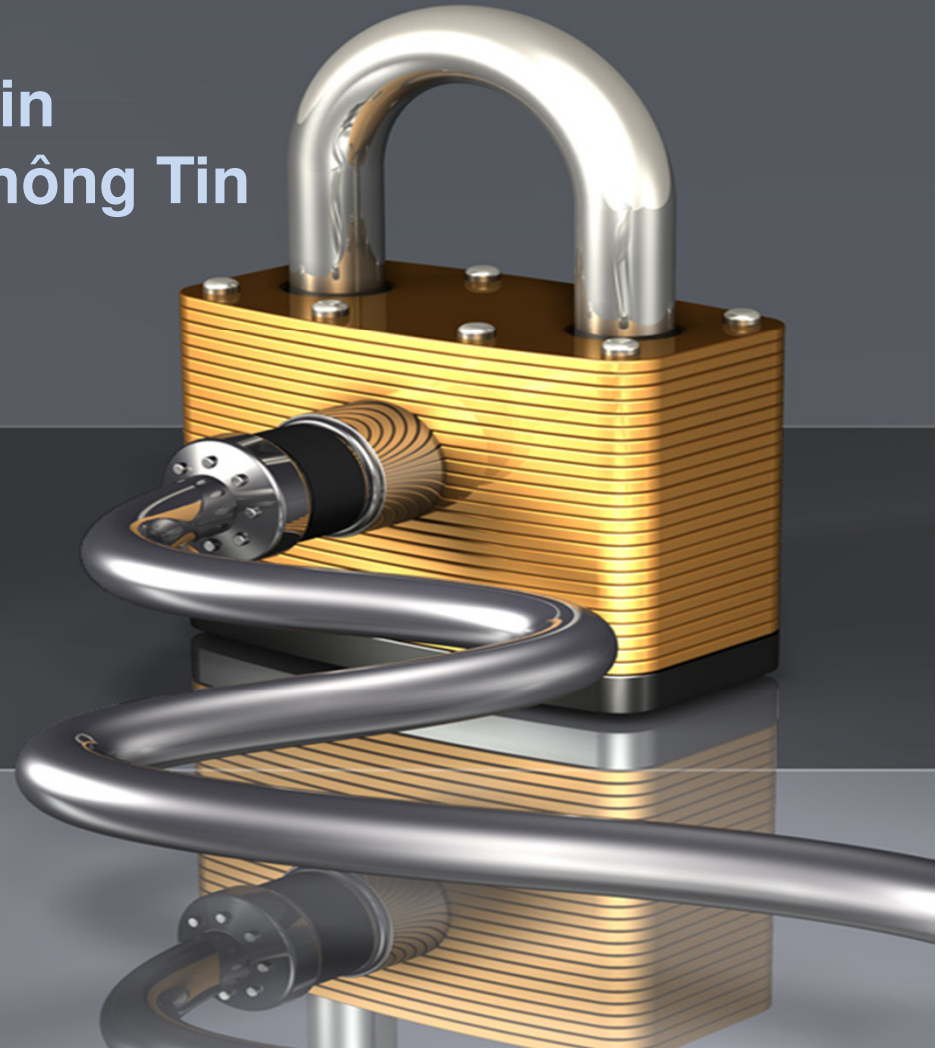


**Khoa An Toàn Thông Tin**  
**Bộ Môn: Khoa Học An Toàn Thông Tin**

**Hệ mật khoá bí mật**  
**- Các hệ mật cổ điển**



# Nội dung

1

**Giới  
thiệu  
về hệ  
mật  
khóa  
bí mật**

2

**Các  
hệ mật  
thay  
thế  
đơn  
biểu**

3

**Các  
hệ mật  
thay  
thế đa  
biểu**

4

**Các  
hệ mật  
thay  
thế  
không  
tuần  
hoàn**

5

**Các hệ  
mật  
chuyển  
vị**

6

**Chuẩn  
mã dữ  
liệu  
DES**

7

**Chuẩn  
mã dữ  
liệu  
tiền  
tiến  
AES**

# Nội dung

1

**Giới  
thiệu  
về hệ  
mật  
khóa  
bí mật**

2

**Các  
hệ mật  
thay  
thế  
đơn  
biểu**

3

**Các  
hệ mật  
thay  
thế đa  
biểu**

4

**Các  
hệ mật  
thay  
thế  
không  
tuần  
hoàn**

5

**Các hệ  
mật  
chuyển  
vị**

6

**Chuẩn  
mã dữ  
liệu  
DES**

7

**Chuẩn  
mã dữ  
liệu  
tiền  
tiến  
AES**

# Các hệ mật thay thế đơn biểu

## 1. Mã dịch vòng (Shift Cipher):

$P = C = K = \mathbb{Z}_{26}$  với  $0 \leq k \leq 25$ , ta định nghĩa:

$$y = e_k(x) = x + k \bmod 26$$

$$x = d_k(y) = y - k \bmod 26$$

- Ví dụ:

- Bản rõ: HOC TAP TOT LAO DONG TOT
- Khoá  $k = 5$



- Tìm bản mã
- Từ bản mã thu được giải mã để thu bản rõ ban đầu.

