

Lecture 2-2: Classical Cryptography

–Cryptographic Algorithms and Protocols

Instructor: Xiujie Huang 黄秀姐

Office: Nanhai Building, Room 411

E-mail: t_xiujie@jnu.edu.cn

Department of Computer Science
School of Information Science and Technology
Jinan University

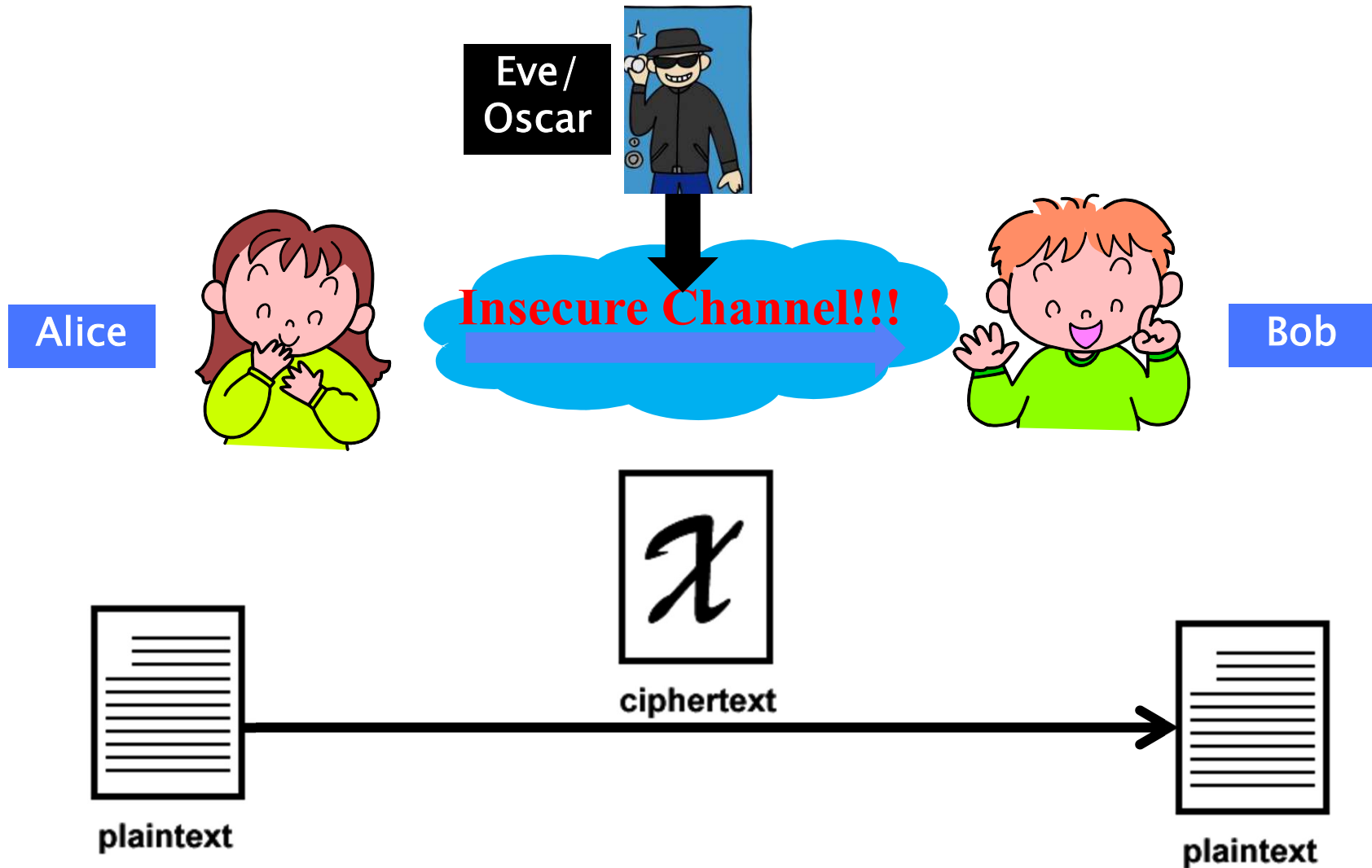
Outline

- 1 Basics of a Cryptosystem
- 2 Substitution Ciphers
- 3 The Permutation Cipher
- 4 Stream Ciphers
- 5 Cryptanalysis
- 6 Conclusions

