licence master professionnel en protection informatique

Co-funded by the Erasmus+ Programme of the European Union

HOCHIMINH CITY UNIVERSITY OF TECHNOLOGY

Cryptosystems

Truong Tuan Anh
CSE-HCMUT
anhtt@hcmut.edu.vn

In This Lecture

- Cryptography
- Cryptosystem: Definition
- Simple Cryptosystem
  - Shift cipher
  - Substitution cipher
  - Affine cipher
- Cryptanalysis

Cryptography

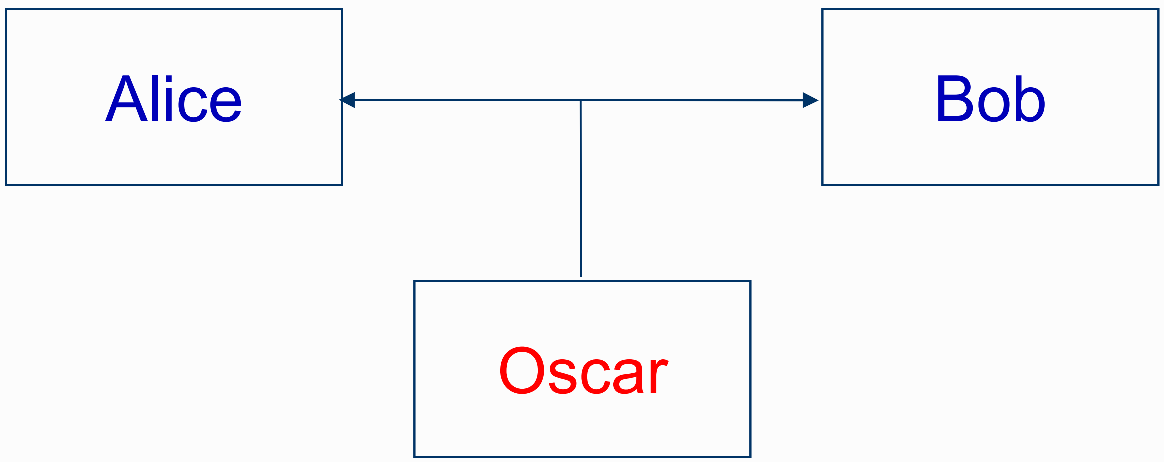
Perfect Model

- Alice and Bob want to secretly communicate to each other

1. Two parties – Alice and Bob
2. Secure communication line
3. Send messages **confidentially**

Real Model

- Alice and Bob want to secretly communicate to each other



1. Many parties – Alice, Bob, Oscar, etc…
2. Insecure communication line
3. Send messages **inconfidentially**

The Fundamental Objective

- Alice and Bob communicate over an insecure channel
  - Telephone line, computer network, etc…

→ **Objective**:

An adversary, called Oscar, **cannot understand** the conversation

Cryptography

- Cryptography is the science of using mathematics to encrypt and decrypt data

- Cryptography enables people to store sensitive information/data or transmit it across insecure networks so that no one can read it except the intended recipient

Basic Notations

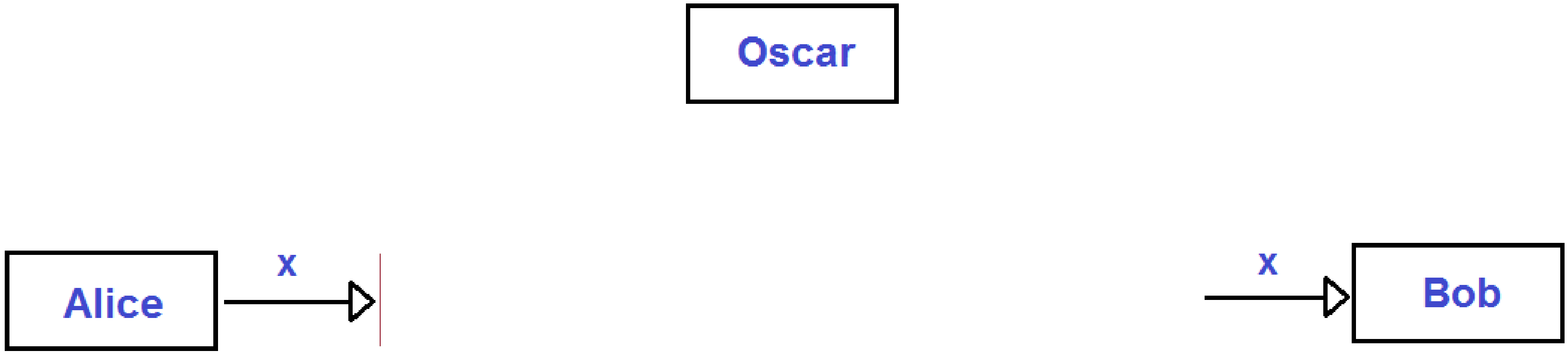
- **Plaintext**: the information Alice wants to send to Bob and vice versa
  - The structure is completely arbitrary: English text, numerical data, …
- **Ciphertext**: encrypted plaintext using a predetermined key (**encryption key**)
- **Decryption key**: for decrypting ciphertext to plaintext

