

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 về an ninh mạng
2. Các phần mềm gây hại
3. Các giải thuật mã hoá dữ liệu
4. Mã hoá khoá công khai và quản lý khoá
5. Chứng thực dữ liệu
6. Một số giao thức bảo mật mạng
7. Bảo mật mạng không dây
8. Bảo mật mạng vành đai
9. Tìm kiếm phát hiện xâm nhập

## BÀI 3

# 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

## ■ Một số khái niệm

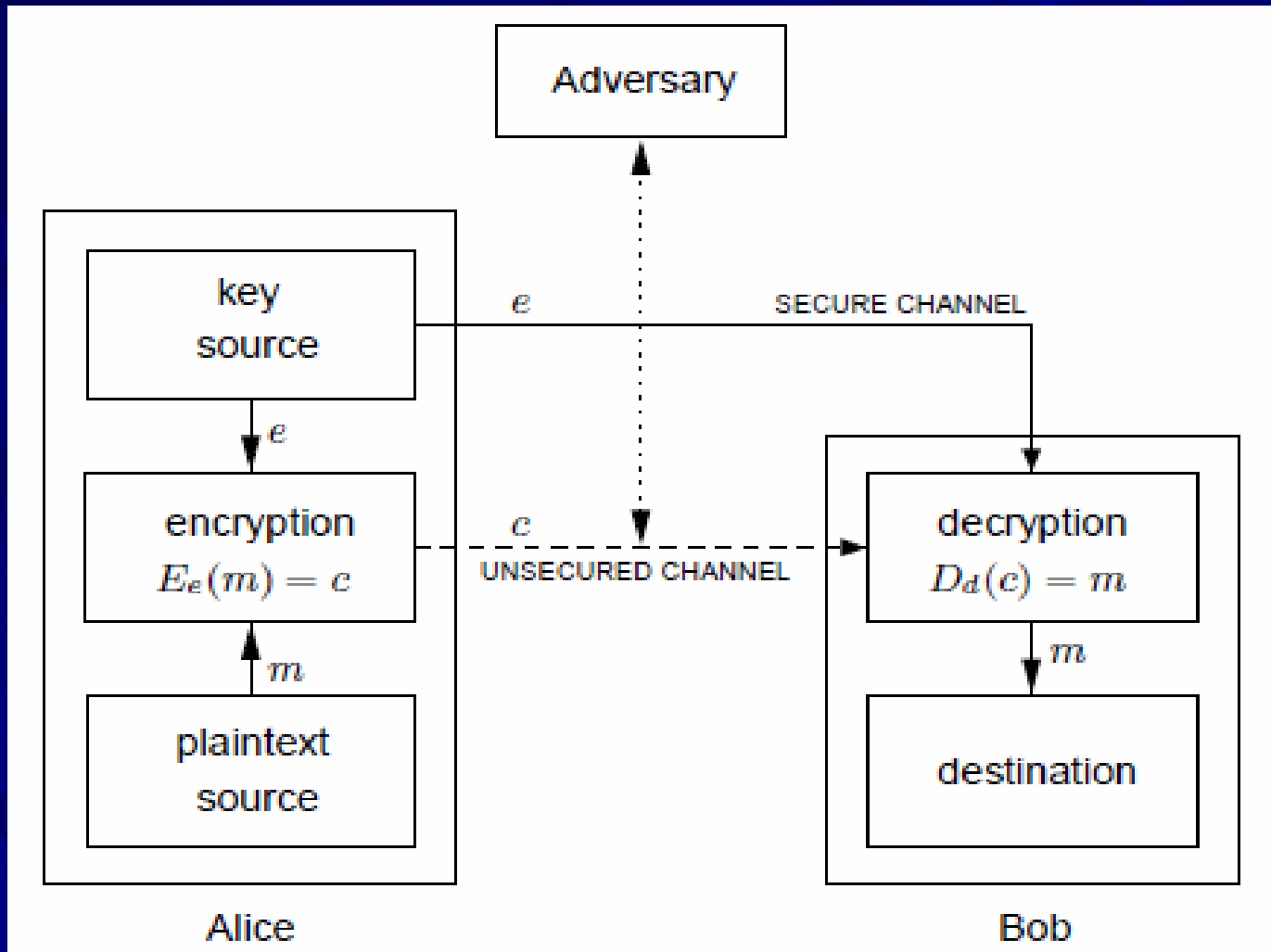
- Thông báo, văn bản: là một chuỗi hữu hạn các ký hiệu lấy từ một bảng chữ cái  $Z$  nào đó và được ký hiệu là  $m$ .
- Mật mã hoá: là việc biến đổi một thông báo sao cho nó không thể hiểu nổi đối với bất kỳ người khác ngoài người nhận được mong muốn.
- Phép mật mã hoá thường được ký hiệu là  $e(m)$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





## 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 khóa 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 bằng 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

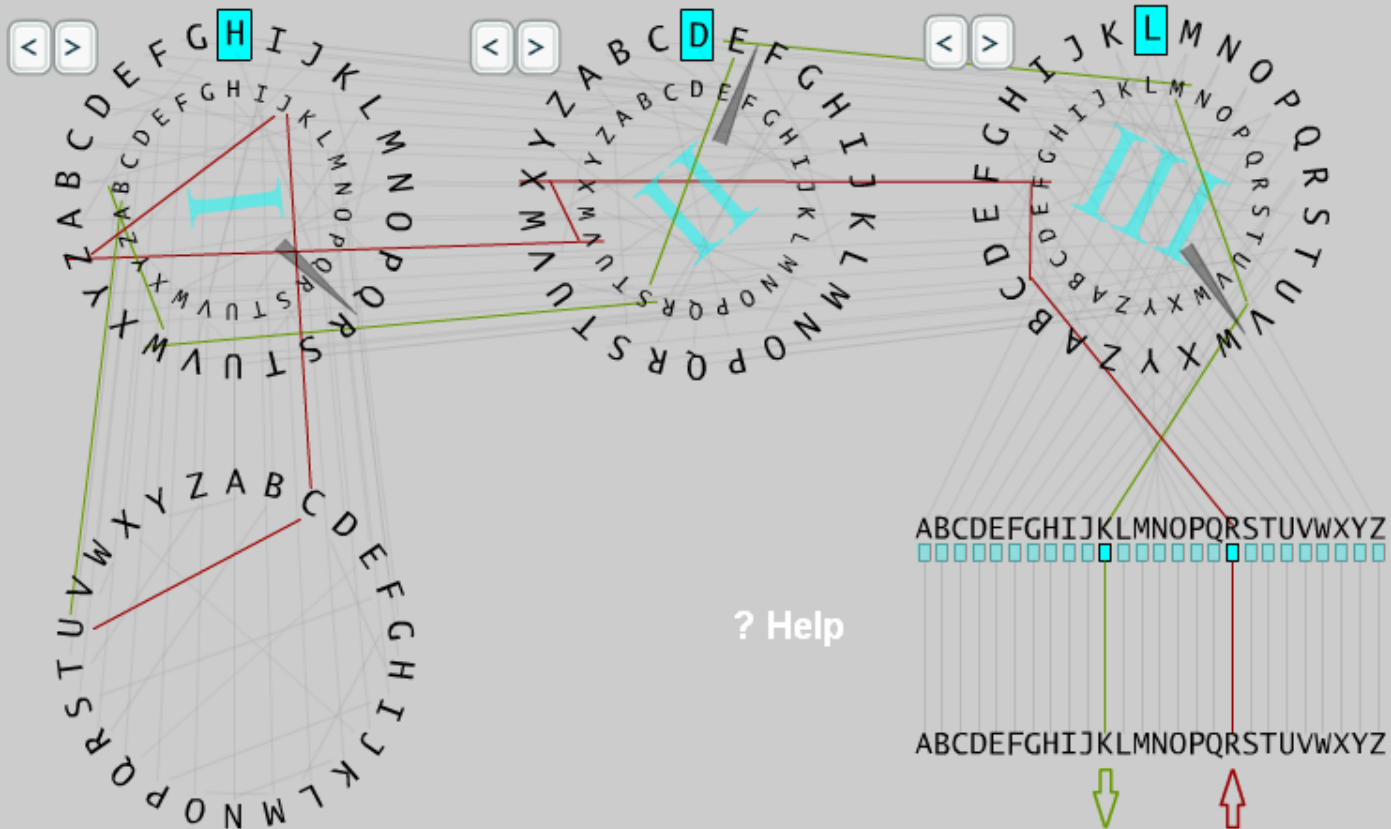
- **Mật mã học trong thế chiến thứ 2**
  - Người Đức sử dụng rộng rãi một hệ thống máy rôto cơ điện tử có tên gọi là máy Enigma.
  - Phe Đồng minh sử dụng máy TypeX của Anh và máy SIGABA của Mỹ, đều là những thiết kế cơ điện dùng rôto tương tự như máy Enigma, song với nhiều nâng cấp hơn.



# Máy Enigma

ATMMT - TNNQ





? Help

Input:

COMPUTER

Output:

HEYGBZSK

Status Highlighted wires show encryption steps.

# Máy Enigma

## 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 hoá công khai 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).

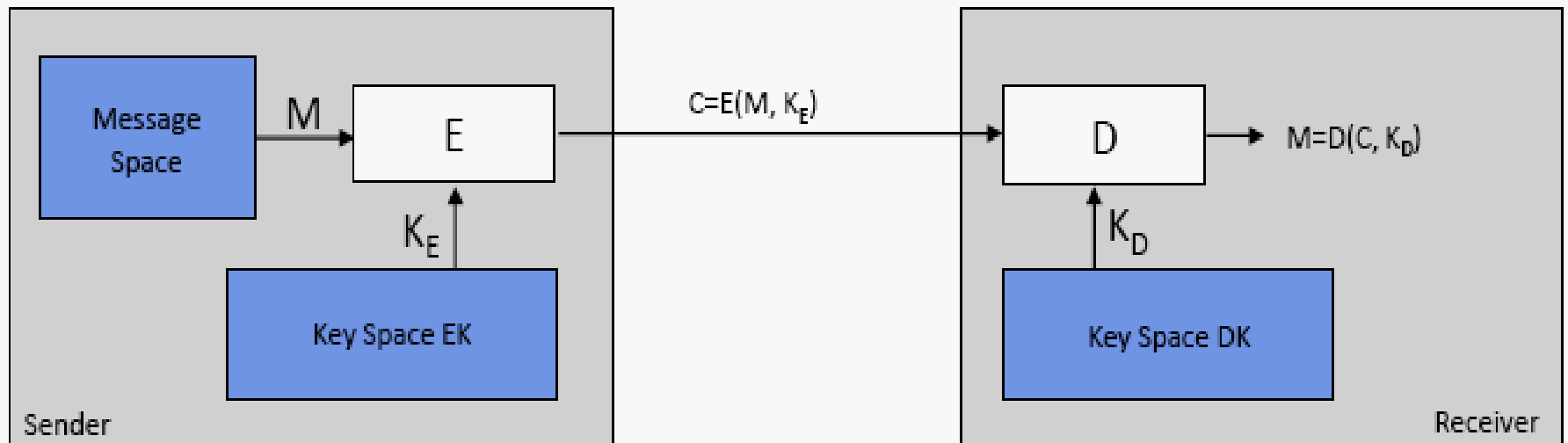
## 2. Lịch sử của mật mã

### ■ 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 mật 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 hoá RSA.

## 2. Lịch sử của mật mã

### ■ Mật mã học hiện đại



a) Symmetric Encryption:

$$\begin{array}{c} \text{secret} \\ \swarrow \quad \searrow \\ K_E = K_D \end{array} \quad (\text{e.g. AES})$$

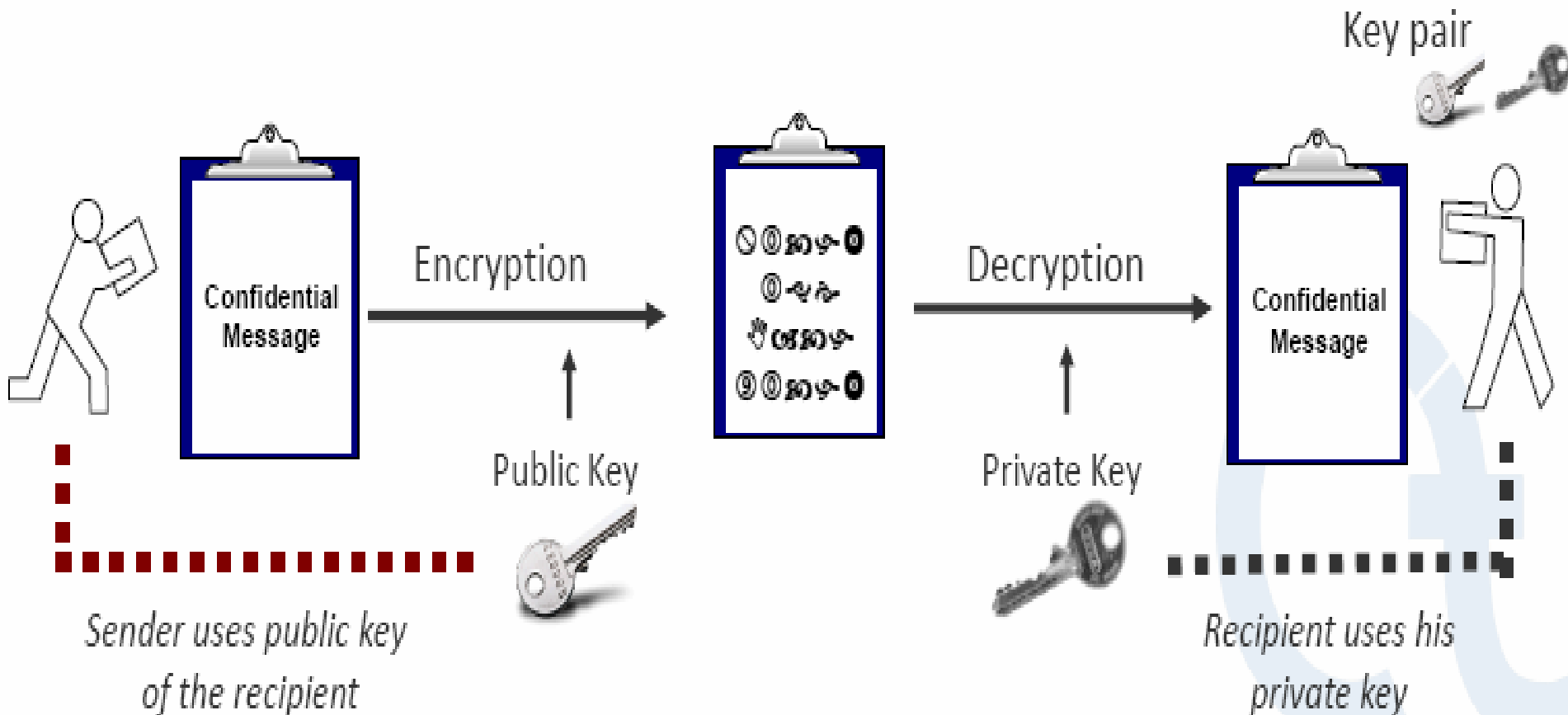
b) Asymmetric Encryption:

$$\begin{array}{c} K_E \neq K_D \\ \swarrow \quad \searrow \\ \text{public} \quad \text{private/secret} \end{array} \quad (\text{e.g. RSA})$$



## 2. Lịch sử của mật mã

### ■ Mật mã học hiện đại



Mã hoá 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

- **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

## ■ 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

## ■ Mã thay thế n-gram

- Thay vì thay thế các ký tự, người ta có thể thay thế cho từng cụm 2 ký tự (digram), 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.
- $\Rightarrow$  Phá mã?

