Classical Cryptography

- Shift cipher
- Substitution cipher
- Affine cipher
- Vigenère Cipher
- Hill Cipher

References

- Douglas Stinson, Cryptography: Theory and Practice, 3rd, Chapman & Hall CRC, 2006.
  - Chapter 1

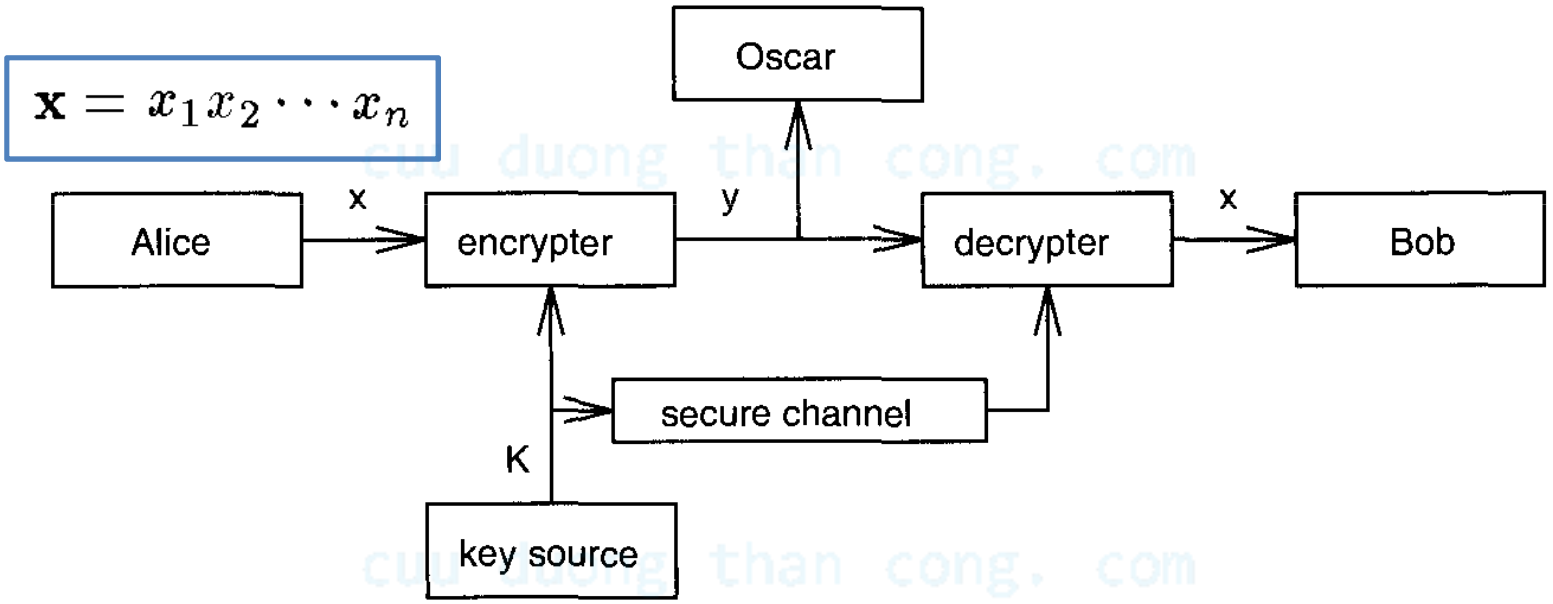
cuu duong than cong. com

Secure communication scheme

$$\mathbf{y} = y_1 y_2 \cdots y_n$$

$$y_i = e_K(x_i), 1 \leq i \leq n,$$

$$\mathbf{x} = x_1 x_2 \cdots x_n$$



The set of integers modulo m: $\mathbb{Z}_m$

- Remarks:
  - ***Congruences*** $a \equiv b \pmod{m}$ if m divides $b-a$.
  - $\mathbb{Z}_m$ is the set $\{0, \ldots, m-1\}$
  - $\mathbb{Z}_m$ is a ***ring***.
- Examples:
  - $\mathbb{Z}_{26} = \{0, 1, 2, \ldots, 25\}$.
  - $14 + 20 = 8$ in $\mathbb{Z}_{26}$.
  - $5*7 = 9$ in $\mathbb{Z}_{26}$.

