CHƯƠNG 3:

CÁC HỆ MÃ BÍ MẬT

Chương 3:
Các hệ mã bí mật

3.1. Một số hệ mã cổ điển

Hệ mật mã có khóa đối xứng, tức là những hệ mật mã mà khóa lập mật mã và khóa giải mật mã là trùng nhau.

Thực tế thì hai khóa (mã hóa, giải mã) có thể khác nhau, trong trường hợp này thì một khóa nhận được từ khóa kia bằng phép tính toán đơn giản.

→ vì vậy khóa mật mã chung đó phải được **giữ bí mật**

Chương 3:
Các hệ mã bí mật

Để mã hóa văn bản đơn giản sử dụng bảng 26 chữ cái, {A, B, C, …, X, Y, Z}, ta sẽ dùng các con số {0, 1, 2,…, 24, 25} đại diện cho 26 chữ cái này và dùng các phép toán số học theo modulo 26 để diễn tả các phép biến đổi trên bảng chữ cái.

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

Chương 3:
Các hệ mã bí mật

3.1.1 Mã dịch chuyển (Shift Cipher)
Mã Ceasar

Chương 3:
Các hệ mã bí mật

3.1.1. Mã dịch chuyển (Shift Cipher) – mã Ceasar

Giả sử bảng chữ cái tiếng Anh có thể xem là một vành Z_{26} ta có mã dịch chuyển định nghĩa như sau:

- **Định nghĩa:** Mã dịch chuyển: $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$

$$\mathcal{P} = \mathcal{C} = \mathcal{K} = Z_{26}$$

với $\mathrm{k} \in \mathcal{K}$, định nghĩa

$$e_k(x) = (\mathrm{x} + \mathrm{k}) \bmod 26$$

$$d_k(y) = (\mathrm{y} - \mathrm{k}) \bmod 26$$

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

Chương 3:
Các hệ mã bí mật

<u>Ví dụ</u>: Dùng khóa k=9 để mã hóa dòng thư:

"hentoithubay"

Dòng thư đó tương ứng với dòng số

h	e	n	t	o	i	t	h	u	b	a	y
7	4	13	19	14	8	19	7	20	1	0	24

Qua phép mã hóa e_9 sẽ được:

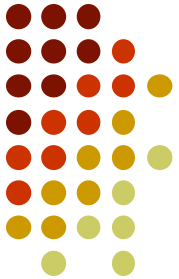
16	13	22	2	23	17	2	16	3	10	9	7
q	**n**	**w**	**c**	**x**	**r**	**c**	**q**	**d**	**k**	**j**	**h**

Như vậy bản mã sẽ là: "**qnwcxrcqdkjh**"

Dùng d_9 giải mã ta sẽ được bản rõ ban đầu

Cách đây *2000* năm mã dịch chuyển đã được Julius Ceasar sử dụng, với khóa k=3 mã dịch chuyển được gọi là mã Ceasar.

Chương 3:
Các hệ mã bí mật



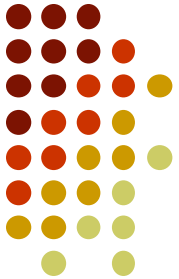
Bài tập: Tìm bản rõ của “RKKRTB” với K = 17

Gợi ý thứ tự các ký tự:

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

Chương 3:
Các hệ mã bí mật



Tính an toàn

- ✓ Mã hóa một thông điệp được biểu diễn bằng các chữ cái từ A đến Z (26 chữ cái), ta sử dụng Z_{26}.
- ✓ Thông điệp được mã hóa sẽ không an toàn và có thể dễ dàng bị giải mã bằng cách thử lần lượt 26 giá trị khóa *k*.
- ✓ Tính trung bình, thông điệp đã được mã hóa có thể bị giải mã sau khoảng 26/2 = 13 lần thử khóa.

Chương 3:
Các hệ mã bí mật

3.1.2 Mã thay thế (Subtitution Cipher)

Chương 3:
Các hệ mã bí mật

3.1.2. Mã thay thế (Subtitution Cipher)

Khóa của mã thay thế là một hoán vị của bảng chữ cái. Gọi S(E) là tập hợp tất cả các phép hoán vị các phần tử của E.