# 3. Giải thuật mã hoá cổ điển

## ■ 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  $26 \times 26$  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

#### ■ 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 = JOHN IS A GOOD ACTOR

Qua phép mã hoá này m sẽ trở thành chuỗi mật mã c sau:

c = 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: HWDUYTLWFUMD (Shift of 5)

$C = (p + 4) \bmod 26$



## Mã dịch chuyển – Shift Cypher

# Vigenère Encryption – Block Cypher (1523 – 1596)

## Ví dụ:

Từ khoá: CHIFFRE

Mã hoá: VIGENERE

Kết quả: XPOJSVVG

	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**

	<b>h</b>	<b>e</b>	<b>l</b>	<b>p</b>	<b>n</b>	<b>e</b>	<b>e</b>	<b>d</b>	<b>e</b>	<b>d</b>
Plaintext:	001	000	010	100	101	000	000	011	000	011
Key:	111	101	110	101	111	100	000	101	110	000
	<hr/>									
	110	101	100	001	010	100	000	110	110	011
Ciphertext:	<b>a</b>	<b>n</b>	<b>p</b>	<b>h</b>	<b>l</b>	<b>p</b>	<b>e</b>	<b>a</b>	<b>a</b>	<b>d</b>

# 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  $x$ ?

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

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

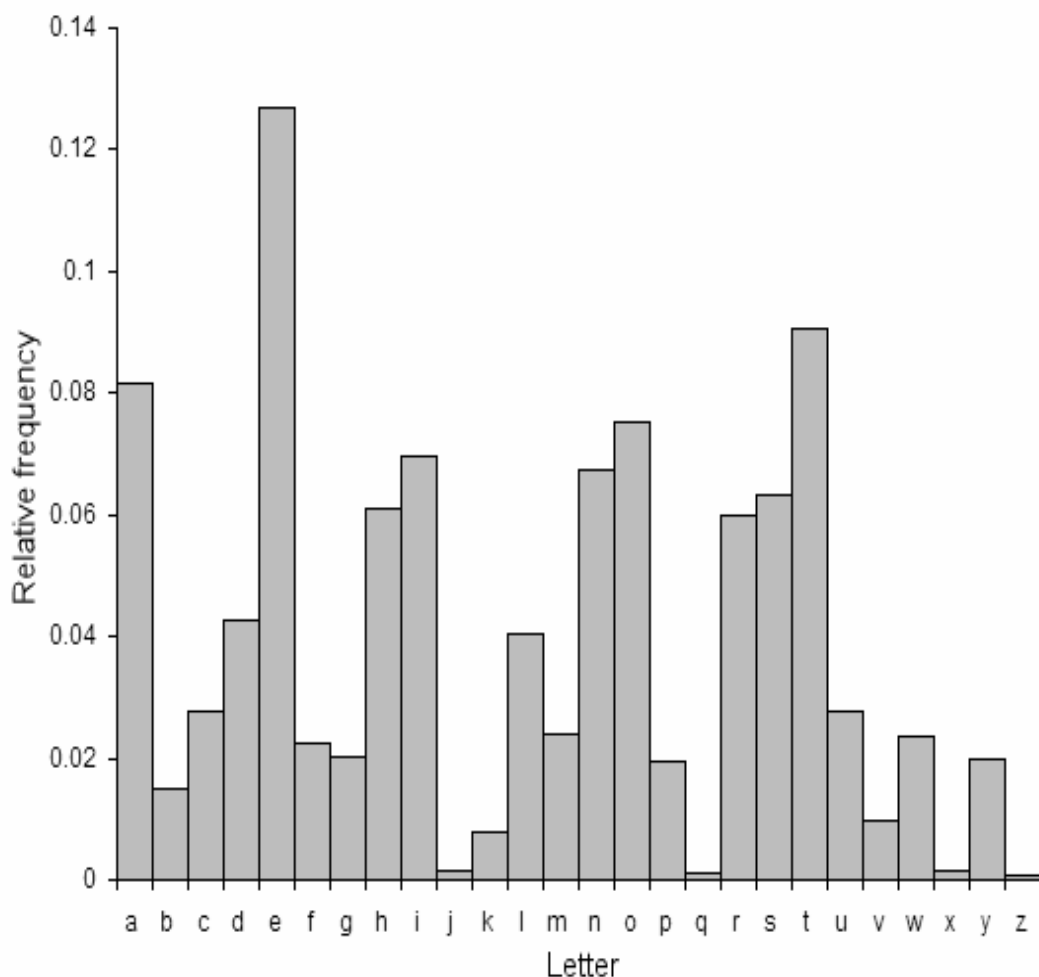
$$x = a^{-1}(y - b) \pmod{26}.$$

# 3. Giải thuật mã hoá cổ điển

## 7. 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
<i>A</i>	.082	<i>N</i>	.067
<i>B</i>	.015	<i>O</i>	.075
<i>C</i>	.028	<i>P</i>	.019
<i>D</i>	.043	<i>Q</i>	.001
<i>E</i>	.127	<i>R</i>	.060
<i>F</i>	.022	<i>S</i>	.063
<i>G</i>	.020	<i>T</i>	.091
<i>H</i>	.061	<i>U</i>	.028
<i>I</i>	.070	<i>V</i>	.010
<i>J</i>	.002	<i>W</i>	.023
<i>K</i>	.008	<i>X</i>	.001
<i>L</i>	.040	<i>Y</i>	.020
<i>M</i>	.024	<i>Z</i>	.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

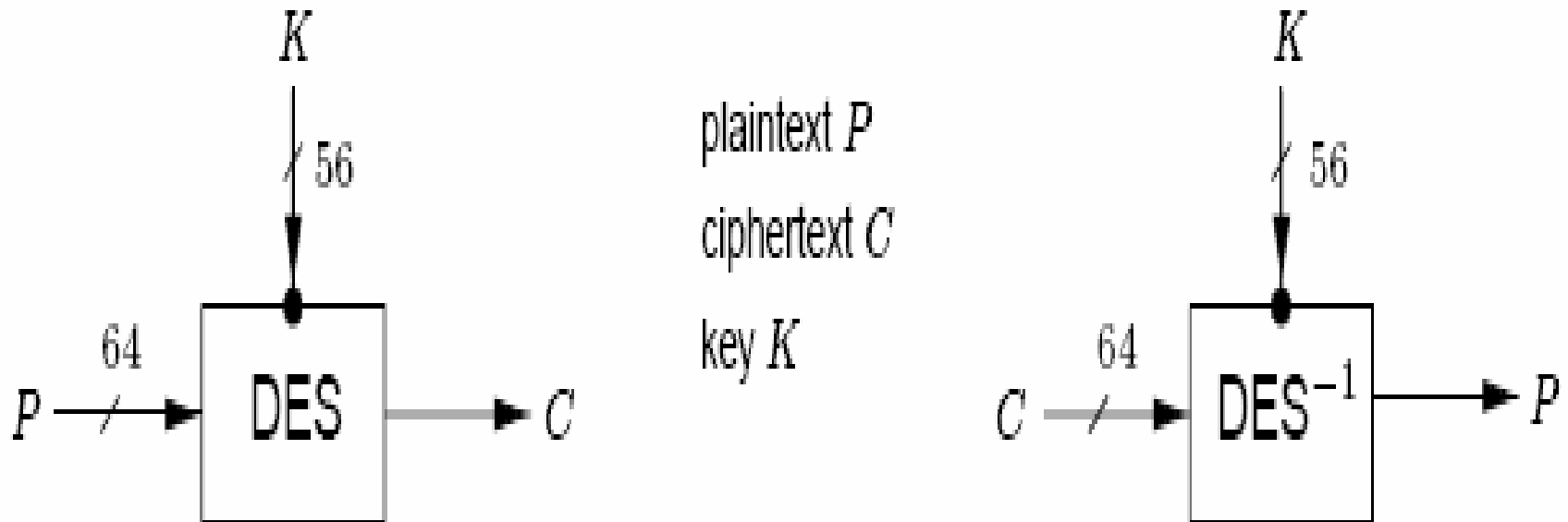
# 4. Giải thuật mã hoá hiện đại

## 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



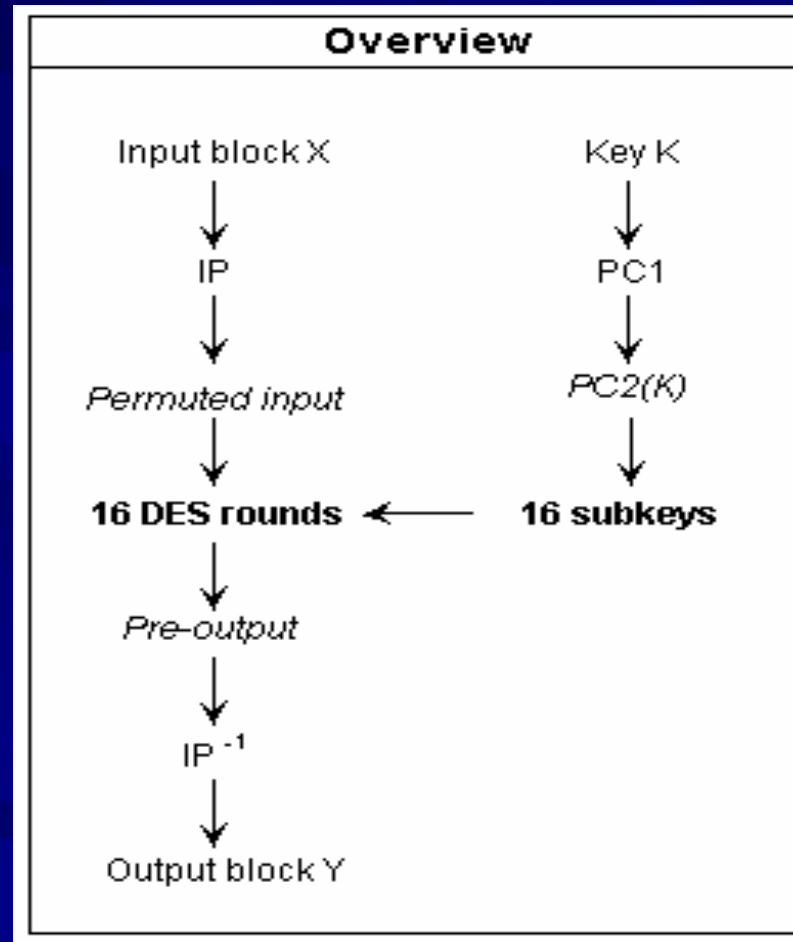
# 4. Giải thuật mã hoá hiện đại

## 2. Chuẩn mã hoá dữ liệu DES

Ngày	Sự kiện
17.3.1975	DES được công bố trên công báo liên bang Hoa kỳ để công chúng đóng góp ý kiến.
11.1976	DES được phê chuẩn làm tiêu chuẩn chính thức.
1992	Biham và Shamir công bố kiểu tấn công thám mã vi sai (trên lý thuyết) với độ phức tạp thấp hơn tấn công bạo lực. Tuy nhiên, kiểu tấn công này đòi hỏi người tấn công lựa chọn $2^{47}$ văn bản rõ (một điều kiện không thực tế).
6.1997	Dự án DESCHALL đã phá vỡ được một bản tin mã hóa bằng DES (lần đầu tiên trước công chúng).
7.1998	Thiết bị thám mã Deep Crack của tổ chức Electronic Frontier Foundation phá được một khóa của DES trong vòng 56 giờ.
1.1999	Deep Crack cùng với distributed.net phá được một khóa của DES trong vòng 22 giờ và 15 phút.
25.10.1999	DES được xác nhận lần thứ tư với tên FIPS 46-3. Lần này phương pháp Triple DES được khuyến cáo sử dụng còn DES chỉ được dùng cho các hệ thống ít quan trọng.
26.5.2002	AES trở thành tiêu chuẩn

