$ below:

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

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 6.7.]

(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 7.2

- Let F be the LFSR of width 4 with taps $\{0,3\}$ of period 15.

The first 20 bits in the keystreams for F with keys $k = (1,0,0,0)$ and $k^\star = (0,0,0,1)$ sum to the sequence $(u_0, u_1, \ldots, u_{19})$ below:

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

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 6.7.]

(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 7.2

- Let F be the LFSR of width 4 with taps $\{0, 3\}$ of period 15.

The first 20 bits in the keystreams for F with keys $k = (1, 0, 0, 0)$ and $k^\star = (0, 0, 0, 1)$ sum to the sequence $(u_0, u_1, \ldots, u_{19})$ below:

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

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 6.7.]

(b) The attacker knows $(u_0, u_1, \ldots, u_{19})$ but cannot learn k and $k^\star$. Can he or she decrypt further ciphertexts?

(A) No (A) Yes

Sum of LFSRs

Example 7.2

- Let F be the LFSR of width 4 with taps $\{0, 3\}$ of period 15.

The first 20 bits in the keystreams for F with keys $k = (1, 0, 0, 0)$ and $k^\star = (0, 0, 0, 1)$ sum to the sequence $(u_0, u_1, \ldots, u_{19})$ below:

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

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 6.7.]

(b) The attacker knows $(u_0, u_1, \ldots, u_{19})$ but cannot learn k and $k^\star$. Can he or she decrypt further ciphertexts?

(A) No (A) Yes

Example 7.2 [continued]

- Let F' be the LFSR of width 3 with taps $\{0, 1\}$ of period 7.

The first 20 bits in the keystreams for F and F' with keys $k = (1, 0, 0, 0)$ and $k' = (0, 0, 1)$ and their sum $(u_0, u_1, \ldots, u_{19})$ are:

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

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 linear algebra method from Question 3 on Sheet 5 shows that the first 10 bits of $(u_0, u_1, u_2, \ldots)$ are generated by the LFSR of width 7 with taps $\{0, 1, 5, 6\}$.

Example 7.2 [continued]

- Let F' be the LFSR of width 3 with taps $\{0,1\}$ of period 7.

The first 20 bits in the keystreams for F and F' with keys $k = (1,0,0,0)$ and $k' = (0,0,1)$ and their sum $(u_0, u_1, \ldots, u_{19})$ are:

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

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 linear algebra method from Question 3 on Sheet 5 shows that the first 10 bits of $(u_0, u_1, u_2, \ldots)$ are generated by the LFSR of width 7 with taps $\{0, 1, 5, 6\}$.

Geffe Generator

Example 7.3

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 $(c_0, c_1, c_2, \ldots)$ be a keystream for G.

The *Geffe keystream* $(u_0, u_1, u_2, \ldots)$ is defined by

$$u_i = \begin{cases} k_i & \text{if } c_i = 0 \\ k'_i & \text{if } c_i = 1. \end{cases}$$

Example 7.3 [continued]

For example, if F is the LFSR of width 3 with taps $\{0,1\}$, F' is the LFSR of width 4 with taps $\{0,3\}$, and G is the LFSR of width 4 with taps $\{0,1\}$ and $(g_0, g_1, g_2, g_3) = (0,0,0,1)$ then [**corrected after lecture: F and F' got swapped by mistake**]

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

Quiz: the period of $u_0 u_1 u_2 \dots$ 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 $(k_0, \dots, k_{n-1})$ and $(u_0, \dots, u_{n-1})$?

(A) 0 (B) 1/4 (C) 1/2 (D) 3/4

Example 7.3 [continued]

For example, if F is the LFSR of width 3 with taps $\{0, 1\}$, F' is the LFSR of width 4 with taps $\{0, 3\}$, and G is the LFSR of width 4 with taps $\{0, 1\}$ and $(g_0, g_1, g_2, g_3) = (0, 0, 0, 1)$ then [**corrected after lecture: F and F' got swapped by mistake**]

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

Quiz: the period of $u_0 u_1 u_2 \ldots$ 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 is the LFSR of width 3 with taps $\{0, 1\}$, F' is the LFSR of width 4 with taps $\{0, 3\}$, and G is the LFSR of width 4 with taps $\{0, 1\}$ and $(g_0, g_1, g_2, g_3) = (0, 0, 0, 1)$ then [**corrected after lecture: F and F' got swapped by mistake**]

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

Quiz: the period of $u_0 u_1 u_2 \ldots$ 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 is the LFSR of width 3 with taps $\{0,1\}$, F' is the LFSR of width 4 with taps $\{0,3\}$, and G is the LFSR of width 4 with taps $\{0,1\}$ and $(g_0, g_1, g_2, g_3) = (0,0,0,1)$ then [**corrected after lecture: F and F' got swapped by mistake**]

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

Quiz: the period of $u_0 u_1 u_2 \ldots$ 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 is the LFSR of width 3 with taps $\{0, 1\}$, F' is the LFSR of width 4 with taps $\{0, 3\}$, and G is the LFSR of width 4 with taps $\{0, 1\}$ and $(g_0, g_1, g_2, g_3) = (0, 0, 0, 1)$ then [**corrected after lecture: F and F' got swapped by mistake**]

k_i	0	0	1	0	1	1	1	0	0	1	0	1	1	1	0	0	1	0	1	1
k'_i	1	0	0	0	1	1	1	1	0	1	0	1	1	0	0	1	0	0	0	1
g_i	0	0	0	1	0	0	1	1	0	1	0	1	1	1	1	0	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
	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 $(k_0, \ldots, k_{19})$ and $(u_0, \ldots, u_{19})$?

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

Example 7.3 [continued]

For example, if F is the LFSR of width 3 with taps $\{0,1\}$, F' is the LFSR of width 4 with taps $\{0,3\}$, and G is the LFSR of width 4 with taps $\{0,1\}$ and $(g_0, g_1, g_2, g_3) = (0,0,0,1)$ then [**corrected after lecture: F and F' got swapped by mistake**]

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

What is the correlation in this case between $(k_0, \ldots, k_{19})$ and $(u_0, \ldots, u_{19})$?

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

Example 7.3 [continued]

For example, if F is the LFSR of width 3 with taps $\{0, 1\}$, F' is the LFSR of width 4 with taps $\{0, 3\}$, and G is the LFSR of width 4 with taps $\{0, 1\}$ and $(g_0, g_1, g_2, g_3) = (0, 0, 0, 1)$ then [**corrected after lecture: F and F' got swapped by mistake**]

k_i	0,	0,	1,	0,	1,	1,	1,	0,	0,	1,	0,	1,	1,	1,	0,	0,	1,	0,	1,	1
k'_i	1,	0,	0,	0,	1,	1,	1,	1,	0,	1,	0,	1,	1,	0,	0,	1,	0,	0,	0,	1
g_i	0,	0,	0,	1,	0,	0,	1,	1,	0,	1,	0,	1,	1,	1,	1,	0,	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
	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 $(k_0, \ldots, k_{19})$ and $(u_0, \ldots, u_{19})$?

(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 is the LFSR of width 3 with taps $\{0, 1\}$, F' is the LFSR of width 4 with taps $\{0, 3\}$, and G is the LFSR of width 4 with taps $\{0, 1\}$ and $(g_0, g_1, g_2, g_3) = (0, 0, 0, 1)$ then [**corrected after lecture: F and F' got swapped by mistake**]

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

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 7.4

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 7.4

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 7.4

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 7.4 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. (There are also faster ways to finish: see Question 1(b) on Sheet 6.)

An attack such as Attack 7.4 is said to be *sub-exhaustive* because it finds the key using fewer guesses than brute-force exhaustive

Quadratic Stream Cipher

Example 7.5

Let F be the LFSR of width 5 with taps $\{0, 2\}$ and let F' be the LFSR of width 6 with taps $\{0, 1, 3, 4\}$. 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 $0 \leq s < m$. The *m-quadratic stream cipher* is the cryptosystem defined using the sequence u_0, u_1,. . . , 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 7.4 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 $\frac{1}{2^m}$. (If time permits this will be proved in the **M.Sc.** course.) 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 7.1.

Exercise 7.6

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 7.7 (TRIVIUM)

Take three LFSRs of widths 93, 84 and 101, tapping positions $\{0, 27\}$, $\{0, 15\}$ and $\{0, 45\}$, with internal states $x \in \mathbb{F}_2^{93}$, $x' \in \mathbb{F}_2^{84}$, $x'' \in \mathbb{F}_2^{101}$. The keystream is defined by

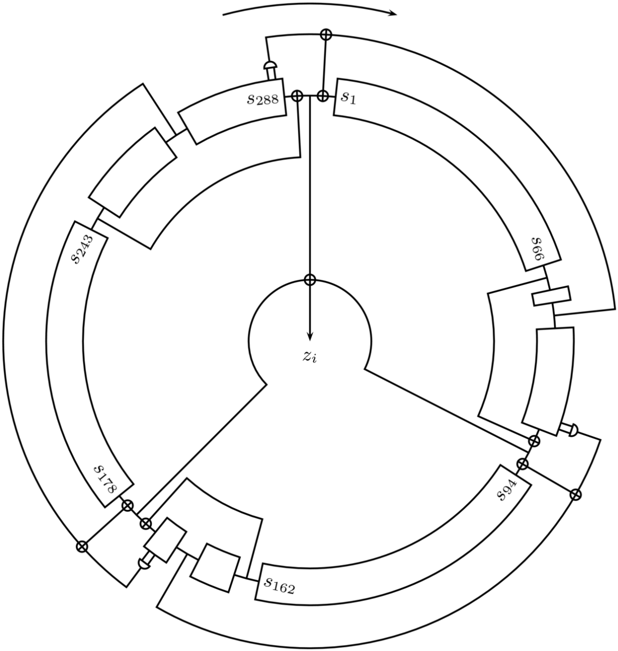
$$k_s = x_0 + x_{27} + x'_0 + x'_{15} + x''_0 + x''_{45}.$$

The feedback functions are

$$\begin{aligned} f\big((x_0, \ldots, x_{92})\big) &= x_0 + x_{27} + x_1 x_2 + x'_6 \\ f'\big((x'_0, \ldots, x'_{84})\big) &= x'_0 + x_{15} + x'_1 x'_2 + x''_{24} \\ f''\big((x''_0, \ldots, x''_{101}\big) &= x''_0 + x''_{14} + x''_1 x''_2 + x_{24} \end{aligned}$$

In each case the final summand introduces a bit from a different shift register.

