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 onwards, and eventually to the back, even if you the person you are passing to already has a copy.**
- Please take a clicker and use it!
- All handouts will be put on Moodle. The first marked problem sheet will be on Moodle by Wednesday.
- **Lectures:** Monday 4pm (MFLEC), Friday 11am (MC201), Friday 4pm (MC336).
- **Extra lecture for MT5462:** Friday 9am (MC201).
- **Office hours in McCrea 240:** Tuesday 3.30pm, Wednesday 10am, Thursday 11am.

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

§1 Introduction: Security Requirements

- **Confidentiality**: Eve cannot read the message.
- **Data integrity**: any change made by Eve 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 Requirements

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

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

(A) False (B) True

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

§1 Introduction: Security Requirements

- **Confidentiality**: Eve cannot read the message.
- **Data integrity**: any change made by Eve 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
- The Equifax share price
- Satoshi Nakamoto
- Edward Snowden?

§2 Alphabet 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) Malcolm (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 `XKIX`. What can she conclude?

Substitution Ciphers

Example 2.3

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

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

then $e_\pi(\mathrm{hello\ there}) = \mathrm{SVOOL\ GSVIV}$. (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.

Frequency Analysis

Example′ 2.4

(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 in Lecture 2, using the MATHEMATICA notebook `AlphabeticCiphers` on Moodle to do the donkey work.

Frequency Analysis

Example′ 2.4

(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 in Lecture 2, 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′ 2.4

(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 in Lecture 2, using the MATHEMATICA notebook `AlphabeticCiphers` on Moodle to do the donkey work.

Exercise′ 2.5

(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?

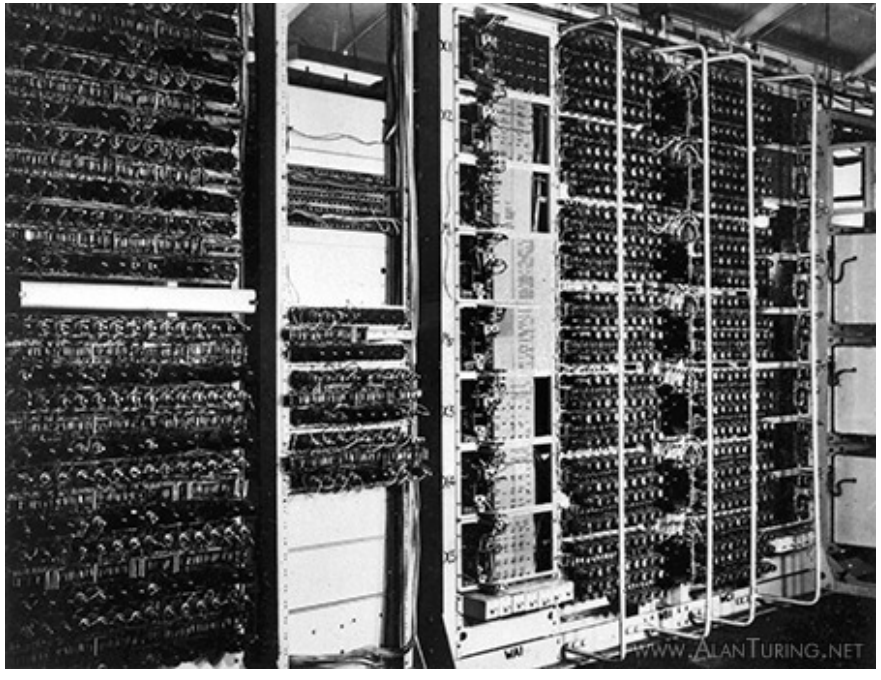
In Praise of Programming

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



Vigenère Cipher

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

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

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

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

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

Vigenère Cipher

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

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

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

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

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

Quiz. 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 $x \mapsto x + s \bmod 26$.

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 2.6

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 2.7

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

A Weakness in the Vigenère Cipher

Exercise 2.8

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

`QXNURA` , `QMUUFM` , `QNRFLX`.

These come from taking every 2nd, 3rd and 4th position in the ciphertext `QQYXMNQU`..., starting at the second `Q`, supposing the plaintext continues '... near the tree'.

(b) Why should we expect the split ciphertext to have the most spiky frequency distribution at the length of the key?

Index of Coincidence

Definition 2.9

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 2.10

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

Index of Coincidence

Definition 2.9

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 2.10

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

There is a simple formula for $I(y)$. (An examinable proof: there are notes on Moodle revising discrete probability.)

Lemma 2.11

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 2.12

Given a Vigenère ciphertext, split it into groups by taking every ℓ-th letter for all small ℓ, as in Exercise 2.8. 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 2.13

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.

Question 3 on Problem Sheet 1

(3) In a *chosen plaintext attack*, the attacker chooses a plaintext x, and is given the corresponding ciphertext $e_k(x)$ for the key k. Explain how to recover the key by a chosen plaintext account when the cipher is

(a) a substitution cipher e_π;

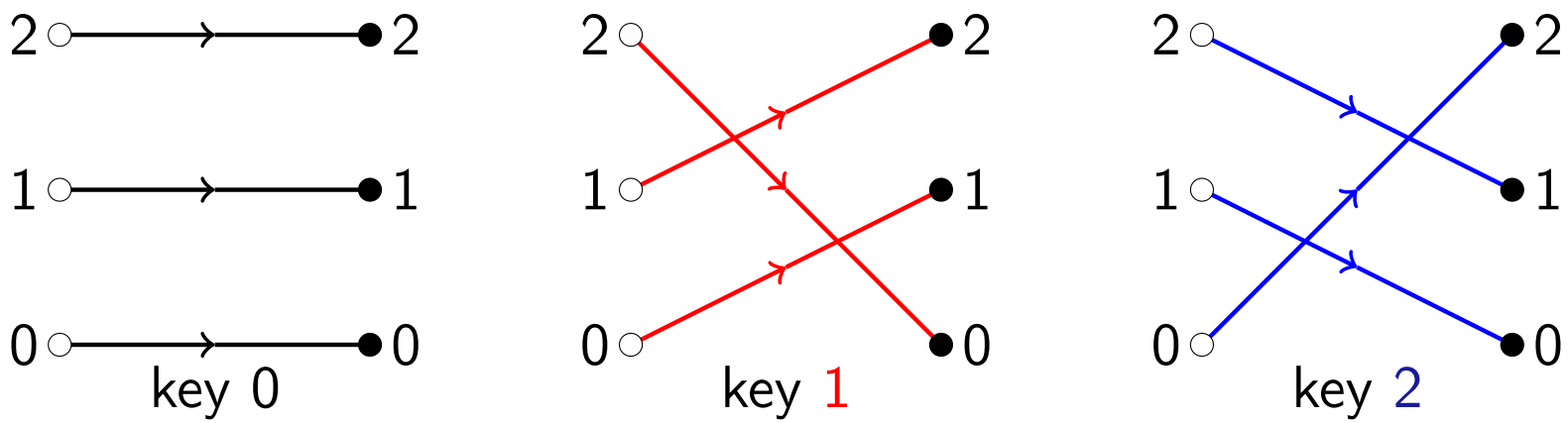
(b) the Vigenère cipher e_k where k has length at most 10.

Administration

- Please take next page of handout
- **Please do the preliminary problem sheet.** We need conditional probability on Friday! Answers will be posted to Moodle this evening.
- **You must do Problem Sheet 1.** Everything relevant has been covered in lectures. Spare copies at front.
  - Deadline: noon Wednesday week: or hand in on Monday.
- **Office hours in McCrea 240:** Tuesday 3.30pm, Wednesday 10am, Thursday 11am.
- Session Id: 131312 (or use a physical clicker)

§3 Cryptosystems, Attack Models and Perfect Secrecy

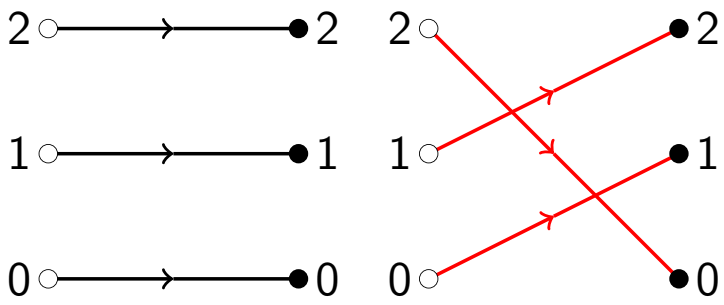
The three different encryption functions for the Caesar cipher on the 'alphabet' $\{0, 1, 2\}$ are shown in the diagram below.



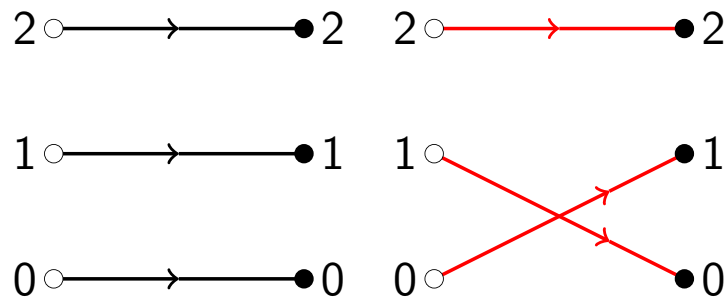
Exercise 3.1: Which are Plausible Cryptosystems?

Please vote A for 'Good', B for 'Bad'

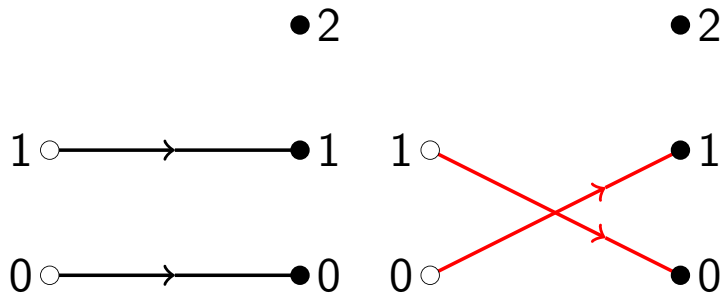
(i)



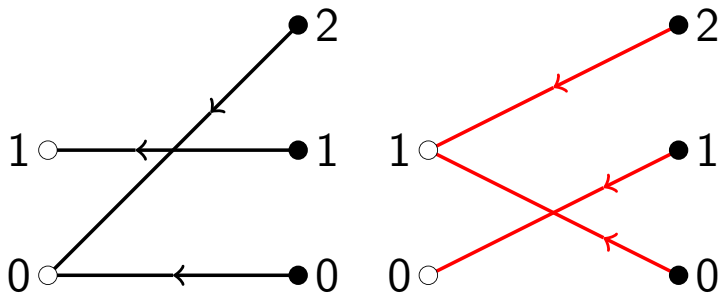
(ii)



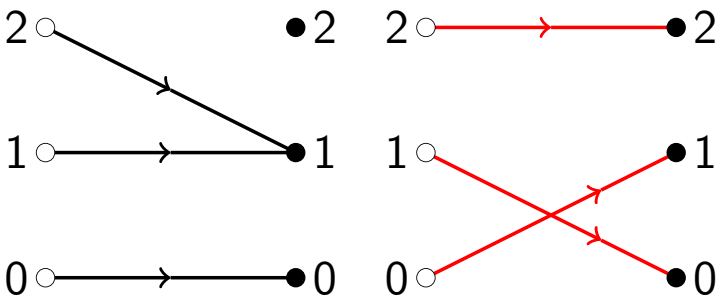
(iii)



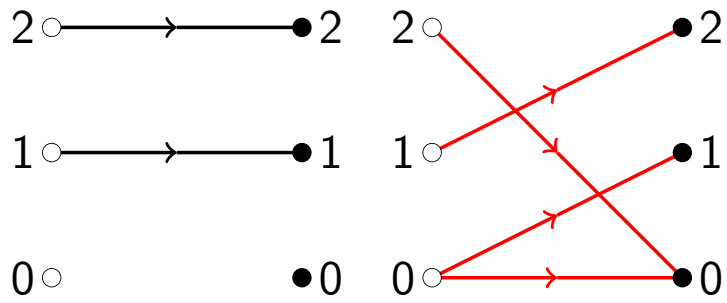
(iv)



(v)



(vi)



Definition of Cryptosystem

Definition 3.2

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

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

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

Definition of Cryptosystem

Definition 3.2

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

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

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 3.3

(a) What is special about ciphertext 2 in (iii)?

(b) Define e_k and $e_{k'}$ so that (iv) becomes a cryptosystem. How many choices did you have? Should (iv) be allowed as the definition of a cryptosystem?

(c) What is the problem with (v)?

(d) What are the two problems with (vi)?

Cryptosystems

Exercise 3.4

Prove that the encryption functions in a cryptosystem are injective and that the decryption functions are surjective.

Cryptosystems

Exercise 3.4

Prove that the encryption functions in a cryptosystem are injective and that the decryption functions are surjective.

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 $f(x) = y$.

Cryptosystems

Exercise 3.4

Prove that the encryption functions in a cryptosystem are injective and that the decryption functions are surjective.

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

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

- the encryption functions determine the decryption functions.
  (A) False (B) True
- 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

Exercise 3.4

Prove that the encryption functions in a cryptosystem are injective and that the decryption functions are surjective.

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

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

- the encryption functions determine the decryption functions.
  (A) False (B) True
- 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

Exercise 3.4

Prove that the encryption functions in a cryptosystem are injective and that the decryption functions are surjective.

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

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

- the encryption functions determine the decryption functions.
  (A) False (B) True
- 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

Exercise 3.4

Prove that the encryption functions in a cryptosystem are injective and that the decryption functions are surjective.

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

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

- the encryption functions determine the decryption functions.
  (A) False (B) True
- 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 3.5

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 3.6

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 Malcolm 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 Malcolm) is to determine k.

- *Known ciphertext*. Eve knows $e_k(x) \in \mathcal{C}$.
- *Known plaintext and ciphertext*. Malcolm knows $x \in \mathcal{P}$ and $e_k(x) \in \mathcal{C}$.
- *Chosen plaintext*. Malcolm may choose any $x \in \mathcal{P}$ and is given the encryption $y = e_k(x)$.
- *Chosen ciphertext*. Malcolm may choose any $y \in \mathcal{C}$ and is given the decryption $x = d_k(y)$.

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 Malcolm) is to determine k.

- *Known ciphertext*. Eve knows $e_k(x) \in \mathcal{C}$.
- *Known plaintext and ciphertext*. Malcolm knows $x \in \mathcal{P}$ and $e_k(x) \in \mathcal{C}$.
- *Chosen plaintext*. Malcolm may choose any $x \in \mathcal{P}$ and is given the encryption $y = e_k(x)$.
- *Chosen ciphertext*. Malcolm 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

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 Malcolm) is to determine k.

- *Known ciphertext*. Eve knows $e_k(x) \in \mathcal{C}$.
- *Known plaintext and ciphertext*. Malcolm knows $x \in \mathcal{P}$ and $e_k(x) \in \mathcal{C}$.
- *Chosen plaintext*. Malcolm may choose any $x \in \mathcal{P}$ and is given the encryption $y = e_k(x)$.
- *Chosen ciphertext*. Malcolm 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.

Remark 3.7

(1) *All the cryptosystems we have seen so far are broken by a chosen plaintext attack. The affine cipher requires two choices and by Question 3 on Sheet 1, the substitution cipher and the Vigenère cipher just one.*

Probability and Perfect Secrecy

Fix a cryptosystem. Suppose that the plaintext $x \in \mathcal{P}$ is sent with probability p_x. Let X, Y and K be the random variables for the plaintext, ciphertext and key, respectively.

Assumption 3.8

The plaintext X and the key K are independent.

Example 3.9

Suppose the keys are chosen with equal probability.

(a) In Exercise 3.1(i),

$$\mathbb{P}[Y = 1] = \frac{p_0 + p_1}{2}, \quad \mathbb{P}[X = 0 | Y = 1] = \frac{p_0}{p_0 + p_1}.$$

In general $\mathbb{P}[X = 0 | Y = 1] \neq p_0$. (For instance take $p_0 = p_1 = p_2 = \frac{1}{3}$) so an Eve intercepting ciphertext 1 learns something about the plaintext.

(b) In the Caesar cipher on $\{0, 1, 2\}$, shown before Exercise 3.1 we have $\mathbb{P}[X = x | Y = y] = p_x$ for all $x, y \in \{0, 1, 2\}$. Knowing the ciphertext tells Eve nothing about the plaintext.

Conditional Probability

Earlier we used the formula for conditional probability:

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

Conditional Probability

Earlier we used the formula for conditional probability:

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

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

Conditional Probability

Earlier we used the formula for conditional probability:

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

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

Perfect secrecy

Definition 3.10

A cryptosystem has *perfect secrecy* 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 $\mathbb{P}[Y = y] > 0$.

By Example 3.9(b), 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 Example 3.9(a), which does not have perfect secrecy.

Perfect secrecy

Definition 3.10

A cryptosystem has *perfect secrecy* 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 $\mathbb{P}[Y = y] > 0$.

By Example 3.9(b), 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 Example 3.9(a), which does not have perfect secrecy.

Quiz. True or false:

(1) 'if and only if' is the pretentious way mathematicians say 'if'.

(A) False (B) True

(2) 'P if and only if Q' can be written as '$P \iff Q$'.

(A) False (B) True

(2) '$P \iff Q$' is the same as $P \implies Q$ *and* $Q \implies P$.

(A) False (B) True

Perfect secrecy

Definition 3.10

A cryptosystem has *perfect secrecy* 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 $\mathbb{P}[Y = y] > 0$.

By Example 3.9(b), 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 Example 3.9(a), which does not have perfect secrecy.

Quiz. True or false:

(1) 'if and only if' is the pretentious way mathematicians say 'if'.

(A) False (B) True

(2) 'P if and only if Q' can be written as '$P \iff Q$'.

(A) False (B) True

(2) '$P \iff Q$' is the same as $P \implies Q$ *and* $Q \implies P$.

(A) False (B) True

Perfect secrecy

Definition 3.10

A cryptosystem has *perfect secrecy* 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 $\mathbb{P}[Y = y] > 0$.

By Example 3.9(b), 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 Example 3.9(a), which does not have perfect secrecy.

Quiz. True or false:

(1) 'if and only if' is the pretentious way mathematicians say 'if'.

(A) False (B) True

(2) 'P if and only if Q' can be written as '$P \iff Q$'.

(A) False (B) True

(2) '$P \iff Q$' is the same as $P \implies Q$ *and* $Q \implies P$.

(A) False (B) True

Perfect secrecy

Definition 3.10

A cryptosystem has *perfect secrecy* 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 $\mathbb{P}[Y = y] > 0$.

By Example 3.9(b), 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 Example 3.9(a), which does not have perfect secrecy.

Quiz. True or false:

(1) 'if and only if' is the pretentious way mathematicians say 'if'.

(A) False (B) True

(2) 'P if and only if Q' can be written as '$P \iff Q$'.

(A) False (B) True

(2) '$P \iff Q$' is the same as $P \implies Q$ *and* $Q \implies P$.

(A) False (B) True

Shannon's Theorem

Lemma 3.11

A cryptosystem has perfect secrecy if and only if

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

for all plaintexts $x \in \mathcal{P}$ such that $p_x > 0$ and all ciphertexts $y \in \mathcal{C}$.

Theorem 3.12 (Shannon 1949)

Suppose a cryptosystem (in our usual notation) has perfect secrecy and that $\mathbb{P}[Y = y] > 0$ for all $y \in \mathcal{C}$.

(a) *For each $x \in \mathcal{P}$ such that $p_x > 0$ and each $y \in \mathcal{C}$ there is a key k such that $e_k(x) = y$.*

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

(c) *Suppose $|\mathcal{K}| = |\mathcal{C}|$. For all $x \in \mathcal{P}$ such that $p_x > 0$ and all $y \in \mathcal{C}$ there exists a unique key $k \in \mathcal{K}$ such that $e_k(x) = y$. Moreover for each fixed $y \in \mathcal{C}$, the keys k such that $e_k(x) = y$ for some $x \in \mathcal{P}$ with $p_x > 0$ are used with equal probability.*

Corollary of Shannon's Theorem

Corollary 3.13

Suppose a cryptosystem (in our usual notation) has perfect secrecy and that

(i) $\mathbb{P}[Y = y] > 0$ *for all* $y \in \mathcal{C}$;

(ii) $|\mathcal{K}| = |\mathcal{C}|$;

(iii) $p_x > 0$ *for all* $x \in \mathcal{P}$.

Then for all $x \in \mathcal{P}$ *and* $y \in \mathcal{C}$ *there exists a unique key* $k \in \mathcal{K}$ *such that* $e_k(x) = y$. *Moreover each key is used with equal probability.*

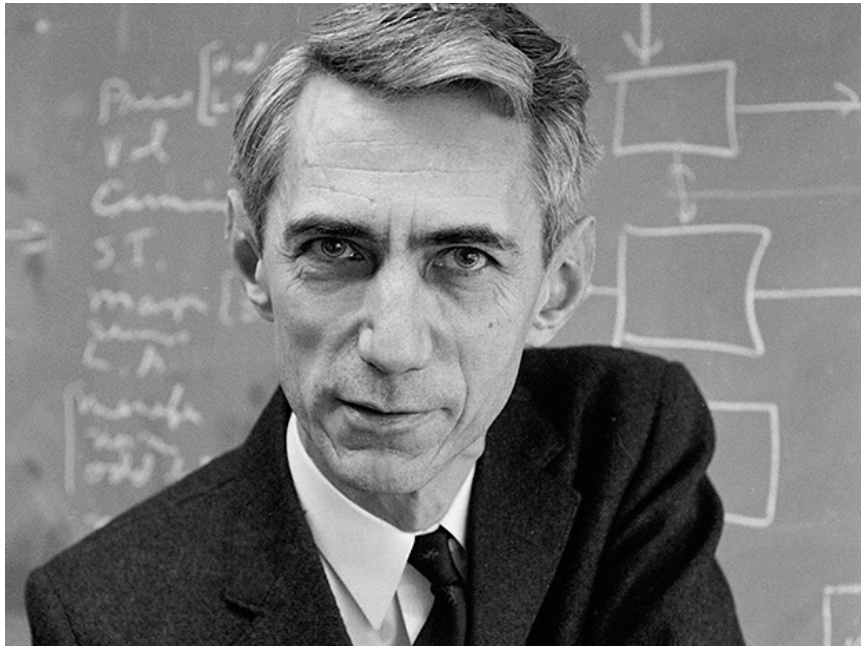
§4 Entropy and Key Uncertainty

The entropy of a random variable is a measure of how uncertain it is. The right mathematical way to capture this notion was discovered by Shannon.