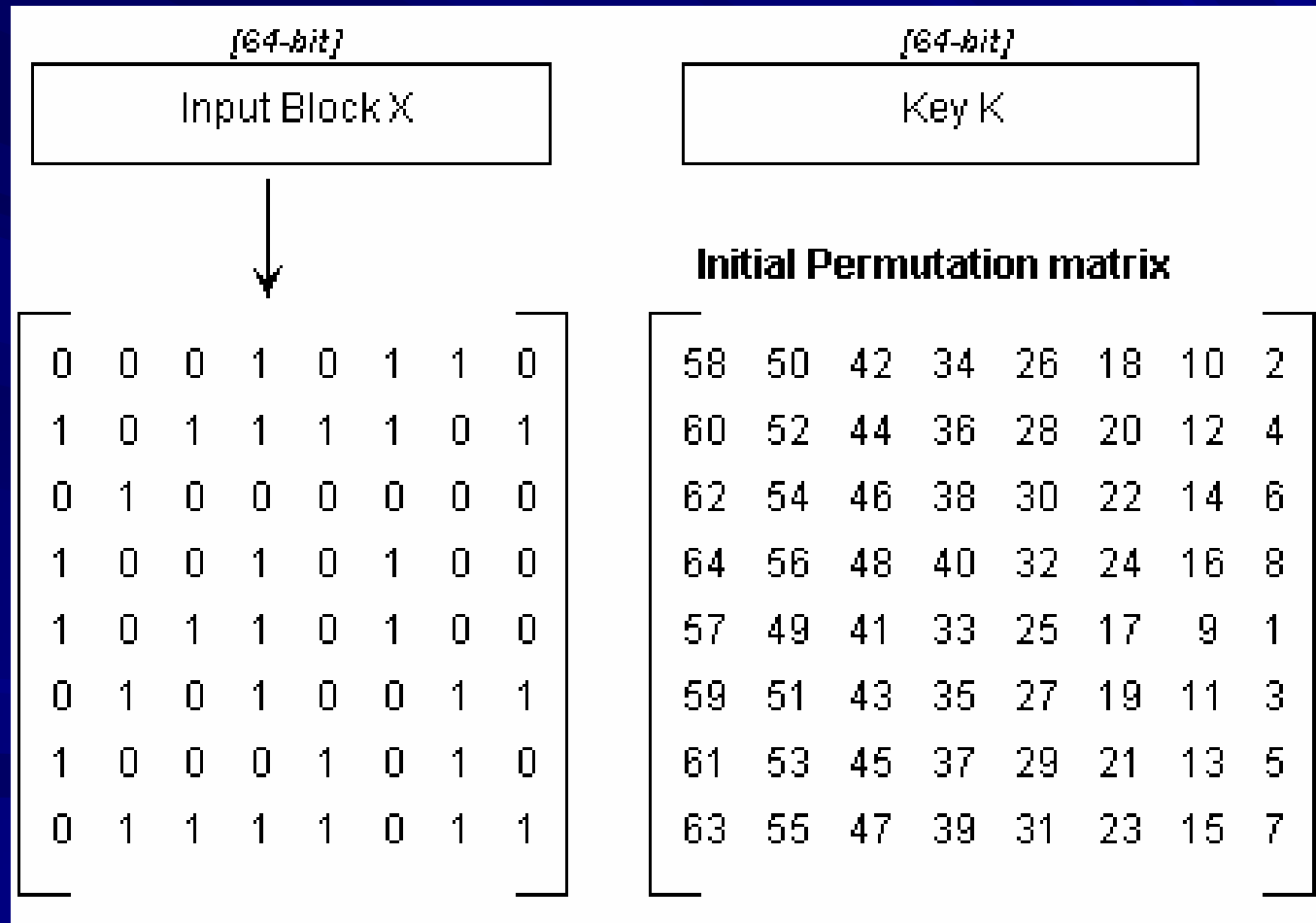
# 4. Giải thuật mã hoá hiện đại

## 2. Chuẩn mã hoá dữ liệu DES



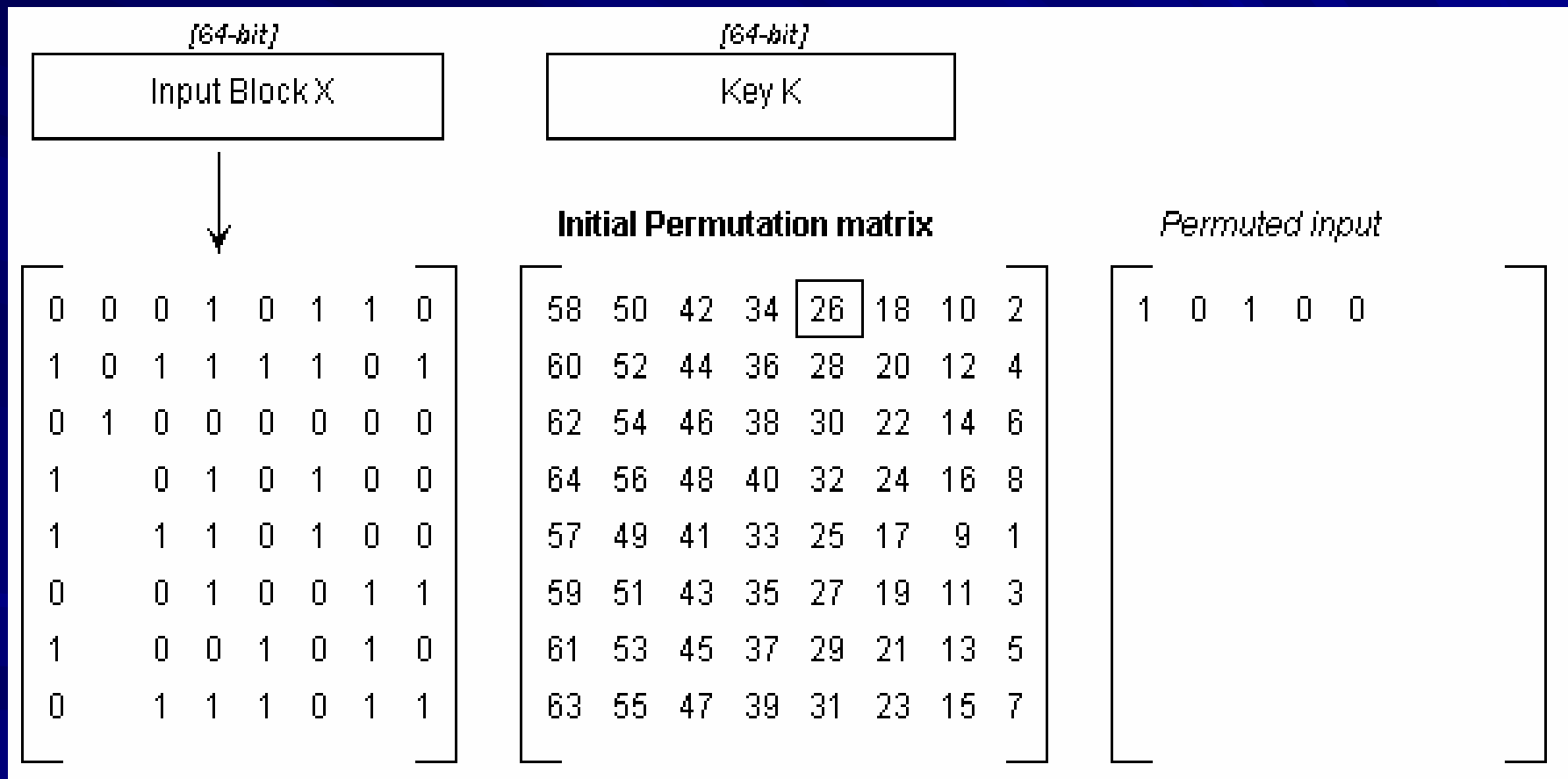
# 4. Giải thuật mã hoá hiện đại

## 2. Chuẩn mã hoá dữ liệu DES



# 4. Giải thuật mã hoá hiện đại

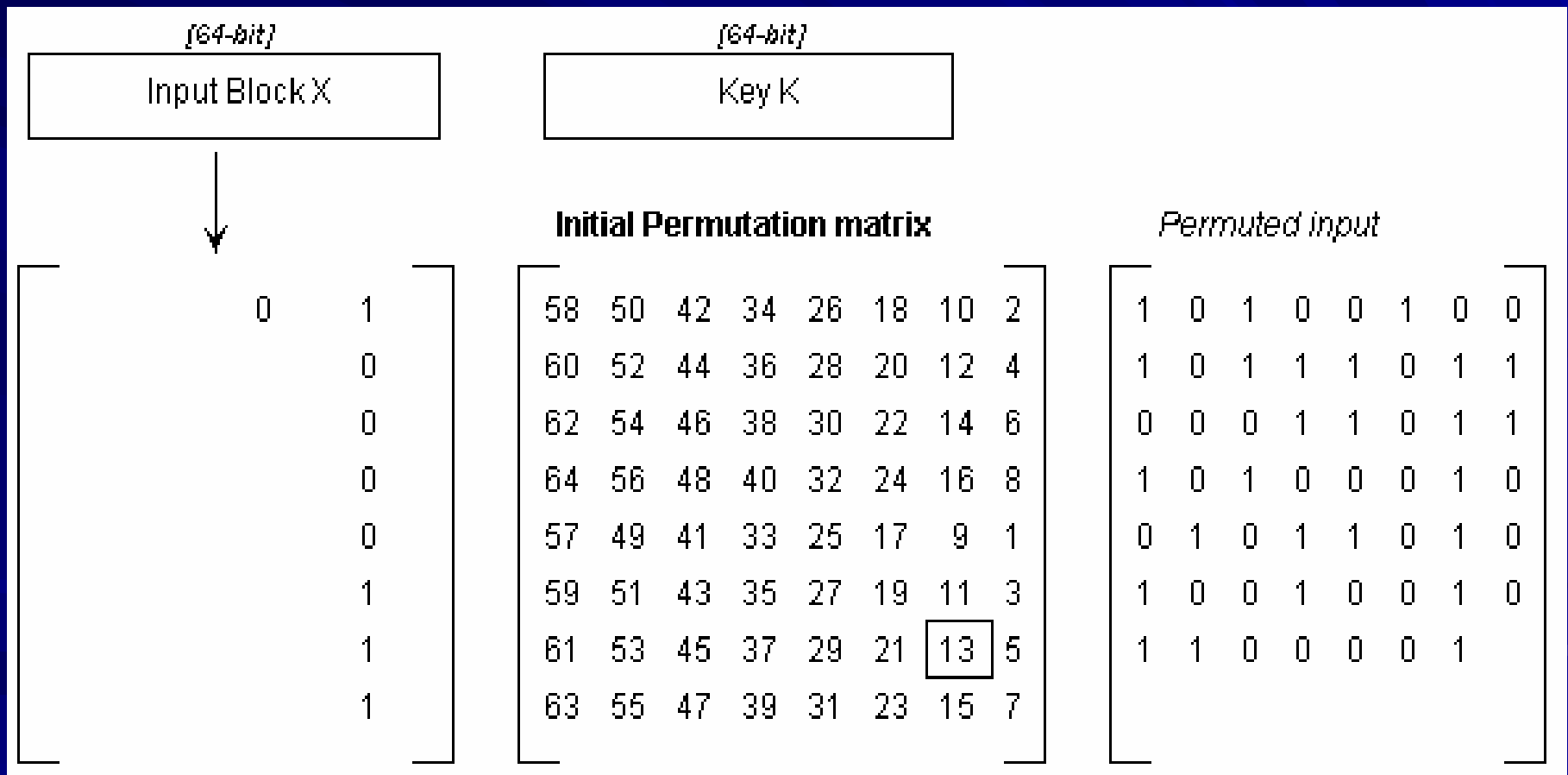
## 2. Chuẩn mã hoá dữ liệu DES





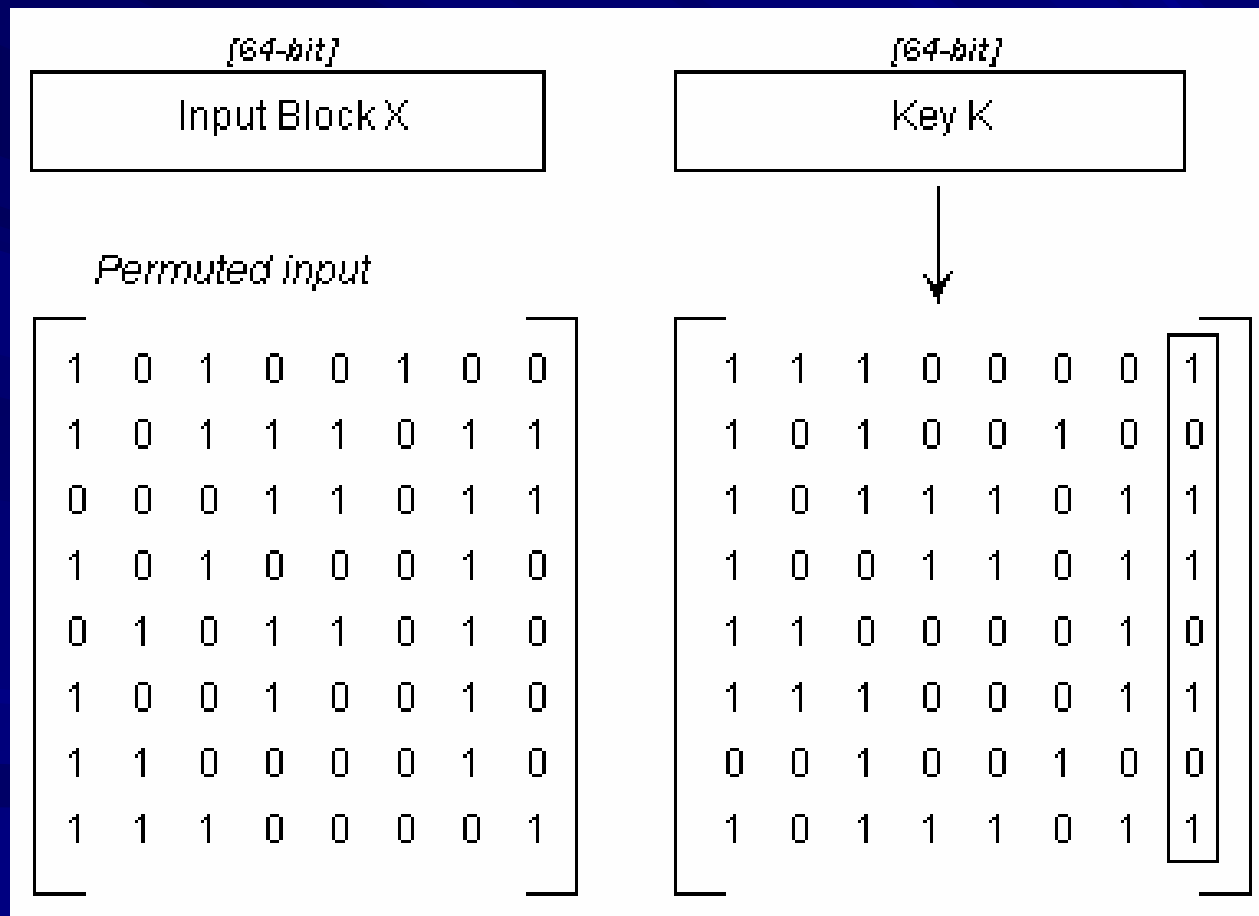
