

# **CHƯƠNG 2**

# **CÁC HỆ MÃ ĐỐI XỨNG**

---

# Một số khái niệm

---

- ❖ **Bản rõ – PlainText** ( $X$ ) được gọi là văn bản gốc. Bản rõ có thể được chia nhỏ có kích thước phù hợp.
- ❖ **Bản mã – CipherText** ( $Y$ ) là bản tin gốc đã được mã hoá.
- ❖ **Mã** là thuật toán ( $E$ ) chuyển **bản rõ** thành **bản mã**.

# Một số khái niệm

---

- ❖ **Khoá** (K) là thông tin tham số dùng để mã hoá, chỉ có người gửi và người nhận biết. Khoa là độc lập với bản rõ và có độ dài phù hợp với yêu cầu bảo mật.
- ❖ **Mã hoá** là quá trình chuyển bản rõ thành bản mã, thông thường bao gồm việc áp dụng thuật toán mã hóa và một số quá trình xử lý thông tin kèm theo.
- ❖ **Giải mã** chuyển bản mã thành bản rõ, đây là quá trình ngược lại của mã hóa.

# Một số khái niệm

---

- ❖ **Mật mã học** là chuyên ngành khoa học của Khoa học máy tính nghiên cứu về các nguyên lý và phương pháp mã hóa. Hiện nay người ta đưa ra nhiều chuẩn an toàn cho các lĩnh vực khác nhau của công nghệ thông tin.

# Một số khái niệm

---

- ❖ **Thám mã** nghiên cứu các nguyên lý và phương pháp giải mã thường là không biết khóa. Thông thường khi đưa các mã mạnh ra làm chuẩn phổ biến công khai các mã đó được các kẻ thám mã cũng như những người phát triển mã tìm hiểu nghiên cứu.

# Một số khái niệm

---

- ❖ **Lý thuyết mã** bao gồm cả **mật mã** và **thám mã** để đánh giá một mã mạnh hay không.

# Giải thuật mật mã hóa

---

## ❖ Các hệ mật mã hóa

- Kiểu của các thao tác được dùng để biến đổi bản rõ thành bản mật: tất cả các giải thuật mã hóa đều dựa trên 2 nguyên lý
  - **Thay thế (substitution)**: mỗi thành phần trong bản rõ được ánh xạ đến thành phần khác.
  - **Chuyển vị (transposition)**: các thành phần trong bản rõ được sắp xếp lại.

# Giải thuật mật mã hóa

---

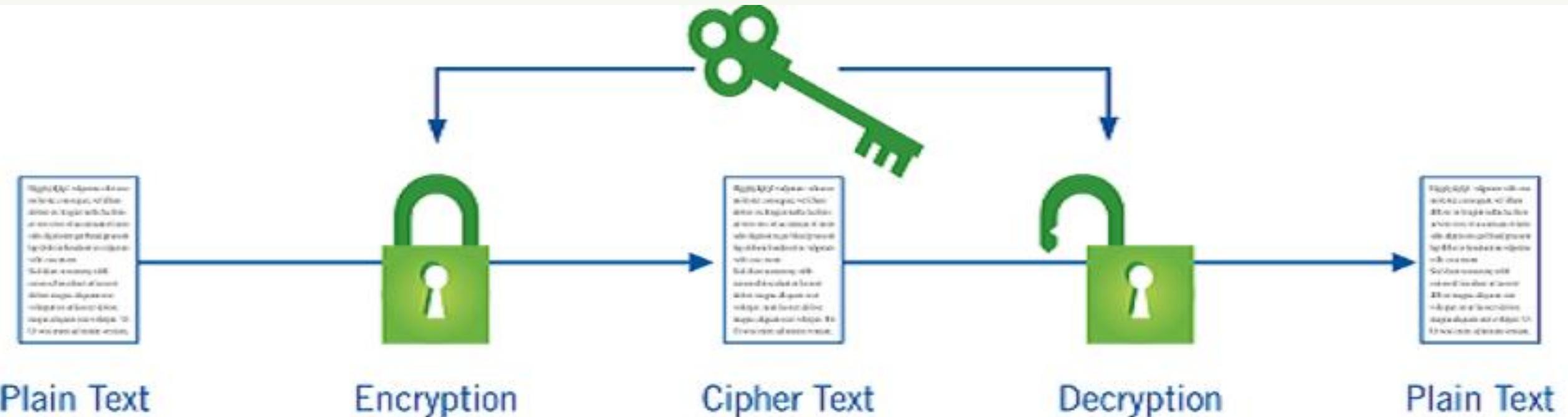
=> **Yêu cầu cơ bản:** thông tin không bị mất

=> Phần lớn các hệ mã kết hợp cả 2 nguyên lý qua nhiều bước.

❖ Số khóa được sử dụng:

- 1 Khóa: người gửi và người nhận sử dụng chung khóa
- 2 Khóa: Khóa bí mật/Khóa công khai
  - Mã hóa dùng 1 khóa và giải mã dùng 1 khóa khác

# Mô hình mã đổi xứng



# Các hệ mã khóa bí mật

---

❖ Các hệ mã khóa bí mật bao gồm:

- Các hệ mật mã cổ điển
- Các hệ mật hiện đại (mã hóa khối)



# Hệ mật mã cổ điển

---

## ❖ Kỹ thuật thay thế

- Mật mã Ceasar
- Mật mã Playfair
- Mật mã Hill
- Mật mã Vigenère

## ❖ Kỹ thuật hoán vị

- Mật mã rail fence
- Kỹ thuật hoán vị nâng cao

# Mật mã Ceasar

---

- ❖ Thế kỷ thứ 3 trước công nguyên, nhà quân sự La Mã Julius Ceasar đưa ra phương pháp mã hóa một bản tin như sau:
  - Thay thế mỗi chữ trong bản tin bằng chữ đứng sau nó k vị trí trong bảng chữ cái.
  - Giả sử chọn  $k = 3$ , ta có bảng chuyển đổi như sau:

<b>Chữ ban đầu</b>	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>Chữ thay thế</b>	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

# Mã hóa Ceasar

---

- ❖ Về toán học, nếu ta gán số thứ tự cho mỗi chữ trong bảng chữ cái. Các chữ ở dòng trên có số thứ tự tương ứng là số ở dòng dưới:

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

# Mã hóa Ceasar

---

- ❖ Mã Ceasar được định nghĩa qua phép tịnh tiến các chữ như sau:

$$c = E(p) = (p + k) \bmod 26$$

$$p = D(c) = (c - k) \bmod 26$$

- ❖ Với:
  - p, c là số thứ tự của ký tự trong bảng chữ cái
  - k là khoá của mã Ceasar
  - E() hàm mã hóa, D() hàm giải mã

# Mã hóa Ceasar

---

- ❖ Bài tập, mã các đoạn văn bản sau:
  - **PHAT TRIEN BAN THAN GIUP ICH GIA DINH VA XA HOI.** Với K = 9, 121
  - **HOC TAP NANG DONG PHAT TRIEN TU DUY.** Với K = 10, 36
  - **DAY MANH TU HOC GOP PHAN PHAT TRIEN BAN THAN.** Với K = 2, 131

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

# Mã hóa Ceasar

---

- ❖ Có 26 giá trị khác nhau của k, nên có 26 khoá khác nhau. Thực tế độ dài khoá ở đây chỉ là 1, vì mọi ký tự đều tịnh tiến đi một khoảng như nhau.