Trivium



Sheet 5 Question 2

Encrypt using the LFSR cryptosystem (take key, make keystream, add to plaintext) using the LFSR F of width 5 and taps $\{0, 2\}$.

(a) Let $k_0 k_1 k_2 \ldots$ be the keystream for your key. Show that $k_{32m} = k_m$ for each $m \in \mathbb{N}_0$.

(d) Decrypt either of the messages from the other two people in your cell. [*Hint:* start by looking at bits 0 and 32 in the ciphertext. If you do not have a ciphertext to decrypt, use the one in the MATHEMATICA notebook.]

(e) What is the smallest number of ciphertext bits needed to determine the key?

Part C: Block ciphers

§8 Introduction to Block Ciphers and Feistel Networks

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

§8 Introduction to Block Ciphers and Feistel Networks

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 8.1

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

§8 Introduction to Block Ciphers and Feistel Networks

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.

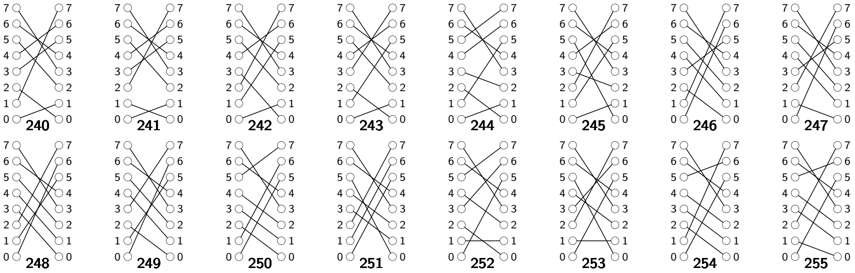
Example 8.1

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 8.2

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 $e_k : \mathbb{F}_2^3 \to \mathbb{F}_2^3$ for $k \in \mathcal{K}$, chosen according to a fairly arbitrary rule (details omitted). For example, since $11111100 \in \mathbb{F}_2^8$ is the binary form of **252**, and $000, 010, 011, 110 \in \mathbb{F}_2^3$ are the binary form of $0, 2, 3, 6$, diagram **252** shows that $e_{11111100}(010) = 000$ and $e_{11111100}(011) = 110$.



The other 240 permutations are posted on Moodle and will be available in the lecture.

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 $e_k(000) = 101$ and $e_k(001) = 111$. One possible key is 254. There are six others: find at least one of them.

(ii) By choosing two further plaintexts Mark learns that $e_k(011) = 001$ and $e_k(110) = 011$. Determine k.

(iii) Later Mark's boss Eve observes the ciphertext 100. What is $d_k(100)$?

In this case since $|\mathbb{F}_2^3| = 8$, there are $8! = 40320$ permutations of $\mathbb{F}_2^3$, of which 256 were used.

Feistel Networks

Definition 8.3

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 8.4

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 8.5 (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:

$$\begin{aligned}(v, w) = (v^{(0)}, v^{(1)}) &\mapsto \big(v^{(1)}, v^{(0)} + S(v^{(1)} + k^{(1)})\big) = (v^{(1)}, v^{(2)})\\ &\mapsto \big(v^{(2)}, v^{(1)} + S(v^{(2)} + k^{(2)})\big) = (v^{(2)}, v^{(3)})\\ &\mapsto \big(v^{(3)}, v^{(2)} + S(v^{(3)} + k^{(3)})\big) = (v^{(3)}, v^{(4)}).\end{aligned}$$

Correction for **M.Sc.** students

In the initialization step for Berlekamp–Massey (page 15 printed notes), please change $\ell_{c+1} = c$ to $\ell_{c+1} = c + 1$.

Explanation (for all). The Berlekamp–Massey Algorithm finds an LFSR generating a given keystream $k_0 k_1 k_2 \ldots$. By definition c is the least numbered position such that $k_c = 1$, so

$$k_0 = \ldots = k_{c-1} = 0, k_c = 1.$$

Any LFSR generating

$$\underset{0}{(0}, \underset{1}{0}, \ldots, \underset{(c-1)}{0}, \underset{c}{1})$$

must have width at least $c + 1$, since otherwise the key that fills the LFSR is all-zeros, so all positions in the keystream are 0.

Q-Block Cipher

Exercise 8.6

(a) Suppose that $k = 0001\,0011\,0000$, shown split into the three round keys. Show that

$$e_k\big((0,0,0,0,0,0,0,0)\big) = (1,1,1,0,1,1,0,1)$$

(b) Find $d_k\big((0,0,0,0,0,0,0,1)\big)$ if the key is as in (a).

(c) Suppose Eve observes the ciphertext $(v^{(3)}, v^{(4)})$ from the Q-block cipher. What does she need to know to determine $v^{(2)}$?

Exercise 8.7

Suppose we change the Feistel function in round i to $x \mapsto S(x) + k^{(i)}$. What is $(v^{(1)}, v^{(2)})$ in terms of v, w and $k^{(1)}$? Which cipher is likely to be stronger?

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 $z = \big(S_1(y^{(1)}), \ldots, S_8(y^{(8)})\big) \in \mathbb{F}_2^{32}$. *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 has no Sub-exhaustive Attacks (43 Years . . .)

But the small keyspace $\mathbb{F}_2^{56}$ makes it insecure.

- 1997: 140 days, distributed search on internet
- 1998: 9 days 'DES cracker' (special purpose) \$250000
- 2017: 6 days 'COPACOBANA' **[Typo: COPACOBONA in printed notes]** (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}

Exercise 8.8

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 has no Sub-exhaustive Attacks (43 Years . . .)

But the small keyspace $\mathbb{F}_2^{56}$ makes it insecure.

- 1997: 140 days, distributed search on internet
- 1998: 9 days ‘DES cracker’ (special purpose) $250000
- 2017: 6 days ‘COPACOBANA’ **[Typo: COPACOBONA in printed notes]** (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}

Exercise 8.8

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 has no Sub-exhaustive Attacks (43 Years . . .)

But the small keyspace $\mathbb{F}_2^{56}$ makes it insecure.

- 1997: 140 days, distributed search on internet
- 1998: 9 days ‘DES cracker’ (special purpose) \$250000
- 2017: 6 days ‘COPACOBANA’ **[Typo: COPACOBONA in printed notes]** (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}

Exercise 8.8

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 has no Sub-exhaustive Attacks (43 Years . . .)

But the small keyspace $\mathbb{F}_2^{56}$ makes it insecure.

- 1997: 140 days, distributed search on internet
- 1998: 9 days ‘DES cracker’ (special purpose) $250000
- 2017: 6 days ‘COPACOBANA’ **[Typo: COPACOBONA in printed notes]** (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}

Exercise 8.8

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 has no Sub-exhaustive Attacks (43 Years . . .)

But the small keyspace $\mathbb{F}_2^{56}$ makes it insecure.

- 1997: 140 days, distributed search on internet
- 1998: 9 days ‘DES cracker’ (special purpose) \$250000
- 2017: 6 days ‘COPACOBANA’ **[Typo: COPACOBONA in printed notes]** (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}

Exercise 8.8

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 $y \in \mathbb{F}_2^{64}$, by some unknown key

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

Meet-in-the-Middle Attack on 2DES

In a chosen plaintext attack on 2DES we may choose any plaintext $x \in \mathbb{F}_2^{64}$ and get its encryption $y \in \mathbb{F}_2^{64}$, by some unknown key

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

We defined

$$E = \{e_k(x) : k \in \mathbb{F}_2^{56}\}$$
$$D = \{d_{k'}(y) : k' \in \mathbb{F}_2^{56}\}$$

Assume that k and k' are chosen independently. Given a random $w \in \mathbb{F}_2^{64}$, what, approximately, is $\mathbb{P}[w \in E]$?

(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 $y \in \mathbb{F}_2^{64}$, by some unknown key

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

We defined

$$E = \{e_k(x) : k \in \mathbb{F}_2^{56}\}$$
$$D = \{d_{k'}(y) : k' \in \mathbb{F}_2^{56}\}$$

Assume that k and k' are chosen independently. Given a random $w \in \mathbb{F}_2^{64}$, what, approximately, is $\mathbb{P}[w \in E]$?

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

What is a good approximation to $\mathbb{P}[w \in E \cap D]$?

(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 $y \in \mathbb{F}_2^{64}$, by some unknown key

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

We defined

$$E = \{e_k(x) : k \in \mathbb{F}_2^{56}\}$$
$$D = \{d_{k'}(y) : k' \in \mathbb{F}_2^{56}\}$$

Assume that k and k' are chosen independently. Given a random $w \in \mathbb{F}_2^{64}$, what, approximately, is $\mathbb{P}[w \in E]$?

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

What is a good approximation to $\mathbb{P}[w \in E \cap D]$?

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

How many encryptions / decryptions does it take to find the 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 $y \in \mathbb{F}_2^{64}$, by some unknown key

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

We defined

$$E = \{e_k(x) : k \in \mathbb{F}_2^{56}\}$$
$$D = \{d_{k'}(y) : k' \in \mathbb{F}_2^{56}\}$$

Assume that k and k' are chosen independently. Given a random $w \in \mathbb{F}_2^{64}$, what, approximately, is $\mathbb{P}[w \in E]$?

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

What is a good approximation to $\mathbb{P}[w \in E \cap D]$?

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

How many encryptions / decryptions does it take to find the 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 $y \in \mathbb{F}_2^{64}$, by some unknown key

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

We defined

$$E = \{e_k(x) : k \in \mathbb{F}_2^{56}\}$$
$$D = \{d_{k'}(y) : k' \in \mathbb{F}_2^{56}\}$$

Assume that k and k' are chosen independently. Given a random $w \in \mathbb{F}_2^{64}$, what, approximately, is $\mathbb{P}[w \in E]$?

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

What is a good approximation to $\mathbb{P}[w \in E \cap D]$?

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

How many encryptions / decryptions does it take to find the 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 $y \in \mathbb{F}_2^{64}$, by some unknown key

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

We defined

$$E = \{e_k(x) : k \in \mathbb{F}_2^{56}\}$$
$$D = \{d_{k'}(y) : k' \in \mathbb{F}_2^{56}\}$$

Assume that k and k' are chosen independently. Given a random $w \in \mathbb{F}_2^{64}$, what, approximately, is $\mathbb{P}[w \in E]$?

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

What is a good approximation to $\mathbb{P}[w \in E \cap D]$?

