

MẬT MÃ HỌC

cuu duong than cong . com

NỘI DUNG MÔN HỌC

Chương 1: Giới thiệu - Mã hoá cổ điển

Chương 2: Mã hoá hiện đại

Chương 3: Mã hoá khoá công khai và quản lý khoá

Chương 4: Chứng thực thông điệp

Chương 5: Chữ ký số

Chương 6: Các giao thức và ứng dụng

CHƯƠNG 2

MÃ HOÁ HIỆN ĐẠI

Nội dung

1. Giới thiệu mã hoá hiện đại
2. Chuẩn mã hoá dữ liệu DES
3. Tiêu chuẩn mã hoá tiên tiến AES
4. Hệ mã hoá khoá công khai RSA
5. Bài tập

1. Giới thiệu 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...

1. Giới thiệu mã hoá hiện đại

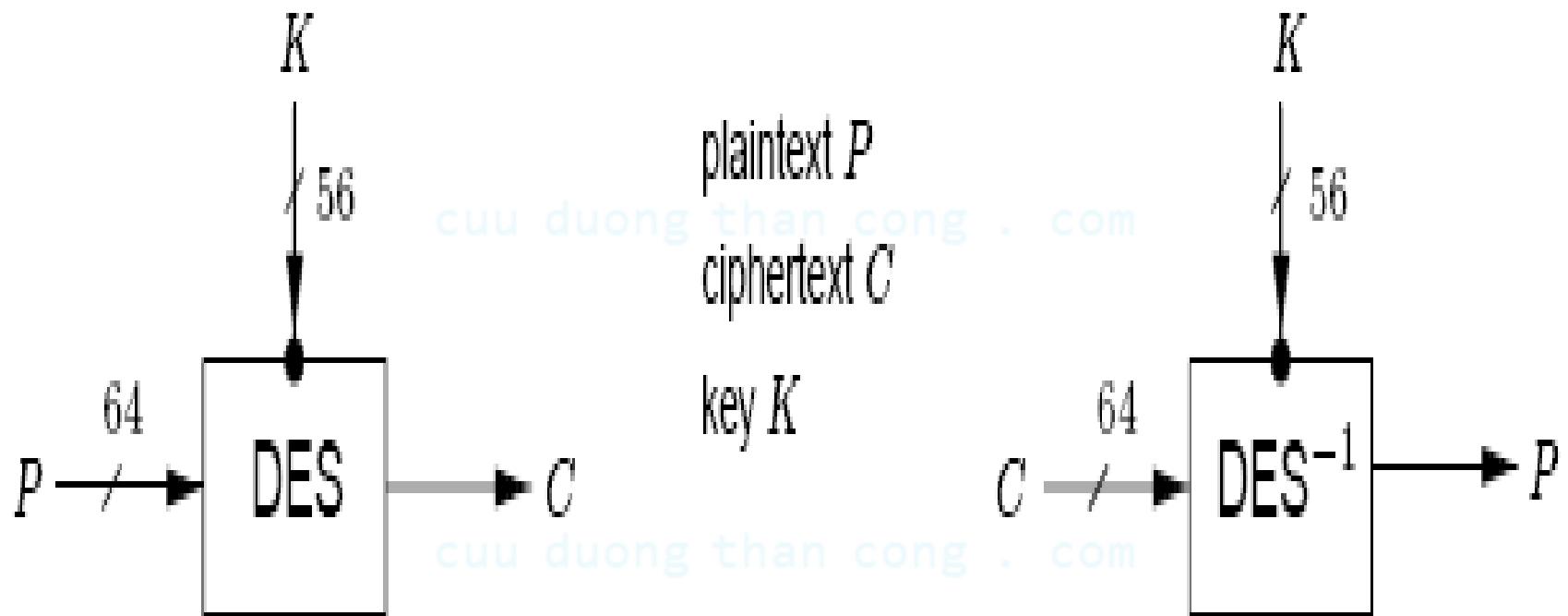
Phân loại

- 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

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.

2. Chuẩn mã hoá dữ liệu DES



2. Chuẩn mã hoá dữ liệu DES

Lịch sử giải thuật 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.

2. Chuẩn mã hoá dữ liệu DES

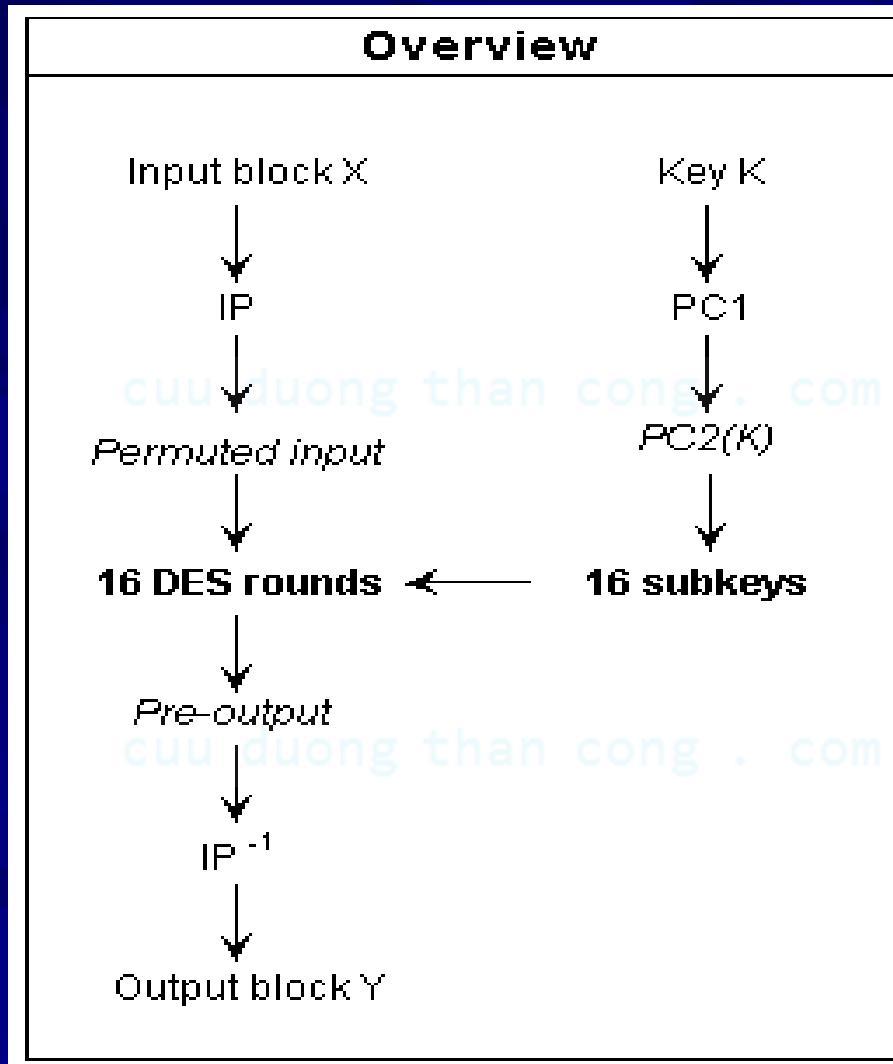
- 07.1998: Thiết bị thám mã Deep Crack của tổ chức Electronic Frontier Foundation phá được một khoá của DES trong vòng 56 giờ.
- 01.1999: Deep Crack cùng với distributed.net phá được DES trong 22 giờ 15 phút.
- 25.10.1999: Triple DES được khuyến cáo sử dụng cho các hệ thống quan trọng.
- 26.05.2002: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

2. Chuẩn mã hoá dữ liệu DES

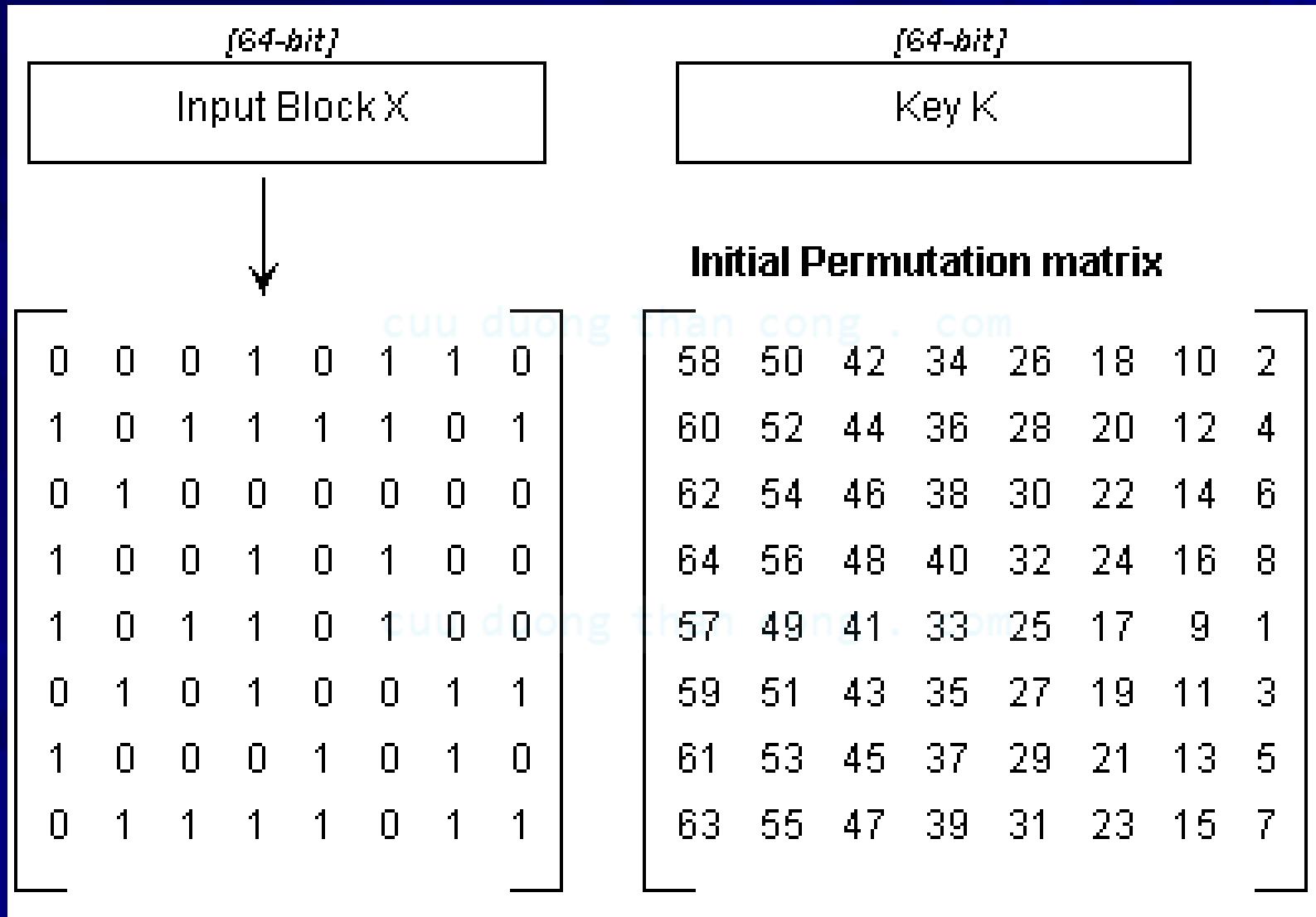
Giải thuật:

- 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.