# Mã hóa Ceasar

---

## ❖ Ví dụ giải mã: k=3

- PHHW PH DIWHU WKH WRJD SDUWB
- MEET ME AFTER THE TOGA PARTY

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

# Mã hóa Ceasar

---

❖ Bài tập, giải mã các đoạn văn sau:

- **AVP TBVU AYV AOHUO UNBVP AOHUO KHA.** Với  $K = 7$
- **AUI SU YK INGV IGTN INU ZNGTN IUTM.** Với  $K = 32$
- **RJDR HDCV IWPI CVPC CVJX CTC WPN IGPC**

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

# Mã hóa Ceasar

---

- ❖ Ngày nay phương pháp mã hóa của Ceasar không được xem là an toàn. Giả sử đối thủ của Ceasar có được bản mã “**phhw ph diwhu wkh wrjd sduwb**” và biết được phương pháp mã hóa và giải mã là phép cộng trừ modulo 26

# Mã hóa Ceasar

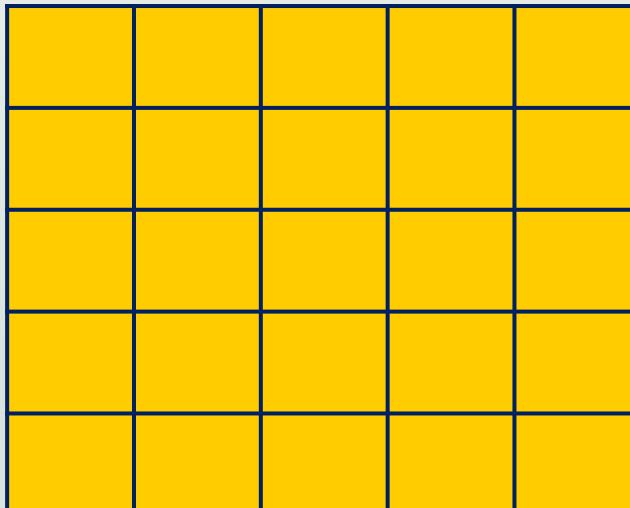
- ❖ Đối thủ có thể thử tất cả 25 trường hợp của k như sau:
- ❖ Người phá mã có thể thử được hết tất cả các trường hợp của khóa rất nhanh chóng.
- ❖ Phương pháp tấn công này được gọi là phương pháp vét cạn khóa (brute-force attack)

KEY	PHHW	PH	DIWHU	WKH	WRJD	SDUWB
1	oggv	og	chvgt	vjg	vqic	rctva
2	nffu	nf	bgufs	uif	uphb	qbsuz
3	meet	me	after	the	toga	party
4	ldds	ld	zesdq	sgd	snfz	ozqsx
5	kccr	kc	ydrccp	rfc	rmey	nyprw
6	jbbq	jb	xcqbo	qeb	qldx	mxoqv
7	iaap	ia	wbpan	pda	pkcw	lwnpu
8	hzzo	hz	vaozm	ocz	ojbv	kvmot
9	gyyn	gy	uznyl	nby	niau	julns
10	fxxm	fx	tymxk	max	mhzt	itkmr
11	ewwl	ew	sxlwj	lzw	lgys	hsjlq
12	dvvk	dv	rwkvi	kyv	kfxr	grikp
13	cuuj	cu	qvjuh	jxu	jewq	fqhjo
14	btti	bt	puitg	iwt	idvp	epgin
15	assh	as	othsf	hvs	hcuo	dofhm
16	zrrg	zr	nsgre	gur	gbtn	cnegl
17	yqqf	yq	mrfqd	ftq	fasm	bmdfk
18	xppe	xp	lqepec	esp	ezrl	alcej
19	wood	wo	kpdob	dro	dyqk	zkbdij
20	vnnc	vn	jocna	cqn	cxpj	yjach
21	ummb	um	inbmz	bpm	bwoi	xizbg
22	tlla	tl	hmaly	aol	avnh	whyaf
23	skkz	sk	glzkx	znk	zumg	vgxze
24	rjyj	rj	fkyjw	ymj	ytlf	ufwyd
25	qiix	qi	ejxiv	xli	xske	tevxc

# Mã Playfair

---

- ❖ Mật mã đa ký tự (mỗi lần mã hóa 2 ký tự liên tiếp nhau)
- ❖ Giải thuật dựa trên một ma trận các chữ cái  $5 \times 5$  được xây dựng từ một khóa (chuỗi các ký tự)



# Mã Playfair

---

- ❖ 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 không được trùng nhau
- ❖ Mật mã hóa
- ❖ Giải mật mã

# Mã Playfair

---

- ❖ Ví dụ: với từ khóa “playfair example”
  - Ma trận khóa

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

# Mã Playfair

---

## ❖ Giải thuật mật mã hóa

- Mã hóa từng cặp “**2 ký tự**” liên tiếp nhau.
- Nếu 2 ký tự này giống nhau thì thêm một ký tự ‘**x**’ hoặc ‘**z**’ vào giữa.
  - VD: **balloon** tách thành **ba lx lo on** (vì *ll* -> *lx l*)
- Nếu dư 1 ký tự thì thêm vào ký tự ‘**q**’ vào cuối.
  - VD: **hat** => **ha tq**

# Mã Playfair

---

- ❖ Giả sử sử dụng từ khoá MORNACHY. 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

# Mã Playfair

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

❖ **Việc mã hóa từng cặp được thực hiện theo quy tắc:**

- Nếu hai ký tự trong cặp thuộc cùng một hàng, thì được thay bằng hai ký tự tiếp theo trong hàng. Nếu đến cuối hàng thì quay về đầu hàng.
- Ví dụ cặp **AR** được mã hóa thành **RM**.

# Mã Playfair

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

❖ **Việc mã hóa từng cặp được thực hiện theo quy tắc:**

- Nếu hai ký tự trong cặp thuộc cùng một cột, thì được thay bằng hai ký tự tiếp theo trong cột. Nếu đến cuối cột thì quay về đầu cột.
- Ví dụ cặp **OV** được mã hóa thành **HO**.

# Mã Playfair

---

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

- ❖ Trong các trường hợp còn lại, hai ký tự được mã hóa sẽ tạo thành đường chéo của một hình chữ nhật và được thay bằng 2 ký tự trên đường chéo kia.
- ❖ Ví dụ: **HS** trở thành **BP** (B cùng dòng với H và P cùng dòng với S); EA trở thành IM (hoặc JM)

**Người ta tin rằng mã hóa Playfair không thể bị phá và được quân đội Anh sử dụng trong chiến tranh thế giới lần thứ nhất.**

# Mã Playfair

---

❖ Mã hóa văn bản sau:

➤ Bài 1:

- **BAO MAT THONG DIEP O CAN THO**
- Mật khẩu: **CANTHO**

➤ Bài 2:

- **THONG TIN SINH VIEN LUON DUOC BAO MAT**
- Mật khẩu: **SINHVIEN**

# Mã Playfair

---

- ❖ Giải thuật giải mã playfair
  - Giải mã từng cặp “**2 ký tự**” liên tiếp nhau.
  - **Không** thêm hoặc bớt ký tự

# Mã Playfair

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

❖ **Việc giải mã từng cặp được thực hiện theo quy tắc:**

- Nếu hai ký tự trong cặp thuộc cùng một hàng, thì được thay bằng hai ký tự ở trước trong hàng. Nếu ở đầu hàng thì quay về cuối hàng.
- Ví dụ cặp **RM** được giải mã thành **AR**.