# Các hệ mật thay thế đơn biểu

Ký tự	A	B	C	D	E	F	G	H	I	J	K	L	M
Mã tương ứng	0	1	2	3	4	5	6	7	8	9	10	11	12
Ký tự	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Mã tương ứng	13	14	15	16	17	18	19	20	21	22	23	24	25

Bản rõ	H	O	C	T	A	P	T	O	T	L	A	O	D	O	N	G	T	O	T
Mã tương ứng (x)	7	14	2	19	0	15	19	14	19	11	0	14	3	14	13	6	19	14	19
$(x + 5) \bmod 26$	12	19	7	24	5	20	24	19	24	16	5	19	8	19	18	11	24	19	24
Bản mã	M	T	H	Y	F	U	Y	T	Y	Q	F	T	I	T	S	L	Y	T	Y

Bản mã thu được: **MTHYFUITYQFTITSLYTY**

Giải mã: SV tự làm!

# Các hệ mật thay thế đơn biểu

- **Nhận xét:**

- Số lượng khoá?

- Tổng cộng có **26 khóa**.

- ⇒ dễ dàng tấn công bằng phương pháp vét cạn!

# Các hệ mật thay thế đơn biểu

## 2. Mã thay thế (Substitution Cipher):

$P = C = Z_{26}$ ,  $K$  là tập tất cả các hoán vị trên  $Z_{26}$ , với mỗi phép hoán vị  $\pi \in K$ , ta định nghĩa:

$$y = e_{\pi}(x) = \pi(x)$$

và

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

trong đó  $\pi^{-1}$  là hoán vị ngược của  $\pi$

# Các hệ mật thay thế đơn biểu

- Ví dụ: mã hoá bản rõ **gap nhau chieu thu bay**

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

Plaintext	g	a	p	n	h	a	u	c	h	i	e	u	t	h	u	b	a	y
Ciphertext	B	D	T	X	J	D	O	V	J	W	F	O	U	J	O	K	D	Z

- Bản mã thu được là: **BDTXJDOVJWFOUJOKDZ**



# Các hệ mật thay thế đơn biểu

## 3. Mã Affin (Affine Cipher):

Cho  $P = C = Z_{26}$ .  $K = \{(a, b) \in Z_{26} \times Z_{26} \mid \text{UCLN}(a, 26) = 1\}$

Với  $k = (a, b) \in K$  ta định nghĩa:

$$y = e_k(x) = ax + b \pmod{26}$$

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

- Ví dụ:

- Cho  $k = (7, 3)$ . Bản rõ: **It is nice today**



- Tìm bản mã.
  - Giải mã bản mã thu được

# Các hệ mật thay thế đơn biểu

- Giải:

- Tìm bản mã của bản rõ: **It is nice today**

- Ta có hàm mã hóa:  $e_k(x) = 7x + 3 \bmod 26$

Ký tự	I	T	I	S	N	I	C	E	T	O	D	A	Y
Mã (x)	8	19	8	18	13	8	2	4	19	14	3	0	24
$7x + 3 \bmod 26$	7	6	7	25	16	7	17	5	6	23	24	3	15
Bản mã	H	G	H	Z	Q	H	R	F	G	X	Y	D	P

- Bản mã thu được là: **HGHZQHRFGXYDP**

# Các hệ mật thay thế đơn biểu

- Giải:
  - Tìm bản rõ của bản mã: **HGHZQHRFGXYDP**
    - Ta có hàm mã:  $d_k(y) = 7^{-1} \cdot (y - 3) \bmod 26 = 15 \cdot (y - 3) \bmod 26$

Bản mã	H	G	H	Z	Q	H	R	F	G	X	Y	D	P
Mã (y)	7	6	7	25	16	7	17	5	6	23	24	3	15
$15(y - 3) \bmod 26$	8	19	8	18	13	8	2	4	19	14	3	0	24
Bản rõ	I	T	I	S	N	I	C	E	T	O	D	A	Y

- Bản mã thu được là: **It is nice today**

# Nội dung

1

**Giới  
thiệu  
về hệ  
mật  
khóa  
bí mật**

2

**Các  
hệ mật  
thay  
thế  
đơn  
biểu**

3

**Các  
hệ mật  
thay  
thế đa  
biểu**

4

**Các  
hệ mật  
thay  
thế  
không  
tuần  
hoàn**

5

**Các hệ  
mật  
chuyển  
vị**

6

**Chuẩn  
mã dữ  
liệu  
DES**

7

**Chuẩn  
mã dữ  
liệu  
tiền  
tiến  
AES**

# Các hệ mật thay thế đa biểu

## 4. Hệ mã Vigenere (Vigenere Cipher):

Cho  $m$  là số nguyên dương.  $P = C = K = (Z_{26})^m$ . Với khoá  $k = (k_1, k_2, \dots, k_m) \in K$  ta xác định:

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

$$\text{và } d_k(y_1, y_2, \dots, y_m) = (y_1 - k_1, y_2 - k_2, \dots, y_m - k_m)$$

(Các phép toán đều thực hiện trên  $Z_{26}$ .)