# 4. Giải thuật mã hoá hiện đại

## 2. Chuẩn mã hoá dữ liệu DES



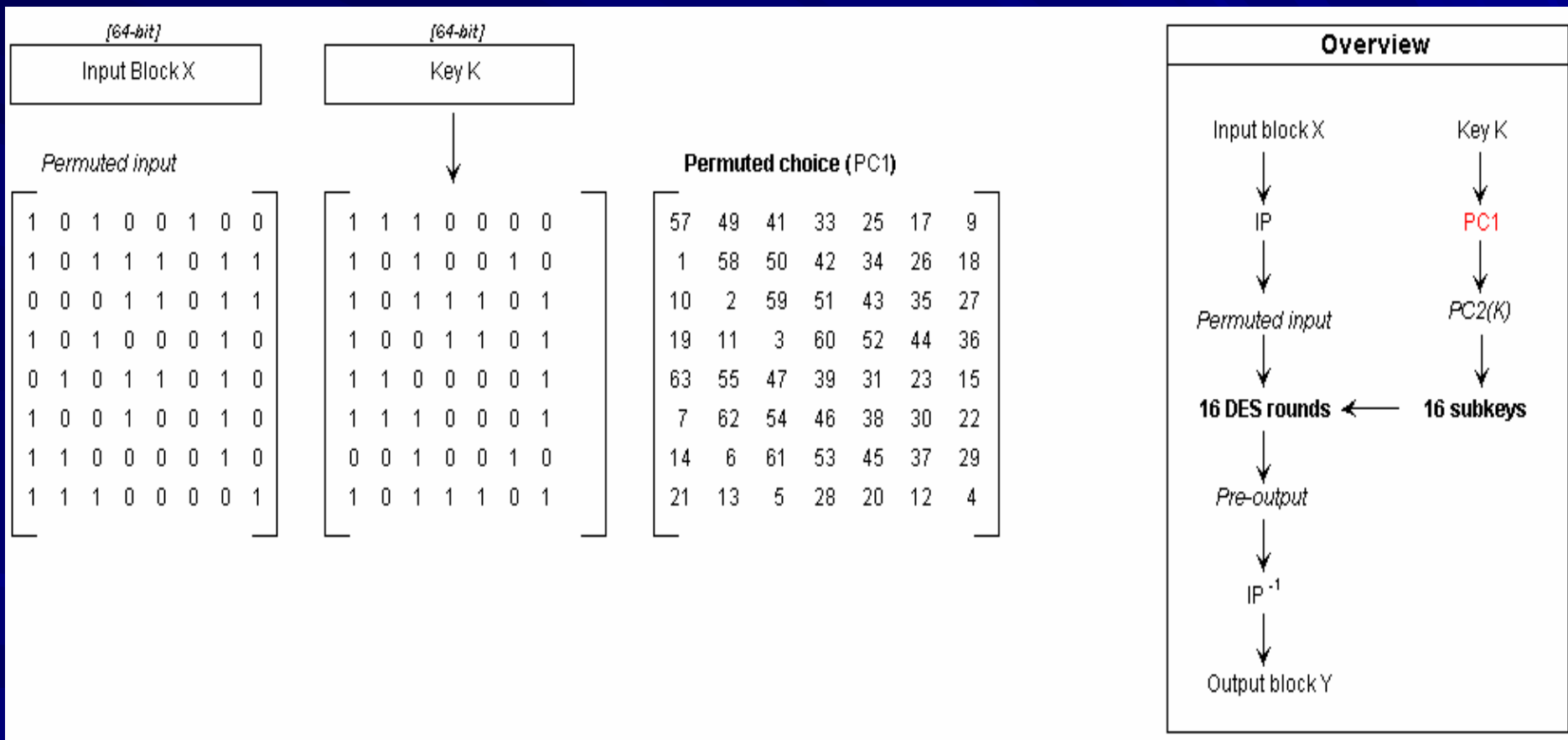
# 4. Giải thuật mã hoá hiện đại

## 2. Chuẩn mã hoá dữ liệu DES



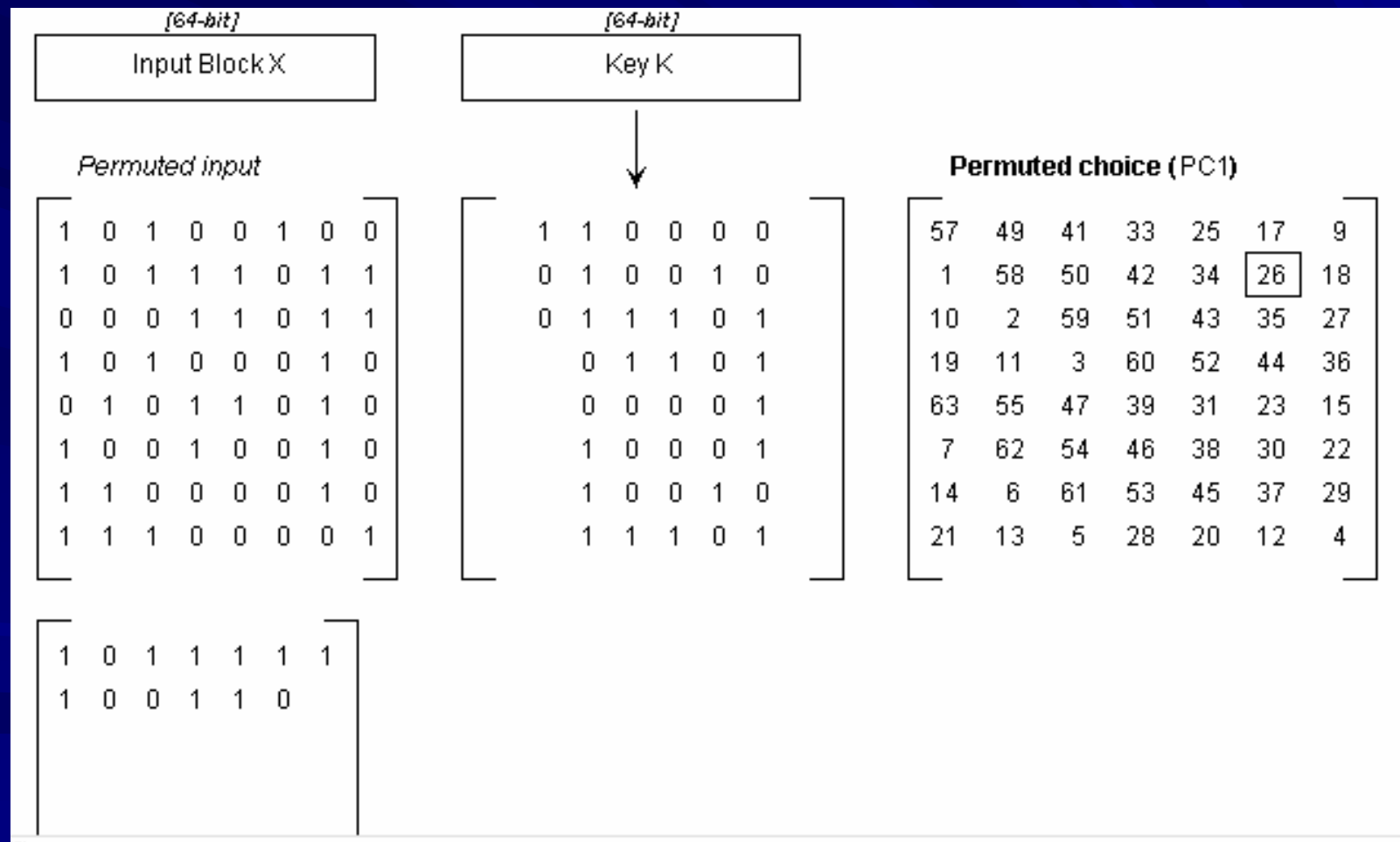
# 4. Giải thuật mã hoá hiện đại

## 2. Chuẩn mã hoá dữ liệu DES



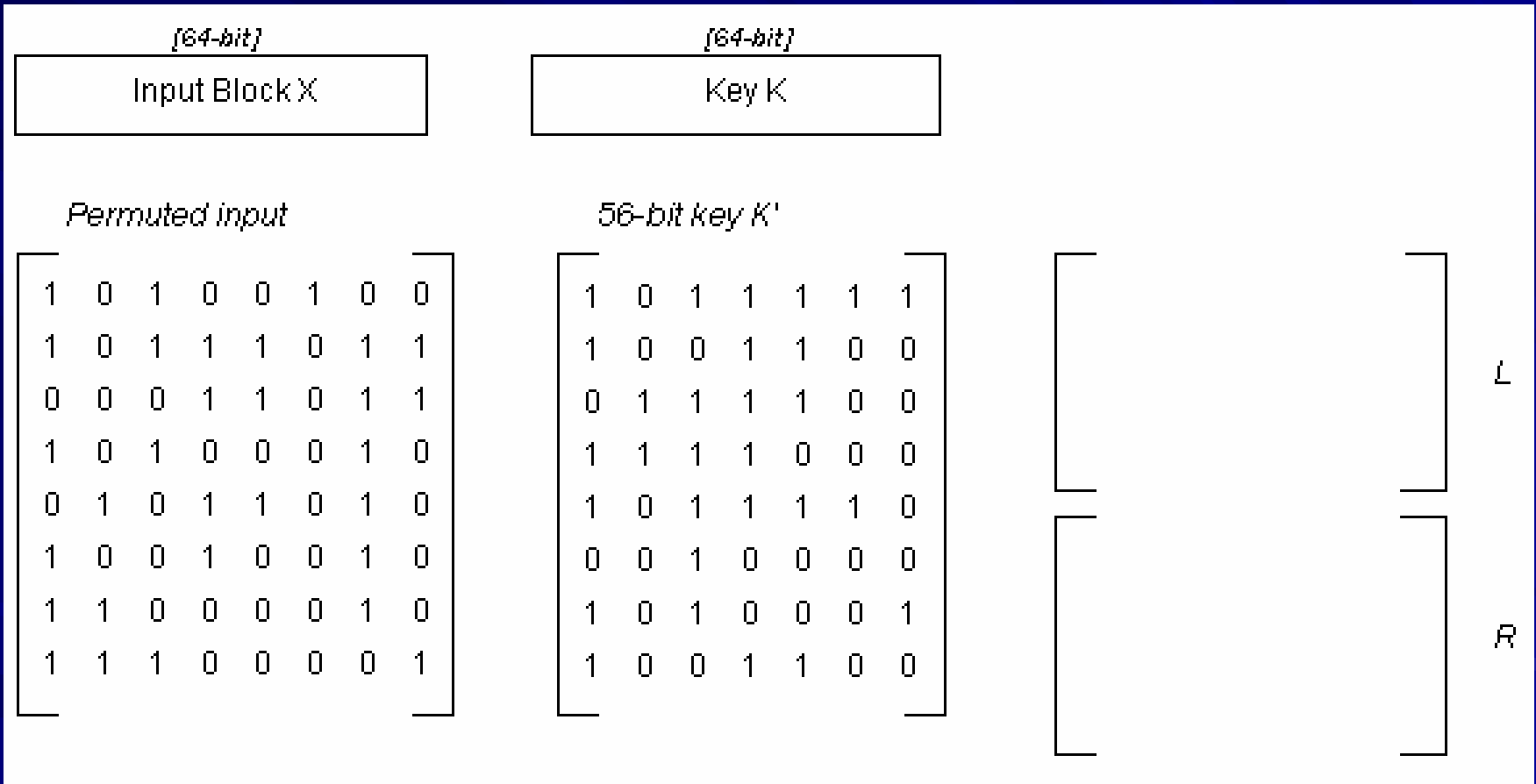