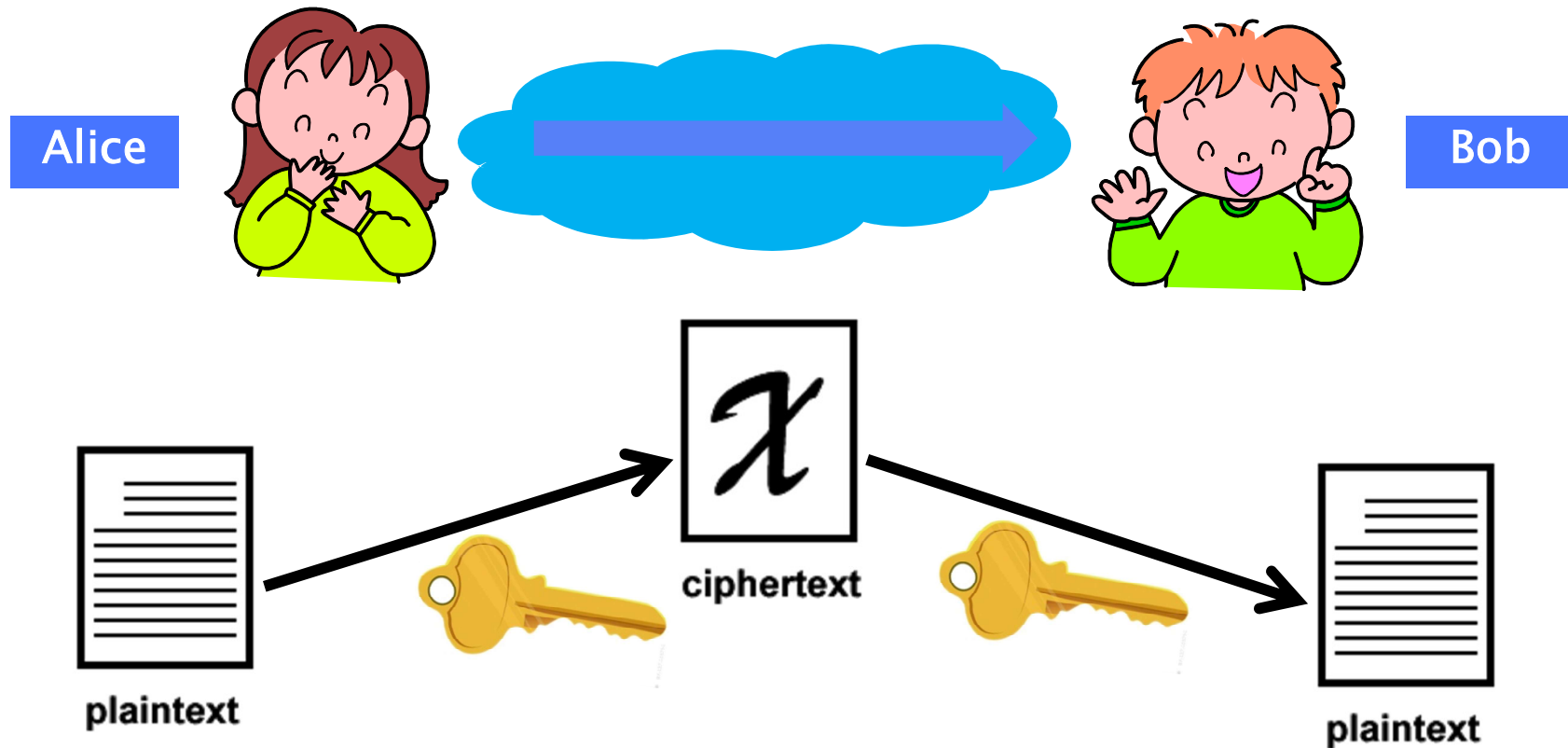
Outline

- 1 Basics of a Cryptosystem
- 2 Substitution Ciphers
- 3 The Permutation Cipher
- 4 Stream Ciphers
- 5 Cryptanalysis
- 6 Conclusions

Intuition on Cryptography



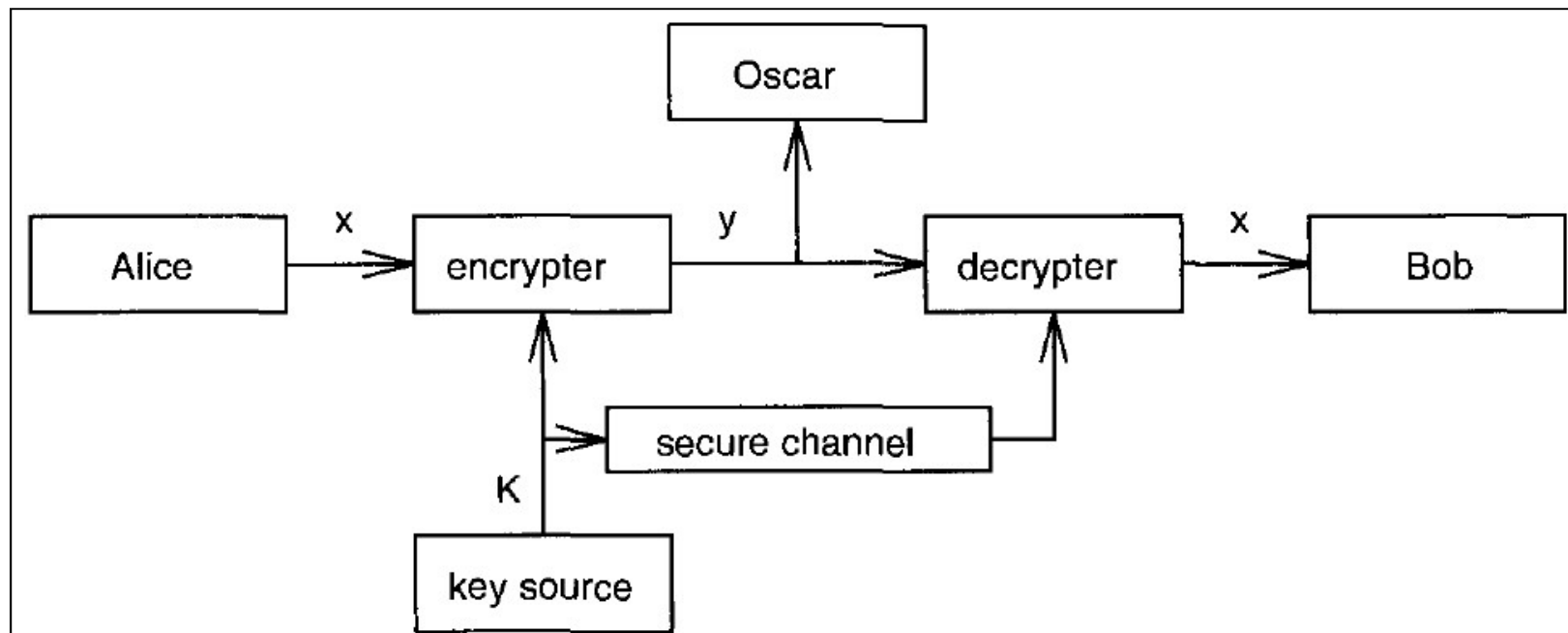
Symmetric-Key Cryptosystem (SKC)



Cryptographic Communication System

Protocol:

- A and B choose a random key K by a secure channel
- A wants to send a string message $\mathbf{x} = x_1x_2 \dots x_n$
- A computes $y_i = e_K(x_i)$ and the resulting string $\mathbf{y} = y_1y_2 \dots y_n$ is sent over the insecure channel
- B receives $\mathbf{y} = y_1y_2 \dots y_n$ and decrypts $x_i = d_K(y_i)$ to obtain $\mathbf{x} = x_1x_2 \dots x_n$



Basics of a Cryptosystem

Objective and Solutions

- Objective: confidentially communicate over insecure channels
- SKC is one of the solutions

Basics of a Cryptosystem

Objective and Solutions

- Objective: confidentially communicate over insecure channels
- SKC is one of the solutions

A Simple Cryptosystem

A cryptosystem is a five-tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, where

- 1 \mathcal{P} is a finite set of all possible plaintexts,
- 2 \mathcal{C} is a finite set of all possible ciphertexts,
- 3 \mathcal{K} is a finite set of all possible keys, called keyspace,
- 4 For each $K \in \mathcal{K}$, $e_K \in \mathcal{E}$, $d_K \in \mathcal{D}$

Encryption rule $e_K : \mathcal{P} \rightarrow \mathcal{C}$; Decryption rule $d_K : \mathcal{C} \rightarrow \mathcal{P}$,
satisfying $d_K(e_K(x)) = x$ for every $x \in \mathcal{P}$.