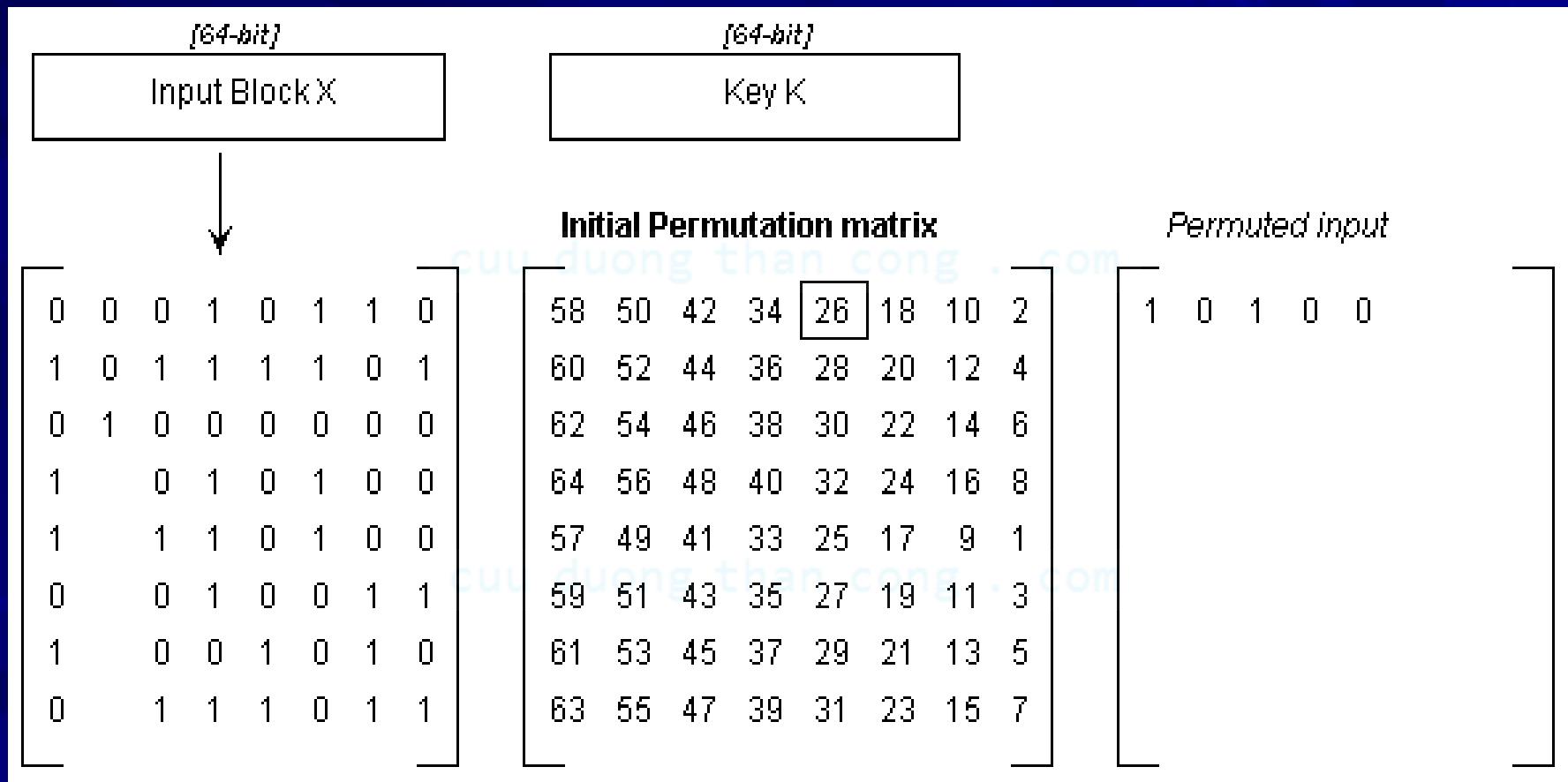
2. Chuẩn mã hoá dữ liệu DES



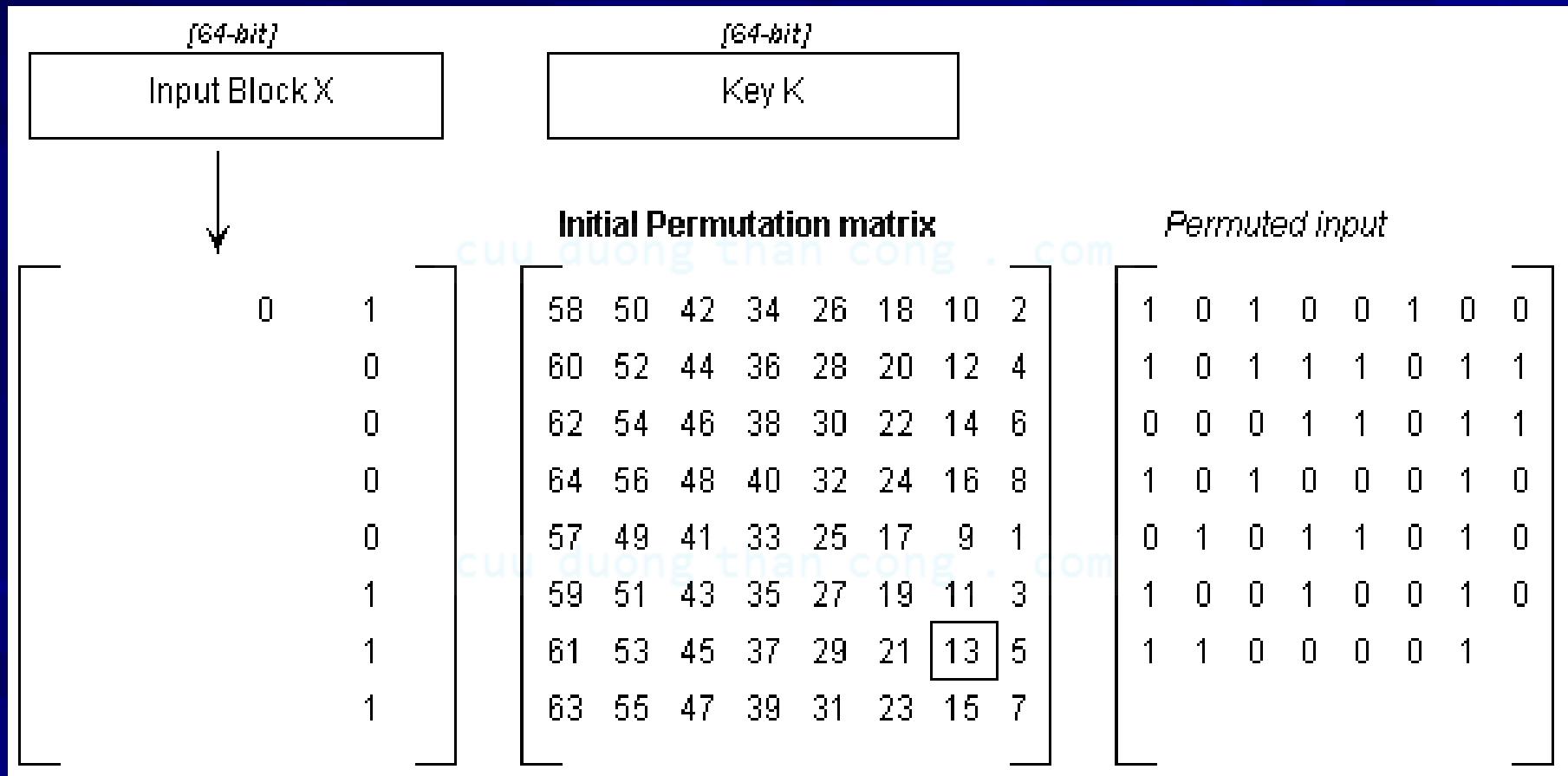
2. Chuẩn mã hoá dữ liệu DES



