

CHƯƠNG 2: CÁC KHÁI NIỆM CƠ SỞ VÀ HỆ MẬT MÃ CỔ ĐIỂN

2.1. Sơ lược về lịch sử mã hóa.

Mật mã học cổ điển

- Các chữ tượng hình được tìm thấy trên các bức tượng Ai Cập cổ đại (cách đây khoảng 4500 năm tr.CN).
- Mã hóa thay thế bằng chữ cái đơn giản như mật mã hóa Atbash (khoảng năm 500-600 tr.CN).



CHƯƠNG 2: CÁC KHÁI NIỆM CƠ SỞ VÀ HỆ MẬT MÃ CỔ ĐIỂN

2.1. Sơ lược về lịch sử mã hóa.

Mật mã học cổ điển

- Mã hóa chuyển vị của người Hy Lạp từ 400 năm tr. CN

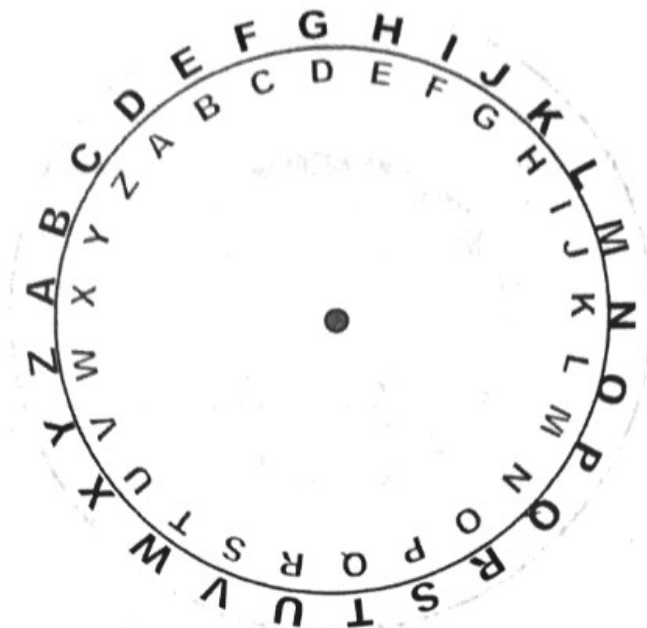


CHƯƠNG 2: CÁC KHÁI NIỆM CƠ SỞ VÀ HỆ MẬT MÃ CỔ ĐIỂN

2.1. Sơ lược về lịch sử mã hóa.

Mật mã học cổ điển

- Người La Mã xây dựng mật mã Caesar (khoảng năm 100-40 tr.CN)



Plaintext: THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

Ciphertext: QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD

CHƯƠNG 2: CÁC KHÁI NIỆM CƠ SỞ VÀ HỆ MẬT MÃ CỔ ĐIỂN

2.1. Sơ lược về lịch sử mã hóa.

Mật mã học cổ điển

- Người hỏi giáo giải mật mã Caesar như thế nào? (khoảng năm 800 sau CN)

Phương pháp phân tích tần suất:

thống kê tần suất xuất hiện của các chữ cái trong văn bản mã hoá

Ví dụ: Giải mã

[ksofshvsqvoadwcb](#)



Al-Kindi (801-873).

CHƯƠNG 2: CÁC KHÁI NIỆM CƠ SỞ VÀ HỆ MẬT MÃ CỔ ĐIỂN

2.1. Sơ lược về lịch sử mã hóa.

Mật mã học cổ điển

- Mã Vigenere (“*mật mã vô địch*”):
cải tiến của mã Ceasar (cuối thế kỷ XVI)

Ý tưởng: Mỗi chữ cái trong văn bản gốc sẽ được mã hóa bằng một bảng chữ cái Ceasar khác nhau.