- Nhận xét:

- Số khoá:  **$26^m$**

- $\Rightarrow$  Tấn công tìm khoá vét cạn là không khả thi <sup>13</sup>

# Các hệ mật thay thế đa biểu

- **Ví dụ minh họa:**

- $m = 6$ ,  $k = \text{cipher}$

- Bản rõ: **Information security**



- Hãy mã hoá bản rõ trên

- Giải mã bản mã vừa thu được

# Các hệ mật thay thế đa biểu

- Giải:
  - Ta có từ khoá **CIPHER**, tương ứng với dãy số: **k = (2, 8, 15, 7, 4, 17)**
  - Chuyển các ký tự rõ thành mã trên  $Z_{26}$  rồi cộng với từ khoá

Bản rõ	I	N	F	O	R	M	A	T	I	O	N	S	E	C	U	R	I	T	Y
Mã	8	13	5	14	17	12	0	19	8	14	13	18	4	2	20	17	8	19	24
Khoá	2	8	15	7	4	17	2	8	15	7	4	17	2	8	15	7	4	17	2
Bản mã	10	21	20	21	21	3	2	1	23	21	17	9	6	10	9	24	12	10	0

- Chuyển các ký tự số thành chữ cái tương ứng. Ta có bản mã: **KVUVVDCBXRJGKJYMKA**

# Các hệ mật thay thế đa biểu

Bản rõ	I	N	F	O	R	M	A	T	I	O	N	S	E	C	U	R	I	T	Y
Bản mã	K	V	U	V	V	D	C	B	X	V	R	J	G	K	J	Y	M	K	A

- Nhận xét?

- Như vậy có chữ mã khác nhau cho cùng một chữ của bản rõ.
  - Ví dụ: Chữ I được mã bởi các chữ: K, X, M; chữ N được mã bởi các chữ V, R; ...
- Tuy nhiên, do độ dài của khoá có hạn, nên có thể tạo nên chu kỳ vòng lặp
  - Ví dụ: Do lặp lại chu kỳ khoá nên chữ O đều được mã hoá bởi chữ V



# Các hệ mật thay thế đa biểu

## 5. Hệ mật Playfair:

- Được sáng tạo bởi Charles Wheastone vào năm 1854 và mang tên người bạn là Baron Playfair.
- Ý tưởng:
  - Mã bộ các chữ, mỗi chữ sẽ được mã bằng một số chữ khác nhau tùy thuộc vào các chữ mà nó đứng cạnh

# Các hệ mật thay thế đa biểu

- **Ma trận khoá Playfair:**

- Cho trước một từ làm khoá. Ta lập ma trận Playfair là ma trận cỡ  $5 \times 5$  dựa trên từ khoá đã cho và gồm các chữ trên bảng chữ cái, được sắp xếp theo thứ tự nhất định.

# Các hệ mật thay thế đa biểu

- Quy tắc sắp xếp:

1

Trước hết viết các chữ của từ khoá vào các hàng của ma trận bắt từ hàng thứ nhất.

2

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.

3

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.

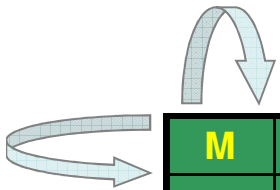
# Các hệ mật thay thế đa biểu

- Giả sử sử dụng từ khoá **MONARCHY**. Lập ma trận khoá Playfair tương ứng như sau:

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

- Cách mã hóa và giải mã:**
  - 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**”.

# Các hệ mật thay thế đa biểu



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

- Nếu cả hai chữ trong cặp đều rơi vào cùng một hàng:
  - Mã mỗi chữ bằng chữ ở phía bên phải nó trong cùng hàng của ma trận khóa (cuộn vòng quanh từ cuối về đầu)
  - Ví dụ:
    - “ar” biến đổi thành “RM”
    - “ps” biến đổi thành “QT”
- Nếu cả hai chữ trong cặp đều rơi vào cùng một cột
  - Mã mỗi chữ bằng chữ ở phía bên dưới nó trong cùng cột của ma trận khóa (cuộn vòng quanh từ cuối về đầu)
  - Ví dụ:
    - “mu” biến đổi thành “CM”
    - “hp” biến đổi thành “FV”

# Các hệ mật thay thế đa biểu

- 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.
  - Ví dụ:
    - “**hs**” mã thành “**BP**”,
    - “**ea**” mã thành “**IM**” hoặc “**JM**” (tùy theo sở thích)

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

# Các hệ mật thay thế đa biểu

- BT:
  - Cho từ khóa: “Charles”. Hãy thiết lập ma trận khóa Playfair tương ứng.
  - Mã hóa bản rõ:

Hen gap nhau vao chieu thu bay.
  - Giải mã bản mã vừa thu được.

# Các hệ mật thay thế đa biểu

## 6. Hệ mật Hill (Hill Cipher):

- Lester S.Hill đưa ra năm 1929
- Ý tưởng: lấy  $m$  tổ hợp tuyến tính của  $m$  kí tự trong một phần tử bản rõ để tạo ra một phần tử  $m$  kí tự trong một phần tử của bản mã.



# Các hệ mật thay thế đa biểu

- **Mô tả:**

Cho  $m$  là số nguyên dương cố định. Cho  $P = C = (Z_{26})^m$ .  
 $K = \{\text{các ma trận khả nghịch cấp } m \times m \text{ trên } Z_{26}\}$ :

Với  $k \in K$ , ta xác định:

$$e_k(x_1, x_2, \dots, x_m) = (x_1, x_2, \dots, x_m) \cdot k$$

$$d_k(y_1, y_2, \dots, y_m) = (y_1, y_2, \dots, y_m) \cdot k^{-1}$$

(Các phép toán đều thực hiện trên  $Z_{26}$ .)