Basic Notations (cont.)

- **Encryption rule** (*e*):
  - Input: plaintext and encryption key
  - Output: corresponding ciphertext

- **Decryption rule** (*d*):
  - Input: ciphertext and decryption key
  - Output: corresponding plaintext

Communication Model



Assumptions

- **Objective**:

  An adversary, called Oscar, **cannot understand** the message **x**

- Assumptions:
  - Oscar knows the rules *e, d*
  - Oscar knows the message space/structure
  - Oscar does not know *keys* used

→ Oscar wants to discover the keys

Cryptosystem

Definition

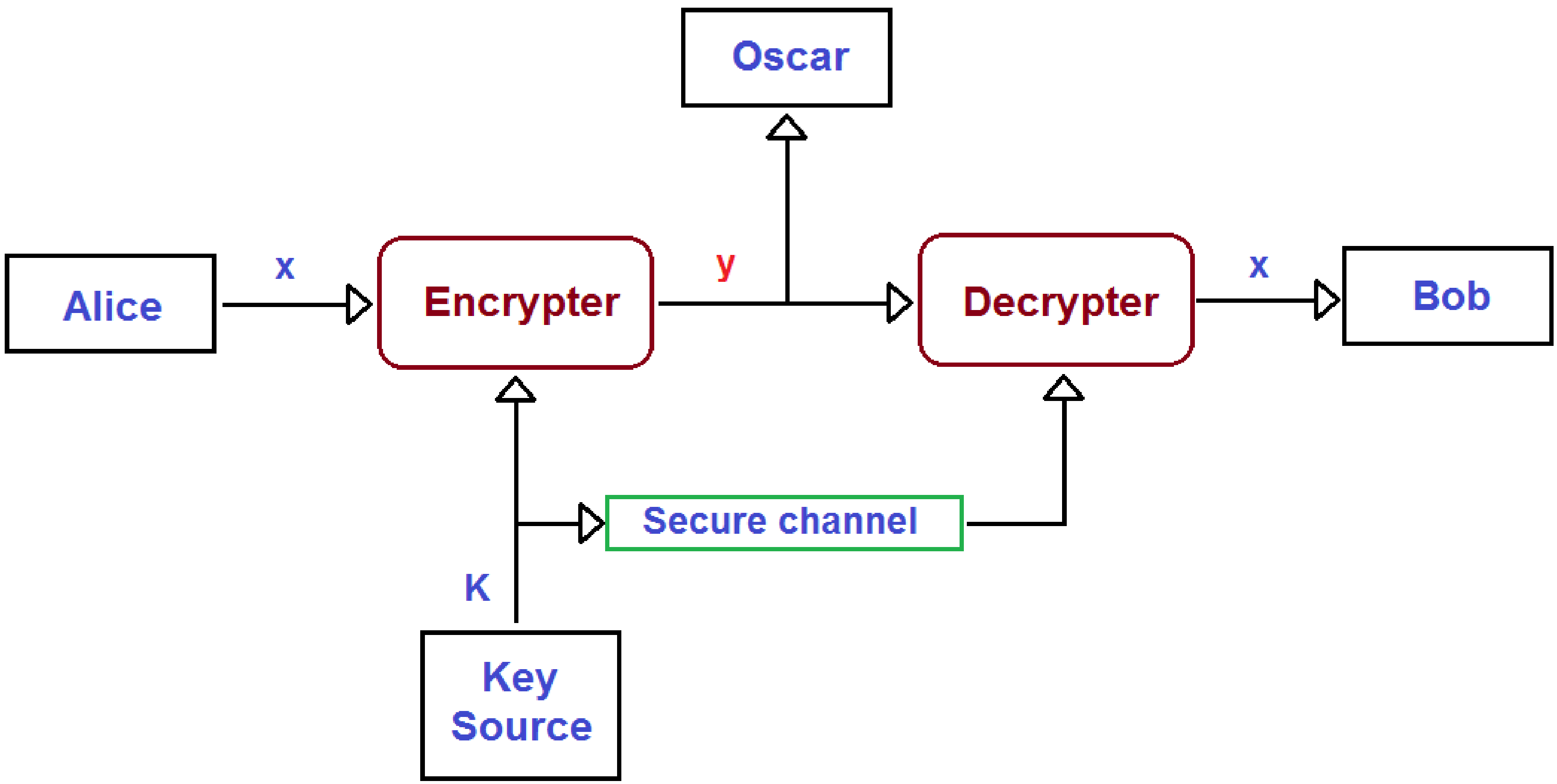