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

How many encryptions / decryptions does it take to find the 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}

AES (Advanced Encryption Standard)

AES is the winner of an open competition to design a successor to DES. Belgian cryptographers Vincent Rijmen and Joan Daemen.

- Block size 128 bits
- Keyspace $\mathbb{F}_2^{128}$ (also versions for $\mathbb{F}_2^{192}$ and $\mathbb{F}_2^{256}$)
- Not Feistel, but still multiple rounds like DES.
- Confusion comes from pseudo-inversion in the finite field $\mathbb{F}_{2^8}$.
- Diffusion comes from an affine transformation of $\mathbb{F}_2^8$.

AES Ingredients: Example 8.9

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 defined by

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

(a) $d_{(A,b)}(y)$ is

(A) $xA^{-1} + b$ (B) $yA^{-1} + b$ (C) $(y + b)A^{-1}$ (D) $y + bA^{-1}$

(b) When $n = 2$, how many plaintexts are required to find the key in a *chosen plaintext* attack?

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

(c) Does repeating the cipher (as in 2DES, so using two different keys) make this cipher any more secure?

(A) No (B) Yes

(d) Does this cipher have the ‘confusion’ property?

(A) No (B) Yes

(e) Does this cipher have the ‘diffusion’ property?

(A) No (B) Yes

AES Ingredients: Example 8.9

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 defined by

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

(a) $d_{(A,b)}(y)$ is

(A) $xA^{-1} + b$ (B) $yA^{-1} + b$ [✓ (C)] $(y + b)A^{-1}$ (D) $y + bA^{-1}$

(b) When $n = 2$, how many plaintexts are required to find the key in a *chosen plaintext* attack?

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

(c) Does repeating the cipher (as in 2DES, so using two different keys) make this cipher any more secure?

(A) No (B) Yes

(d) Does this cipher have the 'confusion' property?

(A) No (B) Yes

(e) Does this cipher have the 'diffusion' property?

(A) No (B) Yes

AES Ingredients: Example 8.9

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 defined by

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

(a) $d_{(A,b)}(y)$ is

(A) $xA^{-1} + b$ (B) $yA^{-1} + b$ [✓ (C) $(y + b)A^{-1}$] (D) $y + bA^{-1}$

(b) When $n = 2$, how many plaintexts are required to find the key in a *chosen plaintext* attack?

(A) 2 [✓ (B) 3] (C) 4 (D) many

(c) Does repeating the cipher (as in 2DES, so using two different keys) make this cipher any more secure?

(A) No (B) Yes

(d) Does this cipher have the 'confusion' property?

(A) No (B) Yes

(e) Does this cipher have the 'diffusion' property?

(A) No (B) Yes

AES Ingredients: Example 8.9

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 defined by

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

(a) $d_{(A,b)}(y)$ is

(A) $xA^{-1} + b$ (B) $yA^{-1} + b$ [✓ (C)] $(y + b)A^{-1}$ (D) $y + bA^{-1}$

(b) When $n = 2$, how many plaintexts are required to find the key in a *chosen plaintext* attack?

(A) 2 [✓ (B)] 3 (C) 4 (D) many

(c) Does repeating the cipher (as in 2DES, so using two different keys) make this cipher any more secure?

[✓ (A) No] (B) Yes

(d) Does this cipher have the 'confusion' property?

(A) No (B) Yes

(e) Does this cipher have the 'diffusion' property?

(A) No (B) Yes

AES Ingredients: Example 8.9

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 defined by

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

(a) $d_{(A,b)}(y)$ is

(A) $xA^{-1} + b$ (B) $yA^{-1} + b$ [✓ (C) $(y + b)A^{-1}$] (D) $y + bA^{-1}$

(b) When $n = 2$, how many plaintexts are required to find the key in a *chosen plaintext* attack?

(A) 2 [✓ (B) 3] (C) 4 (D) many

(c) Does repeating the cipher (as in 2DES, so using two different keys) make this cipher any more secure?

[✓ (A) No] (B) Yes

(d) Does this cipher have the 'confusion' property?

[✓ (A) No] (B) Yes

(e) Does this cipher have the 'diffusion' property?

(A) No (B) Yes

AES Ingredients: Example 8.9

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 defined by

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

(a) $d_{(A,b)}(y)$ is

(A) $xA^{-1} + b$ (B) $yA^{-1} + b$ [✓ (C) $(y + b)A^{-1}$] (D) $y + bA^{-1}$

(b) When $n = 2$, how many plaintexts are required to find the key in a *chosen plaintext* attack?

(A) 2 [✓ (B) 3] (C) 4 (D) many

(c) Does repeating the cipher (as in 2DES, so using two different keys) make this cipher any more secure?

[✓ (A) No] (B) Yes

(d) Does this cipher have the 'confusion' property?

[✓ (A) No] (B) Yes

(e) Does this cipher have the 'diffusion' property?

(A) No [✓ (B) Yes]

AES Ingredients: The Finite Field $\mathbb{F}_{2^8}$

Example 8.10

Let α be an indeterminate. Define

$$\mathbb{F}_{2^8} = \{x_0 + x_1\alpha + \cdots + x_7\alpha^7 : x_0, x_1, \ldots, x_7 \in \mathbb{F}_2\}.$$

Elements of $\mathbb{F}_2^8$ are added and multiplied like polynomials in α with coefficients in $\mathbb{F}_2$, but whenever you see a power α^d where $d \geq 8$, eliminate it using the rule

$$1 + \alpha + \alpha^3 + \alpha^4 + \alpha^8 = 0.$$

For example $(1 + \alpha) + (\alpha + \alpha^5) = 1 + \alpha^5$ and

$$\alpha^9 = \alpha \times \alpha^8 = \alpha(1 + \alpha + \alpha^3 + \alpha^4) = \alpha^2 + \alpha^3 + \alpha^4 + \alpha^5.$$

Multiplying the defining rule for α by α^{-1}, we get $\alpha^{-1} + 1 + \alpha^2 + \alpha^3 + \alpha^7 = 0$ so $\alpha^{-1} = 1 + \alpha^2 + \alpha^3 + \alpha^7$.

Quiz on $\mathbb{F}_{2^8}$

Recall that $\mathbb{F}_{2^8}$ is the set of polynomials in α of degree at most 7 with coefficients in $\mathbb{F}_2$. Higher powers of α must be eliminated using the rule

$$1 + \alpha + \alpha^3 + \alpha^4 + \alpha^8 = 0.$$

Note that $2^8 = 256$. Let $\mathbb{Z}_{2^8} = \{0, 1, \ldots, 255\}$ be the integers modulo 256. (i) True or false? $\mathbb{F}_{2^8} \cong \mathbb{Z}_{2^8}$?

(A) False (B) True

(ii) What is $(1 + \alpha + \alpha^3) + (\alpha + \alpha^3 + \alpha^7)$?

(A) $1 + \alpha + \alpha^7$ (B) $1 + \alpha^7$ (C) $1 + \alpha^3 + \alpha^7$ (D) $\alpha + \alpha^7$

(iii) What is $(\alpha + \alpha^2 + \alpha^3)^2$?

(A) $\alpha^2 + \alpha^3 + \alpha^4 + \alpha^5 + \alpha^6$ (B) α^2 (C) $\alpha^2 + \alpha^4 + \alpha^6$ (D) 0

(iv) What is α^{10}?

(A) α^2 (B) $\alpha + \alpha^2 + \alpha^5 + \alpha^6$

(C) $1 + \alpha + \alpha^3 + \alpha^4 + \alpha^8$ (D) $\alpha^2 + \alpha^3 + \alpha^5 + \alpha^6$

Quiz on $\mathbb{F}_{2^8}$

Recall that $\mathbb{F}_{2^8}$ is the set of polynomials in α of degree at most 7 with coefficients in $\mathbb{F}_2$. Higher powers of α must be eliminated using the rule

$$1 + \alpha + \alpha^3 + \alpha^4 + \alpha^8 = 0.$$

Note that $2^8 = 256$. Let $\mathbb{Z}_{2^8} = \{0, 1, \ldots, 255\}$ be the integers modulo 256. (i) True or false? $\mathbb{F}_{2^8} \cong \mathbb{Z}_{2^8}$?

(A) False (B) True

(ii) What is $(1 + \alpha + \alpha^3) + (\alpha + \alpha^3 + \alpha^7)$?

(A) $1 + \alpha + \alpha^7$ (B) $1 + \alpha^7$ (C) $1 + \alpha^3 + \alpha^7$ (D) $\alpha + \alpha^7$

(iii) What is $(\alpha + \alpha^2 + \alpha^3)^2$?

(A) $\alpha^2 + \alpha^3 + \alpha^4 + \alpha^5 + \alpha^6$ (B) α^2 (C) $\alpha^2 + \alpha^4 + \alpha^6$ (D) 0

(iv) What is α^{10}?

(A) α^2 (B) $\alpha + \alpha^2 + \alpha^5 + \alpha^6$

(C) $1 + \alpha + \alpha^3 + \alpha^4 + \alpha^8$ (D) $\alpha^2 + \alpha^3 + \alpha^5 + \alpha^6$

Quiz on $\mathbb{F}_{2^8}$

Recall that $\mathbb{F}_{2^8}$ is the set of polynomials in α of degree at most 7 with coefficients in $\mathbb{F}_2$. Higher powers of α must be eliminated using the rule

$$1 + \alpha + \alpha^3 + \alpha^4 + \alpha^8 = 0.$$

Note that $2^8 = 256$. Let $\mathbb{Z}_{2^8} = \{0, 1, \ldots, 255\}$ be the integers modulo 256. (i) True or false? $\mathbb{F}_{2^8} \cong \mathbb{Z}_{2^8}$?

(A) False (B) True

(ii) What is $(1 + \alpha + \alpha^3) + (\alpha + \alpha^3 + \alpha^7)$?

(A) $1 + \alpha + \alpha^7$ (B) $1 + \alpha^7$ (C) $1 + \alpha^3 + \alpha^7$ (D) $\alpha + \alpha^7$

(iii) What is $(\alpha + \alpha^2 + \alpha^3)^2$?

(A) $\alpha^2 + \alpha^3 + \alpha^4 + \alpha^5 + \alpha^6$ (B) α^2 (C) $\alpha^2 + \alpha^4 + \alpha^6$ (D) 0

(iv) What is α^{10}?