Definition 4.1

The *entropy* $H(X)$ of a random variable X taking values in a finite set $\mathcal{R}$ is

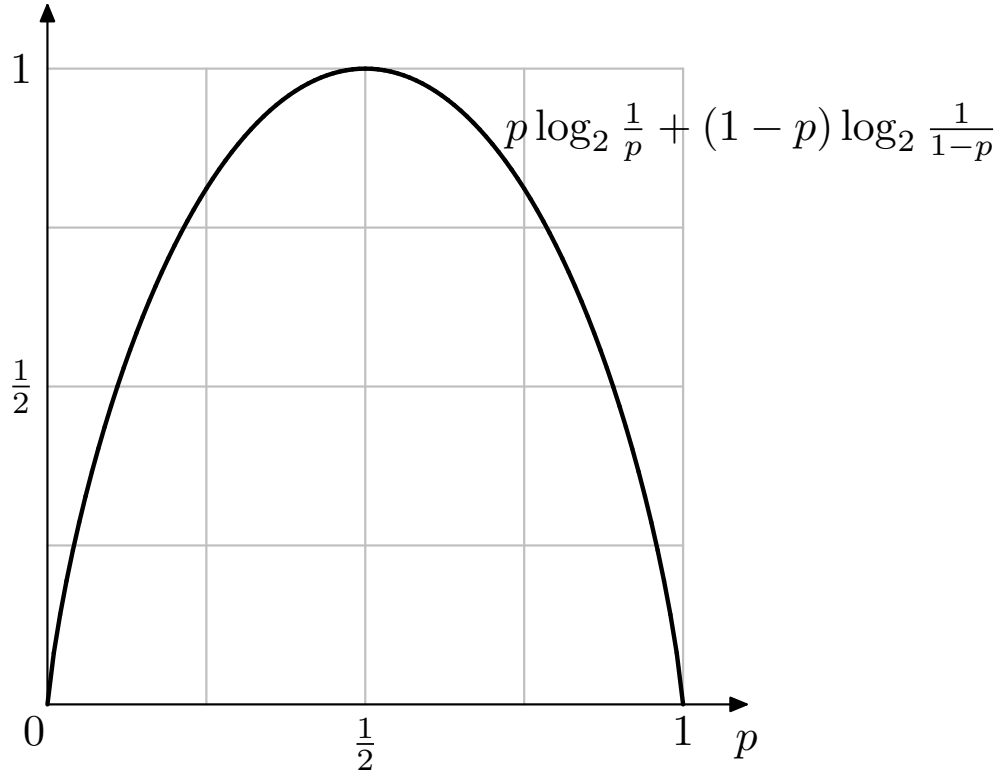
$$H(X) = \sum_{x \in \mathcal{R}} \mathbb{P}[X = x] \log_2 \frac{1}{\mathbb{P}[X = x]}.$$



Entropy Examples

Example 4.2

(1) Suppose X records a single coin flip of a coin, biased to land heads with probability p. Then $H(X) = p \log_2 \frac{1}{p} + (1-p) \log_2 \frac{1}{1-p}$, as shown in the graph below.



Corrections to Problem Sheet 2

- Q4(b): Is there a cryptosystem with perfect secrecy such that $|\mathcal{K}| < |\mathcal{C}|$? [Here $<$ was misprinted as $\leq$.]
- Q8(a): Deduce from Gibbs' inequality that $H(X|Y) \leq H(X)$ .... [Here $H(X)$ was misprinted as $H(Y)$.]

Session Id: 265863.

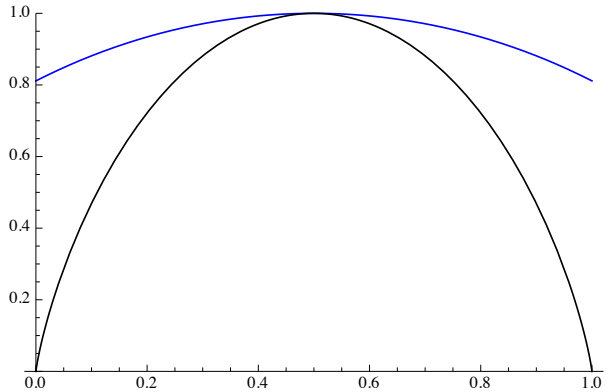
Example 4.2 [continued]

(2) Suppose a cryptographic key K is equally likely to be any element of the keyspace $\mathcal{K}$. If $|\mathcal{K}| = n$ then $H(K) = \log_2 n$.

(3′) Consider the cryptosystem in Exercise 3.1(iii). Suppose that $\mathbb{P}[X = 0] = p$, and so $\mathbb{P}[X = 1] = 1 - p$, and so by (1)

$$H(X) = p \log_2 \frac{1}{p} + (1 - p) \log_2 \frac{1}{1 - p}.$$

Suppose the keys are used with probabilities r (red) and $1 - r$ (black). *Exercise:* find $\mathbb{P}[Y = 0]$ and $\mathbb{P}[Y = 1]$. If $r = \frac{1}{2}$ then $H(Y) = 1$; if $r = 0$ or $r = 1$ then $H(Y) = H(X)$: there is no 'extra' uncertainity from the key. If $r = 1/4$ get (varying p):



blue: $H(Y)$
black: $H(X)$

Example 4.2 [continued]

(4) Consider the affine cipher on $\mathbb{Z}_5$, as in Exercise 3.6. The keys are all (a, c) with $a \in \{1, 2, 3, 4\}$ and $c \in \{0, 1, 2, 3, 4\}$. If each key is used with equal probability then, by (2),

$$H(K) = \log_2 20 \approx 4.322.$$

Exercise: what, intuitively, is the entropy in K, given that Malcolm has observed $e_{(a,c)}(1) = 2$?

Question 2 on Preliminary Problem Sheet

(2) A friend knows a number between 0 and 15 (inclusive).

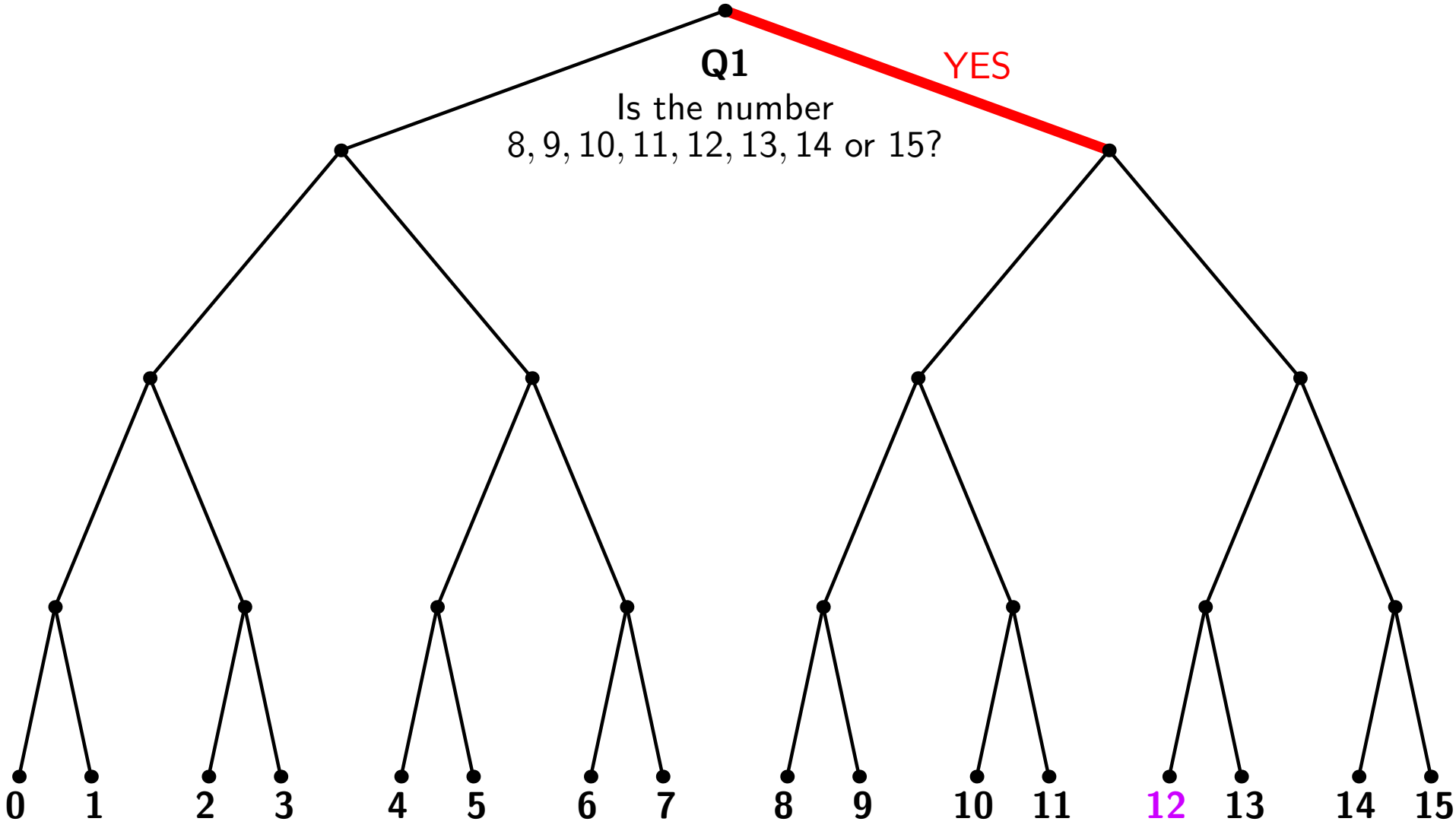
(a) How many questions do you need to guess it? What is the connection to binary? [*Hint:* how many bits do you learn?] How would your answer change if 15 is replaced with 26?

(b) Now suppose your friend is permitted to lie in the answer to at most one question.

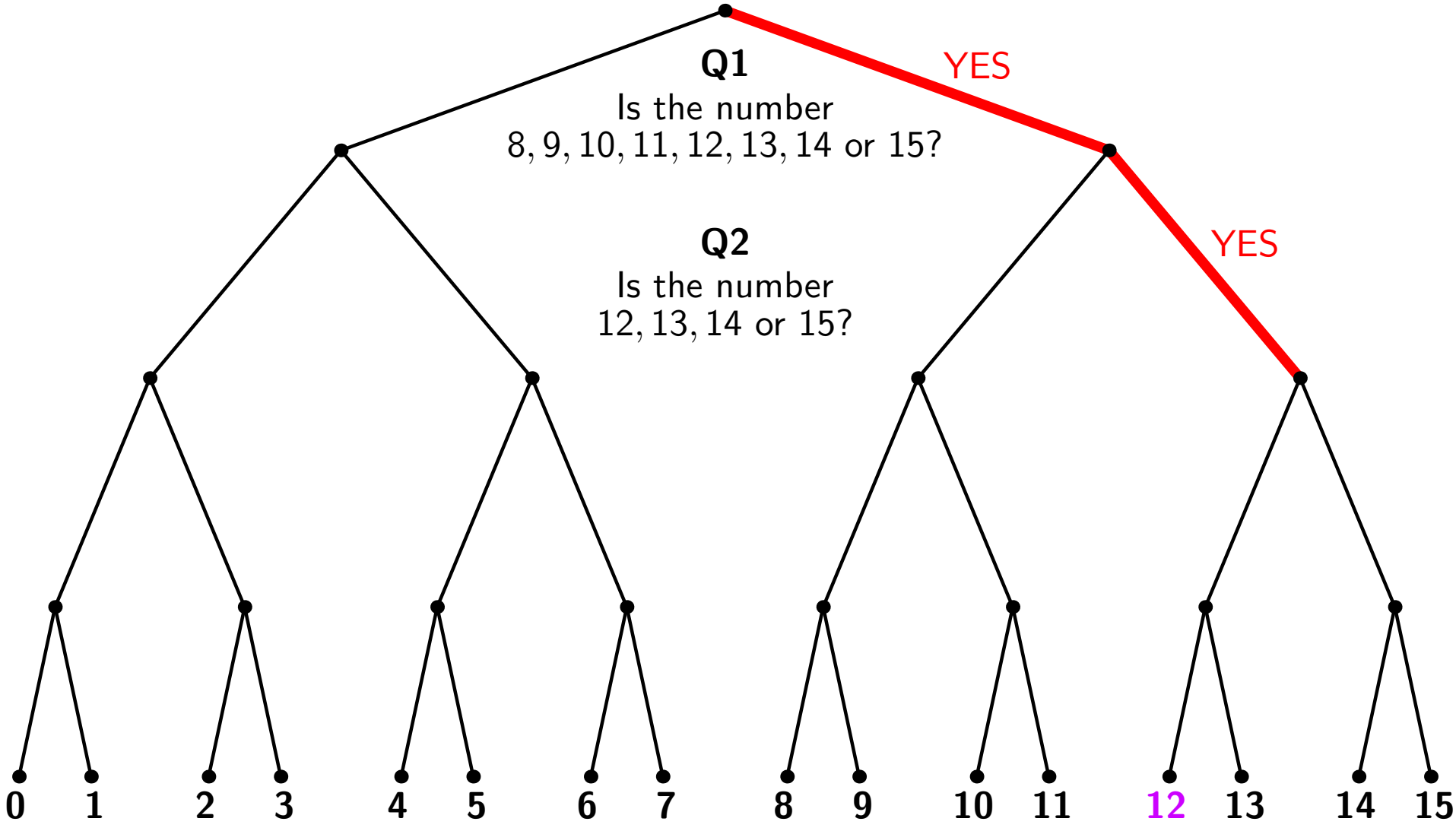
(i) Show that no strategy can guarantee to find the number by asking exactly six questions. [*Hint:* as well as learning four bits of information about the number, you learn about the lie.]

(ii) (Optional, but instructive.) Suggest a good strategy.

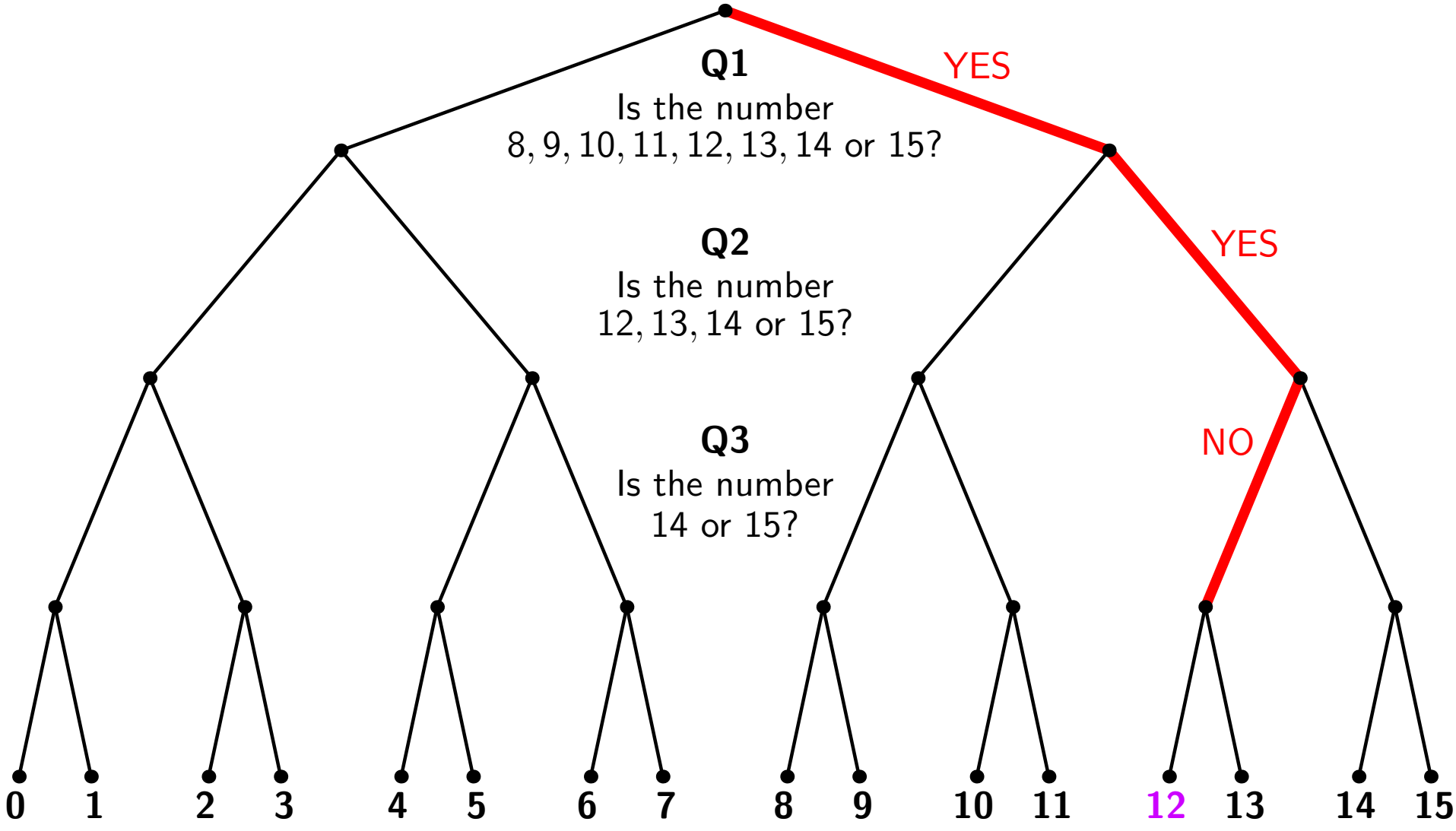
4 Yes/No Questions for 4 Bits of Information



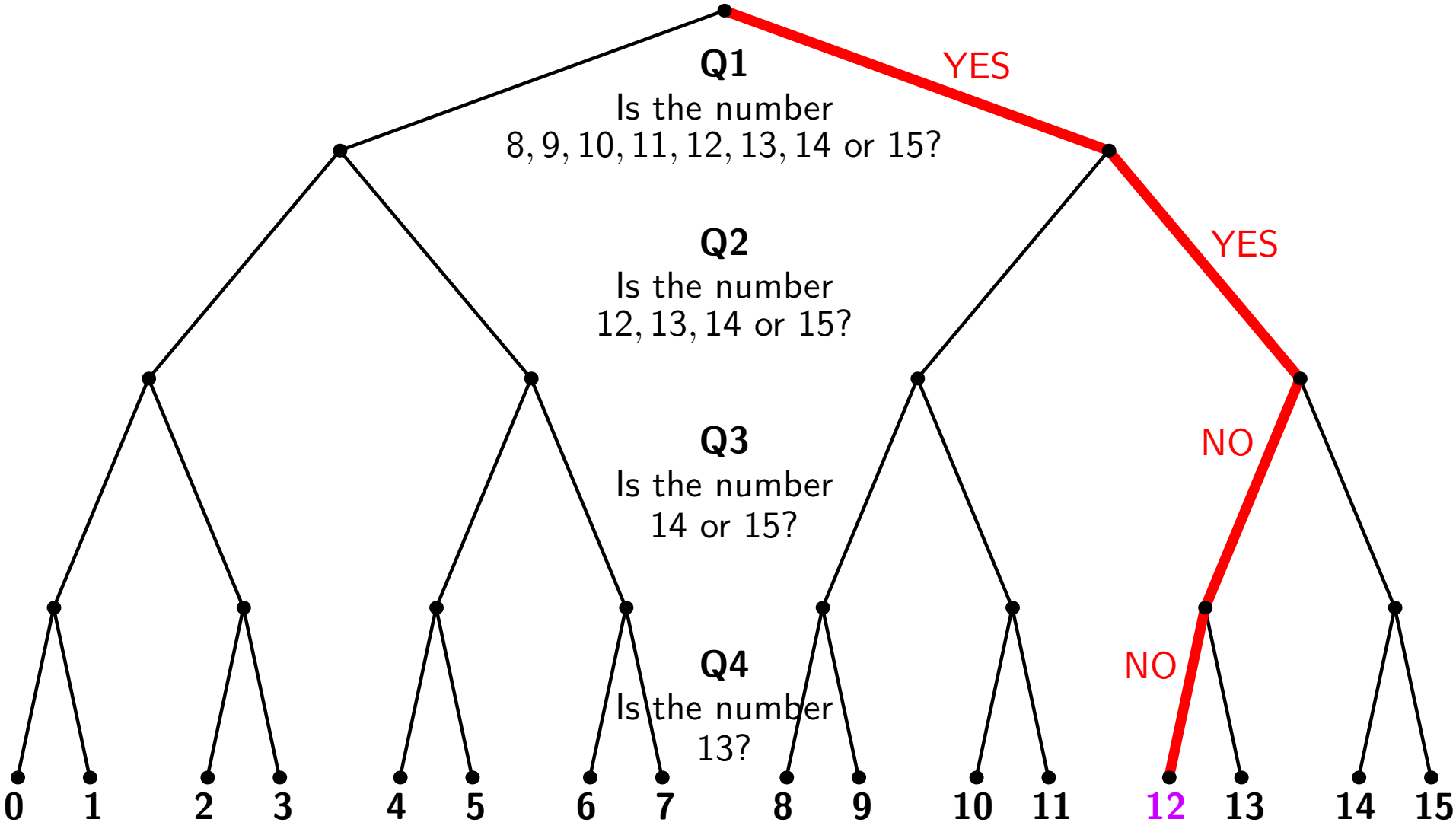
4 Yes/No Questions for 4 Bits of Information



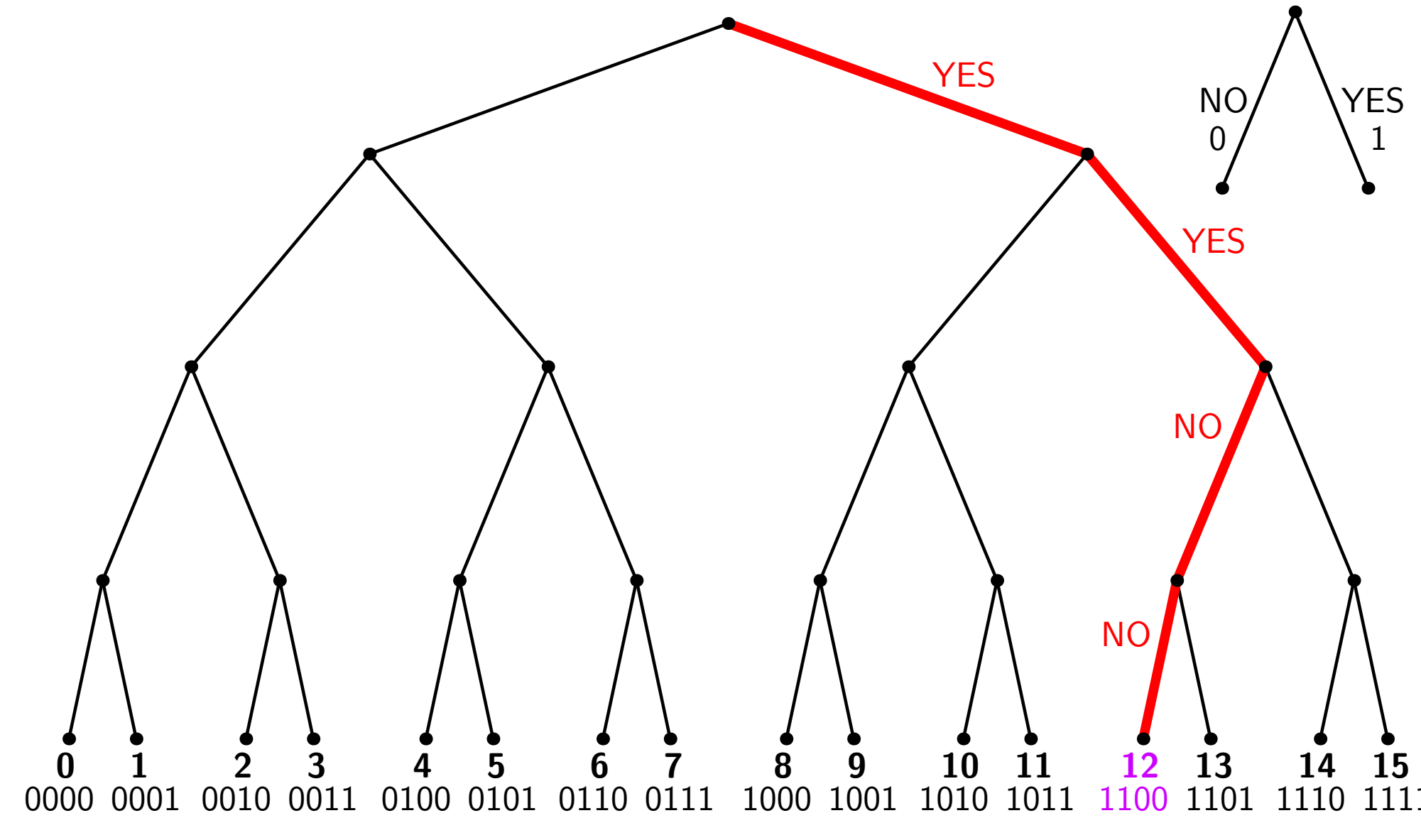
4 Yes/No Questions for 4 Bits of Information



4 Yes/No Questions for 4 Bits of Information



4 Yes/No Questions for 4 Bits of Information



Exercise′ 4.3

(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

Exercise′ 4.3

(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

Exercise′ 4.3

(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

Exercise′ 4.3

(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

Exercise′ 4.3

(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 probabilities it takes each value, not the values themselves.

Exercise′ 4.3

(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 probabilities 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, on average, h well-chosen yes/no questions.