Blaise Vigenère (1523-1596)

CHƯƠNG 2: CÁC KHÁI NIỆM CƠ SỞ VÀ HỆ MẬT MÃ CỔ ĐIỂN

2.1. Sơ lược về lịch sử mã hóa.

Mật mã học cổ điển

- Mã vô địch bị phá như thế nào?

<http://antoanthongtin.vn/gp-mat-ma/tham-mat-ma-vigenere-106294>

Sách tham khảo

Khoa Học Khám Phá - Mật Mã - Từ Cổ Điển Đến Lượng Tử

NXB Trẻ - Tác giả: Simon Singh

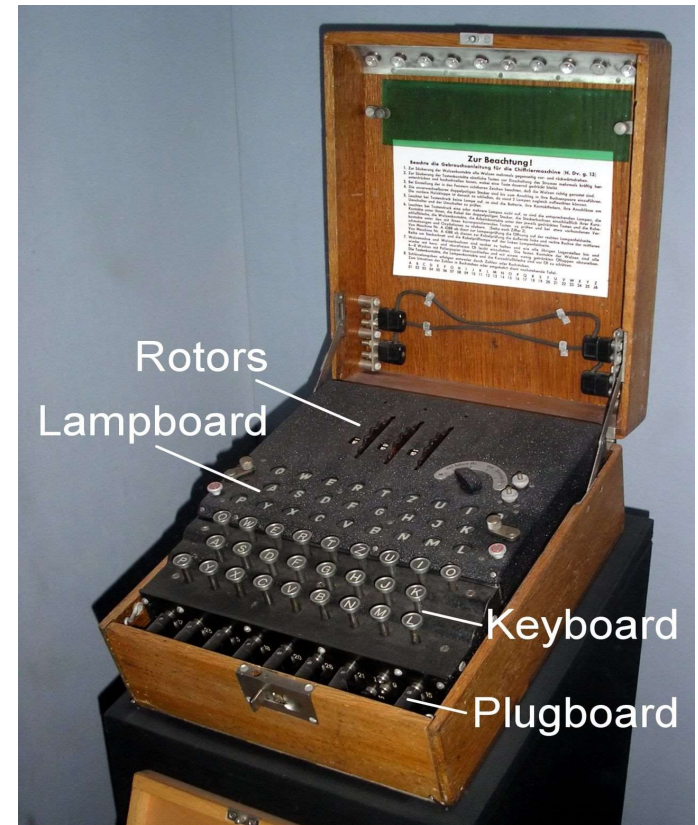


Charles Babbage (1791-1871)

CHƯƠNG 2: CÁC KHÁI NIỆM CƠ SỞ VÀ HỆ MẬT MÃ CỔ ĐIỂN

Mật mã trong thế chiến thứ II – Máy Enigma

- Ra đời năm 1918, song tới năm 1926 mới được sử dụng rộng rãi với mục đích quân sự
- Nếu có 10 người cùng ngồi thử từng thuật toán mã hoá của Enigma, làm việc suốt 24/7 thì phải mất 20 triệu năm mới giải mã được một bức mật hàm. Trong Thế chiến thứ II, quân Đồng Minh chỉ có tối đa 18 tiếng để giải mã, vì cứ sau nửa đêm các cỗ máy Enigma lại được thông báo thay đổi cấu trúc và tạo thành 159 triệu triệu khả năng hoàn toàn khác.
- Khoảng 11.000 người tại Bletchley Park và 4.000 ở Mỹ đã làm việc để giải mã Enigma