A Cryptosysytem/cipher is a five-tuple

$$(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$$

where

- $\mathcal{P}$ is a finite set of possible plaintexts;
- $\mathcal{C}$ is a finite set of possible ciphertexts;
- $\mathcal{K}$, the *keyspace*, is a finite set of possible keys;

Cryptosystem: An Example



Cryptosystem: An Example (cont.)

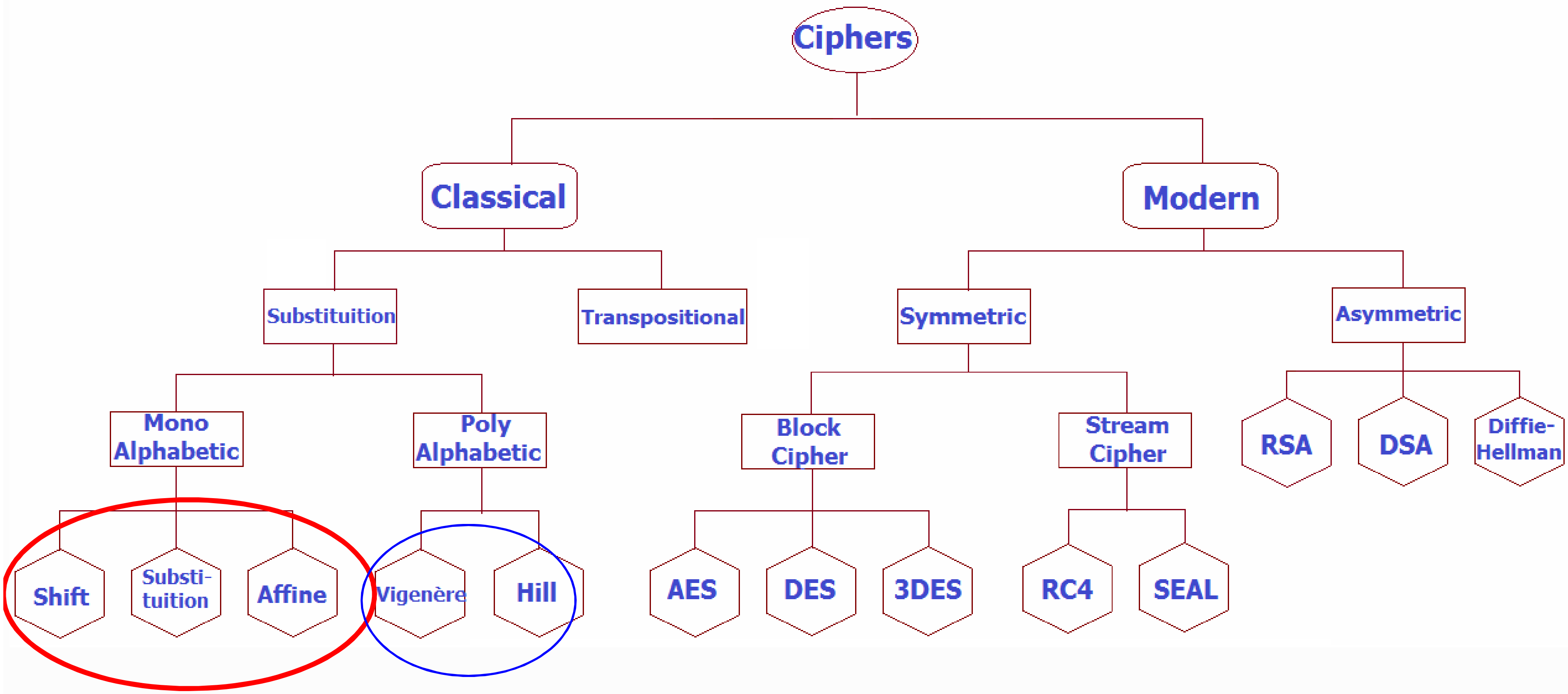
- Alice and Bob choose the same random key K
- Alice wants to send message $x = x_1 x_2 \ldots x_n$
- Alice computes $y_i = e_K(x_i)$
- Alice sends $y = y_1 y_2 \ldots y_n$

