

Trường Đại Học Công Nghệ Thông Tin
Khoa Mạng Máy Tính và Truyền Thông

AN TOÀN MẠNG MÁY TÍNH

ThS. Tô Nguyễn Nhật Quang

NỘI DUNG MÔN HỌC

1. Tổng quan
2. Các phần mềm gây hại – Trojan
3. Các phần mềm gây hại – Virus
4. Các giải thuật mã hoá dữ liệu
5. Mã hoá khoá công khai và quản lý khoá
6. Chứng thực dữ liệu
7. Một số giao thức bảo mật mạng
8. Bảo mật mạng không dây
9. Bảo mật mạng ngoại vi
10. Hệ thống tìm kiếm, phát hiện và ngăn ngừa xâm nhập

BÀI 4

CÁC GIẢI THUẬT MÃ HOÁ DỮ LIỆU



Các giải thuật mã hoá dữ liệu

1. Giới thiệu về mật mã hoá
2. Lịch sử của mật mã
3. Giải thuật mã hoá cổ điển
4. Giải thuật mã hoá hiện đại
5. Bẻ gãy một hệ thống mật mã
6. Bài tập

1. Giới thiệu về mật mã hoá

- **Giới thiệu**

- Mật mã hoá được sử dụng kể từ cổ đại cho đến tận ngày nay.
- Hiện nay, các giao dịch tài chính, chuyển khoản, mua sắm hàng hoá, thư từ, tài liệu... được thực hiện nhiều qua môi trường mạng đòi hỏi dữ liệu phải được bảo mật tốt => phải được mã hoá.

1. Giới thiệu về mật mã hoá

► REASONS TO USE ENCRYPTION



1. Giới thiệu về mật mã hoá

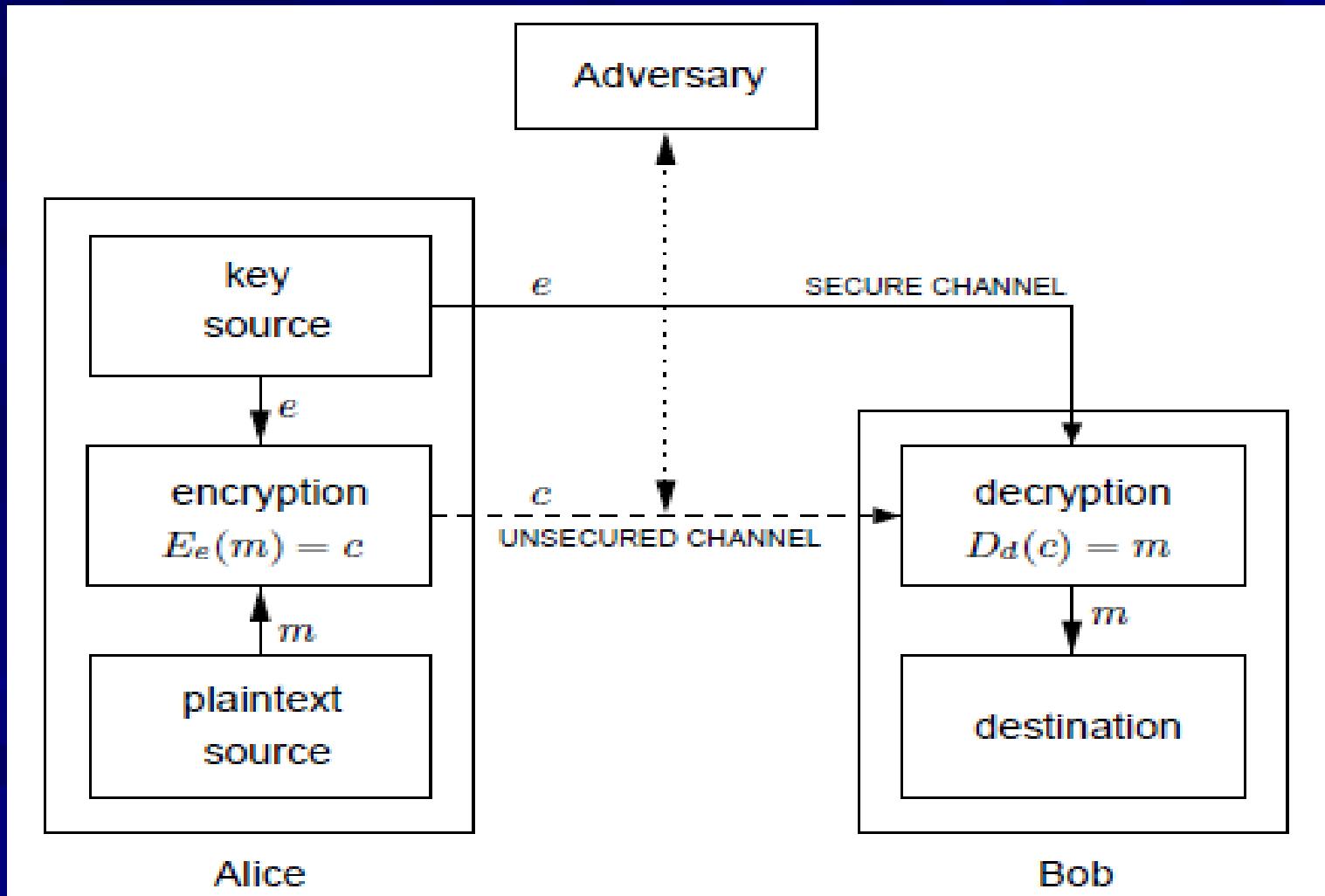
- **Một số khái niệm**

- Thông báo, văn bản: là một chuỗi hữu hạn các ký hiệu lấy từ một bảng chữ cái Z nào đó và được ký hiệu là m.
- Mật mã hoá: là việc biến đổi một thông báo sao cho nó không thể hiểu nổi đối với bất kỳ người khác ngoài người nhận được mong muốn.
- Phép mật mã hoá thường được ký hiệu là e(m), với m là thông báo cần mã hoá.

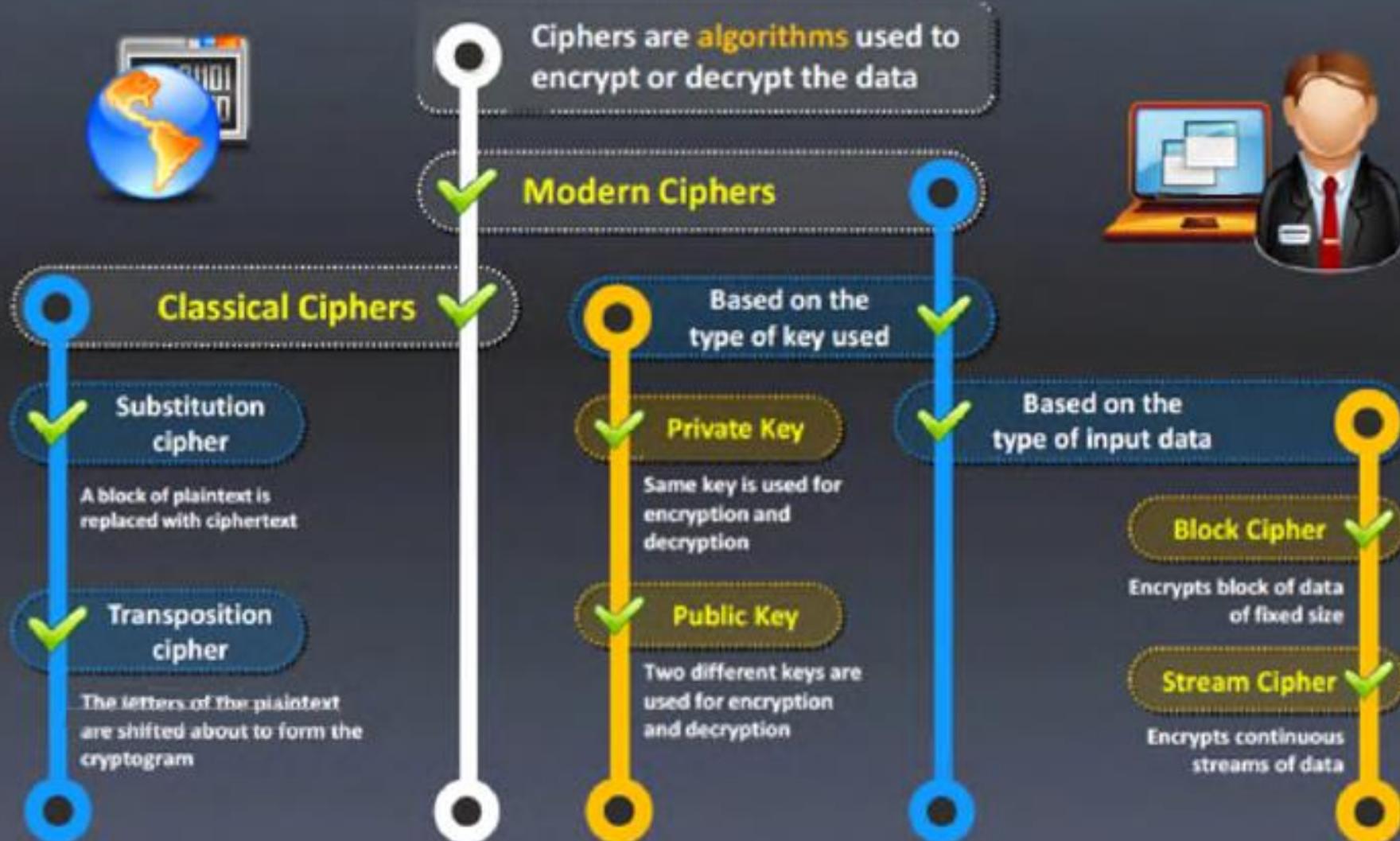
1. Giới thiệu về mật mã hoá

- **Một số khái niệm**
 - Khoá: là một thông số đầu vào của phép mã hoá hoặc giải mã. Khoá dùng để mã hoá ký hiệu là k_e , khoá dùng để giải mã ký hiệu là k_d .
 - Chuỗi mật mã: là chuỗi nguy trang, tức là chuỗi thông báo qua phép mật mã hoá và thường được ký hiệu là $c: c=e(m,k_e)$.
 - Phép giải mã $d(c,k_d)$ là quá trình xác định thông báo gốc (m) từ chuỗi mật mã c và khoá giải mã k_d , và thường được ký hiệu là $d(c,k_d): d(c,k_d)=m$.

1. Giới thiệu về mật mã hóa



1. Giới thiệu về mật mã hóa



2. Lịch sử của mật mã

- Mật mã học là ngành có lịch sử hàng ngàn năm.
- Mật mã học cổ điển với bút và giấy.
- Mật mã học hiện đại với điện cơ, điện tử, máy tính.
- Sự phát triển của mật mã học đi liền với sự phát triển của phá mã (thám mã):
 - Phát hiện ra bức điện Zimmermann khiến Hoa Kỳ tham gia Thế chiến I
 - Việc phá mã thành công hệ thống mật mã của Đức Quốc xã góp phần đẩy nhanh thời điểm kết thúc thế chiến II.
- Hai sự kiện khiến cho mật mã học trở nên đại chúng:
 - Sự xuất hiện của tiêu chuẩn mật mã hóa DES.
 - Sự ra đời của các kỹ thuật mật mã hóa công khai.

2. Lịch sử của mật mã

- Mật mã học cổ điển

- Các chữ tượng hình không tiêu chuẩn tìm thấy trên các bức tượng Ai Cập cổ đại (cách đây khoảng 4500 năm tr.CN).
- Mã hóa thay thế bảng chữ cái đơn giản như mật mã hóa Atbash (khoảng năm 500-600 tr.CN).
- Người La Mã xây dựng mật mã Caesar.

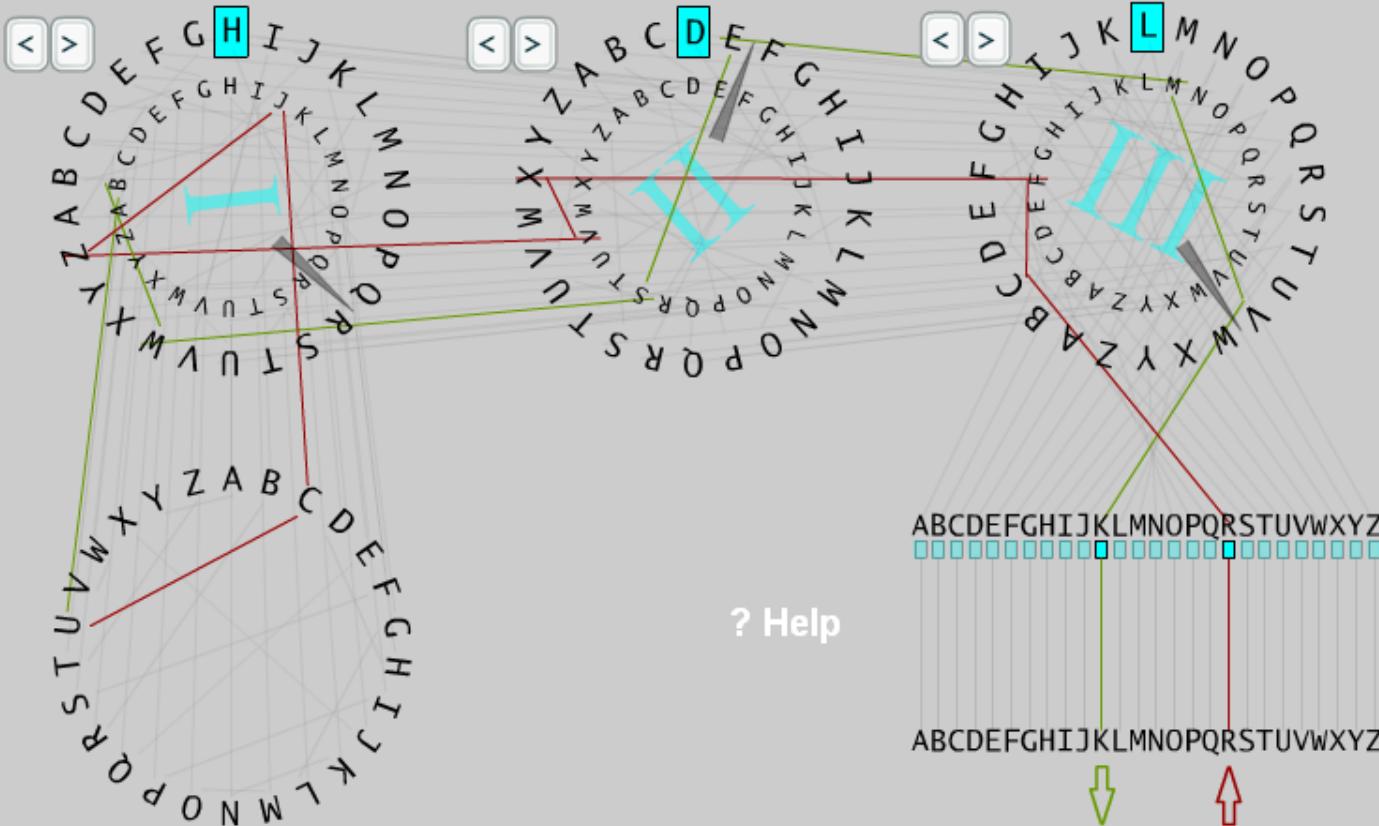
2. Lịch sử của mật mã

- Mật mã học trong thế chiến thứ 2
 - Người Đức sử dụng rộng rãi một hệ thống máy rôto cơ điện tử có tên gọi là máy Enigma.
 - 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.

2. Lịch sử của mật mã

Máy
Enigma





Input:

COMPUTER

Output:

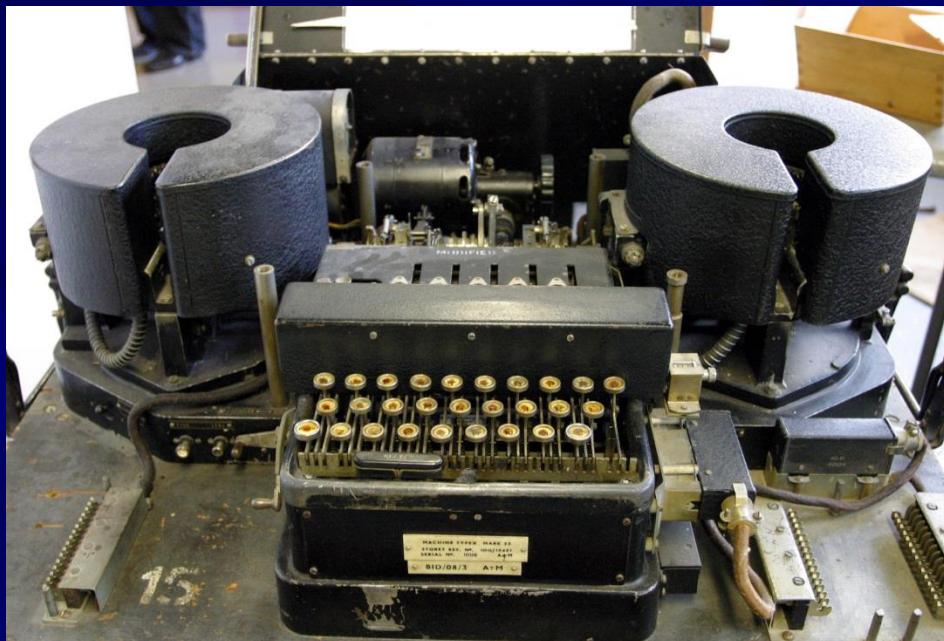
HEYGBZSK

Status Highlighted wires show encryption steps.



Máy Enigma

2. Lịch sử của mật mã



Máy TypeX



2. Lịch sử của mật mã

- Mật mã học hiện đại

- Cha đẻ của mật mã học hiện đại là Claude Shannon.
- Tiêu chuẩn mật mã hóa dữ liệu (Data Encryption Standard) là một phương thức mã hóa được công bố tại Mỹ vào ngày 17.03.1975.
- Với chiều dài khoá chỉ là 56-bit, DES đã được chứng minh là không đủ sức chống lại những tấn công kiểu vét cạn (*brute force attack* - *tấn công dùng bạo lực*).

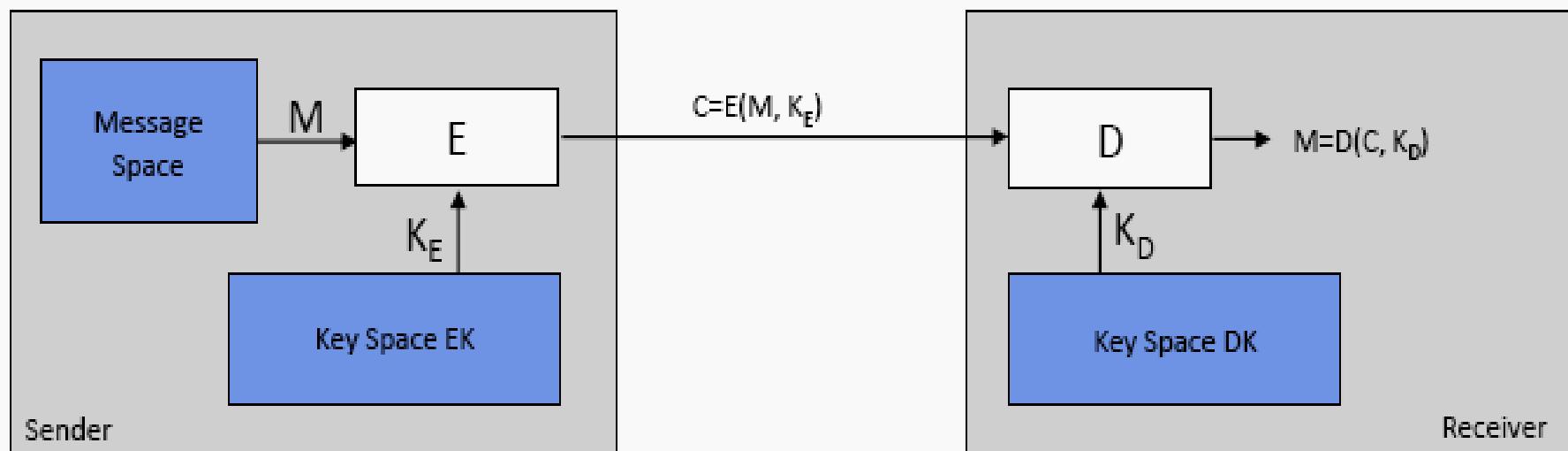
2. Lịch sử của mật mã

- **Mật mã học hiện đại**

- Năm 2001, DES đã chính thức được thay thế bởi AES (*Advanced Encryption Standard - Tiêu chuẩn mã hóa tiên tiến*).
- Trước thời kỳ này, hầu hết các thuật toán mã hóa hiện đại đều là những thuật toán khóa đối xứng (*symmetric key algorithms*), trong đó cả người gửi và người nhận phải dùng chung một khóa, và cả hai người đều phải giữ bí mật về khóa này.
- Đối với mật mã hóa dùng khóa bất đối xứng, người ta phải có một cặp khóa có quan hệ toán học để dùng trong thuật toán, một dùng để mã hóa và một dùng để giải mã. Phổ biến nhất là mã hóa RSA.

2. Lịch sử của mật mã

- Mật mã học hiện đại



a) Symmetric Encryption:

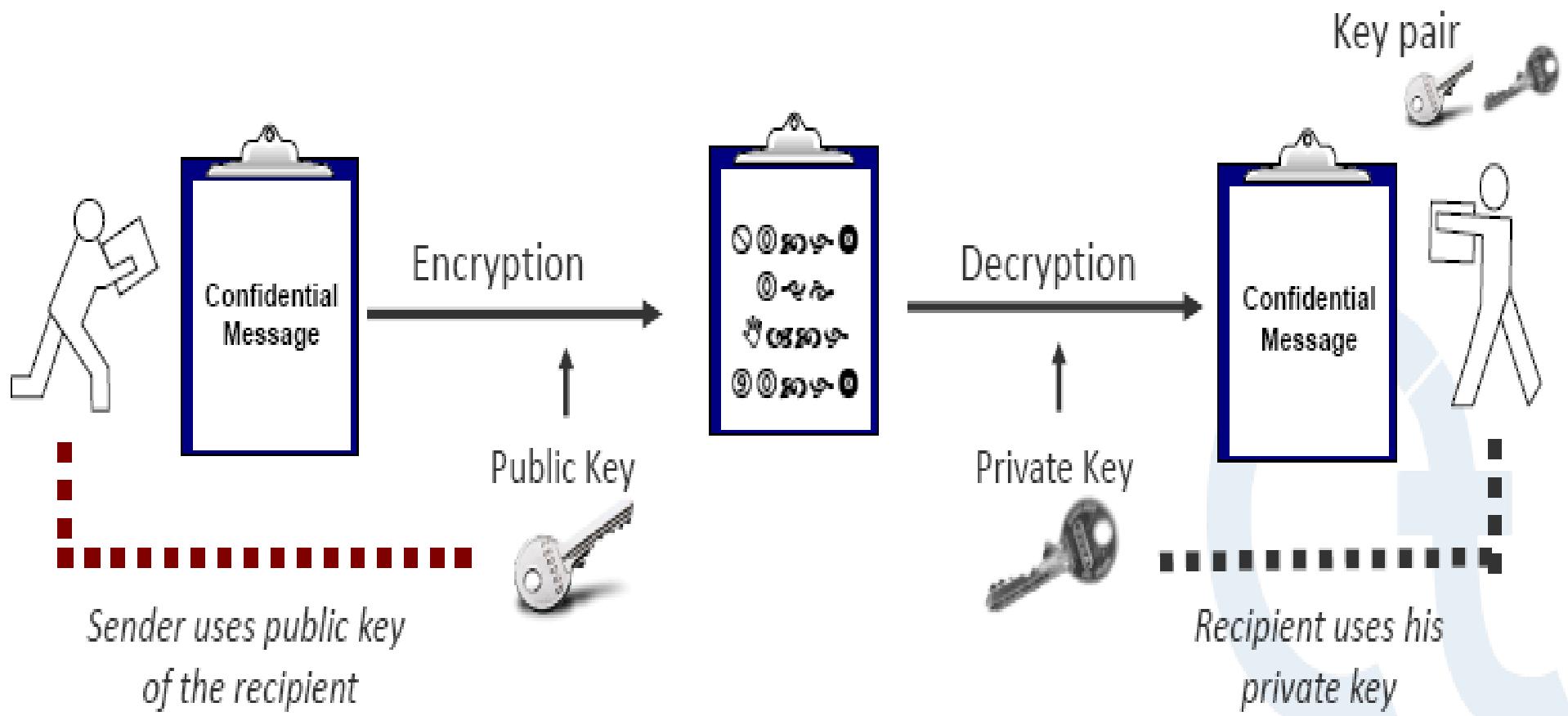
$K_E = K_D$ (e.g. AES)
secret
secret

b) Asymmetric Encryption:

$K_E \neq K_D$ (e.g. RSA)
public
private/secret

2. Lịch sử của mật mã

- Mật mã học hiện đại



Mã hóa RSA

3. Giải thuật mã hoá cổ điển

- Các yêu cầu cơ bản đối với giải thuật mật mã hoá là:
 - Có tính bảo mật cao
 - Công khai, dễ hiểu. Khả năng bảo mật được chốt vào khoá chứ không vào bản thân giải thuật.
 - Có thể triển khai trên các thiết bị điện tử.