# Mã Playfair

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

❖ **Việc giải mã từng cặp được thực hiện theo quy tắc:**

- Nếu hai ký tự trong cặp thuộc cùng một cột, thì được thay bằng hai ký tự ở trên trong cột. Nếu đến đầu cột thì quay về cuối cột.
- Ví dụ cặp **NW** được mã hóa thành **wQ**.

# Mã Playfair

---

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

- ❖ Trong các trường hợp còn lại, hai ký tự được giải mã sẽ tạo thành đường chéo của một hình chữ nhật và được thay bằng 2 ký tự trên đường chéo kia.
- ❖ Ví dụ: **HS** trở thành **BP** (B cùng dòng với H và P cùng dòng với S); EA trở thành IM (hoặc JM)

# Mã Playfair

---

- ❖ Giải mã:
  - Cipher Text: **FC NP TW RB IC EO SH BN UK UR GR UK  
IB ON IG**
  - Khóa: BAUTROI

# Mật mã Hill

---

- ❖ Giải thuật sử dụng m ký tự liên tiếp của bản rõ và thay thế m ký tự khác trong bản mã.
- ❖ Việc thay thế được thực hiện bởi một phương trình tuyến tính trên các ký tự được gán trị ( $a=0, b=1, c=2\dots$ ),  $m=3$ :

# Mật mã Hill

---

- $$\begin{pmatrix} c1 \\ c2 \\ c3 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \begin{pmatrix} p1 \\ p2 \\ p3 \end{pmatrix} \text{ mod } 26$$
- $C = KP \text{ mod } 26$
- ❖ Giải mã
- $P = K^{-1}C \text{ mod } 26$

# Mật mã Hill

---

❖ Mật mã hóa bản rõ sau:

➤ **pay more money**

❖ Với ma trận khóa:

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

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

# Mật mã Hill

---

- ❖ Tìm ma trận nghịch đảo của ma trận khóa K
  - Sử dụng phương pháp tìm ma trận nghịch đảo của đại số tuyến tính
  - Viết ma trận khóa K và ma trận đơn vị I cạnh nhau
    - $$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
  - Áp dụng các phép biến đổi tuyến tính lên cả hai ma trận K và I để biến K thành I. Khi đó I sẽ thành  $K^{-1}$ .

# Mật mã Hill

---

- ❖ Mật mã hóa bản rõ sau:
  - **pay more money**
- ❖ Với ma trận khóa:
  - $K = \begin{pmatrix} 3 & -4 & 5 \\ 1 & -5 & 2 \\ 2 & -2 & 1 \end{pmatrix}$
- ❖ Sau đó áp dụng thuật toán giải mã đoạn ký tự vừa được mã hóa

# Mã hóa thay thế đa bảng

---

## ❖ Mã hóa thay thế đa bảng - Polyalphabetic Substitution Cipher:

- Với sự phát hiện ra quy luật phân bố tần suất, các nhà phá mã đang tạm thời chiếm ưu thế trong cuộc chiến mã hóa-phá mã.
- Cho đến thế kỷ thứ 15, một nhà ngoại giao người Pháp tên là Vigenère đã tìm ra phương án mã hóa thay thế đa bảng. Phương pháp Vigenère dựa trên bảng sau đây

# Bảng tra cứu mã hóa và giả mã

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

# Mã hóa thay thế đa bảng

---

## ❖ Thuật toán

- Sao chép, ghép nội dung khóa sao cho chiều dài khóa bằng với chiều dài bản rõ cần mã hóa.
- Tách từng ký tự trong khóa và từng ký tự trong bản rõ rồi tra cứu trong bảng, giao giữa hàng và cột ta được ký tự đã được mã hóa

❖ Ví dụ mã hóa  
bản tin là “We  
**are**  
**discovered,**  
**save**  
**yourself”**

- Khóa:  
**DECEPTIVE**
- Bản mã: **ZI**  
**CVT**  
**WQNGRZGVT**  
**WAVZH**  
**CQYGLMGJ**

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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	

❖ Mã hóa  
các câu  
sau:

**CHUNG TA  
LA NGUOI  
MOT NHA**

Khóa:

**PHAIKHONG**

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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	

# Mã hóa thay thế đa bảng

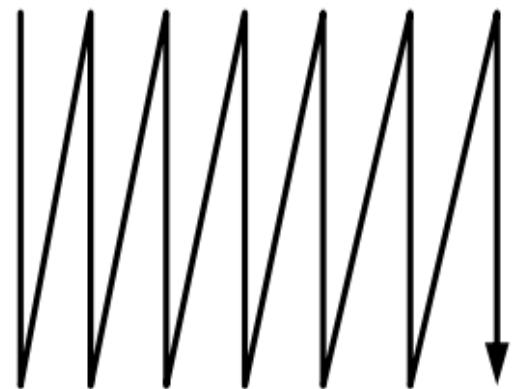
---

- ❖ Trong 3 thế kỷ sau đó mã hóa Vigenère được xem là mã hóa không thể bị phá và được biết dưới cái tên “le chiffre indechiffrable” (mật mã không thể破解 nổi). Các nhà mã hóa lại chiếm ưu thế trở lại so với người破解 mã.
- ❖ Đến thế kỷ 19, nhà khoa học người Anh Charles Babbage, đã tìm ra cách破解 mã Vigenère

# Mã hoán vị (Permutation Cipher)

- ❖ Một cách thực hiện đơn giản là ghi bản rõ theo từng hàng, sau đó kết xuất bản mã dựa trên các cột. Ví dụ bản rõ “attackpostponeduntilthisnoon” được viết lại thành bảng  $4 \times 7$  như sau:

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



“AODHTSUITTNSAPTNCOIOKNLOPETN”