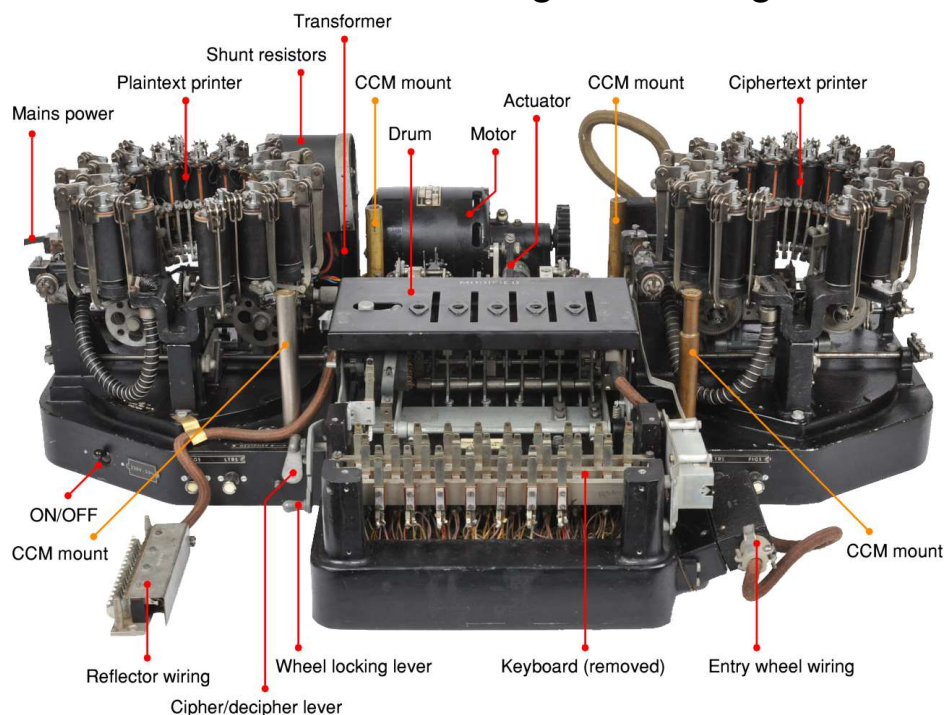
Arthur Scherbius (1878-1929)

CHƯƠNG 2: CÁC KHÁI NIỆM CƠ SỞ VÀ HỆ MẬT MÃ CỔ ĐIỂN

2.1. Sơ lược về lịch sử mã hóa.

Mật mã trong thế chiến thứ 2

- Phe Đồng minh sử dụng máy TypeX của Anh và máy SIGABA của Mỹ, đều là những thiết kế cơ điện dùng rôto tương tự như máy Enigma, song với nhiều nâng cấp hơn.



CHƯƠNG 2: CÁC KHÁI NIỆM CƠ SỞ VÀ HỆ MẬT MÃ CỔ ĐIỂN

2.1. Sơ lược về lịch sử mã hóa.

Mật mã trong thế chiến thứ 2

Mật mã sử dụng máy Enigma bị phá như thế nào?

- Cơ quan mật mã Ba Lan
- Cơ quan tình báo Anh
- Quân đội Mỹ



Alan Turing (1912-1954)
"The Imitation Game"

CHƯƠNG 2: CÁC KHÁI NIỆM CƠ SỞ VÀ HỆ MẬT MÃ CỔ ĐIỂN

2.1. Sơ lược về lịch sử mã hóa.

Mật mã hiện đại

- 1974: Hệ mã Lucifer
- 1975: Tiêu chuẩn mật mã hóa dữ liệu **DES** (**D**ata **E**ncryption **S**tandard): là một phương thức mã hoá được công bố tại Mỹ vào ngày 17.03.1975, bởi nhóm nghiên cứu tại **IBM**
- 1976: Hệ mã hóa khóa công khai

CHƯƠNG 2: CÁC KHÁI NIỆM CƠ SỞ VÀ HỆ MẬT MÃ CỔ ĐIỂN

2.2. Một số thuật ngữ.

- **Văn bản rõ (Plaintext):** là văn bản gốc cần được mã hóa, thường được kí hiệu là PT hay P.
- **Văn bản mã (Ciphertext):** là văn bản mã hóa từ văn bản gốc, thường được kí hiệu là CT hay C.
- **Hệ mật mã (Cryptosystem):** là một phương pháp ngụy trang văn bản.
- **Mật mã học (Cryptography):** nghệ thuật tạo ra và sử dụng các hệ mật mã.
- **Công nghệ mã (Cryptology):** là việc nghiên cứu tổng hợp cả cryptography và cryptanalysis
- **Thám mã hay phân tích mã (Cryptanalysis):** là nghệ thuật phá các hệ mã
- **Mã hoá (Encryption):** là quá trình chuyển đổi từ văn bản rõ thành văn bản mã.
- **Giải mã (Decryption):** là quá trình chuyển ngược lại từ văn bản mã hoá thành văn bản rõ.