3. Giải thuật mã hoá cổ điển

1. Mã thay thế đơn giản (Substitution Cipher)

- Trong phép này, khoá là một hoán vị h của bảng chữ cái Z 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 $26!$ ($\approx 4 \cdot 10^{26}$) hoán vị (khoá)
- Ví dụ: khoá là chuỗi UXEOS..., ký hiệu A trong thông báo sẽ được thay bằng U, ký hiệu B sẽ được thay bằng X...
- \Rightarrow Phá mã?

3. Giải thuật mã hoá cổ điển

1. Mã thay thế đơn giản (Substitution Cipher)

- Chọn một hoán vị $p: \mathbb{Z}_{26} \rightarrow \mathbb{Z}_{26}$ làm khoá.

- VD:

- Mã hoá
 $e_p(a)=X$

a	b	c	d	e	f	g	h	i	j	k	l	m
X	N	Y	A	H	P	O	G	Z	Q	W	B	T
n	o	p	q	r	s	t	u	v	w	x	y	z
S	F	L	R	C	V	M	U	E	K	J	D	I

- Giải mã
 $d_p(A)=d$

A	B	C	D	E	F	G	H	I	J	K	L	M
d	l	r	y	v	o	h	e	z	x	w	p	t
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	g	f	j	q	n	m	u	s	k	a	c	i

3. Giải thuật mã hoá cổ điển

2. Mã thay thế n-gram

- Thay vì thay thế các ký tự, người ta có thể thay thế cho từng cụm 2 ký tự (diagram), 3 ký tự (trigram) hoặc tổng quát cho từng cụm n ký tự (n-gram).
- Với bảng chữ cái gồm 26 ký tự tiếng Anh thì phép thay thế n-gram sẽ có khoá là một hoán vị của 26^n n-gram khác nhau.
- ⇒ Phá mã?

3. Giải thuật mã hoá cổ điển

2. Mã thay thế n-gram

Trong trường hợp diagram thì hoán vị gồm 26^2 diagram và có thể biểu diễn bằng một dãy 2 chiều 26×26 trong đó các hàng biểu diễn ký hiệu đầu tiên, các cột biểu diễn ký hiệu thứ hai, nội dung của các ô biểu diễn chuỗi thay thế.

	A	B	...
A	EG	RS	
B	BO	SC	
...			

3. Giải thuật mã hoá cổ điển

3. 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 $(4 \ 1 \ 3 \ 2 \ 5)$.

3. Giải thuật mã hoá cổ điển

3. Mã hoán vị bậc d

- 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:

$c = \text{NJHO AI S DGOO OATCR}$

- \Rightarrow Phá mã?

3. Giải thuật mã hoá cổ điển

4. Mã dịch chuyển (Shift Cypher)

Vigenère và Caesar

- Trong phương pháp Vigenère, khoá bao gồm một chuỗi có d ký tự. Chúng được viết lặp lại bên dưới thông báo và được cộng modulo 26. Các ký tự trắng được giữ nguyên không cộng.
- Nếu $d=1$ thì khoá chỉ là một ký tự đơn và được gọi là phương pháp Caesar (được đưa ra sử dụng đầu tiên bởi Julius Caesar).
- \Rightarrow Phá mã?

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

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

Ví dụ:

Plaintext: CRYPTOGRAPHY

The classic Caesar Shift chart

Ciphertext: HWUYTLWFUMD (Shift of 5)

$$C = (p+5) \bmod 26$$

ATMMMT - TNNQ



Mã dịch chuyển – Shift Cypher

Vigenère Encryption – Block Cypher (1523 – 1596)

Ví dụ:

Từ khoá: CHIFFRE

Mã hoá: VIGENERE

Kết quả: XPOJSWG

	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

3. Giải thuật mã hoá cổ điển

5. One - time Pad:

e=000 h=001 l=010 d=011 p=100 n=101 a=110

Encryption: Plaintext \oplus Key = Ciphertext

Plaintext:	h	e		p	n	e	e	d	e	d
	001	000	010	100	101	000	000	011	000	011
Key:	111	101	110	101	111	100	000	101	110	000
Ciphertext:	110	101	100	001	010	100	000	110	110	011
	a	n	p	h	l	p	e	a	a	d

3. Giải thuật mã hoá cổ điển

6. Mã tuyến tính (Affine Cipher)

Mã tuyến tính là mã thay thế có dạng:

$$e(x) = ax + b \pmod{26}, \text{ với } a, b \in \mathbb{Z}_{26}.$$

Nếu $a = 1$ ta có mã dịch chuyển.

Giải mã: Tìm x ?

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

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

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

3. Giải thuật mã hoá cổ điển

7. 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.

3. Giải thuật mã hoá cổ điển

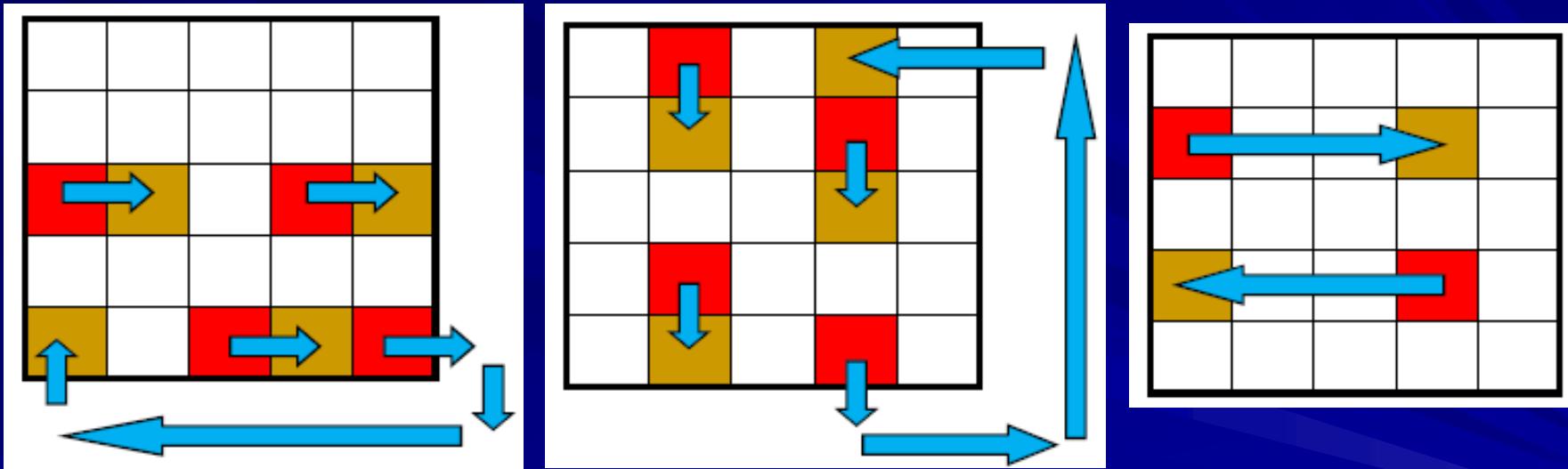
7. Mã Playfair

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.

3. Giải thuật mã hoá cổ điển

7. Mã Playfair



3. Giải thuật mã hoá cổ điển

7. Mã Playfair

Playfair key

Short version of the Playfair key:

PLAYFAIR



Key matrix

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

5x5 matrix

6x6 matrix

**C^a
A^b** Unnamed1

THANH PHO HO CHI MINH

**C^a
A^b** Playfair pre-formatting of <Unnamed1>

TH AN HP HO HO CH IM IN HX

**C^a
A^b** Playfair encryption of <Unnamed1>, key <KB>

QM PQ EA GQ GQ BK DE EU KW

3. Giải thuật mã hoá cổ điển

8. Mã Hill

Giải thuật mã hóa:

- Sử dụng m ký tự liên tiếp của plaintext và thay thế bằng m ký tự trong ciphertext với một phương trình tuyến tính trên các ký tự được gán giá trị lần lượt là A=01, B=02, ..., Z=26.
- Chọn ma trận vuông Hill (ma trận H) làm khoá.
- Mã hoá từng chuỗi n ký tự trên plaintext (vector P) với n là kích thước ma trận vuông Hill.
- $C = HP \text{ mod } 26$
- $P = H^{-1}C \text{ mod } 26$

3. Giải thuật mã hoá cổ điển

8. Mã Hill

Selected alphabet (26 characters)

Value of the first alphabet character

Hill key matrix

Alphabet characters
 Number values

Multiplication variant

(row vector) * (matrix)
 (matrix) * (column vector)

Size of matrix

1x1
 2x2
 3x3
 4x4
 5x5

Alphabet characters

Q	F			
W	Y			

Number values

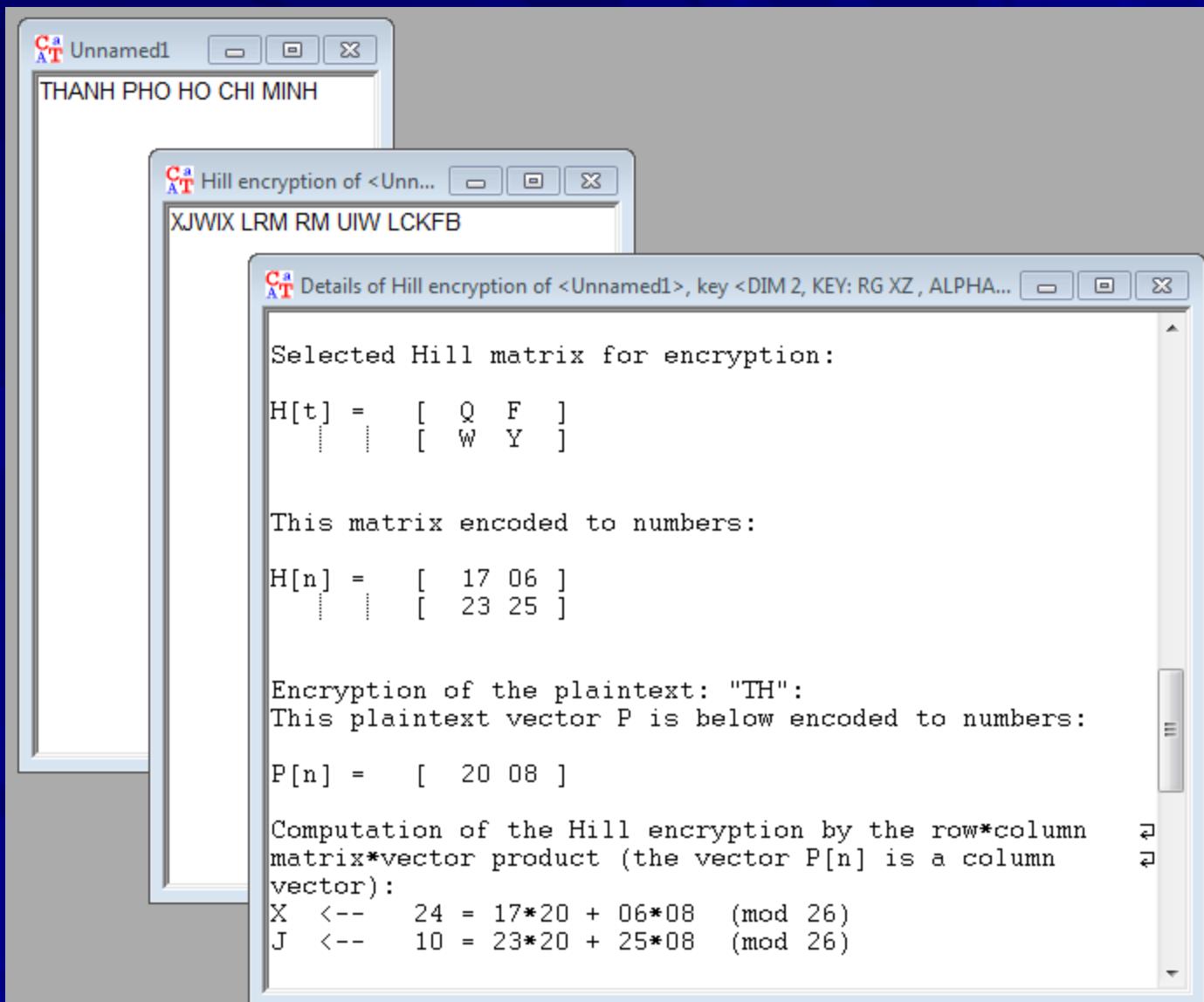
17	06			
23	25			

Generate random key 

Larger matrix

3. Giải thuật mã hoá cổ điển

8. Mã Hill



3. Giải thuật mã hoá cổ điển

8. Mã Hill

The screenshot shows a software window titled "C^aT Unnamed1" containing three nested windows related to Hill encryption.

- Outer Window:** Title bar says "C^aT Unnamed1". Subtitle bar says "THANH PHO HO CHI MINH".
- Middle Window:** Title bar says "C^aT Hill encryption of <Unn...>". Subtitle bar says "XJWIX LRM RM UIW LCKFB".
- Inner Window:** Title bar says "C^aT Details of Hill encryption of <Unnamed1>, key <DIM 2, KEY: RG XZ , ALPHA...>".

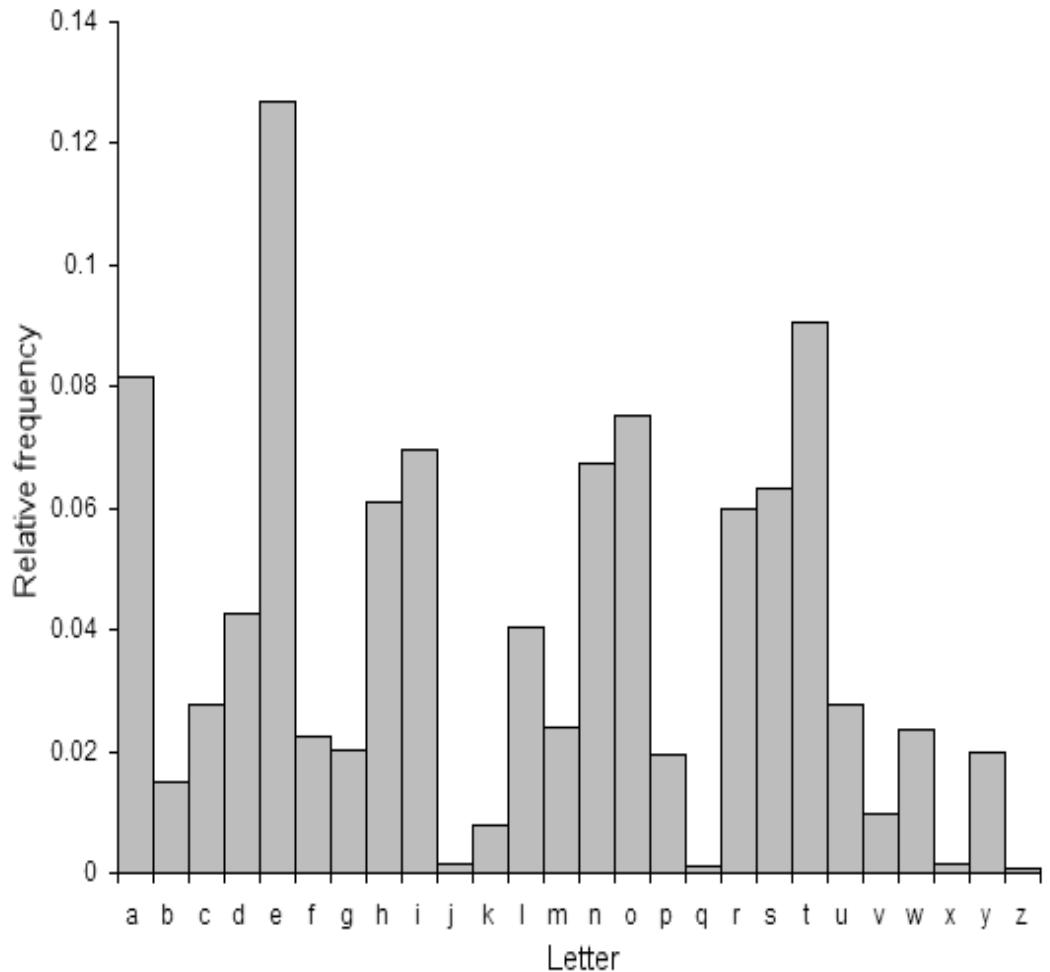
The inner window displays the following details:

- 4. Hill decryption**
- The inverted Hill matrix for decryption:**
$$D[t] = \begin{bmatrix} Y & T \\ C & Q \end{bmatrix}$$
- This matrix encoded to numbers:**
$$D[n] = \begin{bmatrix} 25 & 20 \\ 03 & 17 \end{bmatrix}$$
- Decryption of the ciphertext: "XJ":**
Ciphertext vector C decoded to numbers:
$$C[n] = \begin{bmatrix} 24 & 10 \end{bmatrix}$$
- Computation of the Hill decryption by the row*column matrix*vector product (the vector C[n] is a column vector):**
$$T \leftarrow 20 = 25*24 + 20*10 \pmod{26}$$
$$H \leftarrow 08 = 03*24 + 17*10 \pmod{26}$$
- The Hill plaintext is: "TH".**

3. Giải thuật mã hoá cổ điển

9. Phương pháp phá mã cổ điển:

- Dựa vào đặc điểm ngôn ngữ.
- Dựa vào tần suất xuất hiện của các chữ cái trong bảng chữ cái thông qua thống kê từ nhiều nguồn văn bản khác nhau, dựa vào số lượng các ký tự trong bảng mã để xác định thông báo đầu vào.



letter	probability	letter	probability
A	.082	N	.067
B	.015	O	.075
C	.028	P	.019
D	.043	Q	.001
E	.127	R	.060
F	.022	S	.063
G	.020	T	.091
H	.061	U	.028
I	.070	V	.010
J	.002	W	.023
K	.008	X	.001
L	.040	Y	.020
M	.024	Z	.001

Tần suất của các ký tự trong ngôn ngữ tiếng Anh

4. Giải thuật mã hoá hiện đại

- Thường sử dụng mã khối kết hợp với các phép hoán vị và thay thế.
- Việc biến đổi văn bản được thực hiện nhiều lần trong một số vòng lặp.
- Khoá con của các vòng lặp sẽ khác nhau và được sinh ra từ khoá ban đầu.
- Phổ biến có DES, AES, RSA...

4. Giải thuật mã hoá hiện đại

1. Phân loại

- Mã hoá khoá đối xứng (symmetric):
 - Block ciphers: mã hoá các khối có chiều dài cố định 64 bit hoặc 128 bit. Phổ biến có IDEA, RC2, DES, Triple DES, Rijndael (AES), MARS, RC6, Serpent, Twofish, DESX, DESL, DESXL.
 - Stream ciphers: mã hoá từng bit của thông điệp. Đại diện là RC4.
- Mã hoá khoá bất đối xứng (asymmetric): RSA

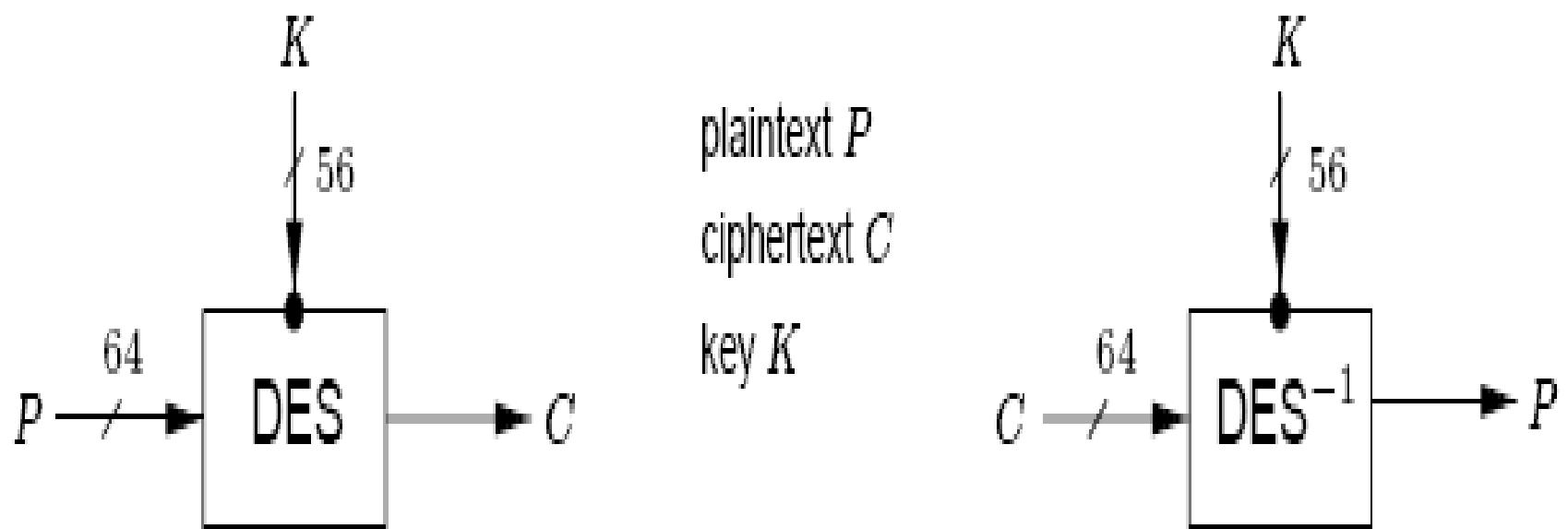
4. Giải thuật mã hoá hiện đại

2. Chuẩn mã hoá dữ liệu DES

- DES (Data Encryption Standard) được sử dụng rộng rãi trên thế giới.
- Dùng khoá có độ dài 56 bit để mã hoá các khối dữ liệu 64 bit.
- Cả bên mã hoá lẫn bên giải mã đều dùng chung một khoá và DES thuộc vào hệ mã khoá bí mật.
- Xét về độ an toàn, hiện nay 3DES (một cải tiến của DES) được đánh giá là có độ an toàn cao vì độ dài khoá của nó gấp 3 lần so với DES.

4. Giải thuật mã hoá hiện đại

2. Chuẩn mã hoá dữ liệu DES



Giải thuật mã hoá DES

2. Chuẩn mã hoá dữ liệu DES

- 17.03.1975: DES được công bố để công chúng đóng góp ý kiến.
- 11.1976: DES được phê chuẩn làm tiêu chuẩn chính thức.
- 1992: Biham và Shamir công bố một phương thức tấn công thám mã vi sai với độ phức tạp thấp hơn tấn công bạo lực (trên lý thuyết). Kiểu tấn công này đòi hỏi người tấn công lựa chọn 2^{47} văn bản rõ (một điều kiện không thực tế).
- 06.1997: Lần đầu tiên, dự án DESCHALL đã phá vỡ được một bản tin mã hoá bằng DES.