- **Định nghĩa:** Mã thay thế: $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$

  $\mathcal{P} = \mathcal{C} = Z_{26}, \mathcal{K} = \mathrm{S}(Z_{26})$

  với mỗi $\Pi \in \mathcal{K}$, tức là một hoán vị trên Z_{26}, ta xác định

  $$e_{\Pi}(x) = \Pi(\mathrm{x})$$

  $$d_{\Pi}(y) = \Pi^{-1}(\mathrm{x})$$

  với $\mathrm{x}, \mathrm{y} \in Z_{26}$, Π^{-1} là nghịch đảo của Π

Chương 3:
Các hệ mã bí mật

Ví dụ: Π được cho bởi (ở đây ta viết các chữ cái thay cho các con số thuộc Z_{26})

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
x	n	y	a	h	p	o	g	z	q	w	b	t	s	f	l	r	c	v	m	u	e	k	j	d	i

Bản rõ:

"hentoithubay"

Sẽ được mã hóa thành bản mã (với khóa Π):

"ghsmfzmgunxd"

Dễ xác định được Π^{-1}, và do đó từ bản mã ta tìm được bản rõ

Chương 3:
Các hệ mã bí mật

Ví dụ: Π được cho bởi (ở đây ta viết các chữ cái thay cho các con số thuộc Z_{26}

Π

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
x	n	y	a	h	p	o	g	z	q	w	b	t	s	f	l	r	c	v	m	u	e	k	j	d	i

Π^{-1}

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
d	l	r	y	v	o	h	e	z	x	w	p	t	b	g	f	j	q	n	m	u	s	k	a	c	i

Bản mã: **“oghsefzyfeza”**

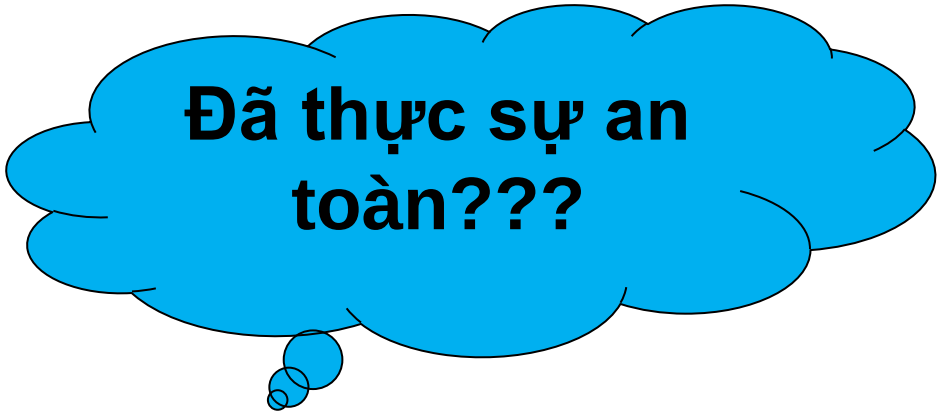
Sẽ được giải mã thành bản rõ (với khóa Π):

“ghenvoicovid”

Chương 3:
Các hệ mã bí mật

Tính an toàn

- ✓ Đơn giản, thao tác mã hóa và giải mã được thực hiện nhanh chóng.
- ✓ Không gian khóa $\mathcal{K}$ gồm *N!* phần tử
- ✓ Khắc phục hạn chế của phương pháp Shift Cipher: việc tấn công vét cạn tất cả các khóa $k \in \mathcal{K}$ là không khả thi.