- Bob receives y
- Bob decrypts $x_i = d_K(y_i)$
- Bob obtains the plaintext $x = x_1 x_2 \ldots x_n$

Note: Each encryption rule e_k must be **one-to-one** function

Why?

Classification



Simple Cryptosystems

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

Simple Cryptosystems

- **Shift Cipher**
- Substitution Cipher
- Affine Cipher
- Vigenère Cipher
- Hill Cipher

Arithmetic Modulo

- Modular arithmetic:

  $x = y \bmod m$ iff $y = m*k + x$ and $0 \le x \le m-1$

  x , y, m, k are integer and x is non-negative

- Examples:

  155 *mod* 8 = ?

  155 mod 8 = 3

  -134 mod 23 = ?

  -134 mod 23 = 4

Arithmetic Modulo

- Modular arithmetic:

  $x = y \bmod m$ iff $y = m*k + x$ and $0 \leq x \leq m-1$

  x , *y*, *m*, *k* are integer and *x* is non-negative

- Examples:

  155 *mod* 8 = 3

  155 = 19*8 + 3

  -134 mod 23 = ?

  -134 mod 23 = 4

Arithmetic Modulo

- Modular arithmetic:

  $x = y \bmod m$ iff $y = m*k + x$ and $0 \le x \le m-1$

  x , y, m, k are integer and *x* is non-negative

- Examples:

  -134 *mod* 23 = ?

  155 = 19*8 + 3

  -134 mod 23 = ?

  -134 mod 23 = 4

Arithmetic Modulo

- Modular arithmetic:

$$x = y \bmod m \text{ iff } y = m*k + x \text{ and } 0 \le x \le m-1$$

x , *y*, *m*, *k* are integer and *x* is non-negative

- Examples:

  -134 *mod* 23 = 4

  -134 = (-6) * 23 + 4

  -134 mod 23 = ?

  -134 mod 23 = 4

Arithmetic Modulo *m* in Z_m

- Z_m is the set {0, 1, …, m-1}
- Operations in Z_m: **+** and **x**
  - Work like real addition and multiplication, except the results are reduced to modulo *m*
- Examples:

  $13 \times 15 = 13$ in Z_{26}

  $21 + 134 =$? in Z_{18}

The Shift Cipher: Definition

A Shift cipher is a five-tuple

$$(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$$

where

- $\mathcal{P} = \mathcal{C} = \mathcal{K} = Z_{26}$;
- For each $0 \leq K \leq 25$:

$$\boxed{e_K(x) = (x + K) \; mod \; 26} \quad \text{and} \quad \boxed{d_K(y) = (y - K) \; mod \; 26}$$

$$(x, y \in Z_{26})$$

- Z_{26}: 26 English letters
- When K = 3, it is the Caesar Cipher and used by Julius Caesar

The Shift Cipher: Example

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

The Shift Cipher: Example (cont.)