Definition 4.4

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

$$H(K,Y) = \sum_{k\in\mathcal{K}}\sum_{y\in\mathcal{C}} \mathbb{P}[K=k \text{ and } Y=y] \log_2 \frac{1}{\mathbb{P}[K=k \text{ and } Y=y]}.$$

The *conditional entropy of K given that $Y=y$* is defined by

$$H(K|Y=y) = \sum_{k\in\mathcal{K}} \mathbb{P}[K=k|Y=y] \log_2 \frac{1}{\mathbb{P}[X=k|Y=y]}.$$

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 4.4

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

$$H(K,Y) = \sum_{k\in\mathcal{K}}\sum_{y\in\mathcal{C}} \mathbb{P}[K=k \text{ and } Y=y] \log_2 \frac{1}{\mathbb{P}[K=k \text{ and } Y=y]}.$$

The *conditional entropy of K given that $Y=y$* is defined by

$$H(K|Y=y) = \sum_{k\in\mathcal{K}} \mathbb{P}[K=k|Y=y] \log_2 \frac{1}{\mathbb{P}[X=k|Y=y]}.$$

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 4.5

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

Definition 4.4

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

$$H(K,Y) = \sum_{k\in\mathcal{K}}\sum_{y\in\mathcal{C}} \mathbb{P}[K=k \text{ and } Y=y] \log_2 \frac{1}{\mathbb{P}[K=k \text{ and } Y=y]}.$$

The *conditional entropy of K given that $Y=y$* is defined by

$$H(K|Y=y) = \sum_{k\in\mathcal{K}} \mathbb{P}[K=k|Y=y] \log_2 \frac{1}{\mathbb{P}[X=k|Y=y]}.$$

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 4.6 (Chaining Rule)

Let K and Y be random variables. Then

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

Shannon's Theorem on Key Uncertainty

Lemma 4.7

Let K and X be random variables.

(a) *If K and X are independent then $H(K, X) = H(K) + H(X)$.*

(b) *If f is a bijective function then $H(f(X)) = X$.*

The proof of (a) is Question 1 on Sheet 3. The idea behind (b) is the same as the final part of Exercise 4.3(b). If this does not convince you then please see the optional Question 7 on Sheet 2.

Theorem 4.8

Take a cryptosystem in our usual notation. Then

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

Alphabetic Ciphers: the One-Time Pad

Exercise 4.9

If Y_n is equally likely to be each element of $\mathcal{A}^n$, what is $H(Y_n)$?

Example 4.10

Fix $n \in \mathbb{N}$. The *one-time pad* is a cryptosystem with plaintexts, ciphertexts and keyspace $\mathcal{A}^n$. The encryption maps 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, $x_i + k_i$ is computed by converting x_i and k_i to numbers and adding modulo 26. For example, if n was fixed as 8,

$$e_{\mathrm{abcdefgh}}(\mathrm{goodwork}) = \mathrm{gpqgatxr}.$$

Suppose that all keys are equally likely. Then

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

Alphabetic Ciphers: the One-Time Pad

Exercise 4.9

If Y_n is equally likely to be each element of $\mathcal{A}^n$, what is $H(Y_n)$?

Example 4.10

Fix $n \in \mathbb{N}$. The *one-time pad* is a cryptosystem with plaintexts, ciphertexts and keyspace $\mathcal{A}^n$. The encryption maps 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, $x_i + k_i$ is computed by converting x_i and k_i to numbers and adding modulo 26. For example, if n was fixed as 8,

$$e_{\mathrm{abcdefgh}}(\mathrm{goodwork}) = \mathrm{gpqgatxr}.$$

Exercise 4.11

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) $n \log_2 26$

Alphabetic Ciphers: the One-Time Pad

Exercise 4.9

If Y_n is equally likely to be each element of $\mathcal{A}^n$, what is $H(Y_n)$?

Example 4.10

Fix $n \in \mathbb{N}$. The *one-time pad* is a cryptosystem with plaintexts, ciphertexts and keyspace $\mathcal{A}^n$. The encryption maps 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, $x_i + k_i$ is computed by converting x_i and k_i to numbers and adding modulo 26. For example, if n was fixed as 8,

$$e_{\mathrm{abcdefgh}}(\mathrm{goodwork}) = \mathrm{gpqgatxr}.$$

Exercise 4.11

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) $n \log_2 26$

Alphabetic Ciphers: the One-Time Pad

Exercise 4.9

If Y_n is equally likely to be each element of $\mathcal{A}^n$, what is $H(Y_n)$?

Example 4.10

Fix $n \in \mathbb{N}$. The *one-time pad* is a cryptosystem with plaintexts, ciphertexts and keyspace $\mathcal{A}^n$. The encryption maps 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, $x_i + k_i$ is computed by converting x_i and k_i to numbers and adding modulo 26. For example, if n was fixed as 8,

$$e_{\mathrm{abcdefgh}}(\mathrm{goodwork}) = \mathrm{gpqgatxr}.$$

Exercise 4.11

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

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

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

Unicity Distance

Exercise 4.12

Show that if Y_n is equally likely to be each element of $\mathcal{A}^n$ then $H(Y_n) - H(X_n) = Rn$ and so

$$H(K|Y) = H(K) - Rn. \qquad (\dagger)$$

What is the largest n for which $(\dagger)$ could hold with equality?

Definition 4.13

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

Exercise 4.14

In Question 2 on Sheet 1, the ciphertext y, of length 356 (without spaces), determined the key π up to $\pi(\mathrm{j})$, $\pi(\mathrm{x})$, $\pi(\mathrm{z}) \in \{\mathtt{F}, \mathtt{S}, \mathtt{V}\}$. Assuming equally likely keys, what is $H(K|Y_{356} = y)$?

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

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

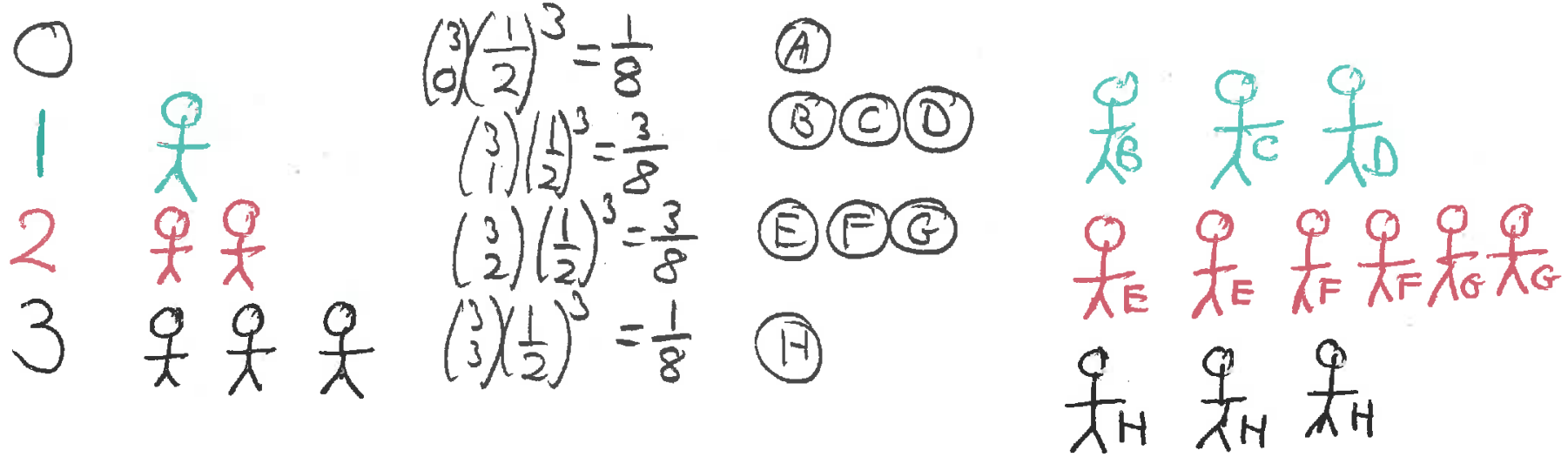
Ciphertexts with High $g(y)$ are More Likely: Intuition

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

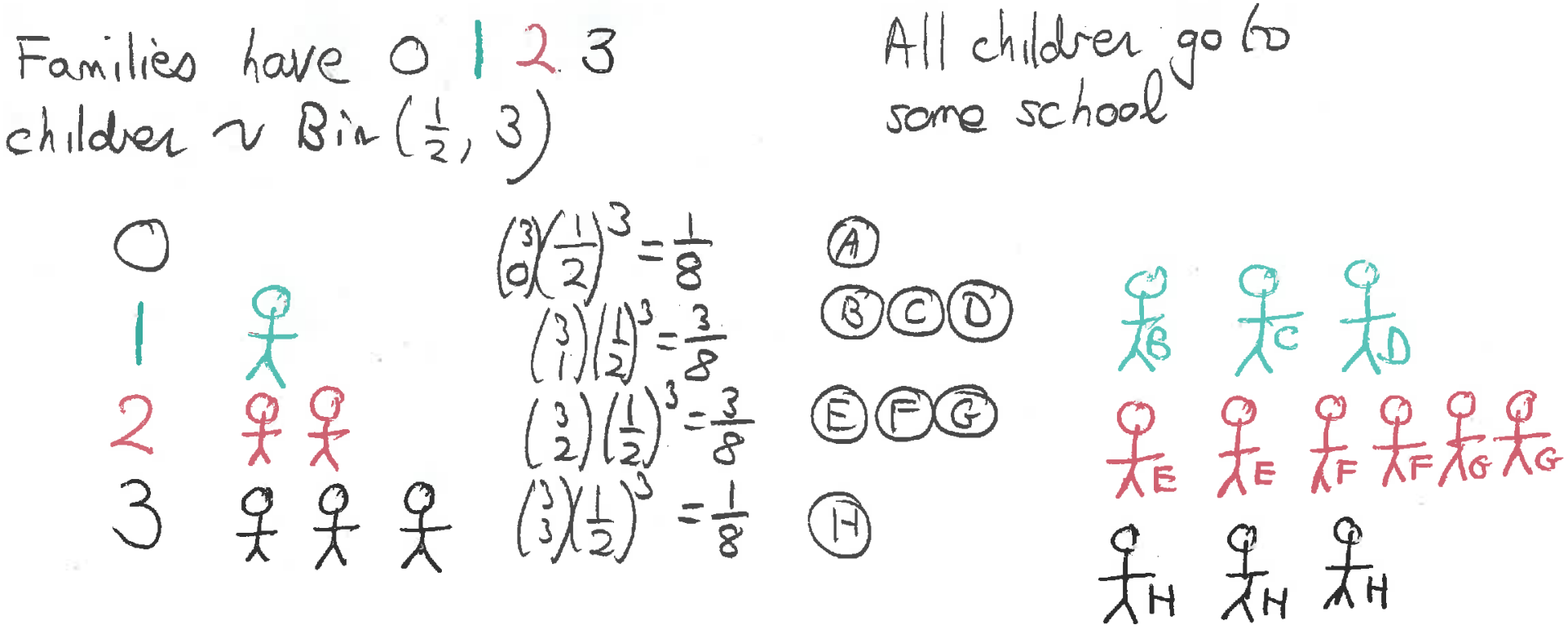
All children go to some school



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

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

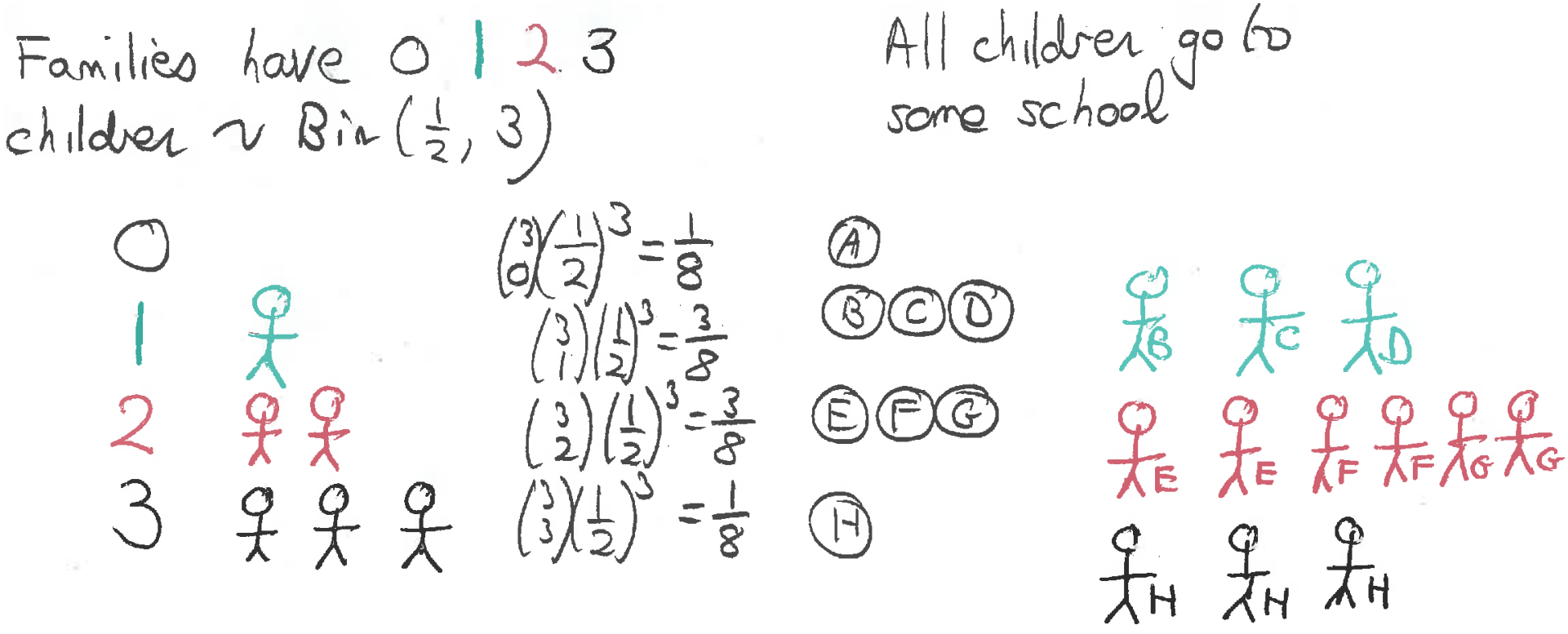


Sampling the school, the observed probabilities are 0 (no children), 1/4 (3 green only children), 1/2 (6 red children), 1/4 (3 black children).

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

Quiz: Suppose I ask 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



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.

Example 4.15

(i) The unicity distance for the substitution cipher is $\log(26!)/R \approx 88.382/3.200 = 27.6$. So 28 characters of ciphertext should, in theory, determine most of the key.

For instance the first 28 characters of the ciphertext in Question 2 on Sheet 1 are (with extra spaces) `XNKWBMOW KWH JKXKRJKRZJ RA KWRJ`. A computer search using a corpus of about 70000 words gives 13 decryptions, all of the form 'although the statistics i$\star$ this'; the only plausible choice for $\star$ is n. This essentially unique decryption is in good agreement with Shannon's argument.

Since 12 characters do not appear in the ciphertext, $H(K|Y = y_{28}) = \log_2 12! = 28.3$. But since π is determined on the most common plaintext letters, further decryptions will not be hard.

Example 4.15(ii)

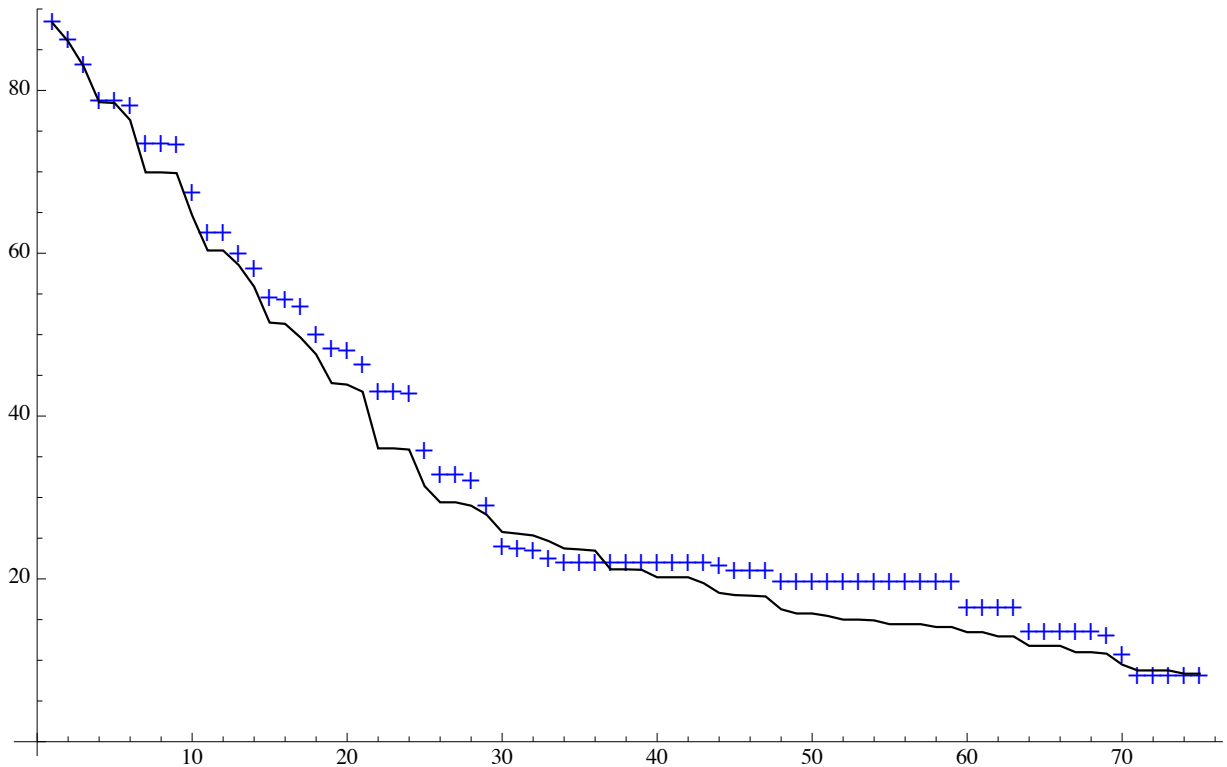
Suppose that the plaintext is made by concatenating arbitrary four letter English words in the New General Service List. There are 493 such words, so $H(X_{4m}) = (\log_2 493)m = 8.945m$, compared with $(4 \log_2 26)m \approx 18.811m$ for an arbitrary string of $4m$ characters. The per-character redundancy is

$$\frac{4 \log_2 26 - \log_2 493}{4} \approx 2.464$$

and so Shannon's argument says that the unicity distance for the substitution cipher is about $\log_2(26!)/2.464 = 35.868$. Therefore about 9 words should determine a large part of the key.

Example 4.15(ii) [ctd]

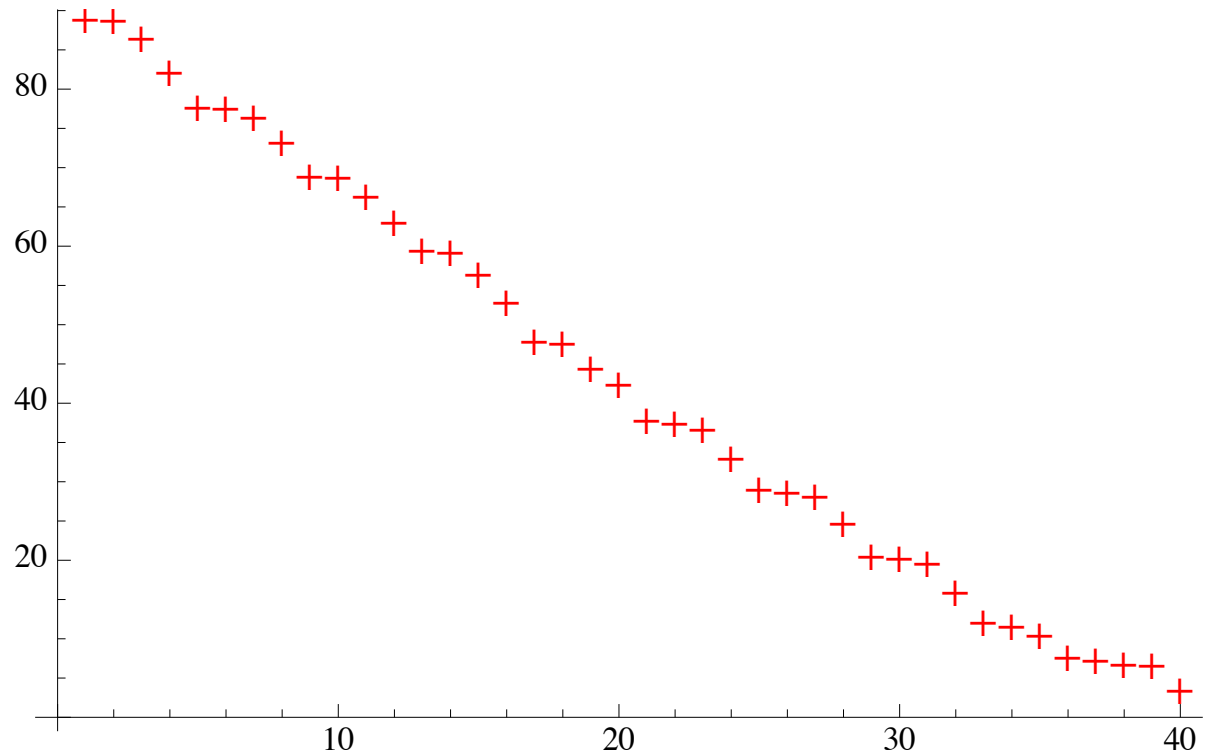
The blue points in the graph below show $H(K|Y_n)$ for the randomly chosen plaintext (shown with spaces for readability) 'case sale thin coal bore will much fuel gain soil site wear form fill wise task bend wild pray easy'. The black line shows the average of over 600 randomly chosen plaintexts.



Again there is good agreement with Shannon's argument.

Example 4.15(ii) [ctd]

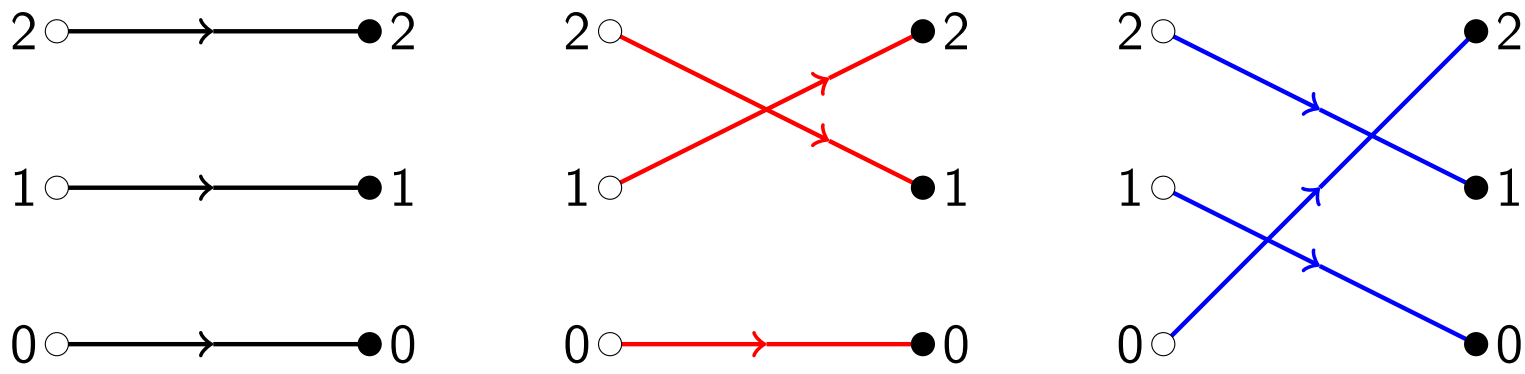
The contrived plaintext ‘away bank city drug exam from have lazy joke pose’ was chosen to contain every letter except ‘q’.