# Các hệ mật thay thế đa biểu

- Cho ma trận:  $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$
- Định thức  $\det A = a_{11} \cdot a_{22} - a_{12} \cdot a_{21}$
- Ma trận là khả nghịch  $\Leftrightarrow \det A \neq 0$
- Vì các phép toán tính theo modulo 26 nên phải có điều kiện:  $\text{UCLN}(\det A, 26) = 1$ .
- Ma trận nghịch đảo:  $A^{-1} = (\det A)^{-1} \cdot \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}$

# Các hệ mật thay thế đa biểu

- **Ví dụ minh họa:**

- Bản rõ: “july”

- Ma trận khoá:  $k = \begin{pmatrix} 1 & 1 & 8 \\ 3 & & 7 \end{pmatrix}$

- Tìm bản mã của bản rõ trên
    - Từ bản mã thu được tìm bản rõ ban đầu.

# Nội dung

1

**Giới  
thiệu  
về hệ  
mật  
khóa  
bí mật**

2

**Các  
hệ mật  
thay  
thế  
đơn  
biểu**

3

**Các  
hệ mật  
thay  
thế đa  
biểu**

4

**Các  
hệ mật  
thay  
thế  
không  
tuần  
hoàn**

5

**Các hệ  
mật  
chuyển  
vị**

6

**Chuẩn  
mã dữ  
liệu  
DES**

7

**Chuẩn  
mã dữ  
liệu  
tiền  
tiến  
AES**

## Các hệ mật thay thế không tuần hoàn

- Phép thế lý tưởng là dùng nhiều bảng chữ cái.
- Vigenere đề xuất hệ mật khoá tự sinh (hệ mật khoá chạy)

# Các hệ mật thay thế không tuần hoàn

## 7. Hệ mật khoá chạy:

### – Ý tưởng:

- Từ khoá được nối tiếp bằng chính bản rõ, sau đó sử dụng mã Vigenere để mã
- Khi biết từ khoá, giải được một số chữ của bản rõ rồi dùng chúng giải nốt phần còn lại
- Sự cải tiến này gây mất khái niệm chu kỳ.

### – Ví dụ:

- Key = **deceptive**
- Bản rõ: **we are discovered save yourself**



– Hãy mã hoá bản rõ trên.

– Giải mã bản mã thu được

# Các hệ mật thay thế không tuần hoàn

## Mã hoá bản rõ

Khoá	D	E	C	E	P	T	I	V	E																		
Bản rõ	W	E	A	R	E	D	I	S	C	O	V	E	R	E	D	S	A	W	E	Y	O	U	R	S	E	L	F
Bản mã	Z	I	C	V	T	W	Q	N	G	K	Z	E	I	I	G	A	S	X	S	T	S	L	V	V	W	L	A

# Các hệ mật thay thế không tuần hoàn

Giải mã bản mã thu được

Khoá	D	E	C	E	P	T	I	V	E																		
Bản mã	Z	I	C	V	T	W	Q	N	G	K	Z	E	I	I	G	A	S	X	S	T	S	L	V	V	W	L	A
Bản rõ	W	E	A	R	E	D	I	S	C	O	V	E	R	E	D	S	A	V	E	Y	O	U	R	S	E	L	F



# Các hệ mật thay thế không tuần hoàn

- Hệ mật Vernam (OTP)

Cho  $n \geq 1$ .  $P = C = K = (Z_2)^n$ . Với khoá  $k = (k_1, k_2, \dots, k_n) \in K$  ta xác định:

$$e_k(x_1, x_2, \dots, x_n) = (x_1 + k_1, x_2 + k_2, \dots, x_n + k_n) \bmod 2$$

$$\text{và } d_k(y_1, y_2, \dots, y_n) = (y_1 + k_1, y_2 + k_2, \dots, y_n + k_n) \bmod 2$$

# Nội dung

1

**Giới  
thiệu  
về hệ  
mật  
khóa  
bí mật**

2

**Các  
hệ mật  
thay  
thế  
đơn  
biểu**

3

**Các  
hệ mật  
thay  
thế đa  
biểu**

4

**Các  
hệ mật  
thay  
thế  
không  
tuần  
hoàn**

5

**Các hệ  
mật  
chuyển  
vị**

6

**Chuẩn  
mã dữ  
liệu  
DES**

7

**Chuẩn  
mã dữ  
liệu  
tiền  
tiến  
AES**

# Các hệ mật chuyển vị

- Ý tưởng:
  - Các chữ trong bản rõ không được thay thế bằng các chữ khác mà chỉ thay đổi vị trí giữa các chữ trong bản rõ.