# 4. Giải thuật mã hoá hiện đại

## 2. Chuẩn mã hoá dữ liệu DES



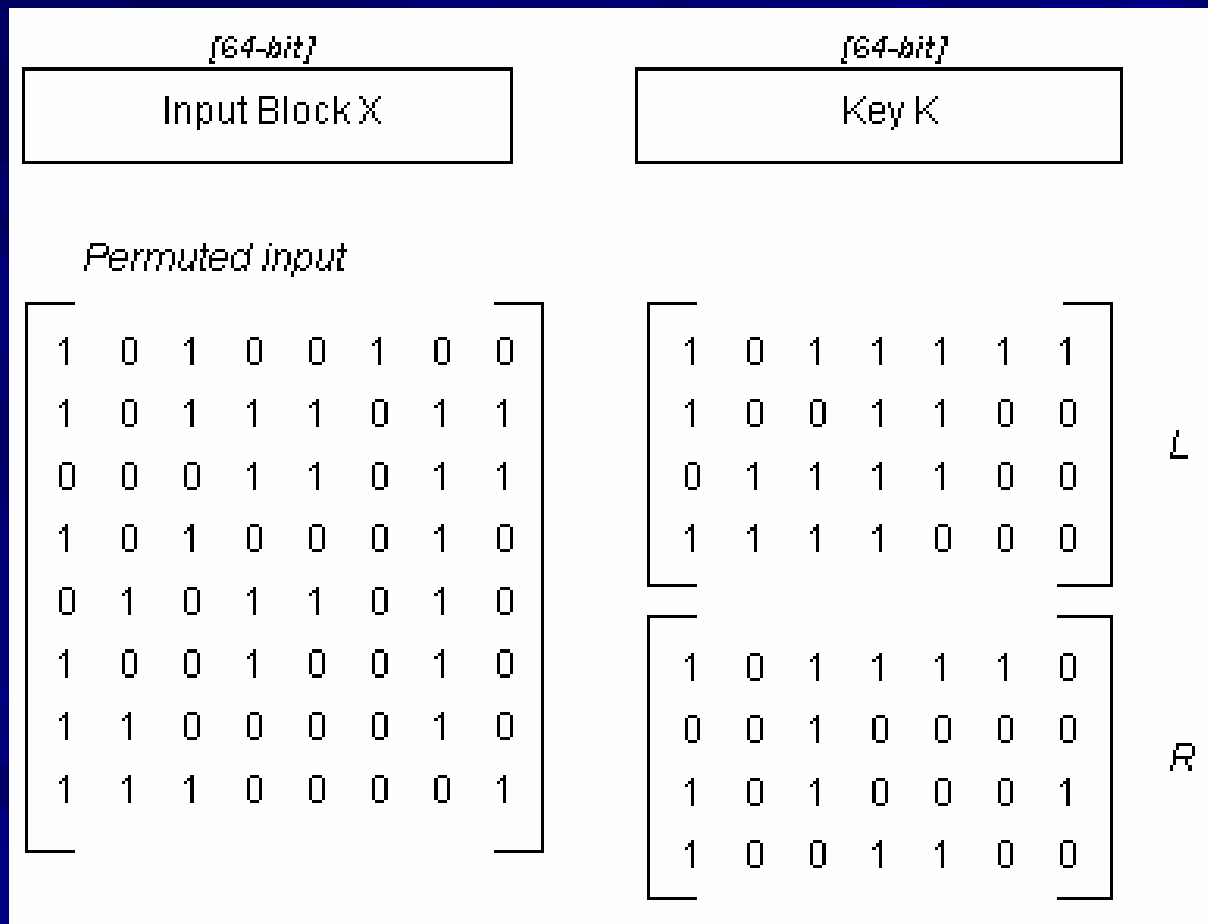
## 4. Giải thuật mã hoá hiện đại

## 2. Chuẩn mã hoá dữ liệu DES



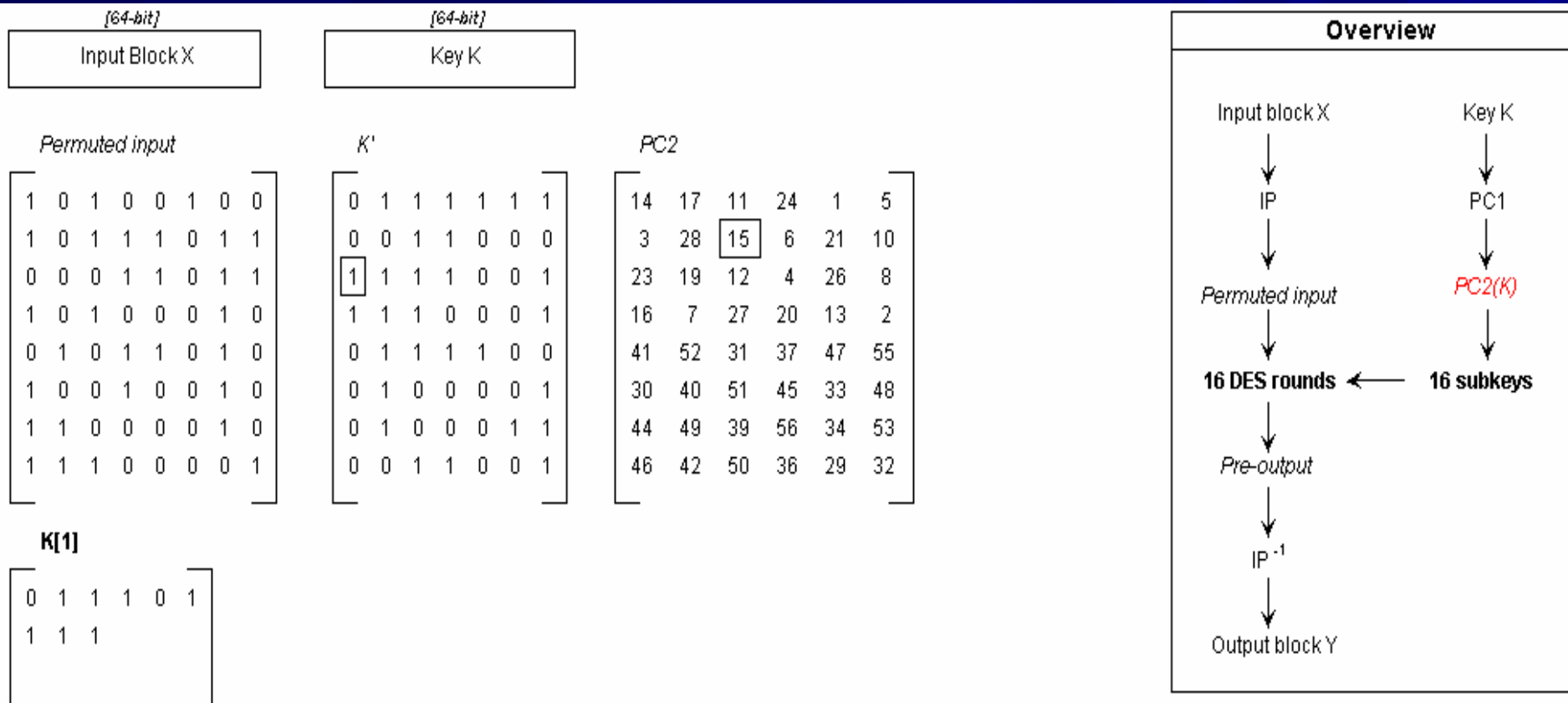
# 4. Giải thuật mã hoá hiện đại

## 2. Chuẩn mã hoá dữ liệu DES



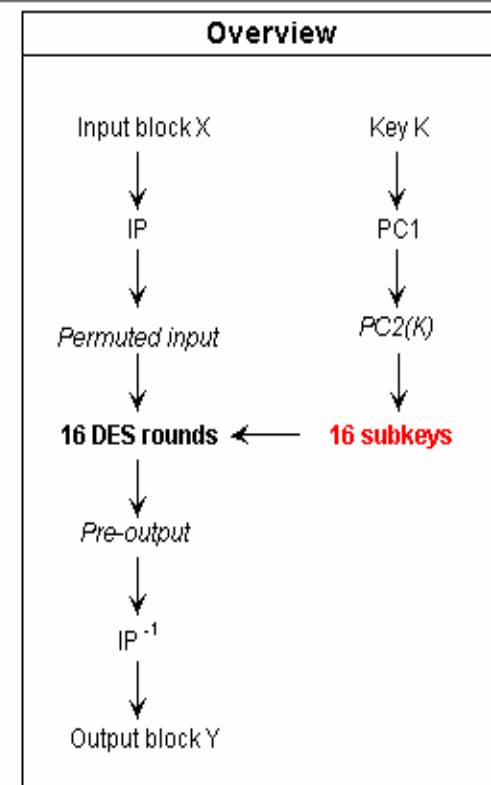
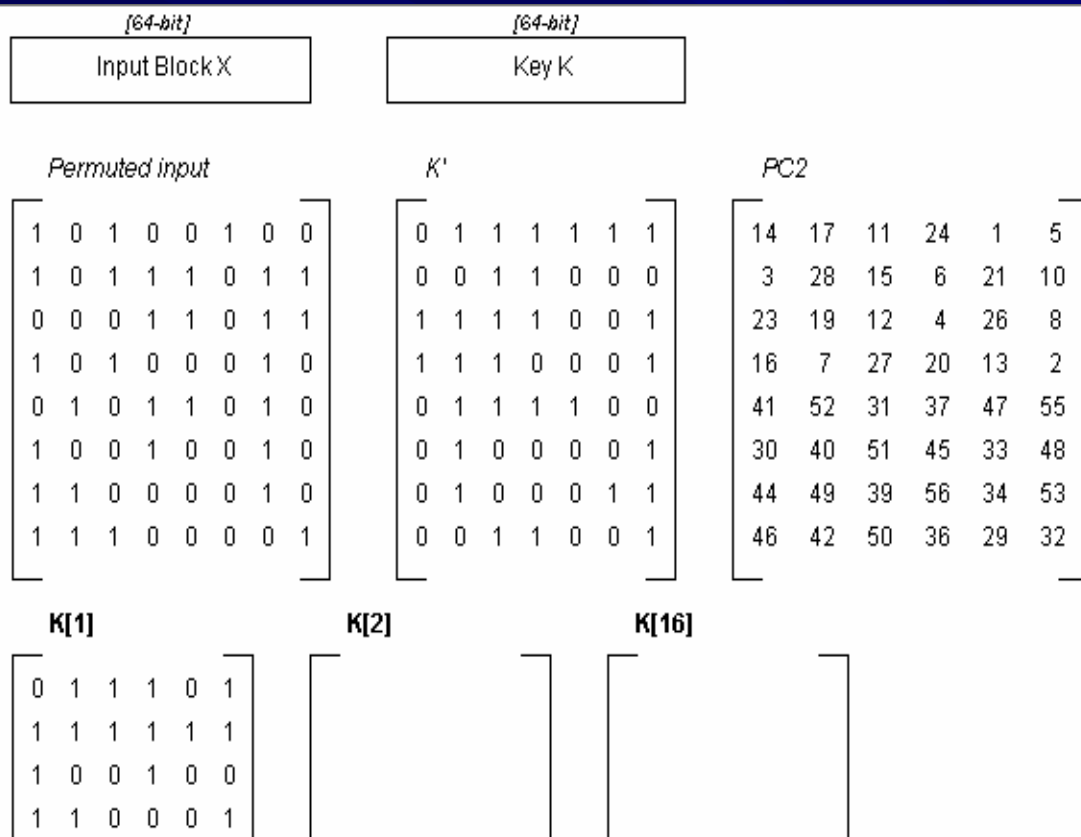
# 4. Giải thuật mã hoá hiện đại