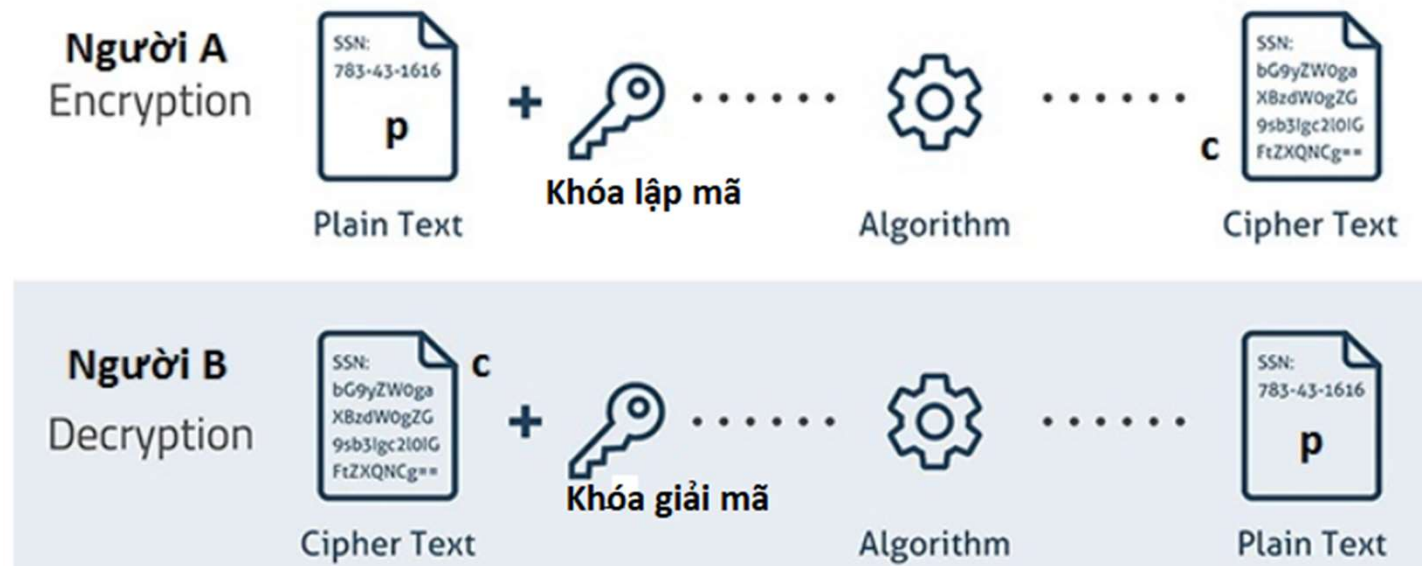
CHƯƠNG 2: CÁC KHÁI NIỆM CƠ SỞ VÀ HỆ MẬT MÃ CỔ ĐIỂN

2.2. Một số thuật ngữ.

- **Mã dòng (stream cipher):** là việc tiến hành mã hóa liên tục trên từng ký tự (hay từng bit).
- **Mã khối (block cipher):** là việc tiến hành mã hóa liên tục trên từng khối văn bản.
- **Phép mã chuyển vị (transposition cipher):** là việc tráo đổi vị trí giữa các ký tự trong văn bản.
- **Phép mã thay thế (substitution cipher):** là việc thay thế một ký tự này bằng một ký tự khác (mà không thay đổi vị trí).
- **Phép mã tích hợp (product cipher):** là việc tiến hành xen kẽ 2 phép mã chuyển vị và thay thế