Chương 3:
Các hệ mã bí mật

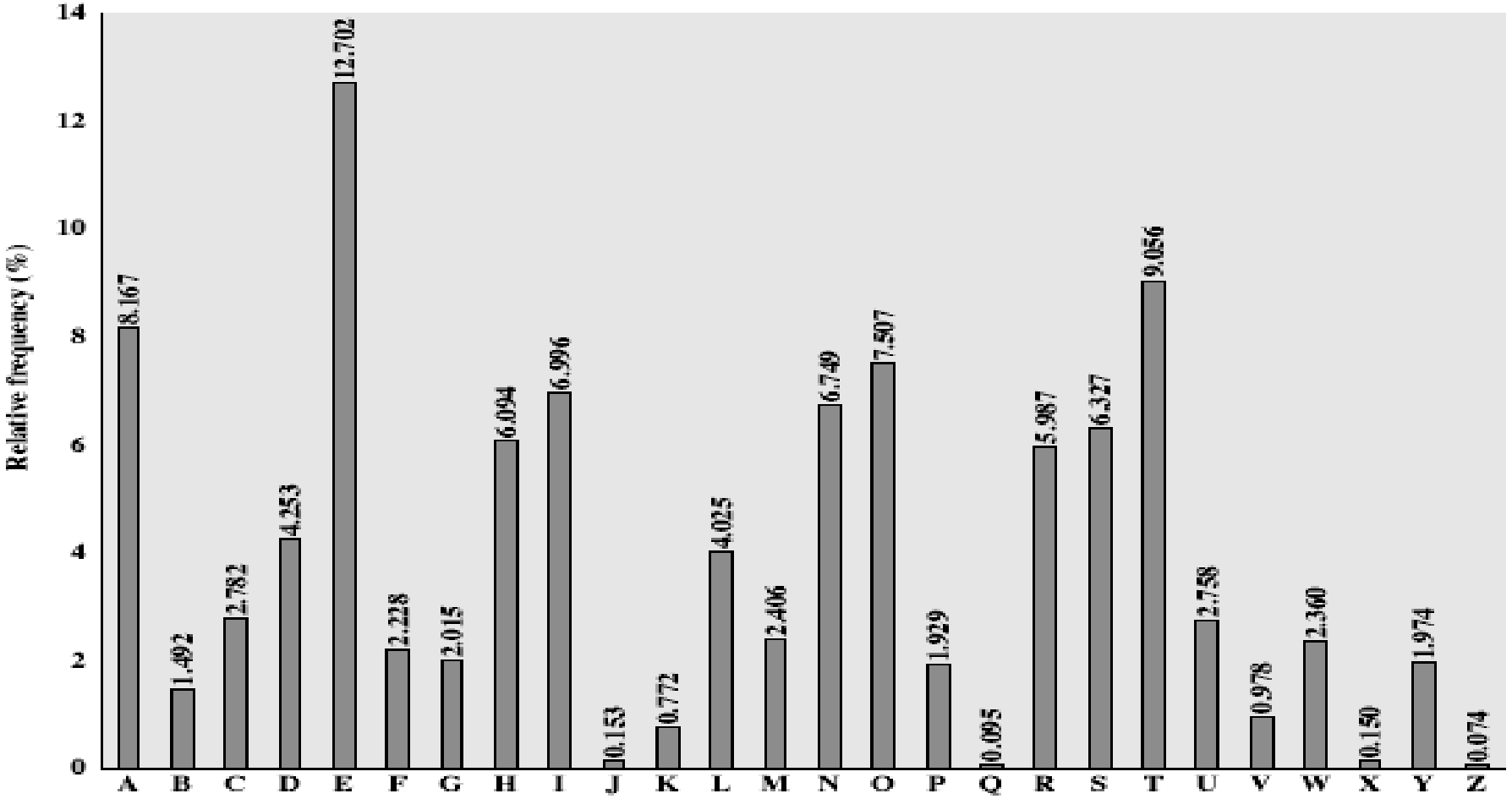
Độ an toàn của mã thay thế

- Một khóa là một hoán vị của 26 chữ cái.
- Có 26! (~4.10^26) hoán vị (khóa).
- Phá mã :
  - Không thể duyệt từng khóa một.
  - Cách khác?

Chương 3:
Các hệ mã bí mật

- Điều quan trọng là mã thế trên bảng chữ đơn không làm thay đổi tần suất tương đối của các chữ, có nghĩa là ta vẫn có bảng tần suất trên nhưng đối với bảng chữ mã tương ứng. Điều đó được phát hiện bởi các nhà khoa học Ai cập từ thế kỷ thứ 9. Do đó có cách thám mã trên bảng chữ đơn như sau:
  - Tính toán tần suất của các chữ trong bản mã
  - So sánh với các giá trị đã biết
  - Tìm kiếm các chữ đơn hay dùng A-I-E, bộ đôi NO và bộ ba RST; và các bộ ít dùng JK, X-Z..
  - Trên bảng chữ đơn cần xác định các chữ dùng các bảng bộ đôi và bộ ba trợ giúp.