## 2. Chuẩn mã hoá dữ liệu DES



# 4. Giải thuật mã hoá hiện đại

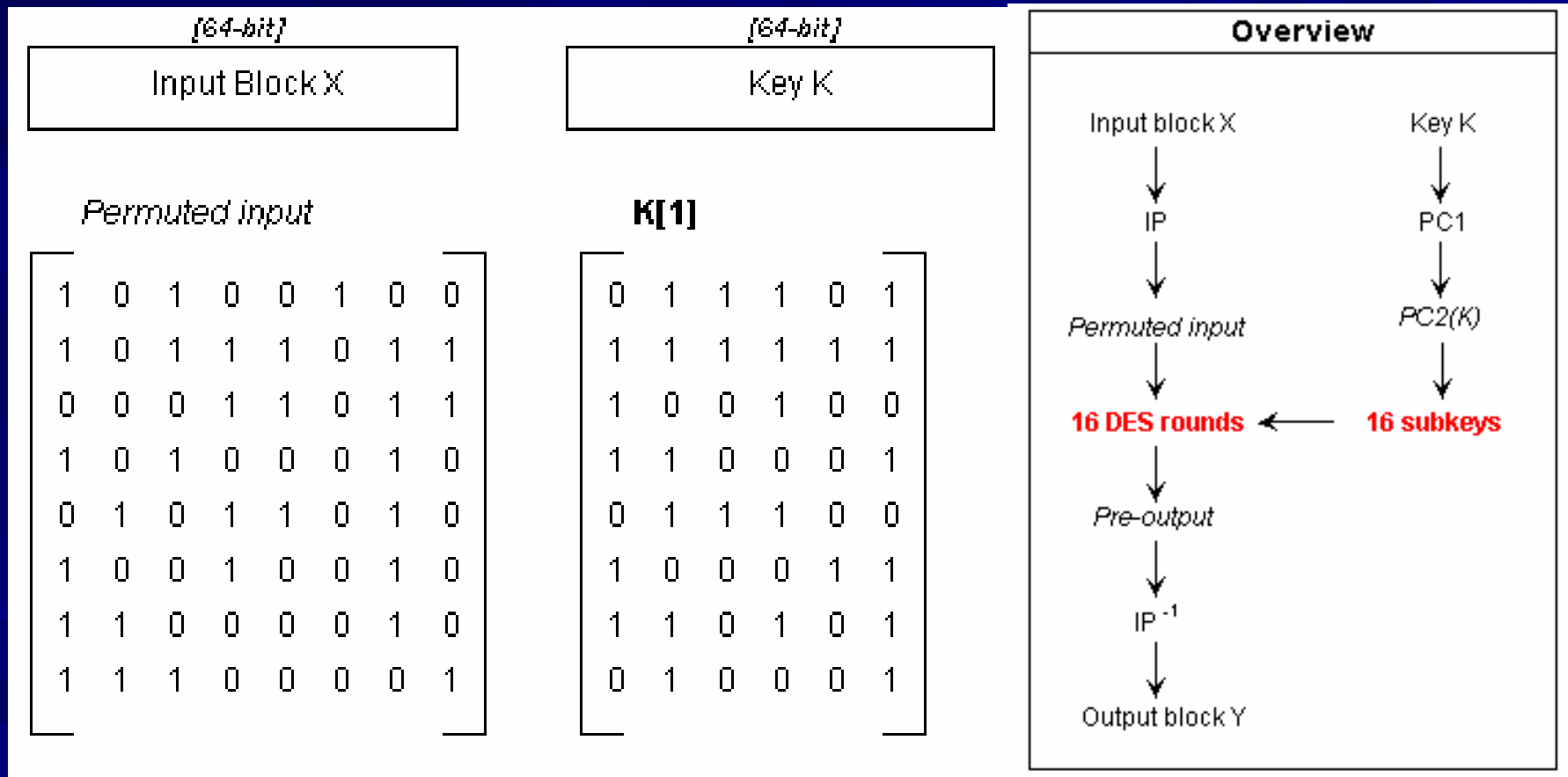
## 2. Chuẩn mã hoá dữ liệu DES





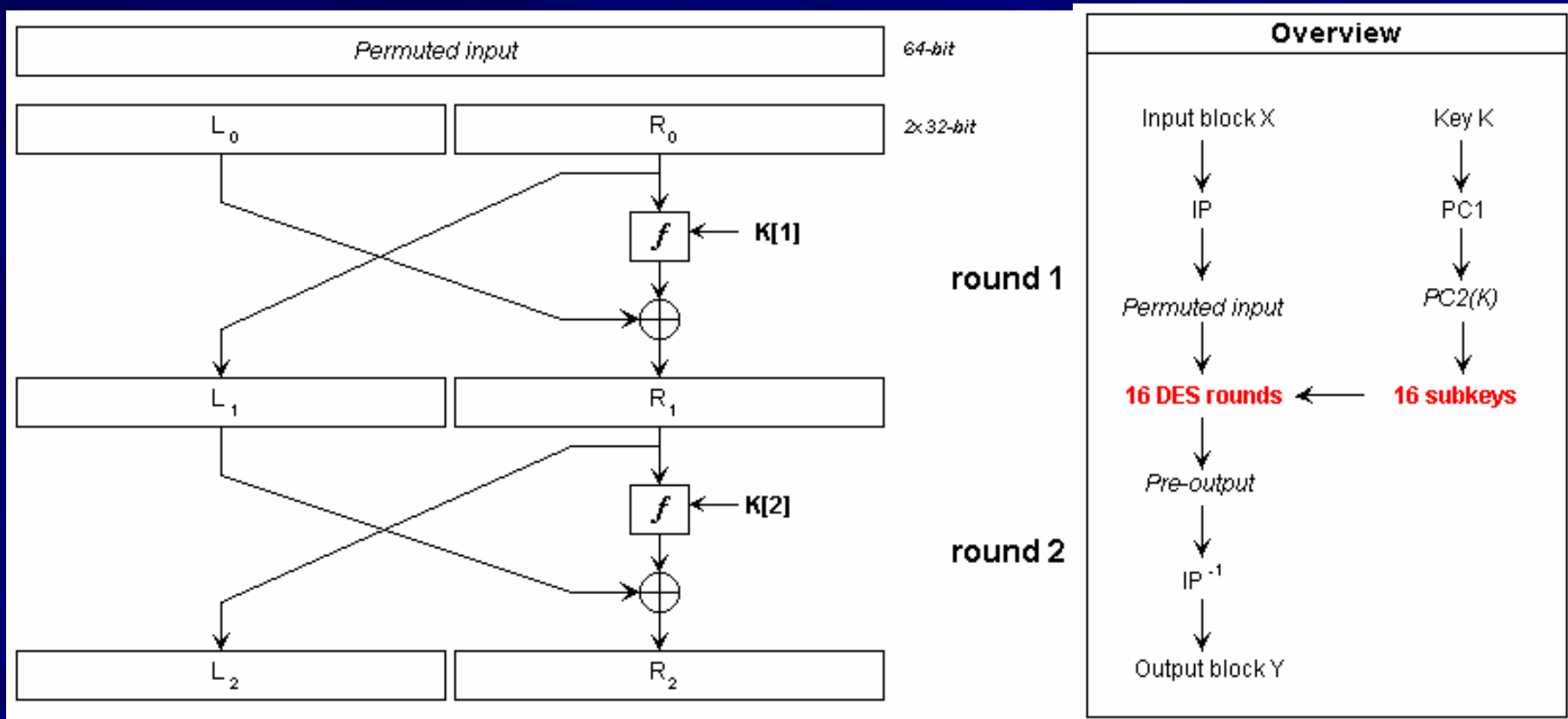
# 4. Giải thuật mã hoá hiện đại

## 2. Chuẩn mã hoá dữ liệu DES



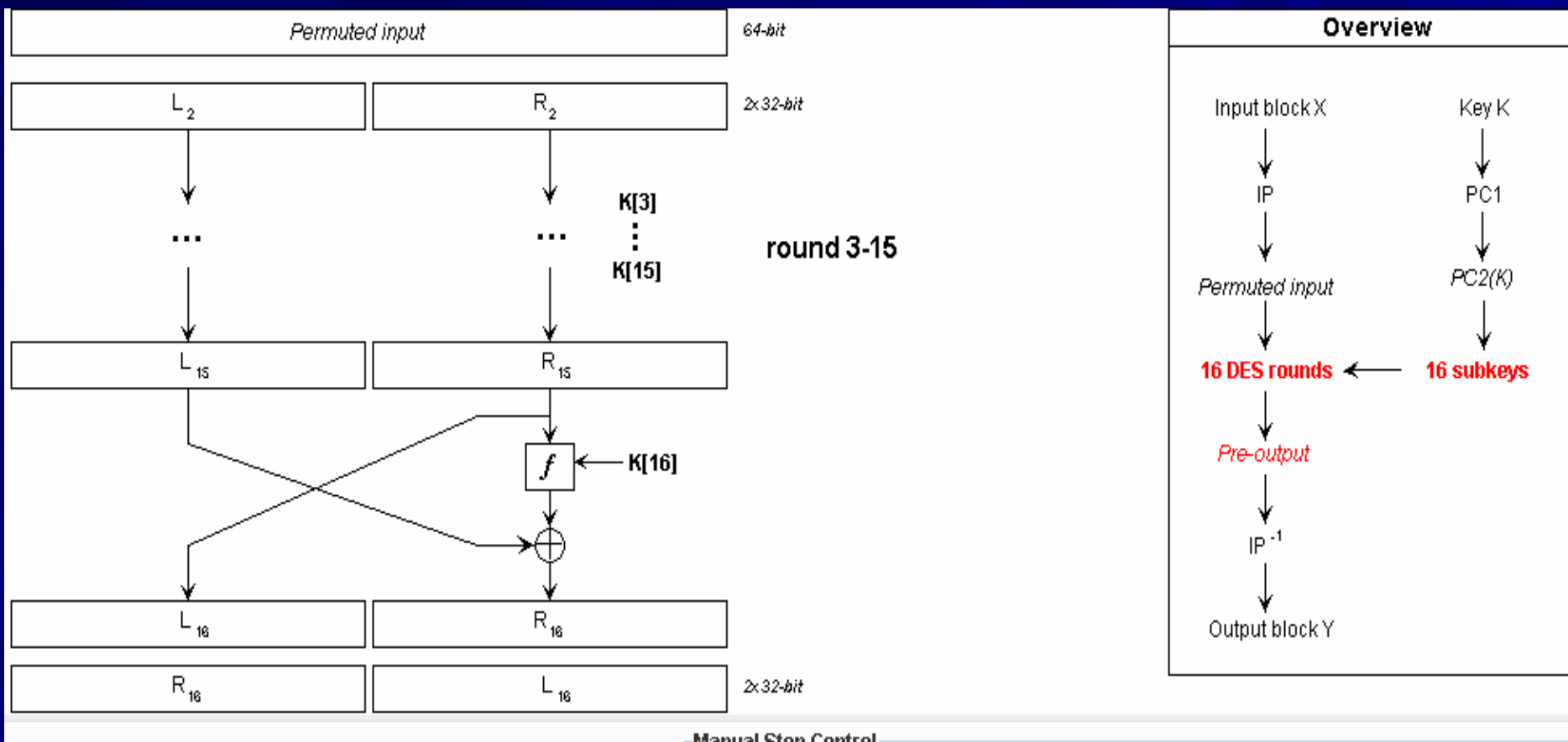
# 4. Giải thuật mã hoá hiện đại

## 2. Chuẩn mã hoá dữ liệu DES



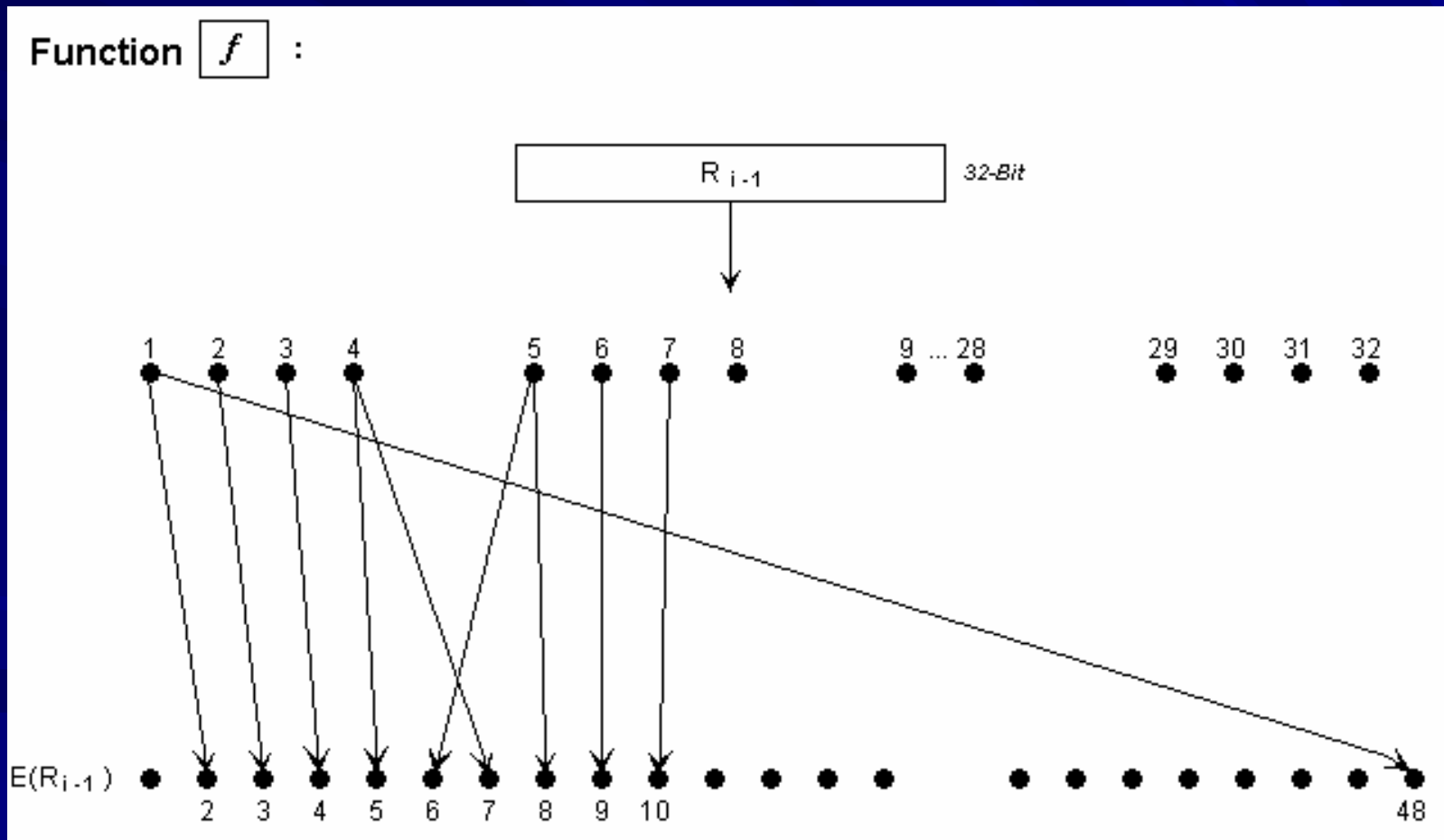
# 4. Giải thuật mã hoá hiện đại

## 2. Chuẩn mã hoá dữ liệu DES



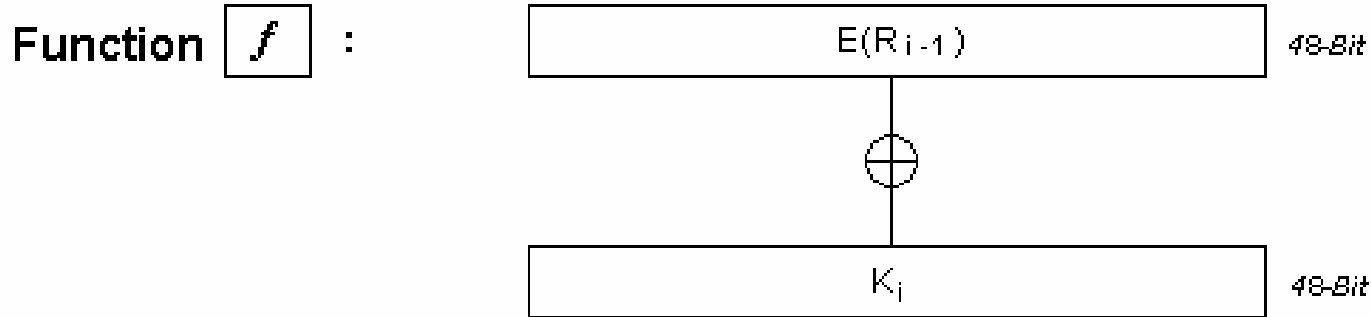
# 4. Giải thuật mã hoá hiện đại

## 2. Chuẩn mã hoá dữ liệu DES



## 4. Giải thuật mã hoá hiện đại

## 2. Chuẩn mã hoá dữ liệu DES



	<b>E(R[0])</b>	1	0	1	0	1	1	1	1	0	1	0	1	0	1	0	0	1	0	0	1	0	1	0	0	0	0	0	1	0	1	0	0	0	0	0	1	0
XOR	<b>K[1]</b>	0	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	0	0	1	0	0	1	0	0	0	1	1	1	0	0	1	1	0	1	0	1	0
=	<b>B</b>	1	1	0	1	1	0	0	0	1	0	1	0	1	1	0	0	1	0	0	0	1	0	0	1	0	0	0	1	1	0	1	0	0	1	1	0	1
		↓		↓		↓		↓		↓		↓		↓		↓		↓		↓		↓		↓		↓		↓		↓		↓		↓		↓		
		<b>B[1]</b>		<b>B[2]</b>		<b>B[3]</b>		<b>B[4]</b>		<b>B[5]</b>		<b>B[6]</b>		<b>B[7]</b>		<b>B[8]</b>																						

# 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:**

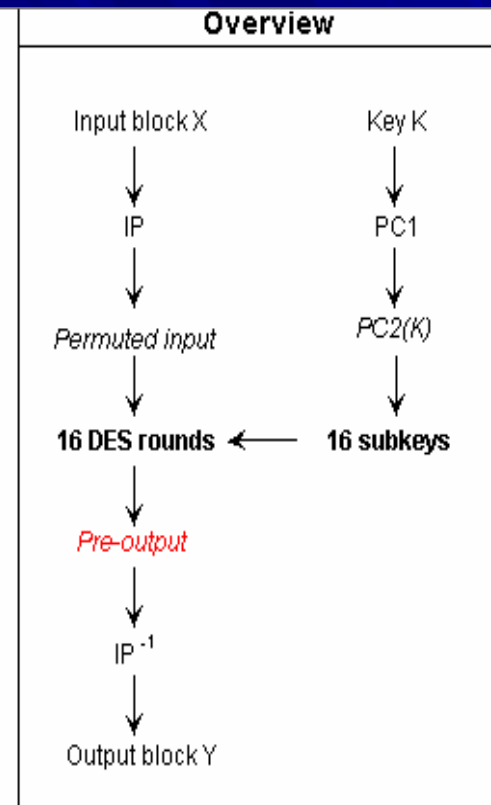
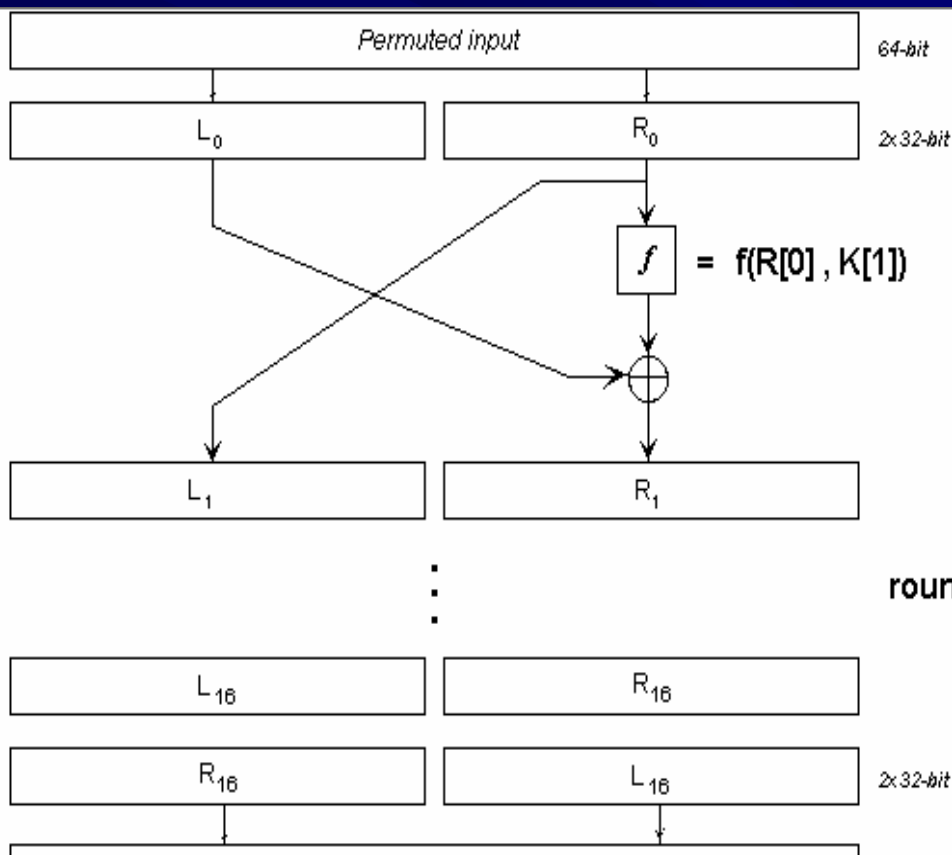
column row	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	0	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	3
⋮																