CHƯƠNG 2: CÁC KHÁI NIỆM CƠ SỞ VÀ HỆ MẬT MÃ CỔ ĐIỂN

2.3. Hệ mã hóa (Cryptosystem).



Quy trình hoạt động của hệ mật mã

CHƯƠNG 2: CÁC KHÁI NIỆM CƠ SỞ VÀ HỆ MẬT MÃ CỔ ĐIỂN

2.3. Hệ mã hóa (Cryptosystem).

Một hệ mã hóa là một bộ **(P, C, K, E, D)** trong đó:

- **P** là tập các văn bản gốc cần mã hóa
- **C** là tập các văn bản mã hóa
- **K** là tập các khóa
- **E** = $\{e_k: k \in K\}$, trong đó: $e_k: P \rightarrow C$ là các hàm lập mã
- **D** = $\{d_k: k \in K\}$, trong đó: $d_k: C \rightarrow P$ là các hàm giải mã

CHƯƠNG 2: CÁC KHÁI NIỆM CƠ SỞ VÀ HỆ MẬT MÃ CỔ ĐIỂN

2.4. Các hệ mã hóa cổ điển

2.4.1. Mã thay thế đơn giản (Substitution Cipher)

- Trong phép này, khoá là một hoán vị h của bảng chữ cái và mỗi ký hiệu của thông báo được thay thế bằng ảnh của nó qua hoán vị h .
- Khoá thường được biểu diễn bằng một chuỗi 26 ký tự. Có $26!$ ($\approx 4.10^{26}$) hoán vị (khoá)

CHƯƠNG 2: CÁC KHÁI NIỆM CƠ SỞ VÀ HỆ MẬT MÃ CỔ ĐIỂN

2.4. Các hệ mã hóa cổ điển

2.4.2. Mã hoán vị bậc d (Permutation Cypher)

- Đối với một số nguyên dương d bất kỳ, chia thông báo m thành từng khối có chiều dài d . Rồi lấy một hoán vị h của $1, 2, \dots, d$ và áp dụng h vào mỗi khối.
- Ví dụ: nếu $d=5$ và $h=(4\ 1\ 3\ 2\ 5)$, hoán vị $(1\ 2\ 3\ 4\ 5)$ sẽ được thay thế bằng hoán vị mới $(4\ 1\ 3\ 2\ 5)$.
- Ví dụ: ta có thông báo $m = \text{JOHN IS A GOOD ACTOR}$ Qua phép mã hoá này m sẽ trở thành chuỗi mật mã c sau: $c = \text{NJHO AI S DGOO OATCR}$

CHƯƠNG 2: CÁC KHÁI NIỆM CƠ SỞ VÀ HỆ MẬT MÃ CỔ ĐIỂN

2.4. Các hệ mã hóa cổ điển

2.4.3. Mã tuyến tính (Affine Cipher):

Mã tuyến tính là mã thay thế có dạng:

$e(x) = ax + b \pmod{26}$, với a, b là các số nguyên không âm không lớn hơn 26.

Nếu $a = 1$ ta có mã Ceasar.

Giải mã: Tìm x ?

$$y = ax + b \pmod{26}$$

$$ax = y - b \pmod{26}$$

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

CHƯƠNG 2: CÁC KHÁI NIỆM CƠ SỞ VÀ HỆ MẬT MÃ CỔ ĐIỂN

2.4. Các hệ mã hóa cổ điển

2.4.4. Mã Playfair

Mật mã đa ký tự (mỗi lần mã hoá 2 ký tự liên tiếp nhau): Giải thuật dựa trên một ma trận các chữ cái $n \times n$ ($n=5$ hoặc $n=6$) được xây dựng từ một khóa (chuỗi các ký tự).