Giải thuật mã hoá DES

2. Chuẩn mã hoá dữ liệu DES

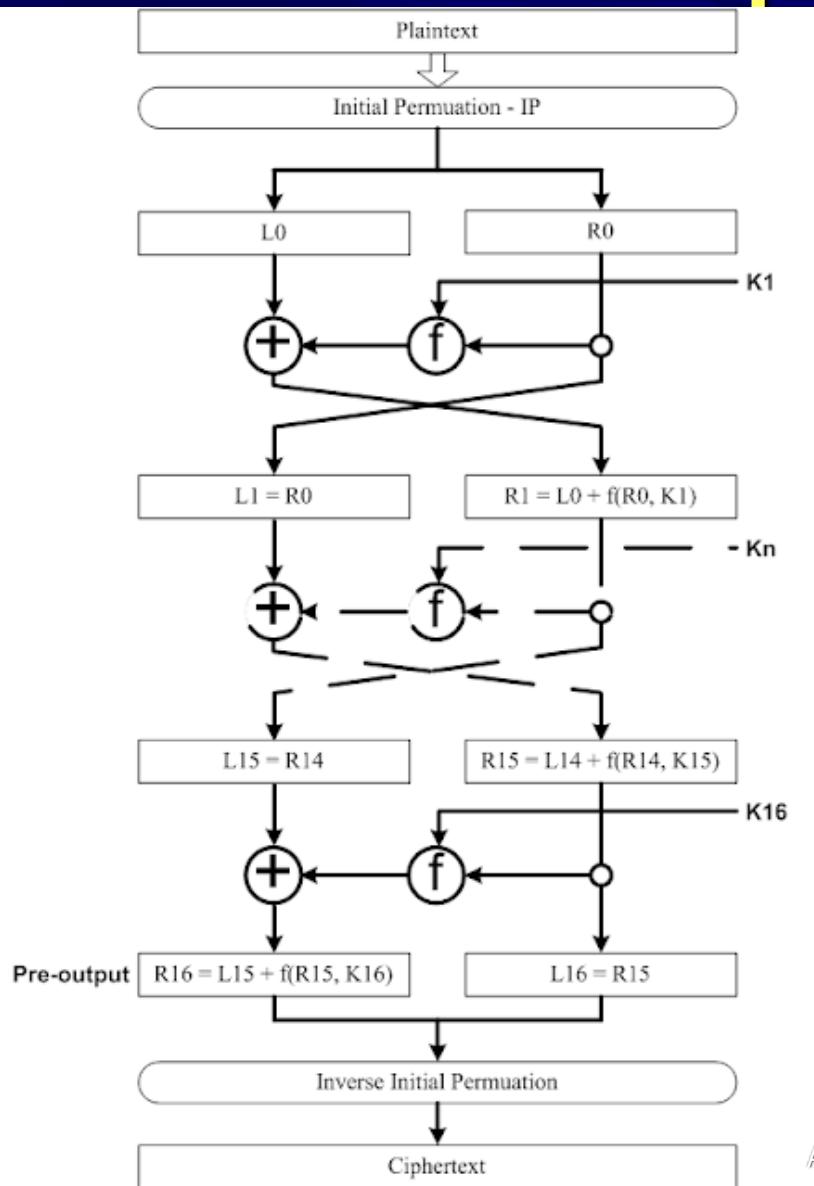
- 07.1998: Thiết bị thám mã Deep Crack của tổ chức Electronic Frontier Foundation phá được một khoá của DES trong vòng 56 giờ.
- 01.1999: Deep Crack cùng với distributed.net phá được DES trong 22 giờ 15 phút.
- 25.10.1999: Triple DES được khuyến cáo sử dụng cho các hệ thống quan trọng.
- 26.05.2002: AES trở thành tiêu chuẩn thay thế cho DES.

Giải thuật mã hoá DES

Giải thuật:

- Sử dụng một khoá K tạo ra n khoá con K_1, K_2, \dots, K_n .
- Hoán vị dữ liệu.
- Thực hiện n vòng lặp. Tại mỗi vòng lặp:
 - Dữ liệu được chia thành hai phần
 - Áp dụng phép toán thay thế lên một phần, phần còn lại giữ nguyên.
 - Hoán vị hai phần cho nhau.
- Hoán vị dữ liệu.

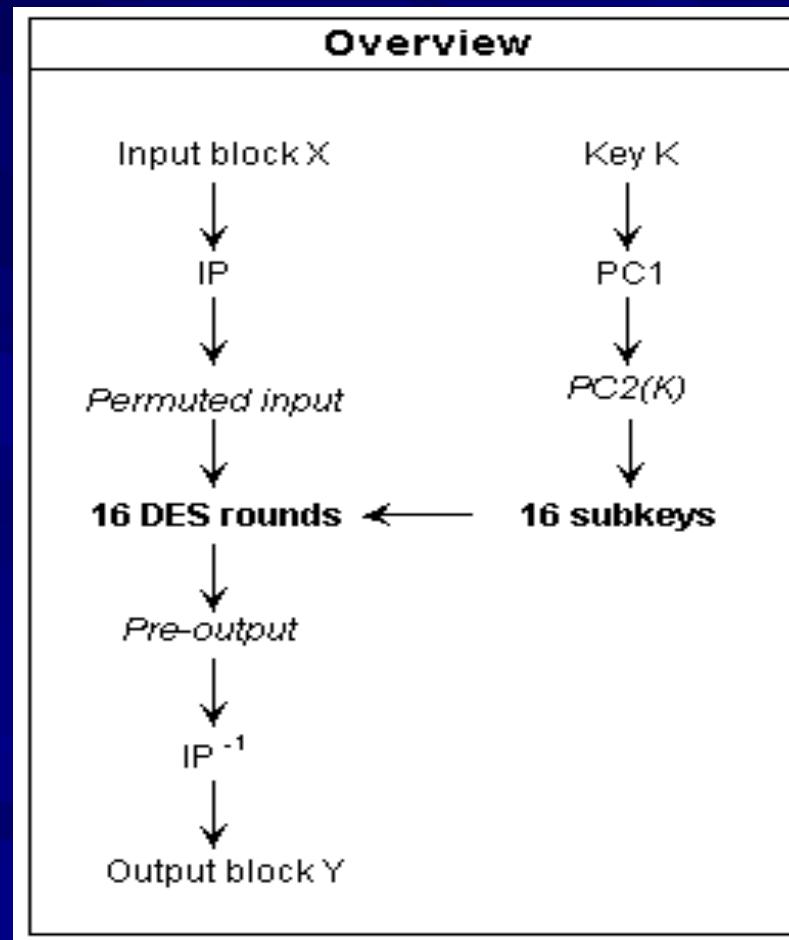
4. Giải thuật mã hoá hiện đại



2. Chuẩn mã hoá dữ liệu DES

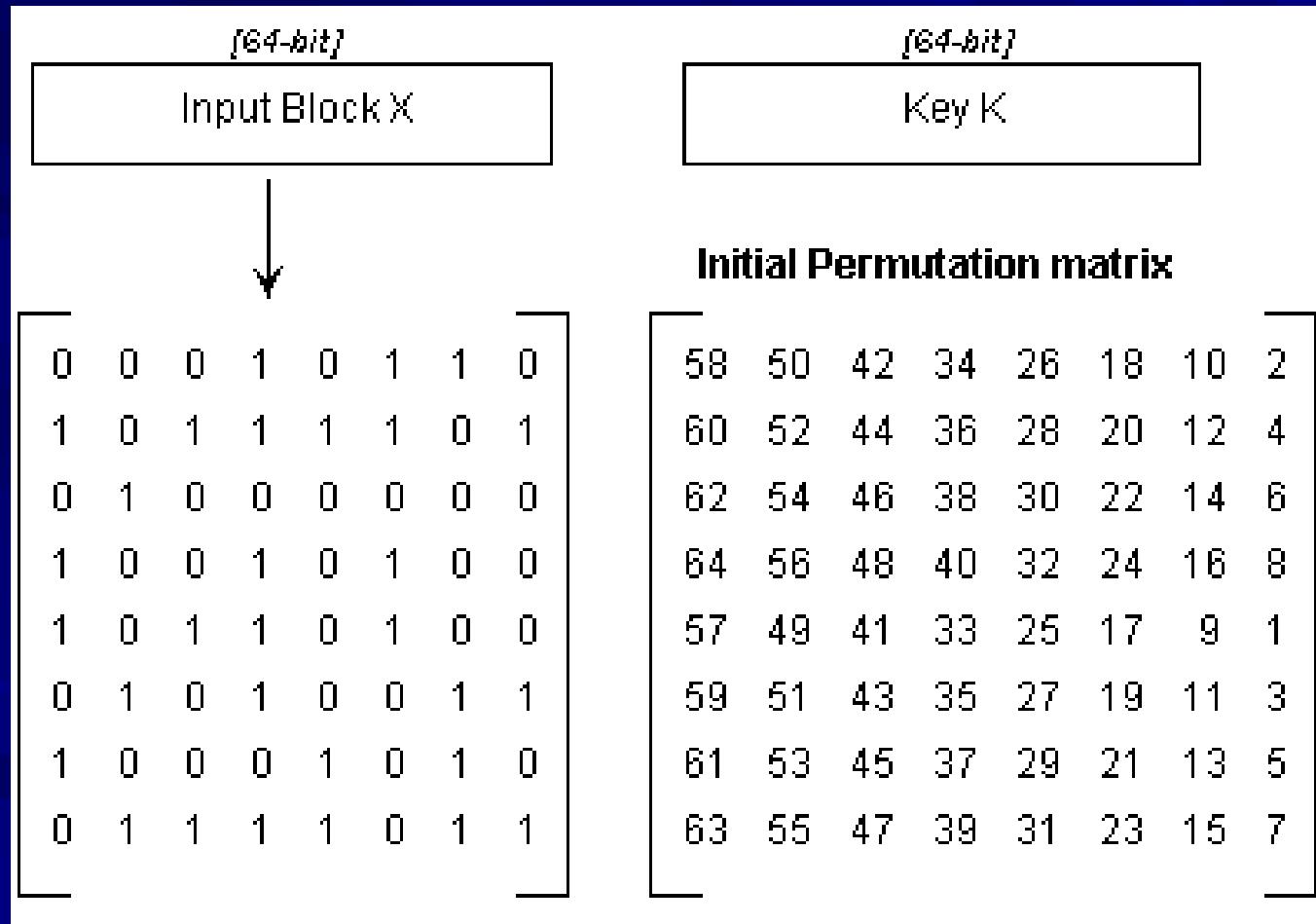
4. Giải thuật mã hoá hiện đại

2. Chuẩn mã hoá dữ liệu DES



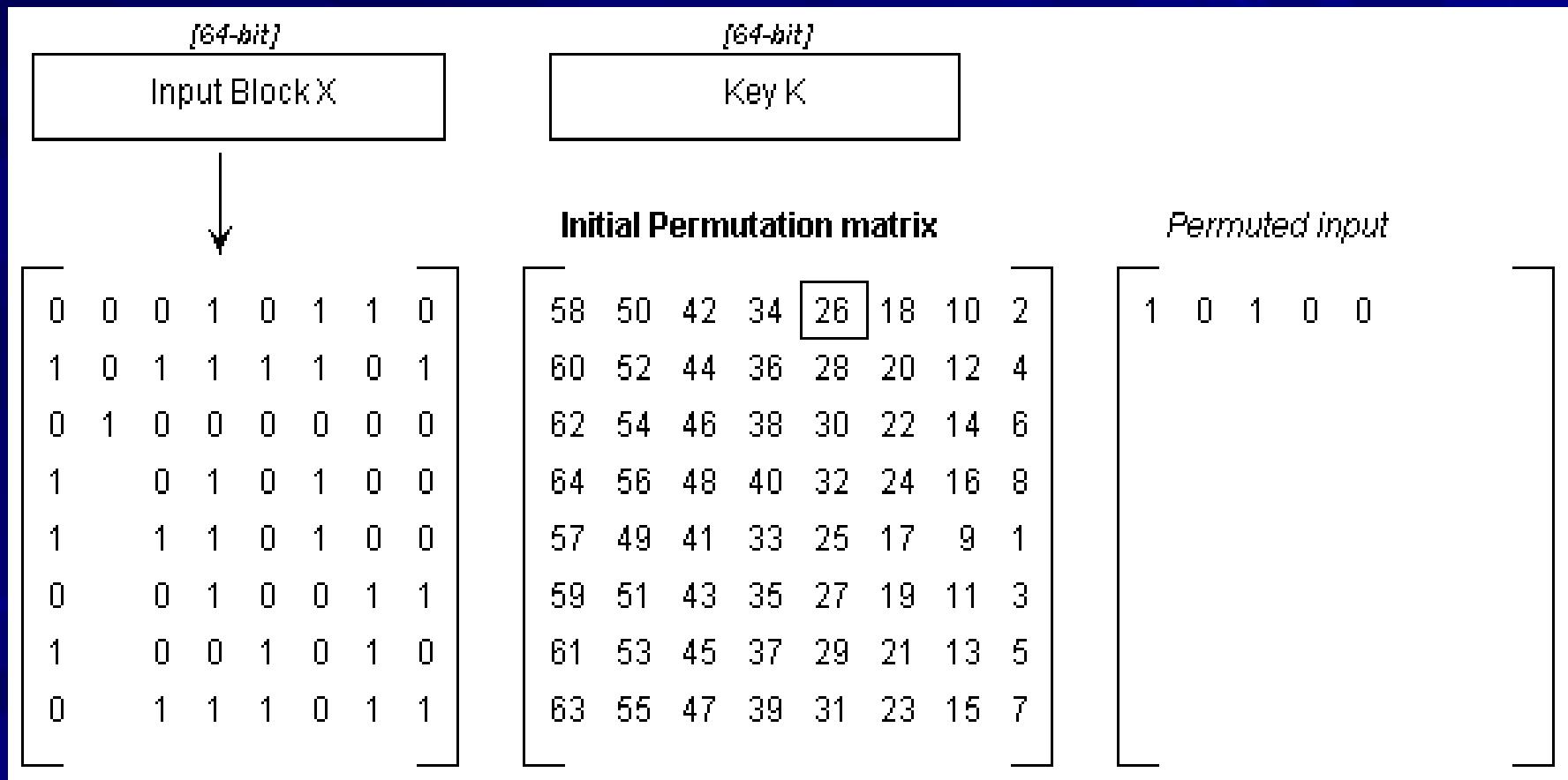
4. Giải thuật mã hoá hiện đại

2. Chuẩn mã hoá dữ liệu DES



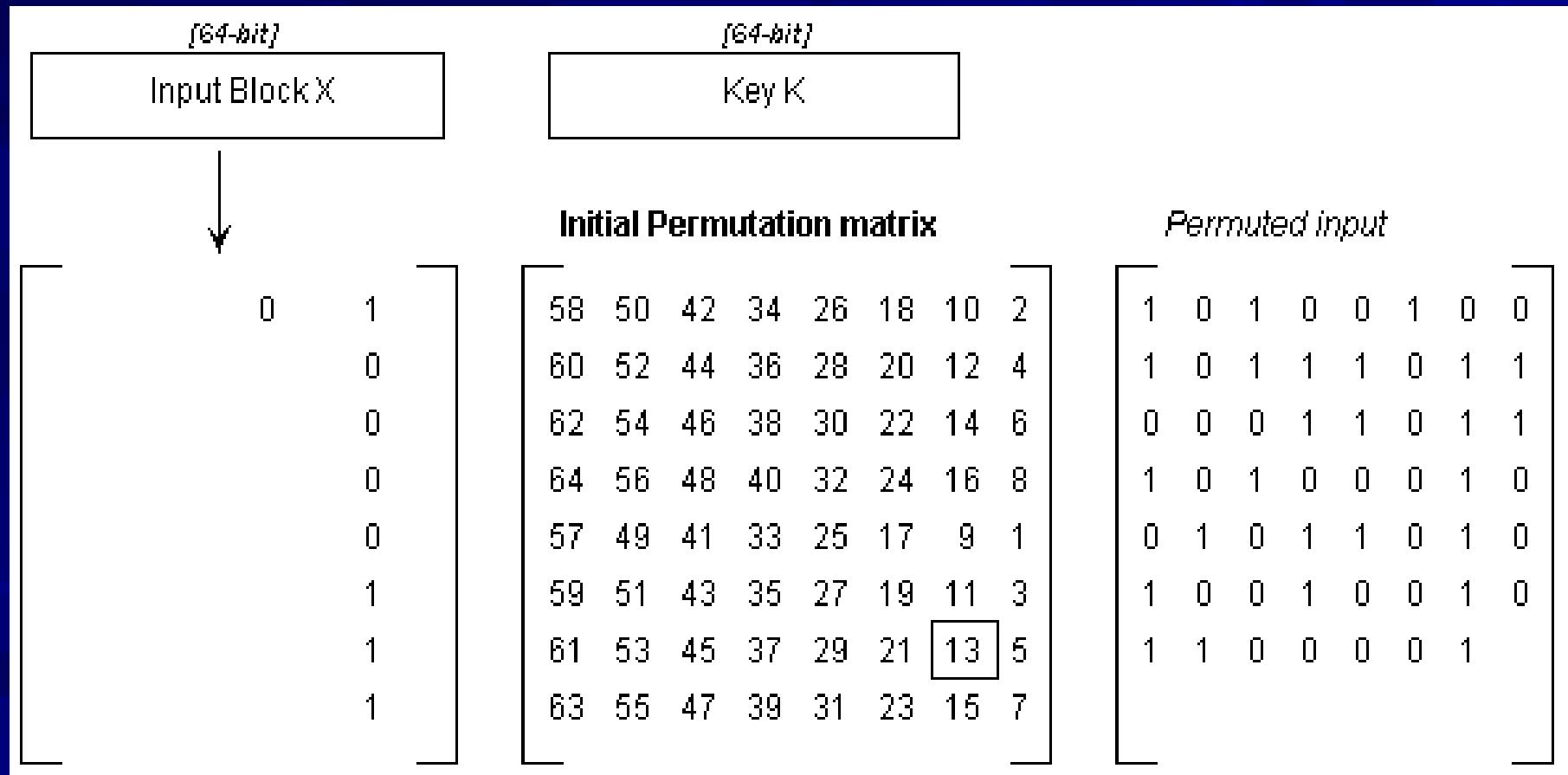
4. Giải thuật mã hoá hiện đại

2. Chuẩn mã hoá dữ liệu DES



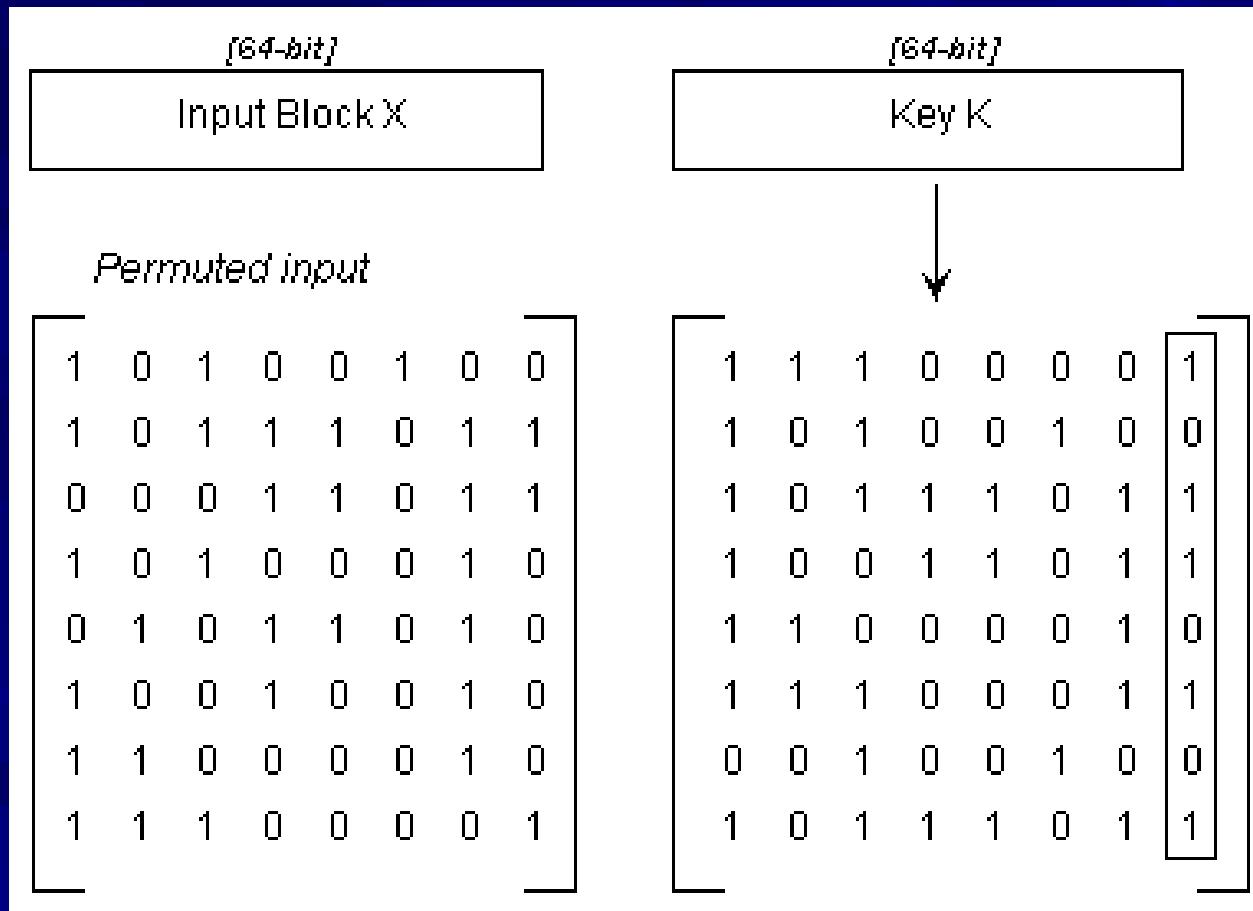
4. Giải thuật mã hoá hiện đại

2. Chuẩn mã hoá dữ liệu DES



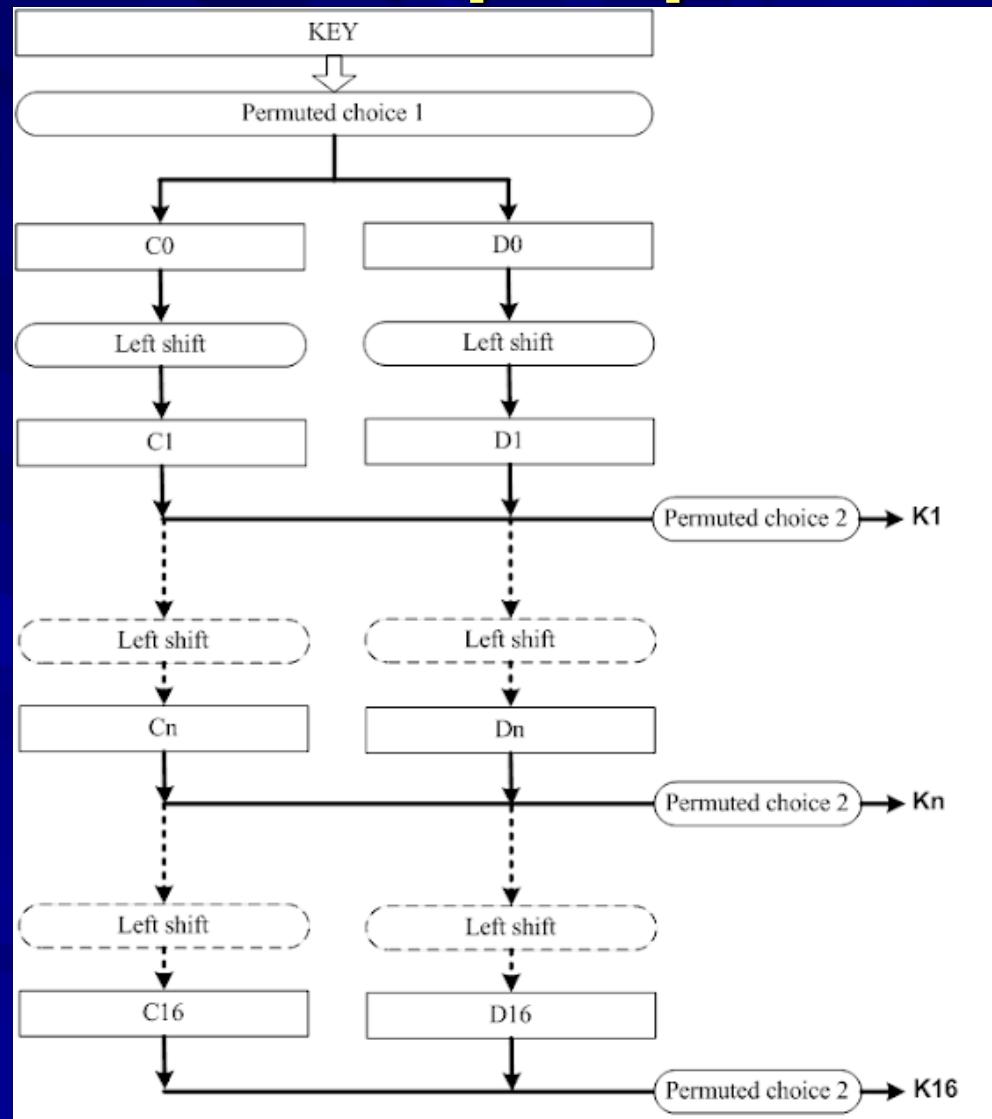
4. Giải thuật mã hoá hiện đại

2. Chuẩn mã hoá dữ liệu DES



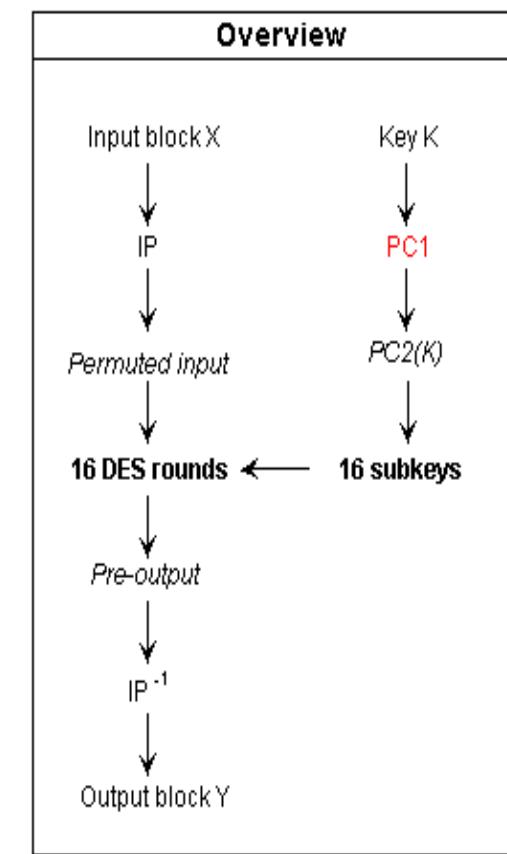
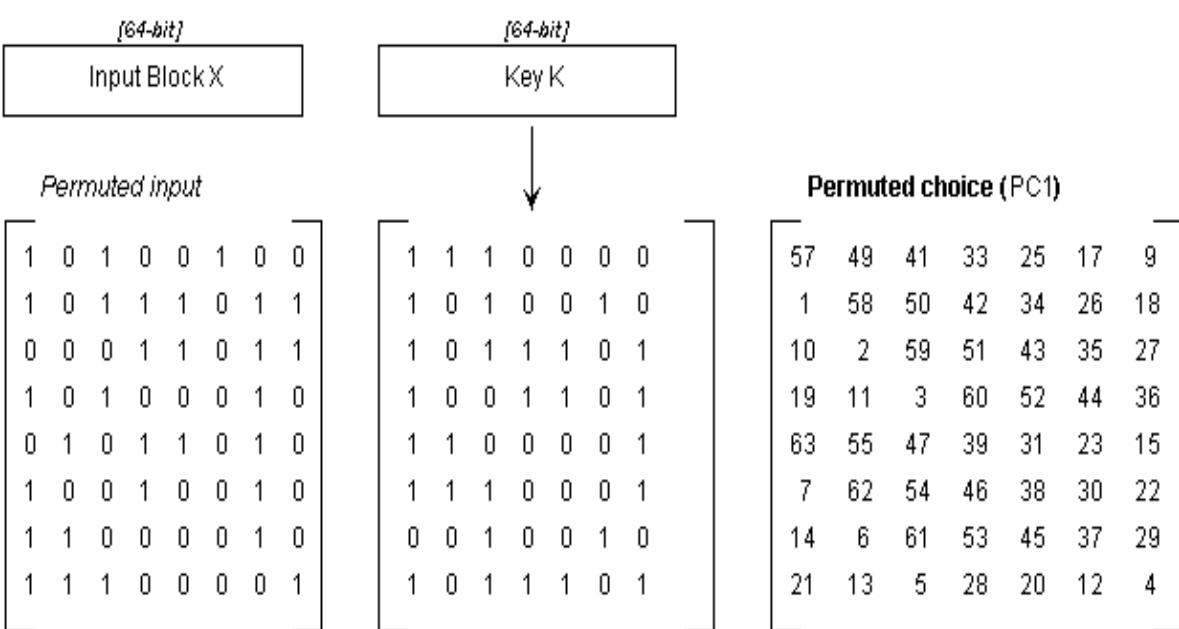
4. Giải thuật mã hoá hiện đại