We will always consider (a mod b) >= 0

Lab computing: try operators + and * modulo m in C, Java, Maple, Matlab and Python.

Exercises

Lab computing: try "MOD" or "%" operator in C, Java, Maple, Matlab and Python.

1.1 Evaluate the following:

(a) $7503 \bmod 81$

(b) $(-7503) \bmod 81$

(c) $81 \bmod 7503$

(d) $(-81) \bmod 7503$.

1.2 Suppose that $a, m > 0$, and $a \not\equiv 0 \pmod{m}$. Prove that

$$(-a) \bmod m = m - (a \bmod m).$$

1.4 Prove that $a \bmod m = a - \left\lfloor \frac{a}{m} \right\rfloor m$,

The Shift Cipher

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

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

$$e_K(x) = (x + K) \bmod 26$$

and

$$d_K(y) = (y - K) \bmod 26$$

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

For the particular key K = 3, the cryptosystem is often called the ***Caesar Cipher***, which was purportedly used by Julius Caesar.

The Shift Cipher Encryption

Suppose the key for a *Shift Cipher* is $K = 11$, and the plaintext is

```
wewillmeetatmidnight.
```

We first convert the plaintext to a sequence of integers using the specified correspondence, obtaining the following:

22	4	22	8	11	11	12	4	4	19
0	19	12	8	3	13	8	6	7	19

Next, we add 11 to each value, reducing each sum modulo 26:

7	15	7	19	22	22	23	15	15	4
11	4	23	19	14	24	19	17	18	4

Finally, we convert the sequence of integers to alphabetic characters, obtaining the ciphertext:

```
HPHTWWXPPELEXTOYTRSE.
```

The Shift Cipher Decryption

To decrypt the ciphertext, Bob will first convert the ciphertext to a sequence of integers, then subtract 11 from each value (reducing modulo 26), and finally convert the sequence of integers to alphabetic characters. □

HPHTWWXPPELEXTOYTRSE.

7	15	7	19	22	22	23	15	15	4
11	4	23	19	14	24	19	17	18	4

22	4	22	8	11	11	12	4	4	19
0	19	12	8	3	13	8	6	7	19

wewillmeetatmidnight.

Caesar cipher (K = 3)

- x = “NGUYENTHANHNHUT”
- y = “QJXBHQWKDQKQKXW”

Now Cryptool it!

Practical cryptosystems

1. Each encryption function e_k and each decryption function d_k should be efficiently computable.
2. An opponent, upon seeing a ciphertext string y, should be unable to determine the key k that was used, or the plaintext string x.

"***Security***"

The process of attempting to compute the key k, given a string of ciphertext y, is called ***cryptanalysis***.

Security of the Shift cipher

- The Shift Cipher (modulo 26) is not secure.
- It can be cryptanalyzed by the obvious method of exhaustive key search.
  - Since there are only 26 possible keys, it is easy to try every possible decryption rule d_k ($k = 0, \ldots, 25$) until a "meaningful" plaintext string is obtained.
  - On average, a plaintext will be computed using this method after trying 26/2 = 13 decryption rules.

→ a necessary condition for a cryptosystem to be secure is that an exhaustive key search should be infeasible; i.e., the keyspace should be very large.

Exercise

Lab computing: build a ShiftCipher encrypt and decrypt functions to do this

Take a short break ☺

1.5 Use exhaustive key search to decrypt the following ciphertext, which was encrypted using a *Shift Cipher*:

BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUYJIIKFUHCQD.

1.6 If an encryption function e_K is identical to the decryption function d_K, then the key K is said to be an *involutory key*. Find all the involutory keys in the *Shift Cipher* over $\mathbb{Z}_{26}$.

The Substitution Cipher

π.

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

$$e_\pi(x) = \pi(x)$$

A	B	C	D	E	F	G	H	I	J	K	L	M
d	l	r	y	v	o	h	e	z	x	w	p	t

π^{-1}

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	g	f	j	q	n	m	u	s	k	a	c	i

$$d_\pi(y) = \pi^{-1}(y)$$

The Substitution Cipher

Lab computing: decrypt this by define a SubCipher decrypt function

MGZVYZLGHCMHJMYXSSFMNHAHYCDLMHA.