Basics of a Cryptosystem

Objective and Solutions

- Objective: confidentially communicate over insecure channels
- SKC is one of the solutions

A Simple Cryptosystem

A cryptosystem is a five-tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, where

- 1 \mathcal{P} is a finite set of all possible *plaintexts*,
- 2 \mathcal{C} is a finite set of all possible *ciphertexts*,
- 3 \mathcal{K} is a finite set of all possible *keys*, called *keyspace*,
- 4 For each $K \in \mathcal{K}$, $e_K \in \mathcal{E}$, $d_K \in \mathcal{D}$

Encryption rule $e_K : \mathcal{P} \rightarrow \mathcal{C}$; Decryption rule $d_K : \mathcal{C} \rightarrow \mathcal{P}$,
satisfying $d_K(e_K(x)) = x$ for every $x \in \mathcal{P}$.

- Encryption rule e_K is a **injective function (单射)**, i.e., one-to-one.
If $x_1 \neq x_2$, then $e_K(x_1) \neq e_K(x_2)$.

Outline

1 Basics of a Cryptosystem

2 Substitution Ciphers

- The Shift Cipher
- The Affine Cipher
- The Vigenere Cipher
- The Hill Cipher

3 The Permutation Cipher

4 Stream Ciphers

5 Cryptanalysis

6 Conclusions

The Substitution Cipher

Cryptosystem 2.2: Substitution Cipher, 替换密码(on Page 21)

Let $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$. Let \mathcal{K} consists of all possible **permutations** of the 26 elements in \mathbb{Z}_{26} . For each permutation $\pi \in \mathcal{K}$, define

- Encryption rule $e_\pi : \mathcal{P} \rightarrow \mathcal{C}$, $e_\pi(x) = \pi(x)$
- Decryption rule $d_\pi : \mathcal{C} \rightarrow \mathcal{P}$, $d_\pi(y) = \pi^{-1}(y)$

where π^{-1} is the inverse permutation to π .

The Substitution Cipher

Cryptosystem 2.2: Substitution Cipher, 替换密码(on Page 21)

Let $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$. Let \mathcal{K} consists of all possible **permutations** of the 26 elements in \mathbb{Z}_{26} . For each permutation $\pi \in \mathcal{K}$, define

- Encryption rule $e_\pi : \mathcal{P} \rightarrow \mathcal{C}$, $e_\pi(x) = \pi(x)$
- Decryption rule $d_\pi : \mathcal{C} \rightarrow \mathcal{P}$, $d_\pi(y) = \pi^{-1}(y)$

where π^{-1} is the inverse permutation to π . $\mathbb{Z}_{26} \leftrightarrow$ the English alphabet (π 是英文字母表的一个置换, π^{-1} 是置换 π 的逆置换.)

Relation of \mathbb{Z}_{26} and the 26-letter English Alphabet:

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

plaintext -- lower case letter, ciphertext -- upper case letter

The Substitution Cipher

An Example

Let π be the permutation over the English alphabet as follows:

a	b	c	d	e	f	g	h	i	j	k	l	m
X	N	Y	A	H	P	O	G	Z	Q	W	B	T
n	o	p	q	r	s	t	u	v	w	x	y	z
S	F	L	R	C	V	M	U	E	K	J	D	I

$e_{\pi}(\text{ihaveanapple}) = \pi(\text{ihaveanapple}) = \text{ZGXEHSXLLBH}$

$d_{\pi}(\text{ZGXEHSXLLBH}) = \pi^{-1}(\text{ZGXEHSXLLBH}) = \text{ihaveanapple}$

The Substitution Cipher

An Example

Let π be the permutation over the English alphabet as follows:

a	b	c	d	e	f	g	h	i	j	k	l	m
X	N	Y	A	H	P	O	G	Z	Q	W	B	T
n	o	p	q	r	s	t	u	v	w	x	y	z
S	F	L	R	C	V	M	U	E	K	J	D	I

$e_{\pi}(\text{ihaveanapple}) = \pi(\text{ihaveanapple}) = \text{ZGXEHSXLLBH}$

$d_{\pi}(\text{ZGXEHSXLLBH}) = \pi^{-1}(\text{ZGXEHSXLLBH}) = \text{ihaveanapple}$

Some Issues:

- The size of Keyspace \mathcal{K} is $= 26! > 4.0 \times 10^{26}$.

The Substitution Cipher

An Example

Let π be the permutation over the **English alphabet** as follows:

a	b	c	d	e	f	g	h	i	j	k	l	m
X	N	Y	A	H	P	O	G	Z	Q	W	B	T
n	o	p	q	r	s	t	u	v	w	x	y	z
S	F	L	R	C	V	M	U	E	K	J	D	I

$e_{\pi}(\text{ihaveanapple}) = \pi(\text{ihaveanapple}) = \text{ZGXEHSXLLBH}$

$d_{\pi}(\text{ZGXEHSXLLBH}) = \pi^{-1}(\text{ZGXEHSXLLBH}) = \text{ihaveanapple}$

Some Issues:

- The size of Keyspace \mathcal{K} is $= 26! > 4.0 \times 10^{26}$.
- An exhaustive key search is infeasible.
But it can easily be cryptanalyzed by some statistic methods.

An example of a ciphertext-only attack on the substitution cipher

The Shift Cipher

Cryptosystem 2.1: Shift Cipher, 移位密码(on Page 18)

Let $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$. For $0 \leq K \leq 25$, define

- Encryption rule $e_K : \mathcal{P} \rightarrow \mathcal{C}$ as $e_K(x) = \underline{(x + K)} \bmod 26$,
- Decryption rule $d_K : \mathcal{C} \rightarrow \mathcal{P}$ as $d_K(y) = \underline{(y - K)} \bmod 26$.

where $x, y \in \mathbb{Z}_{26}$.