(A) α^2 (B) $\alpha + \alpha^2 + \alpha^5 + \alpha^6$

(C) $1 + \alpha + \alpha^3 + \alpha^4 + \alpha^8$ (D) $\alpha^2 + \alpha^3 + \alpha^5 + \alpha^6$

Quiz on $\mathbb{F}_{2^8}$

Recall that $\mathbb{F}_{2^8}$ is the set of polynomials in α of degree at most 7 with coefficients in $\mathbb{F}_2$. Higher powers of α must be eliminated using the rule

$$1 + \alpha + \alpha^3 + \alpha^4 + \alpha^8 = 0.$$

Note that $2^8 = 256$. Let $\mathbb{Z}_{2^8} = \{0, 1, \ldots, 255\}$ be the integers modulo 256. (i) True or false? $\mathbb{F}_{2^8} \cong \mathbb{Z}_{2^8}$?

(A) False (B) True

(ii) What is $(1 + \alpha + \alpha^3) + (\alpha + \alpha^3 + \alpha^7)$?

(A) $1 + \alpha + \alpha^7$ (B) $1 + \alpha^7$ (C) $1 + \alpha^3 + \alpha^7$ (D) $\alpha + \alpha^7$

(iii) What is $(\alpha + \alpha^2 + \alpha^3)^2$?

(A) $\alpha^2 + \alpha^3 + \alpha^4 + \alpha^5 + \alpha^6$ (B) α^2 (C) $\alpha^2 + \alpha^4 + \alpha^6$ (D) 0

(iv) What is α^{10}?

(A) α^2 (B) $\alpha + \alpha^2 + \alpha^5 + \alpha^6$

(C) $1 + \alpha + \alpha^3 + \alpha^4 + \alpha^8$ (D) $\alpha^2 + \alpha^3 + \alpha^5 + \alpha^6$

Quiz on $\mathbb{F}_{2^8}$

Recall that $\mathbb{F}_{2^8}$ is the set of polynomials in α of degree at most 7 with coefficients in $\mathbb{F}_2$. Higher powers of α must be eliminated using the rule

$$1 + \alpha + \alpha^3 + \alpha^4 + \alpha^8 = 0.$$

Note that $2^8 = 256$. Let $\mathbb{Z}_{2^8} = \{0, 1, \ldots, 255\}$ be the integers modulo 256. (i) True or false? $\mathbb{F}_{2^8} \cong \mathbb{Z}_{2^8}$?

(A) False (B) True

(ii) What is $(1 + \alpha + \alpha^3) + (\alpha + \alpha^3 + \alpha^7)$?

(A) $1 + \alpha + \alpha^7$ (B) $1 + \alpha^7$ (C) $1 + \alpha^3 + \alpha^7$ (D) $\alpha + \alpha^7$

(iii) What is $(\alpha + \alpha^2 + \alpha^3)^2$?

(A) $\alpha^2 + \alpha^3 + \alpha^4 + \alpha^5 + \alpha^6$ (B) α^2 (C) $\alpha^2 + \alpha^4 + \alpha^6$ (D) 0

(iv) What is α^{10}?

(A) α^2 (B) $\alpha + \alpha^2 + \alpha^5 + \alpha^6$

(C) $1 + \alpha + \alpha^3 + \alpha^4 + \alpha^8$ (D) $\alpha^2 + \alpha^3 + \alpha^5 + \alpha^6$

Pseudo-Inversion

Definition 8.11

Let $\mathbb{F}_{2^8}$ be the finite field of size 2^8 as in Example 8.10. 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 $\mathbb{F}_2(\alpha)$ by

$$(x_0, x_1, \ldots, x_7) \longleftrightarrow x_0 + x_1\alpha + x_2\alpha^2 + \cdots + x_7\alpha^7.$$

For example, writing elements of $\mathbb{F}_2^8$ as words of length 8,

(1) $1000\,0000 \longleftrightarrow 1 \in \mathbb{F}_{2^8}$ so $P(1000\,0000) = 10000000$

(2) $0100\,0000 \longleftrightarrow \alpha \in \mathbb{F}_{2^8}$ and $\alpha^{-1} = 1 + \alpha^2 + \alpha^3 + \alpha^7$ was found in Example 8.10, so $P(0100\,0000) = 10110001$.

Quiz: What is $P(0010\,0000)$?

(A) $1100\,0011$ (B) $1101\,0011$ (C) $1100\,0001$ (D) $1100\,0011$

Pseudo-Inversion

Definition 8.11

Let $\mathbb{F}_{2^8}$ be the finite field of size 2^8 as in Example 8.10. 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 $\mathbb{F}_2(\alpha)$ by

$$(x_0, x_1, \ldots, x_7) \longleftrightarrow x_0 + x_1\alpha + x_2\alpha^2 + \cdots + x_7\alpha^7.$$

For example, writing elements of $\mathbb{F}_2^8$ as words of length 8,

(1) $1000\,0000 \longleftrightarrow 1 \in \mathbb{F}_{2^8}$ so $P(1000\,0000) = 10000000$

(2) $0100\,0000 \longleftrightarrow \alpha \in \mathbb{F}_{2^8}$ and $\alpha^{-1} = 1 + \alpha^2 + \alpha^3 + \alpha^7$ was found in Example 8.10, so $P(0100\,0000) = 10110001$.

Quiz: What is $P(0010\,0000)$?

(A) $1100\,0011$ (B) $1101\,0011$ (C) $1100\,0001$ (D) $1100\,0011$

Definition of AES

There are 10 rounds in AES. In each round, the input $x \in \mathbb{F}_2^{128}$ is split into 16 subblocks each in $\mathbb{F}_2^8$.

- The pseudo inverse function $P : \mathbb{F}_2^8 \to \mathbb{F}_2^8$ is applied to each subblock, followed by an affine transformation $\mathbb{F}_2^8 \to \mathbb{F}_2^8$, as in the affine block cipher. This gives confusion and diffusion *within each subblock*.

- Diffusion comes from a row permutation of the 16 subblocks, organized into a 4 × 4 grid:

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

  Each column is then mixed by an invertible linear map, giving further diffusion.

- The round key in $\mathbb{F}_2^{128}$ is added after these two steps.

There are no known sub-exhaustive attacks on AES. It is the most commonly used block cipher.

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 $x^{(1)}, \dots, x^{(m)} \in \mathbb{F}_2^n$:

$$x = (x^{(1)}, \dots, x^{(m)}).$$

Fix a key $k \in \mathcal{K}$: this is only key used.

- Electronic Codebook Mode:

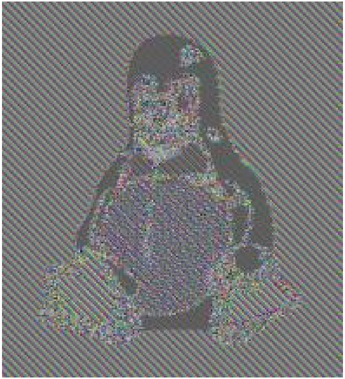
$$\begin{aligned} x^{(1)} &\mapsto e_k(x^{(1)}) \\ x^{(2)} &\mapsto e_k(x^{(2)}) \\ &\vdots \\ x^{(m)} &\mapsto e_k(x^{(m)}) \end{aligned}$$

- 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.

§9 Differential Cryptanalysis

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 $k_{\mathrm{otp}} \in \mathbb{F}_2^n$, and known ciphertexts $x + k_{\mathrm{otp}}$ and $x' + k_{\mathrm{otp}}$. Adding the known ciphertexts gives $x + x'$, independent of k_{otp}.

§9 Differential Cryptanalysis

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 $k_{\mathrm{otp}} \in \mathbb{F}_2^n$, and known ciphertexts $x + k_{\mathrm{otp}}$ and $x' + k_{\mathrm{otp}}$. Adding the known ciphertexts gives $x + x'$, independent of k_{otp}.

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

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

This shows the one-time-pad is weak to differences.

§9 Differential Cryptanalysis

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 $k_{\mathrm{otp}} \in \mathbb{F}_2^n$, and known ciphertexts $x + k_{\mathrm{otp}}$ and $x' + k_{\mathrm{otp}}$. Adding the known ciphertexts gives $x + x'$, independent of k_{otp}.

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

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

This shows the one-time-pad is weak to differences.

Quiz: If this is a difference attack, where are all the minus signs?

§9 Differential Cryptanalysis

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 $k_{\mathrm{otp}} \in \mathbb{F}_2^n$, and known ciphertexts $x + k_{\mathrm{otp}}$ and $x' + k_{\mathrm{otp}}$. Adding the known ciphertexts gives $x + x'$, independent of k_{otp}.

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

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

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

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

§9 Differential Cryptanalysis

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 $k_{\mathrm{otp}} \in \mathbb{F}_2^n$, and known ciphertexts $x + k_{\mathrm{otp}}$ and $x' + k_{\mathrm{otp}}$. Adding the known ciphertexts gives $x + x'$, independent of k_{otp}.

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

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

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

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

The DES S-boxes and the pseudo-inverse function $P : \mathbb{F}_2^8 \to \mathbb{F}_2^8$ in AES are chosen to avoid this weakness. By the exercise below an output difference of 1 to P can come from many different input differences.

Exercise 9.1

Let $\Gamma \in \mathbb{F}_2^8$ be non-zero. Show that

$$\left\{w \in \mathbb{F}_2^8 : P(w) + P(w + \Gamma) = 1000\,0000\right\}$$

has size 0 or 2, except when $\Gamma = 1000\,0000$, when it has size 4. [*Hint:* quadratic equations over any field have at most two roots.]

Exercise 9.2

Fix $\Gamma = \mathbb{F}_2^8$. Let $w \in \mathbb{F}_2^8$ be chosen uniformly at random. What are the possible values for $\mathbb{P}[P(w) + P(w + \Gamma) = 1000\,0000]$ as Γ varies in $\mathbb{F}_2^8$?

(A) $\{0, 1\}$ (B) $\{0, \frac{1}{256}, \frac{1}{128}\}$ (C) $\{0, \frac{1}{128}, \frac{1}{64}\}$ (D) $\{\frac{1}{128}, \frac{1}{64}\}$

The DES S-boxes and the pseudo-inverse function $P : \mathbb{F}_2^8 \to \mathbb{F}_2^8$ in AES are chosen to avoid this weakness. By the exercise below an output difference of 1 to P can come from many different input differences.

Exercise 9.1

Let $\Gamma \in \mathbb{F}_2^8$ be non-zero. Show that

$$\bigl\{ w \in \mathbb{F}_2^8 : P(w) + P(w + \Gamma) = 1000\,0000 \bigr\}$$

has size 0 or 2, except when $\Gamma = 1000\,0000$, when it has size 4. [*Hint:* quadratic equations over any field have at most two roots.]