A	B	C	D	E	F	G	H	I	J	K	L	M
d	l	r	y	v	o	h	e	z	x	w	p	t

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	g	f	j	q	n	m	u	s	k	a	c	i

Try Cryptool it!

- A key for the Substitution Cipher just consists of a permutation of the 26 alphabetic characters.
- The number of possible permutations is 26!, which is more than $4*10^{26}$, a very large number.

Euler phi-function

Definition 1.3: Suppose $a \geq 1$ and $m \geq 2$ are integers. If $\gcd(a, m) = 1$, then we say that a and m are *relatively prime*. The number of integers in $\mathbb{Z}_m$ that are relatively prime to m is often denoted by $\phi(m)$ (this function is called the *Euler phi-function*).

Lab computing: define GCD and PHI functions in Python to compute gcd(a,b) and phi(n). Compare time running with MAPLE.

Ex:

- $\phi(10) = 4$.
- $\phi(11) = 10$.

Compute the Euler phi-function

THEOREM 1.2 *Suppose*

$$m = \prod_{i=1}^{n} {p_i}^{e_i},$$

where the p_i*'s are distinct primes and* $e_i > 0$, $1 \leq i \leq n$. *Then*

$$\phi(m) = \prod_{i=1}^{n} ({p_i}^{e_i} - p_i^{e_i - 1}).$$

$$60 = 2^2 \times 3^1 \times 5^1$$

$$\phi(60) = (4 - 2) \times (3 - 1) \times (5 - 1) = 2 \times 2 \times 4 = 16.$$

The multiplicative inverse modulo m

Definition 1.4: Suppose $a \in \mathbb{Z}_m$. The *multiplicative inverse* of a modulo m, denoted $a^{-1} \bmod m$, is an element $a' \in \mathbb{Z}_m$ such that $aa' \equiv a'a \equiv 1 \pmod{m}$. If m is fixed, we sometimes write a^{-1} for $a^{-1} \bmod m$.

For $m = 26$:

$$1^{-1} = 1,$$

$$3^{-1} = 9,$$

$$5^{-1} = 21,$$

$$7^{-1} = 15, \qquad 7 \times 15 = 105 \equiv 1 \pmod{26}$$

$$11^{-1} = 19,$$

$$17^{-1} = 23, \text{ and}$$

$$25^{-1} = 25.$$

Exercise

1.8 List all the invertible elements in $\mathbb{Z}_m$ for $m = 28, 33$ and 35.

1.9 For $1 \leq a \leq 28$, determine $a^{-1} \mod 29$ by trial and error.

The Affine Cipher

Let $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$ and let

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

For $K = (a, b) \in \mathcal{K}$, define

$$e_K(x) = (ax + b) \bmod 26$$

and

$$d_K(y) = a^{-1}(y - b) \bmod 26$$

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

Example 1.3 Suppose that $K = (7, 3)$. As noted above, $7^{-1} \bmod 26 = 15$. The encryption function is

$$e_K(x) = 7x + 3,$$

and the corresponding decryption function is

$$d_K(y) = 15(y - 3) = 15y - 19,$$

To illustrate, let's encrypt the plaintext *hot*. We first convert the letters h, o, t to residues modulo 26. These are respectively 7, 14, and 19. Now, we encrypt:

$$\begin{aligned}(7 \times 7 + 3) \bmod 26 &= 52 \bmod 26 = 0\\ (7 \times 14 + 3) \bmod 26 &= 101 \bmod 26 = 23\\ (7 \times 19 + 3) \bmod 26 &= 136 \bmod 26 = 6.\end{aligned}$$

So the three ciphertext characters are 0, 23, and 6, which corresponds to the alphabetic string AXG.

Security of the Affine cipher

THEOREM 1.1 *The congruence* $ax \equiv b \pmod{m}$ *has a unique solution* $x \in \mathbb{Z}_m$ *for every* $b \in \mathbb{Z}_m$ *if and only if* $\gcd(a, m) = 1$.

Since $26 = 2 \times 13$, the values of $a \in \mathbb{Z}_{26}$ such that $\gcd(a, 26) = 1$ are $a = 1$, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, and 25. The parameter b can be any element in $\mathbb{Z}_{26}$. Hence the *Affine Cipher* has $12 \times 26 = 312$ possible keys. (Of course, this is much too small to be secure.)