Chương 3:
Các hệ mã bí mật



Bảng thống kê tần suất ký tự tiếng Anh

Chương 3:
Các hệ mã bí mật

Phân tích của Beker và Peper

- E: có xác suất khoảng 1,120
- T, A, O, I, N, S, H, R : mỗi ký tự có xac suất khoảng 0,06 đến 0,09
- D, L : mỗi ký tự có xác suất chừng 0,04
- C, U, M, W, F, G, Y, P, B: mỗi ký tự có xác suất khoảng 0,015 đến 0,023
- V, K, J, X, Q, Z mỗi ký tự có xác suất nhỏ hơn 0,01

Chương 3:
Các hệ mã bí mật

Phân tích của Beker và Peper

- 30 bộ đôi thông dụng nhất (theo hứ tự giảm dần) là: TH, HE, IN, ER, AN, RE, ED, ON, ES, ST, EN, AT, TO, NT, HA, ND, OU, EA, NG, AS, OR, TI, IS, ET, IT, AR, TE, SE, HI và OF
- 12 bộ ba thông dụng nhất (theo thứ tự giảm dần) là: THE, ING, AND, HER, ERE, ENT, THA, NTH, WAS, ETH, FOR và DTH.

Chương 3:
Các hệ mã bí mật

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBME
TSXAIZVUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXU
ZUHSXEPYEPOPDZSZUFPOUDTMOHMQ

- Tính tần suất các chữ
- Đoán P và Z là e và t.
- Khi đó ZW là th và ZWP là the.
- Suy luận tiếp tục ta có bản rõ:

“it was disclosed yesterday that several informal but direct contacts have been made with politicalrepresentatives in moscow”

Chương 3:
Các hệ mã bí mật

3.1.3 Mã thay thế Playfair

Chương 3:
Các hệ mã bí mật

3.1.3. Mã Playfair

Một trong các hướng khắc phục của phương pháp mã bằng bảng mã đơn là mã bộ các chữ, tức là mỗi chữ sẽ được mã bằng một số chữ khác nhau tùy thuộc vào các chữ mà nó đứng cạnh. Playfair là một trong các mã như vậy, được sáng tạo bởi Charles Wheastone vào năm 1854 và mang tên người bạn là Baron Playfair. Ở đây mỗi chữ có thể được mã bằng một trong 7 chữ khác nhau tùy vào chữ cặp đôi cùng nó trong bản rõ.

Chương 3:
Các hệ mã bí mật

3.1.3. Mã Playfair

Phương pháp là lập ma trận *5x5* dựa trên từ khóa cho trước và các ký tự trên bảng chữ cái

- Trước hết viết các chữ của từ khoá vào các hàng của ma trận bắt đầu từ hàng thứ nhất.
- Nếu ma trận còn trống, viết các chữ khác trên bảng chữ cái chưa được sử dụng vào các ô còn lại. Có thể viết theo một trình tự qui ước trước, chẳng hạn từ đầu bảng chữ cái cho đến cuối.

Chương 3:
Các hệ mã bí mật

3.1.3. Mã Playfair

- Vì có 26 chữ cái tiếng Anh, nên thiếu một ô. Thông thường ta dồn hai chữ nào đó vào một ô chung, chẳng hạn I và J.
- Giả sử sử dụng từ khoá MORNACHY. Lập ma trận khoá Playfair tương ứng như sau:

MONAR
CHYBD
EFGIK
LPQST
UVWXZ

Chương 3:
Các hệ mã bí mật

3.1.3. Mã Playfair

- Chia bản rõ thành từng cặp chữ. Nếu một cặp nào đó có hai chữ như nhau, thì ta chèn thêm một chữ lọc chẳng hạn X. Ví dụ, trước khi mã "balloon" biến đổi thành "ba lx lo on".

- Nếu cả hai chữ trong cặp đều rơi vào cùng một hàng, thì mã mỗi chữ bằng chữ ở phía bên phải nó trong cùng hàng của ma trận khóa (cuộn vòng quanh từ cuối về đầu), chẳng hạn "ar" biến đổi thành "RM"

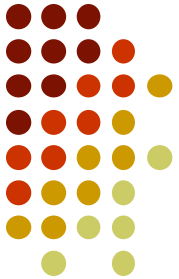
Chương 3:
Các hệ mã bí mật

3.1.3. Mã Playfair

- Nếu cả hai chữ trong cặp đều rơi vào cùng một cột, thì mã mỗi chữ bằng chữ ở phía bên dưới nó trong cùng cột của ma trận khóa (cuộn vòng quanh từ cuối về đầu), chẳng hạn "mu" biến đổi thành "CM"