# Các hệ mật chuyển vị

## 8. Mã hoán vị (Permutation Cipher):

Cho  $m$  là số nguyên dương xác định. Cho  $P = C = (Z_{26})^m$ ,  $K$  là tất cả hoán vị có thể có của  $\{1, 2, \dots, m\}$ :

Với khoá  $\pi \in K$ , ta xác định:

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

$$d_{\pi} = (y_{\pi^{-1}(1)}, \dots, y_{\pi^{-1}(m)}) = (x_1, \dots, x_m)$$

(Trong đó  $\pi^{-1}$  là hoán vị ngược của  $\pi$ )

# Các hệ mật chuyển vị

- Ví dụ 1:

- $m = 6$ ; khóa là phép hoán vị  $\pi$  sau:

1	2	3	4	5	6
3	5	1	6	4	2

- Khi đó phép HV ngược  $\pi^{-1}$ :

1	2	3	4	5	6
3	6	1	5	2	4

- Bản rõ: **Hen gap nhau vào chiều thu bay**

# Các hệ mật chuyển vị

- **Mã hóa:**

- **B1:** Nhóm bản rõ thành các nhóm 6 kí tự

Hengap nhauva ochieu thubay

- **B2:** Mỗi nhóm 6 kí tự sẽ được sắp xếp lại theo theo phép HV  $\pi (3, 5, 1, 6, 4, 2)$ , ta có:

Nahpge avnauh heouic uatybh

- Khi đó ta có bản mã:

**Nahpgeavnauhheouicuatybh**

# Các hệ mật chuyển vị

- **Giải mã:**
  - **B1:** Nhóm bản mã thành các nhóm 6 kí tự
  - **B2:** Mỗi nhóm 6 kí tự sẽ được sắp xếp lại theo theo phép HV  $\pi^{-1}$  (3, 6, 1, 5, 2, 4)

# Thăm mã các hệ mật cổ điển

- **Vấn đề thăm mã các hệ mật**

- Các hệ mật được dùng để *đảm bảo tính bí mật* cho thông tin được trao đổi
  - ⇒ **Do đó, vấn đề quan trọng nhất của Thăm mã là “phá bỏ tính bí mật” đó.**
- Tức là với bản mật mã có thể dễ dàng thu được (trên các kênh truyền công cộng) người thăm mã phải *phát hiện được nội dung thông tin được che dấu trong bản mật mã đó, mà tốt nhất là tìm được bản tin rõ gốc của bản mật mã đó.*



# Thăm mã các hệ mật cổ điển

- **Vấn đề thăm mã các hệ mật**

- Tình huống thường gặp là *bản thân sơ đồ hệ thống mật mã, kể cả phép mã hóa và giải mã ( $E$  và  $D$ ) không nhất thiết là bí mật*

- $\Rightarrow$  do đó bài toán quy về việc tìm khóa mật mã  $k$ , hay khóa giải mã  $k_d$

# Thăm mã các hệ mật cổ điển

- **Vấn đề thăm mã các hệ mật**

- Ngoài ra, người thăm mã có thể biết thêm một số thông tin khác. Tùy theo những thông tin được biết thêm này mà ta có thể phân loại bài toán thăm mã thành các bài toán cụ thể như sau:

- Bài toán thăm mã *chỉ biết bản mã*: Là bài toán phổ biến nhất, người thăm mã chỉ biết bản mật Y.
    - *Biết cả bản rõ*: Người thăm mã biết bản mật Y cùng với bản rõ X tương ứng.
    - *Có bản rõ được chọn*: Người thăm mã có thể chọn một bản rõ X và biết bản mã Y tương ứng (Chiếm được tạm thời máy lập mã)
    - *Có bản mã được chọn*: Thăm mã có thể chọn một bản mã Y và biết bản rõ X tương ứng (Chiếm được tạm thời máy giải mã)

# Thăm mã các hệ mật cổ điển

- **Một số nhận xét**

- Ta vẫn giả thiết bản rõ cũng như bản mã đều được xây dựng trên bảng ký tự tiếng Anh và hơn nữa các thông báo là các văn bản tiếng Anh.
- Như vậy, ta luôn có  $P = C = Z_{26}$  hay  $(Z_{26})^m$  và có thêm thông tin là **các bản rõ tuân theo các quy tắc từ pháp và cú pháp của ngôn ngữ tiếng Anh.**
- Các kết quả chủ yếu được sử dụng nhiều nhất trong thám mã là quy tắc thống kê tần suất xuất hiện các ký tự hay các bộ đôi, bộ ba, ... ký tự liên tiếp trong văn bản tiếng Anh.