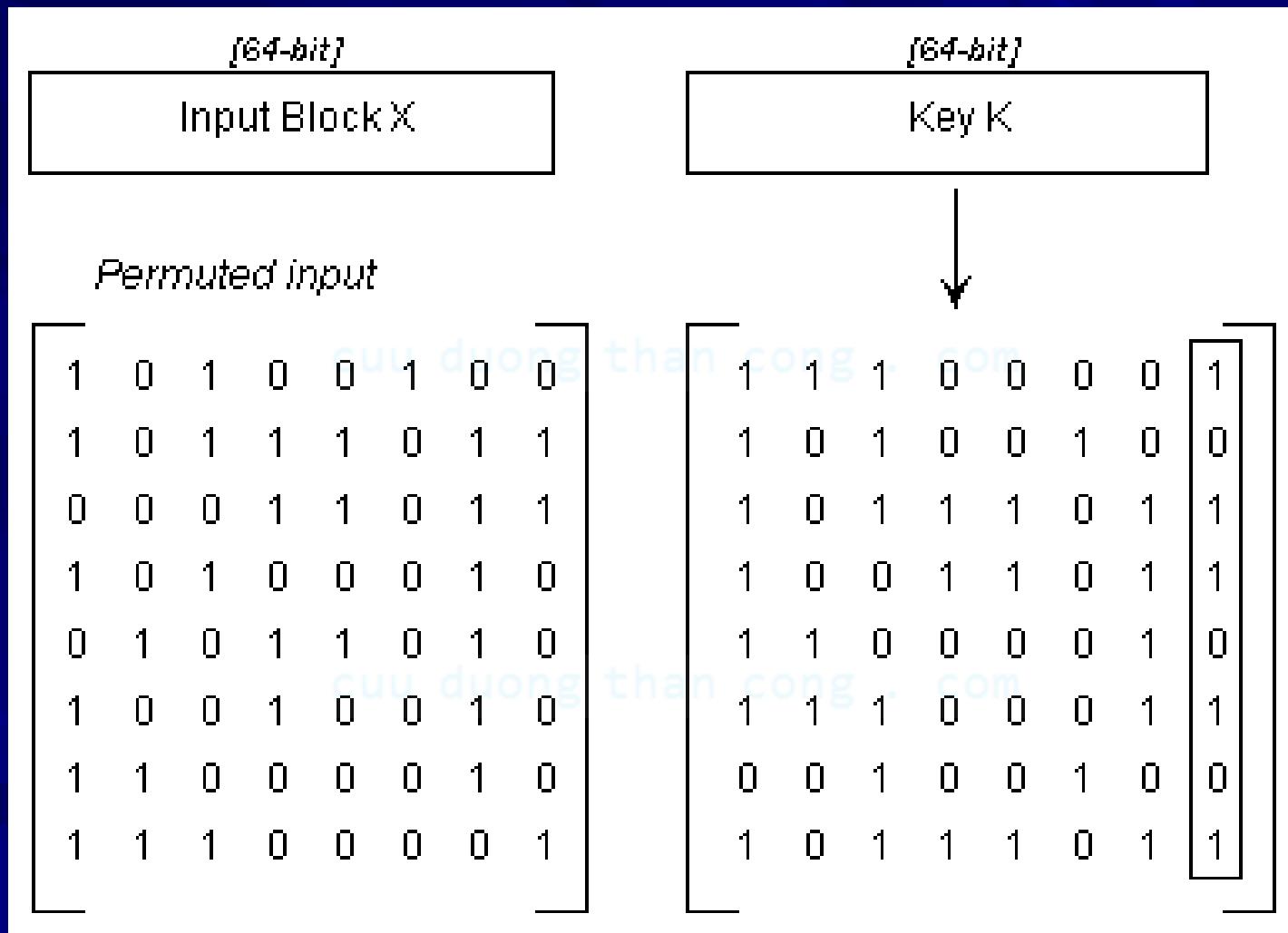
2. Chuẩn mã hoá dữ liệu DES



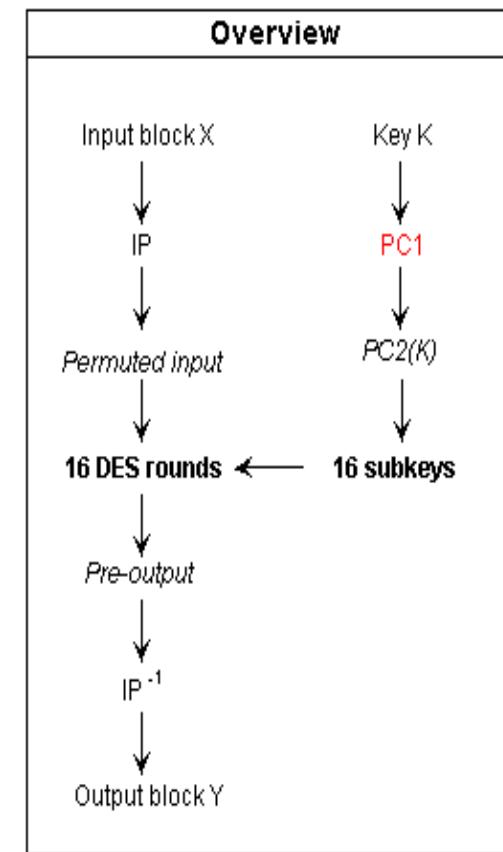
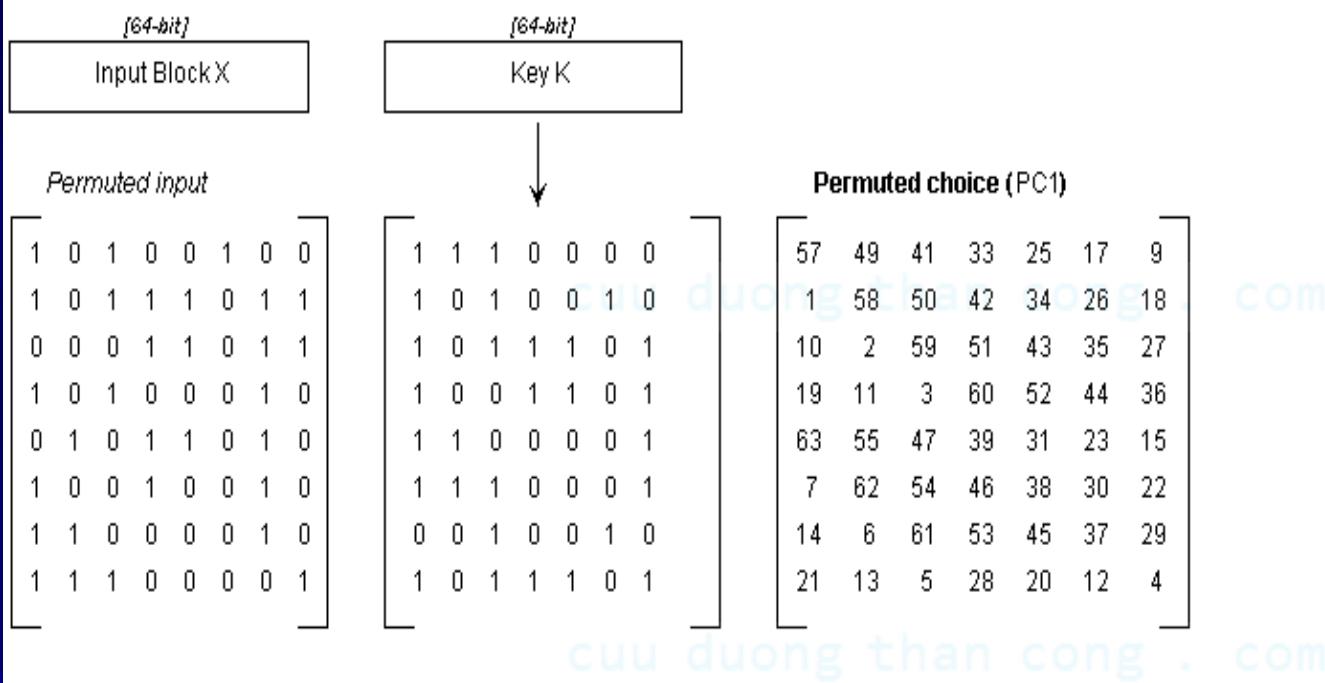
2. Chuẩn mã hoá dữ liệu DES