# Mã hoán vị (Permutation Cipher)

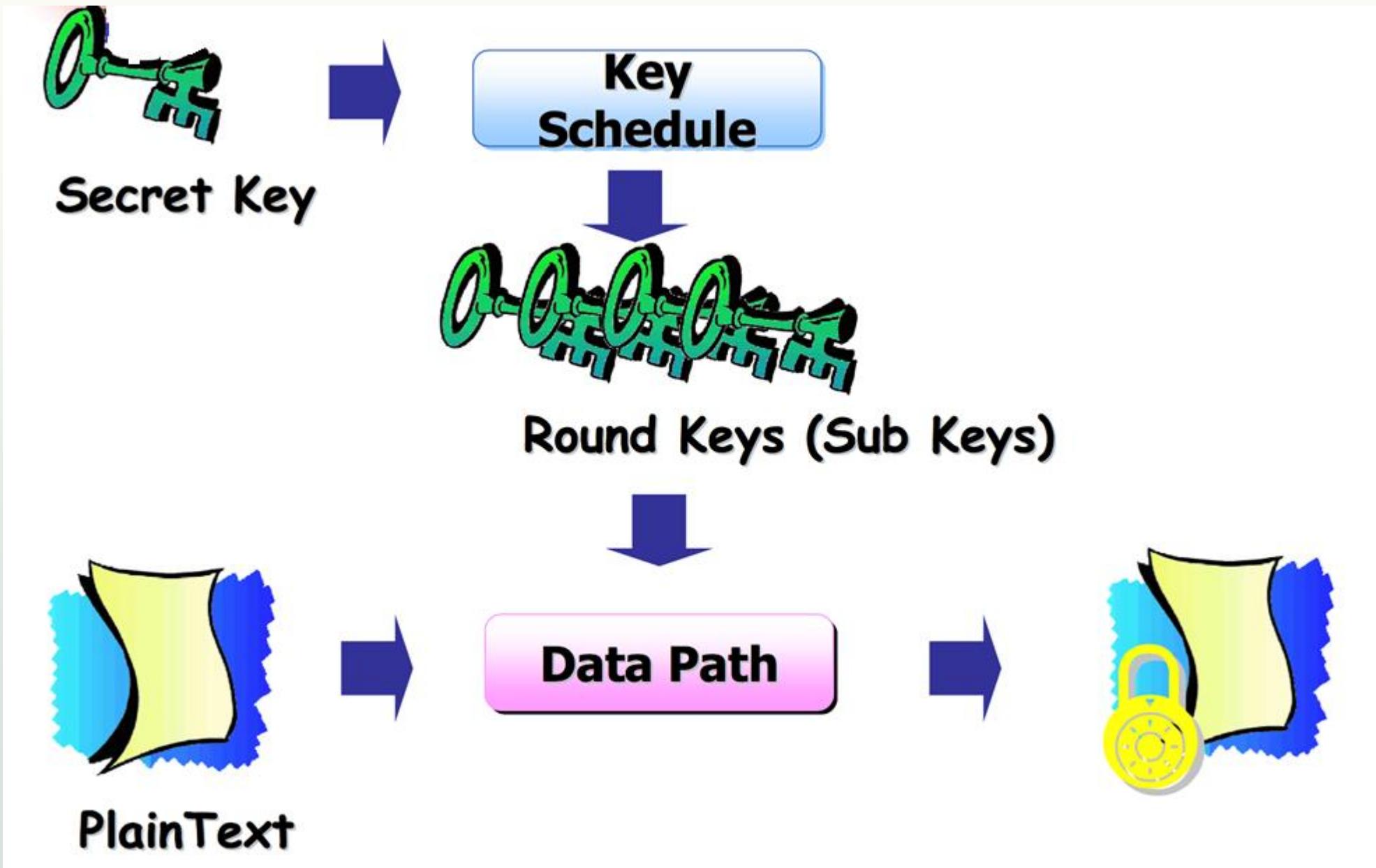
---

- ❖ Mã hóa các đoạn văn bản bằng mã hóa hoán vị
  - **KHI KHONG GIOI THI PHAI CO GANG**
  - **THANH CONG DIEU DUA TREN NO LUC BAN THAN**
  - **TAT CA MOI THU DIEU PHAI DO TU MINH NAM LAY**

# Mã hóa khối (Mã hóa hiện đại)

---

# Quy trình mã hóa theo khối



# Quy trình mã hóa theo khối

---

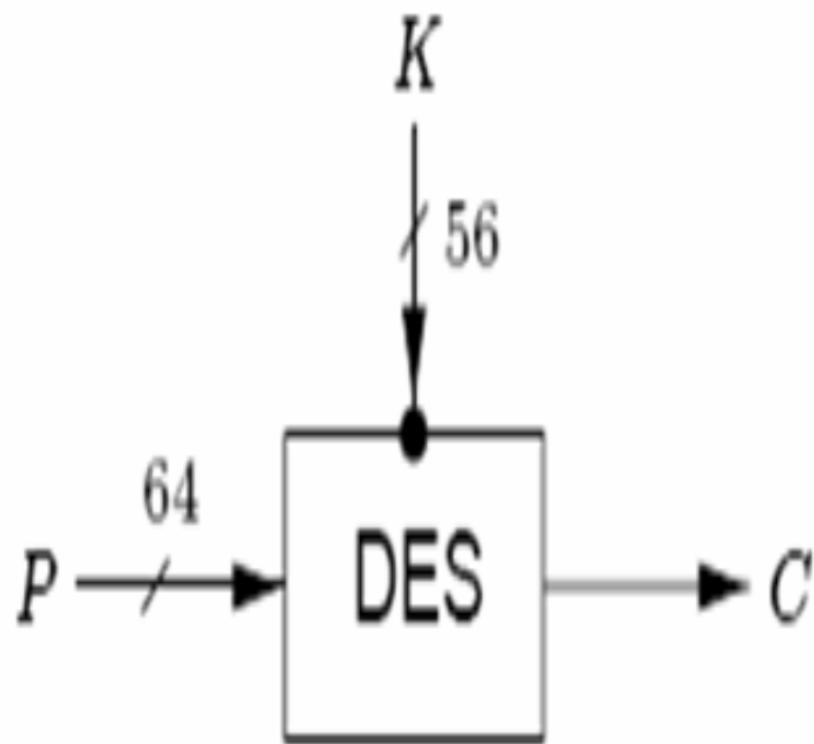
- ❖ **Data Path:** Thông thường, quy trình mã hóa bao gồm nhiều chu kỳ mã hóa (**round**) liên tiếp nhau; mỗi chu kỳ gồm nhiều thao tác mã hóa
- ❖ **Key Schedule:** Từ khóa gốc (**secret key**), phát sinh (có quy luật) các giá trị khóa sẽ được sử dụng trong mỗi chu kỳ mã hóa (**round key**)