- Choose ***K*** **= 13**
- The plaintext is *weareatclass*

→ Encrypt it using the Shift Cipher?

- **Step 1**: convert plaintext to integers

w	e	a	r	e	a	t	c	l	a	s	s
22	4	0	17	4	0	19	2	11	0	18	18

The Shift Cipher: Example (cont.)

- **Step 2**: use the encryption rule $\boldsymbol{e_{13}}$ to add 13 to each integer and then reduce to modulo 26

22	4	0	17	4	0	19	2	11	0	18	18
13	13	13	13	13	13	13	13	13	13	13	13
9	17	13	4	17	13	6	15	24	13	5	5

- **Step 3**: convert to characters

9	17	13	4	17	13	6	15	24	13	5	5
j	r	n	e	r	n	g	p	y	n	f	f

→ The ciphertext: ***jrnerngpynff***

How to decrypt the ciphertext?

The Shift Cipher: Example (cont.)

- Choose ***K* = 11**
- The ciphertext is *hphtwwxppelextoytrse*

→ Decrypt it using the Shift Cipher?

The Shift Cipher: Review

Not secure: keyspace is 26

- Exhaustive key search is feasible

- Example: *jbcrclqrwcrvnbjenbwrwn*
  - Key 0: *jbcrclqrwcrvnbjenbwrwn*
  - Key 1: *iabqbkpqvbqumaidmavqvm*
  - …
  - Key 9: astitchintimesavesnine

  → plaintext: *a stitch in time saves nine*

- **To be secure**
  - The key space should be very large

Simple Cryptosystems

- Shift Cipher
- **Substitution Cipher**
- Affine Cipher
- Vigenère Cipher
- Hill Cipher

The Substitution Cipher: Definition

A Substitution cipher is a five-tuple

$$(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$$

where

- $\mathcal{P} = \mathcal{C} = Z_{26}$;
- $\mathcal{K}$ consists of all possible permutations of the 26 symbols 0, 1, ...,25
- For each permutation $\pi \in \mathcal{K}$:

$$\boxed{e_\pi(x) = \pi(x)} \quad \text{and} \quad \boxed{d_\pi(y) = \pi^{-1}(y)}$$

($x, y \in Z_{26}$ and π^{-1} is the inverse pemutation to π)

The Substitution Cipher: Example

- Consider the following permutation

Plain	A	B	C	D	E	F	G	H	I	J	K	L	M
Cipher	W	H	O	V	I	B	P	L	C	J	Q	X	D
Plain	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher	K	R	Y	E	S	Z	A	F	T	M	G	N	U

- Plaintext: *a t t a c k a t d a w n*
- Ciphertext: *w a a w o q w a v w m k*

How to decrypt the ciphertext?

The Substitution Cipher: Example (cont.)

- Consider the following permutation

Plain	A	B	C	D	E	F	G	H	I	J	K	L	M
Cipher	W	H	O	V	I	B	P	L	C	J	Q	X	D

Plain	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher	K	R	Y	E	S	Z	A	F	T	M	G	N	U

- Plaintext: *we are studying cryptography*
- Ciphertext: ***?***

The Substitution Cipher: Review

- **$26! \sim 4*10^{28}$**

$\rightarrow$ **Large enough**

- An exhaustive key search is infeasible

Simple Cryptosystems

- Shift Cipher
- Substitution Cipher
- **Affine Cipher**
- Vigenère Cipher
- Hill Cipher

Why Affine?

- Affine functions:

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

$$a,b \in Z_{26}$$

- Suppose $e(x) = (4x + 7) \bmod 26$

  $e(3) = ?$

  $e(10) = ?$

  $e(16) = ?$

Why Affine?