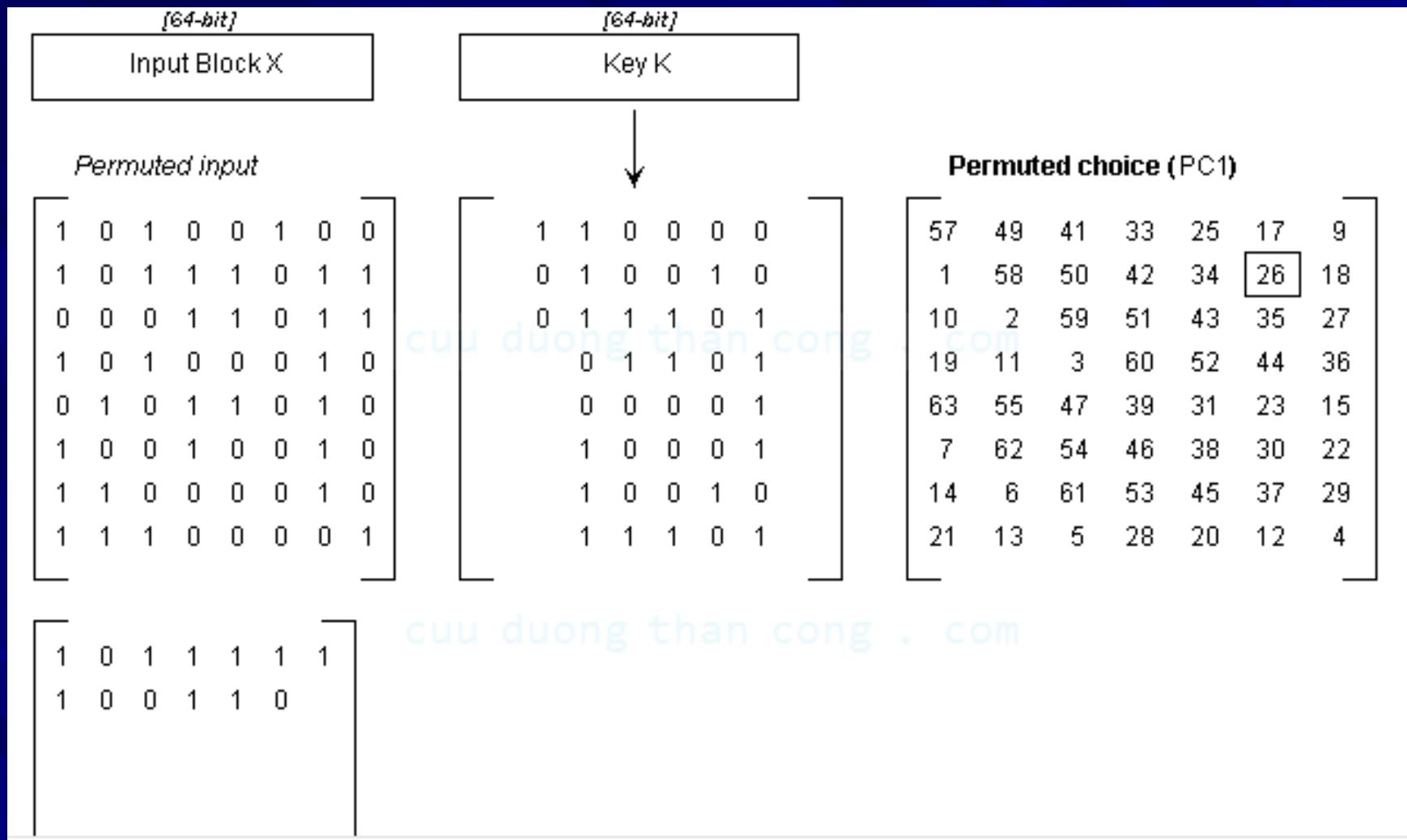
2. Chuẩn mã hoá dữ liệu DES



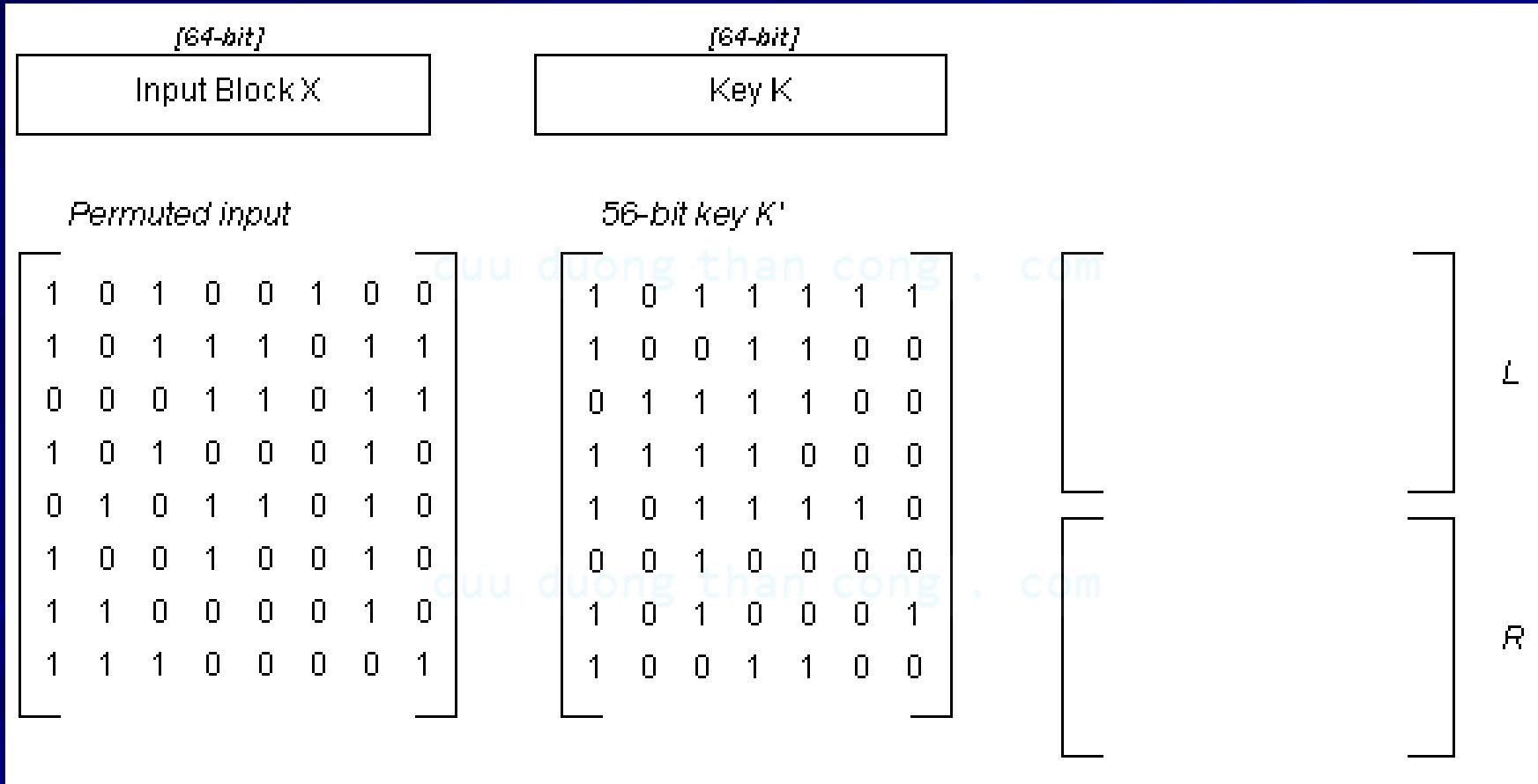
2. Chuẩn mã hoá dữ liệu DES



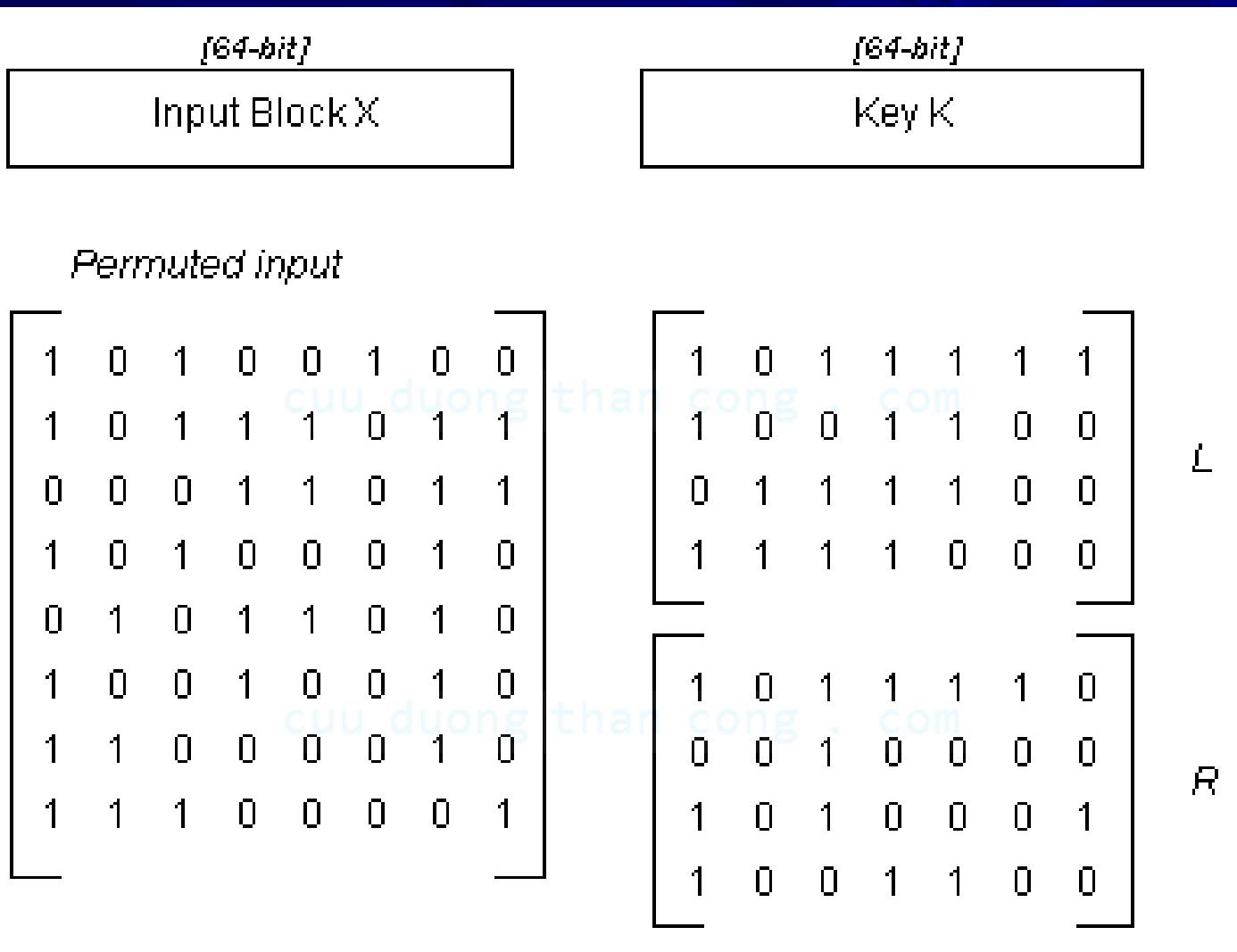
2. Chuẩn mã hoá dữ liệu DES



2. Chuẩn mã hoá dữ liệu DES

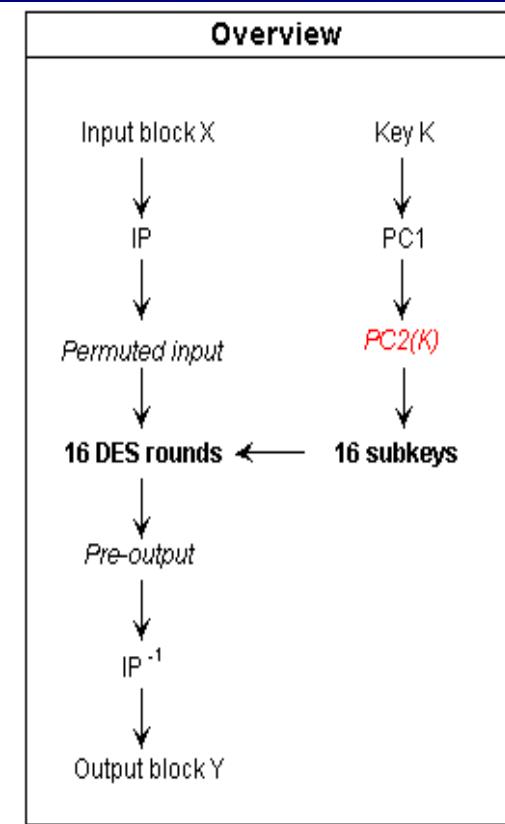


2. Chuẩn mã hoá dữ liệu DES



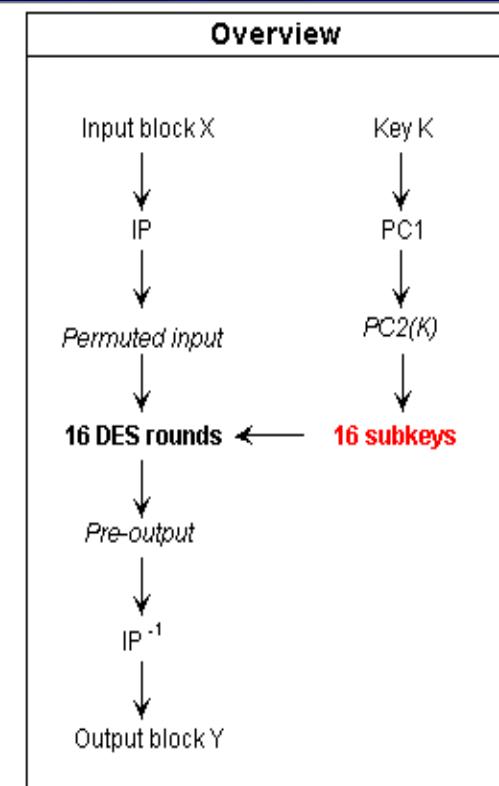
2. Chuẩn mã hoá dữ liệu DES

[64-bit]	[64-bit]
Input Block X	Key K
<i>Permuted input</i>	<i>K'</i>
$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \end{bmatrix}$
<i>PC2</i>	
	$\begin{bmatrix} 14 & 17 & 11 & 24 & 1 & 5 \\ 3 & 28 & 15 & 6 & 21 & 10 \\ 23 & 19 & 12 & 4 & 26 & 8 \\ 16 & 7 & 27 & 20 & 13 & 2 \\ 41 & 52 & 31 & 37 & 47 & 55 \\ 30 & 40 & 51 & 45 & 33 & 48 \\ 44 & 49 & 39 & 56 & 34 & 53 \\ 46 & 42 & 50 & 36 & 29 & 32 \end{bmatrix}$
K[1]	
$\begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$	

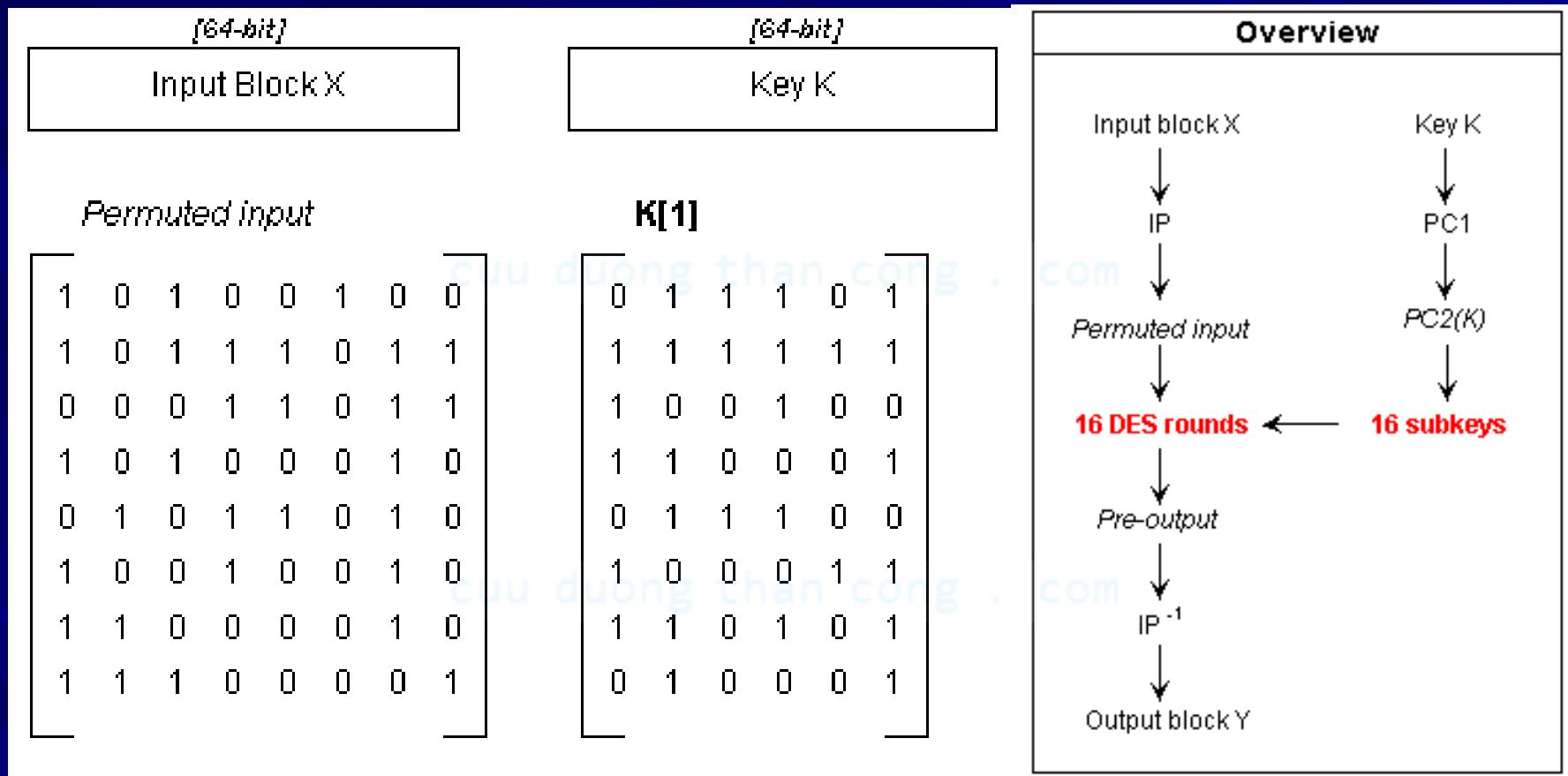


2. Chuẩn mã hoá dữ liệu DES

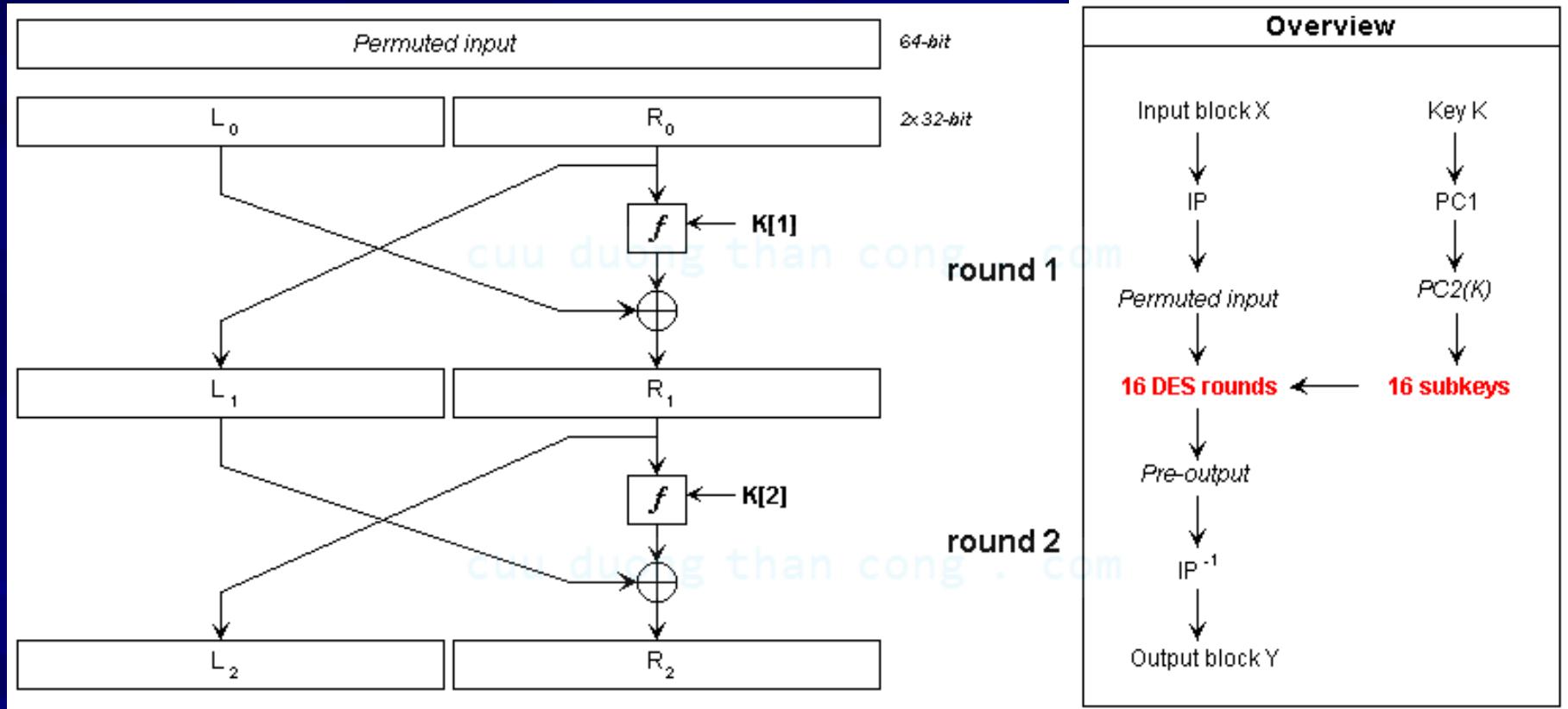