Almost all the key is known by the unicity distance. In fact, by the final character, there are just 6 decryptions consistent with the NGSL; one is the plaintext, another is ‘away bank city drug exam from save lazy joke hope’, obtained by permuting the plaintext by the 3-cycle $h \mapsto s \mapsto p \mapsto h$.

Sheet 2: Reminder of Notation

(1) The cryptosystem shown below uses three keys from the affine cipher on $\mathbb{Z}_3$, each with probability $\frac{1}{3}$. Suppose that plaintext 1 is sent with probability p and plaintext 2 is sent with probability $1-p$.



Here $\mathcal{P} = \mathcal{C} = \{0, 1, 2\}$. The diagrams show the encryption functions for three different keys. The probability that the plaintext is 0 is $p_0 = 0$, since $p_1 + p_2 = p + (1-p) = 1$.

(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?

Sheet 2: Hint for Question (2)

Let q be prime. Suppose that Alice and Bob communicate using the affine cipher on $\mathbb{Z}_q$, and that Alice sends plaintext $x \in \mathbb{Z}_q$ with probability p_x.

(a) What is the size $|\mathcal{K}|$ of the key space?

(b) Show that for each x, $y \in \mathbb{Z}_q$ there are exactly $q-1$ keys k such that $e_k(x) = y$.

(c) Show that if each key is used with equal probability then the cryptosystem has perfect secrecy.

(d) Show that the key can be determined by a chosen plaintext attack using two plaintexts. Does this contradict perfect secrecy? Does a single plaintext suffice?

In Question 1 we used three keys from the affine cipher on $\mathbb{Z}_3$. So a good example to look at is $\mathbb{Z}_3$. For instance, in (b), suppose $x = 1$, $y = 2$ (for an example). We have

$$e_{(a,c)}(1) = 2 \iff a \times 1 + c = 2 \iff a + c = 2.$$

You need to show this equation has exactly $q - 1 = 2$ solutions $(a, c) \in \mathcal{K}$.

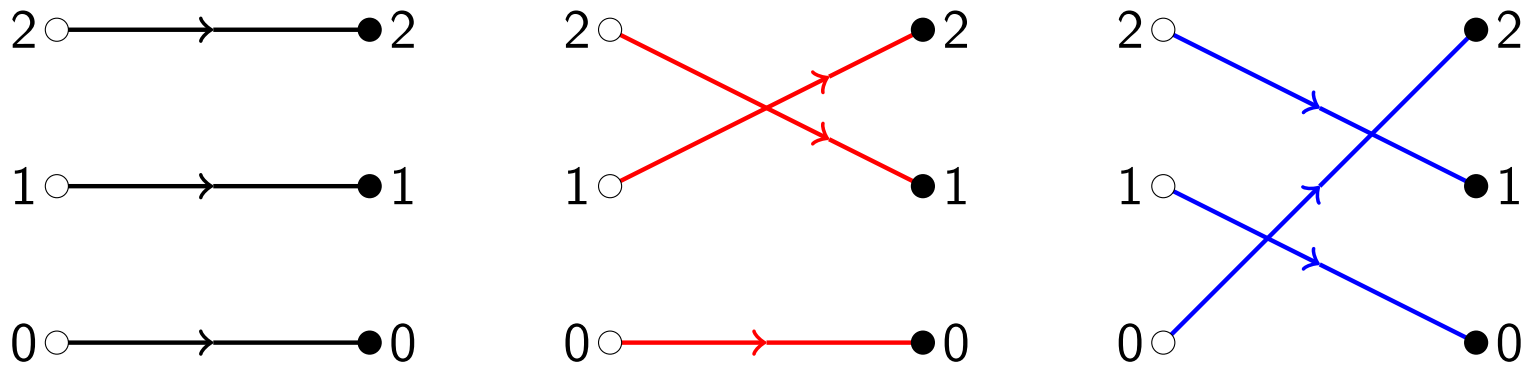
Correction to Problem Sheet 3

(2) Eve intercepts the three ciphertexts `cqhk`, `wqvj`, `bqsq` [**typo: was** `bpsq`] encrypted using the same one-time pad. Find all three plaintexts and the key.

[*Hint:* the code used in the lecture is online at `https://repl.it/M78M/3`. If you do it by hand, it will be helpful to know that the plaintexts are four letter words related to cryptography.]

Sheet 2

(1) The cryptosystem shown below uses three keys from the affine cipher on $\mathbb{Z}_3$, each with probability $\frac{1}{3}$. Suppose that plaintext 1 is sent with probability p and plaintext 2 is sent with probability $1-p$.



(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?

Sheet 2

(2) Let q be prime. Suppose that Alice and Bob communicate using the affine cipher on $\mathbb{Z}_q$, and that Alice sends plaintext $x \in \mathbb{Z}_q$ with probability p_x.

(a) What is the size $|\mathcal{K}|$ of the key space?

(b) Show that for each x, $y \in \mathbb{Z}_q$ there are exactly $q - 1$ keys k such that $e_k(x) = y$.

(c) Show that if each key is used with equal probability then the cryptosystem has perfect secrecy.

(d) Show that the key can be determined by a chosen plaintext attack using two plaintexts. Does this contradict perfect secrecy? Does a single plaintext suffice?

Part B: Stream ciphers

§5 Linear Feedback Shift Registers

Example 5.1

Consider the function $F : \mathbb{F}_2^4 \to \mathbb{F}_2^4$ 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) Starting with $x = 0001$, the sequence $x, F(x), F^2(x), F^3(x), \ldots$ is $(0001, 0010, 0100, 1001, 0011, 0110, \ldots)$.

Quiz: What is the set of $m \in \mathbb{Z}$ such that $F^m(x) = x$?

(A) $\{15, 30, 45, \ldots\}$ (B) $\{0, 15, 30, 45, \ldots\}$ (C) $15\mathbb{Z}$ (D) other

Would your answer change if x was replaced with any other $x' \in \mathbb{F}_2^\ell$? (Be careful!)

(A) No (B) Yes

§5 Linear Feedback Shift Registers

Example 5.1

Consider the function $F : \mathbb{F}_2^4 \to \mathbb{F}_2^4$ 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) Starting with $x = 0001$, the sequence $x, F(x), F^2(x), F^3(x), \ldots$ is $(0001, 0010, 0100, 1001, 0011, 0110, \ldots)$.

Quiz: What is the set of $m \in \mathbb{Z}$ such that $F^m(x) = x$?

(A) $\{15, 30, 45, \ldots\}$ (B) $\{0, 15, 30, 45, \ldots\}$ (C) $15\mathbb{Z}$ (D) other

Would your answer change if x was replaced with any other $x' \in \mathbb{F}_2^\ell$? (Be careful!)

(A) No (B) Yes

§5 Linear Feedback Shift Registers

Example 5.1

Consider the function $F : \mathbb{F}_2^4 \to \mathbb{F}_2^4$ 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) Starting with $x = 0001$, the sequence $x, F(x), F^2(x), F^3(x), \ldots$ is $(0001, 0010, 0100, 1001, 0011, 0110, \ldots)$.

Quiz: What is the set of $m \in \mathbb{Z}$ such that $F^m(x) = x$?

(A) $\{15, 30, 45, \ldots\}$ (B) $\{0, 15, 30, 45, \ldots\}$ (C) $15\mathbb{Z}$ (D) other

Would your answer change if x was replaced with any other $x' \in \mathbb{F}_2^\ell$? (Be careful!)

(A) No (B) Yes

Part B: Stream ciphers

§5 Linear Feedback Shift Registers

Example 5.1

Consider the function $F : \mathbb{F}_2^4 \to \mathbb{F}_2^4$ 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) Starting with $x = 0001$, the sequence $x, F(x), F^2(x), F^3(x), \ldots$ is $(0001, 0010, 0100, 1001, 0011, 0110, \ldots)$.

Example′ 5.2

Define $H : \mathbb{F}_2^4 \to \mathbb{F}_2^4$ by $H\big((x_0, x_1, x_2, x_3)\big) = (x_1, x_2, x_3, x_1 + x_2)$.
True or false: H is invertible?

(A) False (B) True

There is a cycle of length 7 in H.

(A) False (B) True

Part B: Stream ciphers

§5 Linear Feedback Shift Registers

Example 5.1

Consider the function $F : \mathbb{F}_2^4 \to \mathbb{F}_2^4$ 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) Starting with $x = 0001$, the sequence $x, F(x), F^2(x), F^3(x), \ldots$ is $(0001, 0010, 0100, 1001, 0011, 0110, \ldots)$.

Example′ 5.2

Define $H : \mathbb{F}_2^4 \to \mathbb{F}_2^4$ by $H\big((x_0, x_1, x_2, x_3)\big) = (x_1, x_2, x_3, x_1 + x_2)$.
True or false: H is invertible?

(A) False (B) True

There is a cycle of length 7 in H.

(A) False (B) True

Part B: Stream ciphers

§5 Linear Feedback Shift Registers

Example 5.1

Consider the function $F : \mathbb{F}_2^4 \to \mathbb{F}_2^4$ 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) Starting with $x = 0001$, the sequence $x, F(x), F^2(x), F^3(x), \ldots$ is $(0001, 0010, 0100, 1001, 0011, 0110, \ldots)$.

Example′ 5.2

Define $H : \mathbb{F}_2^4 \to \mathbb{F}_2^4$ by $H\big((x_0, x_1, x_2, x_3)\big) = (x_1, x_2, x_3, x_1 + x_2)$.
True or false: H is invertible?

(A) False (B) True

There is a cycle of length 7 in H.

(A) False (B) True

Definition of LFSRs

Definition 5.3

A *linear feedback shift register* of *width* $\ell \in \mathbb{N}$ 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

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

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*.

We abbreviate 'linear feedback shift register' to LFSR. 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 $\ell - 1$.

Exercise 5.4

What is 'linear' about an LFSR?

Exercise 5.5

(a) Let F be as in Example 5.1. Find the sequence $F^t(0111)_0$ for $t \in \mathbb{N}_0$. (Note that F^0 is, by definition, the identity function.)

(b) Let F be an LFSR of width ℓ and let $k \in \mathbb{F}_\ell$. Show that $F^t(k)_0 = k_t$ if $0 \leq t < \ell$ and that $F^\ell(k)_0 = f(k_0, \ldots, k_{\ell-1})$.

Definition 5.6

Let F be an LFSR of width ℓ.

(a) The *keystream* defined by F with key $k \in \mathbb{F}_2^\ell$ is the sequence

$$(k_0, k_1, k_2, \ldots, k_t, \ldots)$$

where $k_t = F^t(k)_0$ for each $t \in \mathbb{N}_0$.

(b) Fix $n \in \mathbb{N}$. 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 $x \in \mathcal{P}$.

Keystream Example

Example 5.7

In Exercise 5.5(a) we found that the keystream for the LFSR F in Example 5.1 with key $k = 0111$ was

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

By Question 2 on Sheet 4,

$$F^s(k) = (k_s, k_{s+1}, \ldots, k_{s+\ell-1})$$

for each $s \in \mathbb{N}$. For example,

$$F^3(0111) = (k_3, k_4, k_5, k_6) = (1,1,0,0)$$
$$F^{14}(0111) = (k_{14}, k_{15}, k_{16}, k_{17}) = (1,0,1,1)$$
$$F^{15}(0111) = (k_{15}, k_{16}, k_{17}, k_{18}) = (0,1,1,1) = k.$$

The keystream has period 15. Correspondingly 15 is the smallest number m such that $F^m\big((0,1,1,1)\big) = (0,1,1,1)$.

Keystream Example

Example 5.7

In Exercise 5.5(a) we found that the keystream for the LFSR F in Example 5.1 with key $k = 0111$ was

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

By Question 2 on Sheet 4,

$$F^s(k) = (k_s, k_{s+1}, \ldots, k_{s+\ell-1})$$

for each $s \in \mathbb{N}$. For example,

$$\begin{aligned} F^3(0111) &= (k_3, k_4, k_5, k_6) = (1, 1, 0, 0) \\ F^{14}(0111) &= (k_{14}, k_{15}, k_{16}, k_{17}) = (1, 0, 1, 1) \\ F^{15}(0111) &= (k_{15}, k_{16}, k_{17}, k_{18}) = (0, 1, 1, 1) = k. \end{aligned}$$

The keystream has period 15. Correspondingly 15 is the smallest number m such that $F^m\big((0, 1, 1, 1)\big) = (0, 1, 1, 1)$.

Keystream Example

Example 5.7

In Exercise 5.5(a) we found that the keystream for the LFSR F in Example 5.1 with key $k = 0111$ was

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

By Question 2 on Sheet 4,

$$F^s(k) = (k_s, k_{s+1}, \ldots, k_{s+\ell-1})$$

for each $s \in \mathbb{N}$. For example,

$$F^3(0111) = (k_3, k_4, k_5, k_6) = (1,1,0,0)$$
$$F^{14}(0111) = (k_{14}, k_{15}, k_{16}, k_{17}) = (1,0,1,1)$$
$$F^{15}(0111) = (k_{15}, k_{16}, k_{17}, k_{18}) = (0,1,1,1) = k.$$

The keystream has period 15. Correspondingly 15 is the smallest number m such that $F^m\big((0,1,1,1)\big) = (0,1,1,1)$.

Keystream Example

Example 5.7

In Exercise 5.5(a) we found that the keystream for the LFSR F in Example 5.1 with key $k = 0111$ was

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

By Question 2 on Sheet 4,

$$F^s(k) = (k_s, k_{s+1}, \ldots, k_{s+\ell-1})$$

for each $s \in \mathbb{N}$. For example,

$$F^3(0111) = (k_3, k_4, k_5, k_6) = (1,1,0,0)$$
$$F^{14}(0111) = (k_{14}, k_{15}, k_{16}, k_{17}) = (1,0,1,1)$$
$$F^{15}(0111) = (k_{15}, k_{16}, k_{17}, k_{18}) = (0,1,1,1) = k.$$

The keystream has period 15. Correspondingly 15 is the smallest number m such that $F^m\big((0,1,1,1)\big) = (0,1,1,1)$.

Matrix Representation of an LFSR

Definition 5.8

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

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

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

Extra Example of Matrix Representing an LFSR

Let F be the LFSR of width 4 with taps $\{0, 1\}$ seen in Examples 5.1, 5.5(a), 5.7, so $F\big((x_0, x_1, x_2, x_3)\big) = (x_1, x_2, x_3, x_0 + x_1)$. The keystream for key 0111 was found in Example 5.7.

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

By Proposition 5.9, F is represented by $M = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$. So

$F(x) = xM$ for each $x \in \mathbb{F}_2^\ell$ and we can compute the keystream by repeatedly multiplying by M: each time M shifts the bits to the left, and we get a new bit at the far right.

Extra Example of Matrix Representing an LFSR

Let F be the LFSR of width 4 with taps $\{0, 1\}$ seen in Examples 5.1, 5.5(a), 5.7, so $F\big((x_0, x_1, x_2, x_3)\big) = (x_1, x_2, x_3, x_0 + x_1)$. The keystream for key 0111 was found in Example 5.7.

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

By Proposition 5.9, F is represented by $M = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$. So $F(x) = xM$ for each $x \in \mathbb{F}_2^\ell$ and we can compute the keystream by repeatedly multiplying by M: each time M shifts the bits to the left, and we get a new bit at the far right.

$$(0, 1, 1, 1) \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} = (1, 1, 1, 1)$$

Extra Example of Matrix Representing an LFSR

Let F be the LFSR of width 4 with taps $\{0, 1\}$ seen in Examples 5.1, 5.5(a), 5.7, so $F\big((x_0, x_1, x_2, x_3)\big) = (x_1, x_2, x_3, x_0 + x_1)$. The keystream for key 0111 was found in Example 5.7.

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

By Proposition 5.9, F is represented by $M = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$. So $F(x) = xM$ for each $x \in \mathbb{F}_2^\ell$ and we can compute the keystream by repeatedly multiplying by M: each time M shifts the bits to the left, and we get a new bit at the far right.

$$(1, 1, 1, 1) \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} = (1, 1, 1, 0)$$

Extra Example of Matrix Representing an LFSR

Let F be the LFSR of width 4 with taps $\{0, 1\}$ seen in Examples 5.1, 5.5(a), 5.7, so $F\big((x_0, x_1, x_2, x_3)\big) = (x_1, x_2, x_3, x_0 + x_1)$. The keystream for key 0111 was found in Example 5.7.

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

By Proposition 5.9, F is represented by $M = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$. So $F(x) = xM$ for each $x \in \mathbb{F}_2^\ell$ and we can compute the keystream by repeatedly multiplying by M: each time M shifts the bits to the left, and we get a new bit at the far right.

$$(1, 1, 1, 0) \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} = (1, 1, 0, 0)$$

Extra Example of Matrix Representing an LFSR

Let F be the LFSR of width 4 with taps $\{0, 1\}$ seen in Examples 5.1, 5.5(a), 5.7, so $F\big((x_0, x_1, x_2, x_3)\big) = (x_1, x_2, x_3, x_0 + x_1)$. The keystream for key 0111 was found in Example 5.7.

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

By Proposition 5.9, F is represented by $M = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$. So $F(x) = xM$ for each $x \in \mathbb{F}_2^\ell$ and we can compute the keystream by repeatedly multiplying by M: each time M shifts the bits to the left, and we get a new bit at the far right.

For Lemma 5.10 we look at action on column vectors

Extra Example of Matrix Representing an LFSR

Let F be the LFSR of width 4 with taps $\{0, 1\}$ seen in Examples 5.1, 5.5(a), 5.7, so $F\big((x_0, x_1, x_2, x_3)\big) = (x_1, x_2, x_3, x_0 + x_1)$. The keystream for key 0111 was found in Example 5.7.

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

By Proposition 5.9, F is represented by $M = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$. So $F(x) = xM$ for each $x \in \mathbb{F}_2^\ell$ and we can compute the keystream by repeatedly multiplying by M: each time M shifts the bits to the left, and we get a new bit at the far right.

For Lemma 5.10 we look at action on column vectors

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

Extra Example of Matrix Representing an LFSR

Let F be the LFSR of width 4 with taps $\{0, 1\}$ seen in Examples 5.1, 5.5(a), 5.7, so $F\big((x_0, x_1, x_2, x_3)\big) = (x_1, x_2, x_3, x_0 + x_1)$. The keystream for key 0111 was found in Example 5.7.

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

By Proposition 5.9, F is represented by $M = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$. So $F(x) = xM$ for each $x \in \mathbb{F}_2^\ell$ and we can compute the keystream by repeatedly multiplying by M: each time M shifts the bits to the left, and we get a new bit at the far right.

For Lemma 5.10 we look at action on column vectors

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

Extra Example of Matrix Representing an LFSR

Let F be the LFSR of width 4 with taps $\{0, 1\}$ seen in Examples 5.1, 5.5(a), 5.7, so $F\big((x_0, x_1, x_2, x_3)\big) = (x_1, x_2, x_3, x_0 + x_1)$. The keystream for key 0111 was found in Example 5.7.

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

By Proposition 5.9, F is represented by $M = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$. So $F(x) = xM$ for each $x \in \mathbb{F}_2^\ell$ and we can compute the keystream by repeatedly multiplying by M: each time M shifts the bits to the left, and we get a new bit at the far right.

For Lemma 5.10 we look at action on column vectors

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

Extra Example of Matrix Representing an LFSR

Let F be the LFSR of width 4 with taps $\{0, 1\}$ seen in Examples 5.1, 5.5(a), 5.7, so $F\big((x_0, x_1, x_2, x_3)\big) = (x_1, x_2, x_3, x_0 + x_1)$. The keystream for key 0111 was found in Example 5.7.

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

By Proposition 5.9, F is represented by $M = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$. So $F(x) = xM$ for each $x \in \mathbb{F}_2^\ell$ and we can compute the keystream by repeatedly multiplying by M: each time M shifts the bits to the left, and we get a new bit at the far right.

For Lemma 5.10 we look at action on column vectors

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

Minimal Polynomial of an LFSR

Recall that the *minimal polynomial* of a matrix M with coefficients in $\mathbb{F}_2$ is the non-zero polynomial $g(X) \in \mathbb{F}_2[X]$ of least degree such that $g(M) = 0$.

In the following lemma we work with column vectors of length ℓ. For $i \in \{0, 1, \ldots, \ell - 1\}$, let $\mathbf{v}(i)$ denote the column vector with 1 in position i (numbering positions from 0), and 0 in all other positions.

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.

Period of an LFSR

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

Correction: in the 'useful property' of the minimal polynomial $g(X)$ of a matrix M, I said

> *if* $f(M) = 0$ *then* $g(X)$ *divides* $h(X)$

here $h(X)$ should be $f(X)$.

Corollary 5.11

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

It is a useful fact that every invertible LFSR has a cycle of length equal to its period. For a proof see the optional Question 7 on Sheet 4.

To illustrate Corollary 5.11 we find an LFSR with period $2^{11} - 1 = 2047$ using MATHEMATICA to do the calculations.

Attacks on LFSRs

Example 5.12

Malcolm the mole knows the plaintext/ciphertext pair

$$x = (0,0,1,1,0,1,0,1,1,0,1,0,1,1,0,0,1,1,1,1)$$
$$y = (0,0,1,1,1,0,1,0,0,0,0,0,0,1,0,1,0,1,1,1)$$
$$\quad 0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9$$

for an LFSR cryptosystem of width 5, and deduces the keystream starts

$$x + y = (0,0,0,0,1,1,1,1,1,0,1,0,1,0,0,1,1,0,0,0)$$
$$\quad k_0\ k_1\ k_2\ k_3\ k_4\ k_5\ k_6\ k_7\ k_8\ k_9\ k_{10} \qquad \ldots \qquad k_{19}$$

The keystream does not obviously repeat, so he guesses that the period of the LFSR is more than 20. Taking the first five bits, Malcolm learns that $k = (0,0,0,0,1)$.

Example 5.12 [continued]

By Question 2 on Sheet 4 (see also Example 5.7), he knows that

$$F(k) = (k_1, \ldots, k_5) = (0, 0, 0, 1, 1)$$
$$F^2(k) = (k_2, \ldots, k_6) = (0, 0, 1, 1, 1)$$
$$F^3(k) = (k_3, \ldots, k_7) = (0, 1, 1, 1, 1)$$

and so on. The six vectors $k, F(k), \ldots, F^5(k)$ lie in the 5-dimensional vector space $\mathbb{F}_2^5$ so are linearly dependent. By row-reducing the matrix

$$\begin{array}{c} k \\ F(k) \\ F^2(k) \\ F^3(k) \\ F^4(k) \\ F^5(k) \end{array} \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

or by inspection, he sees that $k + F^4(k) + F^5(k) = (0, 0, 0, 0, 0)$. This suggests that the minimal polynomial of the LFSR is $1 + X^4 + X^5$, and so the taps are $\{0, 4\}$.

Quiz on Perfect Secrecy (Explanation on Next Slide)

Fix a cryptosystem with plaintexts $\mathcal{P}$, ciphertexts $\mathcal{C}$ and keyspsace $\mathcal{K}$. Assume that all ciphertexts are used in the cryptosystem, so $\mathbb{P}[Y = y] > 0$ for each $y \in \mathcal{C}$.

(a) Perfect secrecy means the cryptosystem is unbreakable.
(A) False (B) True

(b) The system is perfectly secret if and only if $\mathbb{P}[X = x | Y = y] = \mathbb{P}[X = x]$ for all $x \in \mathcal{P}$ and $y \in \mathcal{C}$.
(A) False (B) True

(c) If all ciphertexts are equally likely to appear then the cryptosystem is perfectly secret.
(A) False (B) True

(d) If all keys are used with equal probability then the cryptosystem is perfectly secret.
(A) False (B) True

(e) Suppose $|\mathcal{C}| = |\mathcal{K}|$ and $p_x > 0$ for all $x \in \mathcal{P}$. The cryptosystem is perfectly secret if and only if all keys are used with equal probability.
(A) False (B) True

Quiz on Perfect Secrecy (Explanation on Next Slide)

Fix a cryptosystem with plaintexts $\mathcal{P}$, ciphertexts $\mathcal{C}$ and keyspsace $\mathcal{K}$. Assume that all ciphertexts are used in the cryptosystem, so $\mathbb{P}[Y = y] > 0$ for each $y \in \mathcal{C}$.