# Thăm mã các hệ mật cổ điển

- **Một số nhận xét**

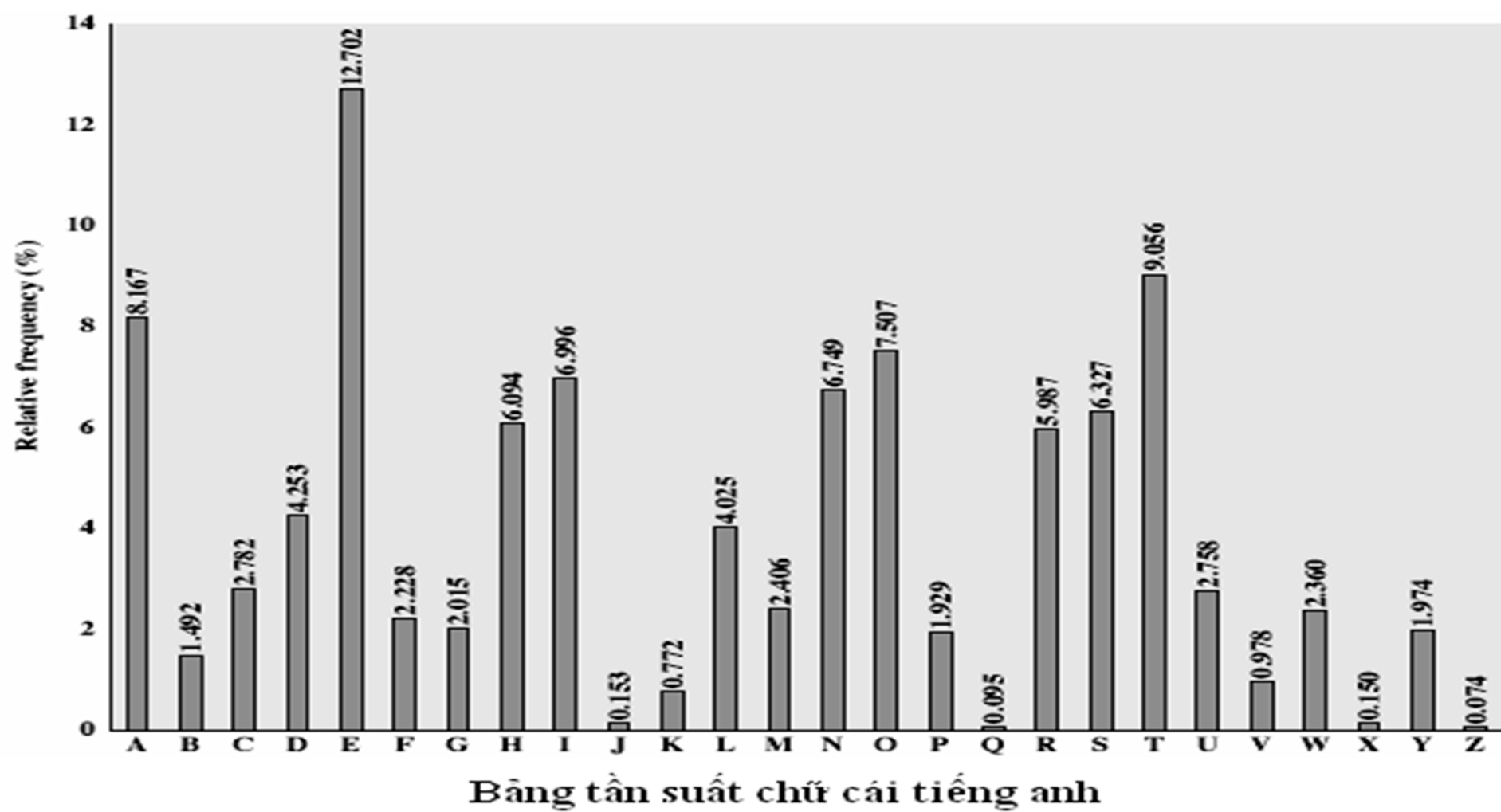
- Trên cơ sở phân tích các số liệu thống kê từ một số lượng rất lớn các văn bản thư từ, sách vở, báo chí,... người ta đã thu được những kết quả và được tổng hợp lại như sau:

1. Ký tự *e* có xác suất xuất hiện cao nhất là 0.127
2. Các ký tự *t, a, o, l, n, s, h, r* có xác suất từ 0.060 đến 0.090
3. Các ký tự *d, i* có xác suất khoảng 0.04
4. Các ký tự *c, u, m, w, f, g, y, p, b* từ 0.015 đến 0.028
5. Các ký tự *v, k, j, x, q, z* có xác suất dưới 0.01

# Thăm mã các hệ mật cổ điển

- **Một số nhận xét**

- Trên cơ sở phân tích các số liệu thống kê từ một số lượng rất lớn các văn bản thư từ, sách vở, báo chí,... người ta đã thu được những kết quả và được tổng hợp lại như sau:
  - ...
  - Ba mươi bộ đôi ký tự có xác suất xuất hiện cao nhất 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, of*
  - Mười hai bộ ba ký tự có xác suất xuất hiện cao nhất là: *the, ing, and, her, ere, ent, tha, nth, was, eth, for, dth*
- Sau đây là bảng thống kê tần suất của các ký tự



# Thăm mã các hệ mật cổ điển

- Nhận xét về các hệ mật thay thế đơn biểu:
    - Mỗi ký tự của bản rõ được ánh xạ đến một ký tự duy nhất của bản mã.
    - Các đặc trưng về ngôn ngữ, tần suất xuất hiện của các chữ trong bản rõ và chữ tương ứng trong bản mã là như nhau
- ⇒ **Phương pháp thám mã bằng thống kê tần suất!**

# Thăm mã các hệ mật cổ điển

- Phương pháp thăm mã bằng thống kê tần suất:
  - Bảng cách thống kê trên bản mã:
    - Đếm tần suất của các chữ trong bản mã
    - So sánh với các giá trị đã biết
    - Tìm kiếm các chữ đơn, bộ đôi và bộ ba hay dùng; và các bộ ít dùng
    - Dựa vào bảng tần suất xuất hiện của các chữ cái để đoán và tìm ra bản rõ



# Thám mã các hệ mật cổ điển

- Thám mã Affin bằng pp thống kê tần suất:
  - Nếu biết 2 cặp bản rõ, bản mã  $(x, y)$  khác nhau ta có được hệ 2 phương trình tuyến tính để từ đó tìm ra  $a, b$
  - Ví dụ: Ta có bản mã

*fmxvedkaphferbndkrxrsrefmorudsdkdvshvufedkapr  
kdlyevlrhhrh*

Hãy tìm khóa và bản rõ tương ứng?