The Shift Cipher

Cryptosystem 2.1: Shift Cipher, 移位密码(on Page 18)

Let $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$. For $0 \leq K \leq 25$, define

- Encryption rule $e_K : \mathcal{P} \rightarrow \mathcal{C}$ as $e_K(x) = (x + K) \bmod 26$,
- Decryption rule $d_K : \mathcal{C} \rightarrow \mathcal{P}$ as $d_K(y) = (y - K) \bmod 26$.

where $x, y \in \mathbb{Z}_{26}$.

Some Issues:

- The Shift Cipher is a special case of the Substitution Cipher.
- When $K = 3$, it is called the *Caesar Cipher*.
- The size of Keyspace \mathcal{K} is $= 26$. (only 26 permutations)
- NOT SECURE!!! (exhaustive key search)
- a necessary condition to be secure is that an exhaustive key search should be infeasible.

The Affine Cipher

Cryptosystem 2.3: Affine Cipher, 仿射密码(on Page 25)

Let $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$. Let the keyspace be

$$\mathcal{K} = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : \gcd(a, 26) = 1\} = \mathbb{Z}_{26}^* \times \mathbb{Z}_{26} \quad (2.1)$$

For each key $K = (a, b) \in \mathcal{K}$, define $(x, y \in \mathbb{Z}_{26})$

- Encryption rule $e_K(x) = \underline{(ax + b) \bmod 26}$
- Decryption rule $d_K(y) = \underline{a^{-1}(y - b) \bmod 26}$

The Affine Cipher

Cryptosystem 2.3: Affine Cipher, 仿射密码(on Page 25)

Let $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$. Let the keyspace be

$$\mathcal{K} = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : \gcd(a, 26) = 1\} = \mathbb{Z}_{26}^* \times \mathbb{Z}_{26} \quad (2.1)$$

For each key $K = (a, b) \in \mathcal{K}$, define $(x, y \in \mathbb{Z}_{26})$

- Encryption rule $e_K(x) = (ax + b) \bmod 26$
- Decryption rule $d_K(y) = a^{-1}(y - b) \bmod 26$

Some Issues:

- Verification of $d_K(e_K(x)) = x$: $d_K(e_K(x)) = a^{-1}((ax + b) \bmod 26 - b) \bmod 26 = a^{-1}ax \bmod 26 = x$.

The Affine Cipher

Cryptosystem 2.3: Affine Cipher, 仿射密码(on Page 25)

Let $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$. Let the keyspace be

$$\mathcal{K} = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : \gcd(a, 26) = 1\} = \mathbb{Z}_{26}^* \times \mathbb{Z}_{26} \quad (2.1)$$

For each key $K = (a, b) \in \mathcal{K}$, define $(x, y \in \mathbb{Z}_{26})$

- Encryption rule $e_K(x) = (ax + b) \bmod 26$
- Decryption rule $d_K(y) = a^{-1}(y - b) \bmod 26$

Some Issues:

- Verification of $d_K(e_K(x)) = x$: $d_K(e_K(x)) = a^{-1}((ax + b) \bmod 26 - b) \bmod 26 = a^{-1}ax \bmod 26 = x$.
- The size of keyspace is $\phi(26) \times 26 = 12 \times 26 = 312$. (312 permutations)

The Affine Cipher

Cryptosystem 2.3: Affine Cipher, 仿射密码(on Page 25)

Let $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$. Let the keyspace be

$$\mathcal{K} = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : \gcd(a, 26) = 1\} = \mathbb{Z}_{26}^* \times \mathbb{Z}_{26} \quad (2.1)$$

For each key $K = (a, b) \in \mathcal{K}$, define $(x, y \in \mathbb{Z}_{26})$

- Encryption rule $e_K(x) = (ax + b) \bmod 26$
- Decryption rule $d_K(y) = a^{-1}(y - b) \bmod 26$

Some Issues:

- Verification of $d_K(e_K(x)) = x$: $d_K(e_K(x)) = a^{-1}((ax + b) \bmod 26 - b) \bmod 26 = a^{-1}ax \bmod 26 = x$.
- The size of keyspace is $\phi(26) \times 26 = 12 \times 26 = 312$. (312 permutations)
- The Affine Cipher is a special case of the Substitution Cipher.

The Affine Cipher

Cryptosystem 2.3: Affine Cipher, 仿射密码(on Page 25)

Let $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$. Let the keyspace be

$$\mathcal{K} = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : \gcd(a, 26) = 1\} = \mathbb{Z}_{26}^* \times \mathbb{Z}_{26} \quad (2.1)$$

For each key $K = (a, b) \in \mathcal{K}$, define $(x, y \in \mathbb{Z}_{26})$

- Encryption rule $e_K(x) = (ax + b) \bmod 26$
- Decryption rule $d_K(y) = a^{-1}(y - b) \bmod 26$

Some Issues:

- Verification of $d_K(e_K(x)) = x$: $d_K(e_K(x)) = a^{-1}((ax + b) \bmod 26 - b) \bmod 26 = a^{-1}ax \bmod 26 = x$.
- The size of keyspace is $\phi(26) \times 26 = 12 \times 26 = 312$. (312 permutations)
- The Affine Cipher is a special case of the Substitution Cipher.
- For the general case of $\mathcal{P} = \mathcal{C} = \mathbb{Z}_m$, $\mathcal{K} = \mathbb{Z}_m^* \times \mathbb{Z}_m$?

The Affine Cipher

Cryptosystem 2.3: Affine Cipher, 仿射密码(on Page 25)

Let $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$. Let the keyspace be

$$\mathcal{K} = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : \gcd(a, 26) = 1\} = \mathbb{Z}_{26}^* \times \mathbb{Z}_{26} \quad (2.1)$$

For each key $K = (a, b) \in \mathcal{K}$, define $(x, y \in \mathbb{Z}_{26})$

- Encryption rule $e_K(x) = (ax + b) \bmod 26$
- Decryption rule $d_K(y) = a^{-1}(y - b) \bmod 26$

Some Issues:

- Verification of $d_K(e_K(x)) = x$: $d_K(e_K(x)) = a^{-1}((ax + b) \bmod 26 - b) \bmod 26 = a^{-1}ax \bmod 26 = x$.
- The size of keyspace is $\phi(26) \times 26 = 12 \times 26 = 312$. (312 permutations)
- The Affine Cipher is a special case of the Substitution Cipher.
- For the general case of $\mathcal{P} = \mathcal{C} = \mathbb{Z}_m$, $\mathcal{K} = \mathbb{Z}_m^* \times \mathbb{Z}_m$?
The size of keyspace is $\phi(m) \times m$.