(a) Perfect secrecy means the cryptosystem is unbreakable.
(A) False (B) True

(b) The system is perfectly secret if and only if $\mathbb{P}[X = x|Y = y] = \mathbb{P}[X = x]$ for all $x \in \mathcal{P}$ and $y \in \mathcal{C}$.
(A) False (B) True

(c) If all ciphertexts are equally likely to appear then the cryptosystem is perfectly secret.
(A) False (B) True

(d) If all keys are used with equal probability then the cryptosystem is perfectly secret.
(A) False (B) True

(e) Suppose $|\mathcal{C}| = |\mathcal{K}|$ and $p_x > 0$ for all $x \in \mathcal{P}$. The cryptosystem is perfectly secret if and only if all keys are used with equal probability.
(A) False (B) True

Quiz on Perfect Secrecy (Explanation on Next Slide)

Fix a cryptosystem with plaintexts $\mathcal{P}$, ciphertexts $\mathcal{C}$ and keyspsace $\mathcal{K}$. Assume that all ciphertexts are used in the cryptosystem, so $\mathbb{P}[Y = y] > 0$ for each $y \in \mathcal{C}$.

(a) Perfect secrecy means the cryptosystem is unbreakable.
(A) False (B) True

(b) The system is perfectly secret if and only if $\mathbb{P}[X = x | Y = y] = \mathbb{P}[X = x]$ for all $x \in \mathcal{P}$ and $y \in \mathcal{C}$.
(A) False (B) True

(c) If all ciphertexts are equally likely to appear then the cryptosystem is perfectly secret.
(A) False (B) True

(d) If all keys are used with equal probability then the cryptosystem is perfectly secret.
(A) False (B) True

(e) Suppose $|\mathcal{C}| = |\mathcal{K}|$ and $p_x > 0$ for all $x \in \mathcal{P}$. The cryptosystem is perfectly secret if and only if all keys are used with equal probability.
(A) False (B) True

Quiz on Perfect Secrecy (Explanation on Next Slide)

Fix a cryptosystem with plaintexts $\mathcal{P}$, ciphertexts $\mathcal{C}$ and keyspsace $\mathcal{K}$. Assume that all ciphertexts are used in the cryptosystem, so $\mathbb{P}[Y = y] > 0$ for each $y \in \mathcal{C}$.

(a) Perfect secrecy means the cryptosystem is unbreakable.
(A) False (B) True

(b) The system is perfectly secret if and only if $\mathbb{P}[X = x | Y = y] = \mathbb{P}[X = x]$ for all $x \in \mathcal{P}$ and $y \in \mathcal{C}$.
(A) False (B) True

(c) If all ciphertexts are equally likely to appear then the cryptosystem is perfectly secret.
(A) False (B) True

(d) If all keys are used with equal probability then the cryptosystem is perfectly secret.
(A) False (B) True

(e) Suppose $|\mathcal{C}| = |\mathcal{K}|$ and $p_x > 0$ for all $x \in \mathcal{P}$. The cryptosystem is perfectly secret if and only if all keys are used with equal probability.
(A) False (B) True

Quiz on Perfect Secrecy (Explanation on Next Slide)

Fix a cryptosystem with plaintexts $\mathcal{P}$, ciphertexts $\mathcal{C}$ and keyspsace $\mathcal{K}$. Assume that all ciphertexts are used in the cryptosystem, so $\mathbb{P}[Y = y] > 0$ for each $y \in \mathcal{C}$.

(a) Perfect secrecy means the cryptosystem is unbreakable.
(A) False (B) True

(b) The system is perfectly secret if and only if $\mathbb{P}[X = x|Y = y] = \mathbb{P}[X = x]$ for all $x \in \mathcal{P}$ and $y \in \mathcal{C}$.
(A) False (B) True

(c) If all ciphertexts are equally likely to appear then the cryptosystem is perfectly secret.
(A) False (B) True

(d) If all keys are used with equal probability then the cryptosystem is perfectly secret.
(A) False (B) True

(e) Suppose $|\mathcal{C}| = |\mathcal{K}|$ and $p_x > 0$ for all $x \in \mathcal{P}$. The cryptosystem is perfectly secret if and only if all keys are used with equal probability.
(A) False (B) True

Quiz on Perfect Secrecy (Explanation on Next Slide)

Fix a cryptosystem with plaintexts $\mathcal{P}$, ciphertexts $\mathcal{C}$ and keyspsace $\mathcal{K}$. Assume that all ciphertexts are used in the cryptosystem, so $\mathbb{P}[Y = y] > 0$ for each $y \in \mathcal{C}$.

(a) Perfect secrecy means the cryptosystem is unbreakable.
(A) False (B) True

(b) The system is perfectly secret if and only if $\mathbb{P}[X = x|Y = y] = \mathbb{P}[X = x]$ for all $x \in \mathcal{P}$ and $y \in \mathcal{C}$.
(A) False (B) True

(c) If all ciphertexts are equally likely to appear then the cryptosystem is perfectly secret.
(A) False (B) True

(d) If all keys are used with equal probability then the cryptosystem is perfectly secret.
(A) False (B) True

(e) Suppose $|\mathcal{C}| = |\mathcal{K}|$ and $p_x > 0$ for all $x \in \mathcal{P}$. The cryptosystem is perfectly secret if and only if all keys are used with equal probability.
(A) False (B) True

Quiz on Perfect Secrecy (Explanation on Next Slide)

Fix a cryptosystem with plaintexts $\mathcal{P}$, ciphertexts $\mathcal{C}$ and keyspsace $\mathcal{K}$. Assume that all ciphertexts are used in the cryptosystem, so $\mathbb{P}[Y = y] > 0$ for each $y \in \mathcal{C}$.

(a) Perfect secrecy means the cryptosystem is unbreakable.
(A) False (B) True

(b) The system is perfectly secret if and only if $\mathbb{P}[X = x|Y = y] = \mathbb{P}[X = x]$ for all $x \in \mathcal{P}$ and $y \in \mathcal{C}$.
(A) False (B) True

(c) If all ciphertexts are equally likely to appear then the cryptosystem is perfectly secret.
(A) False (B) True

(d) If all keys are used with equal probability then the cryptosystem is perfectly secret.
(A) False (B) True

(e) Suppose $|\mathcal{C}| = |\mathcal{K}|$ and $p_x > 0$ for all $x \in \mathcal{P}$. The cryptosystem is perfectly secret if and only if all keys are used with equal probability.
(A) False (B) True

Explanations for Quiz on Perfect Secrecy

(a) False: perfect secrecy has the technical definition in (b) which you will have to learn.

(b) True: an informal interpretation of the definition is 'observing a single ciphertext gives no information about the plaintext'. Different observations may give more information. For example, the one-time pad with equiprobable keys is perfectly secret. But:

- the key can usually be found from multiple known ciphertexts: See Question 2 on Sheet 3;
- the key can trivially be found from a known plaintext / ciphertext pair x, $y = x + k$ by subtracting x from y.

Explanations for Quiz on Perfect Secrecy

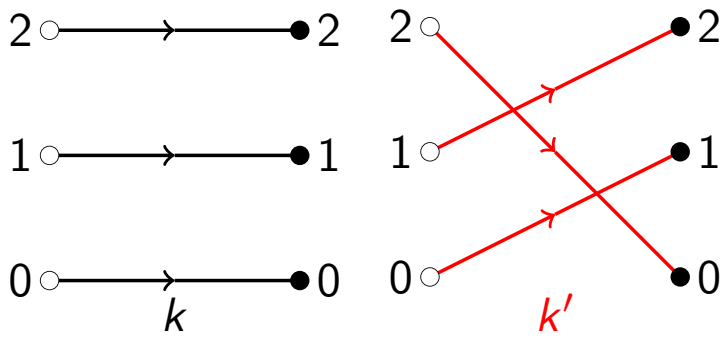
(c) False: For example take the cryptosystem in Example 3.1(i) with

$$\mathbb{P}[K = k] = \mathbb{P}[K = k'] = \tfrac{1}{2}$$

and $P[X = 1] = \mathbb{P}[X = 2] = \mathbb{P}[X = 3] = \frac{1}{3}$. All ciphertexts are equally likely, but

$$\mathbb{P}[X = 0 | Y = 2] = 0 \neq \tfrac{1}{3} = \mathbb{P}[X = 0],$$

so the cryptosystem is not perfectly secret.



(d) False: The keys are equiprobable in this example.

(e) True: This is Corollary 3.13.

Quiz on Rest of Sheet 3

(a) If K is chosen equiprobably from $\mathcal{K}$ then $H(K)$ is
(A) 0 (B) $\log_2 |\mathcal{K}|$ (C) $\log_2 |\mathcal{K}|!$ (D) need more information

(b) $\mathbb{P}[Y = y|X = x] = \mathbb{P}[Y = y]p_x$
(A) False (B) True

(c) Let $\mathcal{A} = \{\mathrm{a}, \ldots, \mathrm{z}\}$. The number of bijections $\mathcal{A} \to \mathcal{A}$ is
(A) 26 (B) 26×25 (C) $26!$ (D) 26^{26}

(d) A good way to break a substitution cipher by a chosen plaintext attack is frequency analysis.
(A) False (B) True

(e) The sequence 00101110010111 . . . of period 7 is the output of an LFSR of width 3.
(A) False (B) True

(f) The sequence 00101000001001 could be part of the output of an LFSR of width 5.
(A) False (B) True

Quiz on Rest of Sheet 3

(a) If K is chosen equiprobably from $\mathcal{K}$ then $H(K)$ is
(A) 0 (B) $\log_2 |\mathcal{K}|$ (C) $\log_2 |\mathcal{K}|!$ (D) need more information

(b) $\mathbb{P}[Y = y|X = x] = \mathbb{P}[Y = y]p_x$
(A) False (B) True

(c) Let $\mathcal{A} = \{\mathrm{a}, \ldots, \mathrm{z}\}$. The number of bijections $\mathcal{A} \to \mathcal{A}$ is
(A) 26 (B) 26×25 (C) 26! (D) 26^{26}

(d) A good way to break a substitution cipher by a chosen plaintext attack is frequency analysis.
(A) False (B) True

(e) The sequence 00101110010111 . . . of period 7 is the output of an LFSR of width 3.
(A) False (B) True

(f) The sequence 00101000001001 could be part of the output of an LFSR of width 5.
(A) False (B) True

Quiz on Rest of Sheet 3

(a) If K is chosen equiprobably from $\mathcal{K}$ then $H(K)$ is
(A) 0 (B) $\log_2 |\mathcal{K}|$ (C) $\log_2 |\mathcal{K}|!$ (D) need more information

(b) $\mathbb{P}[Y = y|X = x] = \mathbb{P}[Y = y]p_x$
(A) False (B) True

(c) Let $\mathcal{A} = \{\mathrm{a}, \ldots, \mathrm{z}\}$. The number of bijections $\mathcal{A} \to \mathcal{A}$ is
(A) 26 (B) 26×25 (C) $26!$ (D) 26^{26}

(d) A good way to break a substitution cipher by a chosen plaintext attack is frequency analysis.
(A) False (B) True

(e) The sequence 00101110010111 . . . of period 7 is the output of an LFSR of width 3.
(A) False (B) True

(f) The sequence 00101000001001 could be part of the output of an LFSR of width 5.
(A) False (B) True

Quiz on Rest of Sheet 3

(a) If K is chosen equiprobably from $\mathcal{K}$ then $H(K)$ is
(A) 0 (B) $\log_2 |\mathcal{K}|$ (C) $\log_2 |\mathcal{K}|!$ (D) need more information

(b) $\mathbb{P}[Y = y|X = x] = \mathbb{P}[Y = y]p_x$
(A) False (B) True

(c) Let $\mathcal{A} = \{\mathrm{a}, \ldots, \mathrm{z}\}$. The number of bijections $\mathcal{A} \to \mathcal{A}$ is
(A) 26 (B) 26×25 (C) 26! (D) 26^{26}

(d) A good way to break a substitution cipher by a chosen plaintext attack is frequency analysis.
(A) False (B) True

(e) The sequence 00101110010111 . . . of period 7 is the output of an LFSR of width 3.
(A) False (B) True

(f) The sequence 00101000001001 could be part of the output of an LFSR of width 5.
(A) False (B) True

Quiz on Rest of Sheet 3

(a) If K is chosen equiprobably from $\mathcal{K}$ then $H(K)$ is
(A) 0 (B) $\log_2 |\mathcal{K}|$ (C) $\log_2 |\mathcal{K}|!$ (D) need more information

(b) $\mathbb{P}[Y = y|X = x] = \mathbb{P}[Y = y]p_x$
(A) False (B) True

(c) Let $\mathcal{A} = \{\mathrm{a}, \ldots, \mathrm{z}\}$. The number of bijections $\mathcal{A} \to \mathcal{A}$ is
(A) 26 (B) 26×25 (C) 26! (D) 26^{26}

(d) A good way to break a substitution cipher by a chosen plaintext attack is frequency analysis.
(A) False (B) True

(e) The sequence 00101110010111 . . . of period 7 is the output of an LFSR of width 3.
(A) False (B) True

(f) The sequence 00101000001001 could be part of the output of an LFSR of width 5.
(A) False (B) True

Quiz on Rest of Sheet 3

(a) If K is chosen equiprobably from $\mathcal{K}$ then $H(K)$ is
(A) 0 (B) $\log_2 |\mathcal{K}|$ (C) $\log_2 |\mathcal{K}|!$ (D) need more information

(b) $\mathbb{P}[Y = y|X = x] = \mathbb{P}[Y = y]p_x$
(A) False (B) True

(c) Let $\mathcal{A} = \{\mathrm{a}, \ldots, \mathrm{z}\}$. The number of bijections $\mathcal{A} \to \mathcal{A}$ is
(A) 26 (B) 26×25 (C) $26!$ (D) 26^{26}

(d) A good way to break a substitution cipher by a chosen plaintext attack is frequency analysis.
(A) False (B) True

(e) The sequence 00101110010111 . . . of period 7 is the output of an LFSR of width 3.
(A) False (B) True

(f) The sequence 00101000001001 could be part of the output of an LFSR of width 5.
(A) False (B) True

Quiz on Rest of Sheet 3

(a) If K is chosen equiprobably from $\mathcal{K}$ then $H(K)$ is
(A) 0 (B) $\log_2 |\mathcal{K}|$ (C) $\log_2 |\mathcal{K}|!$ (D) need more information

(b) $\mathbb{P}[Y = y|X = x] = \mathbb{P}[Y = y]p_x$
(A) False (B) True

(c) Let $\mathcal{A} = \{\mathrm{a}, \ldots, \mathrm{z}\}$. The number of bijections $\mathcal{A} \to \mathcal{A}$ is
(A) 26 (B) 26×25 (C) $26!$ (D) 26^{26}

(d) A good way to break a substitution cipher by a chosen plaintext attack is frequency analysis.
(A) False (B) True

(e) The sequence 00101110010111 . . . of period 7 is the output of an LFSR of width 3.
(A) False (B) True

(f) The sequence 00101000001001 could be part of the output of an LFSR of width 5.
(A) False (B) True

False, since after 00000 the only possible next bit is 0 (by linearity). In fact the least width LFSR generating the sequence in (f) has width 7 and taps $\{0, 1, 2, 3, 4, 6\}$. (For interest only.)

§6 Pseudo-random Number Generation

Exercise 6.1

Let F be the LFSR of width 4 with taps $\{0, 1\}$ and period $15 = 2^4 - 1$, the maximum possible. The keystream for $k = (1, 1, 0, 0)$ is $(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0 \ldots)$
By taking the first 15 positions we get the generating cycle

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

(a) Find all positions t with $(k_t, k_{t+1}, k_{t+2}, k_{t+3}) = (0, 1, 1, 1)$.

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

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

(e) Repeat (d) changing $(0, 1, 1)$ to $(0, 1)$ and then $(0, 0)$. Explain!

LFSRs Generate Randomish Sequences

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 $0 \leq t < 2^\ell - 1$.

(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 $m \leq \ell$, 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 $(k_t, \ldots, k_{t+m-1}) = (0, 0, \ldots, 0) \in \mathbb{F}_2^m$.*

Please correct final sentence from lectures to 'there are $2^{\ell-m} - 1$ positions, corresponding to the $2^{\ell-m} - 1$ choices for $(b_1, \ldots, b_{\ell-m})$. (I wrote ℓ both times, and only corrected one.)

Example of Proposition 6.2

The LFSR of width 5 with taps $\{0, 2\}$ has maximum possible period $2^5 - 1$. The first 31 bits in the keystream for key $(0, 0, 0, 0, 1)$ are:

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

According to Proposition 6.2, given any non-zero $y \in \mathbb{F}_2^m$ for $m \leq 5$ there are precisely 2^{5-m} positions t such that $(k_t, \ldots, k_{t+m-1}) = y$. If $y = (0, \ldots, 0)$ there are $2^{5-m} - 1$ positions.

For example when $m = 3$ there should be $2^2 = 4$ positions for each of $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$, $(1, 1, 0)$, $(1, 0, 1)$ $\ldots$, $(1, 1, 1)$ and $2^2 - 1 = 3$ positions for $(0, 0, 0)$.

Proof for $(1, 0, 1)$: extend to $(1, 0, 1, b_1, b_2)$ in 4 ways, each extension appears in a unique position.

Example of Proposition 6.2

The LFSR of width 5 with taps $\{0, 2\}$ has maximum possible period $2^5 - 1$. The first 31 bits in the keystream for key $(0, 0, 0, 0, 1)$ are:

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

According to Proposition 6.2, given any non-zero $y \in \mathbb{F}_2^m$ for $m \leq 5$ there are precisely 2^{5-m} positions t such that $(k_t, \ldots, k_{t+m-1}) = y$. If $y = (0, \ldots, 0)$ there are $2^{5-m} - 1$ positions.

For example when $m = 3$ there should be $2^2 = 4$ positions for each of $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$, $(1, 1, 0)$, $(1, 0, 1)$ $\ldots$, $(1, 1, 1)$ and $2^2 - 1 = 3$ positions for $(0, 0, 0)$.

Proof for $(1, 0, 1)$: extend to $(1, 0, 1, b_1, b_2)$ in 4 ways, each extension appears in a unique position.

Example of Proposition 6.2

The LFSR of width 5 with taps $\{0, 2\}$ has maximum possible period $2^5 - 1$. The first 31 bits in the keystream for key $(0, 0, 0, 0, 1)$ are:

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

According to Proposition 6.2, given any non-zero $y \in \mathbb{F}_2^m$ for $m \leq 5$ there are precisely 2^{5-m} positions t such that $(k_t, \ldots, k_{t+m-1}) = y$. If $y = (0, \ldots, 0)$ there are $2^{5-m} - 1$ positions.

For example when $m = 3$ there should be $2^2 = 4$ positions for each of $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$, $(1, 1, 0)$, $(1, 0, 1)$ $\ldots$, $(1, 1, 1)$ and $2^2 - 1 = 3$ positions for $(0, 0, 0)$.

Proof for $(1, 0, 1)$: extend to $(1, 0, 1, b_1, b_2)$ in 4 ways, each extension appears in a unique position.

Example of Proposition 6.2

The LFSR of width 5 with taps $\{0, 2\}$ has maximum possible period $2^5 - 1$. The first 31 bits in the keystream for key $(0, 0, 0, 0, 1)$ are:

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

According to Proposition 6.2, given any non-zero $y \in \mathbb{F}_2^m$ for $m \leq 5$ there are precisely 2^{5-m} positions t such that $(k_t, \ldots, k_{t+m-1}) = y$. If $y = (0, \ldots, 0)$ there are $2^{5-m} - 1$ positions.

For example when $m = 3$ there should be $2^2 = 4$ positions for each of $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$, $(1, 1, 0)$, $(1, 0, 1)$ $\ldots$, $(1, 1, 1)$ and $2^2 - 1 = 3$ positions for $(0, 0, 0)$.

Proof for $(1, 0, 1)$: extend to $(1, 0, 1, b_1, b_2)$ in 4 ways, each extension appears in a unique position.

Example of Proposition 6.2

The LFSR of width 5 with taps $\{0, 2\}$ has maximum possible period $2^5 - 1$. The first 31 bits in the keystream for key $(0, 0, 0, 0, 1)$ are:

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

According to Proposition 6.2, given any non-zero $y \in \mathbb{F}_2^m$ for $m \leq 5$ there are precisely 2^{5-m} positions t such that $(k_t, \ldots, k_{t+m-1}) = y$. If $y = (0, \ldots, 0)$ there are $2^{5-m} - 1$ positions.

For example when $m = 3$ there should be $2^2 = 4$ positions for each of $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$, $(1, 1, 0)$, $(1, 0, 1)$ $\ldots$, $(1, 1, 1)$ and $2^2 - 1 = 3$ positions for $(0, 0, 0)$.

Proof for $(1, 0, 1)$: extend to $(1, 0, 1, b_1, b_2)$ in 4 ways, each extension appears in a unique position.

Experiment

Exercise 6.3

Write down a sequence of 33 bits, fairly quickly, but trying to make it seem random. Count the number of 0s and the number of 1s. Now count the number of adjacent pairs 00, 01, 10, 11. Does your sequence still seem random?

Monobit Test

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

(b) Show that the χ^2 statistic with (a) as null hypothesis is $(M_0 - M_1)^2/n$.

(c) A sequence with $n = 100$ is observed to have 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 $\mathbb{P}[Z^2 \geq 6.635] \approx 0.01$.]

(d) The 'monobit test' in the 2001 version of FIPS 140-2 required that $9725 < M_0 < 10275$ when $n = 20000$. This requirement was withdrawn in 2002. Suggest a possible reason for this change.

Correlation

Another interesting measure of randomness is the degree to which a sequence is correlated with a shift of itself.

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

$$n_{\text{same}} = \left|\{i : x_i = y_i\}\right|$$
$$n_{\text{diff}} = \left|\{i : x_i \neq y_i\}\right|.$$

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

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. Why is there no need to specify the key?

Autocorrelation for LFSRs

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

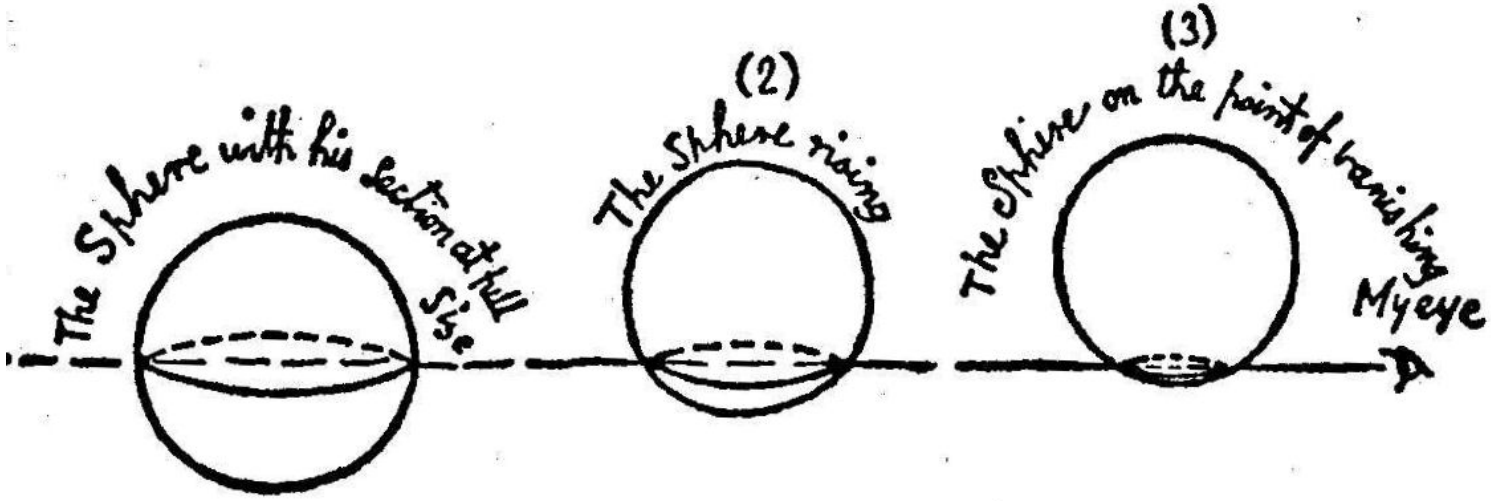
Race Equality Survey

- This survey will be invaluable in helping us understand your experiences of studying here, and identify issues you/your fellow students may be facing.
- On the back on the survey, we will develop a 4-year action plan which we will share with you.
- It is important that ALL STUDENTS from ALL BACKGROUNDS complete the survey, including those who don't identify as members of ethnic minority groups.
- Search 'race equality survey rhul' on Google.
- £1 donation for each survey completed to your choice of
  - The Sickle Cell Society
  - African Caribbean Careers & Employment Support Services UK (Access UK)
  - Rethink Mental Illness
  - UK Black Pride
- Harvard Project Implicit: `implicit.harvard.edu`

Flatland: a Romance of Many Dimensions

(Or, a Geometric Satire on Victorian Values.)