Exercise 9.2

Fix $\Gamma = \mathbb{F}_2^8$. Let $w \in \mathbb{F}_2^8$ be chosen uniformly at random. What are the possible values for $\mathbb{P}[P(w) + P(w + \Gamma) = 1000\,0000]$ as Γ varies in $\mathbb{F}_2^8$?

(A) $\{0, 1\}$ (B) $\{0, \frac{1}{256}, \frac{1}{128}\}$ (C) $\{0, \frac{1}{128}, \frac{1}{64}\}$ (D) $\{\frac{1}{128}, \frac{1}{64}\}$

Feedback on Sheet 7 / Other Question

- Always $+$ denotes vector space addition. E.g. in $\mathbb{F}_2^4$

  $$0011 + 1010 = 1001.$$

  (In cryptography it is usual to use $\boxplus$ for addition of integers: $0011 \boxplus 1010 = 1101$ is $3 + 10 = 13$.)

- Question 4. Working with DES, so the key length is 56, how many operations are needed to compute all the triples $\big(k, k', d_{k'}(e_k(x))\big)$ for all $k, k' \in \mathbb{F}_2^{56}$?

  (A) 2^{56} (B) 2^{57} (C) 2^{112} (D) other

- Question: how are block ciphers actually implemented?
  Answer: the operations are chosen to be efficient on modern computers that store everything in binary. For instance

  - `int x = 341`

  tells the C compiler to put 341 in a new memory location, and label it x. Since $341 = 1 + 4 + 16 + 64 + 256$, this represents $x = \ldots 01010101 \in \mathbb{F}_2^{32}$. To add a key, we use binary XOR:

  - `int y = 341 ^ 15`

  makes $\ldots 01010101 + \ldots 00001111 = \ldots 01011010$.

Feedback on Sheet 7 / Other Question

- Always $+$ denotes vector space addition. E.g. in $\mathbb{F}_2^4$

  $$0011 + 1010 = 1001.$$

  (In cryptography it is usual to use $\boxplus$ for addition of integers: $0011 \boxplus 1010 = 1101$ is $3 + 10 = 13$.)
- Question 4. Working with DES, so the key length is 56, how many operations are needed to compute all the triples $\big(k, k', d_{k'}(e_k(x))\big)$ for all $k, k' \in \mathbb{F}_2^{56}$?

  (A) 2^{56} (B) 2^{57} (C) 2^{112} (D) other
- Question: how are block ciphers actually implemented?
  Answer: the operations are chosen to be efficient on modern computers that store everything in binary. For instance
  - `int x = 341`

  tells the C compiler to put 341 in a new memory location, and label it `x`. Since $341 = 1 + 4 + 16 + 64 + 256$, this represents $x = \ldots 01010101 \in \mathbb{F}_2^{32}$. To add a key, we use binary XOR:
  - `int y = 341 ^ 15`

  makes $\ldots 01010101 + \ldots 00001111 = \ldots 01011010$.

Attack 9.3

Let $e_k : \mathbb{F}_2^n \to \mathbb{F}_2^n$ for $k \in \mathbb{F}_2^\ell$ be the encryption functions for a block cipher of block size n and key length ℓ. For $(k_{\mathrm{otp}}, k) \in \mathbb{F}_2^n \times \mathbb{F}_2^\ell$ define $E_{(k_{\mathrm{otp}},k)} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ by

$$E_{(k_{\mathrm{otp}},k)}(x) = e_k(x + k_{\mathrm{otp}}).$$

Let $\Delta \in \mathbb{F}_2^n$. In a chosen plaintext attack on this 'composed' cipher, we choose $x \in \mathbb{F}_2^n$ and obtain the ciphertexts

$$\begin{aligned} z &= E_{(k_{\mathrm{otp}},k)}(x) \\ z_\Delta &= E_{(k_{\mathrm{otp}},k)}(x + \Delta) \end{aligned}$$

Set $\Gamma = z + z_\Delta$. Then $e_k^{-1}(z) + e_k^{-1}(z_\Delta) = \Delta$. Moreover, for $k_{\mathrm{guess}} \in \mathbb{F}_2^\ell$, either

$$e_{k_{\mathrm{guess}}}^{-1}(z) + e_{k_{\mathrm{guess}}}^{-1}(z_\Delta) \neq \Delta$$

and we deduce $k_{\mathrm{guess}} \neq k$, or

$$e_{k_{\mathrm{guess}}}^{-1}(z) + e_{k_{\mathrm{guess}}}^{-1}(z_\Delta) = \Delta$$

and $k_{\mathrm{guess}} \in \mathcal{K}_z = \big\{ k_{\mathrm{guess}} \in \mathbb{F}_2^n : e_{k_{\mathrm{guess}}}^{-1}(z) + \mathrm{e}_{k_{\mathrm{guess}}}^{-1}(z + \Gamma) = \Delta \big\}$.

Attack 9.3

Intuitively: for the correct key k, undoing the second cipher we get back the difference Δ; for wrong keys, we get Δ only if k_{guess} has the special property that $k_{\text{guess}} \in \mathcal{K}_z$, where $z = E_{(k_{\text{otp}},k)}(x)$.

If the block cipher is good then $\mathcal{K}_z$ is small. Therefore *false keys*, where we do not immediately see that our guess is wrong, are rare. Note that we do not guess k_{otp}, only k.

Correction: in the printed notes there is a suggested exercise after Attack 9.3. It is incorrect as stated and should be deleted. (Exercise 9.5 is what was meant.)

Example 9.4

Let $n = 8$, $\ell = 8$ and let $P : \mathbb{F}_2^8 \to \mathbb{F}_2^8$ be the pseudo-inverse function. For $k \in \mathbb{F}_2^8$, define $e_k(y) = P(y) + k$. Note that $e_k^{-1}(z) = P(z + k)$ and so

$$e_{k_{\text{guess}}}^{-1}(z) + e_{k_{\text{guess}}}^{-1}(z_\Delta) = P(z + k_{\text{guess}}) + P(z_\Delta + k_{\text{guess}}).$$

By definition $z_\Delta = z + \Gamma$. Hence the set $\mathcal{K}_z$ in Attack 9.3 is

$$\mathcal{K}_z = \{k_{\text{guess}} \in \mathbb{F}_2^8 : P(z + k_{\text{guess}}) + P(z + k_{\text{guess}} + \Gamma) = \Delta\}.$$

Running the attack: Take $\Delta = 1000\,0000$; this corresponds to $1 \in \mathbb{F}_{2^8}$. For each $k_{\text{guess}} \in \mathbb{F}_2^8$, we compute

$$P(z + k_{\text{guess}}) + P(z_\Delta + k_{\text{guess}}).$$

If the answer is Δ then $k_{\text{guess}} \in \mathcal{K}_z$ and k_{guess} is either k or a false key. Otherwise we reject k_{guess}.

By Exercise 9.1, there are usually exactly two different $k_{\text{guess}} \in \mathbb{F}_2^8$ such that $P(z + k_{\text{guess}}) + P(z + k_{\text{guess}} + \Gamma) = \Delta$. One must be k.

Example 9.4 [continued]

In the following examples we take $k_{\mathrm{otp}} = 0000\,0000$.

(1) If $k = 0000\,0000$ and $x = 0100\,0000$ then, since $P(0100\,0000) = 1011\,0001$ and $P(1100\,0000) = 0110\,1111$, $\Gamma = z + z_\Delta = 1101\,1110$. There are exactly 2 keys k_{guess} such that $k \in \mathcal{K}_z$, namely

$$0000\,0000, \; 1101\,1110.$$

For instance, suppose we make the incorrect guess $k_{\mathrm{guess}} = 0000\,0001$. Given that $P(1011\,0000) = 1000\,0111$ and $P(0110\,1110) = 0101\,1101$, what difference do we observe when we run the attack?

(A) $1000\,0111$ (B) $0101\,1101$

(C) $1101\,1010$ (D) $1101\,1000$

Is this consistent with the input difference of $\Delta = 1000\,0000$?

(A) No (B) Yes

Example 9.4 [continued]

In the following examples we take $k_{\mathrm{otp}} = 0000\,0000$.

(1) If $k = 0000\,0000$ and $x = 0100\,0000$ then, since $P(0100\,0000) = 1011\,0001$ and $P(1100\,0000) = 0110\,1111$, $\Gamma = z + z_\Delta = 1101\,1110$. There are exactly 2 keys k_{guess} such that $k \in \mathcal{K}_z$, namely

$$0000\,0000, \;\; 1101\,1110.$$

For instance, suppose we make the incorrect guess $k_{\mathrm{guess}} = 0000\,0001$. Given that $P(1011\,0000) = 1000\,0111$ and $P(0110\,1110) = 0101\,1101$, what difference do we observe when we run the attack?

(A) $1000\,0111$ (B) $0101\,1101$

(C) $1101\,1010$ (D) $1101\,1000$

Is this consistent with the input difference of $\Delta = 1000\,0000$?

(A) No (B) Yes

Example 9.4 [continued]

In the following examples we take $k_{\mathrm{otp}} = 0000\,0000$.

(1) If $k = 0000\,0000$ and $x = 0100\,0000$ then, since $P(0100\,0000) = 1011\,0001$ and $P(1100\,0000) = 0110\,1111$, $\Gamma = z + z_\Delta = 1101\,1110$. There are exactly 2 keys k_{guess} such that $k \in \mathcal{K}_z$, namely

$$0000\,0000, \;\; 1101\,1110.$$

For instance, suppose we make the incorrect guess $k_{\mathrm{guess}} = 0000\,0001$. Given that $P(1011\,0000) = 1000\,0111$ and $P(0110\,1110) = 0101\,1101$, what difference do we observe when we run the attack?

(A) $1000\,0111$ (B) $0101\,1101$

(C) $1101\,1010$ (D) $1101\,1000$

Is this consistent with the input difference of $\Delta = 1000\,0000$?

(A) No (B) Yes

Example 9.4 [continued]

In the following examples we take $k_{\mathrm{otp}} = 0000\,0000$.