1.7 Determine the number of keys in an *Affine Cipher* over $\mathbb{Z}_m$ for $m = 30$, 100 and 1225.

1.10 Suppose that $K = (5, 21)$ is a key in an *Affine Cipher* over $\mathbb{Z}_{29}$.

(a) Express the decryption function $d_K(y)$ in the form $d_K(y) = a'y + b'$, where $a', b' \in \mathbb{Z}_{29}$.

(b) Prove that $d_K(e_K(x)) = x$ for all $x \in \mathbb{Z}_{29}$.

1.11

(a) Suppose that $K = (a, b)$ is a key in an *Affine Cipher* over $\mathbb{Z}_n$. Prove that K is an involutory key if and only if $a^{-1} \bmod n = a$ and $b(a + 1) \equiv 0 \pmod{n}$.

(b) Determine all the involutory keys in the *Affine Cipher* over $\mathbb{Z}_{15}$.

(c) Suppose that $n = pq$, where p and q are distinct odd primes. Prove that the number of involutory keys in the *Affine Cipher* over $\mathbb{Z}_n$ is $n + p + q + 1$.

Take a short break ☺

The Vigenère Cipher

Let m be a positive integer. Define $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_{26})^m$. For a key $K = (k_1, k_2, \ldots, k_m)$, we define

$$e_K(x_1, x_2, \ldots, x_m) = (x_1 + k_1, x_2 + k_2, \ldots, x_m + k_m)$$

and

$$d_K(y_1, y_2, \ldots, y_m) = (y_1 - k_1, y_2 - k_2, \ldots, y_m - k_m),$$

- Each key k is an alphabetic string of length m, called a ***keyword***.
- The Vigenere Cipher encrypts m alphabetic characters at a time.

Example 1.4 Suppose $m = 6$ and the keyword is $CIPHER$. This corresponds to the numerical equivalent $K = (2, 8, 15, 7, 4, 17)$. Suppose the plaintext is the string

`thiscryptosystemisnotsecure.`

We convert the plaintext elements to residues modulo 26, write them in groups of six, and then "add" the keyword modulo 26, as follows:

19	7	8	18	2	17	24	15	19	14	18	24	
2	8	15	7	4	17	2	8	15	7	4	17	
21	15	23	25	6	8	0	23	8	21	22	15	

18	19	4	12	8	18	13	14	19	18	4	2	20	17	4
2	8	15	7	4	17	2	8	15	7	4	17	2	8	15
20	1	19	19	12	9	15	22	8	25	8	19	22	25	19

`VPXZGIAXIVWPUBTTMJPWIZITWZT.`

Try Cryptool it!

Security of the Vigenere Cipher

- The number of possible keywords of length m is 26^m, even for relatively small values of m, an exhaustive key search would require a long time.
- An alphabetic character can be mapped to one of m possible alphabetic characters (assuming that the keyword contains m distinct characters). Such a cryptosystem is called a ***polyalphabetic cryptosystem***.
- In general, cryptanalysis is more difficult for polyalphabetic than for ***monoalphabetic cryptosystems*** (Shift Cipher, Substitution Cipher).

The Hill Cipher

Let $m \geq 2$ be an integer. Let $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m$ and let

$$\mathcal{K} = \{m \times m \text{ invertible matrices over } \mathbb{Z}_{26}\}.$$

For a key K, we define

$$e_K(x) = xK$$

and

$$d_K(y) = yK^{-1},$$

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

Example 1.5 Suppose the key is

$$K = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}.$$

in $\mathbb{Z}_{26}$:

$$\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}^{-1} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$$

since

$$\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}\begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} = \begin{pmatrix} 11 \times 7 + 8 \times 23 & 11 \times 18 + 8 \times 11 \\ 3 \times 7 + 7 \times 23 & 3 \times 18 + 7 \times 11 \end{pmatrix}$$

$$= \begin{pmatrix} 261 & 286 \\ 182 & 131 \end{pmatrix}$$

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

Suppose we want to encrypt the plaintext *july*. We have two elements of plaintext to encrypt: $(9, 20)$ (corresponding to *ju*) and $(11, 24)$ (corresponding to *ly*). We compute as follows:

$$(9, 20)\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} = (99 + 60, 72 + 140) = (3, 4)$$

and

$$(11, 24)\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} = (121 + 72, 88 + 168) = (11, 22).$$

Hence, the encryption of *july* is *DELW*. To decrypt, Bob would compute:

$$(3, 4)\begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} = (9, 20)$$

and

$$(11, 22)\begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} = (11, 24).$$

Hence, the correct plaintext is obtained.