# Thám mã các hệ mật cổ điển

- Thám mã Apphin bằng pp thống kê tần suất:
  - Ví dụ: Ta có bản mã  
*fmxvedkaphferbndkrxrsrefmorudsdkdvshvufedkapr  
kdlyevlrhhrh*
  - *r* xuất hiện 8 lần, *d* 7 lần, *e*, *k*, *h* mỗi ký tự 5 lần,  
*f*, *s*, *v* mỗi ký tự 4 lần, v.v...

# Thám mã các hệ mật cổ điển

- Thám mã Affin bằng pp thống kê tần suất:
  - Như vậy có thể phán đoán  $r$  là mã của  $e$ ,  $d$  là mã của  $t$ , khi đó ta có:
$$17 = 4a + b \bmod 26$$
$$3 = 19a + b \bmod 26$$
$$a = ?, b = ?$$

# Thám mã các hệ mật cổ điển

- Thám mã Affin bằng pp thống kê tần suất:
  - Thử chọn một phán đoán khác:  $r$  là mã của  $e$ ,  $h$  là mã của  $t$ . Khi đó ta có:
$$17 = 4a + b \text{ mod } 26$$
$$7 = 19a + b \text{ mod } 26$$
$$a = ?, b = ?$$

# Thám mã các hệ mật cổ điển

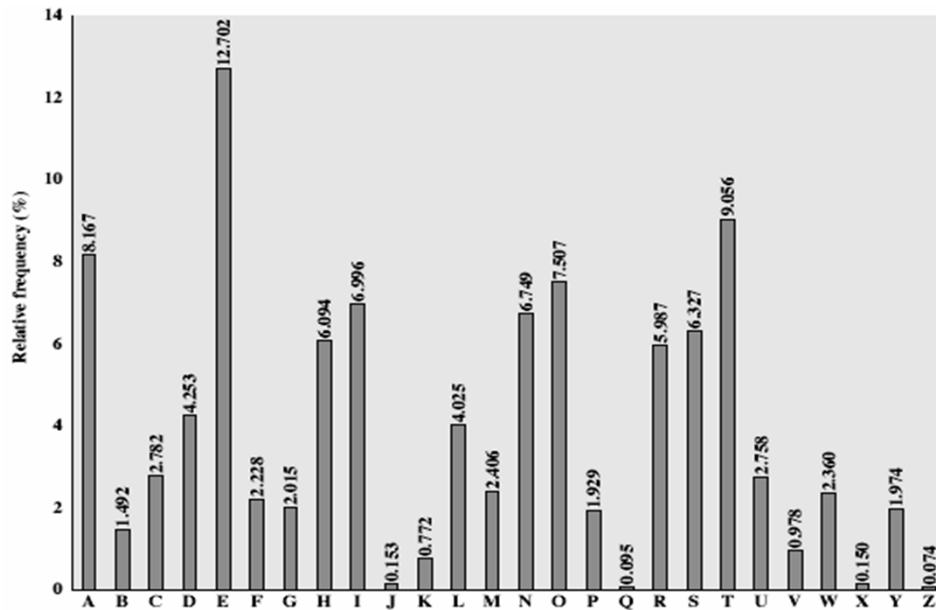
- **Ví dụ:** Giả sử ta có bản mã bởi hệ mật apphin

GWNBA	GRQPB	AGNBH	WNDJD	ORGGR	ANIBR	OGWNI	ZFNIZ
WRRKR	QGWNN	ONLVD	ORGHR	LZOTE	JGROR	JARPO	ANBKZ
ONDDG	RANHN	ZMNWZ	LORGR	OGWNH	WBOHN	RQWZD	ORGBG
GBHFZ	OTEJG	ABGWN	AROGW	NQBHG	GWBGP	NWBKL	BKNRJ
AURDZ	GZROJ	OBDDDB	ZIBEI				

- Thám mã bằng phương pháp thống kê tần suất?

# Thăm mã các hệ mật cổ điển

- Bước 1:** xác định tần suất



Bảng tần suất chữ cái tiếng anh

Kí tự	Tần suất xuất hiện	Kí tự	Tần suất xuất hiện
G	22	I	5
N	21	K	4
R	21	L	4
B	16	Q	4
O	16	E	3
W	13	P	3
Z	11	F	2
A	9	T	2
D	9	M	1
H	7	U	1
J	6	V	1

# Thám mã các hệ mật cổ điển

- **Bước 2:** Tách nhóm

- Từ bảng tần suất, giả sử

- **G (6)** là mã hóa của **E (4)**

- **N (13)** là mã hóa của **T (19)**

- Thiết lập hệ phương trình 
$$\begin{cases} 4a + b = 6 \\ 19a + b = 13 \end{cases}$$

- Giải hệ được  **$a = 23$ ,  $b = -8 = 18$** . Ta có hàm mã:

$$e_k(x) = 23x + 18 \bmod 26$$

- Hàm giải mã tương ứng:

$$d_k(y) = 17(y - 18) = (17y + 6) \bmod 26$$

# Thám mã các hệ mật cổ điển

- **Bước 3:** Tìm bản rõ
  - Từ hàm giải mã, ta có bản rõ tương ứng:

aefps	atwzp	safpx	efjrr	cyaat	sfuht	caefu	vdfuv
ettot	waeff	cflhj	ctaxt	lvcng	ratct	rstzc	sfpov
cfjja	tafxf	vifev	lctat	caefx	epcxf	twevj	ctapa
apxdv	cngra	apaef	atcae	fwpxa	aepaz	fepol	poftr
aktjv	avtcr	cpjjp	vupgu				