(1) If $k = 0000\,0000$ and $x = 0100\,0000$ then, since $P(0100\,0000) = 1011\,0001$ and $P(1100\,0000) = 0110\,1111$, $\Gamma = z + z_\Delta = 1101\,1110$. There are exactly 2 keys k_{guess} such that $k \in \mathcal{K}_z$, namely

$$0000\,0000,\ 1101\,1110.$$

(2) If $k = 0000\,0000$ and $x = 0000\,0000$ then $\Gamma = z + z_\Delta = 1000\,0000$ and there are exactly 4 keys k_{guess} such that $k \in \mathcal{K}_z$, namely

$$0000\,0000,\ 1000\,0000,\ 0011\,1101,\ 1011\,1101.$$

(To check this you need $P(0011\,1101) = 1011\,1101$ and so, since $P(P(x)) = x$ for all $x \in \mathbb{F}_2^8$, $P(1011\,1101) = 0011\,1101$.) This is the exceptional case when $\Delta^{-1} = \Gamma$.

(3) *Exercise:* let $k = 1111\,1111$. What are the possible keys k_{guess} if $x = 0100\,0000$? What if $x = 0000\,0000$? [*Hint:* these can be deduced from (1) and (2) since the difference Γ is same.]

Cost of the Attack

Exercise 9.6

(a) Show that the attack typically finds k and the false key $k + \Gamma$ using at most 2×2^8 decryptions to calculate $e_{k_{\text{guess}}}^{-1}(z)$ and $e_{k_{\text{guess}}}^{-1}(z_\Delta)$.

(b) How many encryptions are needed to test all the pairs (k_{otp}, k) and $(k_{\text{otp}}, k + \Gamma)$ for $k_{\text{otp}} \in \mathbb{F}_2^8$?

(c) Deduce that the attack finds the key (k_{otp}, k) using at most 2^{10} decryptions/encryptions. Why is this sub-exhaustive?

Attack on the Q-Block Cipher: Weak First Round

Recall from Example 8.4 that round i of the Q-block cipher is

$$(v, w) \mapsto \big(w, w + S(v + k^{(i)})\big)$$

where $k^{(i)} \in \mathbb{F}_2^4$ is the round key. There are three rounds:

$$\begin{aligned}(v, w) = (v^{(0)}, v^{(1)}) &\mapsto \big(v^{(1)}, v^{(0)} + S(v^{(1)} + k^{(1)})\big) = (v^{(1)}, v^{(2)}) \\ &\mapsto \big(v^{(2)}, v^{(1)} + S(v^{(2)} + k^{(2)})\big) = (v^{(2)}, v^{(3)}) \\ &\mapsto \big(v^{(3)}, v^{(2)} + S(v^{(3)} + k^{(3)})\big) = (v', w').\end{aligned}$$

Lemma 9.7

(i) *For any $x \in \mathbb{F}_2^4$ we have $S(x + 1000) = S(x) + 0010$.*

(ii) *For any $(v, w) \in \mathbb{F}_2^8$ and any round key $k^{(1)} \in \mathbb{F}_2^4$ we have*

$$\begin{aligned}\big(w, v + S(w + k^{(1)})\big) + \big(w + 1000, v + S(w + 1000 + k^{(1)})\big) \\ = (1000, 0010).\end{aligned}$$

Why Difference Attacks beat Exhaustion

Suppose Alice and Bob have secret numbers $a, b \in \{0, 1, \ldots, 15\}$.

(1) You can ask Alice and Bob together: 'is the pair of your numbers (c, d)'? The two confer (in secret) and you get a single yes/no answer. In the worst case, how many guesses do you need to learn both numbers?

(A) 31 (B) 32 (C) 255 (D) 256

(2) Now you can ask either Alice or Bob 'is your number e'? How many guesses do you need in the worst case to learn both numbers?

(A) 30 (B) 31 (C) 255 (D) 256

Why Difference Attacks beat Exhaustion

Suppose Alice and Bob have secret numbers $a, b \in \{0, 1, \ldots, 15\}$.

(1) You can ask Alice and Bob together: ‘is the pair of your numbers (c, d)’? The two confer (in secret) and you get a single yes/no answer. In the worst case, how many guesses do you need to learn both numbers?

(A) 31   (B) 32   [✓ (C) 255]   (D) 256

(2) Now you can ask either Alice or Bob ‘is your number e’? How many guesses do you need in the worst case to learn both numbers?

(A) 30   (B) 31   (C) 255   (D) 256

Why Difference Attacks beat Exhaustion

Suppose Alice and Bob have secret numbers $a, b \in \{0, 1, \ldots, 15\}$.

(1) You can ask Alice and Bob together: 'is the pair of your numbers (c, d)'? The two confer (in secret) and you get a single yes/no answer. In the worst case, how many guesses do you need to learn both numbers?

(A) 31 (B) 32 (C) 255 (D) 256

(2) Now you can ask either Alice or Bob 'is your number e'? How many guesses do you need in the worst case to learn both numbers?

(A) 30 (B) 31 (C) 255 (D) 256

Attack on the Q-Block Cipher

Example′ 9.8

We run Attack 9.3 on the Q-block cipher by taking $\Delta = (0000, 1000)$ and guessing the final 8 bits of the key k to undo the final two rounds. Take $k = 0001\,0011\,0111$.

$$0000\,0000 \xmapsto{0001} 0000\,0100 \xmapsto{0011,0111} 1110\,0010$$

$$\Delta = 0000\,1000 \qquad \Delta' = 1000\,0010 \qquad \Gamma = 0011\,1110$$

$$0000\,1000 \xmapsto{0001} 1000\,0110 \xmapsto{0011,0111} 1101\,1100$$

Attack on the Q-Block Cipher

Example′ 9.8

We run Attack 9.3 on the Q-block cipher by taking $\Delta = (0000, 1000)$ and guessing the final 8 bits of the key k to undo the final two rounds. Take $k = 0001\,0011\,0111$.

$$0000\,0000 \overset{0001}{\longmapsto} 0000\,0100 \overset{0011,0111}{\longmapsto} 1110\,0010$$

$$\Delta = 0000\,1000 \qquad \Delta' = 1000\,0010 \qquad \Gamma = 0011\,1110$$

$$0000\,1000 \overset{0001}{\longmapsto} 1000\,0110 \overset{0011,0111}{\longmapsto} 1101\,1100$$

(1) For the guess $k^{(2)}_{\text{guess}} = 0011$, $k^{(3)}_{\text{guess}} = 0011$,

$$w = 0101\,0101, \; w_\Delta = 0110\,0101.$$

What is the observed difference between w and w_Δ?

(A) 0101 0101 (B) 0110 0101

(C) 0111 0000 (D) 0011 0000

Does the attack rule out this guess?

(A) No (B) Yes

Attack on the Q-Block Cipher

Example′ 9.8

We run Attack 9.3 on the Q-block cipher by taking $\Delta = (0000, 1000)$ and guessing the final 8 bits of the key k to undo the final two rounds. Take $k = 0001\,0011\,0111$.

$$0000\,0000 \overset{0001}{\longmapsto} 0000\,0100 \overset{0011,0111}{\longmapsto} 1110\,0010$$

$$\Delta = 0000\,1000 \qquad \Delta' = 1000\,0010 \qquad \Gamma = 0011\,1110$$

$$0000\,1000 \overset{0001}{\longmapsto} 1000\,0110 \overset{0011,0111}{\longmapsto} 1101\,1100$$

(1) For the guess $k^{(2)}_{\text{guess}} = 0011$, $k^{(3)}_{\text{guess}} = 0011$,

$$w = 0101\,0101, \; w_\Delta = 0110\,0101.$$

What is the observed difference between w and w_Δ?

(A) 0101 0101 (B) 0110 0101

(C) 0111 0000 [✓ (D) 0011 0000]

Does the attack rule out this guess?

(A) No (B) Yes

Attack on the Q-Block Cipher

Example′ 9.8

We run Attack 9.3 on the Q-block cipher by taking $\Delta = (0000, 1000)$ and guessing the final 8 bits of the key k to undo the final two rounds. Take $k = 0001\,0011\,0111$.

$$0000\,0000 \xmapsto{0001} 0000\,0100 \xmapsto{0011,0111} 1110\,0010$$

$\Delta = 0000\,1000$ $\qquad\Delta' = 1000\,0010$ $\qquad\Gamma = 0011\,1110$

$$0000\,1000 \xmapsto{0001} 1000\,0110 \xmapsto{0011,0111} 1101\,1100$$

(1) For the guess $k^{(2)}_{\text{guess}} = 0011$, $k^{(3)}_{\text{guess}} = 0011$,

$$w = 0101\,0101,\ w_\Delta = 0110\,0101.$$

What is the observed difference between w and w_Δ?

(A) 0101 0101 (B) 0110 0101

(C) 0111 0000 (D) 0011 0000

Does the attack rule out this guess?

(A) No (B) Yes

Attack on the Q-Block Cipher

Example′ 9.8

We run Attack 9.3 on the Q-block cipher by taking $\Delta = (0000, 1000)$ and guessing the final 8 bits of the key k to undo the final two rounds. Take $k = 0001\,0011\,0111$.

$$0000\,0000 \overset{0001}{\longmapsto} 0000\,0100 \overset{0011,0111}{\longmapsto} 1110\,0010$$

$$\Delta = 0000\,1000 \qquad \Delta' = 1000\,0010 \qquad \Gamma = 0011\,1110$$

$$0000\,1000 \overset{0001}{\longmapsto} 1000\,0110 \overset{0011,0111}{\longmapsto} 1101\,1100$$

(2) For the guess $k^{(2)}_{\text{guess}} = 0011$, $k^{(3)}_{\text{guess}} = 1111$,

$$w = 1011\,0110, \;\; w_{\Delta} = 0011\,0100.$$

Does the attack rule out this guess?

(A) No (B) Yes

Attack on the Q-Block Cipher

Example′ 9.8

We run Attack 9.3 on the Q-block cipher by taking $\Delta = (0000, 1000)$ and guessing the final 8 bits of the key k to undo the final two rounds. Take $k = 0001\,0011\,0111$.

$$0000\,0000 \overset{0001}{\longmapsto} 0000\,0100 \overset{0011,0111}{\longmapsto} 1110\,0010$$

$$\Delta = 0000\,1000 \qquad \Delta' = 1000\,0010 \qquad \Gamma = 0011\,1110$$

$$0000\,1000 \overset{0001}{\longmapsto} 1000\,0110 \overset{0011,0111}{\longmapsto} 1101\,1100$$

(2) For the guess $k^{(2)}_{\text{guess}} = 0011$, $k^{(3)}_{\text{guess}} = 1111$,

$$w = 1011\,0110, \;\; w_\Delta = 0011\,0100.$$

Does the attack rule out this guess?