- Trong các trường hợp khác, mỗi chữ trong cặp được mã bởi chữ cùng hàng với nó và cùng cột với chữ cùng cặp với nó trong ma trận khóa. Chẳng hạn, "hs" mã thành "BP", và "ea" mã thành "IM" hoặc "JM" (tuỳ theo sở thích)

Chương 3:
Các hệ mã bí mật



3.1.3. Mã Playfair

Hãy tìm hiểu quá trình mã hóa và giải mã bằng phương pháp mã Playfair

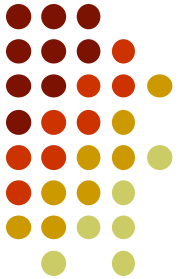
Bản rõ P = “**DAI HOC SAI GON**”

Khóa K = “**tinhoc**”

Chương 3:
Các hệ mã bí mật

3.1.4 Mã Apphin (Apphin Cipher)

Chương 3:
Các hệ mã bí mật



3.1.4. Mã Apphin (Apphin Cipher)

Phép lập mã được cho bởi một hàm Apphin dạng:

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

Trong đó a, b ∈ Z_{26} (chú ý: nếu a=1 ta có mã dịch chuyển).

Khi **gcd(a, 26)=1** thì có số $a^{-1} \in Z_{26}$ sao cho: $a.a^{-1} = a^{-1}.a = 1 \bmod 26$, và do đó hàm giải mã

$$d(x) = a^{-1}. (y-b) \bmod 26$$

Chương 3:
Các hệ mã bí mật

3.1.4. Mã Apphin (Apphin Cipher)

- **Định nghĩa:** Mã Apphin($\mathcal{P}$, $\mathcal{C}$, $\mathcal{K}$, $\mathcal{E}$, $\mathcal{D}$)

$\mathcal{P} = \mathcal{C} = Z_{26}$, $\mathcal{K}$ = {(a, b) ∈ Z_{26} x Z_{26}): (a, 26)=1}

với mỗi k=(a, b) ∈ $\mathcal{K}$, ta định nghĩa

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

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

trong đó x, y ∈ Z_{26}

Chương 3:
Các hệ mã bí mật

- Ví dụ: **k=(5, 6)**

  Bản rõ:

  “hentoithubay”

	h	e	n	t	o	i	t	h	u	b	a	y
x	7	4	13	19	14	8	19	7	20	1	0	24

y = 5x + 6 mod 26

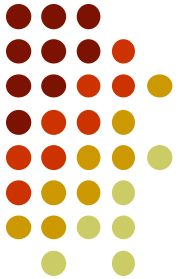
y	15	0	19	23	24	20	23	15	2	11	6	22
	p	a	t	x	y	u	x	p	c	l	g	w

Bản mã: “patxyuxpclgw”

Thuật toán giải mã trong trường hợp này có dạng:

$$d_k(y) = 21(y-6) \bmod 26$$

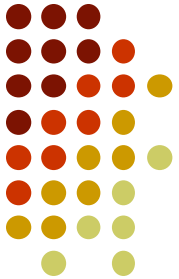
Chương 3:
Các hệ mã bí mật



- **Bài tập**
  - a = 5, b = 3: y = 5x + 3 (mod 26)
  - Mã hóa: **ANTOAN → ?**

DQUVDQ

Chương 3:
Các hệ mã bí mật



Độ an toàn của hệ mã Affine

Gọi $\phi(n)$ là số lượng phần tử thuộc Z_n và nguyên tố cùng nhau với n

Nếu n =$\prod_{i=1}^{m} p_i^{e_i}$ với p_i là các số nguyên tố khác nhau và

$e_i \in \boldsymbol{Z}^+$, 1 ≤ i ≤ m thì $\phi(n) = \prod_{i=1}^{m}(p_i^{e_i} - p_i^{e_i-1})$

- *n* khả năng chọn giá trị *b*
- $\phi(n)$ khả năng chọn giá trị *a*
- $n \times \phi(n)$ khả năng chọn lựa khóa *k* = *(a, b)*