# Mã hóa theo khối

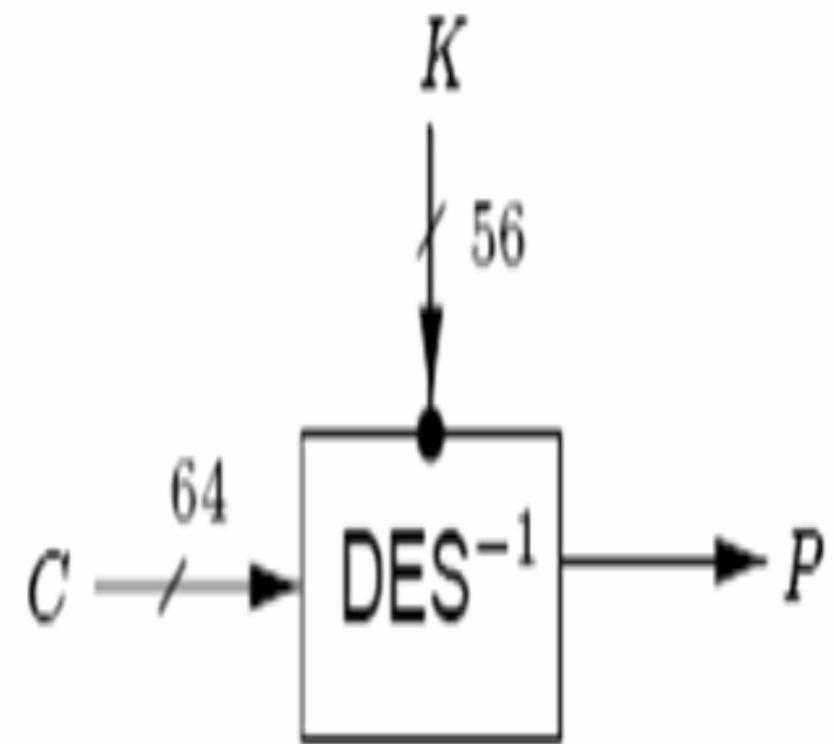
---

- ❖ Ý tưởng: mã hóa tích
  - Key: **56 bit**
  - Block: **64 bit**
- ❖ Được IBM phát triển từ phương pháp Lucifer
- ❖ Chính thức công bố năm 1975
- ❖ Được chọn là Chuẩn xử lý thông tin liên bang (Federal Information Processing Standard - FIPS) năm 1976

# Mã hóa theo khối



plaintext  $P$   
ciphertext  $C$   
key  $K$



*DES input-output.*

# Thuật toán DES

---

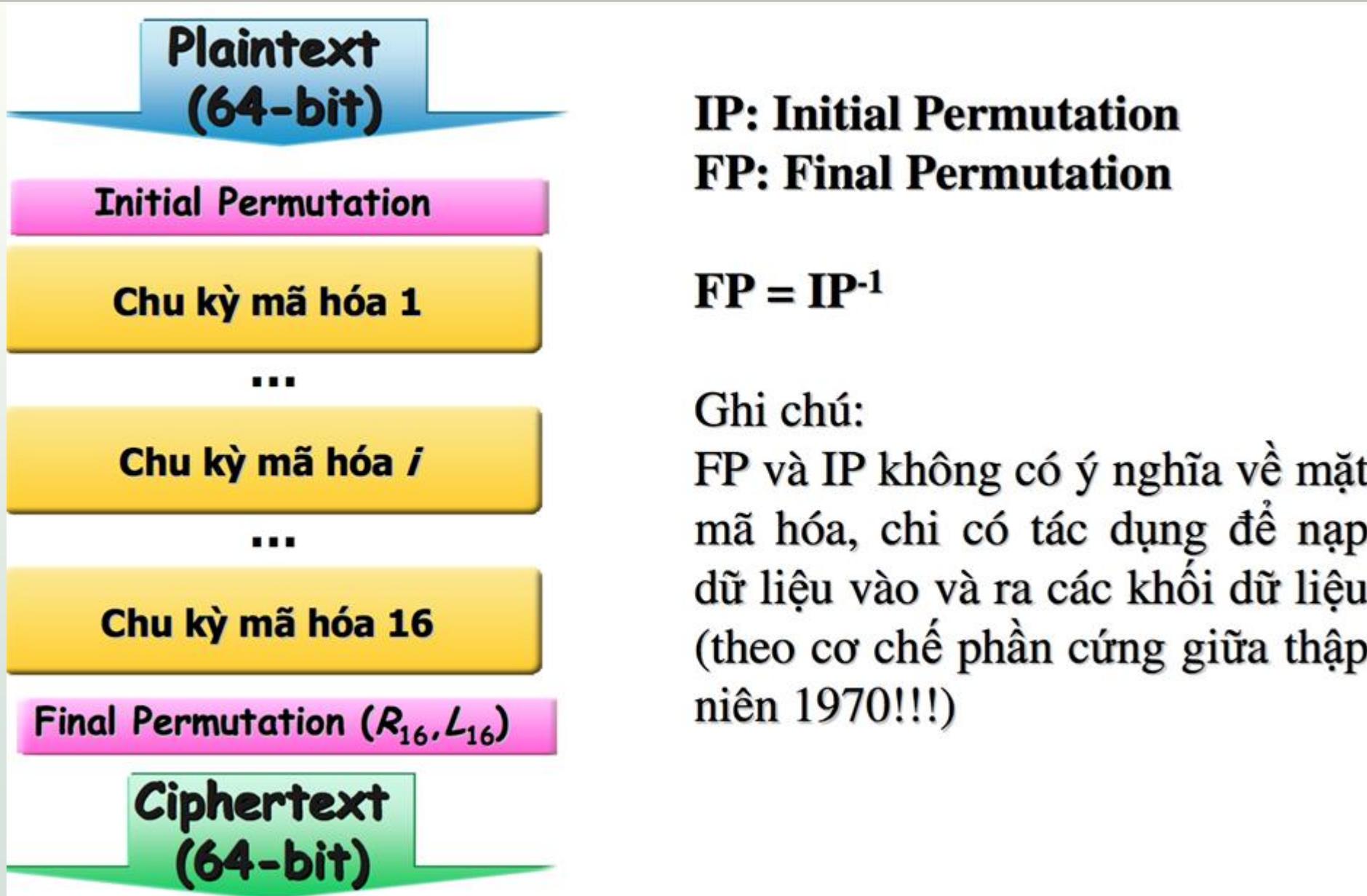
- ❖ Về mặt khái niệm DES là thuật toán mở, nghĩa là mọi người đều biết thuật toán này.
- ❖ Tuy nhiên chìa khoá của DES có độ dài tới **56 bit**, nghĩa là số lần thử tối đa để tìm được chìa khoá lên đến  $2^{56}$ , trung bình là  **$2^{55} = 36.028.797.018.963.968$**  lần, một con số rất lớn
- ❖ DES được thực hiện nhờ các phép dịch, hoán vị và các phép toán logic trên các bit