Cryptanalysis of the Affine Cipher

A ciphertext-only attack on the Affine cipher

Oscar knows a string of ciphertext, y , and that is obtained using the Affine cipher.

The Affine cipher can be broken by using the Statistical properties of the English language.

The Vigenere Cipher

Cryptosystem 2.4: Vigenere Cipher (on Page 26)

Let $n \in \mathbb{Z}^+$. Let $\mathcal{P} = \mathcal{K} = \mathcal{C} = (\mathbb{Z}_{26})^n$. For a key $K = (k_1, k_2, \dots, k_n)$,

- Encryption: $e_K(x_1, x_2, \dots, x_n) = (x_1 + k_1, x_2 + k_2, \dots, x_n + k_n)$;
- Decryption: $d_K(y_1, y_2, \dots, y_n) = (y_1 - k_1, y_2 - k_2, \dots, y_n - k_n)$.

where all operations are performed in \mathbb{Z}_{26} .

The Vigenere Cipher

Cryptosystem 2.4: Vigenere Cipher (on Page 26)

Let $n \in \mathbb{Z}^+$. Let $\mathcal{P} = \mathcal{K} = \mathcal{C} = (\mathbb{Z}_{26})^n$. For a key $K = (k_1, k_2, \dots, k_n)$,

- Encryption: $e_K(x_1, x_2, \dots, x_n) = (x_1 + k_1, x_2 + k_2, \dots, x_n + k_n)$;
- Decryption: $d_K(y_1, y_2, \dots, y_n) = (y_1 - k_1, y_2 - k_2, \dots, y_n - k_n)$.

where all operations are performed in \mathbb{Z}_{26} .

An example

Assume the keyword is "CIPHER" which $\leftrightarrow K = (2, 8, 15, 7, 4, 17)$.

Plaintext: thiscryptosystemisnotsecure

The Vigenere Cipher

Cryptosystem 2.4: Vigenere Cipher (on Page 26)

Let $n \in \mathbb{Z}^+$. Let $\mathcal{P} = \mathcal{K} = \mathcal{C} = (\mathbb{Z}_{26})^n$. For a key $K = (k_1, k_2, \dots, k_n)$,

- Encryption: $e_K(x_1, x_2, \dots, x_n) = (x_1 + k_1, x_2 + k_2, \dots, x_n + k_n)$;
- Decryption: $d_K(y_1, y_2, \dots, y_n) = (y_1 - k_1, y_2 - k_2, \dots, y_n - k_n)$.

where all operations are performed in \mathbb{Z}_{26} .

An example

Assume the keyword is "CIPHER" which $\leftrightarrow K = (2, 8, 15, 7, 4, 17)$.

Plaintext: thiscryptosystemisnotsecure

$\leftrightarrow 19 \ 7 \ 8 \ 18 \ 2 \ 17 \ 24 \ 15 \ 19 \ 14 \ 18 \ 24 \ 18 \ 19 \ 4 \ 12 \ 8 \ 18 \dots$

The Vigenere Cipher

Cryptosystem 2.4: Vigenere Cipher (on Page 26)

Let $n \in \mathbb{Z}^+$. Let $\mathcal{P} = \mathcal{K} = \mathcal{C} = (\mathbb{Z}_{26})^n$. For a key $K = (k_1, k_2, \dots, k_n)$,

- Encryption: $e_K(x_1, x_2, \dots, x_n) = (x_1 + k_1, x_2 + k_2, \dots, x_n + k_n)$;
- Decryption: $d_K(y_1, y_2, \dots, y_n) = (y_1 - k_1, y_2 - k_2, \dots, y_n - k_n)$.

where all operations are performed in \mathbb{Z}_{26} .

An example

Assume the keyword is "CIPHER" which $\leftrightarrow K = (2, 8, 15, 7, 4, 17)$.

Plaintext: thiscryptosystemisnotsecure

$$\begin{array}{cccccccccccccccccccccccc} \leftrightarrow & 19 & 7 & 8 & 18 & 2 & 17 & 24 & 15 & 19 & 14 & 18 & 24 & 18 & 19 & 4 & 12 & 8 & 18 & \dots \\ \oplus & 2 & 8 & 15 & 7 & 4 & 17 & 2 & 8 & 15 & 7 & 4 & 17 & 2 & 8 & 15 & 7 & 4 & 17 & \dots \end{array}$$

The Vigenere Cipher

Cryptosystem 2.4: Vigenere Cipher (on Page 26)

Let $n \in \mathbb{Z}^+$. Let $\mathcal{P} = \mathcal{K} = \mathcal{C} = (\mathbb{Z}_{26})^n$. For a key $K = (k_1, k_2, \dots, k_n)$,

- Encryption: $e_K(x_1, x_2, \dots, x_n) = (x_1 + k_1, x_2 + k_2, \dots, x_n + k_n)$;
- Decryption: $d_K(y_1, y_2, \dots, y_n) = (y_1 - k_1, y_2 - k_2, \dots, y_n - k_n)$.

where all operations are performed in \mathbb{Z}_{26} .

An example

Assume the keyword is "CIPHER" which $\leftrightarrow K = (2, 8, 15, 7, 4, 17)$.

Plaintext: thiscryptosystemisnotsecure

$$\begin{array}{cccccccccccccccc|cccccccccccccccc|cccccccccccccccc} \leftrightarrow & 19 & 7 & 8 & 18 & 2 & 17 & & 24 & 15 & 19 & 14 & 18 & 24 & & 18 & 19 & 4 & 12 & 8 & 18 & \dots \\ \oplus & 2 & 8 & 15 & 7 & 4 & 17 & & 2 & 8 & 15 & 7 & 4 & 17 & & 2 & 8 & 15 & 7 & 4 & 17 & \dots \\ \Rightarrow & 21 & 15 & 23 & 25 & 6 & 8 & & 0 & 23 & 8 & 21 & 22 & 15 & & 20 & 1 & 19 & 19 & 12 & 9 & \dots \end{array}$$

Ciphertext: VPXZGIAXICWPUBTTMJPWIZITWZT

The Vigenere Cipher

Cryptosystem 2.4: Vigenere Cipher (on Page 26)

Let $n \in \mathbb{Z}^+$. Let $\mathcal{P} = \mathcal{K} = \mathcal{C} = (\mathbb{Z}_{26})^n$. For a key $K = (k_1, k_2, \dots, k_n)$,

- Encryption: $e_K(x_1, x_2, \dots, x_n) = (x_1 + k_1, x_2 + k_2, \dots, x_n + k_n)$;
- Decryption: $d_K(y_1, y_2, \dots, y_n) = (y_1 - k_1, y_2 - k_2, \dots, y_n - k_n)$.

where all operations are performed in \mathbb{Z}_{26} .