Chương 3:
Các hệ mã bí mật

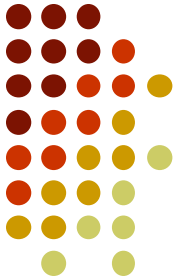
3.1.5 Mã hóa Vigenere

Chương 3:
Các hệ mã bí mật

3.1.5. Mã hóa Vigenere

- Trong phương pháp mã hóa bằng thay thế: với một khóa *k* được chọn, mỗi phần tử x ∈ $\mathcal{P}$ được ánh xạ vào duy nhất một phần tử y ∈ $\mathcal{C}$.
- Phương pháp Vigenere sử dụng khóa có độ dài *m.*
- Được đặt tên theo nhà khoa học Blaise de Vigenere (thế kỷ 16).
- Có thể xem phương pháp mã hóa Vigenere bao gồm *m* phép mã hóa bằng dịch chuyển được áp dụng luân phiên nhau theo chu kỳ.
- Không gian khóa K của phương pháp Vigenere có số phần tử là n^m
- Ví dụ: *n*=26, *m*=5 thì không gian khóa ~1.1 x 10^7

Chương 3:
Các hệ mã bí mật



- **Định nghĩa:** Mã Vigenere($\mathcal{P}$, $\mathcal{C}$, $\mathcal{K}$, $\mathcal{E}$, $\mathcal{D}$)

  Cho m là số nguyên dương

  $\mathcal{P} = \mathcal{C} = \mathcal{K} = Z_{26}$

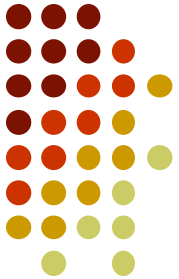
  với mỗi k=$(k_1, k_2, \ldots, k_m) \in \mathcal{K}$ có

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

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

Các phép cộng trừ đều lấy theo Modulo 26

Chương 3:
Các hệ mã bí mật



- **Ví dụ:**
- m = 6 và keyword là CIPHER
- Suy ra, khóa k = (2, 8, 15, 7, 4, 17)
- Cho bản rõ: **thiscryptosystemisnotsecure**

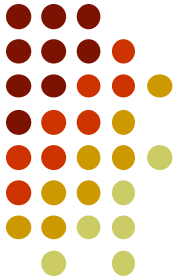
  thiscr yptosy stemis notsec ure

  Vậy bản mã là: “vpxzgiaxivwoubttmjpwizitwzt”

Chương 3:
Các hệ mã bí mật

3.1.6 Mã hóa Hill

Chương 3:
Các hệ mã bí mật



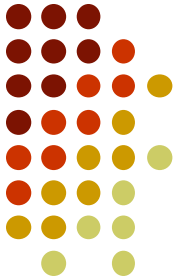
3.1.6. Mã hóa Hill

- Phương pháp Hill (1929)
- Tác giả: Lester S.Hill
- Ý tưởng chính: Sử dụng *m* tổ hợp tuyến tính của *m* ký tự trong plaintext để tạo ra *m* ký tự trong cyphertext
- Ví dụ:

$$y_1 = 11x_1 + 3x_2$$
$$y_2 = 8x_1 + 7x_2$$

$$(y1, y2) = (x1, x2) = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$$

Chương 3:
Các hệ mã bí mật



3.1.6. Mã hóa Hill

Chọn số nguyên dương *m.* Định nghĩa:

P = *C* = $(Z_n)^m$ và *K* là tập hợp các ma trận *mxm* khả nghịch

Với mỗi khóa *k* = $\begin{bmatrix} k_{1,1} & k_{1,2} & \dots & k_{1,m} \\ k_{2,1} & k_{2,2} & \dots & k_{2,m} \\ \vdots & \vdots & \vdots & \vdots \\ k_{m,1} & k_{m,2} & \dots & k_{m,m} \end{bmatrix}$ ∈ *K*, định nghĩa:

$e_k(x) = xk = (x_1, x_2, \dots, x_m)\begin{bmatrix} k_{1,1} & k_{1,2} & \dots & k_{1,m} \\ k_{2,1} & k_{2,2} & \dots & k_{2,m} \\ \vdots & \vdots & \vdots & \vdots \\ k_{m,1} & k_{m,2} & \dots & k_{m,m} \end{bmatrix}$ với x = $(x_1, x_2, \dots, x_m) \in P$

Và $d_k(y) = yk^{-1}$ với $y \in C$

Mọi phép toán số học đều được thực hiện trên Z_n

Chương 3:
Các hệ mã bí mật

3.1.6. Mã hóa Hill

Ví dụ: cho hệ mã Hill có M=2 (khóa là các ma trận vuông cấp 2) và bảng chữ cái là bảng chữ cái tiếng Anh, tức là N = 26.