# Quy trình của thuật toán DES

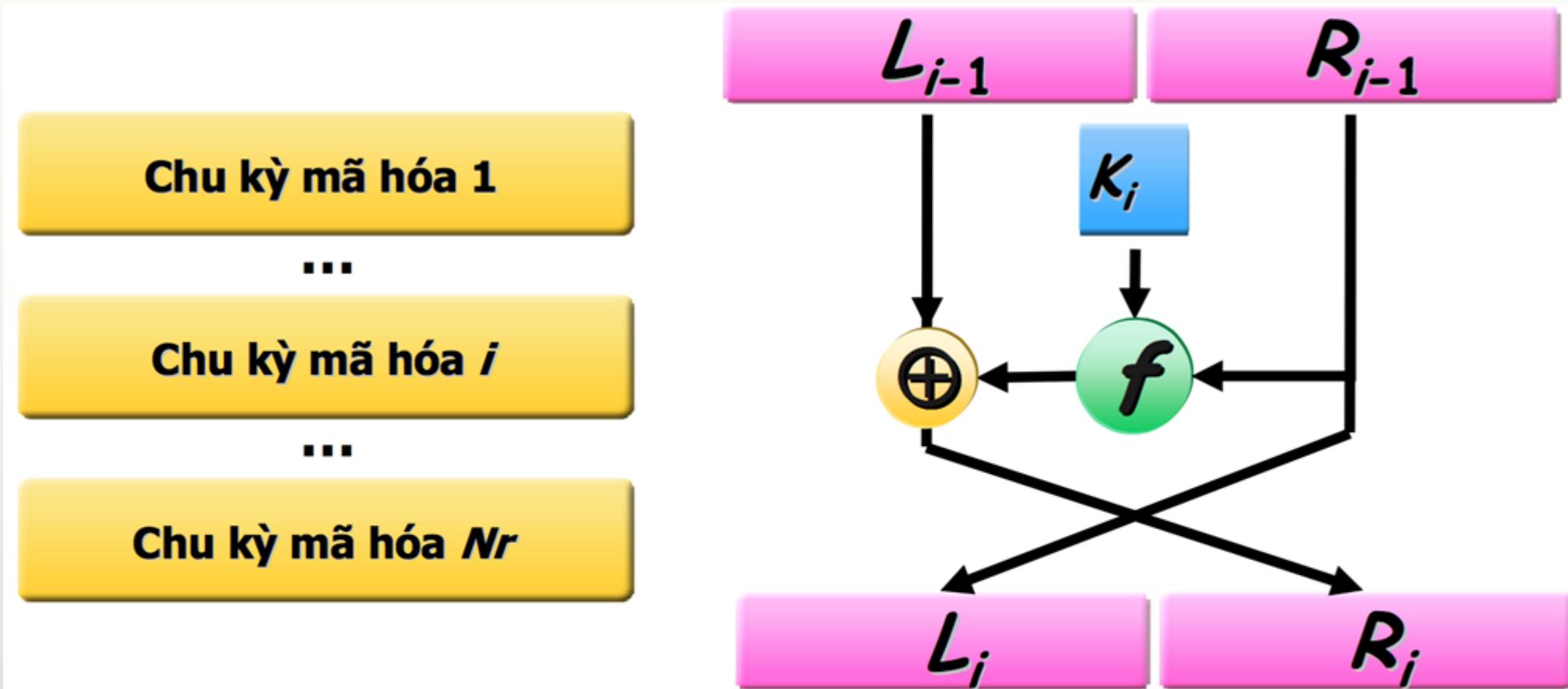
---

- ❖ DES nhận vào một thông điệp  $M$  64 bit, một khóa  $K$  56 bit và cho ra một bảng mã  $C$  64 bit.
  - **Bước 1:** áp dụng một phép hoán vị bit khởi tạo IP (Initial Permutation) vào  $M$  cho ra  $M'$ :  $M' \leftarrow IP(M)$ .
  - **Bước 2:** chia  $M'$  thành hai phần: nửa trái  $L_0 = 32$  bit và nửa phải  $R_0 = 32$  bit.
  - **Bước 3:** thực hiện các phép toán sau với  $i = 1, 2, \dots, 16$  (có 16 vòng).
    - $L_i = R_{i-1}$
    - $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$
  - **Bước 4:** Hoán vị với phép hoán vị  $IP^{-1}$  để được bản mã cuối cùng  $C$ .

# Quy trình của thuật toán DES



# Quy trình của thuật toán DES



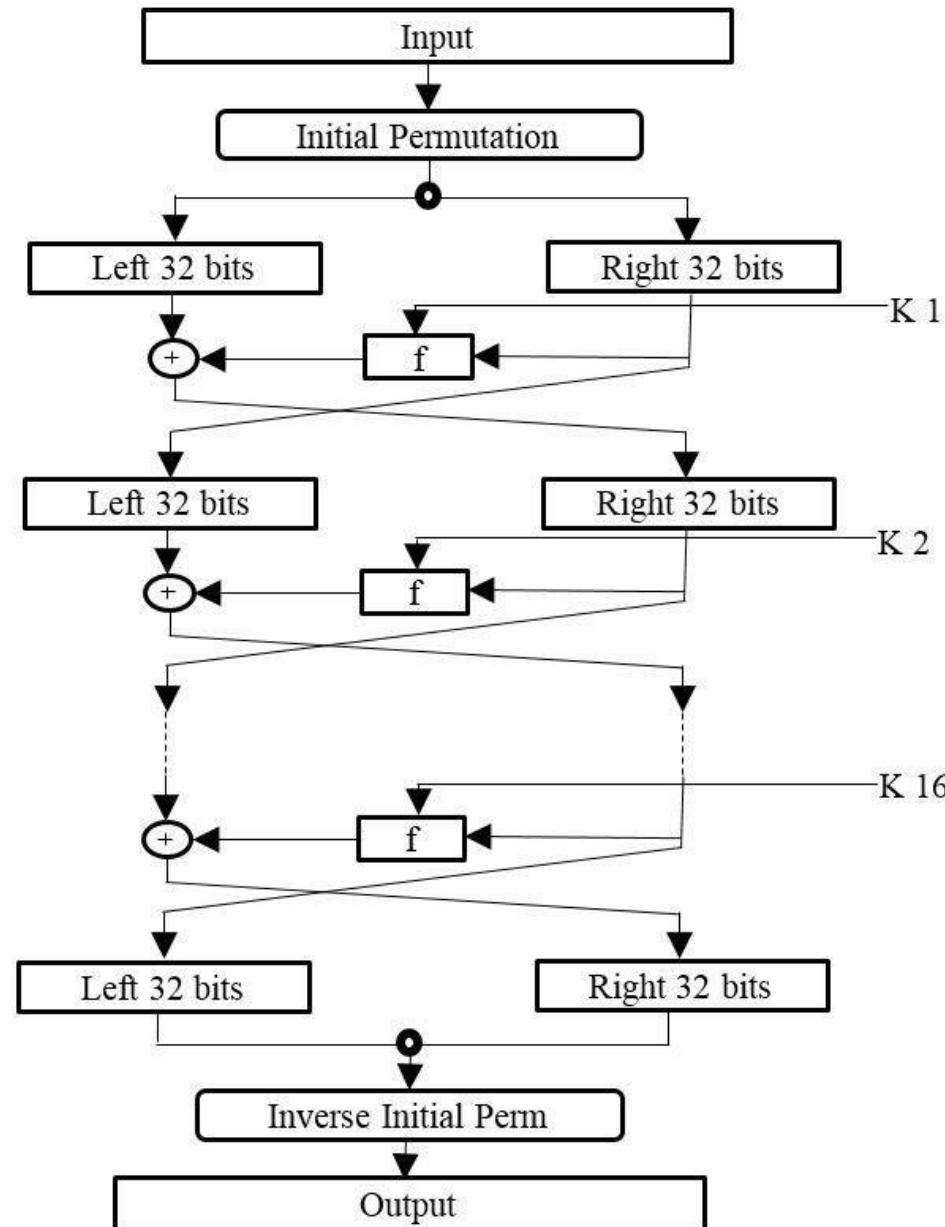
$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