**S-box 8:**

column row	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

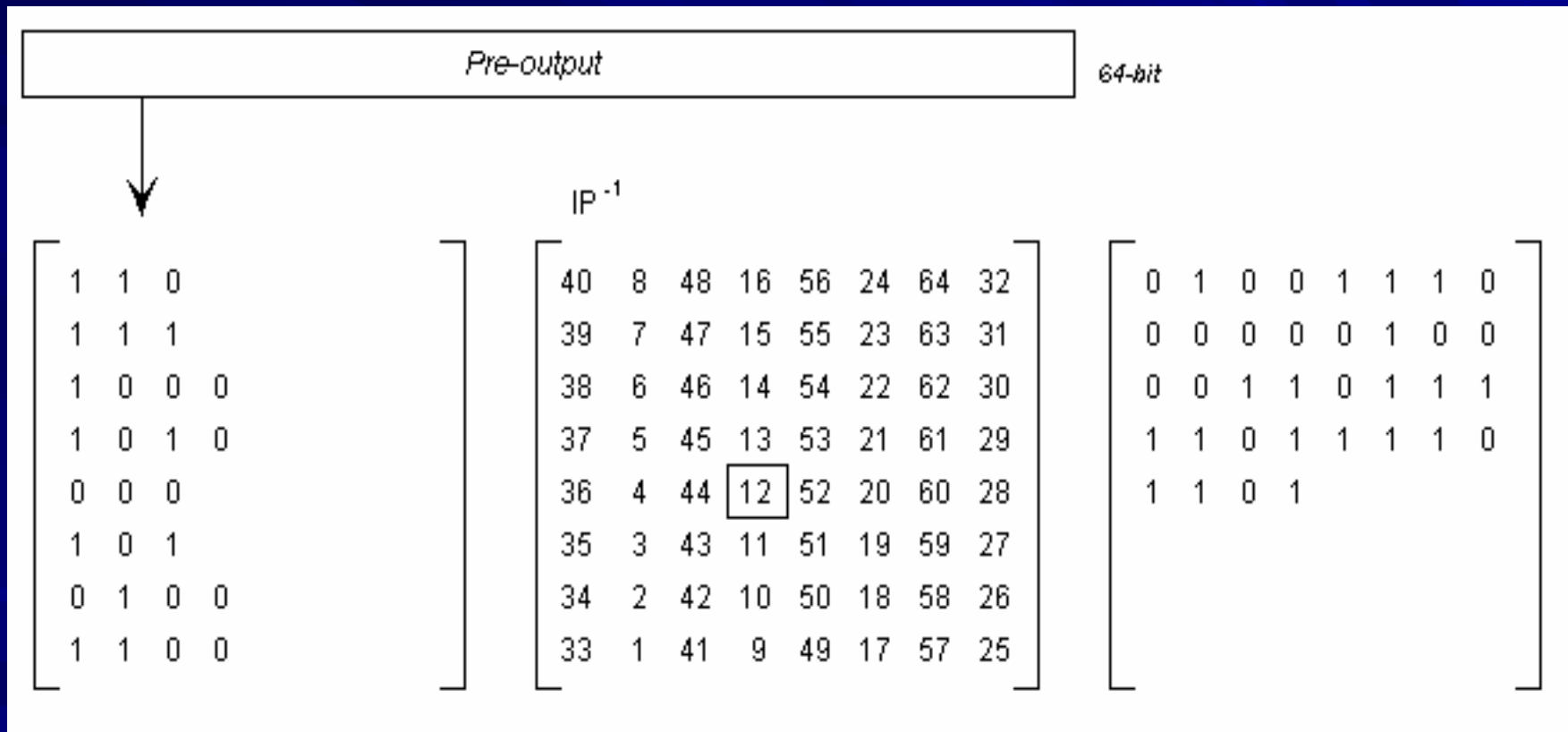
## 2. Chuẩn mã hoá dữ liệu DES





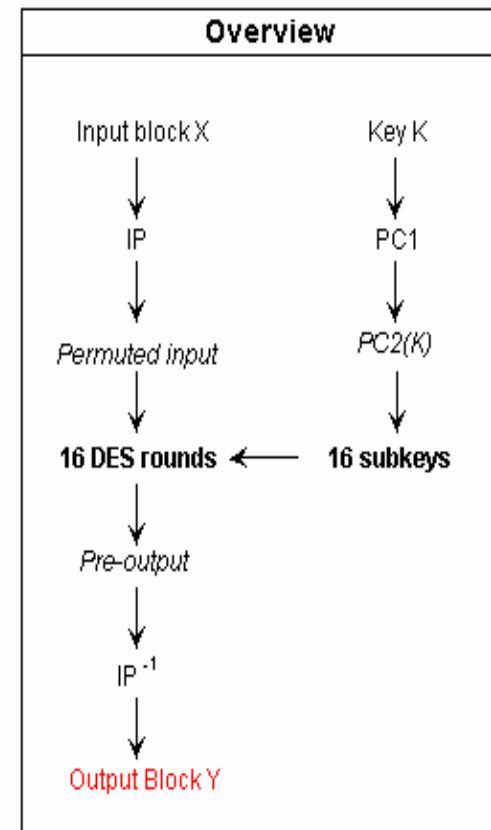
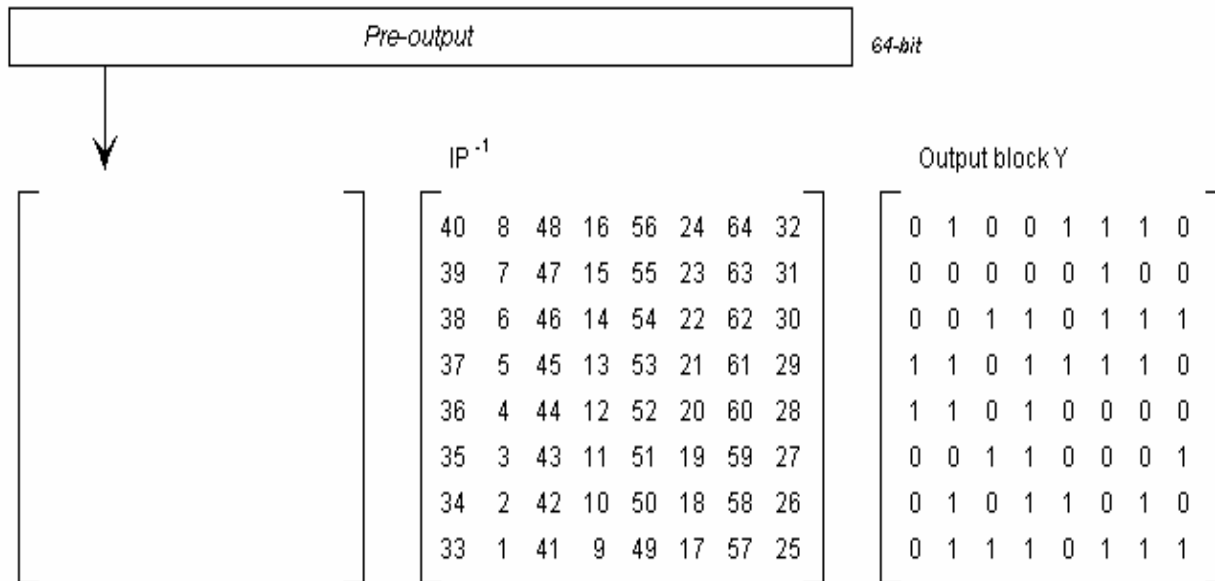
# 4. Giải thuật mã hoá hiện đại

## 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. Hệ mã hoá 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

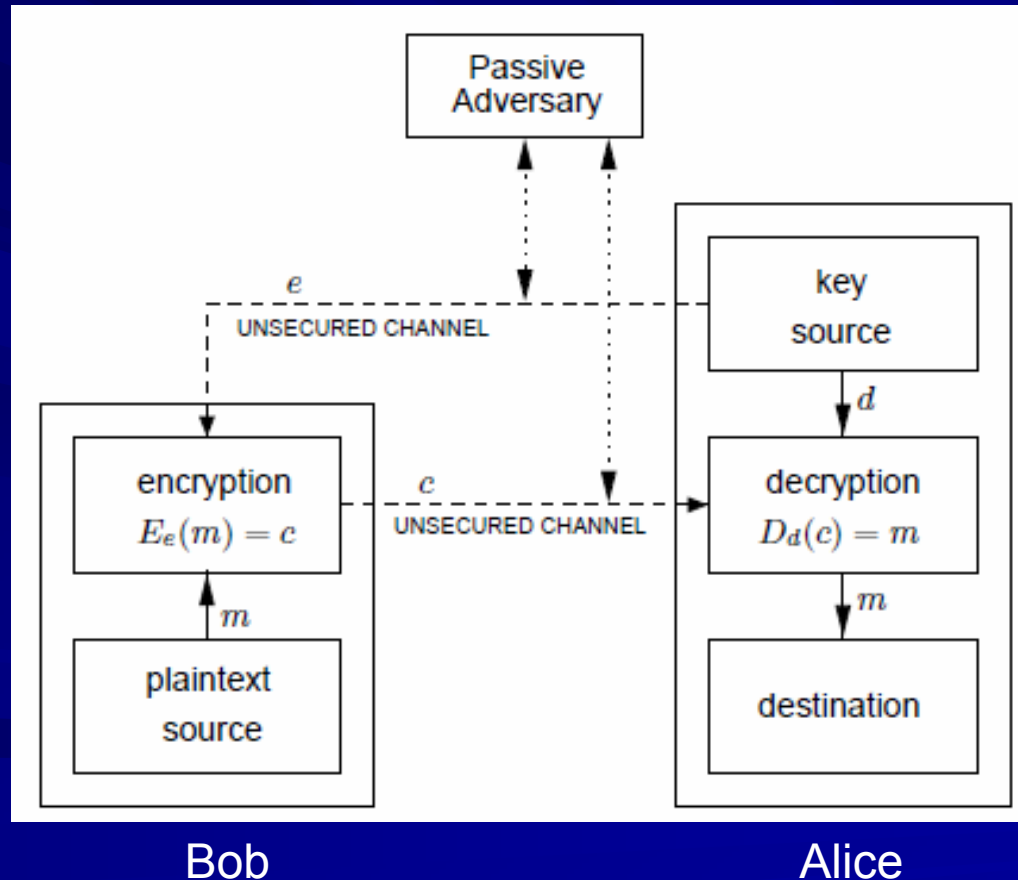
### 3. Hệ mã hoá công khai RSA

Ta 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.

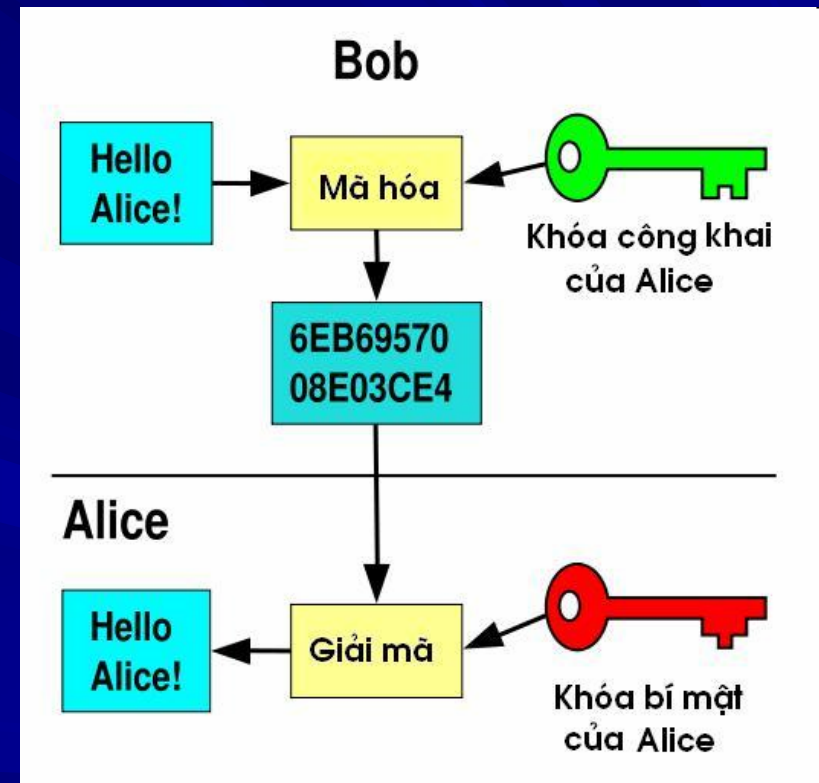
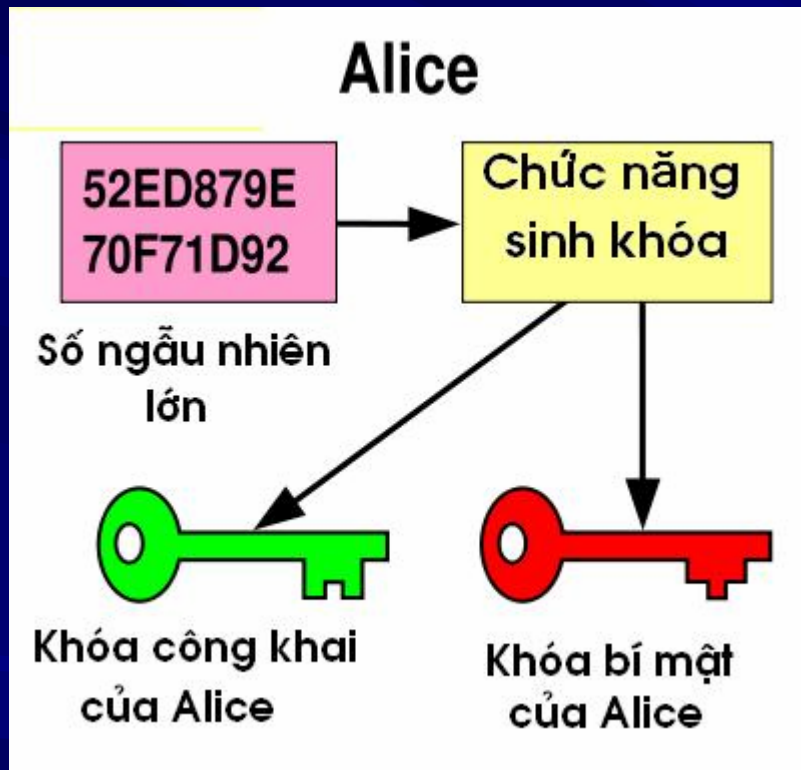
## 4. Giải thuật mã hoá hiện đại

### 3. Hệ mã hoá công khai RSA



# 4. Giải thuật mã hoá hiện đại

## 3. Hệ mã hoá công khai RSA

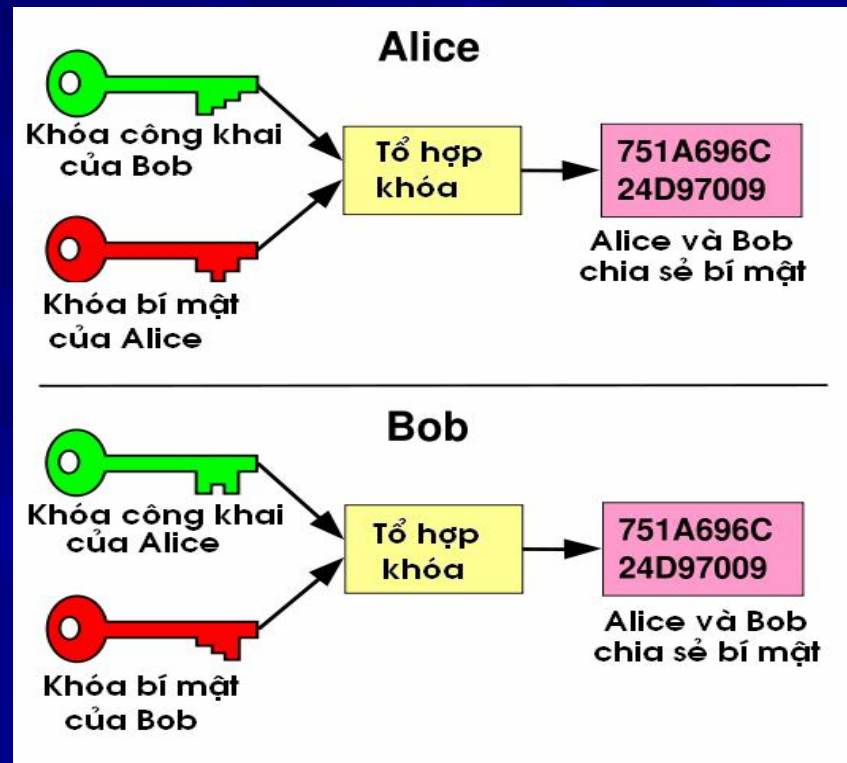
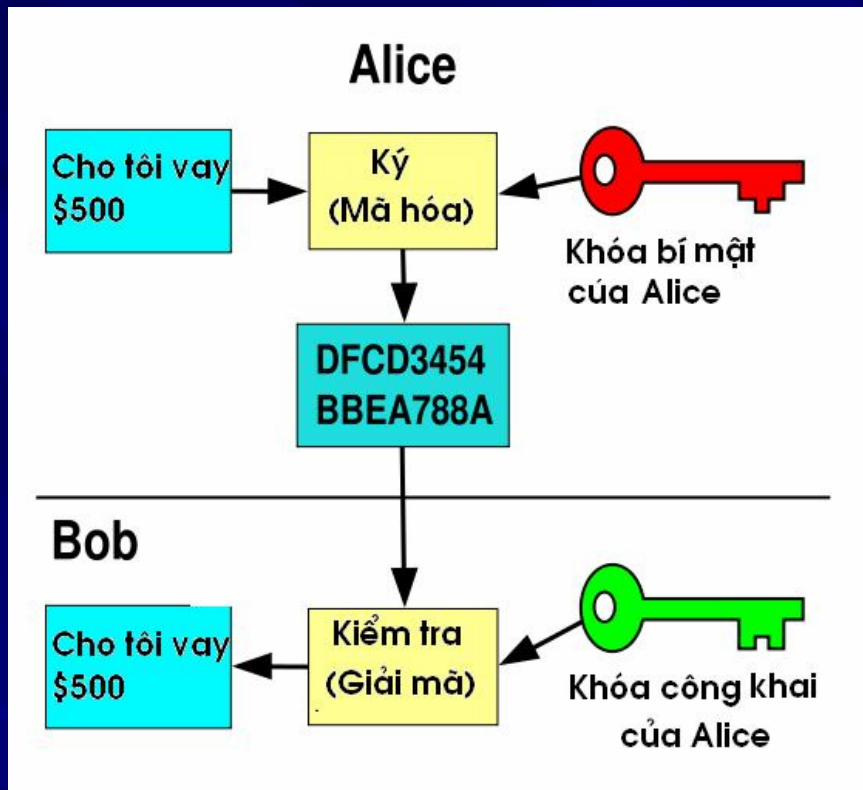