An example

Assume the keyword is "CIPHER" which $\leftrightarrow K = (2, 8, 15, 7, 4, 17)$.

Plaintext: thiscryptosystemisnotsecure

$$\begin{array}{cccccccccccccccccccccccc} \leftrightarrow & 19 & 7 & 8 & 18 & 2 & 17 & 24 & 15 & 19 & 14 & 18 & 24 & 18 & 19 & 4 & 12 & 8 & 18 & \dots \\ \oplus & 2 & 8 & 15 & 7 & 4 & 17 & 2 & 8 & 15 & 7 & 4 & 17 & 2 & 8 & 15 & 7 & 4 & 17 & \dots \\ =: & 21 & 15 & 23 & 25 & 6 & 8 & 0 & 23 & 8 & 21 & 22 & 15 & 20 & 1 & 19 & 19 & 12 & 9 & \dots \end{array}$$

Ciphertext: VPXZGIAXICWPUBTTMJPWIZITWZT

A plaintext letter may be decrypted as different cipher letters.

polyalphabetic

The Vigenere Cipher

monoalphabetic (单表) v.s. polyalphabetic (多表)

- the **monoalphabetic** (单表) cryptosystem: each alphabetic character is mapped to a unique alphabetic character.
- the **polyalphabetic** (多表) cryptosystem: an alphabetic character can be mapped to one of several possible alphabetic characters.

Some Issues:

- The Vigenere cipher is **polyalphabetic**:
 - the key is a string of length n ;
 - n characters are encrypted at a time;
 - an alphabetic character can be mapped to one of n possible alphabetic characters if the keyword contains n distinct characters.
- It is named after Blaise de Vigenere (in the sixteenth century).
- The size of Keyspace is 26^n ; $26^5 \approx 1.19 \times 10^7$, $26^{10} \approx 1.4 \times 10^{14}$.
- It can be analyzed by some statistical methods **Kasiski test, index of coincidence --> n**

The Hill Cipher

Cryptosystem 2.5: Hill Cipher (on Page 32)

Let $n \in \mathbb{Z}^+$ and $n \geq 2$. Let $\mathcal{P} = \mathcal{K} = \mathcal{C} = (\mathbb{Z}_{26})^n$. Let

$$\mathcal{K} = \{n \times n \text{ invertible matrices over } \mathbb{Z}_{26}\}. \quad (2.2)$$

For a key $K \in \mathcal{K}$, define

- Encryption: $e_K(x) = xK$;
- Decryption: $d_K(y) = yK^{-1}$.

where all operations are performed in \mathbb{Z}_{26} .

Theorem 2.3 on Page 30

$$K^{-1} = (\det K)^{-1} K^*$$

K^* is the adjoint matrix of K

$$k_{ij}^* = (-1)^{i+j} \det K_{ji}$$

The Hill Cipher

Cryptosystem 2.5: Hill Cipher (on Page 32)

Let $n \in \mathbb{Z}^+$ and $n \geq 2$. Let $\mathcal{P} = \mathcal{K} = \mathcal{C} = (\mathbb{Z}_{26})^n$. Let

$$\mathcal{K} = \{n \times n \text{ invertible matrices over } \mathbb{Z}_{26}\}. \quad (2.2)$$

For a key $K \in \mathcal{K}$, define

- Encryption: $e_K(x) = \underline{x}K$;
- Decryption: $d_K(y) = \underline{y}K^{-1}$.

where all operations are performed in \mathbb{Z}_{26} .

Some Issues:

- The Hill cipher is another **polyalphabetic** cryptosystem, invented in 1929 by Lester S. Hill.
- The Hill cipher can be broken using the known plaintext attack, which assumes that Oscar knows at least n distinct plaintext-ciphertext pairs.

Outline

- 1 Basics of a Cryptosystem
- 2 Substitution Ciphers
- 3 The Permutation Cipher**
- 4 Stream Ciphers
- 5 Cryptanalysis
- 6 Conclusions

The Permutation Cipher

Cryptosystem 2.6: Permutation Cipher, 置换密码(on Page 33)

Let $m \in \mathbb{Z}^+$. Let $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m$. Let \mathcal{K} consist of all **permutations of** $\mathcal{M} = \{1, 2, \dots, m\}$. For a key $\pi \in \mathcal{K}$, define

- Encryption: $e_\pi(x_1, x_2, \dots, x_m) = (x_{\pi(1)}, x_{\pi(2)}, \dots, x_{\pi(m)})$;
- Decryption: $d_\pi(y_1, y_2, \dots, y_m) = (y_{\pi^{-1}(1)}, y_{\pi^{-1}(2)}, \dots, y_{\pi^{-1}(m)})$.

The Permutation Cipher

Cryptosystem 2.6: Permutation Cipher, 置换密码(on Page 33)

Let $m \in \mathbb{Z}^+$. Let $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m$. Let \mathcal{K} consist of all permutations of $\mathcal{M} = \{1, 2, \dots, m\}$. For a key $\pi \in \mathcal{K}$, define

- Encryption: $e_\pi(x_1, x_2, \dots, x_m) = (x_{\pi(1)}, x_{\pi(2)}, \dots, x_{\pi(m)})$;
- Decryption: $d_\pi(y_1, y_2, \dots, y_m) = (y_{\pi^{-1}(1)}, y_{\pi^{-1}(2)}, \dots, y_{\pi^{-1}(m)})$.

此处, π 是位置集合 $\mathcal{M} = \{1, 2, \dots, m\}$ 上的一个置换, π^{-1} 是 π 的逆置换.

The Permutation Cipher

Cryptosystem 2.6: Permutation Cipher, 置换密码(on Page 33)

Let $m \in \mathbb{Z}^+$. Let $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m$. Let \mathcal{K} consist of all **permutations of** $\mathcal{M} = \{1, 2, \dots, m\}$. For a key $\pi \in \mathcal{K}$, define

- Encryption: $e_\pi(x_1, x_2, \dots, x_m) = (x_{\pi(1)}, x_{\pi(2)}, \dots, x_{\pi(m)})$;
- Decryption: $d_\pi(y_1, y_2, \dots, y_m) = (y_{\pi^{-1}(1)}, y_{\pi^{-1}(2)}, \dots, y_{\pi^{-1}(m)})$.