1.12

(a) Let p be prime. Prove that the number of 2×2 matrices that are invertible over $\mathbb{Z}_p$ is $(p^2 - 1)(p^2 - p)$.

HINT Since p is prime, $\mathbb{Z}_p$ is a field. Use the fact that a matrix over a field is invertible if and only if its rows are linearly independent vectors (i.e., there does not exist a non-zero linear combination of the rows whose sum is the vector of all 0's).

(b) For p prime and $m \geq 2$ an integer, find a formula for the number of $m \times m$ matrices that are invertible over $\mathbb{Z}_p$.

1.13 For $n = 6, 9$ and 26,

how many 2×2 matrices are there that are invertible over $\mathbb{Z}_n$?

1.14

(a) Prove that $\det A \equiv \pm 1 \pmod{26}$ if A is a matrix over $\mathbb{Z}_{26}$ such that $A = A^{-1}$.

(b) Use the formula given in Corollary 1.4 to determine the number of involutory keys in the *Hill Cipher* (over $\mathbb{Z}_{26}$) in the case $m = 2$.

1.15 Determine the inverses of the following matrices over $\mathbb{Z}_{26}$:

(a) $\begin{pmatrix} 2 & 5 \\ 9 & 5 \end{pmatrix}$

(b) $\begin{pmatrix} 1 & 11 & 12 \\ 4 & 23 & 2 \\ 17 & 15 & 9 \end{pmatrix}$

- **Think about the security of the Hill Cipher!**

The Permutation Cipher

Let m be a positive integer. Let $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m$ and let $\mathcal{K}$ consist of all permutations of $\{1, \ldots, m\}$. For a key (i.e., a permutation) π, we define

$$e_\pi(x_1, \ldots, x_m) = (x_{\pi(1)}, \ldots, x_{\pi(m)})$$

and

$$d_\pi(y_1, \ldots, y_m) = (y_{\pi^{-1}(1)}, \ldots, y_{\pi^{-1}(m)}),$$

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

Example 1.7 Suppose $m = 6$ and the key is the following permutation π:

x	1	2	3	4	5	6
$\pi(x)$	3	5	1	6	4	2

π^{-1} can be constructed by interchanging the two rows.

x	1	2	3	4	5	6
$\pi^{-1}(x)$	3	6	1	5	2	4

Now, suppose we are given the plaintext

shesellsseashellsbytheseashore.

We first partition the plaintext into groups of six letters:

shesel | lsseas | hellsb | ythese | ashore

x	1	2	3	4	5	6
$\pi(x)$	3	5	1	6	4	2

Now each group of six letters is rearranged according to the permutation π, yielding the following:

EESLSH | SALSES | LSHBLE | HSYEET | HRAEOS

So, the ciphertext is:

EESLSHSALSESLSHBLEHSYEETHRAEOS.

1.16

(a) Suppose that π is the following permutation of $\{1, \ldots, 8\}$:

x	1	2	3	4	5	6	7	8
$\pi(x)$	4	1	6	2	7	3	8	5

Compute the permutation π^{-1}.

(b) Decrypt the following ciphertext, for a *Permutation Cipher* with $m = 8$, which was encrypted using the key π:

TGEEMNELNNTDROEOAAHDOETCSHAEIRLM.

1.17

(a) Prove that a permutation π in the *Permutation Cipher* is an involutory key if and only if $\pi(i) = j$ implies $\pi(j) = i$, for all $i, j \in \{1, \ldots, m\}$.

(b) Determine the number of involutory keys in the *Permutation Cipher* for $m = 2, 3, 4, 5$ and 6.

The Permutation Cipher is a special case of the Hill Cipher

$K_\pi = (k_{i,j})$ according to the formula

$$k_{i,j} = \begin{cases} 1 & \text{if } i = \pi(j) \\ 0 & \text{otherwise.} \end{cases}$$

x	1	2	3	4	5	6
$\pi(x)$	3	5	1	6	4	2

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