2. Chuẩn mã hoá dữ liệu DES



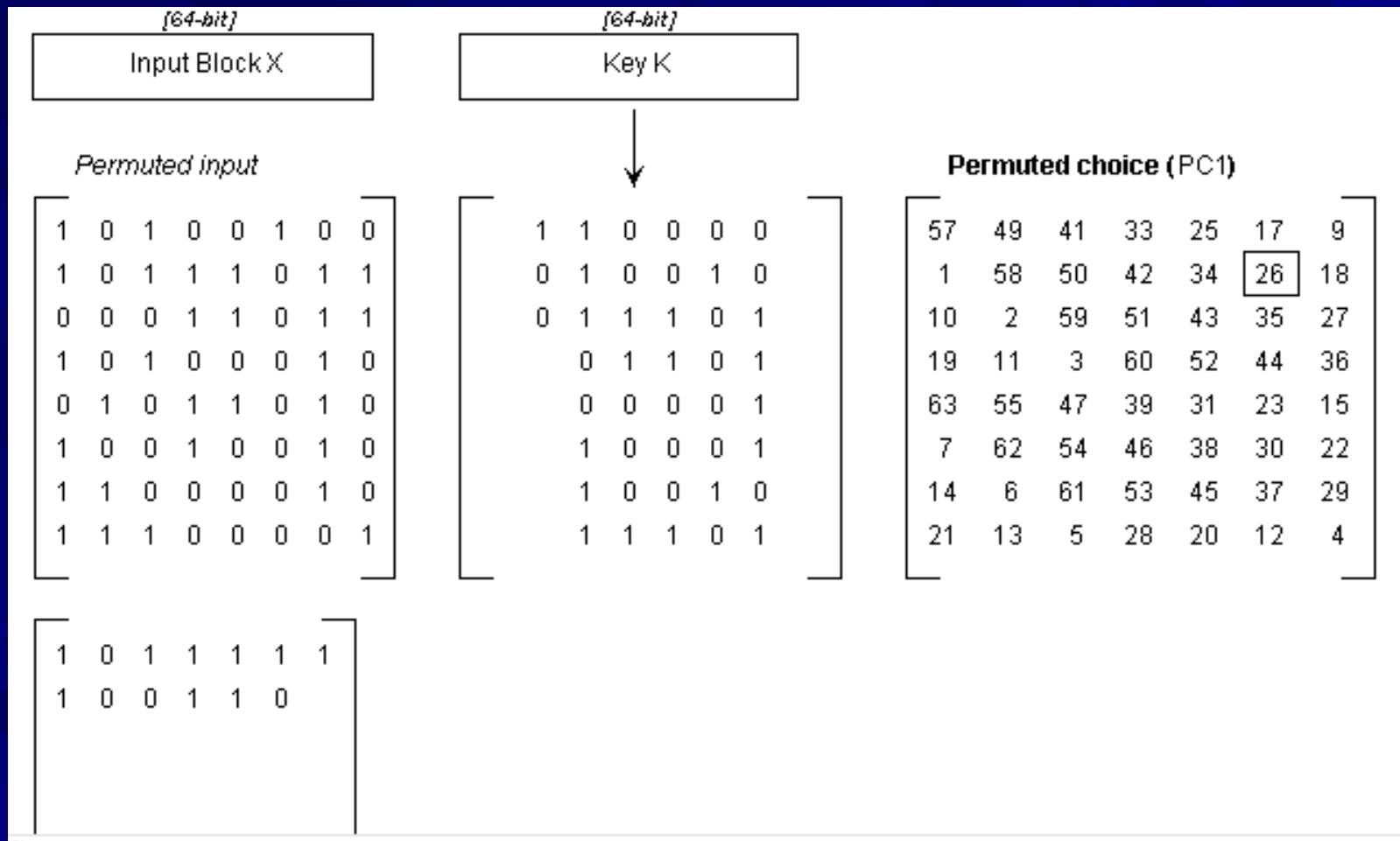
4. Giải thuật mã hoá hiện đại

2. Chuẩn mã hoá dữ liệu DES



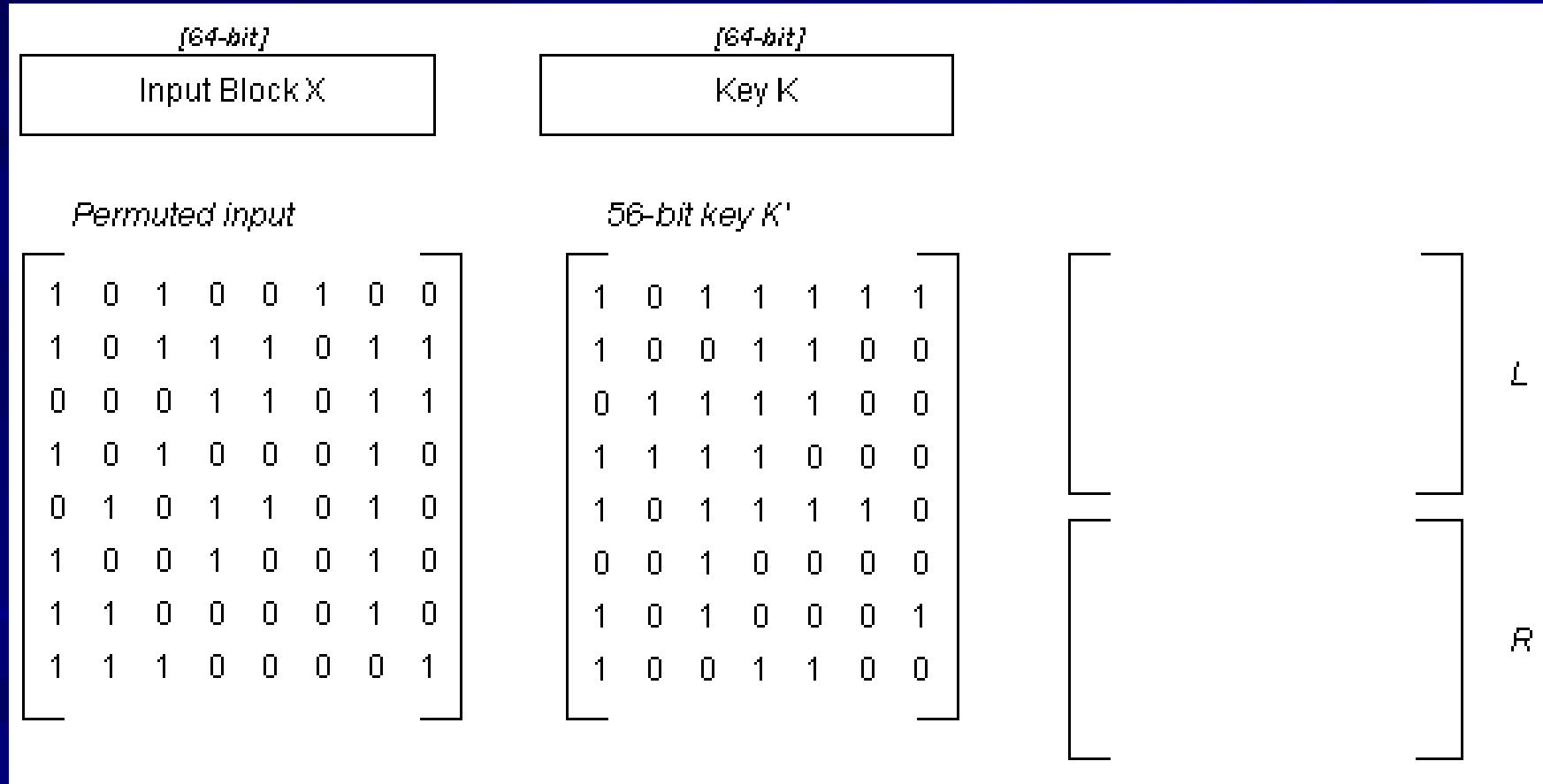
4. Giải thuật mã hoá hiện đại

2. Chuẩn mã hoá dữ liệu DES



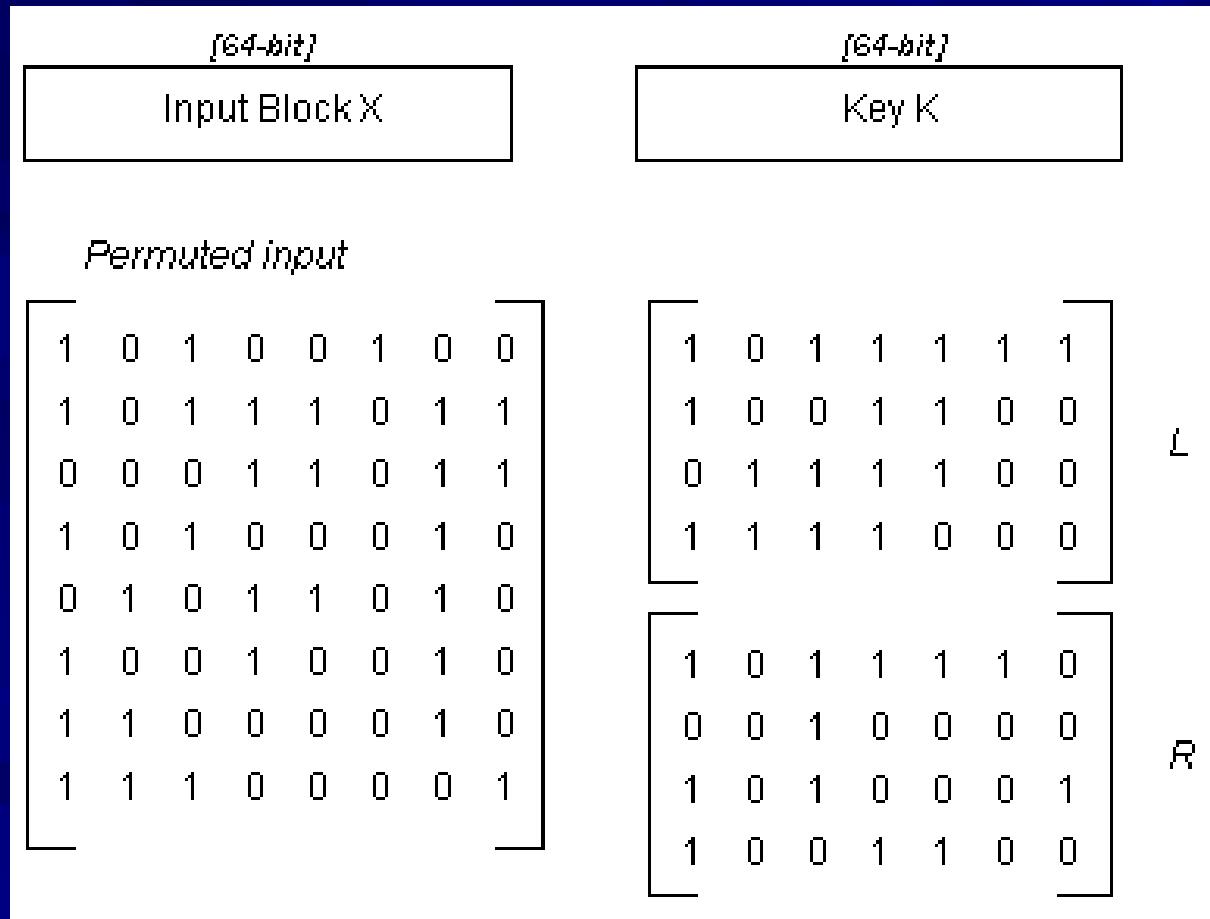
4. Giải thuật mã hoá hiện đại

2. Chuẩn mã hoá dữ liệu DES



4. Giải thuật mã hoá hiện đại

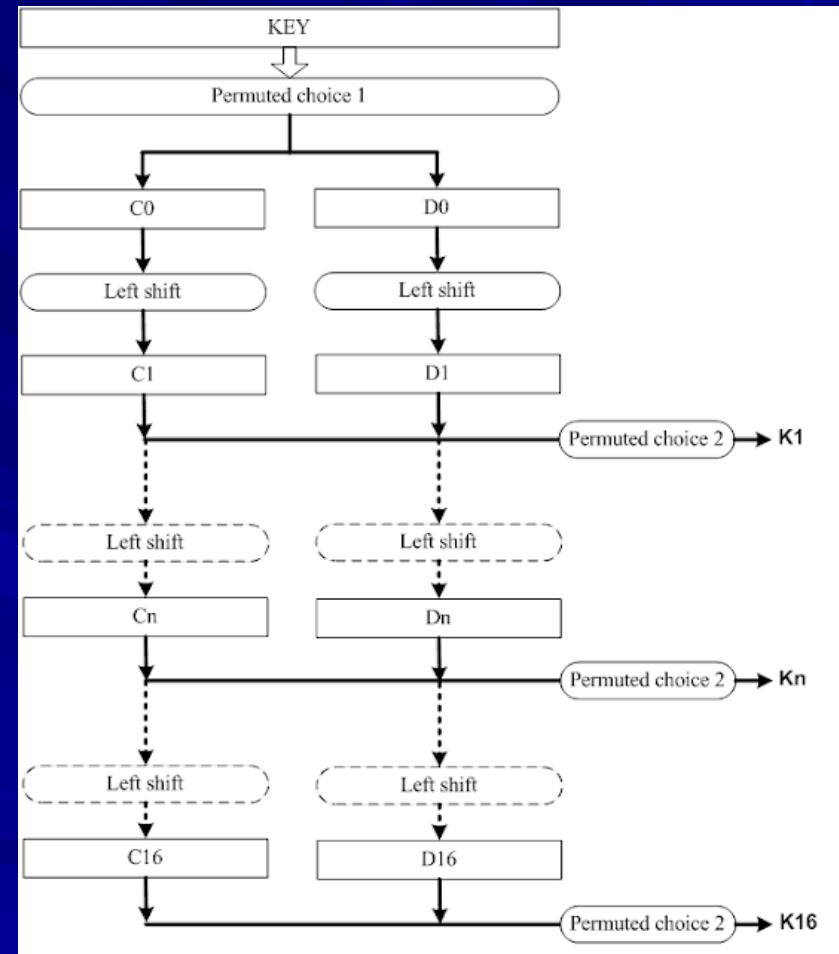
2. Chuẩn mã hoá dữ liệu DES



4. Giải thuật mã hoá hiện đại

2. Chuẩn mã hoá dữ liệu DES

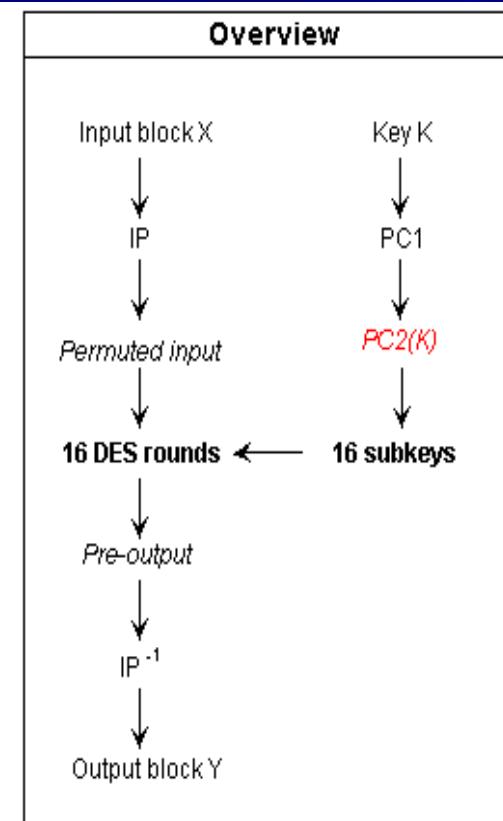
Iteration Number	Number of Left Shifts
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1



4. Giải thuật mã hoá hiện đại

2. Chuẩn mã hoá dữ liệu DES

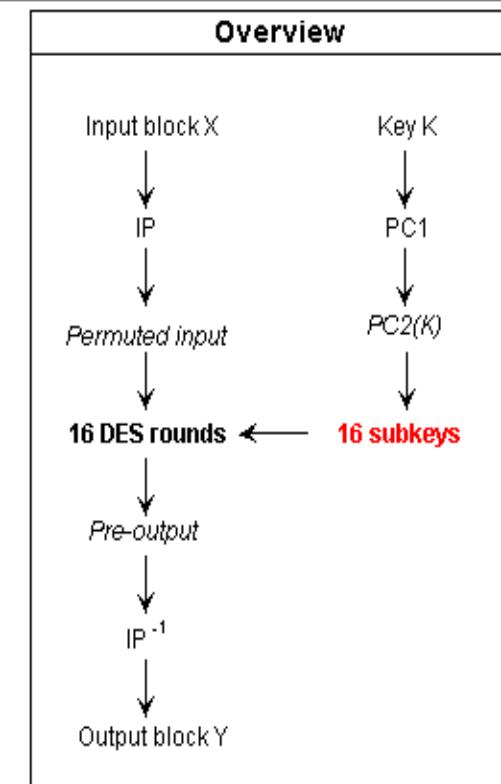
[64-bit]	[64-bit]
Input Block X	Key K
<i>Permuted input</i>	
$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$
$\begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$
$\begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \end{bmatrix}$
$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$
$\begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$
$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$
$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}$
$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \end{bmatrix}$
K[1]	
$\begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$	



4. Giải thuật mã hoá hiện đại

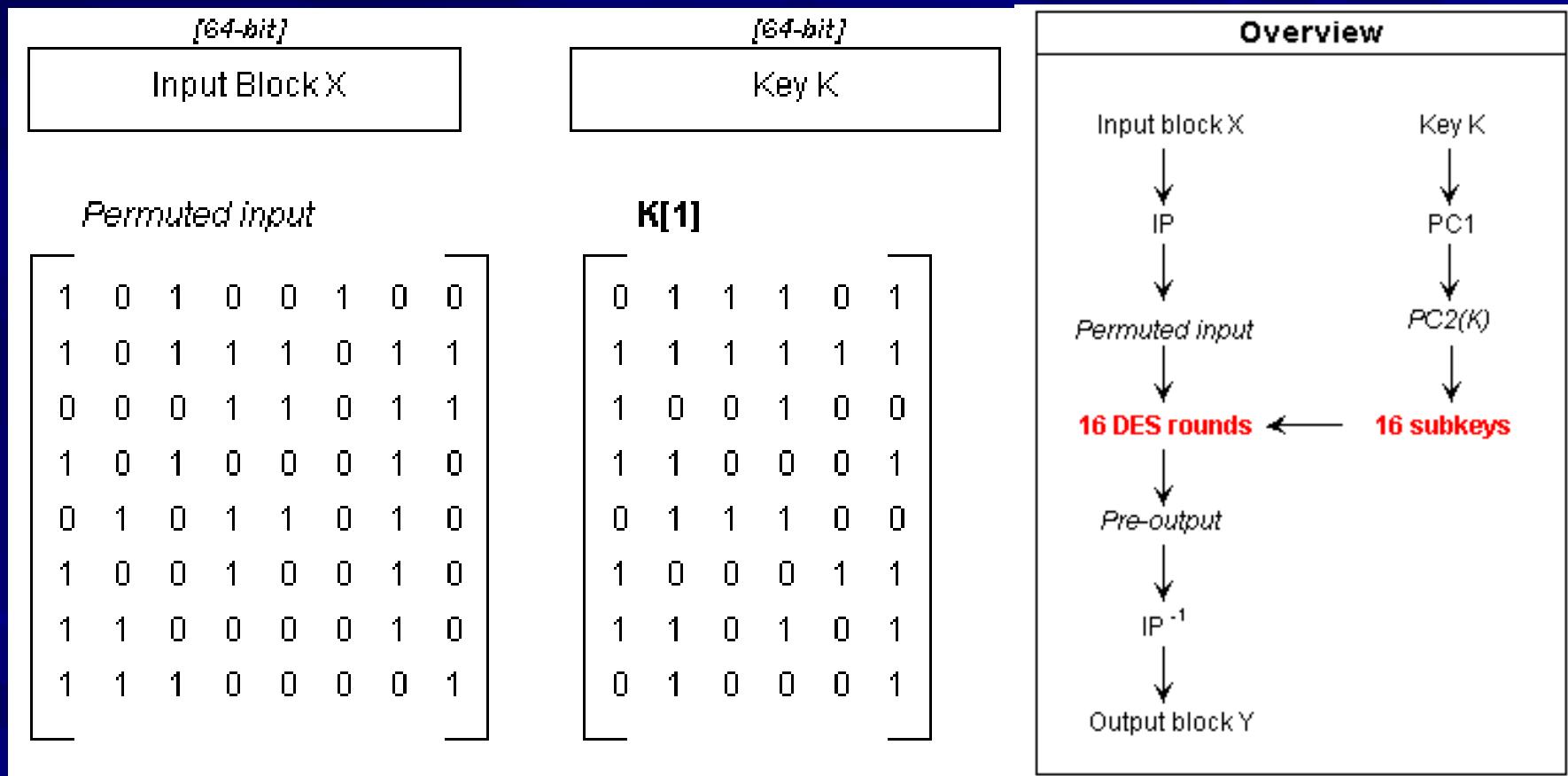
2. Chuẩn mã hoá dữ liệu DES

[64-bit]	[64-bit]
Input Block X	Key K
<i>Permuted input</i>	
$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$
$K[1]$	$K[2]$
$\begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$	$\begin{bmatrix} \quad & \quad & \quad & \quad \end{bmatrix}$
$K[16]$	
$\begin{bmatrix} \quad & \quad & \quad & \quad \end{bmatrix}$	$\begin{bmatrix} \quad & \quad & \quad & \quad \end{bmatrix}$