# Thám mã các hệ mật cổ điển

- Quay lại bước 2
  - Giả sử **G** là mã hóa của **T**
  - **N** là mã hóa của **E**
  - Ta lại có hệ: 
$$\begin{cases} 19a + b = 6 \\ 4a + b = 13 \end{cases}$$
  - Giải hệ được **a = 3, b = 1**. Ta có hàm mã:
$$e_k(x) = 3x + 1 \bmod 26$$
  - Hàm giải mã tương ứng:
$$d_k(y) = 9(y - 1) = 9y + 17 \bmod 26$$

# Thám mã các hệ mật cổ điển

- **Bước 3:** Bản rõ tương ứng

“The art of war teaches us to rely not on the likelihood of the enemy’s not coming but on our own readiness to receive him not on the chance of his not attacking but rather on the fact that we have made our position unassailable”

- **BTVN:** Thám mã Affine bằng phương pháp thống kê tần suất. Bản mã:

**AHMKEHXCNOFOOPCWSKPUMCP**

# Thăm mã các hệ mật cổ điển

- Thăm mã đối với hệ mật Hill:
  - Hệ mật Hill khó bị khám phá bởi việc thăm mã *chỉ dựa vào bản mã*
  - Nhưng lại là dễ bị khám phá nếu có thể sử dụng phương pháp thăm mã kiểu *biết cả bản rõ*

# Thăm mã các hệ mật cổ điển

- Thăm mã đối với hệ mật Hill:
  - Trước hết ta giả thiết là **đã biết giá trị  $m$**
  - Mục đích của thăm mã là phát hiện được khóa mật mã  $k$

*Trong trường hợp này là một ma trận vuông cấp  $m$  có các thành phần thuộc  $Z_{26}$*

# Thám mã các hệ mật cổ điển

- Thám mã đối với hệ mật Hill:
  - Ta chọn một bản rõ gồm  $m$  bộ  $m$  thành phần khác nhau các ký tự:

$$x_1 = (x_{11}, \dots, x_{1m}), \dots, x_m = (x_{m1}, \dots, x_{mm})$$

- Và giả thiết biết bản mã tương ứng của chúng là

$$y_1 = (y_{11}, \dots, y_{1m}), \dots, y_m = (y_{m1}, \dots, y_{mm})$$

# Thăm mã các hệ mật cổ điển

- Thăm mã đối với hệ mật Hill:
  - Ta ký hiệu  $x$  và  $y$  là 2 ma trận vuông cấp  $m$ :  
$$x = (x_{ij}) \text{ và } y = (y_{ij})$$
  - Theo định nghĩa của mã Hill ta có phương trình:  
$$y = x.k$$
  - Nếu  $x_i$  được chọn sao cho  $x$  có nghịch đảo  $x^{-1}$  thì ta tìm được  $k = x^{-1}.y$

# Thám mã các hệ mật cổ điển

- Thám mã đối với hệ mật Hill:
  - Ví dụ: Giả sử mã Hill được sử dụng với  $m = 2$ , có bản mã là *pqcfku* và biết bản rõ tương ứng là *friday*
  - Như vậy ta biết  $e_k(5,17)=(15,16)$ ;  $e_k(8,3)=(2,5)$  và  $e_k(0,24)=(10,20)$
  - Từ 2 ptinh đầu ta có: 
$$\begin{bmatrix} 15 & 16 \\ 2 & 5 \end{bmatrix} = \begin{bmatrix} 5 & 17 \\ 8 & 3 \end{bmatrix} \cdot k$$

# Thăm mã các hệ mật cổ điển

- Thăm mã đối với hệ mật Hill:
  - Khóa  $k$  được xem là đúng nếu ngoài  $m$  cặp bộ  $m$  dùng để tìm khóa,  $k$  vẫn nghiệm đúng với các cặp bộ  $m$  khác mà ta có thể chọn để thử.



# Nội dung

1

**Giới  
thiệu  
về hệ  
mật  
khóa  
bí mật**

2

**Các  
hệ mật  
thay  
thế  
đơn  
biểu**

3

**Các  
hệ mật  
thay  
thế đa  
biểu**

4

**Các  
hệ mật  
thay  
thế  
không  
tuần  
hoàn**

5

**Các hệ  
mật  
chuyển  
vị**

6

**Chuẩn  
mã dữ  
liệu  
DES**

7

**Chuẩn  
mã dữ  
liệu  
tiền  
tiến  
AES**

# Nội dung

1

**Giới  
thiệu  
về hệ  
mật  
khóa  
bí mật**

2

**Các  
hệ mật  
thay  
thế  
đơn  
biểu**

3

**Các  
hệ mật  
thay  
thế đa  
biểu**

4

**Các  
hệ mật  
thay  
thế  
không  
tuần  
hoàn**

5

**Các hệ  
mật  
chuyển  
vị**

6

**Chuẩn  
mã dữ  
liệu  
DES**

7

**Chuẩn  
mã dữ  
liệu  
tiền  
tiến  
AES**