此处, π 是位置集合 $\mathcal{M} = \{1, 2, \dots, m\}$ 上的一个置换, π^{-1} 是 π 的逆置换.

Some Issues:

- The Permutation Cipher
keeps the plaintext characters unchanged, but alters their positions.
- The size of Keyspace is $m!$.

The Permutation Cipher

Cryptosystem 2.6: Permutation Cipher, 置换密码(on Page 33)

Let $m \in \mathbb{Z}^+$. Let $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m$. Let \mathcal{K} consist of all **permutations of** $\mathcal{M} = \{1, 2, \dots, m\}$. For a key $\pi \in \mathcal{K}$, define

- Encryption: $e_\pi(x_1, x_2, \dots, x_m) = (x_{\pi(1)}, x_{\pi(2)}, \dots, x_{\pi(m)});$
- Decryption: $d_\pi(y_1, y_2, \dots, y_m) = (y_{\pi^{-1}(1)}, y_{\pi^{-1}(2)}, \dots, y_{\pi^{-1}(m)}).$

此处, π 是位置集合 $\mathcal{M} = \{1, 2, \dots, m\}$ 上的一个置换, π^{-1} 是 π 的逆置换.

Some Issues:

- The Permutation Cipher
keeps the plaintext characters unchanged, but alters their positions.
- The size of Keyspace is $m!$.

Examples

See Pages 32-33, Example 2.7.

The Permutation Cipher is a special case of the Hill Cipher.

Outline

- 1 Basics of a Cryptosystem
- 2 Substitution Ciphers
- 3 The Permutation Cipher
- 4 Stream Ciphers**
- 5 Cryptanalysis
- 6 Conclusions

Block cipher v.s. Stream Cipher

- Block cipher: successive plaintext elements are encrypted by the same key:

$$\mathbf{y} = y_1 y_2 \cdots = e_K(x_1) e_K(x_2) \cdots$$

- Stream cipher: to generate a Keystream $\mathbf{z} = z_1 z_2 \cdots$, and use it to encrypt a plaintext string:

$$\mathbf{y} = y_1 y_2 \cdots = e_{z_1}(x_1) e_{z_2}(x_2) \cdots$$

A block cipher can be seen as a special case of a stream cipher.

Stream Ciphers

Block cipher v.s. Stream Cipher

- Block cipher: successive plaintext elements are encrypted by the same key:

$$\mathbf{y} = y_1 y_2 \cdots = e_K(x_1) e_K(x_2) \cdots$$

- Stream cipher: to generate a Keystream $\mathbf{z} = z_1 z_2 \cdots$, and use it to encrypt a plaintext string:

$$\mathbf{y} = y_1 y_2 \cdots = e_{z_1}(x_1) e_{z_2}(x_2) \cdots$$

A block cipher can be seen as a special case of a stream cipher.

Synchronous v.s. Non-Synchronous

- Is the keystream constructed from the key which is independent of the plaintext and ciphertext?

The Synchronous Stream Cipher

Definition 2.6: Synchronous Stream Cipher, **SSC** (on Page 35)

An **SSC** is a six-tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{L}, \mathcal{E}, \mathcal{D})$ with a function g :

- ① \mathcal{P} is a finite set of all possible *plaintexts*,
- ② \mathcal{C} is a finite set of all possible *ciphertexts*,
- ③ \mathcal{K} is a finite set of all possible *keys*, called *keyspace*,
- ④ \mathcal{L} is a finite set called the *keystream alphabet*,
- ⑤ g is the *keystream generator*. g takes a key $K \in \mathcal{K}$ as input, and generates an infinite string $z_1 z_2 \cdots$ called the *keystream*, $z_i \in \mathcal{L}$,
- ⑥ For each $z \in \mathcal{L}$, there is $e_z \in \mathcal{E}$ & $d_z \in \mathcal{D}$
Encryption rule $e_z : \mathcal{P} \rightarrow \mathcal{C}$ & Decryption rule $d_z : \mathcal{C} \rightarrow \mathcal{P}$,
satisfying $d_z(e_z(x)) = x$ for every $x \in \mathcal{P}$.

The Synchronous Stream Cipher

Definition 2.6: Synchronous Stream Cipher, **SSC** (on Page 35)

An **SSC** is a six-tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{L}, \mathcal{E}, \mathcal{D})$ with a function g :

- ① \mathcal{P} is a finite set of all possible *plaintexts*,
- ② \mathcal{C} is a finite set of all possible *ciphertexts*,
- ③ \mathcal{K} is a finite set of all possible *keys*, called *keyspace*,
- ④ \mathcal{L} is a finite set called the *keystream alphabet*,
- ⑤ g is the *keystream generator*. g takes a key $K \in \mathcal{K}$ as input, and generates an infinite string $z_1 z_2 \dots$ called the *keystream*, $z_i \in \mathcal{L}$,
- ⑥ For each $z \in \mathcal{L}$, there is $e_z \in \mathcal{E}$ & $d_z \in \mathcal{D}$
Encryption rule $e_z : \mathcal{P} \rightarrow \mathcal{C}$ & Decryption rule $d_z : \mathcal{C} \rightarrow \mathcal{P}$,
satisfying $d_z(e_z(x)) = x$ for every $x \in \mathcal{P}$.

Some Issues:

- A stream cipher is *periodic* with period d if $z_{i+d} = z_i$ for **all** integers $i \geq 1$.

The Vigenere Cipher can be defined as a periodic SSC.

The SSC over Binary Alphabets

Let $\mathcal{P} = \mathcal{C} = \mathcal{L} = \mathbb{Z}_2$, $\mathcal{K} = \{k_1, k_2, \dots, k_m; c_0, c_1, \dots, c_{m-1}\} = \mathbb{Z}_2^{2m}$.

- ① The keystream is generated by a linear recurrence g of degree m :

$$z_{i+m} = \sum_{j=0}^{m-1} c_j z_{i+j} \pmod{2}, \quad (4.1)$$

for all $i \geq 1$, where $c_0, \dots, c_{m-1} \in \mathbb{Z}_2$ are constants, and $z_i = k_i, 1 \leq i \leq m$.