[64-bit]	[64-bit]
Input Block X	Key K
<i>Permuted input</i>	
$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}$
<i>K[1]</i>	<i>K[2]</i>
$\begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$	$\begin{bmatrix} \quad & \quad & \quad & \quad & \quad & \quad & \quad \\ \quad & \quad & \quad & \quad & \quad & \quad & \quad \\ \quad & \quad & \quad & \quad & \quad & \quad & \quad \\ \quad & \quad & \quad & \quad & \quad & \quad & \quad \end{bmatrix}$
<i>K[16]</i>	
	$\begin{bmatrix} \quad & \quad & \quad & \quad & \quad & \quad & \quad \\ \quad & \quad & \quad & \quad & \quad & \quad & \quad \\ \quad & \quad & \quad & \quad & \quad & \quad & \quad \\ \quad & \quad & \quad & \quad & \quad & \quad & \quad \end{bmatrix}$
	$\begin{bmatrix} 14 & 17 & 11 & 24 & 1 & 5 \\ 3 & 28 & 15 & 6 & 21 & 10 \\ 23 & 19 & 12 & 4 & 26 & 8 \\ 16 & 7 & 27 & 20 & 13 & 2 \\ 41 & 52 & 31 & 37 & 47 & 55 \\ 30 & 40 & 51 & 45 & 33 & 48 \\ 44 & 49 & 39 & 56 & 34 & 53 \\ 46 & 42 & 50 & 36 & 29 & 32 \end{bmatrix}$