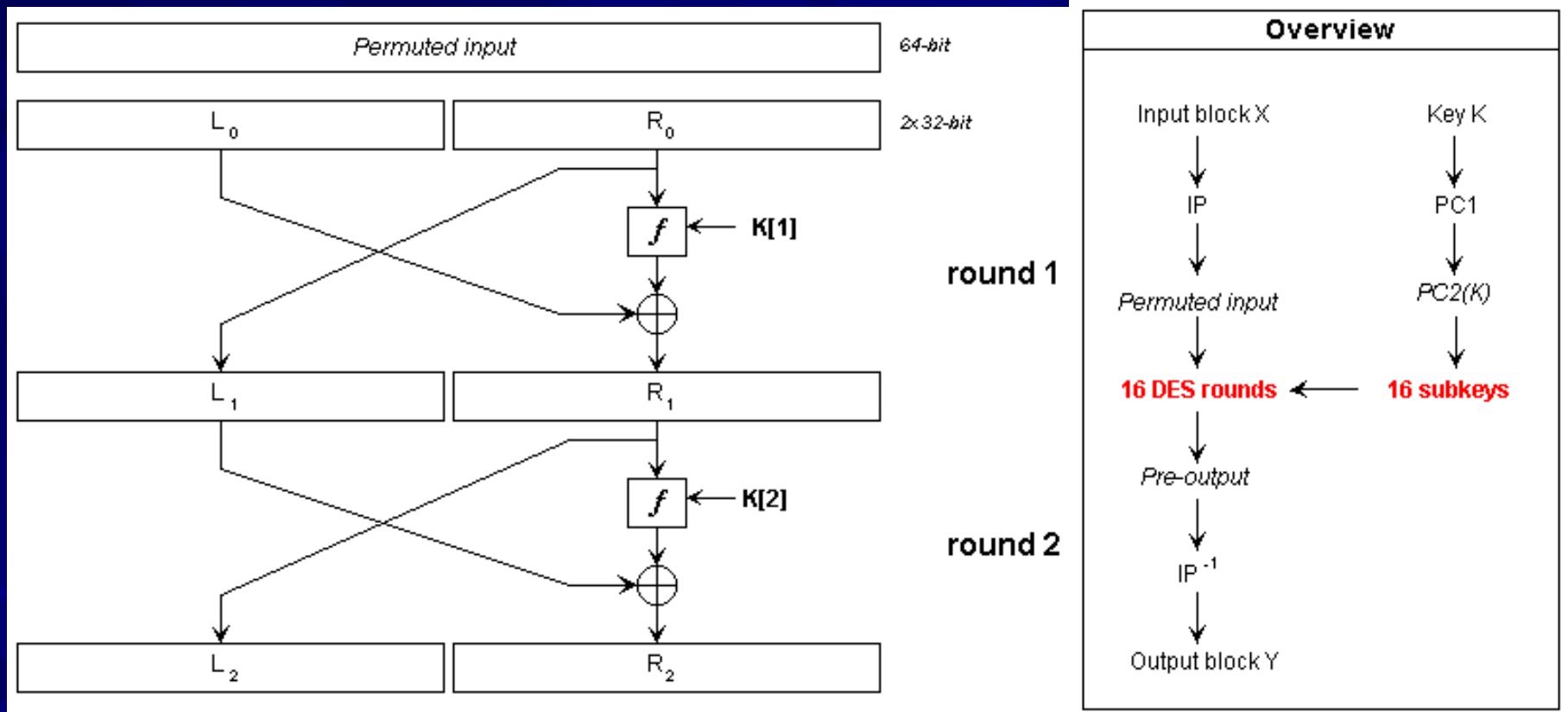
4. Giải thuật mã hoá hiện đại

2. Chuẩn mã hoá dữ liệu DES



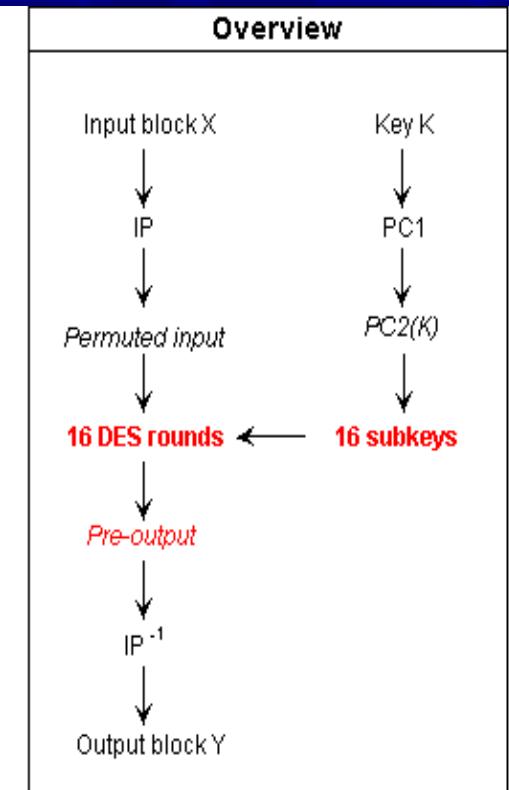
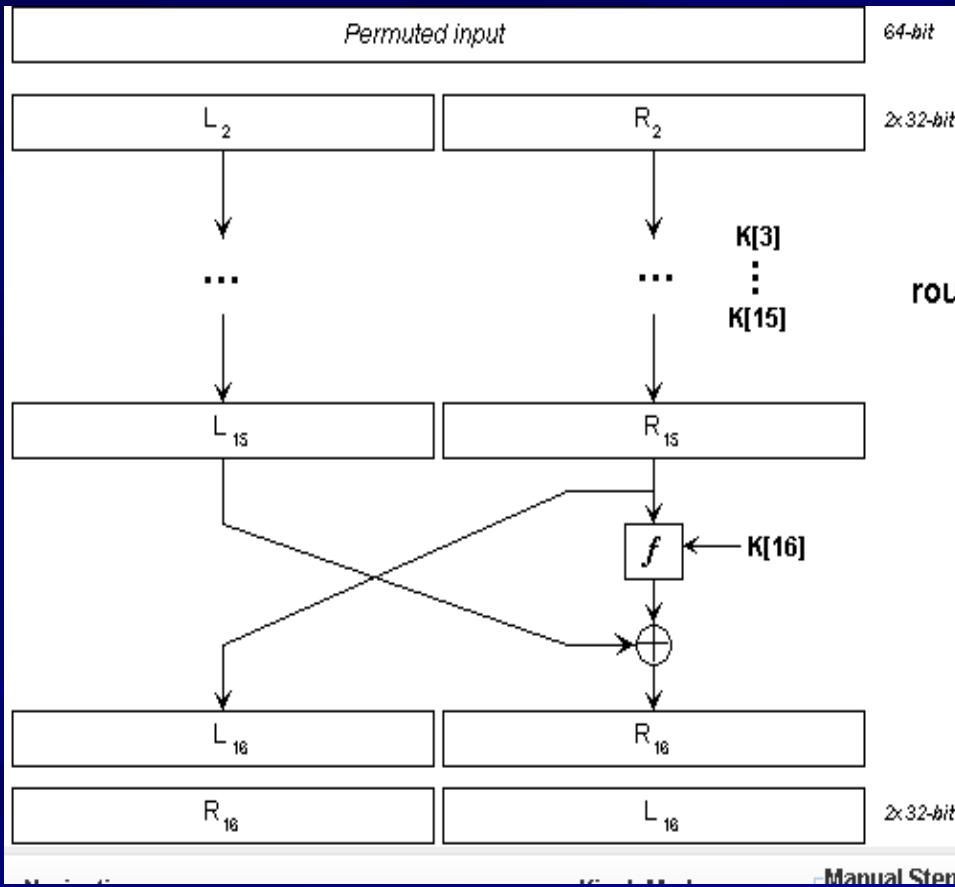
4. Giải thuật mã hoá hiện đại

2. Chuẩn mã hoá dữ liệu DES



4. Giải thuật mã hoá hiện đại

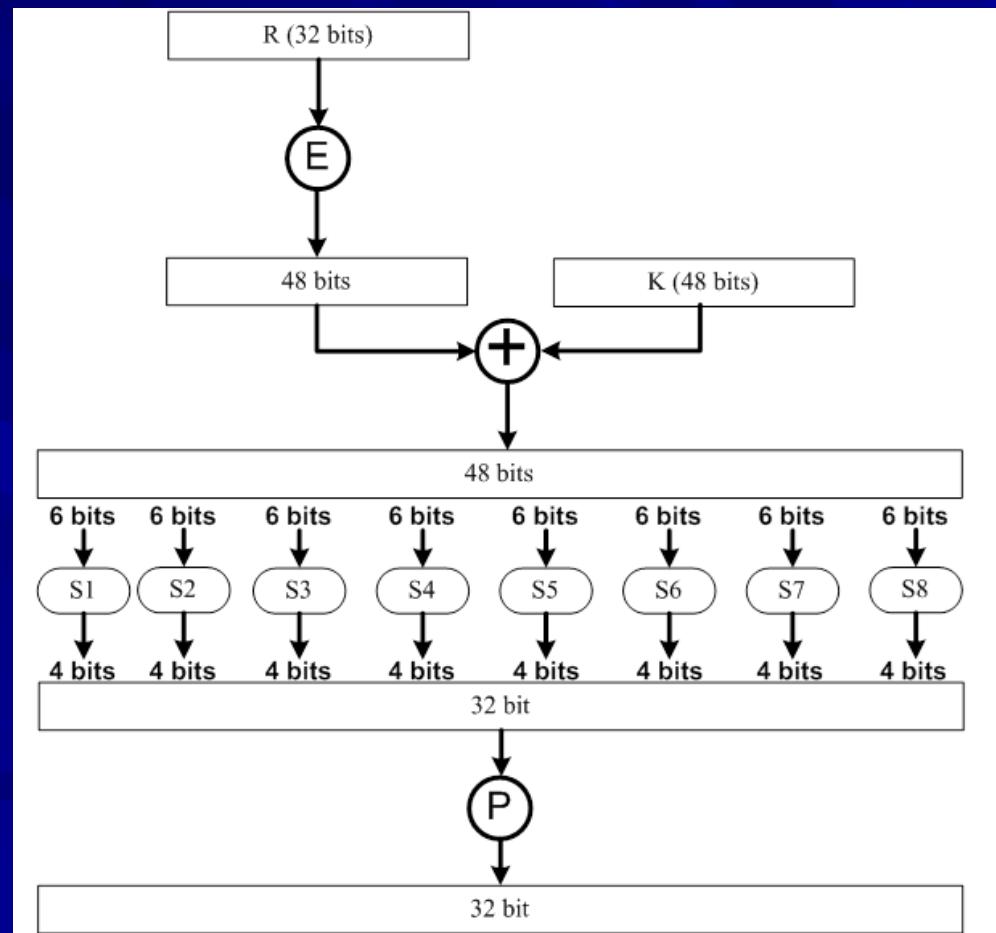
2. Chuẩn mã hoá dữ liệu DES



4. Giải thuật mã hóa hiện đại

2. Chuẩn mã hóa dữ liệu DES

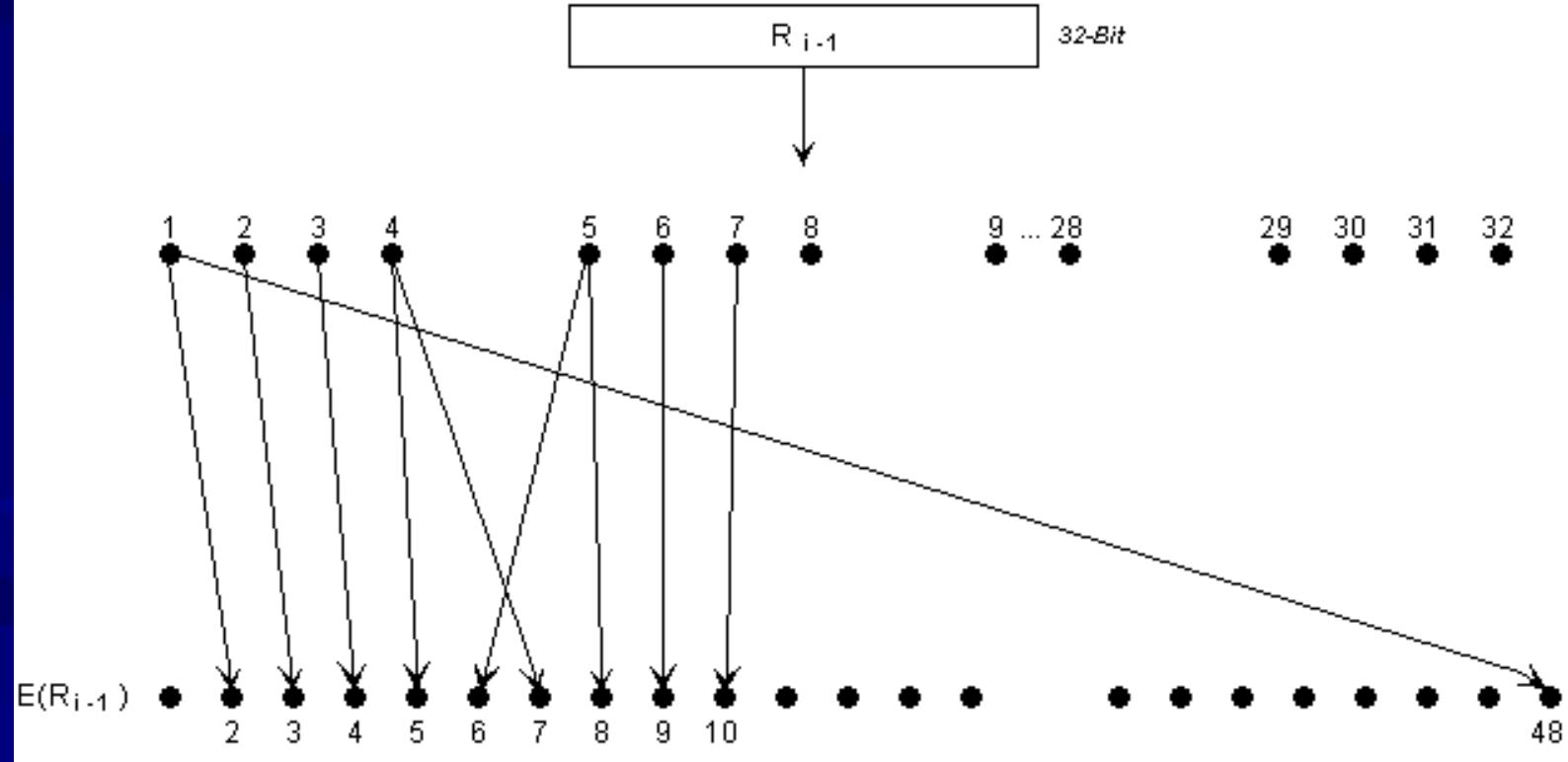
Hàm mã hóa $f(R, K)$



4. Giải thuật mã hoá hiện đại

2. Chuẩn mã hoá dữ liệu DES

Function f :



4. Giải thuật mã hoá hiện đại

2. Chuẩn mã hoá dữ liệu DES

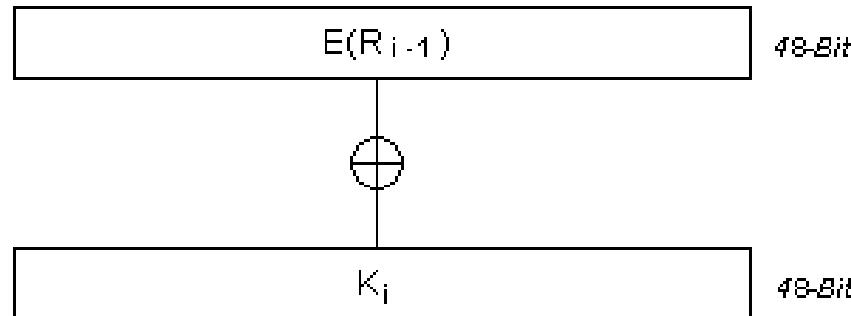
E BIT-SELECTION TABLE

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

4. Giải thuật mã hoá hiện đại

2. Chuẩn mã hoá dữ liệu DES

Function f :



$E(R[0])$	101011	110101	010010	100101	011000	000101	011100	000010
XOR $K[1]$	011101	111111	100100	110001	011100	100011	110101	010001
= B	110110	001010	110110	010100	000100	100110	101001	010011

Below the table, arrows point from each column of the result row to the corresponding $B[i]$ label below it:

\downarrow \downarrow \downarrow \downarrow \downarrow \downarrow \downarrow \downarrow \downarrow

$B[1]$ $B[2]$ $B[3]$ $B[4]$ $B[5]$ $B[6]$ $B[7]$ $B[8]$

4. Giải thuật mã hoá hiện đại

2. Chuẩn mã hoá dữ liệu DES

Function f :

110110	001010	110110	010100	000100	100110	101001	010011
B[1]	B[2]	B[3]	B[4]	B[5]	B[6]	B[7]	B[8]

S-box 1:

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

S-box 8:

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

4. Giải thuật mã hoá hiện đại

2. Chuẩn mã hoá dữ liệu DES

Function f :

110110 001010 110110 010100 000100 100110 101001 010011
B[1] B[2] B[3] B[4] B[5] B[6] B[7] B[8]

7

S-box 1:

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

.

.

.

S-box 8:

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

4. Giải thuật mã hoá hiện đại

2. Chuẩn mã hoá dữ liệu DES

S_1																S_2															
14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3																S_4															
10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5																S_6															
2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7																S_8															
4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Các hàm S (selection function)

4. Giải thuật mã hoá hiện đại

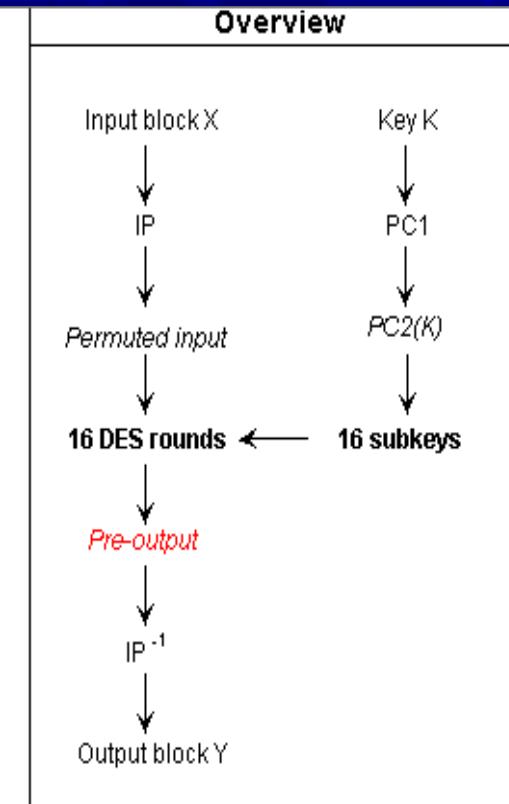
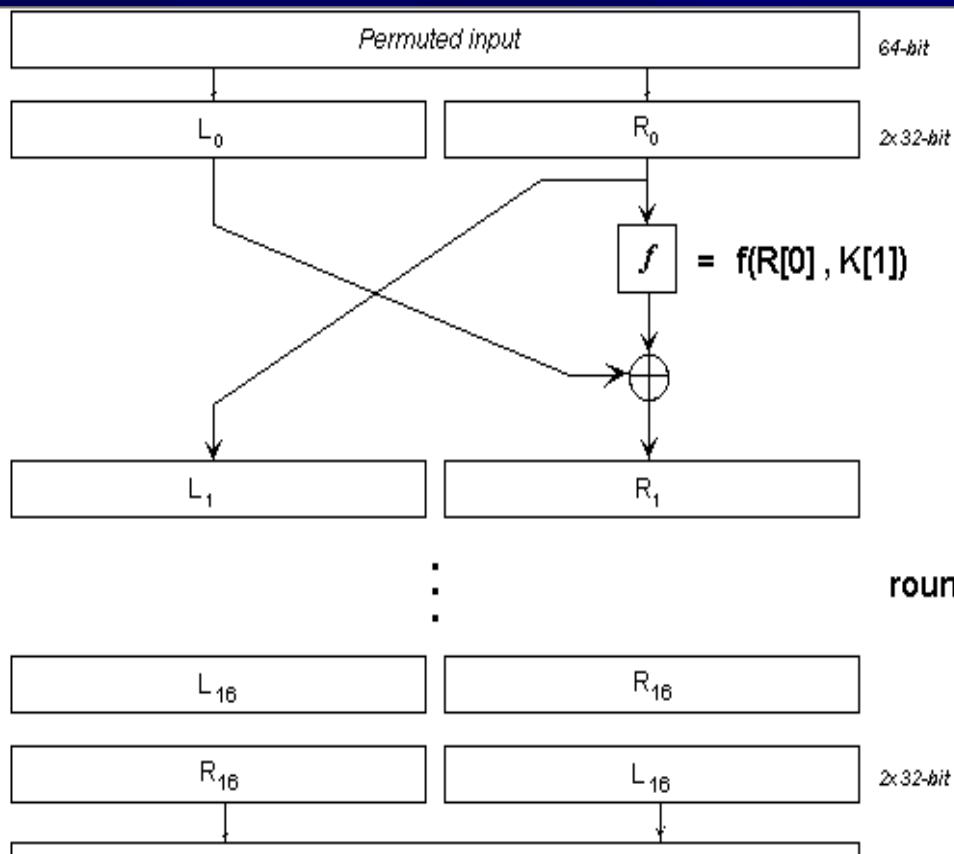
2. Chuẩn mã hoá dữ liệu DES