(A) No (B) Yes

Attack on the Q-Block Cipher

Example′ 9.8

We run Attack 9.3 on the Q-block cipher by taking $\Delta = (0000, 1000)$ and guessing the final 8 bits of the key k to undo the final two rounds. Take $k = 0001\,0011\,0111$.

$$0000\,0000 \overset{0001}{\longmapsto} 0000\,0100 \overset{0011,0111}{\longmapsto} 1110\,0010$$

$$\Delta = 0000\,1000 \qquad \Delta' = 1000\,0010 \qquad \Gamma = 0011\,1110$$

$$0000\,1000 \overset{0001}{\longmapsto} 1000\,0110 \overset{0011,0111}{\longmapsto} 1101\,1100$$

(3) For the guess $k^{(2)}_{\text{guess}} = 0011$, $k^{(3)}_{\text{guess}} = 0000$,

$$w = 1100\,1011,\ w_\Delta = 1111\,1011.$$

Does the attack rule out this guess?

(A) No   (B) Yes

Attack on the Q-Block Cipher

Example′ 9.8

We run Attack 9.3 on the Q-block cipher by taking $\Delta = (0000, 1000)$ and guessing the final 8 bits of the key k to undo the final two rounds. Take $k = 0001\,0011\,0111$.

$$0000\,0000 \xmapsto{0001} 0000\,0100 \xmapsto{0011,0111} 1110\,0010$$

$$\Delta = 0000\,1000 \qquad \Delta' = 1000\,0010 \qquad \Gamma = 0011\,1110$$

$$0000\,1000 \xmapsto{0001} 1000\,0110 \xmapsto{0011,0111} 1101\,1100$$

(3) For the guess $k^{(2)}_{\text{guess}} = 0011$, $k^{(3)}_{\text{guess}} = 0000$,

$$w = 1100\,1011, \; w_\Delta = 1111\,1011.$$

Does the attack rule out this guess?

(A) No (B) Yes

Attack on the Q-Block Cipher

Example′ 9.8

We run Attack 9.3 on the Q-block cipher by taking $\Delta = (0000, 1000)$ and guessing the final 8 bits of the key k to undo the final two rounds. Take $k = 0001\,0011\,0111$.

$$0000\,0000 \overset{0001}{\longmapsto} 0000\,0100 \overset{0011,0111}{\longmapsto} 1110\,0010$$

$$\Delta = 0000\,1000 \qquad \Delta' = 1000\,0010 \qquad \Gamma = 0011\,1110$$

$$0000\,1000 \overset{0001}{\longmapsto} 1000\,0110 \overset{0011,0111}{\longmapsto} 1101\,1100$$

The 16 keys $k^{(2)}_{\text{guess}} k^{(3)}_{\text{guess}} \in \mathbb{F}_2^8$ in $\mathcal{K}_z$ are all binary words of the form $\star\star\star 1 \star 1 bb$. Trying each guess together with all 16 possibilities for $k^{(1)}_{\text{guess}} \in F_2^4$ shows that

$$k \in \left\{ \begin{matrix} 0001\,0011\,0111, & 0010\,1111\,0100 \\ 1001\,0001\,1111, & 1010\,1101\,1100 \end{matrix} \right\}.$$

All these keys encrypt $0000\,0000$ to 11100010, so cannot be distinguished without choosing another plaintext.

Attack on a 5-round Q-block cipher

By definition, round i of the Q-block cipher is

$$(v, w) \mapsto \big(w, v + S(v + k^{(i)})\big)$$

By taking a key of length $4r$ we can define the Q-block cipher for any number of rounds. With 5 rounds there is a 20 bit key

$$k = (k^{(1)}, k^{(2)}, k^{(3)}, k^{(4)}, k^{(5)})$$

After 1 round the difference $\Delta = 0000\,1000$ always goes to $\Delta' = 0001\,0010$. By Question 1 on Problem Sheet 8, after 2 rounds there are four possibilities:

$$0010\,0000, \quad 0010\,0001, \quad 0010\,0010, \quad 0010\,0011.$$

Guessing the 12 bit key $(k^{(3)}, k^{(4)}, k^{(5)})$ we rule out k_{guess} if

$e^{-1}_{k_{\text{guess}}}(z) + e^{-1}_{k_{\text{guess}}}(z_\Delta) \not\in \{0010\,0000, 0010\,0001, 0010\,0010, 0010\,001\}$.

After 2^{12} guesses there are $64 = 2^6$ possible keys k_{guess}. Trying each of these with the $256 = 2^8$ possibilities for $(k^{(1)}, k^{(2)})$ gives 64 possibilities for k. The total work is $2^{12} + 2^6 \times 2^8 = 2^{12} + 2^{14}$. This is about $64 = 2^6$ times faster than guessing all of k in one go.

Correction to Problem Sheet 8: Q1(d)

- Let $\Gamma = 0000\,0010$. [**Not** $0000\,1000$]. Let $(v, w) \in \mathbb{F}_2^8$ be chosen uniformly at random. Let (v', w') and (v'_Γ, w'_Γ) be the encryptions of (v, w) and $(v, w) + \Gamma$, respectively. Show that no matter what the key is, $(v', w') + (v'_\Gamma, w'_\Gamma)$ is equally likely to be each of the four differences

$$\{0010\,1000, 0010\,1001, 0010\,1010, 0010\,1011\}.$$

[**Corrected: first bit in second block was wrongly** 0.]

§10 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 10.1

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 mod p. Bob sends Alice 2^b mod p.

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

(4) Now Alice and Bob both know 2^{ab} mod p. They each write 2^{ab} mod 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 10.2

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 10.2

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 10.2

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 $\{1, \dots, p-1\}$ 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 mod 131	1	2	4	8	16	32	64	128	125	119	...

If $2^m = y$ mod 131 where $0 \le m \le 129$ then we say that m is the *discrete log* of y (with respect to 2), working modulo 131. For example $2^{46} \equiv 5$ mod 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 mod 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 mod 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 mod 131	1	2	4	8	16	32	64	128	125	119	...

If $2^m = y$ mod 131 where $0 \le m \le 129$ then we say that m is the *discrete log* of y (with respect to 2), working modulo 131. For example $2^{46} \equiv 5$ mod 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 mod 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,

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

Please complete the online course questionnaire. You should have been emailed a link. The response rate is 9% for 362 at the moment.

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 $\mathsf{P} \neq \mathsf{NP}$: very roughly, if $\mathsf{P} = \mathsf{NP}$ 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.

Exercise 10.3

Why do we exclude $p-1$ from the domain of f?

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 10.4

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 10.4, 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 10.5

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 10.6

Let $p = 11$, $q = 17$, so $n = pq = 187$ and $(p-1)(q-1) = 160$. Let $a = 9$. Adapting the proof for Lemma 10.4, 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 10.5. But it is believed to be hard to find r given only a and n. This makes $x \mapsto x^a$ mod n suitable for use in a cryptosystem.

RSA Cryptosystem

Let $n = pq$ be the product of distinct primes p and q. In the RSA Cryptosystem, with *RSA modulus* n,

$$\mathcal{P} = \mathcal{C} = \{0, 1, \ldots, n-1\}$$

and

$$\mathcal{K} = \bigl\{(p, q, c) : c \in \{1, \ldots, n-1\}, \mathrm{hcf}\bigl(c, (p-1)(q-1)\bigr) = 1\bigr\}.$$

The *public key* corresponding to (p, q, c) is (n, c) and the *private key* corresponding to (p, q, c) is (n, r), where $cr \equiv 1 \bmod (p-1)(q-1)$. The encryption function for (p, q, c) is

$$x \mapsto x^c \text{ mod } n$$

and the decryption function is

$$y \mapsto y^r \text{ mod } n.$$

Note that anyone knowing the public key can encrypt, but only someone knowing the private key (or the entire key (p, q, c)) 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 mod 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 mod 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 mod 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 mod 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 mod 221 as?

  (A) 2 (B) 35 (C) 223 (D) 256

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 10.7

(1) For a small example, take p and q as in Example 10.6. If Alice's public key is $(9, 187)$ then her private key is $(89, 187)$. If Bob's plaintext is 10 then he sends 109 to Alice, since $10^9 \equiv 109 \bmod 187$. Alice decrypts to 10 by computing 109^{89} mod 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 cell 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 $g^a \bmod p$.

(A) False (B) True

(b) Given g and $g^a \bmod p$, with a known to be in $\{1, \ldots, p-2\}$, it is fast to compute a.

(A) False (B) True

(c) The function $\{1, \ldots, p-1\} \rightarrow \{1, \ldots, p-1\}$ defined by $x \mapsto x^2$ is invertible.

(A) False (B) True

(d) If $\mathrm{hcf}(a, p-1) = 1$ then the function $\{1, \ldots, p-1\} \rightarrow \{1, \ldots, p-1\}$ defined by $x \mapsto x^a \bmod p$ 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 $\{1, \ldots, n-1\} \rightarrow \{1, \ldots, n-1\}$ defined by $x \mapsto x^a \bmod n$ is invertible.

(A) False (B) True

(f) Suppose $x \mapsto x^a \bmod n$ 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 $g^a \bmod p$.

(A) False [✓ (B) True]

(b) Given g and $g^a \bmod p$, 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 $x \mapsto x^a \bmod p$ 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 $x \mapsto x^a \bmod n$ is invertible.

(A) False (B) True

(f) Suppose $x \mapsto x^a \bmod n$ 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 $g^a \bmod p$.

(A) False (B) True

(b) Given g and $g^a \bmod p$, 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 $x \mapsto x^a \bmod p$ is invertible, and it is fast to compute its inverse.

(A) False (B) True

(e) If $\mathrm{hcf}\bigl(a, (p-1)(q-1)\bigr) = 1$ then the function $\{1, \ldots, n-1\} \to \{1, \ldots, n-1\}$ defined by $x \mapsto x^a \bmod n$ is invertible.

(A) False (B) True

(f) Suppose $x \mapsto x^a \bmod n$ 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 $g^a \bmod p$.

(A) False [✓ (B) True]

(b) Given g and $g^a \bmod p$, 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 $x \mapsto x^a \bmod p$ 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 $x \mapsto x^a \bmod n$ is invertible.