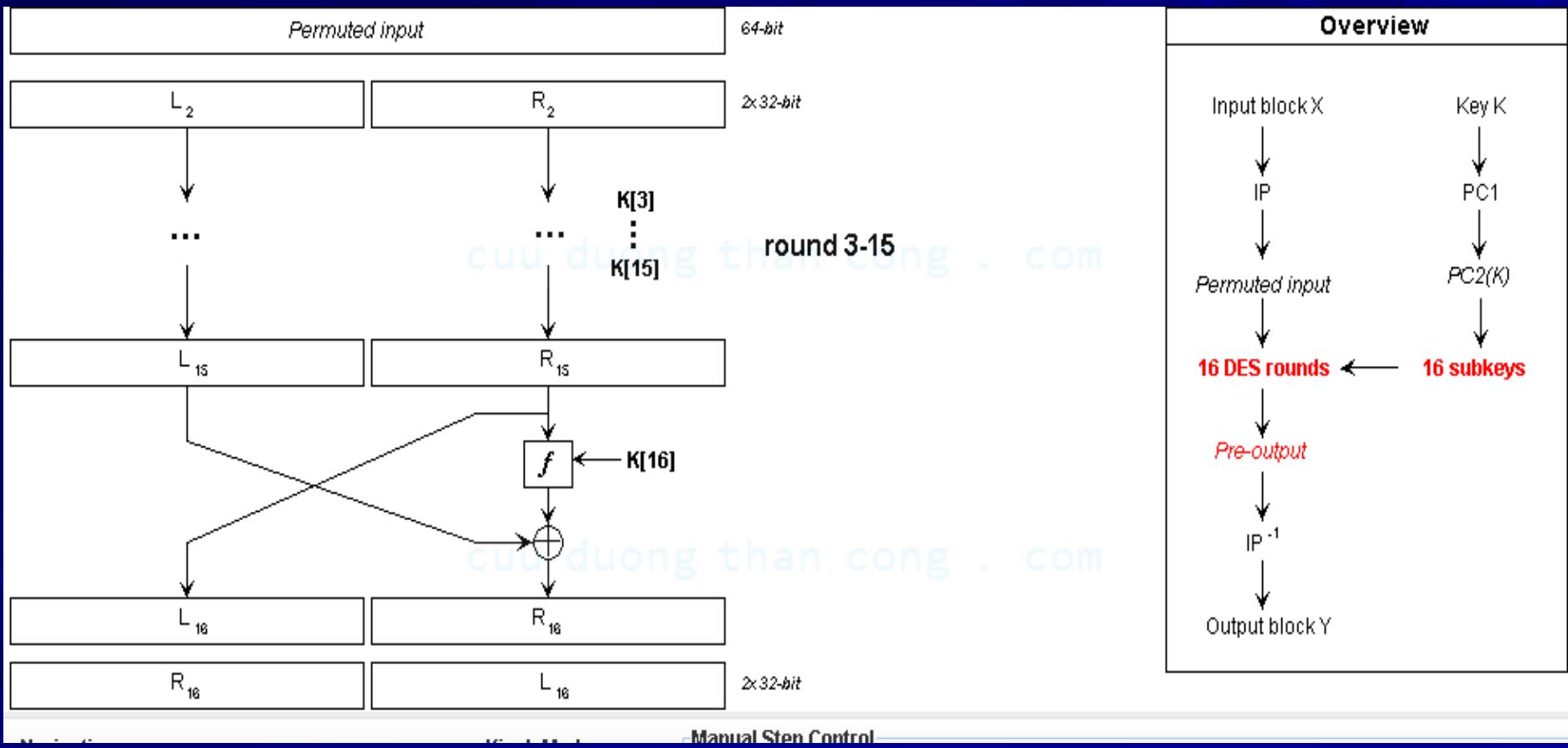
2. Chuẩn mã hoá dữ liệu DES



2. Chuẩn mã hoá dữ liệu DES

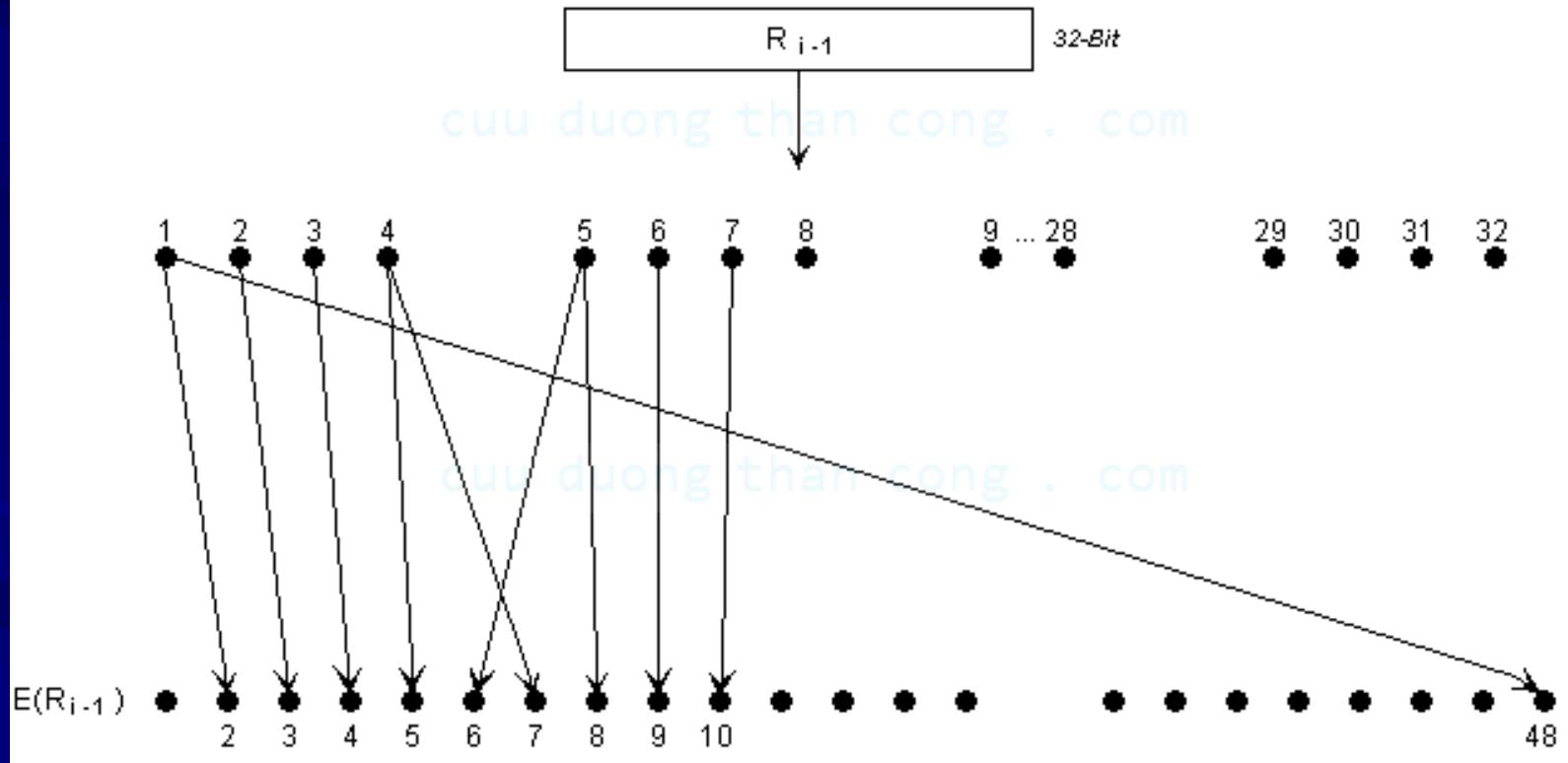


2. Chuẩn mã hoá dữ liệu DES



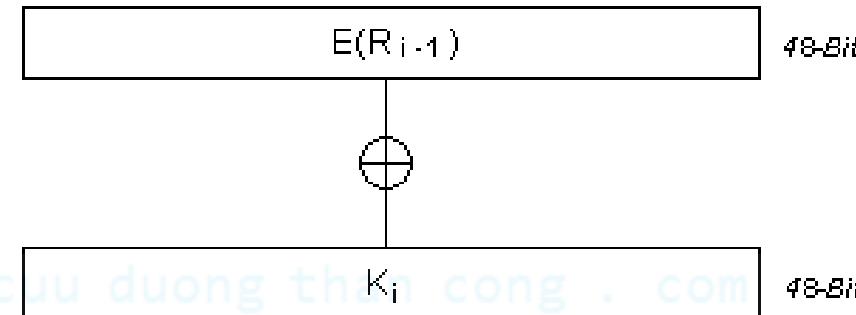
2. Chuẩn mã hoá dữ liệu DES

Function f :



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 downwards from each column to labels $B[1]$, $B[2]$, $B[3]$, $B[4]$, $B[5]$, $B[6]$, $B[7]$, and $B[8]$.