<u>P</u>			
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

Hoán vị P trong thuật toán tính hàm mã hóa $f(R, K)$

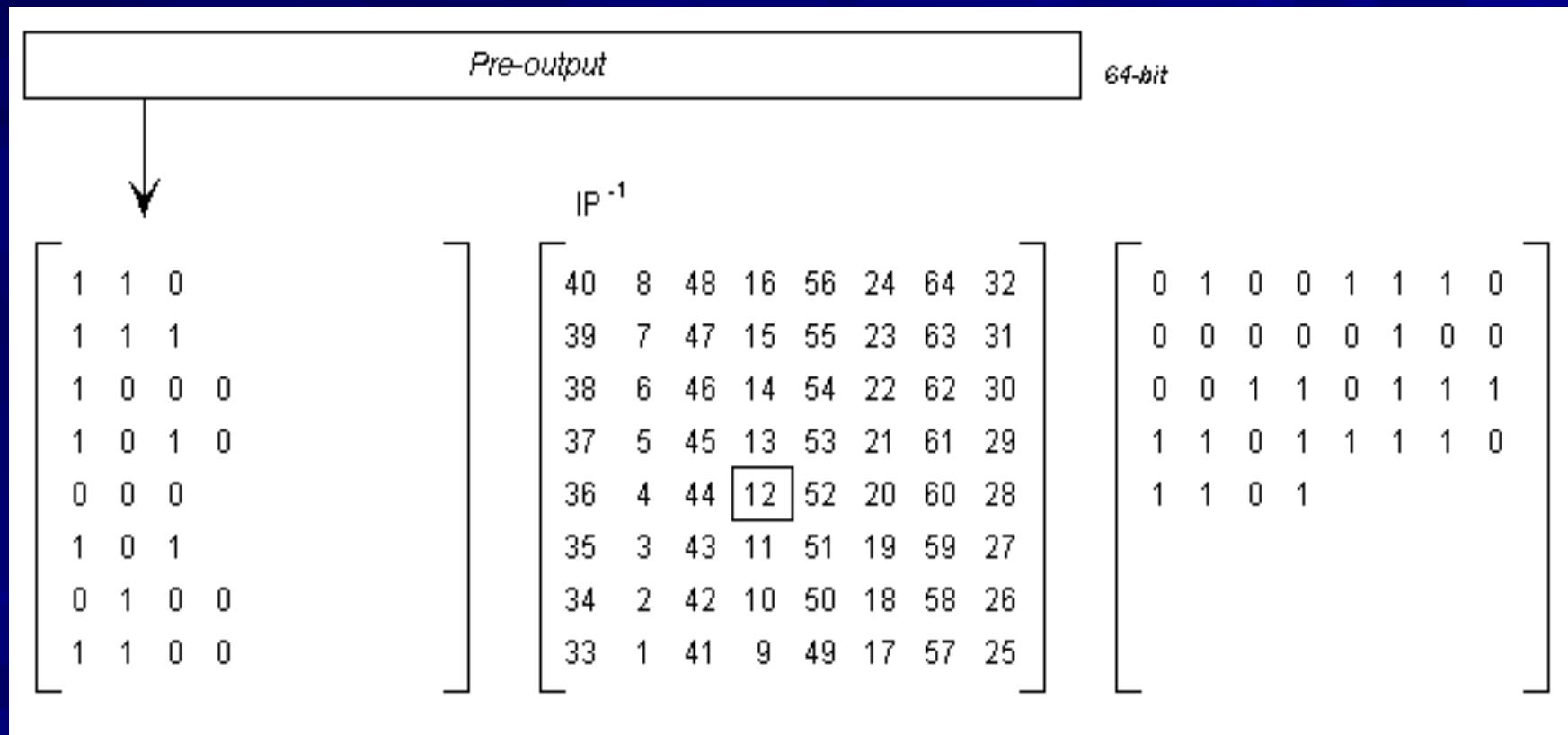
4. Giải thuật mã hoá hiện đại

2. Chuẩn mã hoá dữ liệu DES



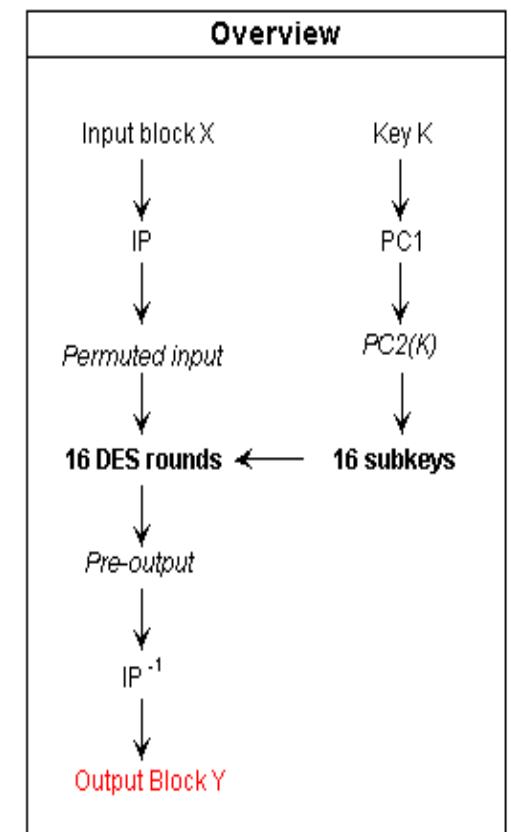
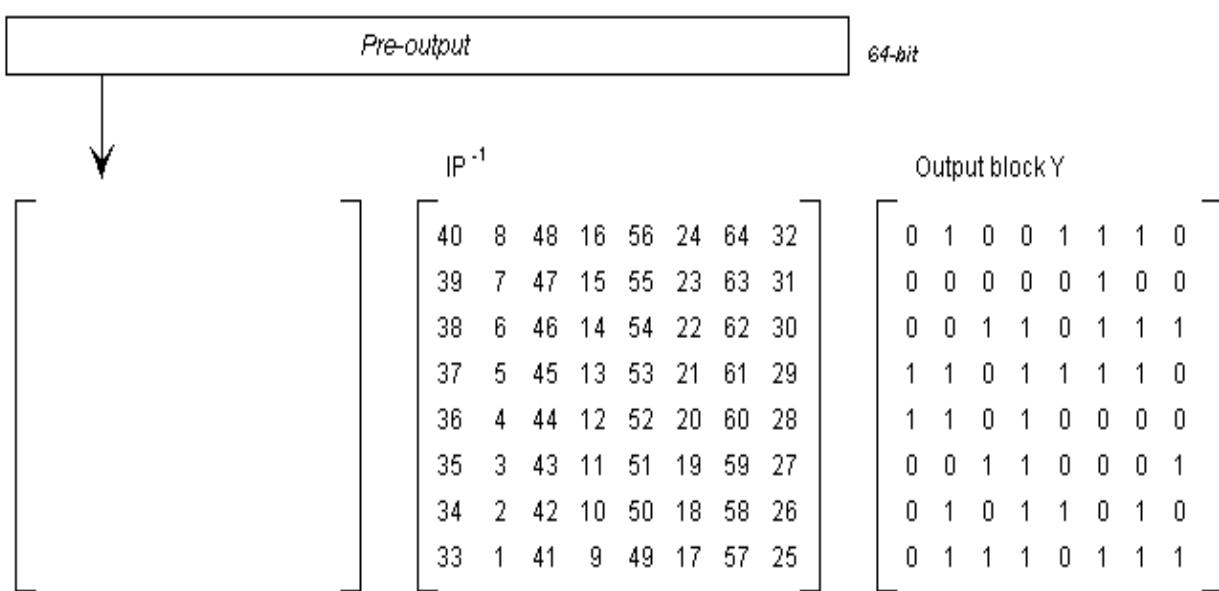
4. Giải thuật mã hoá hiện đại

2. Chuẩn mã hoá dữ liệu DES



4. Giải thuật mã hoá hiện đại

2. Chuẩn mã hoá dữ liệu DES



4. Giải thuật mã hoá hiện đại

3. Giải thuật mã hoá AES

- AES (Advanced Encryption Standard – Tiêu chuẩn mã hoá tiên tiến) là một giải thuật mã hoá khoá đối xứng được công bố năm 2000 để thay thế cho DES. Giải thuật này thực hiện mã hoá khối bằng cách lặp lại nhiều lần các bước xử lý.
- Giải thuật (còn có tên gọi khác là Rijndael) được đề xuất bởi hai nhà mật mã học người Bỉ là Joan Daemen và Vincent Rijmen.

4. Giải thuật mã hoá hiện đại

3. Giải thuật mã hoá AES

- Kích thước khối dữ liệu đầu vào là 128 bit, kích thước khoá lần lượt là 128, 192, 256 bit (AES-128, AES-192, AES-256).
- Mỗi khoá con là một cột gồm 4 bytes.
- Mỗi khối dữ liệu 128 bit đầu vào, tương ứng với 16 bytes, tạo thành một ma trận 4×4 của các byte, gọi là ma trận trạng thái. Ma trận trạng thái này sẽ biến đổi trong quá trình thực hiện mã hoá.

4. Giải thuật mã hoá hiện đại

3. Giải thuật mã hoá AES

AES Pseudocode

```
Cipher (byte in[4*Nb], byte out[4*Nb],
word w[Nb*(Nr+1)])
begin
    byte state[4,Nb]
    state = in
    AddRoundKey(state, w)
    for round = 1 step 1 to Nr-1
        SubBytes(state)
        ShiftRows(state)
        MixColumns(state)
        AddRoundKey(state, w+round*Nb)
    end for
    SubBytes(state)
    ShiftRows(state)
    AddRoundKey(state, w+Nr*Nb)
    out = state
end
```

4. Giải thuật mã hoá hiện đại

3. Giải thuật mã hoá AES

- Hàm SubBytes: mỗi byte trong state được thay thế với các byte khác, sử dụng một bảng look-up được gọi là S-box. S-box được dùng bắt nguồn từ hàm ngược trên trường $GF(2^8)$.
- Hàm ShiftRows: mỗi hàng được chuyển tuần tự với một số lượng bước cố định. Các phần tử của hàng đầu tiên sẽ không thay đổi vị trí, hàng thứ hai dịch sang trái một cột, hàng thứ ba dịch sang trái hai cột, hàng cuối cùng sẽ dịch sang trái ba cột, đảm bảo mỗi cột của bảng đều ra đều được tạo thành từ các cột của bảng trạng thái đầu vào.

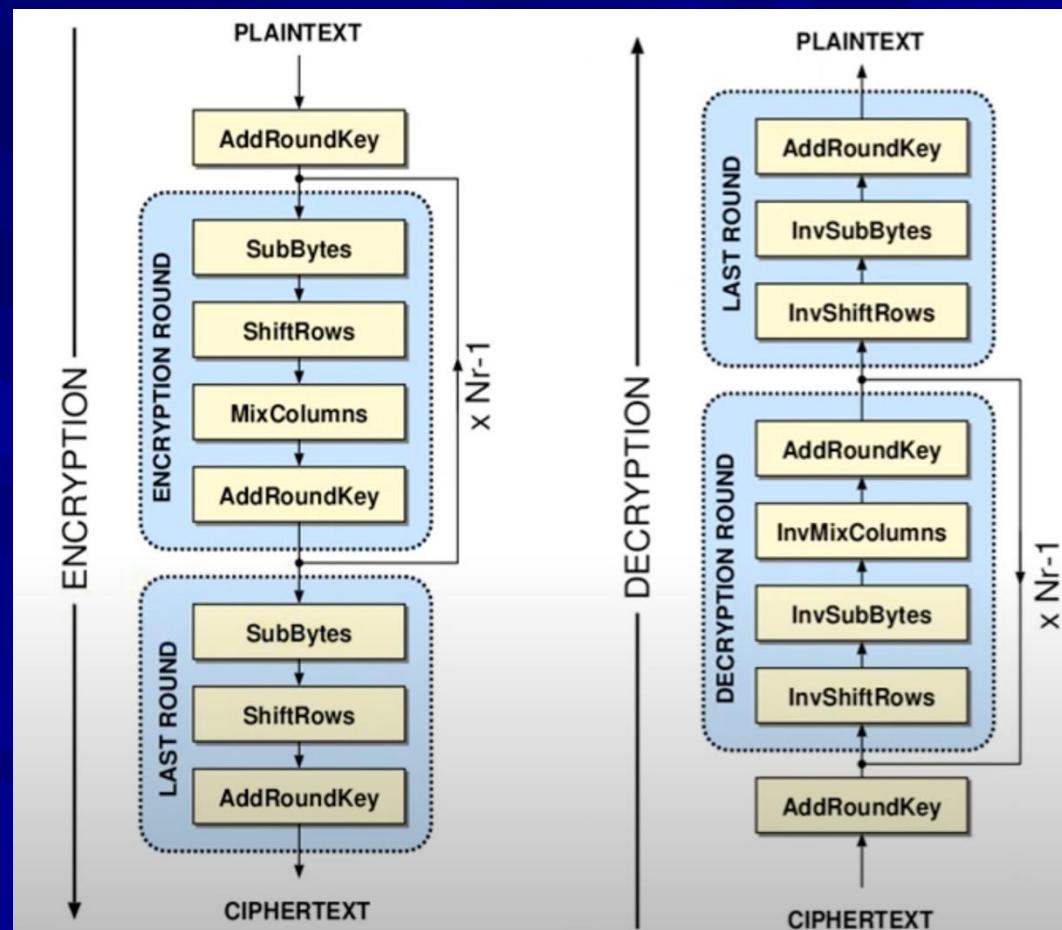
4. Giải thuật mã hoá hiện đại

3. Giải thuật mã hoá AES

- Hàm MixColumns: mỗi cột được chuyển đổi tuyến tính bằng cách nhân nó với một ma trận trong trường hữu hạn. Mỗi cột được xem như một đa thức trong trường $GF(2^8)$ và được nhân modulo $x^4 + 1$ với một biểu thức cố định $c(x)=3x^3+x^2+x+2$.
- Hàm AddRoundKey: mỗi byte trong bảng trạng thái được thực hiện phép XOR với một khoá vòng, quá trình xử lý AES thu được 11 khoá vòng từ các key mã hoá được phân phát cho kỹ thuật mã hoá.

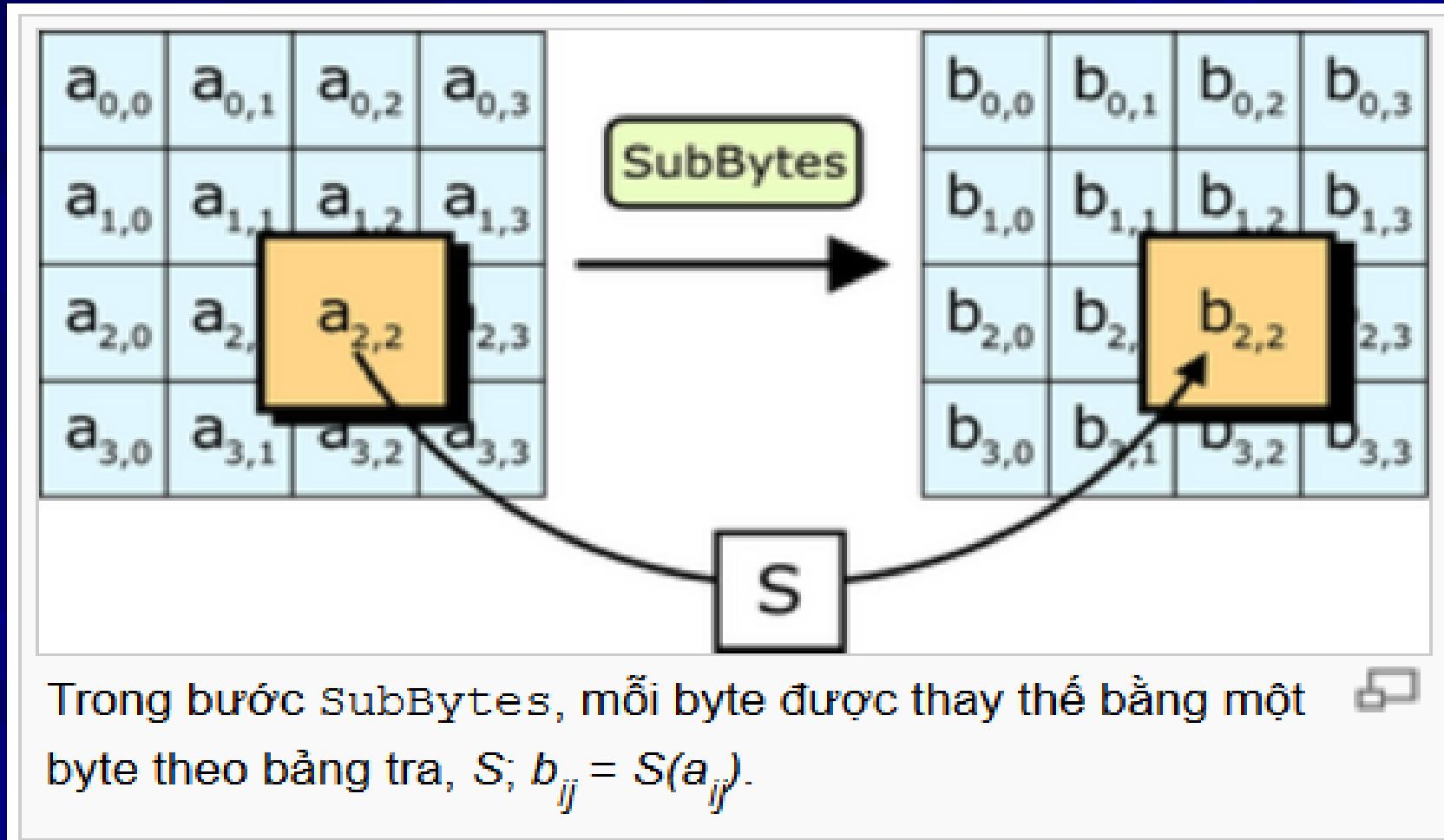
4. Giải thuật mã hoá hiện đại

3. Giải thuật mã hoá AES



4. Giải thuật mã hoá hiện đại

3. Giải thuật mã hoá AES



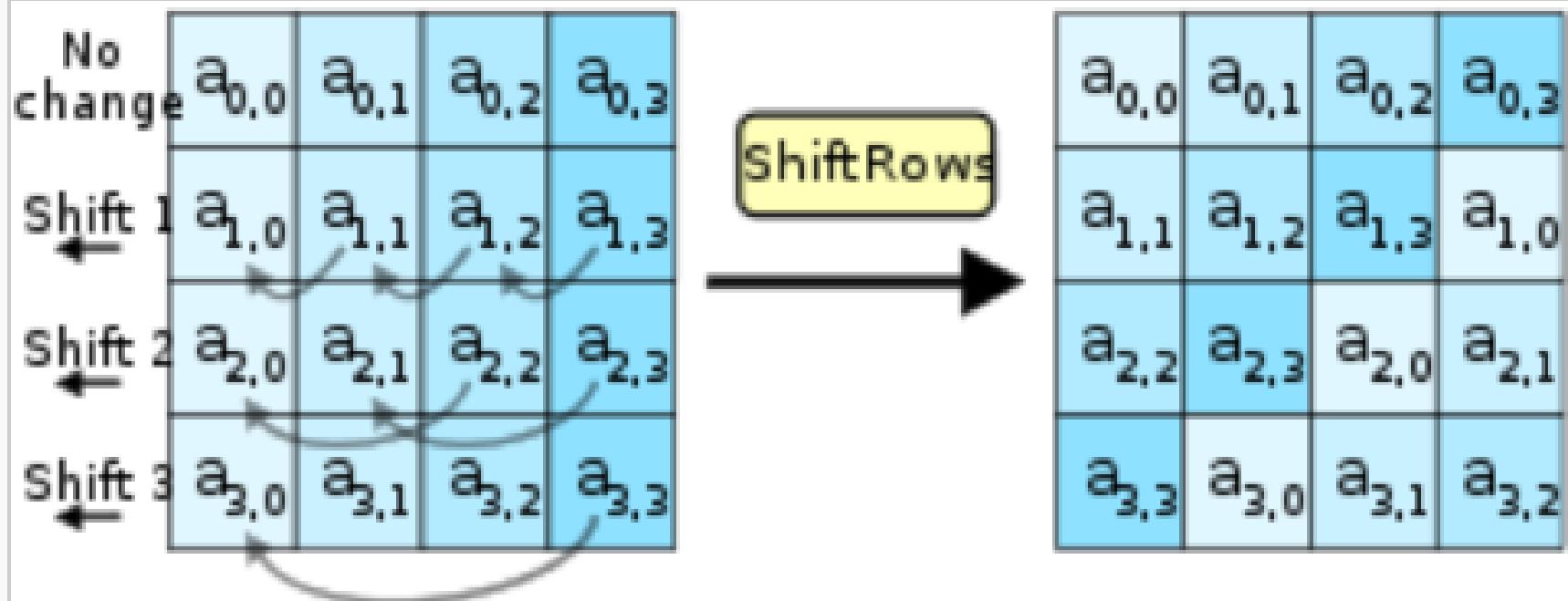
4. Giải thuật mã hoá hiện đại

3. Giải thuật mã hoá AES

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

4. Giải thuật mã hoá hiện đại

3. Giải thuật mã hoá AES

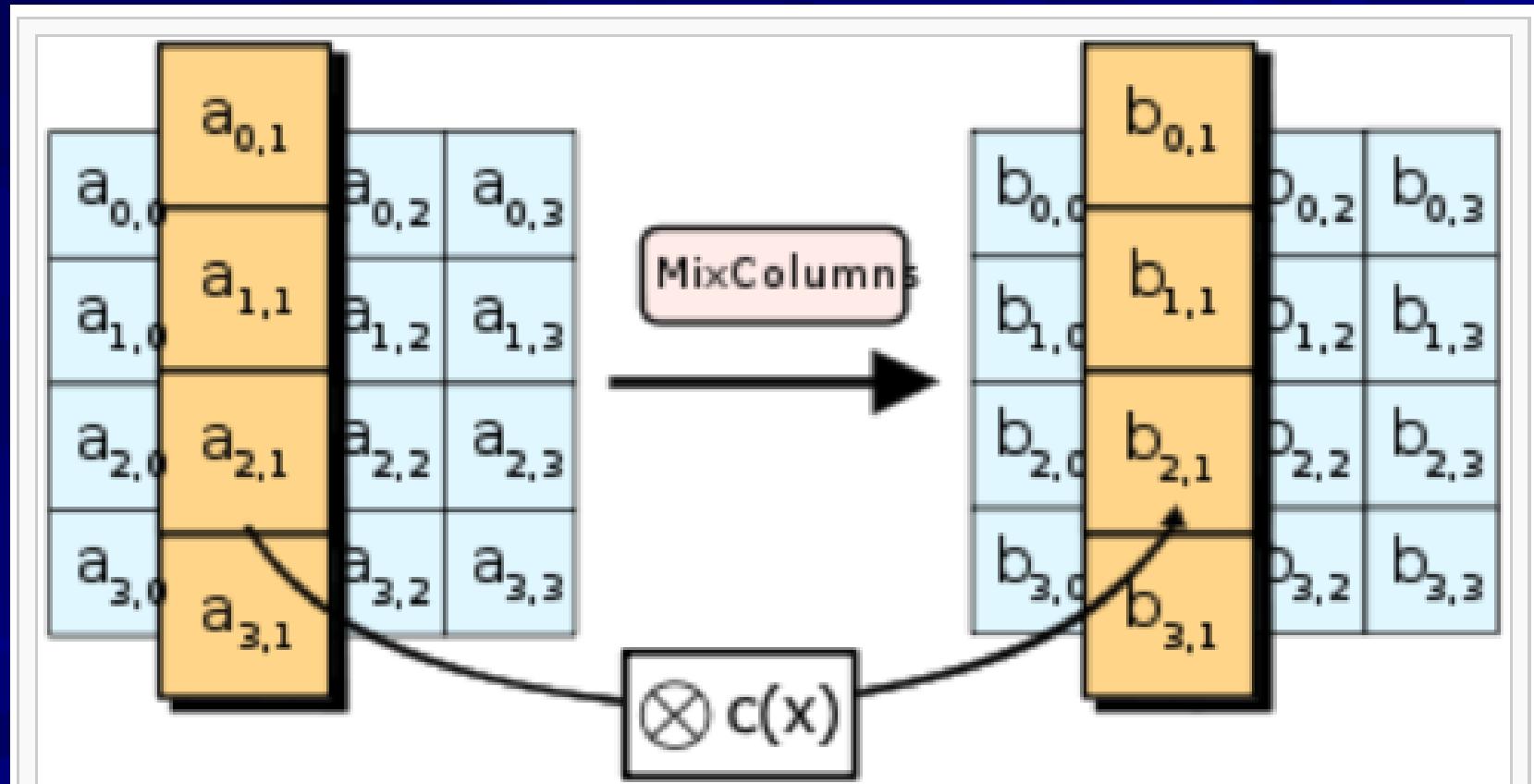


Trong bước ShiftRows, các byte trong mỗi hàng được dịch vòng trái. Số vị trí dịch chuyển tùy thuộc từng hàng.



4. Giải thuật mã hoá hiện đại

3. Giải thuật mã hoá AES

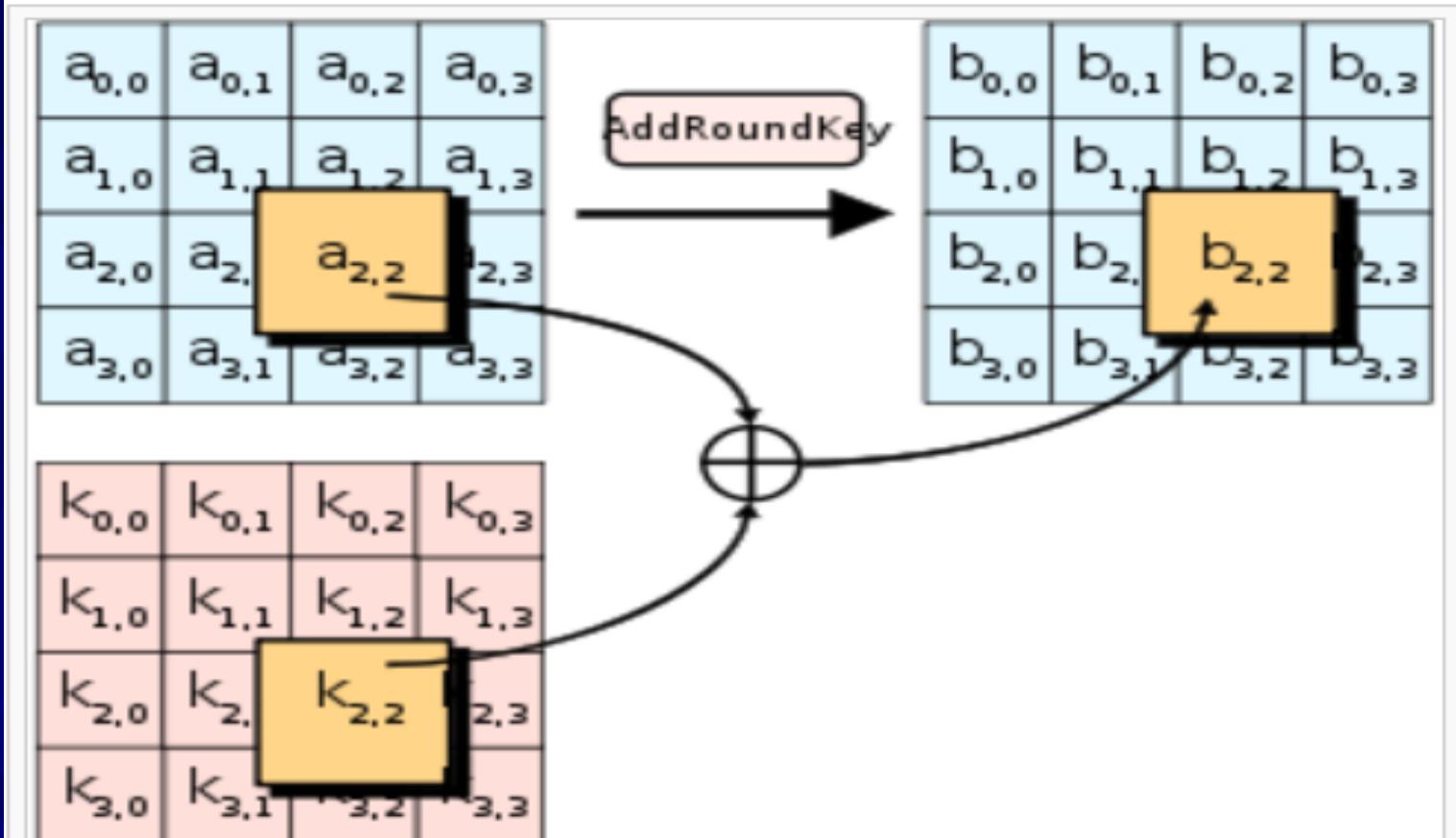


Trong bước MixColumns, mỗi cột được nhân với một hệ số cố định $c(x)$.