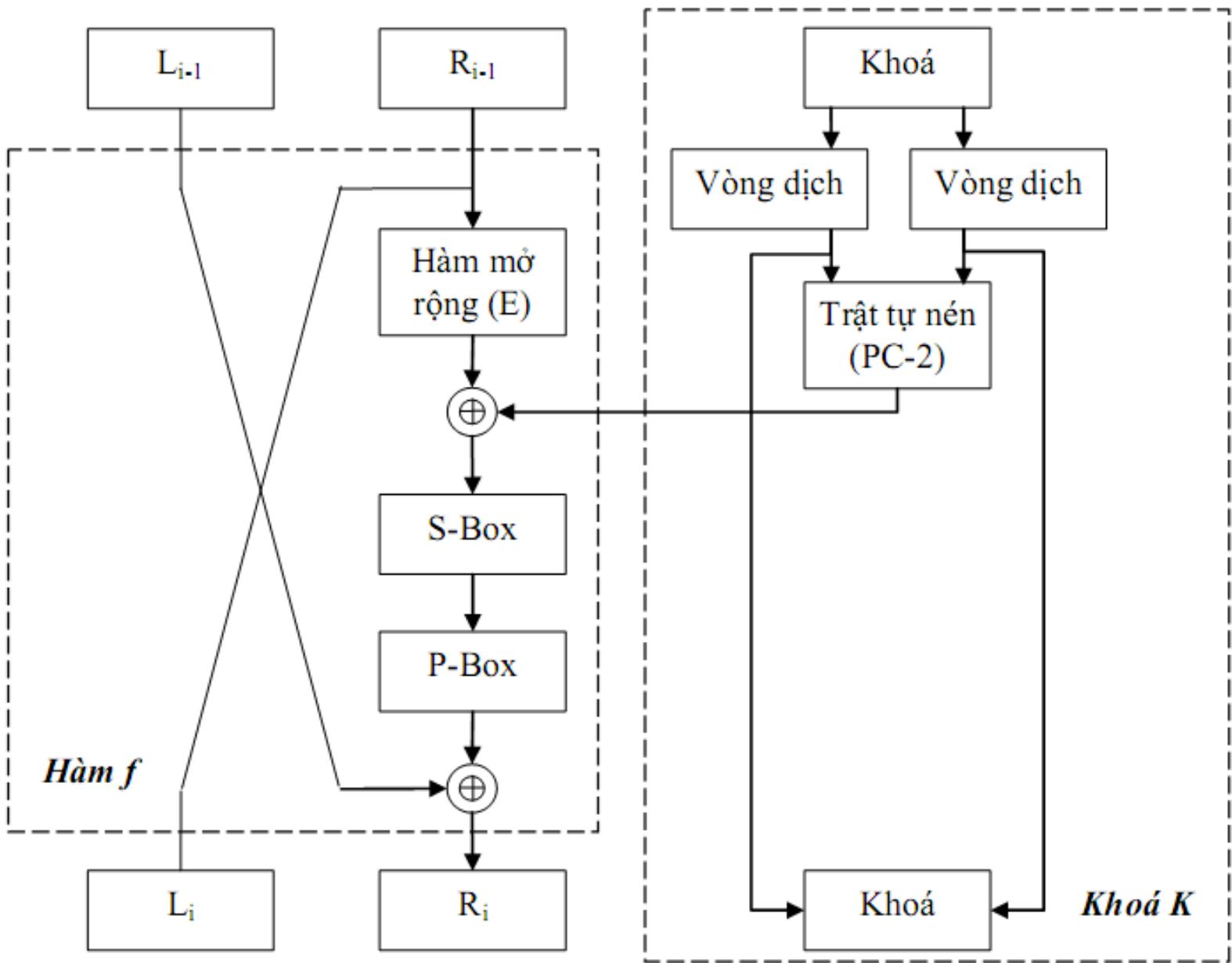
# Quy trình của thuật toán DES

IP							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

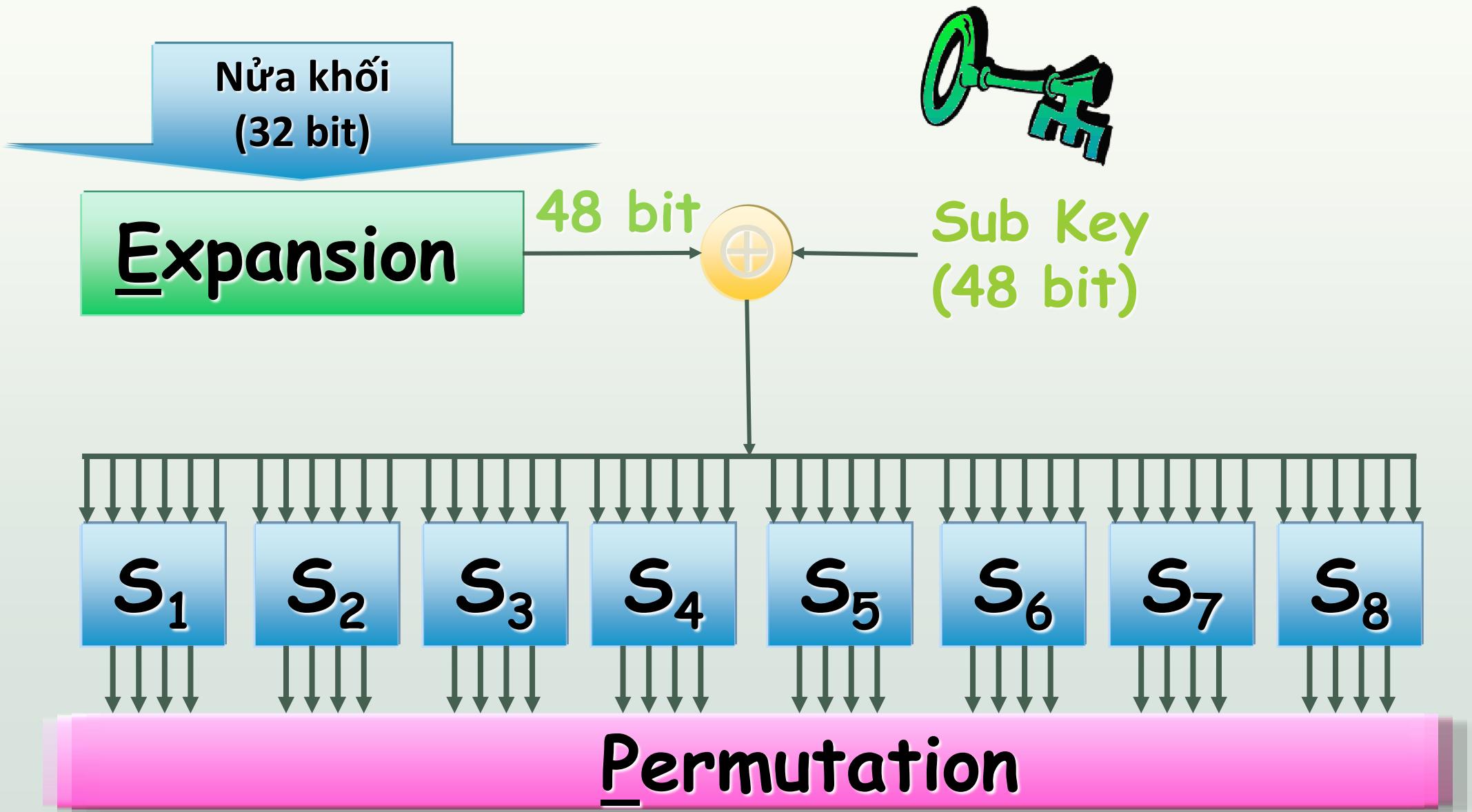
# Quy trình của thuật toán DES



# Quy trình của thuật toán DES



# Hàm f trong DES



# Expansion

Bảng E: quy tắc mở rộng từ 32 bit thành 48 bit

Bảng chọn lựa bit E					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

# S-box

<b>S<sub>1</sub></b>															
14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