Xây dựng ma trận khóa:

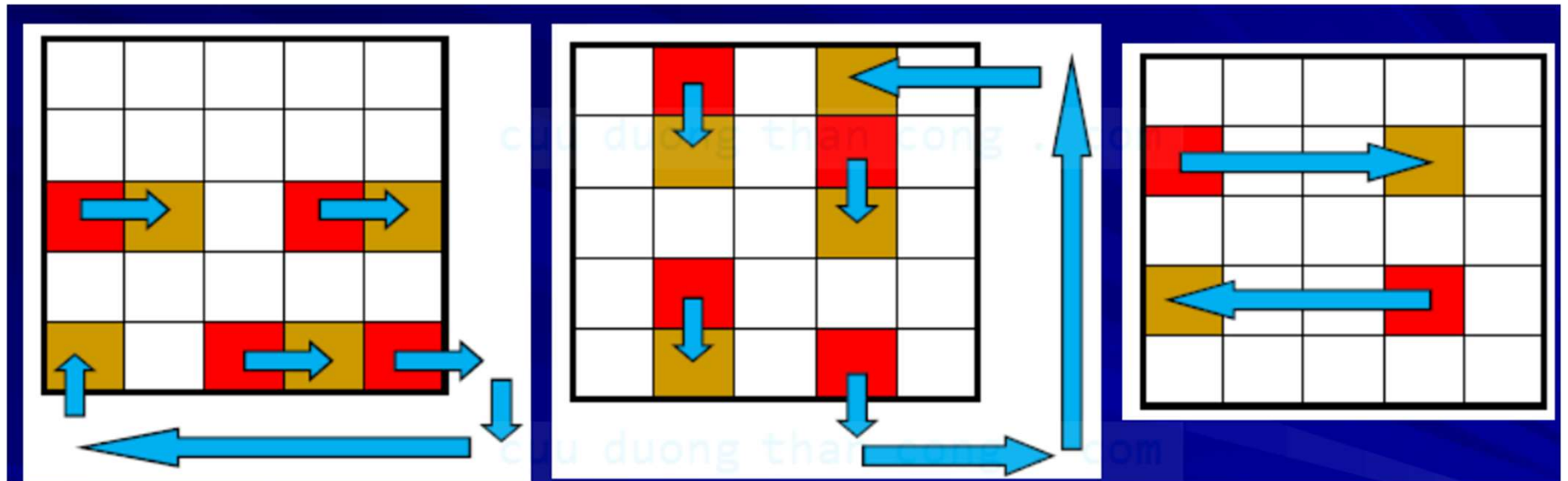
- Lần lượt thêm từng ký tự của khóa vào ma trận.
- Nếu ma trận chưa đầy, thêm các ký tự còn lại trong bảng chữ cái vào ma trận theo thứ tự A – Z.
- I và J xem như 1 ký tự.
- Các ký tự trong ma trận khoá không được trùng nhau.

CHƯƠNG 2: CÁC KHÁI NIỆM CƠ SỞ VÀ HỆ MẬT MÃ CỔ ĐIỂN

Giải thuật mã hóa:

- Mã hóa từng cặp 2 ký tự liên tiếp nhau.
- Nếu dư 1 ký tự, thêm ký tự “x” vào cuối.
- Nếu 2 ký tự nằm cùng dòng, thay thế bằng 2 ký tự tương ứng bên phải. Ký tự ở cột cuối cùng được thay bằng ký tự ở cột đầu tiên.
- Nếu 2 ký tự nằm cùng cột được thay thế bằng 2 ký tự bên dưới.
- Ký tự ở hàng cuối cùng được thay thế bằng ký tự ở hàng trên cùng
- Nếu 2 ký tự lập thành hình chữ nhật được thay thế bằng 2 ký tự tương ứng trên cùng dòng ở hai góc còn lại.