(A) False [✓ (B) True]

(f) Suppose $x \mapsto x^a \bmod n$ 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

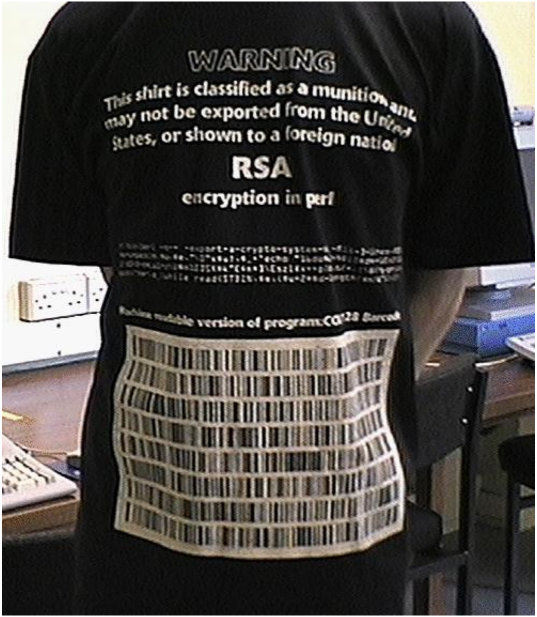
(e) If $\mathrm{hcf}\big(a, (p-1)(q-1)\big) = 1$ then the function $\{1, \ldots, n-1\} \to \{1, \ldots, n-1\}$ defined by $x \mapsto x^a$ mod n is invertible.

(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


WARNING
This shirt is classified as a munition and
may not be exported from the United
States, or shown to a foreign nation
RSA
encryption in perl
Machine readable version of program: CODE128 Barcode

§11 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 Bob wants to tell Alice his bank details in a message x. He looks up her public key (a, m) and sends her $x^a \bmod m$.

Malcolm cannot decrypt $x^a \bmod m$, because he does not know r. But if he has control of the channel, he can replace $x^a \bmod m$ with another $x'^a \bmod m$, of his choice.

§11 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 Bob wants to tell Alice his bank details in a message x. He looks up her public key (a, m) and sends her $x^a \bmod m$.

Malcolm cannot decrypt $x^a \bmod m$, because he does not know r. But if he has control of the channel, he can replace $x^a \bmod m$ with another $x'^a \bmod m$, of his choice.

This requires Malcolm to know Alice'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 Alice be confident that a message signed 'Bob' is from Bob, and not from Malcolm pretending to Bob?

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 11.1

Alice is expecting a message from Bob. She receives z, and computes $d_a(z) = z^r \bmod m$, but gets garbage. Thinking that Bob has somehow confused the keys, she computes $z^b \bmod n$, and gets the ASCII encoding of

'Bob here, my account number is 40081234'.

(a) Should Alice believe z was sent by Bob?

(A) No (B) Yes

(b) How did Bob compute z?

(c) Can Malcolm read Bob's message?

(A) No (B) Yes

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 11.1

Alice is expecting a message from Bob. She receives z, and computes $d_a(z) = z^r \bmod m$, but gets garbage. Thinking that Bob has somehow confused the keys, she computes $z^b \bmod n$, and gets the ASCII encoding of

'Bob here, my account number is 40081234'.

(a) Should Alice believe z was sent by Bob?

(A) No [✓ (B) Yes]

(b) How did Bob compute z?

(c) Can Malcolm read Bob's message?

(A) No (B) Yes

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 11.1

Alice is expecting a message from Bob. She receives z, and computes $d_a(z) = z^r \bmod m$, but gets garbage. Thinking that Bob has somehow confused the keys, she computes $z^b \bmod n$, and gets the ASCII encoding of

'Bob here, my account number is 40081234'.

(a) Should Alice believe z was sent by Bob?

(A) No (B) Yes

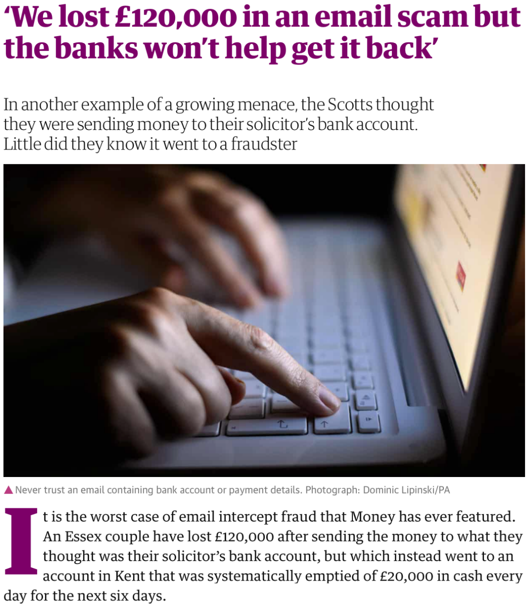
(b) How did Bob compute z?

(c) Can Malcolm read Bob's message?

(A) No (B) Yes

(d) How can Bob avoid the problem in (c)?

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 Bob's message. If Bob's RSA number n 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 $2048/8 = 2^{11-3} = 2^8 = 256$ characters can be sent.

Bob can get round this by splitting the message into blocks, but computing $d_b(x^{(i)})$ for each block $x^{(i)} \in \{1, \ldots, n-1\}$ is slow. It is better to send x, and then append $d_b(h(x))$ where $h(x) \in \{0, \ldots, n-1\}$ is a hash of x.

Hash Functions

Definition 11.2

(i) A *hash function* of length m is a function $h : \mathbb{N}_0 \to \mathbb{F}_2^m$. The value $h(x)$ is the *hash* of the message $x \in \mathbb{N}_0$.

(ii) Let (n, b) be Bob's public key in the RSA cryptosystem. The pair $\bigl(x, d_b(h(x))\bigr)$ is a *signed message* from Bob.

Alice *verifies* that a pair (x, s) is a valid signed message from Bob by checking that $h(x) = e_b(s)$.

Hash Functions

Definition 11.2

(i) A *hash function* of length m is a function $h : \mathbb{N}_0 \to \mathbb{F}_2^m$. The value $h(x)$ is the *hash* of the message $x \in \mathbb{N}_0$.

(ii) Let (n, b) be Bob's public key in the RSA cryptosystem. The pair $\bigl(x, d_b(h(x))\bigr)$ is a *signed message* from Bob.

Alice *verifies* that a pair (x, s) is a valid signed message from Bob by checking that $h(x) = e_b(s)$.

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.*)

Birthday Paradox

Exercise 11.3

Let $h : \mathbb{N} \to \mathbb{F}_2^m$ be a good hash function. On average, how many hashes does an attacker need to calculate to find a pair (x, x') with $h(x) = h(x')$?

Assume hash values are distributed uniformly at random in $\mathbb{F}_2^m$.

- 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, $x^{(1)}, \dots, x^{(R)}$. 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 11.3

Let $h : \mathbb{N} \to \mathbb{F}_2^m$ be a good hash function. On average, how many hashes does an attacker need to calculate to find a pair (x, x') with $h(x) = h(x')$?

Assume hash values are distributed uniformly at random in $\mathbb{F}_2^m$.

- 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 11.3

Let $h : \mathbb{N} \to \mathbb{F}_2^m$ be a good hash function. On average, how many hashes does an attacker need to calculate to find a pair (x, x') with $h(x) = h(x')$?

Assume hash values are distributed uniformly at random in $\mathbb{F}_2^m$.

- 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 11.3

Let $h : \mathbb{N} \to \mathbb{F}_2^m$ be a good hash function. On average, how many hashes does an attacker need to calculate to find a pair (x, x') with $h(x) = h(x')$?

Assume hash values are distributed uniformly at random in $\mathbb{F}_2^m$.

- 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, $x^{(1)}, \dots, x^{(R)}$. 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 11.4

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.

Hash Functions In Practice

A block cipher of length m can be used as a hash function. Chop the message x (this might be already encrypted) into blocks $x^{(1)}, x^{(2)}, \ldots, x^{(t)}$, such that each $x^{(i)} < 2^m$. Let $b^{(i)} \in \mathbb{F}_2^m$ be the binary form of $x^{(i)}$. Then apply the block cipher in cipher block chaining mode (see page 41), to get

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

- Should the chosen key k be secret?

(A) No (B) Yes

Hash Functions In Practice

A block cipher of length m can be used as a hash function. Chop the message x (this might be already encrypted) into blocks $x^{(1)}, x^{(2)}, \ldots, x^{(t)}$, such that each $x^{(i)} < 2^m$. Let $b^{(i)} \in \mathbb{F}_2^m$ be the binary form of $x^{(i)}$. Then apply the block cipher in cipher block chaining mode (see page 41), to get

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

- Should the chosen key k be secret?

  (A) No (B) Yes

  If Alice receives (x, t), where t is the claimed hash, then Alice needs to know k so that she can repeat the calculation above and verify that the hash of x is t.

SHA-256

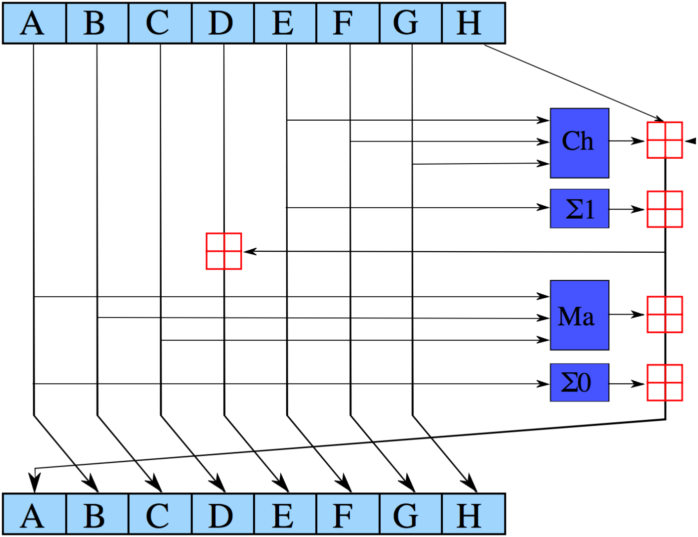
Example 11.5 (SHA-256)

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) when the number of rounds is reduced to 46.

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 11.6

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 11.7 (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 $\bigl(x', d_a(h(x'))\bigr)$ where x' says 'I Alice give Charlie the bitcoin b'.

To avoid this, transactions are *validated*. To validate a list of transactions

$$\bigl(b^{(1)}, x^{(1)}, d_{a^{(1)}}(h(x^{(1)}))\bigr), \bigl(b^{(2)}, x^{(2)}, d_{a^{(2)}}(h(x^{(2)}))\bigr), \ldots$$

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 11.7 [continued]

When Bob receives $\bigl(b, x', d_a(h(x'))\bigr)$, 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.

Last night the bitcoin traded at \$3245.00; last year in December it was at a near record high of \$15879.79. 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.