Cho khóa: K = $\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$

Hãy mã hóa xâu P = “HELP” và giải mã ngược lại bản mã thu được.

Chương 3:
Các hệ mã bí mật

3.1.6. Mã hóa Hill

Để mã hóa chúng ta chia xâu bản rõ thành 2 vecto hàng 2 chiều "HE" (7 4) và "LP" (11 15) và tiến hành mã hóa lần lượt

- Với P_1=(7 4) ta có C_1= P_1*K = (7 4)$\begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$ = (3 15) = (D P)
- Với P_2=(11 15) ta có C_2= P_2*K = (11 15)$\begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$ = (11 4) = (L E)

Vậy bản mã thu được là C = "DPLE"

Chương 3:
Các hệ mã bí mật

3.1.6. Mã hóa Hill

Để giải mã ta tính khóa giải mã là ma trận nghịch đảo của ma trận khóa trên Z_{26} theo công thức sau:

Với K = $\begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix}$ và det(K) = $(k_{11} * k_{22} - k_{21} * k_{12})$ *mod N* là một phần tử có phần tử nghịch đảo trên Z_N (ký hiệu là $\det(K)^{-1}$) thì khóa giải mã sẽ là:

$$\boldsymbol{K^{-1} = det(K)^{-1} * \begin{bmatrix} k_{22} & -k_{12} \\ -k_{21} & k_{11} \end{bmatrix}}$$

Áp dụng vào trường hợp trên ta có det(K) = (15 - 6) mod 26 = 9.

GCD(9, 26) = 1 nên áp dụng thuật toán Euclid mở rộng tìm được $\det(K)^{-1}$ = 3. Vậy K^{-1} = 3 * $\begin{bmatrix} 5 & 23 \\ 24 & 3 \end{bmatrix}$ = $\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}$

Chương 3:
Các hệ mã bí mật

3.1.6. Mã hóa Hill

Giải mã C = “DP” = (3 15), P = C*K^{-1} = (3 15) * $\begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix}$ = (7 4) = “HE”

Tương tự giải mã xâu C=“LE” kết quả sẽ được bản rõ P=“LP”

Chú ý là trong ví dụ trên chúng ta sử dụng khóa K có kích thước nhỏ nên dễ dàng tìm được khóa để giải mã còn trong trường hợp tổng quát điều này là không dễ dàng.

Chương 3:
Các hệ mã bí mật

Giải thích cách tìm khóa

Giả sử: k = $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ta có ma trận nghịch đảo k^{-1}=$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}$

được tính:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix}$$

Chương 3:
Các hệ mã bí mật

Giải thích cách tìm khóa

Một chú ý là để phép chia luôn thực hiện được trên tập Z_{26} thì nhất thiết định thức của *k*: det(*k*) = (ad – bc) phải có phần tử nghịch đảo trên Z_{26}.

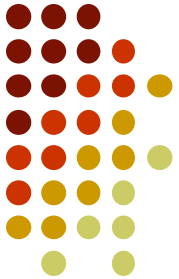
Nghĩa là (ad - bc) phải là một trong các giá trị: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23 hoặc 25. Đây cũng là điều kiện để ma trận *k* tồn tại ma trận nghịch đảo.

Chương 3:
Các hệ mã bí mật

- Khi đó: $k^{-1}.\ k = I$ là ma trận đơn vị (đường chéo chính bằng 1)

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Chương 3:
Các hệ mã bí mật



- Định thức của $\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$ là 11.7 – 8.3 = 1 ≡ 1 mod 26
- Khi đó $\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}^{-1} = \begin{pmatrix} 7 & -8 \\ -3 & 11 \end{pmatrix} \equiv \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$ mod 26

Chương 3:
Các hệ mã bí mật

- Vận dụng cho k = $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$
- Tìm K^{-1}

$$\begin{pmatrix} 5 & 12 \\ 15 & 25 \end{pmatrix}$$