- Affine functions:

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

$$a,b \in Z_{26}$$

- Suppose $e(x) = (4x + 7) \bmod 26$

  $e(3) = 19$

  $e(10) = 21$

  $e(16) = 19$

The Affine Cipher: Condition

- The affine functions have unique solution for every x iff

$$gcd(a,26) = 1$$

gcd: the greatest common divisor

- Examples:

gcd(4,26) = 2

→ $e(x)$ is not a valid encryption function

gcd(7,26) = 1

→ $e(x)$ is a valid encryption function

Congruence

- *a, b* are integer; *m* is a positive integer
  a ≡ b (mod m), called a congruence, if
  (a-b) divides *m*

- <u>In other words:</u>
  a ≡ b (mod m) iff *a mod m = b mod m*

- Example: 105 ≡ 1 (*mod* 26)
  ? ≡ 8 (*mod* 18)

Multiplicative Inverse

- Suppose $a \in Z_m$
- The multiplicative inverse of *a* module *m*:
  - denoted $a^{-1} \ mod \ m$
  - is an element $a' \in Z_m$ such that:

$$\boxed{aa' \equiv a'a \equiv 1 \ (mod \ m)}$$

if m is fixed, we sometimes write a^{-1} for $a^{-1} \ mod \ m$

- Examples: in Z_{26}

$3^{-1} = ?$

$17^{-1} = ?$

The Affine Cipher: Definition

An Affine cipher is a five-tuple

$$(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$$

where

- $\mathcal{P} = \mathcal{C} = Z_{26}$;
- $\mathcal{K} = \{(a, b) \in Z_{26} \times Z_{26} : gcd(a, 26) = 1\}$
- For each $K = (a, b) \in \mathcal{K}$:

$$\boxed{e_K(x) = (ax + b) \ mod \ 26} \quad \text{and} \quad \boxed{d_K(y) = a^{-1}(y - b) \ mod \ 26}$$

$$(x, y \in Z_{26})$$

The Affine Cipher: Example

- Suppose $K = (9, 5)$ in Z_{26}

$$e_k(x) = 9x + 5$$

Calculate the decryption rule:

$$9^{-1} = ?$$

$$\rightarrow d_k(y) = 3(y - 5) = 3y - 15$$

Now, let encrypt x = *the weather is good*

Step 1: convert to integers

19 7 4 22 4 0 19 7 4 17 8 18 6 14 14 3

The Affine Cipher: Example

- Suppose $K = (9, 5)$ in Z_{26}

$$e_k(x) = 9x + 5$$

Calculate the decryption rule:

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

$$\rightarrow d_k(y) = 3(y - 5) = 3y - 15$$

- Now, let encrypt the plaintext x = *the weather is good*

- **Step 1**: convert to integers

  19 7 4 22 4 0 19 7 4 17 8 18 6 14 14 3

The Affine Cipher: Example

- **Step 2**: encrypt integers using $e_k(x)$

  19 7 4 22 4 0 19 7 4 17 8 18 6 14 14 3

  20 16 15 21 15 5 20 16 15 2 25 11 7 1 1 6

- **Step 3**: convert to string

  u q p v p f u q p c z l h b b g

→ Ciphertext: *uqpvpfuqpczlhbbg*

- Now, let **decrypt** the ciphertext *axg* with the key $K = (7,3)$ in Z_{26}**?**

The Affine Cipher: Review

- Key space?
  - *gcd(a,26) = 1*, so *a* must be 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25
  - *b* can be any element in Z_{26}

  → **too small to be secure**

The Vigenère Cipher

The Vigenère Cipher: Definition

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

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

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

Note: all the operations must be reduced to modulo 26

The Vigenère Cipher: Example

- Suppose $m = 6$ and the keyword is *cipher*. So, the key $K = (2, 8, 15, 7, 4, 17)$
- The plaintext is x = *itisveryhottoday*
- How to encrypt it using the Vigenère Cipher?