4. Giải thuật mã hoá hiện đại

3. Giải thuật mã hoá AES

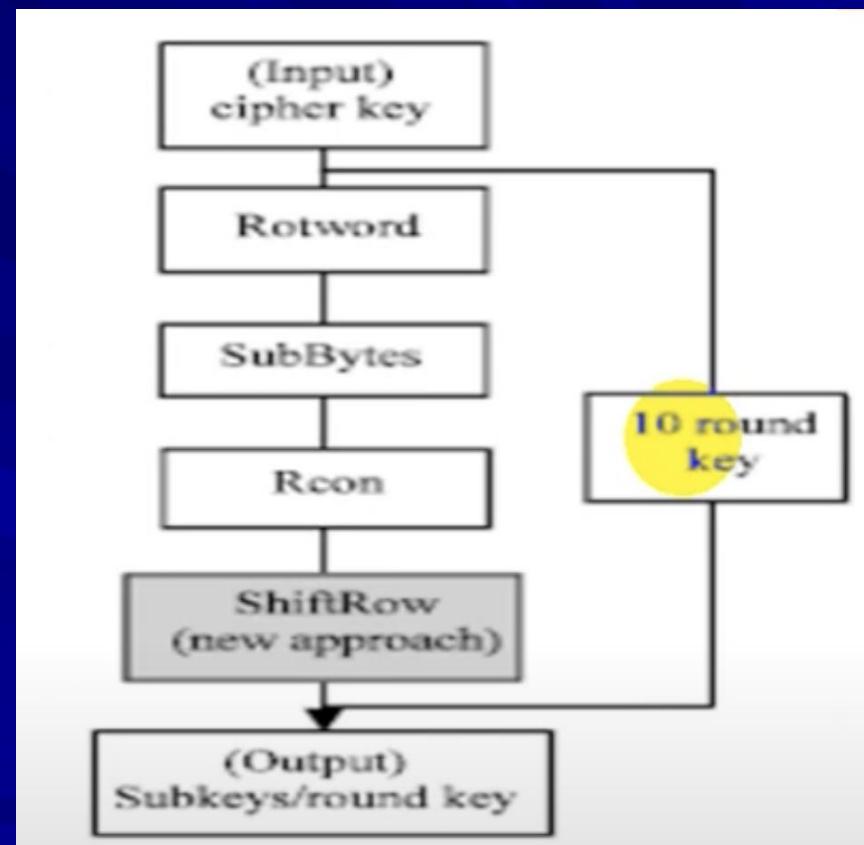


Trong bước AddRoundKey, mỗi byte được kết hợp với một byte trong khóa con của chu trình sử dụng phép toán **XOR** (\oplus).



4. Giải thuật mã hoá hiện đại

3. Giải thuật mã hoá AES



KeyExpansion

4. Giải thuật mã hoá hiện đại

4. Giải thuật mã hoá RC4, RC5, RC6

RC4



A variable **key size stream cipher** with byte-oriented operations, and is based on the use of a random permutation

RC5



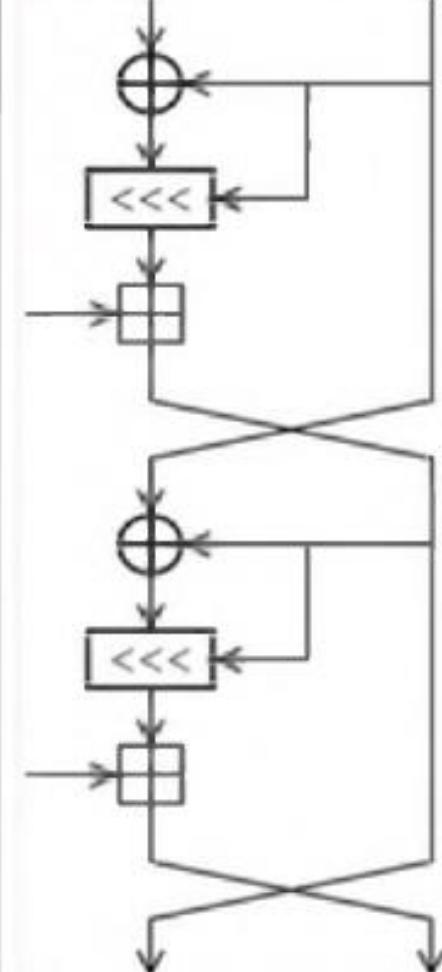
It is a **parameterized algorithm** with a variable block size, a variable key size, and a variable number of rounds. The key size is 128-bits

RC6



RC6 is a symmetric key block cipher derived from RC5 with two additional features:

- Uses Integer multiplication
- Uses four 4-bit working registers (RC5 uses two 2-bit registers)



4. Giải thuật mã hóa hiện đại

5. Hệ mã hóa công khai RSA

- Được sử dụng phổ biến trong thương mại điện tử
- Đảm bảo an toàn với điều kiện độ dài khóa đủ lớn.
- Thuật toán RSA có hai khóa:
 - khóa công khai (hay khóa công cộng)
 - khóa bí mật (hay khóa cá nhân).
- Mỗi khóa là những số cố định sử dụng trong quá trình mã hóa và giải mã.
- Khóa công khai được công bố rộng rãi cho mọi người và được dùng để mã hóa. Những thông tin được mã hóa bằng khóa công khai chỉ có thể được giải mã bằng khóa bí mật tương ứng.

4. Giải thuật mã hoá hiện đại

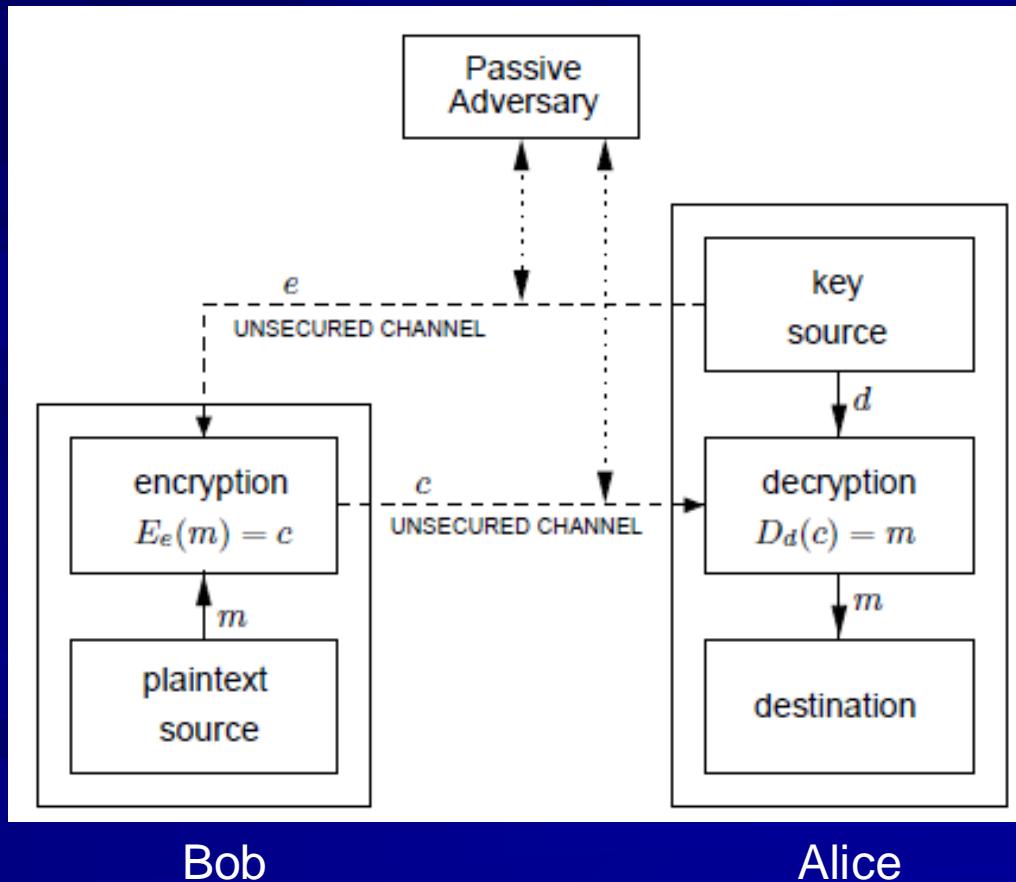
5. Hệ mã hoá công khai RSA

Có thể mô phỏng trực quan một hệ mật mã khoá công khai như sau :

- Bob muốn gửi cho Alice một thông tin mật.
- Alice sẽ gửi cho Bob một chiếc hộp có khóa đã mở sẵn và giữ lại chìa khóa.
- Bob nhận chiếc hộp, cho vào đó một tờ giấy viết thư bình thường và khóa.
- Sau đó Bob gửi chiếc hộp lại cho Alice.
- Alice mở hộp với chìa khóa của mình và đọc thông tin trong thư.
- Trong ví dụ này, chiếc hộp với khóa mở đóng vai trò khóa công khai, chiếc chìa khóa chính là khóa bí mật.

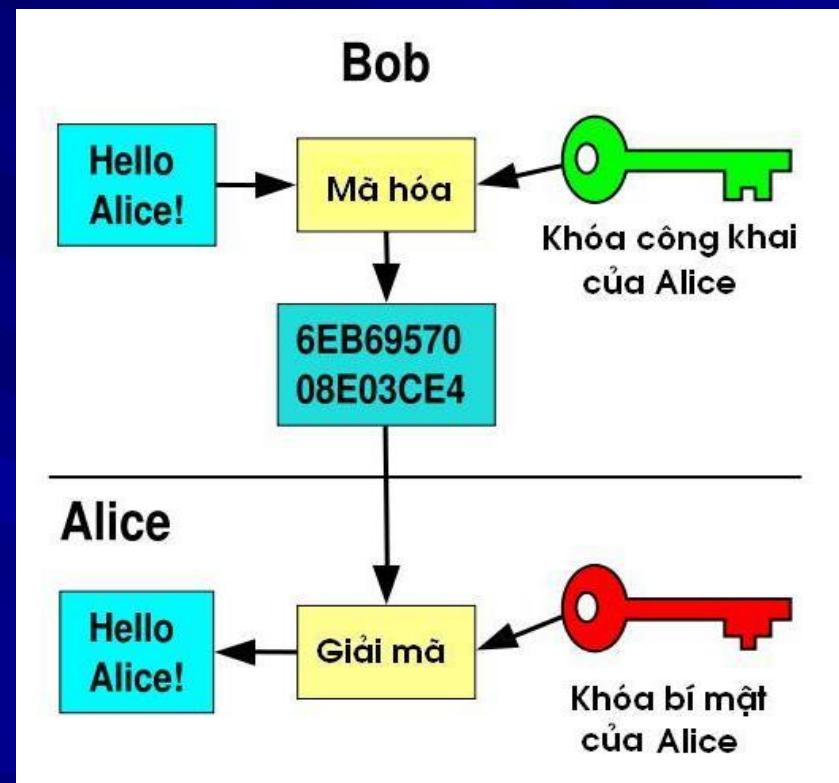
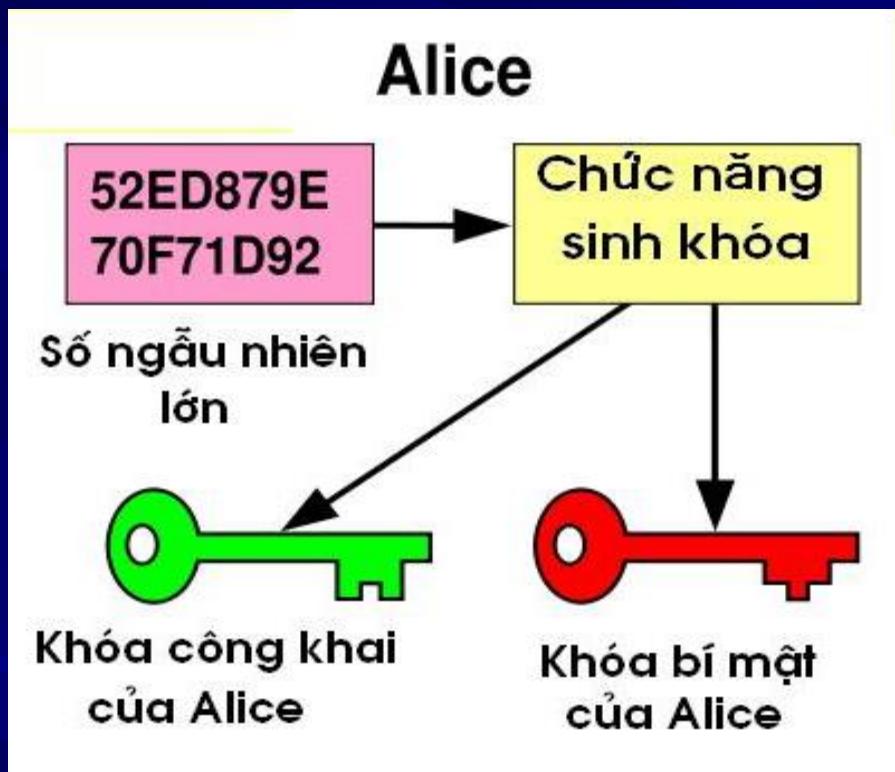
4. Giải thuật mã hoá hiện đại

5. Hệ mã hoá công khai RSA



4. Giải thuật mã hoá hiện đại

5. Hệ mã hoá công khai RSA



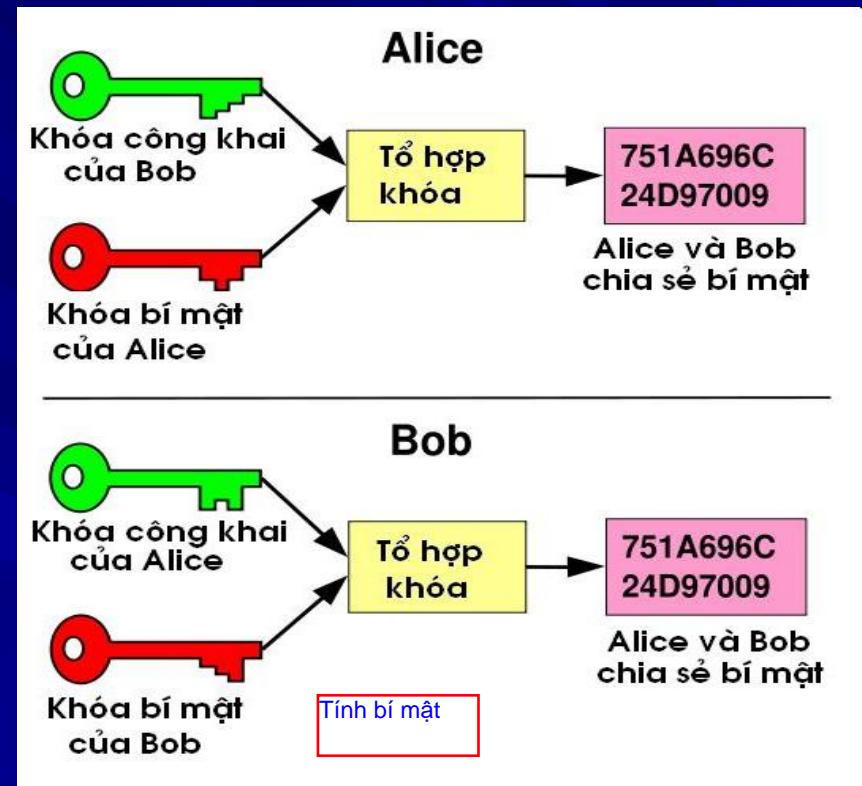
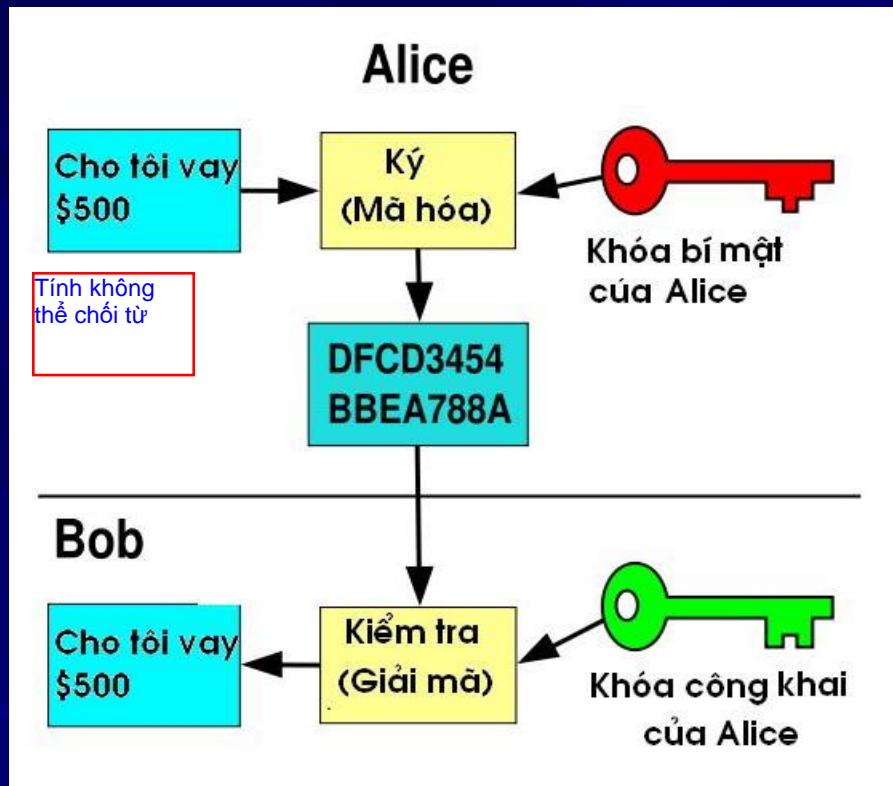
Chọn một số ngẫu nhiên lớn để sinh cặp khóa.

TÍNH BÍ MẬT
CỦA THÔNG
TIN

Dùng khoá công khai để mã hóa,
nhưng dùng khoá bí mật để giải mã.

4. Giải thuật mã hoá hiện đại

5. Hệ mã hoá công khai RSA



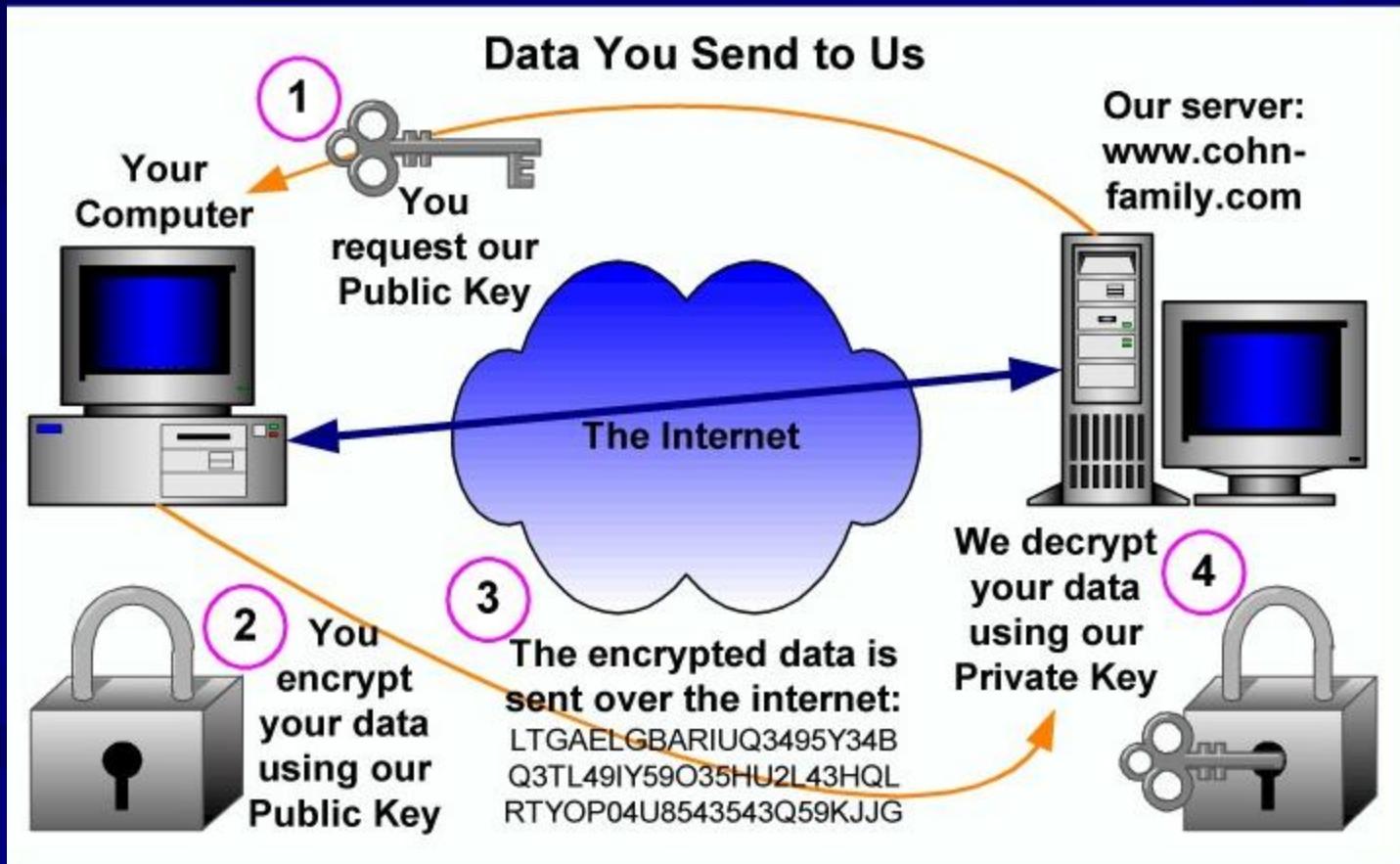
Dùng khoá bí mật để ký một thông báo; dùng
khoá công khai để xác minh chữ ký.

Tổ hợp khoá bí mật của mình với khoá bí
mật của người khác tạo ra khoá dùng
chung chỉ hai người biết.