`http://www.gutenberg.org/ebooks/97`. Unfortunately this is missing the illustrations, which add a lot to the charm. Here is one from near the end of the book, when the Sphere visits Flatland.



Quiz on Random Sequences

Let $(B_0, B_1, \ldots, B_{31})$ be a random cyclic sequence of 32 bits.

- How many 10s do you expect to see on average? (Allow wrap around so if $B_{31} = 1$ and $B_0 = 0$, this counts as a 10.)

  (A) 4 (B) 8 (C) 16 (D) 24

- How many 11s do you expect to see on average?

  (A) 4 (B) 8 (C) 16 (D) 24

- What is the probability that 10 occurs before 11, assuming at least one occurs?

  (A) $< \frac{1}{2}$ (B) $\frac{1}{2}$ (C) $> \frac{1}{2}$ (D) about $\frac{2}{3}$

- What is the probability that 01 occurs before 11, assuming at least one occurs?

  (A) $< \frac{1}{2}$ (B) $\frac{1}{2}$ (C) $> \frac{1}{2}$ (D) about $\frac{2}{3}$

Quiz on Random Sequences

Let $(B_0, B_1, \ldots, B_{31})$ be a random cyclic sequence of 32 bits.

- How many 10s do you expect to see on average? (Allow wrap around so if $B_{31} = 1$ and $B_0 = 0$, this counts as a 10.)

  (A) 4 (B) 8 (C) 16 (D) 24

- How many 11s do you expect to see on average?

  (A) 4 (B) 8 (C) 16 (D) 24

- What is the probability that 10 occurs before 11, assuming at least one occurs?

  (A) $< \frac{1}{2}$ (B) $\frac{1}{2}$ (C) $> \frac{1}{2}$ (D) about $\frac{2}{3}$

- What is the probability that 01 occurs before 11, assuming at least one occurs?

  (A) $< \frac{1}{2}$ (B) $\frac{1}{2}$ (C) $> \frac{1}{2}$ (D) about $\frac{2}{3}$

Quiz on Random Sequences

Let $(B_0, B_1, \ldots, B_{31})$ be a random cyclic sequence of 32 bits.

- How many 10s do you expect to see on average? (Allow wrap around so if $B_{31} = 1$ and $B_0 = 0$, this counts as a 10.)

  (A) 4 (B) 8 (C) 16 (D) 24

- How many 11s do you expect to see on average?

  (A) 4 (B) 8 (C) 16 (D) 24

- What is the probability that 10 occurs before 11, assuming at least one occurs?

  (A) $< \frac{1}{2}$ (B) $\frac{1}{2}$ (C) $> \frac{1}{2}$ (D) about $\frac{2}{3}$

- What is the probability that 01 occurs before 11, assuming at least one occurs?

  (A) $< \frac{1}{2}$ (B) $\frac{1}{2}$ (C) $> \frac{1}{2}$ (D) about $\frac{2}{3}$

Quiz on Random Sequences

Let $(B_0, B_1, \ldots, B_{31})$ be a random cyclic sequence of 32 bits.

- How many 10s do you expect to see on average? (Allow wrap around so if $B_{31} = 1$ and $B_0 = 0$, this counts as a 10.)

  (A) 4 (B) 8 (C) 16 (D) 24

- How many 11s do you expect to see on average?

  (A) 4 (B) 8 (C) 16 (D) 24

- What is the probability that 10 occurs before 11, assuming at least one occurs?

  (A) $< \frac{1}{2}$ (B) $\frac{1}{2}$ (C) $> \frac{1}{2}$ (D) about $\frac{2}{3}$

- What is the probability that 01 occurs before 11, assuming at least one occurs?

  (A) $< \frac{1}{2}$ (B) $\frac{1}{2}$ (C) $> \frac{1}{2}$ (D) about $\frac{2}{3}$

Quiz on Random Sequences

Let $(B_0, B_1, \ldots, B_{31})$ be a random cyclic sequence of 32 bits.

- How many 10s do you expect to see on average? (Allow wrap around so if $B_{31} = 1$ and $B_0 = 0$, this counts as a 10.)

  (A) 4 (B) 8 (C) 16 (D) 24

- How many 11s do you expect to see on average?

  (A) 4 (B) 8 (C) 16 (D) 24

- What is the probability that 10 occurs before 11, assuming at least one occurs?

  (A) $< \frac{1}{2}$ (B) $\frac{1}{2}$ (C) $> \frac{1}{2}$ (D) about $\frac{2}{3}$

- What is the probability that 01 occurs before 11, assuming at least one occurs?

  (A) $< \frac{1}{2}$ (B) $\frac{1}{2}$ (C) $> \frac{1}{2}$ (D) about $\frac{2}{3}$

Quiz on Random Sequences

Let $(B_0, B_1, \ldots, B_{31})$ be a random cyclic sequence of 32 bits.

- How many 10s do you expect to see on average? (Allow wrap around so if $B_{31} = 1$ and $B_0 = 0$, this counts as a 10.)

  (A) 4 (B) 8 (C) 16 (D) 24

- How many 11s do you expect to see on average?

  (A) 4 (B) 8 (C) 16 (D) 24

- What is the probability that 10 occurs before 11, assuming at least one occurs?

  (A) $< \frac{1}{2}$ (B) $\frac{1}{2}$ (C) $> \frac{1}{2}$ (D) about $\frac{2}{3}$

- What is the probability that 01 occurs before 11, assuming at least one occurs?

  (A) $< \frac{1}{2}$ (B) $\frac{1}{2}$ (C) $> \frac{1}{2}$ (D) about $\frac{2}{3}$

§7 Non-linear Stream Ciphers

Mathematically an LFSR of width ℓ is a function $F : \mathbb{F}_2^\ell \to \mathbb{F}_2^\ell$. The domain $\mathbb{F}_2^\ell$ corresponds to the ℓ bits stored in the registers: we call these bits the *internal state* of the LFSR. It is updated by the linear function F.

The cryptosystem in Definition 5.6(b) is trivially broken by a known plaintext/ciphertext attack (see bottom page 27) because every bit of internal state appears, unmodified, in the keystream.

Sum of LFSRs

Example 7.1

Totally Trusted Transmission Technologies thinks that taking the sum of the keystreams for two LFSRs with different keys should obscure the keys and give a cryptographically strong sequence.

- Let F be the LFSR of width 3 with taps $\{0, 1\}$.
- Let F' be the LFSR of width 4 with taps $\{0, 3\}$.

The periods of F and F' are 7 and 15, maximum possible for their widths.

Example 7.1 [continued]

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

k_i	0,	0,	0,	1,	1,	1,	1,	0,	1,	0,	1,	1,	0,	0,	1,	0,	0,	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
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

TTTT are soon informed by an irate customer that $(u_0, u_1, u_2, \ldots)$ is generated by F'.

Quiz: which key for F' gives $(u_0, u_1, u_2, \ldots)$?

(A) 0001 (B) 1001 (C) 1000 (D) 1010

Quiz: can the keys k and k' be recovered from $(u_0, u_1, \ldots, u_{19})$?

(A) No (B) Yes

If so, explain how; if not, will this deter attackers?

Example 7.1 [continued]

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

k_i	0,	0,	0,	1,	1,	1,	1,	0,	1,	0,	1,	1,	0,	0,	1,	0,	0,	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
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

TTTT are soon informed by an irate customer that $(u_0, u_1, u_2, \ldots)$ is generated by F'.

Quiz: which key for F' gives $(u_0, u_1, u_2, \ldots)$?

(A) 0001 (B) 1001 (C) 1000 (D) 1010

Quiz: can the keys k and k' be recovered from $(u_0, u_1, \ldots, u_{19})$?

(A) No (B) Yes

If so, explain how; if not, will this deter attackers?

Example 7.1 [continued]

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

k_i	0,	0,	0,	1,	1,	1,	1,	0,	1,	0,	1,	1,	0,	0,	1,	0,	0,	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
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

TTTT are soon informed by an irate customer that $(u_0, u_1, u_2, \ldots)$ is generated by F'.

Quiz: which key for F' gives $(u_0, u_1, u_2, \ldots)$?

(A) 0001 (B) 1001 (C) 1000 (D) 1010

Quiz: can the keys k and k' be recovered from $(u_0, u_1, \ldots, u_{19})$?

(A) No (B) Yes

If so, explain how; if not, will this deter attackers?

Example 7.1 [continued]

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

k_i	0,	0,	0,	1,	1,	1,	1,	0,	1,	0,	1,	1,	0,	0,	1,	0,	0,	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
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

TTTT are soon informed by an irate customer that $(u_0, u_1, u_2, \ldots)$ is generated by F'.

Quiz: which key for F' gives $(u_0, u_1, u_2, \ldots)$?

(A) 0001 (B) 1001 (C) 1000 (D) 1010

Quiz: can the keys k and k' be recovered from $(u_0, u_1, \ldots, u_{19})$?

(A) No (B) Yes

If so, explain how; if not, will this deter attackers?

Example 7.1 [continued]

(b) TTTT decides their error was to use the same LFSR twice. The first 20 bits in the keystreams for F and F' with keys $k = (0, 0, 1)$ and $k' = (1, 0, 0, 0)$ and their sum $(u_0, u_1, \ldots, u_{19})$ are:

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
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

Quiz: what is the period of $(u_0, u_1, u_2, \ldots)$?

(A) 7 (B) 15 (C) 105 (D) need more info

The linear algebra method from Example 5.13 or Question 2 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 $\{0, 1, 5, 6\}$.

Exercise: check this holds for the first 20 bits.

Example 7.1 [continued]

(b) TTTT decides their error was to use the same LFSR twice. The first 20 bits in the keystreams for F and F' with keys $k = (0, 0, 1)$ and $k' = (1, 0, 0, 0)$ and their sum $(u_0, u_1, \ldots, u_{19})$ are:

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
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

Quiz: what is the period of $(u_0, u_1, u_2, \ldots)$?

(A) 7 (B) 15 (C) 105 (D) need more info

The linear algebra method from Example 5.13 or Question 2 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 $\{0, 1, 5, 6\}$.

Exercise: check this holds for the first 20 bits.

Geffe Generator

Example 7.2

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 7.2 [continued]

For example, if F and F' and their keystreams are as in Example 7.1 and G is the LFSR of width 4 with taps $\{0, 1\}$ and $(c_0, c_1, c_2, c_3) = (0, 0, 0, 1)$ then

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
c_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

Quiz: What is $\mathbb{P}[k_i = u_i]$?

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

Example 7.2 [continued]

For example, if F and F' and their keystreams are as in Example 7.1 and G is the LFSR of width 4 with taps $\{0, 1\}$ and $(c_0, c_1, c_2, c_3) = (0, 0, 0, 1)$ then

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
c_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

Quiz: What is $\mathbb{P}[k_i = u_i]$?

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

For instance, suppose we guess (wrongly) that $(k_0, k_1, k_2) = (1, 1, 0)$. The correlation between the implied keystream $(v_0, v_1, v_2, \ldots, v_{19})$ and $(u_0, u_1, \ldots, u_{19})$ is $(7 - 13)/20 = -\frac{3}{10}$.

v_i	1,	1,	0,	0,	1,	0,	1,	1,	1,	0,	0,	1,	0,	1,	1,	1,	0,	0,	1,	0
u_i	0,	0,	1,	0,	1,	1,	1,	1,	0,	1,	0,	1,	1,	0,	0,	0,	1,	0,	0,	1

Correlation Attack on Geffe Generator

Attack 7.3

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 $(k_0, \ldots, k_{\ell-1}) = (v_0, \ldots, v_{\ell-1})$.

Exercise: is it better to guess the key for F or for F'?

Correlation Attack on Geffe Generator

Attack 7.3

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 $(k_0, \ldots, k_{\ell-1}) = (v_0, \ldots, v_{\ell-1})$.

Exercise: is it better to guess the key for F or for F'?

One can repeat Attack 7.3 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 on Sheet 7.)

Q-cipher

Exercise 7.4

Let x, y, z be independent unbiased bits. Find the correlation between $xy + z$ and x, and between $xy + z$ and z.

Q-cipher

Exercise 7.4

Let x, y, z be independent unbiased bits. Find the correlation between $xy + z$ and x, and between $xy + z$ and z.

Alternative: This morning we found $\mathbb{P}[xy = 0] = \frac{3}{4}$. Hence

$$\operatorname{corr}(xy, 0) = \mathbb{P}[xy = 0] - \mathbb{P}[xy \neq 0] = \tfrac{3}{4} - \tfrac{1}{4} = \tfrac{1}{2}.$$

Adding z (same to both sides ...) shows that

$$\operatorname{corr}(xy + z, z) = \operatorname{corr}(xy, 0) = \tfrac{1}{2}.$$

Example 7.5

Let F be the LFSR of width 5 with taps $\{0\}$. The keystream of F with key $(k_0, k_1, k_2, k_3, k_4)$ is simply $(k_0, k_1, k_2, k_3, k_4, k_0, k_1, \ldots)$.

Define $Q(x_0, x_1, x_2, x_3, x_4) = (x_1, x_2, x_3, x_4, x_0 + x_1 x_2)$.

Exercise. Prove that Q is invertible.

Example 7.5 [continued]

Define the *Q-state stream* for key $(k_0, k_1, k_2, k_3, k_4)$ by

$$q_s = Q^s(k_0, k_1, k_2, k_3, k_4)_0 \quad \text{for } s \in \mathbb{N}_0$$

For example, since 00011 is in the cycle $00011 \to 00110 \to 01100 \to 11001 \to \ldots \to 11100 \to 110000 \to 10001 \to 00011$ of Q of length 21, its Q-state stream is

q_s	0	0	0	1	1	0	0	1	1	1	0	1	0	1	1	0	1	1	1	1	1
	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0

of period 21.

Since Q is invertible, any 5 consecutive bits in the Q-state stream determine the internal state and hence the key. For example, if $(q_7, q_8, q_9, q_{10}, q_{11}) = (1, 1, 0, 1, 1)$ then working back through the state stream above shows that the key is $(0, 1, 1, 1, 0)$.

No problem sheet this week. (Part B notes refer to Question 1 on Sheet 7: this should have been Question 2(b) on Sheet 6.)

Example 7.5 [continued]

We avoid this weakness by taking the bits in even-numbered positions in the state stream to define the *Q-keystream*. For example, the Q-keystreams for keys $(0,0,0,1,1)$ and $(1,1,1,0,1)$ are **[Correction: please use u_s not k_s for keystream, to avoid a notational clash: e.g. $(u_0,u_1,u_2,u_3)=(k_0,k_2,k_4,k_1+k_2k_3)$]**

u_s	0	0	1	0	1	0	0	1	1	1	1	0	1	0	1	1	1	1	0	1	1
u'_s	1	1	1	1	0	1	1	0	0	1	0	1	0	0	1	1	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	0
	0	2	4	6	8	0	2	4	6	8	0	2	4	6	8	0	2	4	6	8	0

where the bottom row shows the positions in the state stream.

Exercise 7.6

(a) Check the Q-keystream for $(1,1,1,0,1)$ is as claimed. [*Hint:* you can use the Q-state stream for $(0,0,0,1,1)$.]

(b) Why is the period of both keystreams 21?

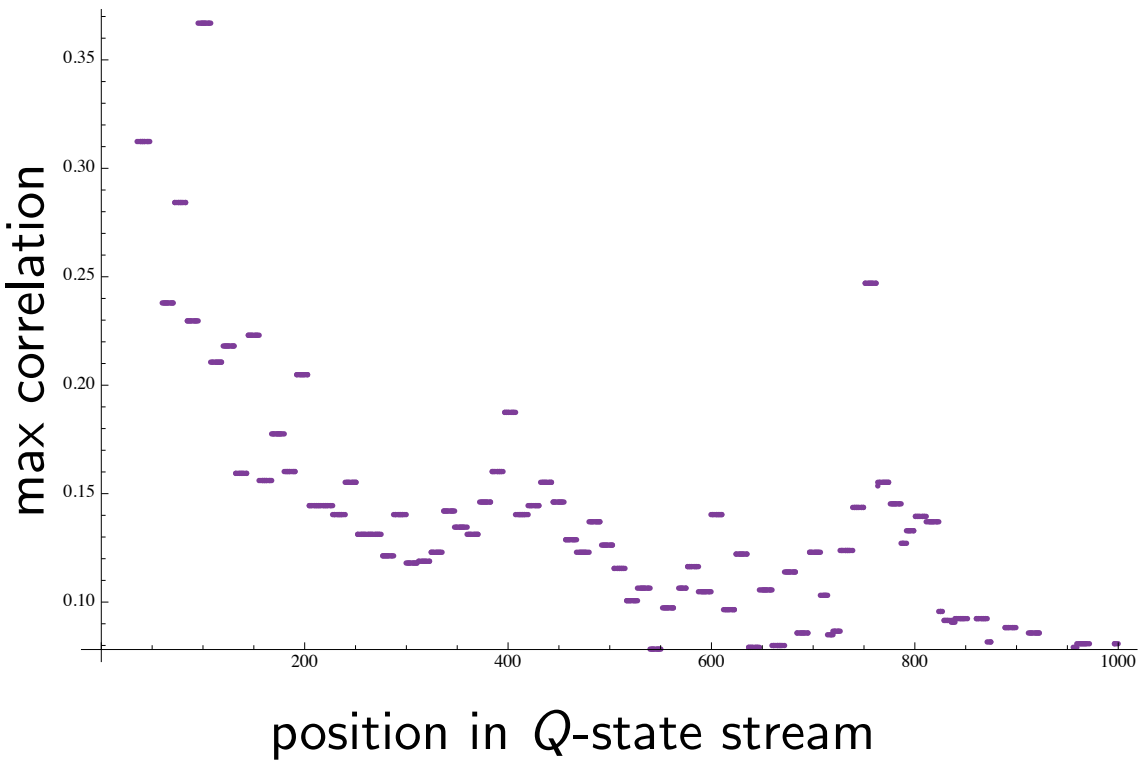
(c) Show by example that 5 consecutive bits in the Q-keystream do not, in general, determine the key.

Exercise 7.7

Suppose we take $\ell = 12$ and, since the first few bits in the Q-keystream are noticeably less random, drop the first 200 bits. For $200 \leq s \leq 1000$, the maximum correlation between a bit q_s of the Q-state stream and one of the bits k_j of the key is

$$\frac{1012}{2^{12}} = \frac{253}{2^{10}} \approx \frac{1}{4};$$

with equality when $(s, j) \in \{(751, 0), (752, 1), \ldots, (762, 11)\}$.



Exercise 7.7

Suppose we take $\ell = 12$ and, since the first few bits in the Q-keystream are noticeably less random, drop the first 200 bits. For $200 \leq s \leq 1000$, the maximum correlation between a bit q_s of the Q-state stream and one of the bits k_j of the key is

$$\frac{1012}{2^{12}} = \frac{253}{2^{10}} \approx \frac{1}{4};$$

with equality when $(s, j) \in \{(751, 0), (752, 1), \ldots, (762, 11)\}$.

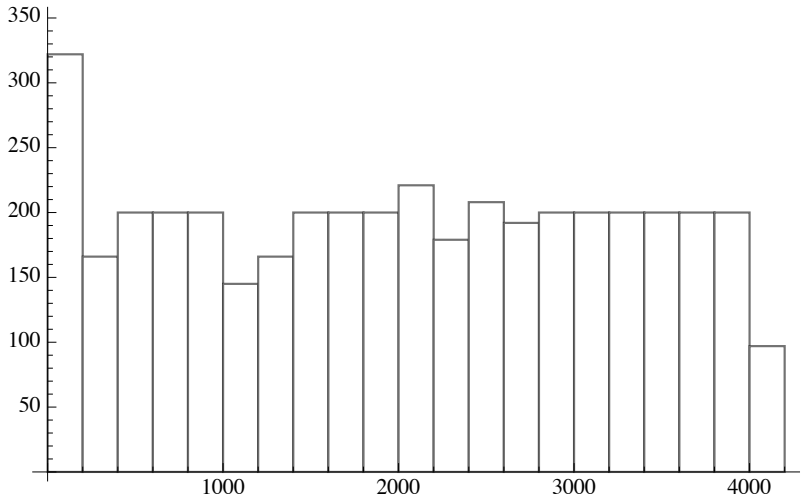
Note that $q_{752} = u_{376}$, and so on, up to $q_{762} = u_{381}$. You know $(u_{376}, u_{377}, u_{377}, u_{378}, u_{379}, u_{380}, u_{381})$ and have to guess the key. How should the search be organized?

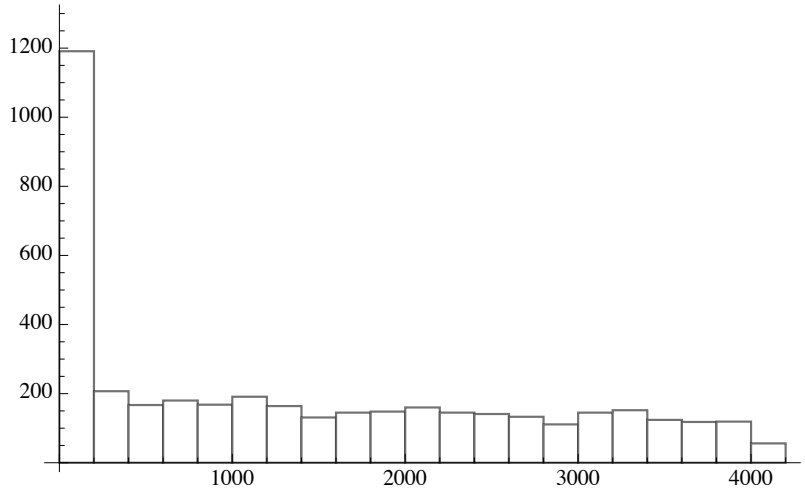
Correlation attack on Q-cipher

A naive search going through all 2^{12} keys in lexicographic order requires on average 2018.8 guesses. (The code is online at `https://repl.it/NE32/3`.) Ordering the keys so that the 64 keys of the form

$$(\star, u_{376}, \star, u_{377}, \star, u_{378}, \star, u_{379}, \star, u_{380}, \star, u_{381})$$

are tried first, then the 64×6 keys differing in a single odd numbered position, and so on, reduces the mean number of guesses to 1425.0. The histograms below show the distribution of the number of guesses for the naive search (left) versus the organized search (right).





Entropy Argument

Remark 7.8

This improvement can be predicted theoretically. The correlation between q_{752} and k_1 is $\mathbb{P}[q_{752} = k_1] - \mathbb{P}[q_{752} \neq k_1]$, or equivalently, $2\mathbb{P}[q_{752} = k_1] - 1$. Therefore $\mathbb{P}[q_{752} = k_1] \approx \frac{1}{2}(1 + \frac{1}{4}) \approx \frac{5}{8}$, and similarly, for $\mathbb{P}[q_{754} = k_3]$, and so on. Therefore the entropy in the key is

$$6 \times f(\tfrac{1}{2}) + 6 \times f(\tfrac{5}{8}) \approx 6 \times 1 + 6 \times 0.9544 = 11.7266$$

where $f(p) = -p \log_2 p - (1 - p) \log_2 p$, as in Example 4.2(1), gives the entropy for each bit. Since on average we find the key halfway through the search, this predicts that $2^{11.7266-1} \approx 1694.45$ guesses (or 'questions about the key') will be required, versus $2^{12-1} = 2048$ for a naive search. In practice the attack is better than this argument predicts.