CHƯƠNG 2: CÁC KHÁI NIỆM CƠ SỞ VÀ HỆ MẬT MÃ CỔ ĐIỂN



Plain text: **th em at ch is ov er**

Cipher text: **QE AE EU BO LQ HW OT**

Từ khoá: **HOME**

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

CHƯƠNG 2: CÁC KHÁI NIỆM CƠ SỞ VÀ HỆ MẬT MÃ CỔ ĐIỂN

2.4. Các hệ mã hóa cổ điển

2.4.5. Mã Hill

- Trong mã Hill, mỗi chữ cái được gán cho một số nguyên từ 0 đến 25.
- Thay thế mỗi m ký tự bản rõ thành m ký tự bản mã, thông qua m phương trình tuyến tính

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Giả sử $m = 3$.

$$c_1 = k_{11}p_1 + k_{12}p_2 + k_{13}p_3 \mod 26$$

$$c_2 = k_{21}p_1 + k_{22}p_2 + k_{23}p_3 \mod 26$$

$$c_3 = k_{31}p_1 + k_{32}p_2 + k_{33}p_3 \mod 26$$

$$\begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix} \mod 26 \quad \text{hay} \quad C = KP \mod 26$$

CHƯƠNG 2: CÁC KHÁI NIỆM CƠ SỞ VÀ HỆ MẬT MÃ CỔ ĐIỂN

2.4. Các hệ mã hóa cổ điển

2.4.5. Mã Hill (Lester S. Hill - 1929)

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Ví dụ: Cho bản rõ: 'PAYMOREMONEY', với khóa K là

$$K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

Ba chữ cái đầu tiên trong bản rõ tương ứng với vector $P = (15, 0, 24)$. Vậy

$$\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 15 \\ 0 \\ 24 \end{bmatrix} \mod 26 = \begin{bmatrix} 11 \\ 13 \\ 18 \end{bmatrix} = \text{LNS}$$

Thực hiện đầy đủ với từng cụm 3 ký tự ta thu được bản mã 'LNSHDLEWMTRW'

CHƯƠNG 2: CÁC KHÁI NIỆM CƠ SỞ VÀ HỆ MẬT MÃ CỔ ĐIỂN

2.4. Các hệ mã hóa cổ điển

2.4.5. Mã Hill

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Để giải mã chúng ta có công thức:

$$K^{-1}C \bmod 26 = K^{-1}KP \bmod 26 = P$$

$$K^{-1} = \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix}$$

Vì:

$$\begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix} \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} = \begin{bmatrix} 443 & 442 & 442 \\ 858 & 495 & 780 \\ 494 & 52 & 365 \end{bmatrix} \bmod 26 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

CHƯƠNG 2: CÁC KHÁI NIỆM CƠ SỞ VÀ HỆ MẬT MÃ CỔ ĐIỂN

2.4. Các hệ mã hóa cổ điển

2.4.5. Mã Vigenere

- Dòng thứ k của bảng là một mã hóa Caesar k-1 vị trí

Ví dụ: 'We are discovered save yourself'

Với khóa K = 'DECEPTIVE'

plaintext: wearediscoveredsaveyourself
key: DECEPTIVEDECEPTIVEDECEPTIVE
ciphertext: ZICVTWQNGRZGVTWAVZHCQYGLMGJ

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

CHƯƠNG 2: CÁC KHÁI NIỆM CƠ SỞ VÀ HỆ MẬT MÃ CỔ ĐIỂN

2.4.6. Mã One-time pad

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

	H	E	L	L	O	message
	7 (H)	4 (E)	11 (L)	11 (L)	14 (O)	message
+	23 (X)	12 (M)	2 (C)	10 (K)	11 (L)	key
=	30	16	13	21	25	message + key
=	4 (E)	16 (Q)	13 (N)	21 (V)	25 (Z)	(message + key) mod 26
	E	Q	N	V	Z	→ ciphertext