**Chọn một số ngẫu nhiên lớn để sinh cặp khóa.**

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

# 4. Giải thuật mã hoá hiện đại

## 3. Hệ mã hoá công khai RSA



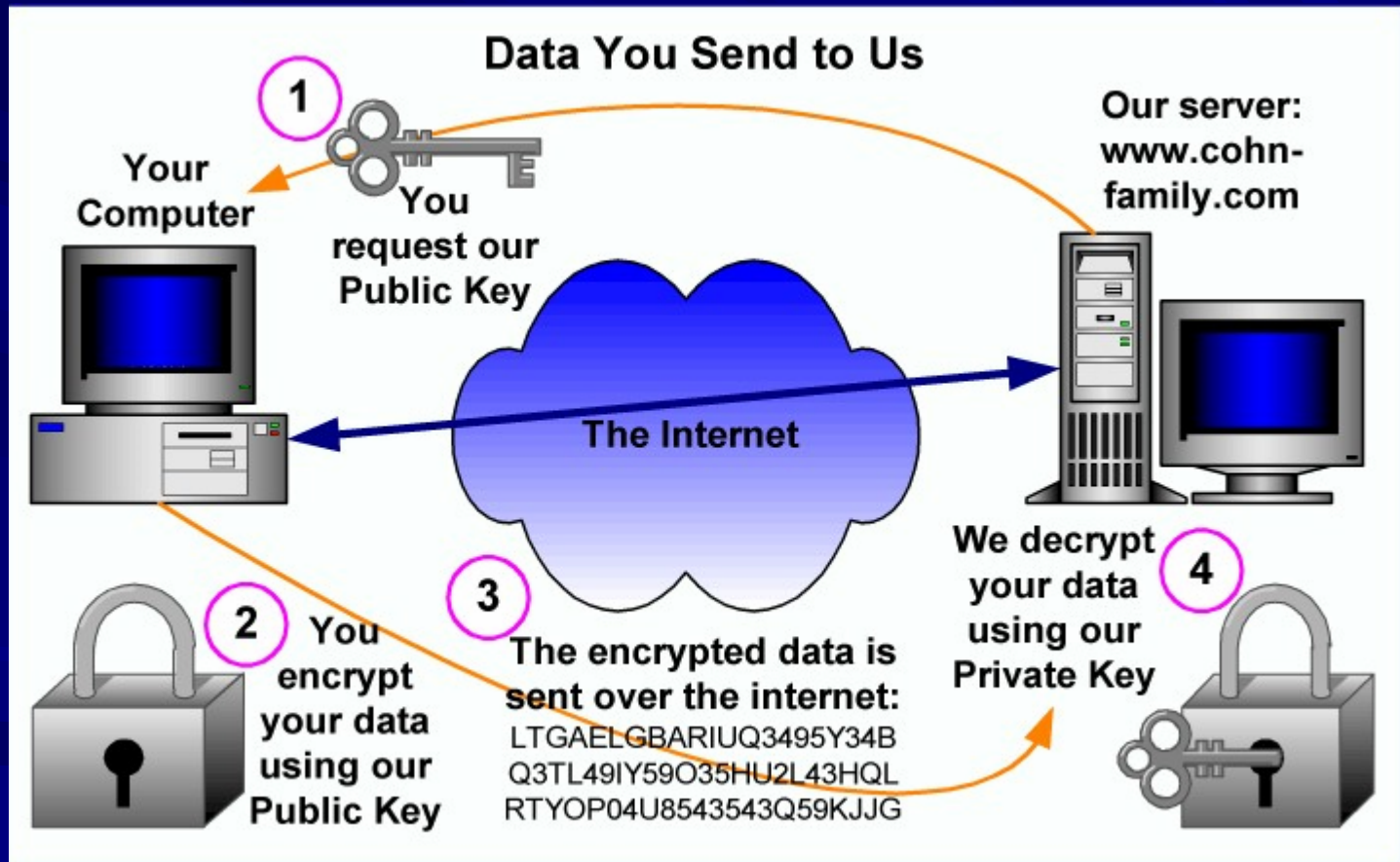
Dùng khoá bí mật để ký một thông báo; dùng khoá công khai để xác minh chữ ký.

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



# 4. Giải thuật mã hoá hiện đại

## 3. Hệ mã hoá công khai RSA





## 4. Giải thuật mã hoá hiện đại

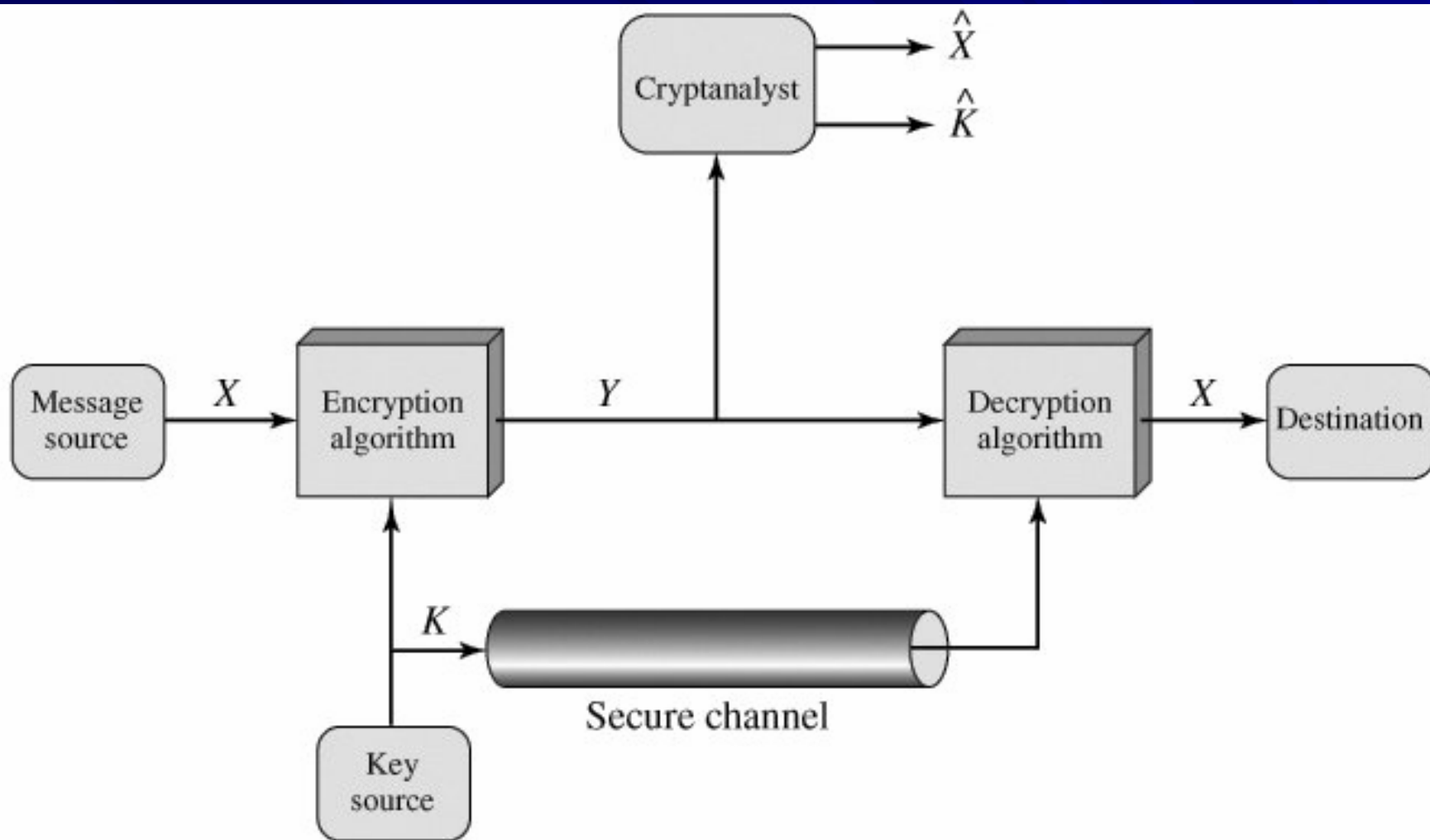
### 3. Hệ mã hoá công khai RSA

- 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 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:*

1. Tấn công chỉ dựa trên chuỗi mật mã (cryptogram-only attack): đối phương chỉ biết một vài mẫu chuỗi mật mã  $c$ .
2. 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.
3. Tấn công dựa trên văn bản được chọn (chosen-plaintext attack): những người tấn công có thể đã có được một số lượng tùy 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 <b>máy mã hoá</b> . Tự chọn văn bản p và mã hoá lấy được văn bản mã c tương ứng.
chosen ciphertext attack	Đột nhập được vào <b>máy giải mã</b> . Tự chọn văn bản mã c và giải mã lấy được văn bản p tương ứng.

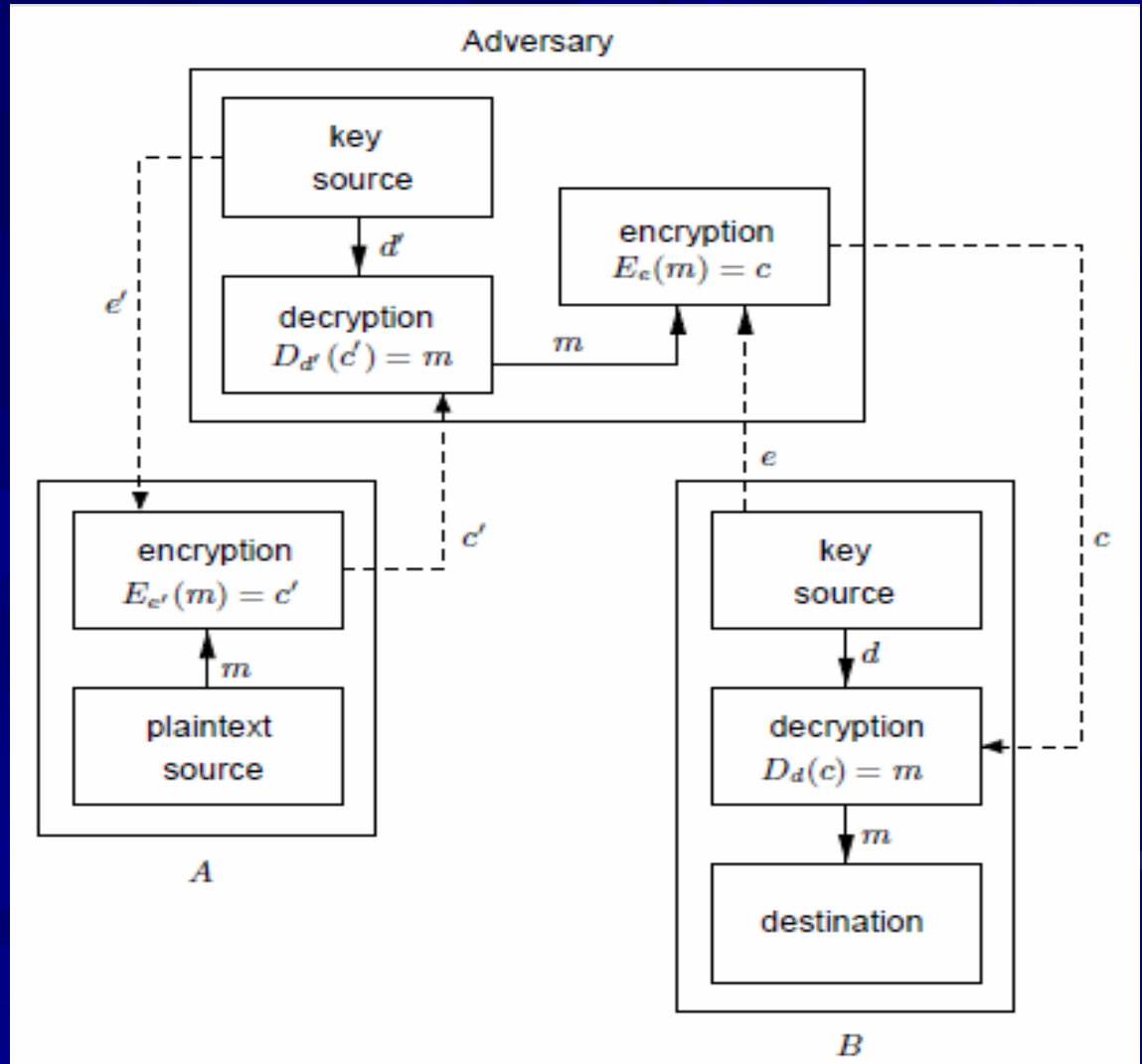
# 5. Bẻ gãy một hệ thống mật mã

Thời gian trung bình để tìm khoá theo kiểu vét cạn

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

## 6. Bài tập

1. 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:

- Mỗi biểu tượng trong số chín biểu tượng xuất hiện trong mảng dưới đây ( $\triangle \blacktriangleleft \blacktriangleright \bigcirc \heartsuit \spadesuit \diamondsuit \clubsuit \bullet$ ) mã hóa duy nhất một trong các chữ số 1 đến 9.
- Cột ngoài cùng bên phải là các tổng số ở mỗi hàng
- Hàng dưới cùng cho các tổng số ở mỗi cột.
- Một dấu hỏi có thể đại diện cho bất kỳ một hoặc hai chữ số và không nhất thiết phải cùng một số trong mỗi trường hợp.



## 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:
  - i. Vigenère
  - ii. Hill.
  - iii. Affine
  - iv. Playfair
  - v. Solitaire

## 6. Bài tập

5. Nêu chi tiết cơ chế hoạt động của giải thuật mã hoá DES.
6. Trình bày tổng quan về cơ chế hoạt động của các giải thuật RC4 và RSA.
7. Viết ứng dụng mã hoá và giải mã cho một giải thuật mã hoá hiện đại tùy chọn.

**THANK YOU!**