- **Step 1**: convert the plaintext to integers

8 19 8 18 21 4 17 24 7 14 19 19 14 3 0 24

The Vigenère Cipher: Example

- **Step 2**: add the keyword then modulo 26

8 19 8 18 21 4 17 24 7 14 19 19 14 3 0 24

2 8 15 7 4 17 2 8 15 7 4 17 2 8 15 7

10 1 23 25 25 21 19 6 22 21 23 10 16 11 15 5

- Step 3: convert integers to string

k b x z z v t g w v x k q l p f

→ Ciphertext: *kbxzzvtgwvxkqlpf*

The Vigenère Cipher: Example

- Suppose $m = 6$ and the keyword is *cipher*. So, the key $K = (2, 8, 15, 7, 4, 17)$
- The ciphertext is y =

  vpxzgiaxivwpubttmjpwizitwzt

- Let decrypt it using the Vigenère Cipher?

- The plaintext is x =

  thiscryptosystemisnotsecure

The Vigenère Cipher: Review

- Key space?
  - ***26^m*** where *m* is the length of the keyword
  - Exhaustive key search by hand is infeasible

- An alphabetic character can be mapped to one of *m* possible alphabetic characters

→ **polyalphabetic cryptosystem**

The Hill Cipher

Basic Linear Algebra

- **Matrix** *A*: *l* * *m*

$$\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}$$

- **Matrix product**: $AB = (c_{i,k})$
  - $A = (a_{i,j})$ is an $l*m$ matrix and $B = (a_{j,k})$ is an $m*n$ matrix
  - $l*n$ matrix

$$c_{i,k} = \sum_{j=1}^{m} a_{i,j} b_{j,k}$$

  - $(AB)C = A(BC)$ but not $AB = BA$

- **Identity matrix** I_m: $m*m$ matrix with 1's on the main diagonal and 0's elsewhere

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

Basic Linear Algebra

- **Inverse matrix** of A: $m * m$
  - A^{-1} such that $AA^{-1} = A^{-1}A = I_m$
  - Not all matrices have inverse but if it is exists, it is unique

  → <u>when a matrix has inverse?</u>

- **Determinant (*det*)** of $A = (a_{i,j})$, an $m*m$ matrix
  - Define $A_{i,j}$ to be the matrix obtained from A by deleting the row *i*th and the column *j*th
  - $m = 1$: **det** $A = a_{1,1}$
  - $m > 1$: choose i is any fixed integer between 1 to m

$$\det A = \sum_{j=1}^{m} (-1)^{i+j} a_{i,j} \det A_{ij}$$

Basic Linear Algebra

- $A = (a_{i,j})$: 2*2 matrix
  - **det** $A = a_{1,1}a_{2,2} - a_{1,2}a_{2,1}$
- $A = (a_{i,j})$: 3*3 matrix
  - **det** $A = a_{1,1}a_{2,2}a_{3,3} + a_{1,2}a_{2,3}a_{3,1} + a_{1,3}a_{2,1}a_{3,2} - (a_{1,1}a_{2,3}a_{3,2} + a_{1,2}a_{2,1}a_{3,3} + a_{1,3}a_{2,2}a_{3,1})$
- A simple case: suppose $A = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}$ and A has inverse then

$$A^{-1} = (\det A)^{-1} \begin{pmatrix} a_{2,2} & -a_{1,2} \\ -a_{2,1} & a_{1,1} \end{pmatrix}$$

Important Condition

- When a matrix has inverse?
  - *A matrix A has inverse iff its **det** is non-zero*
  - *A matrix A has **inverse modulo 26** iff*

    *gcd(**det** A, 26) = 1*

The Hill Cipher: Definition

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 $\mathbb{Z}_{26}$.

Note: ***all operation must be reduced to modulo 26***

The Hill Cipher: Example

- Suppose the key $K = \begin{pmatrix} 13 & 9 \\ 6 & 8 \end{pmatrix}$

- The plaintext is x = *good*
- How to encrypt it using the Hill Cipher?

- **Encrypt is ok but not for decryption!!!**

The Hill Cipher: Example

- Suppose the key $K = \begin{pmatrix} 11 & 8 \\ 12 & 9 \end{pmatrix}$
- The plaintext is x = *good*
- How to encrypt it using the Hill Cipher?
- Encrypt and decrypt are ok!