Tạo ra 1 khoá
bí mật (bàn
giao)

4. Giải thuật mã hoá hiện đại

5. Hệ mã hoá công khai RSA



4. Giải thuật mã hoá hiện đại

5. Hệ mã hoá công khai RSA

```
P = 61    <= first prime number (destroy this after computing E and D)
Q = 53    <= second prime number (destroy this after computing E and D)
PQ = 3233 <= modulus (give this to others)
E = 17    <= public exponent (give this to others)
D = 2753  <= private exponent (keep this secret!)

Your public key is (E,PQ).
Your private key is D.
```

The encryption function is: $\text{encrypt}(T) = (T^E) \bmod PQ$
 $= (T^{17}) \bmod 3233$

The decryption function is: $\text{decrypt}(C) = (C^D) \bmod PQ$
 $= (C^{2753}) \bmod 3233$

To encrypt the plaintext value 123, do this:

```
encrypt(123) = (123^17) mod 3233
                = 337587917446653715596592958817679803 mod 3233
                = 855
```

To decrypt the cipher text value 855, do this:

```
decrypt(855) = (855*2753) mod 3233
                = 123
```



4. Giải thuật mã hoá hiện đại

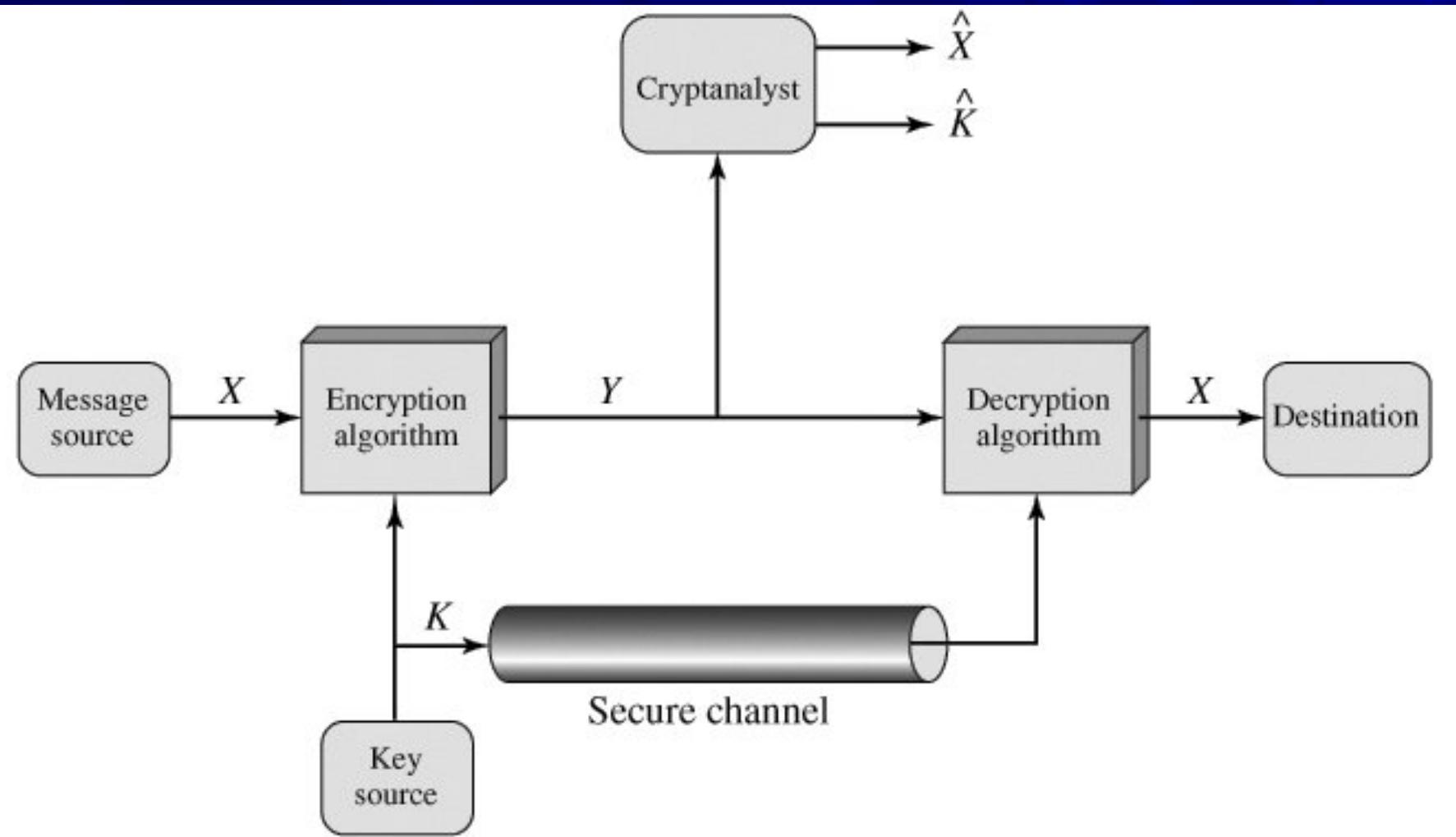
5. Hệ mã hoá công khai RSA

- Các giải thuật mã hoá DES và RSA còn được ứng dụng vào chữ ký điện tử.
- Giải thuật RSA là rất an toàn nhưng tốc độ mã hoá và giải mã chậm hơn giải thuật DES hàng ngàn lần.
- Thông thường người ta thường kết hợp hai phương pháp mã hoá DES và RSA như sau:
 - DES mã hoá khối văn bản.
 - RSA để mã hoá khoá mà DES đã dùng để mã hoá khối văn bản.

5. Bẻ gãy một hệ thống mật mã

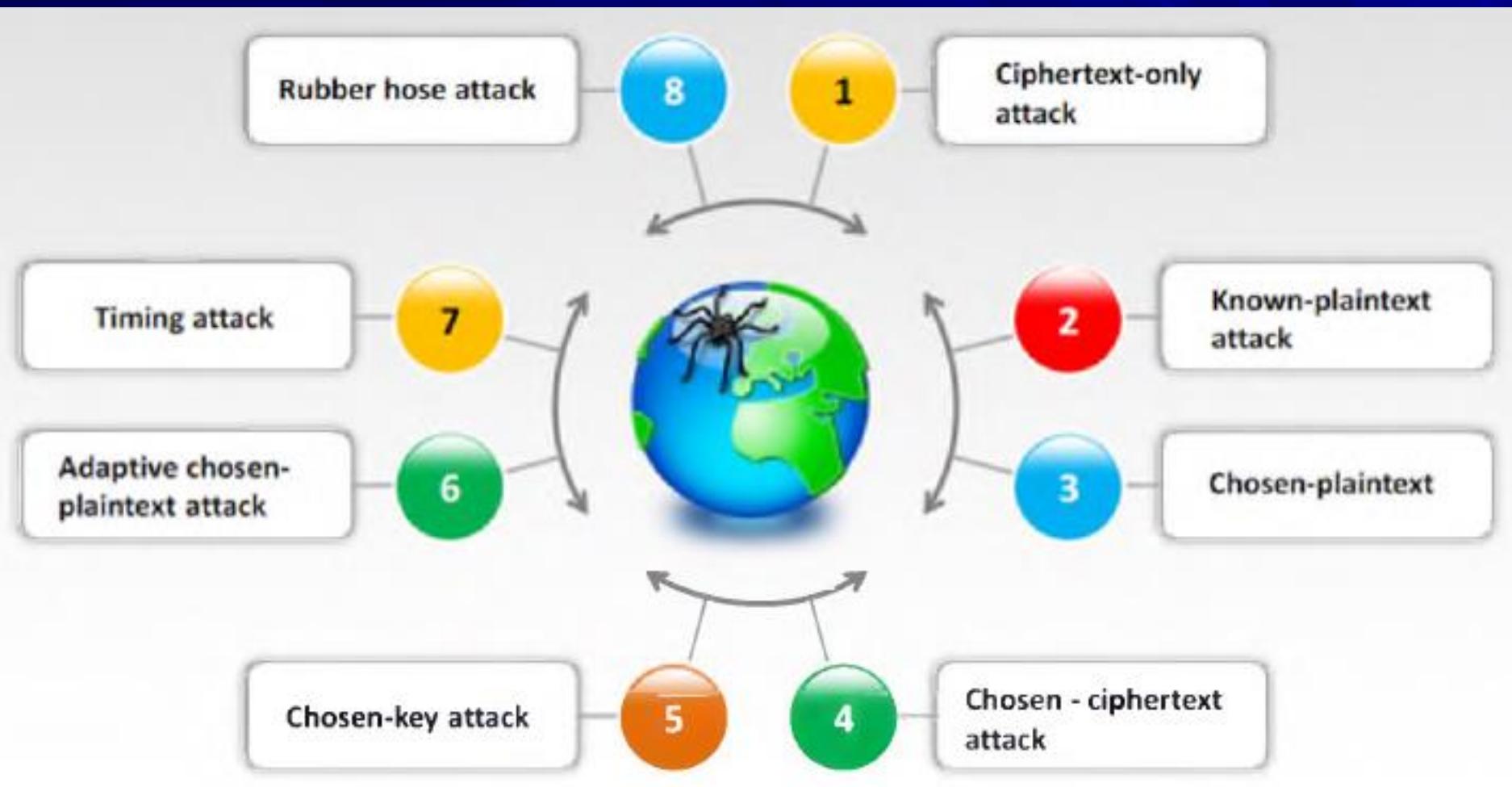
- Những chuyên gia mật mã hay những kẻ tấn công thường được giả thiết biết đầy đủ thông tin về hàm mã hoá e và hàm giải mã d.
- Các chuyên gia này cũng có thể có thêm nhiều thông tin hỗ trợ như các thống kê về ngôn ngữ, kiến thức về ngôn ngữ cảnh...
- Với một chuỗi mật mã nào đó, họ thiếu khoá k để có thể sử dụng d để giải mã c một cách chính xác.

5. Bẻ gãy một hệ thống mật mã



5. Bẻ gãy một hệ thống mật mã

Các khả năng tấn công trên hệ thống:



5. Bẻ gãy một hệ thống mật mã

Các khả năng tấn công trên hệ thống:

- Tấn công chỉ dựa trên chuỗi mật mã (cryptogram-only attack): đối phương chỉ biết một vài mẫu chuỗi mật mã c.
- Tấn công dựa trên văn bản đã biết (known-plaintext attack): Trong trường hợp này những người tấn công được giả thiết là đã biết một độ dài đáng kể của văn bản thông báo và chuỗi mật mã tương ứng, và từ đó cố gắng tìm ra khoá.
- Tấn công dựa trên văn bản được chọn (chosen-plaintext attack): những người tấn công có thể đã có được một số lượng tuỳ ý của các cặp thông báo và chuỗi mật mã tương ứng (m, c).

5. Bẻ gãy một hệ thống mật mã

Các khả năng tấn công trên hệ thống:

Kiểu tấn công	Đối phương nắm được
ciphertext only attack	Chỉ văn bản mã c
known plaintext attack	Cả văn bản nguồn p và văn bản mã c
chosen plaintext attack	Đột nhập được vào máy mã hoá . Tự chọn văn bản p và mã hoá lấy được văn bản mã c tương ứng.
chosen ciphertext attack	Đột nhập được vào máy giải mã . Tự chọn văn bản mã c và giải mã lấy được văn bản p tương ứng.

5. Bẻ gãy một hệ thống mật mã

Thời gian trung bình để tìm khoá theo kiểu vét cạn

Key size (bits)	Number of alternative keys	Time required at 1 decryption/μs	Time required at 10^6 decryption/μs
32	$2^{32} = 4.3 \times 10^9$	$2^{31} \mu\text{s} = 35.8$ minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55} \mu\text{s} = 1142$ years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127} \mu\text{s} = 5.4 \times 10^{24}$ years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167} \mu\text{s} = 5.9 \times 10^{36}$ years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26} \mu\text{s} = 6.4 \times 10^{12}$ years	6.4×10^6 years

5. Bẻ gãy một hệ thống mật mã

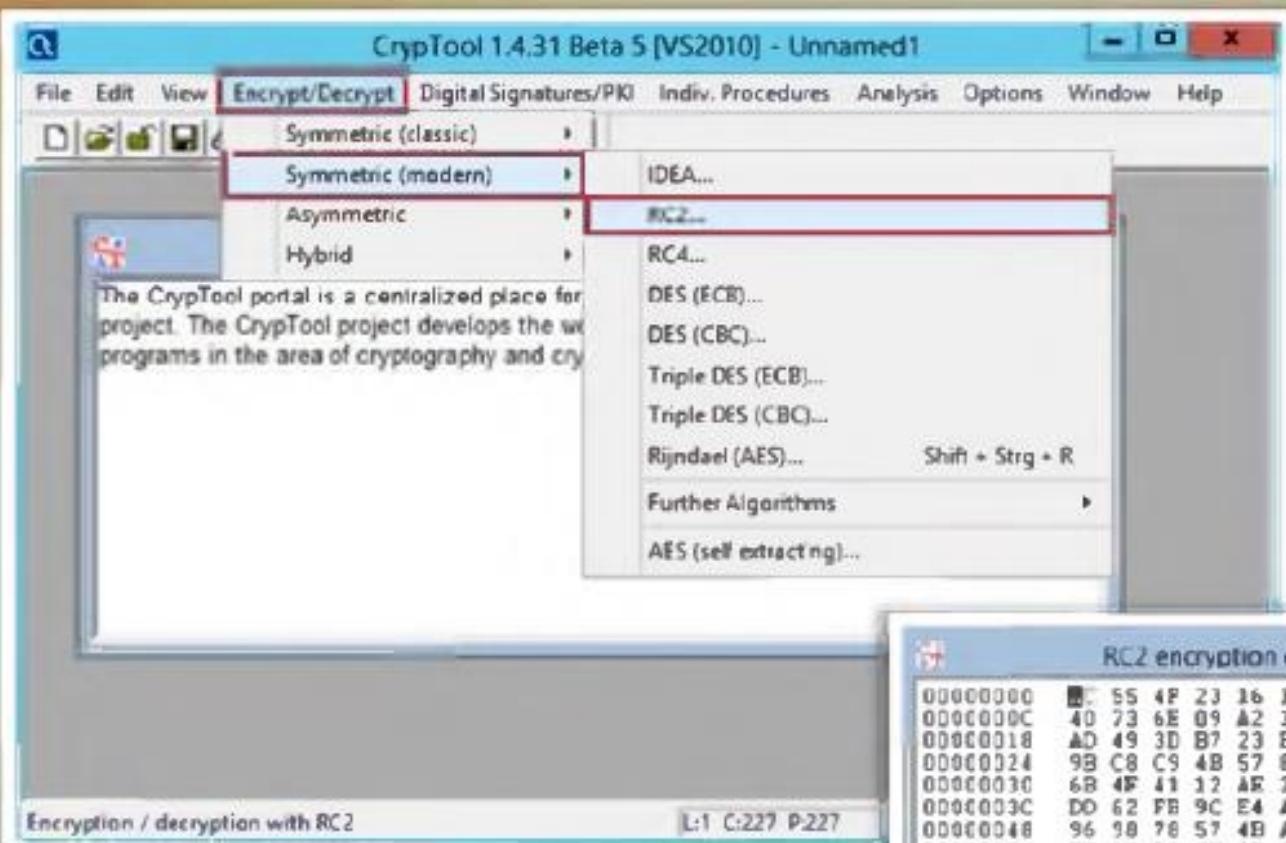
Thời gian trung bình để tìm khoá theo kiểu vét cạn

Power/Cost	40 bits (5 char)	56 bit (7 char)	64 bit (8 char)	128 bit (16 char)
\$ 2K (1 PC. Can be achieved by an individual)	1.4 min	73 days	50 years	10^{20} years
\$ 100K (this can be achieved by a company)	2 sec	35 hours	1 year	10^{19} years
\$ 1M (Achieved by a huge organization or a state)	0.2 sec	3.5 hours	37 days	10^{18} years

Estimate Time for Successful Brute-force Attack

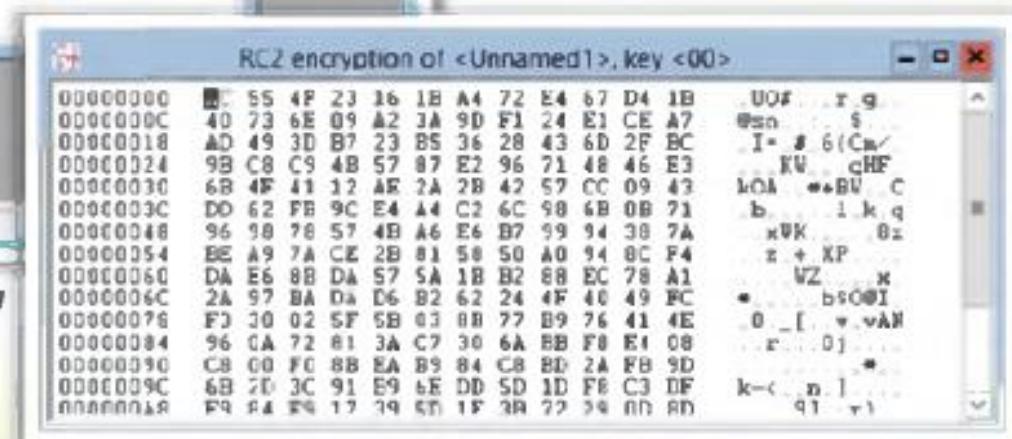
5. Bẻ gãy một hệ thống mật mã

Công cụ phân tích Cryptool



The screenshot shows the Cryptool 1.4.31 Beta 5 interface. The main window title is "CryptTool 1.4.31 Beta 5 [VS2010] - Unnamed1". The "Encrypt/Decrypt" menu is highlighted, and its sub-menu "Symmetric (modern)" is open, with "RC2..." selected. A tooltip message in the center-left says: "The CrypTool portal is a centralized place for project. The CrypTool project develops the software programs in the area of cryptography and cry...". At the bottom left, it says "Encryption / decryption with RC2". Below the main window, the URL <http://www.cryptool.org> is displayed.

- CrypTool is a free e-learning program in the area of **cryptography** and **cryptoanalysis**
- Subprojects of CrypTool:
 - CrypTool 1 (CT1)
 - CrypTool 2 (CT2)
 - JCrypTool (JCT)
 - CrypTool-Online (CTO)

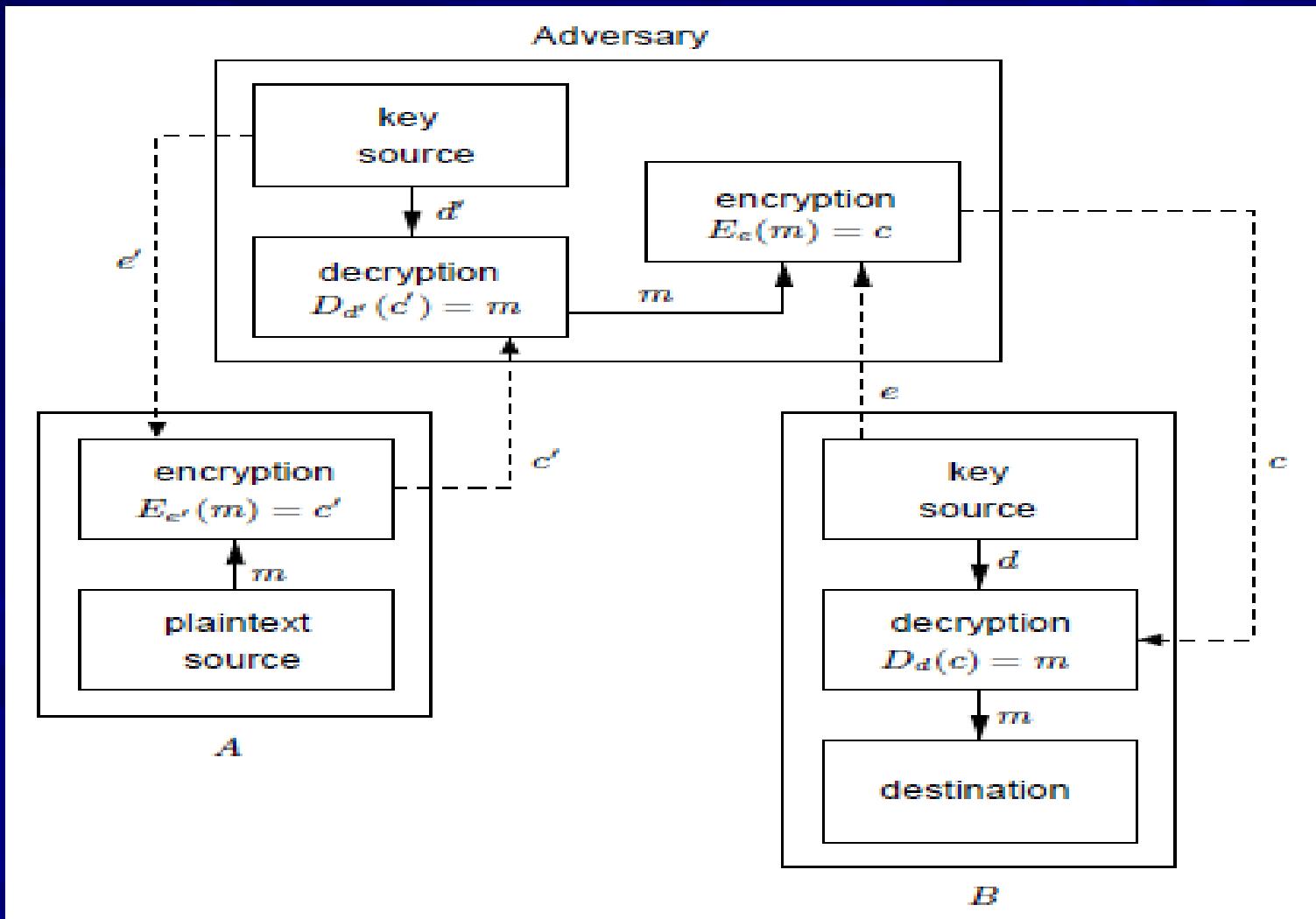


This window displays the results of an RC2 encryption operation. The title bar reads "RC2 encryption of <Unnamed1>, key <00>". The content area shows a grid of hex values representing the encrypted data. The first few rows of data are:

Index	00000000	0000000C	00000018	00000024	00000030	0000003C	00000048	00000054	00000060	0000006C	00000076	00000084	00000090	0000009C	000000A8
0	55 4F 23 16 1B A4 72 E4 67 D4 1B 00F r g	40 73 6E 09 A2 3A 9D F1 24 E1 CE A7 00n s	AD 49 3D B7 23 B5 36 28 43 6D 2F BC I= # 6(Cm/	98 C8 C9 4B 57 87 E2 96 71 48 46 E3 KU CHF	6B 4F 41 12 A8 2A 2B 42 57 CC 09 43 MOA *+BV C	62 FB 9C E4 A4 C2 6C 98 6B 0B 71 b l k q	96 98 78 57 4B A6 E6 B7 99 94 38 7A xVK Bi	A9 7A CE 2B 81 58 50 A0 94 8C F4 z + XP	E6 8B DA 57 5A 1B B2 88 EC 78 A1 VZ x	97 BA DA D6 B2 62 24 4F 40 49 FC * b508I	30 02 5F 5B 03 0B 77 B9 76 41 4E 0 _ [v.vAN	CA 72 81 3A C7 30 6A BB F8 E1 08 r D1 *	00 4C 8B EA B9 84 C8 BD 2A FB 9D k- c n 1	2D 3C 91 E9 6E DD SD 1D FB C3 DF q1 v1	F9 FA FG 17 39 61 1F 3B 77 34 0D FD

6. Bài tập

- Giải thích cơ chế của việc bẻ gãy mật mã của hệ thống sau:



6. Bài tập

2. Tìm mã hoá của các ký số 1-9:

1	2	3	4	
				?
?	?			
?				

6. Bài tập

3. Sử dụng công cụ Cryptool

- Cryptool là một ứng dụng miễn phí chạy trên Windows, thường được sử dụng để phân tích các giải thuật mã hoá. Phiên bản hiện nay là 1.4.30.
- Địa chỉ download Cryptool:

<http://www.cryptool.org/>

6. Bài tập

4. Nêu cơ chế hoạt động và viết ứng dụng cho phép mã hoá và giải mã với 2 (hai) trong số những giải thuật mã hoá sau:
 - Vigenère
 - Hill.
 - Affine
 - Playfair
 - Solitaire

6. Bài tập

5. Nêu chi tiết cơ chế hoạt động của giải thuật mã hoá DES.
6. Cài đặt ứng dụng Advanced Encryption Package. Cho biết cách sử dụng công cụ này.
7. Trình bày tổng quan về cơ chế hoạt động của các giải thuật RC2, RC4, RC6.

6. Bài tập

8. Trình bày tổng quan về cơ chế hoạt động của giải thuật RSA.
9. Viết ứng dụng mã hoá và giải mã cho một giải thuật mã hoá hiện đại tuỳ chọn giữa DES và AES.
10. Viết ứng dụng mô phỏng giao thức trao đổi khoá Diffie – Hellman.

6. Bài tập

11. Viết ứng dụng mô phỏng giải thuật mã hóa RSA.
12. Nêu cách sử dụng công cụ mã hóa TrueCrypt.
13. Thực hiện mã hóa và giải mã dữ liệu với công cụ EFS (Encrypt File System).

THANK YOU!