- ② For each $z \in \mathcal{L}$, define

Encryption rule $e_z(x) = (x + z) \pmod{2}$;

Decryption rule $d_z(y) = (y + z) \pmod{2}$.

- g : degree m (if $c_0 = 1$), linear, period $2^m - 1$ (for binary case) if c_0, \dots, c_{m-1} are proper;

The SSC over Binary Alphabets

Let $\mathcal{P} = \mathcal{C} = \mathcal{L} = \mathbb{Z}_2$, $\mathcal{K} = \{k_1, k_2, \dots, k_m; c_0, c_1, \dots, c_{m-1}\} = \mathbb{Z}_2^{2m}$.

- ① The keystream is generated by a linear recurrence g of degree m :

$$z_{i+m} = \sum_{j=0}^{m-1} c_j z_{i+j} \pmod{2}, \quad (4.1)$$

for all $i \geq 1$, where $c_0, \dots, c_{m-1} \in \mathbb{Z}_2$ are constants, and $z_i = k_i, 1 \leq i \leq m$.

- ② For each $z \in \mathcal{L}$, define

Encryption rule $e_z(x) = (x + z) \pmod{2}$;

Decryption rule $d_z(y) = (y + z) \pmod{2}$.

- g : degree m (if $c_0 = 1$), linear, period $2^m - 1$ (for binary case) if c_0, \dots, c_{m-1} are proper;
- keystream can be produced in hardware by a Linear Feedback Shift Register

The SSC over Binary Alphabets

Let $\mathcal{P} = \mathcal{C} = \mathcal{L} = \mathbb{Z}_2$, $\mathcal{K} = \{k_1, k_2, \dots, k_m; c_0, c_1, \dots, c_{m-1}\} = \mathbb{Z}_2^{2m}$.

- ① The keystream is generated by a linear recurrence g of degree m :

$$z_{i+m} = \sum_{j=0}^{m-1} c_j z_{i+j} \pmod{2}, \quad (4.1)$$

for all $i \geq 1$, where $c_0, \dots, c_{m-1} \in \mathbb{Z}_2$ are constants, and $z_i = k_i, 1 \leq i \leq m$.

- ② For each $z \in \mathcal{L}$, define

Encryption rule $e_z(x) = (x + z) \pmod{2}$;

Decryption rule $d_z(y) = (y + z) \pmod{2}$.

- g : degree m (if $c_0 = 1$), linear, period $2^m - 1$ (for binary case) if c_0, \dots, c_{m-1} are proper;
- keystream can be produced in hardware by a Linear Feedback Shift Register
- See Pages 36-37, Example 2.8.

Cryptanalysis on the SSC over Binary Alphabets

A known plaintext attack on the LFSR Stream cipher

(See Section 2.2.5)

A Non-Synchronous Stream Cipher

A non-synchronous stream cipher: each keystream element z_i depends on previous plaintext or ciphertext elements as well as the key K

Cryptosystem 2.7: Autokey Cipher (Non-Synchronous) (on Page 38)

Let $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathcal{L} = \mathbb{Z}_{26}$. Let $z_1 = K$, and define $z_i = x_{i-1}$ for all $i \geq 2$. For $0 \leq z \leq 25$, define

Encryption rule $e_z(x) = (x + z)(\text{mod } 26)$;

Decryption rule $d_z(y) = (y - z)(\text{mod } 26)$.

Examples

See Pages 37-38, Example 2.9.

Outline

- 1 Basics of a Cryptosystem
- 2 Substitution Ciphers
- 3 The Permutation Cipher
- 4 Stream Ciphers
- 5 Cryptanalysis**
- 6 Conclusions

A general assumption

- Kerckhoff's Principle: The opponent, Oscar, knows the cryptosystem being used.

A general assumption

- Kerckhoff's Principle: The opponent, Oscar, knows the cryptosystem being used.

The most Common Types of Attack Models:

The attack model specifies the information available to the adversary.

- ① **ciphertext-only attack**: a string of ciphertext y
- ② **known plaintext attack**: plaintext x and the corresponding y
- ③ **chosen plaintext attack**: access Enc, choose x and construct the corresponding y
- ④ **chosen ciphertext attack**: access Dec, choose y and construct the corresponding x

Cryptanalysis

A general assumption

- Kerckhoff's Principle: The opponent, Oscar, knows the cryptosystem being used.

The most Common Types of Attack Models:

The attack model specifies the information available to the adversary.

- ① **ciphertext-only attack**: a string of ciphertext y
- ② **known plaintext attack**: plaintext x and the corresponding y
- ③ **chosen plaintext attack**: access Enc, choose x and construct the corresponding y
- ④ **chosen ciphertext attack**: access Dec, choose y and construct the corresponding x

Objective of the attack

- To determine the key K .

Cryptanalysis

Some Issues:

- The weakest type of attack is the ciphertext-only attack.
- The statistical properties of the English language (see Page 40) are usually used in cryptanalysis.

Cryptanalysis: To determine the key K

- 1 A Ciphertext-only attack on the Affine cipher:
By using Statistical properties of the English language, See pages 40-42.
- 2 A Ciphertext-only attack on the Substitution cipher:
By using Statistical properties of the English language, See pages 42-44.
- 3 A Ciphertext-only attack on the Vigenere cipher:
To determine the keyword length: Kasiski test or the index of coincidence;
To determine the keyword: Statistical methods, See pages 45-48.
- 4 A known plaintext attack on the Hill cipher: (See pages 48-49)
- 5 A known plaintext attack on the LFSR Stream cipher: (See pages 49-51)

Outline

- 1 Basics of a Cryptosystem
- 2 Substitution Ciphers
- 3 The Permutation Cipher
- 4 Stream Ciphers
- 5 Cryptanalysis
- 6 Conclusions**

Conclusions

- 1 Basics of a Cryptosystem
- 2 Substitution Ciphers
- 3 The Permutation Cipher
- 4 Stream Ciphers
- 5 Cryptanalysis
- 6 Conclusions

Homework 1

Problem Set 1

Exercises: 2.1, 2.7, 2.8, 2.9, 2.10, 2.15(a), 2.16,
2.18, 2.23, 2.30(with executable codes)

Thanks for your attention!

Questions?



暨南大學
JINAN UNIVERSITY