	E	Q	N	V	Z	ciphertext
	4 (E)	16 (Q)	13 (N)	21 (V)	25 (Z)	ciphertext
-	23 (X)	12 (M)	2 (C)	10 (K)	11 (L)	key
=	-19	4	11	11	14	ciphertext - key
=	7 (H)	4 (E)	11 (L)	11 (L)	14 (O)	ciphertext - key (mod 26)
	H	E	L	L	O	→ message

CHƯƠNG 2: CÁC KHÁI NIỆM CƠ SỞ VÀ HỆ MẬT MÃ CỔ ĐIỂN

2.4.6. Mã One-time pad

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Ví dụ mã hóa bản tin ‘*wearediscoveredsaveyourself*’

Bản tin P: wearediscoveredsaveyourself

Khóa K_1 : FHWYKLVKVKXCVKDJFSAPXZCVP

Bản mã C: BLWPOODEMJFBTZNVJNJQOJORGGU

Trường hợp 1: Bản mã C: BLWPOODEMJFBTZNJVJNJQOJORGGU

Khóa K_2 : IESRLKBWJFCIFZUCJLZXAXAAPSY

Bản giải mã: theydecidedtoattacktomorrow
(*they decided to attack tomorrow*)

CHƯƠNG 2: CÁC KHÁI NIỆM CƠ SỞ VÀ HỆ MẬT MÃ CỔ ĐIỂN

2.4.6. Mã One-time pad (OTP)

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Ví dụ mã hóa bản tin ‘*wearediscoveredsaveyourself*’

Bản tin P : *wearediscoveredsaveyourself*

Khóa K_1 : FHWYKLVKVKXCVDJSFSAPXZCVP

Bản mã C : BLWPOODEMJFBTZNJVJNJQOJORGGU

Trường hợp 2: Bản mã C : BLWPOODEMJFBTZNJVJNJQOJORGGU

Khóa K_3 : FHAHDDRAIQFIASJGJWQSVVBJAZB

Bản giải mã: *wewillmeetatthepartytonight*

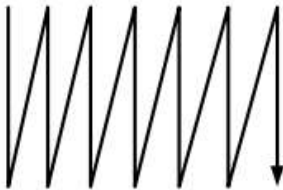
(*we will meet at the party tonight*)

CHƯƠNG 2: CÁC KHÁI NIỆM CƠ SỞ VÀ HỆ MẬT MÃ CỔ ĐIỂN

2.4.7. Biến thể của mã hoán vị (Permutation Cipher)

Ví dụ: Cho bản rõ 'attackpostponeduntilthisnoon'

a	t	t	a	c	k	p
o	s	t	p	o	n	e
d	u	n	t	i	l	t
h	i	s	n	o	o	n



Bản mã:

'AODHTSUITTNSAPTNCIOIKNLOPETN'

Có thể hoán vị các cột trước khi kết xuất bản mã:

M	O	N	A	R	C	H
a	t	t	a	c	k	p
o	s	t	p	o	n	e
d	u	n	t	i	l	t
h	i	s	n	o	o	n

→

A	C	H	M	N	O	R
a	k	p	a	t	t	c
p	n	e	o	t	s	o
t	l	t	d	n	u	i
n	o	n	h	s	i	o

CHƯƠNG 2: CÁC KHÁI NIỆM CƠ SỞ VÀ HỆ MẬT MÃ CỔ ĐIỂN

2.5. Các phương thức thám mã các hệ mã cổ điển

Có 2 phương thức mã hoá cổ điển:

- thay thế một chữ cái trong bản rõ thành một chữ cái khác trong bản mã (**substitution**):
mã hóa Ceasar, mã hóa thay thế đơn bảng, đa bảng, one-time pad
- dùng phương thức hoán vị để thay đổi thứ tự ban đầu của các chữ cái trong bản rõ (**permutation**)

Một số phương thức thám mã:

- Chỉ biết bản mã (**ciphertext-only attack**)
- Biết một số cặp bản rõ – bản mã (**known-plaintext attack**)
- Một số cặp bản rõ – bản được lựa chọn (**chosen-plaintext attack**)