Trivium

Example 7.9 (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

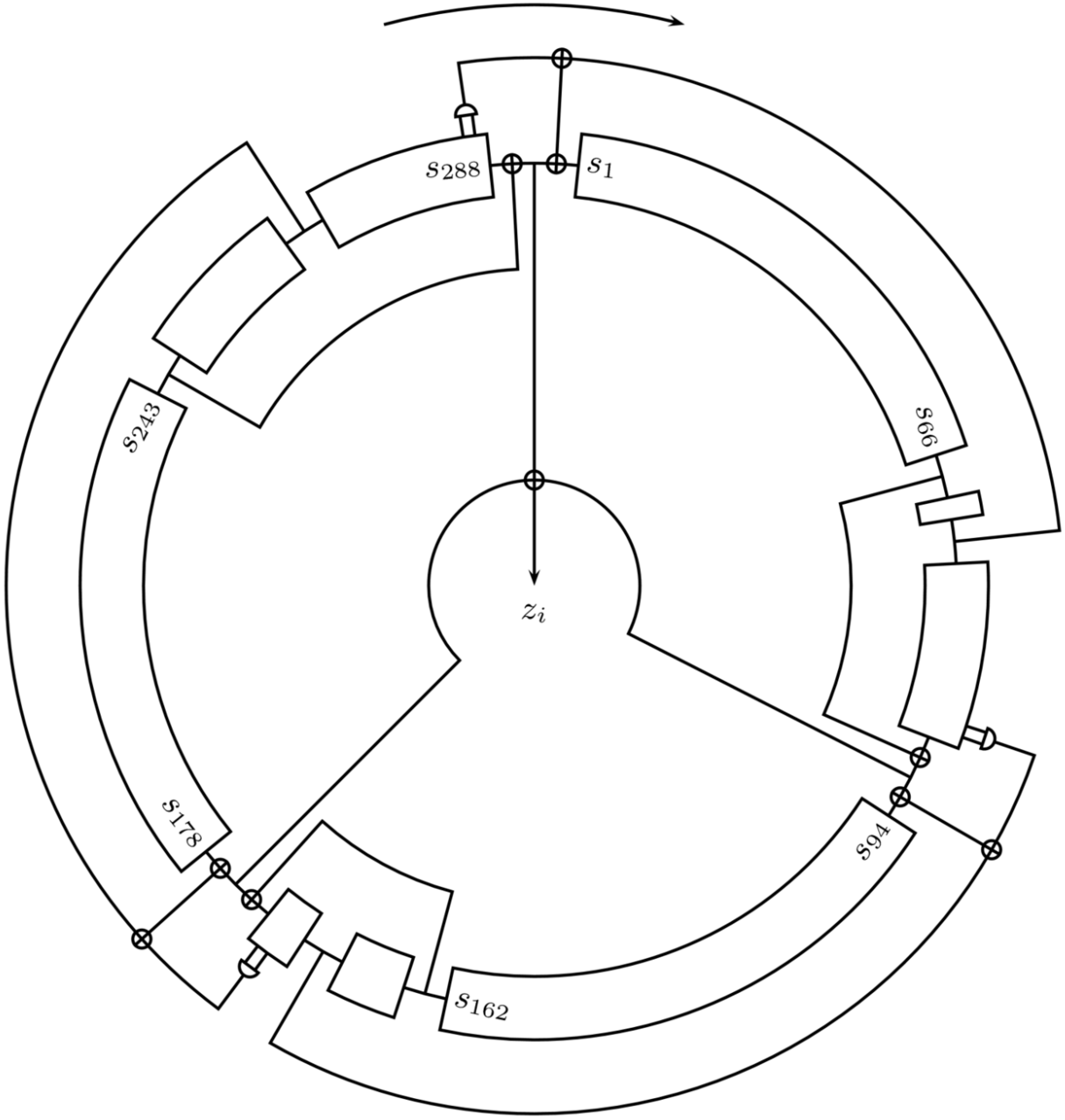
$$k_s = x_0 + x_{27} + x'_0 + x'_{15} + x''_0 + x''_{45}.$$

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 Diagram



Quiz on Sheet 5

Under the null hypothesis, a statistic x has the χ^2-distribution with 3 degrees of freedom. If $X \sim \chi^2_3$ then $\mathbb{P}[X > 0.216] \approx 0.975$, $\mathbb{P}[X > 1] \approx 0.198$ and $\mathbb{P}[X > 7.378] \approx 0.025$.

(a) If $x = 8.3$ then the null hypothesis should be rejected.
(A) False (B) True

(b) If $x = 0.15$ then the null hypothesis should be rejected.
(A) False (B) True

(c) If $x = 0.001$ then one might suspect someone has cheated.
(A) False (B) True

(d) If $x = 1$ the null hypothesis is true with probability about $\frac{4}{5}$.
(A) False (B) True

Quiz on Sheet 5

Under the null hypothesis, a statistic x has the χ^2-distribution with 3 degrees of freedom. If $X \sim \chi^2_3$ then $\mathbb{P}[X > 0.216] \approx 0.975$, $\mathbb{P}[X > 1] \approx 0.198$ and $\mathbb{P}[X > 7.378] \approx 0.025$.

(a) If $x = 8.3$ then the null hypothesis should be rejected.
(A) False (B) True

(b) If $x = 0.15$ then the null hypothesis should be rejected.
(A) False (B) True

(c) If $x = 0.001$ then one might suspect someone has cheated.
(A) False (B) True

(d) If $x = 1$ the null hypothesis is true with probability about $\frac{4}{5}$.
(A) False (B) True

Quiz on Sheet 5

Under the null hypothesis, a statistic x has the χ^2-distribution with 3 degrees of freedom. If $X \sim \chi^2_3$ then $\mathbb{P}[X > 0.216] \approx 0.975$, $\mathbb{P}[X > 1] \approx 0.198$ and $\mathbb{P}[X > 7.378] \approx 0.025$.

(a) If $x = 8.3$ then the null hypothesis should be rejected.
(A) False (B) True

(b) If $x = 0.15$ then the null hypothesis should be rejected.
(A) False (B) True

(c) If $x = 0.001$ then one might suspect someone has cheated.
(A) False (B) True

(d) If $x = 1$ the null hypothesis is true with probability about $\frac{4}{5}$.
(A) False (B) True

Quiz on Sheet 5

Under the null hypothesis, a statistic x has the χ^2-distribution with 3 degrees of freedom. If $X \sim \chi^2_3$ then $\mathbb{P}[X > 0.216] \approx 0.975$, $\mathbb{P}[X > 1] \approx 0.198$ and $\mathbb{P}[X > 7.378] \approx 0.025$.

(a) If $x = 8.3$ then the null hypothesis should be rejected.
(A) False (B) True

(b) If $x = 0.15$ then the null hypothesis should be rejected.
(A) False (B) True

(c) If $x = 0.001$ then one might suspect someone has cheated.
(A) False (B) True

(d) If $x = 1$ the null hypothesis is true with probability about $\frac{4}{5}$.
(A) False (B) True

Quiz on Sheet 5

Under the null hypothesis, a statistic x has the χ^2-distribution with 3 degrees of freedom. If $X \sim \chi^2_3$ then $\mathbb{P}[X > 0.216] \approx 0.975$, $\mathbb{P}[X > 1] \approx 0.198$ and $\mathbb{P}[X > 7.378] \approx 0.025$.

(a) If $x = 8.3$ then the null hypothesis should be rejected.
(A) False (B) True

(b) If $x = 0.15$ then the null hypothesis should be rejected.
(A) False (B) True

(c) If $x = 0.001$ then one might suspect someone has cheated.
(A) False (B) True

(d) If $x = 1$ the null hypothesis is true with probability about $\frac{4}{5}$.
(A) False (B) True

Quiz on Sheet 5

Under the null hypothesis, a statistic x has the χ^2-distribution with 3 degrees of freedom. If $X \sim \chi^2_3$ then $\mathbb{P}[X > 0.216] \approx 0.975$, $\mathbb{P}[X > 1] \approx 0.198$ and $\mathbb{P}[X > 7.378] \approx 0.025$.

(a) If $x = 8.3$ then the null hypothesis should be rejected.
(A) False (B) True

(b) If $x = 0.15$ then the null hypothesis should be rejected.
(A) False (B) True

(c) If $x = 0.001$ then one might suspect someone has cheated.
(A) False (B) True

(d) If $x = 1$ the null hypothesis is true with probability about $\frac{4}{5}$.
(A) False (B) True

For (d), the statement really makes no sense: the probability distribution is on x *assuming the null hypothesis*. There is no probability distribution on the null hypothesis itself.

(More broadly, the absence of evidence against the null hypothesis should not be taken as evidence for it.)

End of Part B Quiz

Let $\mathcal{K}$ and $\mathcal{K}'$ be keyspaces.

(a) An attack exhausting over all keys in $\mathcal{K} \times \mathcal{K}'$ requires on average how many guesses:

(A) $|\mathcal{K}| + |\mathcal{K}'|$ (B) $\frac{|\mathcal{K}|+|\mathcal{K}'|}{2}$ (C) $|\mathcal{K}||\mathcal{K}'|$ (D) $\frac{|\mathcal{K}||\mathcal{K}'|}{2}$

(b) The Geffe attack by correlations finds $k \in \mathcal{K} = \mathbb{F}_2^\ell$ and then, once k is known, finds $k' \in \mathcal{K}' = \mathbb{F}_2^{\ell'}$. On average how many guesses:

(A) $|\mathcal{K}| + |\mathcal{K}'|$ (B) $\frac{|\mathcal{K}|+|\mathcal{K}'|}{2}$ (C) $|\mathcal{K}||\mathcal{K}'|$ (D) $\frac{|\mathcal{K}||\mathcal{K}'|}{2}$

End of Part B Quiz

Let $\mathcal{K}$ and $\mathcal{K}'$ be keyspaces.

(a) An attack exhausting over all keys in $\mathcal{K} \times \mathcal{K}'$ requires on average how many guesses:

(A) $|\mathcal{K}| + |\mathcal{K}'|$ (B) $\frac{|\mathcal{K}|+|\mathcal{K}'|}{2}$ (C) $|\mathcal{K}||\mathcal{K}'|$ (D) $\frac{|\mathcal{K}||\mathcal{K}'|}{2}$

(b) The Geffe attack by correlations finds $k \in \mathcal{K} = \mathbb{F}_2^\ell$ and then, once k is known, finds $k' \in \mathcal{K}' = \mathbb{F}_2^{\ell'}$. On average how many guesses:

(A) $|\mathcal{K}| + |\mathcal{K}'|$ (B) $\frac{|\mathcal{K}|+|\mathcal{K}'|}{2}$ (C) $|\mathcal{K}||\mathcal{K}'|$ (D) $\frac{|\mathcal{K}||\mathcal{K}'|}{2}$

End of Part B Quiz

Let F be an invertible LFSR of width ℓ. As in Definition 5.6(b), a plaintext $(x_0, \ldots, x_{n-1})$ is encrypted by a key $(k_0, \ldots, k_{\ell-1})$ by adding the keystream $(k_0, \ldots, k_{n-1})$.

(c) ℓ consecutive bits from a plaintext/ciphertext pair determine the key

(A) False (B) True

(d) any ℓ bits of keystream determine the key

(A) False (B) True

(e) dropping every other bit of the keystream, to get $k_0, k_2, k_4, \ldots$ would significantly improve the LFSR cryptosystem.

(A) False (B) True

End of Part B Quiz

Let F be an invertible LFSR of width ℓ. As in Definition 5.6(b), a plaintext $(x_0, \ldots, x_{n-1})$ is encrypted by a key $(k_0, \ldots, k_{\ell-1})$ by adding the keystream $(k_0, \ldots, k_{n-1})$.

(c) ℓ consecutive bits from a plaintext/ciphertext pair determine the key

(A) False (B) True

(d) any ℓ bits of keystream determine the key

(A) False (B) True

(e) dropping every other bit of the keystream, to get $k_0, k_2, k_4, \ldots$ would significantly improve the LFSR cryptosystem.

(A) False (B) True

End of Part B Quiz

Let F be an invertible LFSR of width ℓ. As in Definition 5.6(b), a plaintext $(x_0, \ldots, x_{n-1})$ is encrypted by a key $(k_0, \ldots, k_{\ell-1})$ by adding the keystream $(k_0, \ldots, k_{n-1})$.

(c) ℓ consecutive bits from a plaintext/ciphertext pair determine the key

(A) False (B) True

(d) any ℓ bits of keystream determine the key

(A) False (B) True

(e) dropping every other bit of the keystream, to get $k_0, k_2, k_4, \ldots$ would significantly improve the LFSR cryptosystem.

(A) False (B) True

End of Part B Quiz

Let F be an invertible LFSR of width ℓ. As in Definition 5.6(b), a plaintext $(x_0, \ldots, x_{n-1})$ is encrypted by a key $(k_0, \ldots, k_{\ell-1})$ by adding the keystream $(k_0, \ldots, k_{n-1})$.

(c) ℓ consecutive bits from a plaintext/ciphertext pair determine the key

(A) False (B) True

(d) any ℓ bits of keystream determine the key

(A) False (B) True

(e) dropping every other bit of the keystream, to get $k_0, k_2, k_4, \ldots$ would significantly improve the LFSR cryptosystem.

(A) False (B) True

End of Part B Quiz

Let F be an invertible LFSR of width ℓ. As in Definition 5.6(b), a plaintext $(x_0, \ldots, x_{n-1})$ is encrypted by a key $(k_0, \ldots, k_{\ell-1})$ by adding the keystream $(k_0, \ldots, k_{n-1})$.

(c) ℓ consecutive bits from a plaintext/ciphertext pair determine the key

(A) False (B) True

(d) any ℓ bits of keystream determine the key

(A) False (B) True

(e) dropping every other bit of the keystream, to get $k_0, k_2, k_4, \ldots$ would significantly improve the LFSR cryptosystem.

(A) False (B) True

(e) is like Example 5.1: the modified keystream is still the keystream of an LFSR. If F has maximum period $2^\ell - 1$ then $k_0, k_2, k_4, \ldots$ is even generated by F. (The proof needs some finite field theory.)

Part C: Block ciphers

§8 Introduction to Block Ciphers and Feistel Networks

In stream ciphers a binary plaintext of arbitrary length n is encrypted by adding the first n bits of the keystream for the chosen key. In a block cipher of *block size* n, we also have $\mathcal{P} = \mathcal{C} = \mathbb{F}_2^n$, but the plaintext is typically mixed up with the key in more complicated ways.

Since $\mathcal{P} = \mathcal{C}$ each encryption function e_k for $k \in \mathcal{K}$ is bijective, and the cryptoscheme is determined by the encryption functions.

§8 Introduction to Block Ciphers and Feistel Networks

In stream ciphers a binary plaintext of arbitrary length n is encrypted by adding the first n bits of the keystream for the chosen key. In a block cipher of *block size* n, we also have $\mathcal{P} = \mathcal{C} = \mathbb{F}_2^n$, but the plaintext is typically mixed up with the key in more complicated ways.

Since $\mathcal{P} = \mathcal{C}$ each encryption function e_k for $k \in \mathcal{K}$ is bijective, and the cryptoscheme is determined by the encryption functions.

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 stream ciphers a binary plaintext of arbitrary length n is encrypted by adding the first n bits of the keystream for the chosen key. In a block cipher of *block size* n, we also have $\mathcal{P} = \mathcal{C} = \mathbb{F}_2^n$, but the plaintext is typically mixed up with the key in more complicated ways.

Since $\mathcal{P} = \mathcal{C}$ each encryption function e_k for $k \in \mathcal{K}$ is bijective, and the cryptoscheme is determined by the encryption functions.

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 $\mathbb{F}_2^\ell$.

Feistel Networks

Definition 8.2

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 8.3

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 8.4 (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 $x \mapsto S(x + k^{(i)})$. Denoting the output of round i by $(v^{(i)}, w^{(i)})$, the plaintext $(v, w) \in \mathbb{F}_2^{16}$ is encrypted to the cipher text $e_k\big((v, w)\big) = (v^{(4)}, w^{(4)})$ in three rounds:

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

Q-Block Cipher

Exercise 8.5

(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 $(v^{(3)}, w^{(3)})$ from the Q-block cipher. Show that she can determine $w^{(2)}$. What does she need to know to determine $v^{(2)}$?

DES (Data Encryption Standard)

DES is a Feistel block cipher of block size 64. The keyspace is $\mathbb{F}_2^{56}$ and each round key has 48 bits. The Feistel function $f : \mathbb{F}_2^{32} \to \mathbb{F}_2^{32}$ is defined in four steps using 8 functions $S_1, \ldots, S_8 : \mathbb{F}_2^6 \to \mathbb{F}_2^4$. Start with $w \in \mathbb{F}_2^{32}$ and a round key $k^{(i)} \in \mathbb{F}_2^{48}$.

(a) Expand w by a linear function (details omitted) to $w' \in \mathbb{F}_2^{48}$.

(b) Add the 48-bit round key to get $w' + k^{(i)}$.

(c) Let $w' + k^{(i)} = (y^{(1)}, \ldots, y^{(8)})$ where $y^{(i)} \in \mathbb{F}_2^6$. Let $z = \left(S_1(y^{(1)}), \ldots, S_8(y^{(8)})\right) \in \mathbb{F}_2^{32}$. *Confusion*: obscure relationship between plaintext and ciphertext.

(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 is Impressive, but Now Broken

No subexhaustive attacks on DES are known. But the relatively small keyspace $\mathbb{F}_2^{56}$ means that it cannot be considered secure.

- 1997: 140 days, distributed search on internet
- 1998: 9 days 'DES cracker' (special purpose) \$250000
- 2017: 6 days 'COPACOBONA' (35 FPGA's) \$10000

Roughly how many keys does COPACOBONA test in each second?

(A) 2^{32} (B) 2^{36} (C) 2^{37} (D) 2^{40}

Exercise 8.6

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

$$e_{(k,k')}(x) = e'_k\big(e_k(x)\big).$$

(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 COPACOBONA.)

(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 is Impressive, but Now Broken

No subexhaustive attacks on DES are known. But the relatively small keyspace $\mathbb{F}_2^{56}$ means that it cannot be considered secure.

- 1997: 140 days, distributed search on internet
- 1998: 9 days 'DES cracker' (special purpose) \$250000
- 2017: 6 days 'COPACOBONA' (35 FPGA's) \$10000

Roughly how many keys does COPACOBONA test in each second?

(A) 2^{32} (B) 2^{36} (C) 2^{37} (D) 2^{40}

Exercise 8.6

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

$$e_{(k,k')}(x) = e'_k\big(e_k(x)\big).$$

(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 COPACOBONA.)

(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 is Impressive, but Now Broken

No subexhaustive attacks on DES are known. But the relatively small keyspace $\mathbb{F}_2^{56}$ means that it cannot be considered secure.

- 1997: 140 days, distributed search on internet
- 1998: 9 days 'DES cracker' (special purpose) \$250000
- 2017: 6 days 'COPACOBONA' (35 FPGA's) \$10000

Roughly how many keys does COPACOBONA test in each second?

(A) 2^{32} (B) 2^{36} (C) 2^{37} (D) 2^{40}

Exercise 8.6

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

$$e_{(k,k')}(x) = e'_k\big(e_k(x)\big).$$

(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 COPACOBONA.)

(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 is Impressive, but Now Broken

No subexhaustive attacks on DES are known. But the relatively small keyspace $\mathbb{F}_2^{56}$ means that it cannot be considered secure.

- 1997: 140 days, distributed search on internet
- 1998: 9 days 'DES cracker' (special purpose) \$250000
- 2017: 6 days 'COPACOBONA' (35 FPGA's) \$10000

Roughly how many keys does COPACOBONA test in each second?

(A) 2^{32} (B) 2^{36} (C) 2^{37} (D) 2^{40}

Exercise 8.6

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

$$e_{(k,k')}(x) = e'_k\big(e_k(x)\big).$$

(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 COPACOBONA.)

(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 is Impressive, but Now Broken

No subexhaustive attacks on DES are known. But the relatively small keyspace $\mathbb{F}_2^{56}$ means that it cannot be considered secure.

- 1997: 140 days, distributed search on internet
- 1998: 9 days 'DES cracker' (special purpose) \$250000
- 2017: 6 days 'COPACOBONA' (35 FPGA's) \$10000

Roughly how many keys does COPACOBONA test in each second?

(A) 2^{32} (B) 2^{36} (C) 2^{37} (D) 2^{40}

Exercise 8.6

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

$$e_{(k,k')}(x) = e'_k\big(e_k(x)\big).$$

(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 COPACOBONA.)

(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 known plaintext attack on 2DES we are given a plaintext $x \in \mathbb{F}_2^{64}$ and 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 known plaintext attack on 2DES we are given a plaintext $x \in \mathbb{F}_2^{64}$ and 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 is $\mathbb{P}[w \in E]$?

(A) 1/256 (B) 1/128 (C) 1/8 (D) 1

Meet-in-the-Middle Attack on 2DES

In a known plaintext attack on 2DES we are given a plaintext $x \in \mathbb{F}_2^{64}$ and 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 is $\mathbb{P}[w \in E]$?

(A) $1/256$ (B) $1/128$ (C) $1/8$ (D) 1

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

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

Meet-in-the-Middle Attack on 2DES

In a known plaintext attack on 2DES we are given a plaintext $x \in \mathbb{F}_2^{64}$ and 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 is $\mathbb{P}[w \in E]$?

(A) $1/256$ (B) $1/128$ (C) $1/8$ (D) 1

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

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

How many operations does it take to find the key?

(A) 2^{56} (B) 2^{57} (C) $2^{57} + 2^{48}$ (D) 2^{112}

Meet-in-the-Middle Attack on 2DES

In a known plaintext attack on 2DES we are given a plaintext $x \in \mathbb{F}_2^{64}$ and 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 is $\mathbb{P}[w \in E]$?

(A) $1/256$ (B) $1/128$ (C) $1/8$ (D) 1

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

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

How many operations does it take to find the key?

(A) 2^{56} (B) 2^{57} (C) $2^{57} + 2^{48}$ (D) 2^{112}

Meet-in-the-Middle Attack on 2DES

In a known plaintext attack on 2DES we are given a plaintext $x \in \mathbb{F}_2^{64}$ and 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 is $\mathbb{P}[w \in E]$?

(A) $1/256$ (B) $1/128$ (C) $1/8$ (D) 1

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

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

How many operations does it take to find the key?

(A) 2^{56} (B) 2^{57} (C) $2^{57} + 2^{48}$ (D) 2^{112}

Meet-in-the-Middle Attack on 2DES

In a known plaintext attack on 2DES we are given a plaintext $x \in \mathbb{F}_2^{64}$ and 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 is $\mathbb{P}[w \in E]$?

(A) $1/256$ (B) $1/128$ (C) $1/8$ (D) 1

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

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

How many operations does it take to find the key?

(A) 2^{56} (B) 2^{57} (C) $2^{57} + 2^{48}$ (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. In each round:
- Confusion: apply S-box: $P : \mathbb{F}_2^8 \to \mathbb{F}_2^8$ on each subblock. using pseudo-inversion in the finite field $\mathbb{F}_{2^8}$:

$$P(x) = \begin{cases} 0 & \text{if } x \leftrightarrow 0 \\ x^{-1} & \text{otherwise.} \end{cases}$$

- Diffusion: Row permutation and a linear map on columns.
- Key addition: add a round key in $\mathbb{F}_2^{128}$ derived from the key.

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. In each round:
- Confusion: apply S-box: $P : \mathbb{F}_2^8 \to \mathbb{F}_2^8$ on each subblock. using pseudo-inversion in the finite field $\mathbb{F}_{2^8}$:

$$P(x) = \begin{cases} 0 & \text{if } x \leftrightarrow 0 \\ x^{-1} & \text{otherwise.} \end{cases}$$

- Diffusion: Row permutation and a linear map on columns.
- Key addition: add a round key in $\mathbb{F}_2^{128}$ derived from the key.