<b>S<sub>2</sub></b>															
15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

Ví dụ:  $B_j = b_1 b_2 b_3 b_4 b_5 b_6$  thì  $S_j(B_j) = S_j[b_1 b_6][b_2 b_3 b_4 b_5]$

# S-box

$S_3$															
10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

$S_4$															
7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

# S-box

$S_5$

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

$S_6$

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

# S-box

<b>S<sub>7</sub></b>															
4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

<b>S<sub>8</sub></b>															
13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

# Bảng hoán vị P

P			
16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

# Key Schedule

---

- ❖ Thực tế, K là một dãy 64 bits trong đó có 56 bits làm khóa và 8 bits dùng để kiểm tra lỗi (Kiểm tra chẵn lẻ).
- ❖ Các bit nằm ở vị trí 8, 16, 24 ... 64 là các bit dùng để kiểm tra chẵn lẻ.
- ❖ Cho một khóa K 64 bits, ta sẽ bỏ các bit kiểm tra chẵn lẻ ta sẽ được 56 bits khóa.
- ❖ Cho 56 bit này hoán vị theo bảng hoán vị PC-1.
  - Ta có:  $PC-1(K) = C_0 D_0$
  - Trong đó:  $C_0$  chứa 28 bit bên trái  
 $D_0$  chứa 28 bit bên phải

# Key Schedule

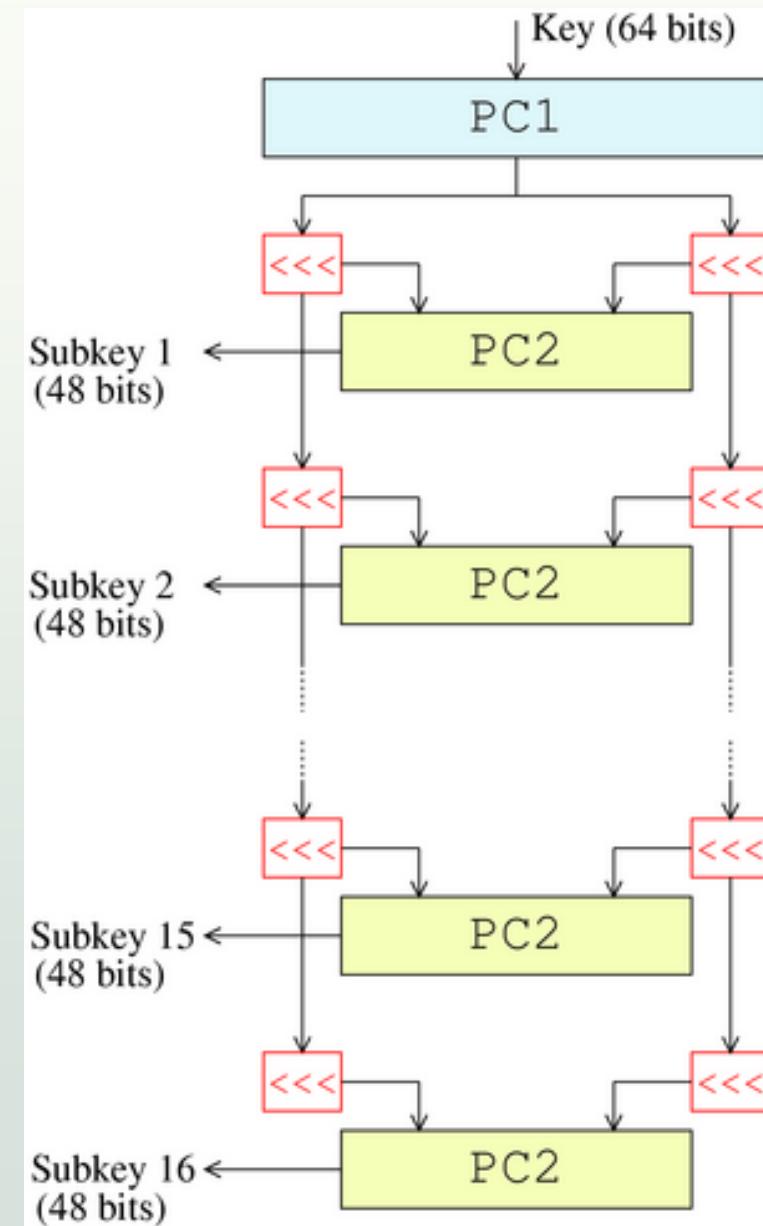
- ❖ Thao tác xoay vòng bit

- <<<: Xoay vòng sang trái
- >>>: Xoay vòng sang phải

- ❖ Với subkey thứ 1, 2, 9, 16: xoay vòng

- 1 vị trí

- ❖ Với subkey còn lại: xoay vòng 2 vị trí



# Các hoán vị trong Key Schedule

PC-1						
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

**Chọn 56 bit**  
**(bỏ bit 8, 16, 24, 32,  
40, 48, 56, 64)**

PC-2					
14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

**Chọn 48 bit**  
**(bỏ bit 9, 18, 22, 25,  
35, 38, 43, 54)**

# **Ưu điểm – Nhược điểm**

---

## **❖ Ưu điểm:**

- Có tính bảo mật cao
- Công khai, dễ hiểu
- Nó có thể triển khai trên thiết bị điện tử có kích thước nhỏ

# Ưu điểm – Nhược điểm

---

- ❖ Nhược điểm:
  - Khóa yếu là các khóa mà theo thuật toán sinh khóa con thì tất cả 16 khóa con đều như nhau :  $K_1=K_2=\dots=K_{16}$

# Một số nhận xét

---

- ❖ 4 khóa yếu (weak key):
  - Gồm toàn bit 0
  - Gồm toàn bit 1
  - Gồm  $\frac{1}{2}$  là bit 0 (liên tiếp),  $\frac{1}{2}$  là bit 1 (liên tiếp)
- ❖ 12 khóa “tương đối yếu” (semi-weak key)
  - Khóa có dạng: 7 bit 0 (liên tiếp), 7 bit 1 (liên tiếp)

# Giải mã DES

---

- ❖ Thực hiện tương tự như mã hóa, tuy nhiên ở vòng lặp  $i$  sẽ sử dụng subkey  $K_{17-i}$
- ❖ Vòng lặp 1 sử dụng  $K_{16}$
- ❖ Vòng lặp 2 sử dụng  $K_{15}$
- ❖ ....

# Thuật toán 3-DES (TripleDES)

---

- ❖ Khắc phục yếu điểm kích thước khóa ngắn của mã hóa DES
- ❖ Sử dụng mã hóa DES nhiều lần với các khóa khác nhau cho cùng một bản tin
- ❖ Chiều dài khóa 168 bit
- ❖  $C = E(D(E(P, K1), K2), K3)$

# Thuật toán 3-DES (TripleDES)