- **Step 1**: convert to integers

g	o	o	d
6	14	14	3

The Hill Cipher: Example

- **Step 2**: Encrypt each block of two integers

g o
6 14

$$\begin{pmatrix} 6 & 14 \end{pmatrix} \begin{pmatrix} 11 & 8 \\ 12 & 9 \end{pmatrix} = \begin{pmatrix} 66+168, & 48+126 \end{pmatrix} = \begin{pmatrix} 0,18 \end{pmatrix}$$

o d
14 3

$$\begin{pmatrix} 14 & 3 \end{pmatrix} \begin{pmatrix} 11 & 8 \\ 12 & 9 \end{pmatrix} = \begin{pmatrix} 154+36, & 112+27 \end{pmatrix} = \begin{pmatrix} 8,9 \end{pmatrix}$$

- **Step 3**: convert each two-integer block to characters
  - The ciphertext is y = *asij*

The Hill Cipher: Example

How to decrypt?

- Compute K^{-1}
  - $det\ K = (11*9 - 12*8) \bmod 26 = 3$
  - *Using*

$$A^{-1} = (\det A)^{-1}\begin{pmatrix} a_{2,2} & -a_{1,2} \\ -a_{2,1} & a_{1,1} \end{pmatrix}$$

$$K^{-1} = (3)^{-1}\begin{pmatrix} 9 & -8 \\ -12 & 11 \end{pmatrix} = (9)\begin{pmatrix} 9 & -8 \\ -12 & 11 \end{pmatrix} = \begin{pmatrix} 3 & 6 \\ 22 & 21 \end{pmatrix}$$

The Hill Cipher: Example

How to decrypt?

- Decrypt each two-integer block of the ciphertext $y =$ *asij*

a s
0 18

$$\begin{pmatrix} 0 & 18 \end{pmatrix} \begin{pmatrix} 3 & 6 \\ 22 & 21 \end{pmatrix} = \begin{pmatrix} 0+396, \ 0+378 \end{pmatrix} = \begin{pmatrix} 6, 14 \end{pmatrix}$$

i j
8 9

$$\begin{pmatrix} 8 & 9 \end{pmatrix} \begin{pmatrix} 3 & 6 \\ 22 & 21 \end{pmatrix} = \begin{pmatrix} 24+198, \ 48+189 \end{pmatrix} = \begin{pmatrix} 14, 3 \end{pmatrix}$$

- Plaintext x = *good*

The Hill Cipher: Example (cont.)

- Suppose the key $K = \begin{pmatrix} 11 & 8 \\ 12 & 9 \end{pmatrix}$
- The plaintext is x = *hello*
- Let encrypt it using the Hill Cipher???

- Suppose the key $K = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$
- The ciphertext is y = *delw*
- Let decrypt it using the Hill Cipher???

The Hill Cipher: Review

- Key space?
- There are 26^{n^2} matrices of dimension *n x n*
- $\log_2\left(26^{n^2}\right)$ is the upper bound on the key size

What else?

- The permutation cipher and
- The stream ciphers

Cryptanalysis

General Assumption

- **Kerckhoffs' Principle:** The opponent, namely Oscar, knows the cryptosystem being used
- If not, his attack is more difficult

- **Attack model**: specifies the information available to the adversary when he mounts his attack

Attack Models

- **Ciphertext only attack**:
  - Oscar possesses a string of ciphertext y
- **Known plaintext attack:**
  - Oscar possesses a string of plaintext x and the corresponding ciphertext y
- **Chosen plaintext attack:**
  - Oscar can temporarily use the encryption rule
- **Chosen ciphertext attack:**
  - Oscar can temporarily use the decryption rule

→ **Objective:** Determine the key

Example

- The Shift cipher

Ciphertext:

jbcrclqrwcrvnbjenbwrwn

- Key 0: *jbcrclqrwcrvnbjenbwrwn*
- Key 1: *iabqbkpqvbqumaidmavqvm*
- …
- Key 9: astitchintimesavesnine

→ plaintext: *a stitch in time saves nine*

Presentations

- Cryptanalysis of the Substitution Cipher
- Cryptanalysis of the Hill Cipher
- Cryptanalysis of the Vigenère Cipher

Takeaways

- What is cryptography
- Cryptosystems
- Cryptanalysis
- Some presentations