What is the pseudo-inverse of β in $\mathbb{F}_4$?

(A) 0 (B) 1 (C) α (D) $1 + \beta$

True or false: the pseudo-inversion function $\mathbb{F}_4 \to \mathbb{F}_4$ is linear?

(A) False (B) True

Surprisingly! It is highly non-linear in any $\mathbb{F}_{2^d}$ for $d \geq 3$.

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. In each round:
- Confusion: apply S-box: $P : \mathbb{F}_2^8 \to \mathbb{F}_2^8$ on each subblock. using pseudo-inversion in the finite field $\mathbb{F}_{2^8}$:

$$P(x) = \begin{cases} 0 & \text{if } x \leftrightarrow 0 \\ x^{-1} & \text{otherwise.} \end{cases}$$

- Diffusion: Row permutation and a linear map on columns.
- Key addition: add a round key in $\mathbb{F}_2^{128}$ derived from the key.

What is the pseudo-inverse of β in $\mathbb{F}_4$?

(A) 0 (B) 1 (C) α (D) $1 + \beta$

True or false: the pseudo-inversion function $\mathbb{F}_4 \to \mathbb{F}_4$ is linear?

(A) False (B) True

Surprisingly! It is highly non-linear in any $\mathbb{F}_{2^d}$ for $d \geq 3$.

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. In each round:
- Confusion: apply S-box: $P : \mathbb{F}_2^8 \to \mathbb{F}_2^8$ on each subblock. using pseudo-inversion in the finite field $\mathbb{F}_{2^8}$:

$$P(x) = \begin{cases} 0 & \text{if } x \leftrightarrow 0 \\ x^{-1} & \text{otherwise.} \end{cases}$$

- Diffusion: Row permutation and a linear map on columns.
- Key addition: add a round key in $\mathbb{F}_2^{128}$ derived from the key.

What is the pseudo-inverse of β in $\mathbb{F}_4$?

(A) 0 (B) 1 (C) α (D) $1 + \beta$

True or false: the pseudo-inversion function $\mathbb{F}_4 \to \mathbb{F}_4$ is linear?

(A) False (B) True

Surprisingly! It is highly non-linear in any $\mathbb{F}_{2^d}$ for $d \geq 3$.

Modes of Operation

A block cipher with block size n encrypts plaintexts $x \in \mathbb{F}_2^n$. If x is longer it has to be split into blocks $x^{(1)}, \ldots, x^{(m)} \in \mathbb{F}_2^n$:

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

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

- Electronic Codebook Mode:

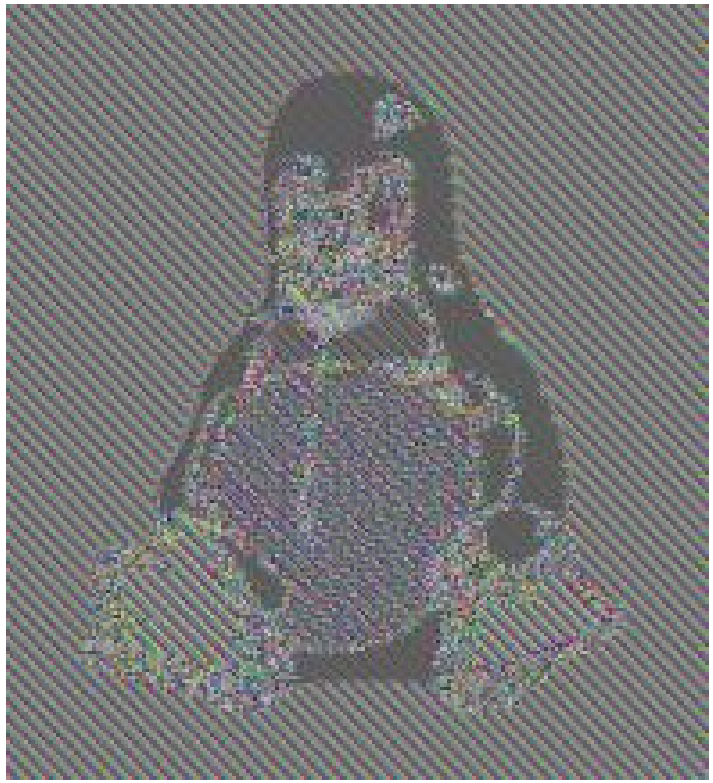
$$\begin{aligned} x^{(1)} &\mapsto e_k(x^{(1)}) \\ x^{(2)} &\mapsto e_k(x^{(2)}) \\ &\vdots \\ x^{(m)} &\mapsto e_k(x^{(m)}) \end{aligned}$$

- Cipher Block Chaining:

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

Same In Implies Same Out

If $x^{(i)} = x^{(j)}$ then, in Electronic Codebook Mode, the ciphertext blocks $e_k(x^{(i)}$ and $e_k(x^{(j)})$ are equal. This is a weakness of the mode of operation, not of the underlying block cipher.



Cipher Block Chaining (and the many other modes of operation you don't need 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 $k_{\mathsf{otp}} \in \mathbb{F}_2^n$, and known ciphertexts $x + k_{\mathsf{otp}}$ and $x' + k_{\mathsf{otp}}$. Adding the known ciphertexts gives $x + x'$, independent of k_{otp}.

Attack 9.1

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 $(k_{\text{otp}}, k) \in \mathbb{F}_2^n \times \mathbb{F}_2^\ell$ [**typo in printed notes**], define $E_{(k_{\text{otp}},k)} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ by

$$E_{(k_{\text{otp}},k)}(x) = e_k(x + k_{\text{otp}}). \textbf{ [Typo in printed notes!]}$$

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

$$z = E_{(k_{\text{otp}},k)}(x)$$
$$z_\Delta = E_{(k_{\text{otp}},k)}(x + \Delta)$$

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

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

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

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

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

Attack 9.1

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.

Attack on the AES S-box

Example 9.2

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, but whenever you see a power α^d where $d \geq 8$, eliminate it using the rule

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

We identify $\mathbb{F}_2^8$ with $\mathbb{F}_2(\alpha)$ by

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

- $1000\,0000 \leftrightarrow 1 \in \mathbb{F}_{2^8}$ and $1^{-1} = 1$, so
$$P(1000\,0000) = 10000000.$$
- $0100\,0000 \leftrightarrow \alpha \in \mathbb{F}_{2^8}$ and, multiplying the defining rule for α by α^{-1}, we get $\alpha^{-1} + 1 + \alpha^2 + \alpha^3 + \alpha^7 = 0$ so $\alpha^{-1} = 1 + \alpha^2 + \alpha^3 + \alpha^7$ and $P(0100\,0000) = 1011\,0001$.

Exercise: Show that $P(0010\,0000) = 1101\,0011$.

Example 9.3

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 $\mathcal{K}_z$ [**typo in printed notes**] in Attack 9.1 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 9.6, 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 9.3 [continued]

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

(1) If $k = 0000\,0000$ and $x = 0100\,0000$ then, since $P(0100\,0000) = 1011\,0001$ and $P(1100\,0000) = 0110\,1111$, $z + z_\Delta = 1101\,1110$. 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 $z + z_\Delta = 1000\,0000$ 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 guesses k_{guess} if $x = 0100\,0000$? What if $x = 0000\,0000$? [*Hint:* these can be deduced from (1) and (2).]

Cost of the Attack

Exercise 9.4

(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?

Exercise 9.5

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

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

has size 0 or 2, except when $\Delta^{-1} = \Gamma$, when it has size 4. [*Hint:* quadratic equations over any field have at most two roots.]

Attack on the Q-Block Cipher: Weak First Round

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

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

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

$$\begin{aligned}(v, w) &\mapsto \left(w, v + S(w + k^{(1)})\right) = (v^{(1)}, w^{(1)}) \\ &\mapsto \left(w^{(1)}, v^{(1)} + S(w^{(1)} + k^{(2)})\right) = (v^{(2)}, w^{(2)}) \\ &\mapsto \left(w^{(2)}, v^{(2)} + S(w^{(2)} + k^{(3)})\right) = (v^{(3)}, w^{(3)})\end{aligned}$$

Lemma 9.6

(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*

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

Attack on the Q-Block Cipher

Example 9.7

We run Attack 9.1 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 $k = 0000\,0000\,0000$ and $x = 0000\,0001$. There are 16 keys $k_{\text{guess}} \in \mathbb{F}_2^8$ such that $k_{\text{guess}} \in \mathcal{K}_z$, namely all binary words of the form $\star 0 \star 0\ \star 0 \star 0$. These are the possibilities for

$$(k_{\text{guess}}^{(2)}, k_{\text{guess}}^{(3)}) \in \mathbb{F}_2^8.$$

Trying each guess together with all 16 possibilities for $k_{\text{guess}}^{(1)} \in F_2^4$ we get

$$k \in \{0000\,0000\,0000,\ 1000\,0010\,1000,\ 1110\,1000\,0010,\ 0110\,1010\,1010\}.$$

All these keys encrypt $0000\,0001$ to the same ciphertext, namely $0000\,0100$.

Attack on a 5-round Q-block cipher

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

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

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

$$e^{-1}_{k_{\text{guess}}}(z) + e^{-1}_{k_{\text{guess}}}(z_\Delta) \notin \{0010\,0000, 0010\,0001, 0010\,0010, 0010\,001\}.$$

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.

Part D: Public Key Cryptography and Digital Signatures

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

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

(4) Now Alice and Bob both know $2^{ab} \bmod p$. They each write $2^{ab} \bmod p$ in binary and take the final 128 bits to get an AES key.

Example 10.1 [continued]

After (2), the eavesdropper Eve knows p, $2^a \bmod p$ and $2^b \bmod p$. It is believed that it is hard for her to use this information to find $2^{ab} \bmod p$. The difficulty can be seen even in small examples.

Exercise 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?

n	0	1	2	3	4	5	6	7	8	9
$2^n \bmod 11$	1	2								
n	10	11	12	13	14	15	16	17	18	19
$2^n \bmod 11$										

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?

n	0	1	2	3	4	5	6	7	8	9
$2^n \bmod 11$	1	2	4	8	5	10	9	7	3	6
n	10	11	12	13	14	15	16	17	18	19
$2^n \bmod 11$	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?

n	0	1	2	3	4	5	6	7	8	9
$2^n \bmod 11$	1	2	4	8	5	10	9	7	3	6
n	10	11	12	13	14	15	16	17	18	19
$2^n \bmod 11$	1	2	4	8	5	10	9	7	3	6

After (4) Alice and Bob can communicate using the AES cryptosystems, which has no known sub-exhaustive attacks.
So remarkably, Alice and Bob can communicate securely *without exchanging any private key material*.

Integers Modulo a Prime

- By Fermat's Little Theorem, $c^{p-1} \equiv 1 \bmod c$ for any c not divisible by p.
- If $c^m \not\equiv 1 \bmod p$ for $m < p-1$ then c is said to be a *primitive root* modulo p and, working modulo p,

$$\{1, c, c^2, \ldots, c^{p-2}\} = \{1, 2, \ldots, p-1\}$$

  Primitive roots always exist: often one can take 2.
- Equivalently: $\mathbb{Z}_p^\times$ is cyclic of order $p-1$.
- For instance 2 is a primitive root modulo 11 but 5 is not, because $5 \equiv 2^4 \bmod 11$, so $5^5 \equiv 2^{10} \equiv 1 \bmod 11$.

Diffie–Hellman Key Exchange

This is nothing more than Example 10.1, modified to avoid some potential weaknesses, and implemented efficiently.

- The prime p is chosen so that $p-1$ has at least one large prime factor. (This is true of most primes. There are fast ways to decide if a number is prime.)
- Rather than use 2, Alice and Bob use a primitive root modulo p, so every element of $\{1, \ldots, p-1\}$ is congruent to a power of g. (The base is public.)
- Alice and Bob compute $g^a \bmod p$ and $g^b \bmod p$ by repeated squaring. See Question 3 on Sheet 8 for the idea. For example $2^{21} \bmod 177$ is computed as follows:
  - $2^2 \equiv 4 \bmod 199$
  - $2^4 \equiv 4^2 = 16 \bmod 199$
  - $2^8 \equiv 16^2 = 256 \equiv 57 \bmod 199$
  - $2^{16} \equiv 57^2 = 3249 \equiv 65 \bmod 199$

  Now use $2^{21} = 2^{16+4+1} \equiv 65 \times 16 \times 2 = 2080 \equiv 90 \bmod 199$.
- The shared key is now $g^{ab} \bmod p$.

One-way Functions

A one-way function is a bijective function that is fast to compute, but whose inverse is hard to compute. It is beyond the scope of this course to make this more precise.

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

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

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

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

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 Cryptosytem for n,

$$\mathcal{P} = \mathcal{C} = \{0, 1, \ldots, n-1\}$$

and

$$\mathcal{K} = \{a \in \{1, \ldots, n-1\} : \mathrm{hcf}\big(a, (p-1)(q-1)\big) = 1.$$

The encryption functions are defined by

$$e_a(x) = x^a \bmod n.$$

Alice's *public key* is the pair (a, n). In private Alice computes r such that $ar \equiv 1 \bmod (p-1)(q-1)$. As just seen, she can do this because she knows p and q, and so $(p-1)(q-1)$. The decryption function is then

$$d_a(y) = y^r \bmod n.$$

Alice's *private key* is the pair (r, n).

No-one has found an 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.

Quiz on Diffie–Hellman and RSA

Let p and q be primes of size about 2^{512}. 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) Suppose $x \mapsto x^a$ mod n is invertible. Given a and n it is fast to compute its inverse.

(A) False (B) True

Quiz on Diffie–Hellman and RSA

Let p and q be primes of size about 2^{512}. 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) Suppose $x \mapsto x^a$ mod n is invertible. Given a and n it is fast to compute its inverse.

(A) False (B) True

Quiz on Diffie–Hellman and RSA

Let p and q be primes of size about 2^{512}. 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) Suppose $x \mapsto x^a$ mod n is invertible. Given a and n it is fast to compute its inverse.

(A) False (B) True

Quiz on Diffie–Hellman and RSA

Let p and q be primes of size about 2^{512}. 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) Suppose $x \mapsto x^a$ mod n is invertible. Given a and n it is fast to compute its inverse.

(A) False (B) True

Quiz on Diffie–Hellman and RSA

Let p and q be primes of size about 2^{512}. 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) Suppose $x \mapsto x^a$ mod n is invertible. Given a and n it is fast to compute its inverse.

(A) False (B) True

Quiz on Diffie–Hellman and RSA

Let p and q be primes of size about 2^{512}. 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) Suppose $x \mapsto x^a$ mod n is invertible. Given a and n it is fast to compute its inverse.

(A) False (B) True

Quiz on Diffie–Hellman and RSA

Let p and q be primes of size about 2^{512}. 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

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

(A) False (B) True

Quiz on Diffie–Hellman and RSA

Let p and q be primes of size about 2^{512}. 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

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

(A) False (B) True

Mathematica Versus Lecturer

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 message is 10 then he sends 109 to Alice, since $10^9 \equiv 109 \bmod 187$. Alice decrypts to 10 by computing $109^{89} \bmod 187$.

(2) The MATHEMATICA notebook `PKCExamples.nb` available from Moodle can be used to give examples where p and q are large.

Mathematica Versus Lecturer

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 message is 10 then he sends 109 to Alice, since $10^9 \equiv 109 \bmod 187$. Alice decrypts to 10 by computing $109^{89} \bmod 187$.

(2) The MATHEMATICA notebook `PKCExamples.nb` available from Moodle can be used to give examples where p and q are large.

At the end of the previous lecture I demonstrated RSA by taking a message m, computing its encryption $e_a(x) \equiv x^a \bmod n$ and its decryption $d_a\big(e_a(m)\big) \equiv (x^a)^r \equiv m \bmod n$.

Mathematica Versus Lecturer

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 message is 10 then he sends 109 to Alice, since $10^9 \equiv 109 \bmod 187$. Alice decrypts to 10 by computing $109^{89} \bmod 187$.

(2) The MATHEMATICA notebook `PKCExamples.nb` available from Moodle can be used to give examples where p and q are large.

At the end of the previous lecture I demonstrated RSA by taking a message m, computing its encryption $e_a(x) \equiv x^a \bmod n$ and its decryption $d_a\big(e_a(m)\big) \equiv (x^a)^r \equiv m \bmod n$.

Unfortunately my message x was more than n. So the decryption was $x \bmod n$ (a number $< n$), not x itself. Otherwise it all worked perfectly!

§11 Digital Signatures and Hash Functions

Suppose Alice and Bob have the RSA keys:

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

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	(a, m)	(r, m)
Bob	(b, m)	(s, n)

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

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

(b) How did Bob compute z?

(c) Can Malcolm read z?

(d) How can Bob avoid the problem in (c)?

Signed Messages using RSA

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 7-bit ASCII coding, it means only $2048/7 \approx 290$ characters can be sent.

Bob can get round this by splitting the message into blocks, but computing $d_s(x^{(i)})$ 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 $h(x) \in \{1, \ldots, n-1\}$ is a hash of x.

The pair $\big(x, d_b(h(x))\big)$ is a *signed message* from Bob. [**Typo in printed notes: d_b, not d_s, is the inverse of e_b.**]

Hash Functions

Definition 11.2

A *hash function* of length r is a function $h : \mathbb{N}_0 \to \mathbb{F}_2^r$. The value $h(x)$ is the *hash* of the message $x \in \mathbb{N}_0$.

A cryptographically useful hash function has the following properties:

(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 $h : \mathbb{N} \to \mathbb{F}_2^r$ be a good hash function. On average, how many hashes does an attacker need to calculate to find a pair (x, x') with $h(x) = h(x')$?

Birthday Paradox

Exercise 11.3

Let $h : \mathbb{N} \to \mathbb{F}_2^r$ be a good hash function. On average, how many hashes does an attacker need to calculate to find a pair (x, x') with $h(x) = h(x')$?

The mathematics behind Exercise 11.3 is the well-known Birthday Paradox: in a room with 23 people, the probability is about $\frac{1}{2}$ that two people have the same birthday.

Lemma 11.4

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

Birthday Paradox

Exercise 11.3

Let $h : \mathbb{N} \to \mathbb{F}_2^r$ be a good hash function. On average, how many hashes does an attacker need to calculate to find a pair (x, x') with $h(x) = h(x')$?

The mathematics behind Exercise 11.3 is the well-known Birthday Paradox: in a room with 23 people, the probability is about $\frac{1}{2}$ that two people have the same birthday.

Lemma 11.4

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

In (c) the birthdays are hash values, so we have $B = 2^r$. Since $\sqrt{2^r} = 2^{r/2}$ we interpret 'hard to find' as 'requires at least $2^{r/2}$ hashes'.

Hash Functions In Practice

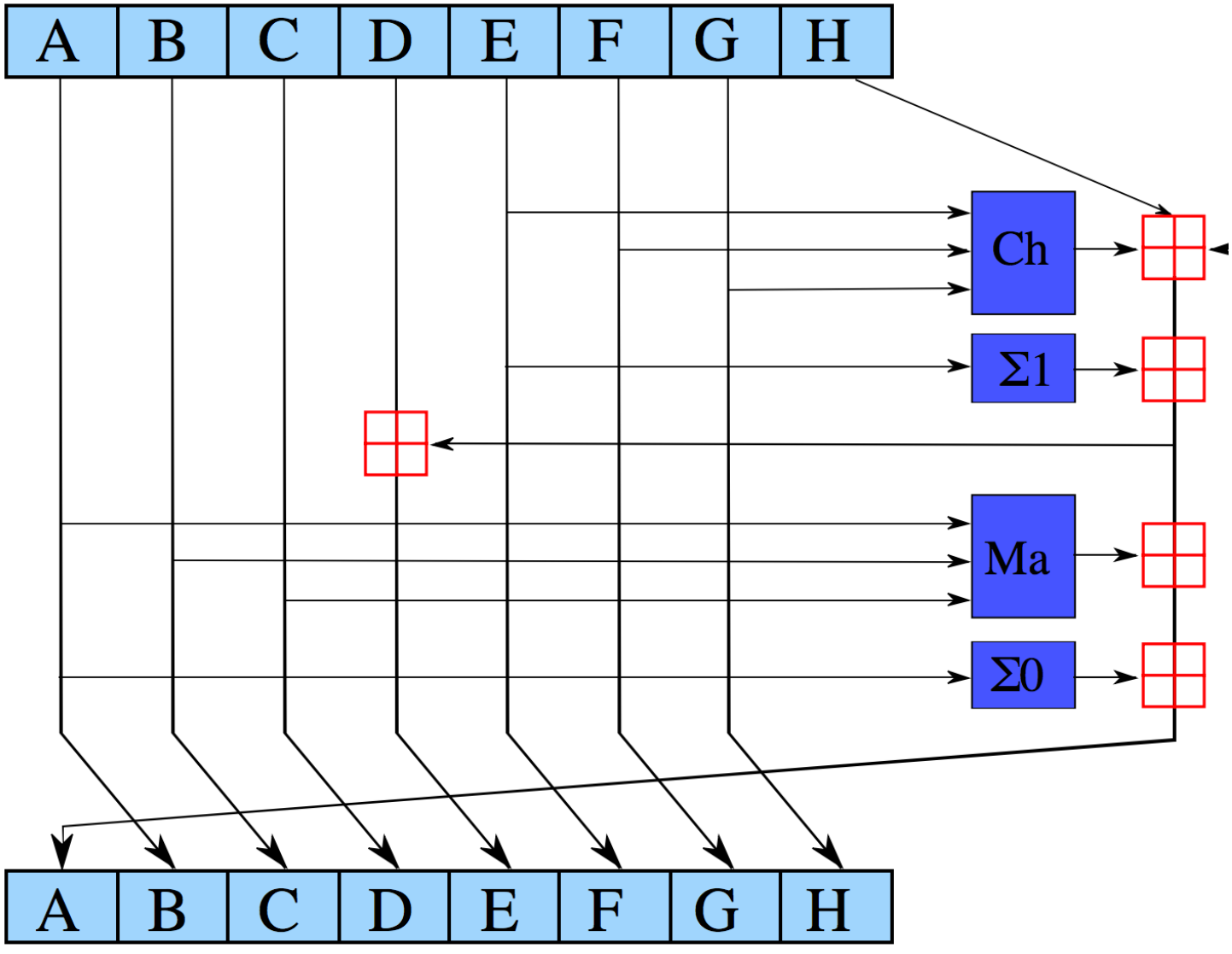
Example 11.5 (SHA-256)

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 $d_a(h(x))$. [**My notation error: b was used for Bob and bitcoin. Changed to Alice on slides and on Moodle printed notes, so sign by d_a.**]

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 make another $\big(b, x', d_a(h(x'))\big)$ where x' says 'I Alice give Charlie the bitcoin b'.

To avoid this, transactions are *validated*. To validate a list of transactions

$$\big(b^{(1)}, x^{(1)}, d_{a^{(1)}}(h(x^{(1)}))\big), \big(b^{(2)}, x^{(2)}, d_{a^{(2)}}(h(x^{(2)}))\big), \ldots$$

a *miner* searches for $c \in \mathbb{N}$ such that, when this list is converted to a number, its hash, by two iterations of SHA-256, has a large number of initial zeros.

Example 11.7 [continued]

When Bob receives $\big(b, x', d_a(h(x'))\big)$, he looks to see if there is a block already containing a transaction involving b. When Bob finds $(b, x, d_a(h(x)))$ as part of a block with the laboriously computed c, Bob knows Alice has cheated.

Vast numbers of hashes must be computed to grow the blockchain. Miners are incentivized to do this: the reward for growing the blockchain is given in bitcoins.

This morning the bitcoin traded at \$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.

Feedback

Please take a 362 or 5462 form as appropriate.

- In this context I am the ‘tutor’.
- Please comment on how you find the pace of the course: much too slow, a bit too slow, about right, a bit too fast, much too fast.
- Any comments will be read very carefully.