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

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:

cuu duong than cong . com

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

cuu duong than cong . com

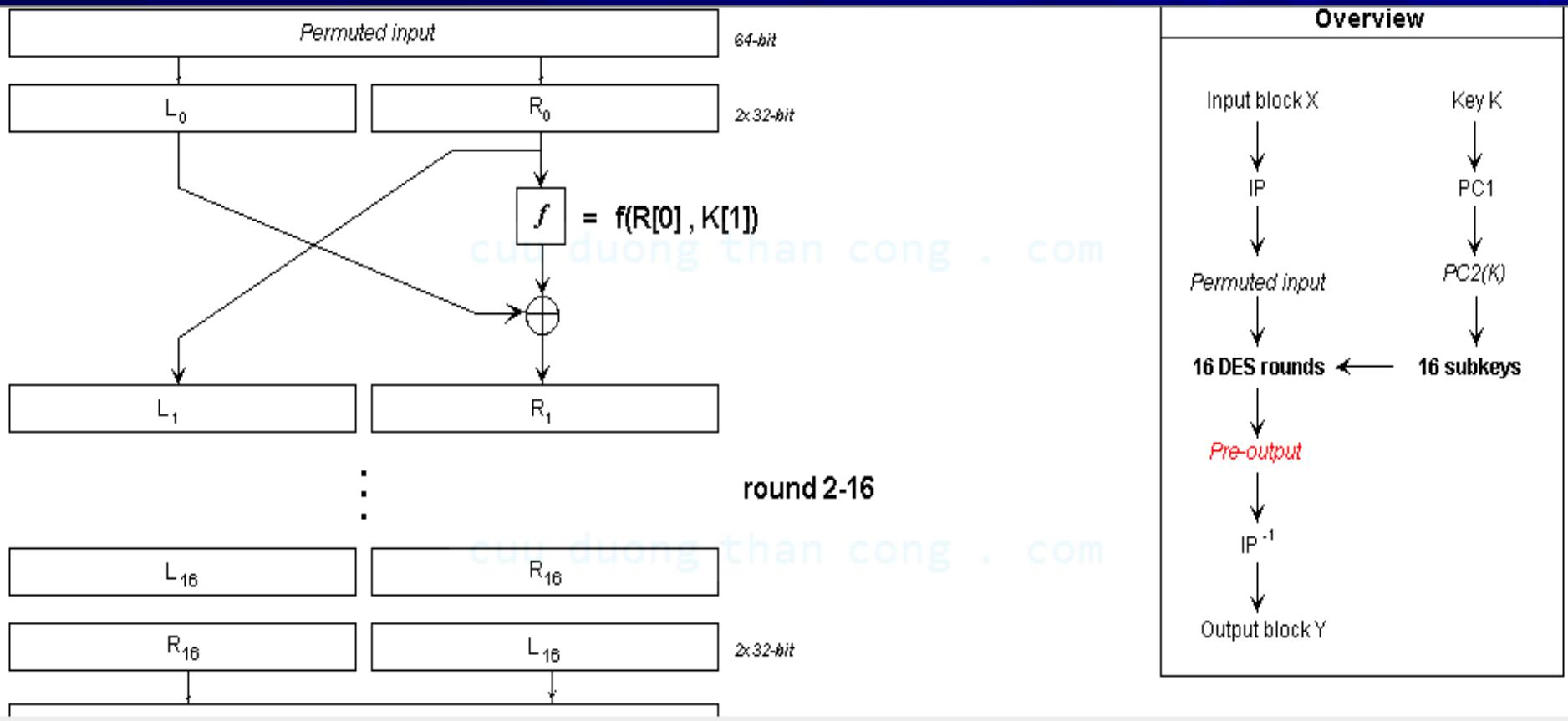
•

•

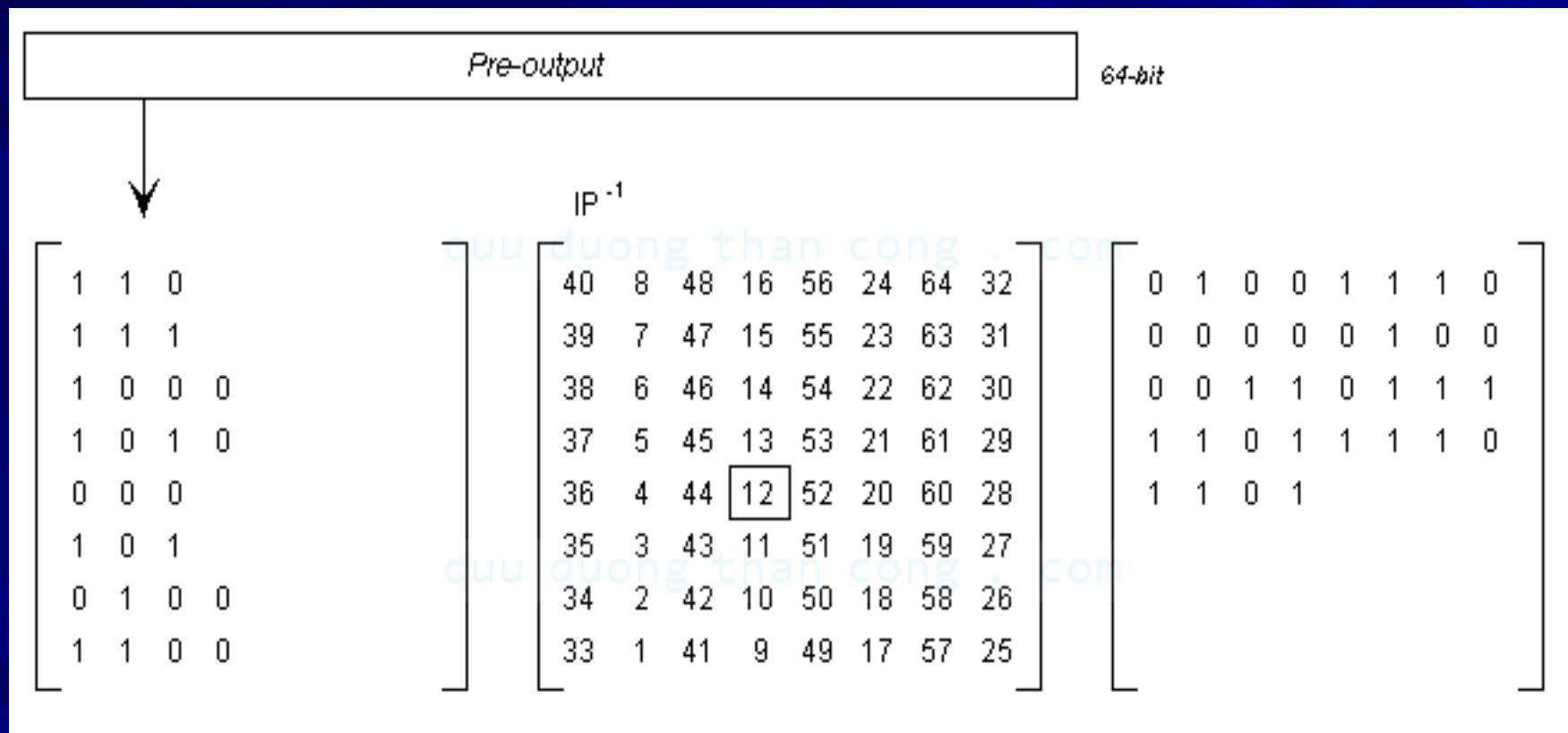
S-box 8:

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

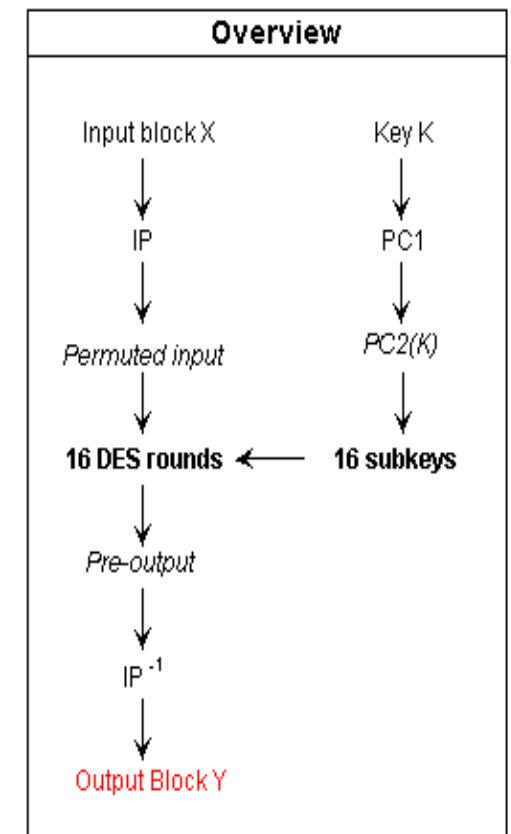
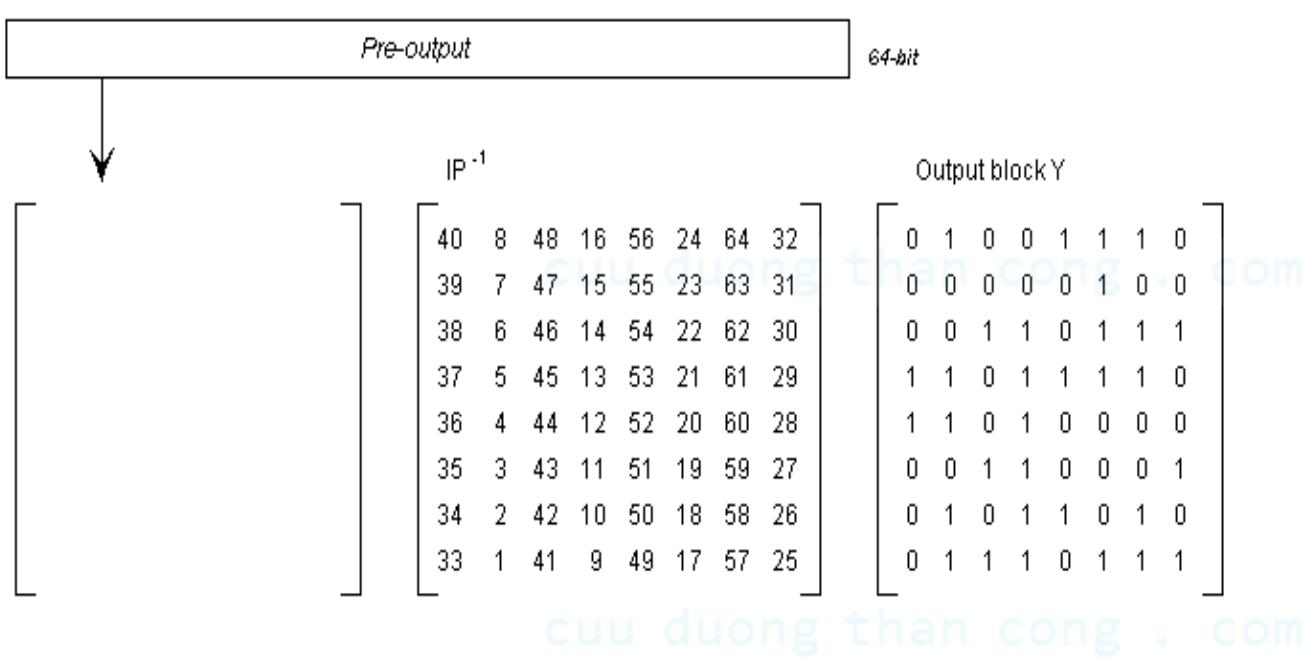
2. Chuẩn mã hoá dữ liệu DES



2. Chuẩn mã hoá dữ liệu DES



2. Chuẩn mã hoá dữ liệu DES



3. Tiêu chuẩn mã hoá tiên tiến 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.

3. Tiêu chuẩn mã hoá tiên tiến 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.

3. Tiêu chuẩn mã hoá tiên tiến 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
```

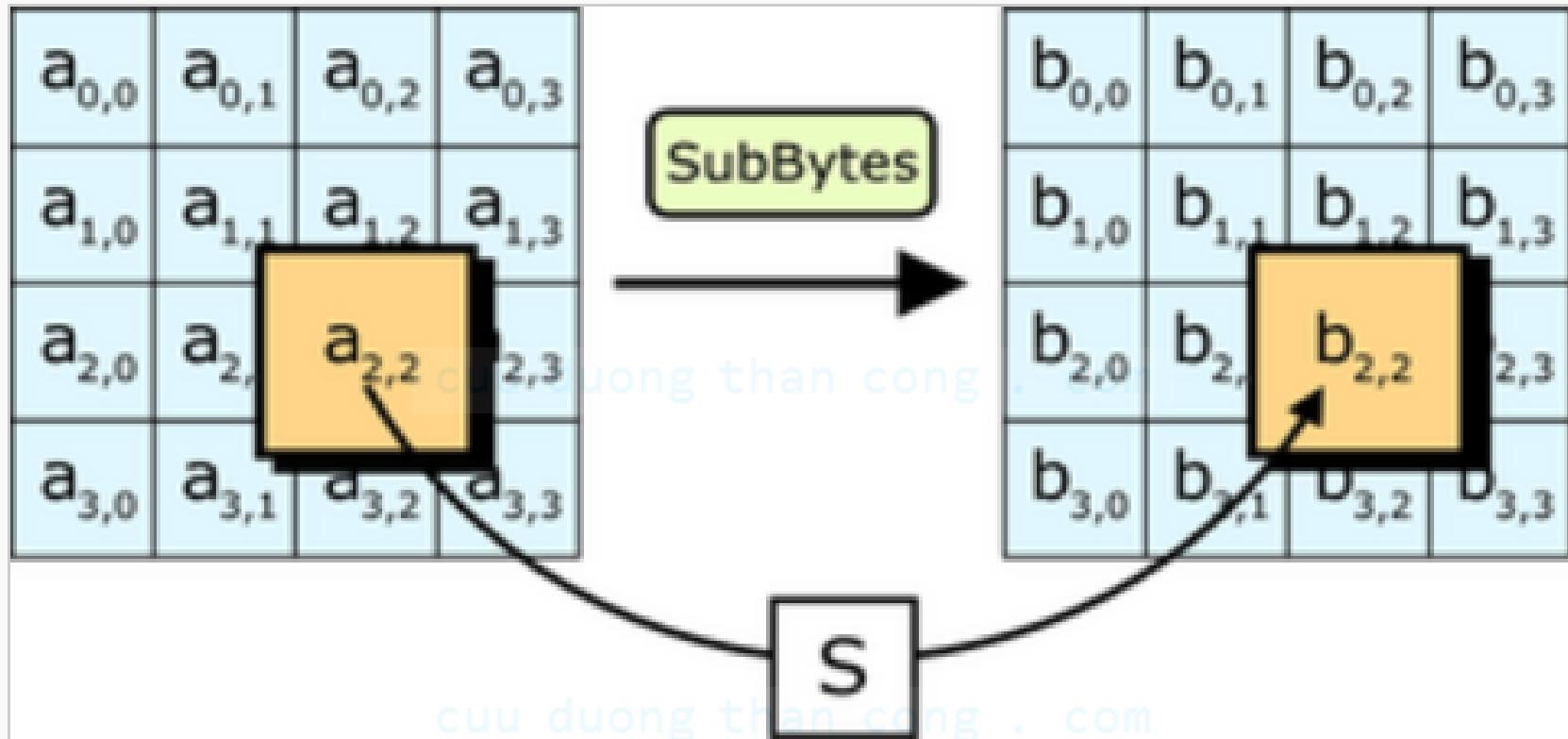
3. Tiêu chuẩn mã hoá tiên tiến AES

- 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.

3. Tiêu chuẩn mã hoá tiên tiến 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.

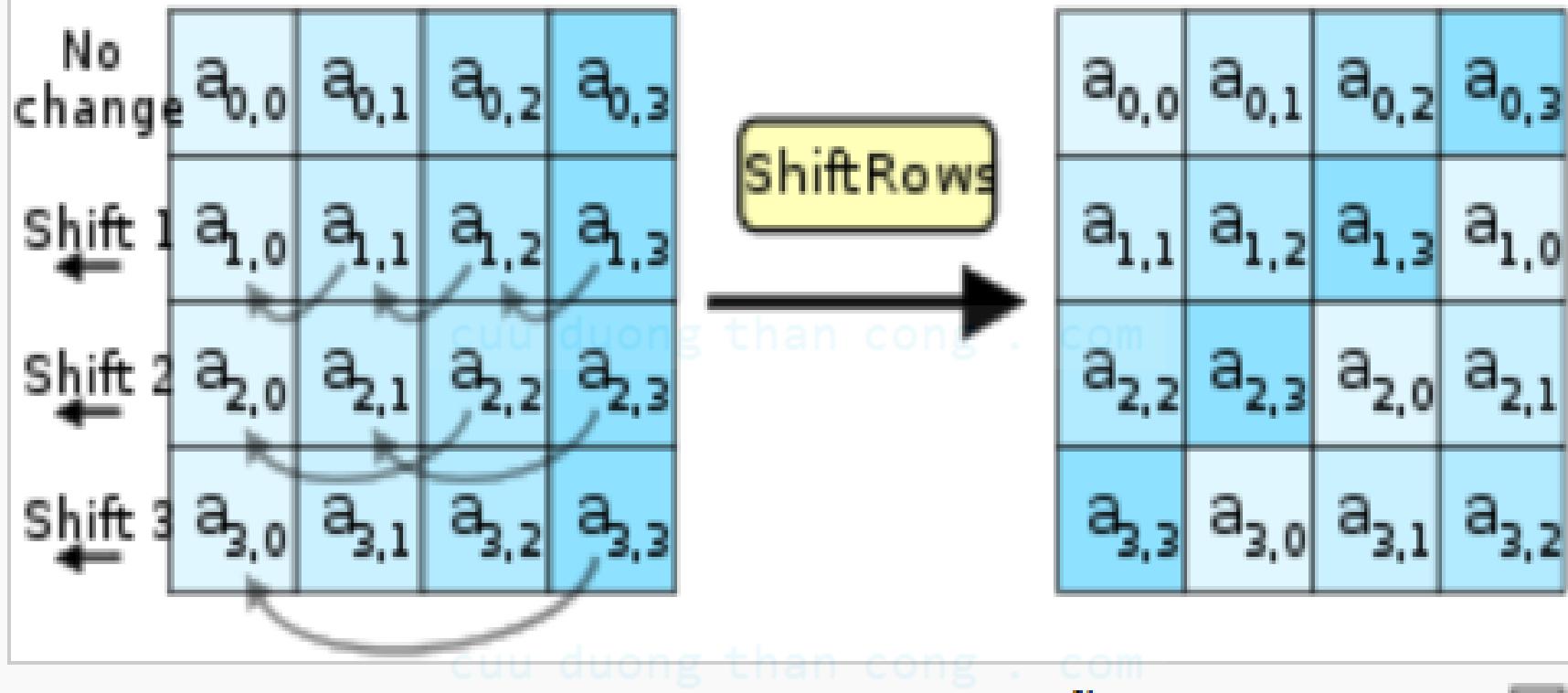
3. Tiêu chuẩn mã hoá tiên tiến AES



Trong bước SubBytes, mỗi byte được thay thế bằng một byte theo bảng tra, S : $b_{ij} = S(a_{ij})$.



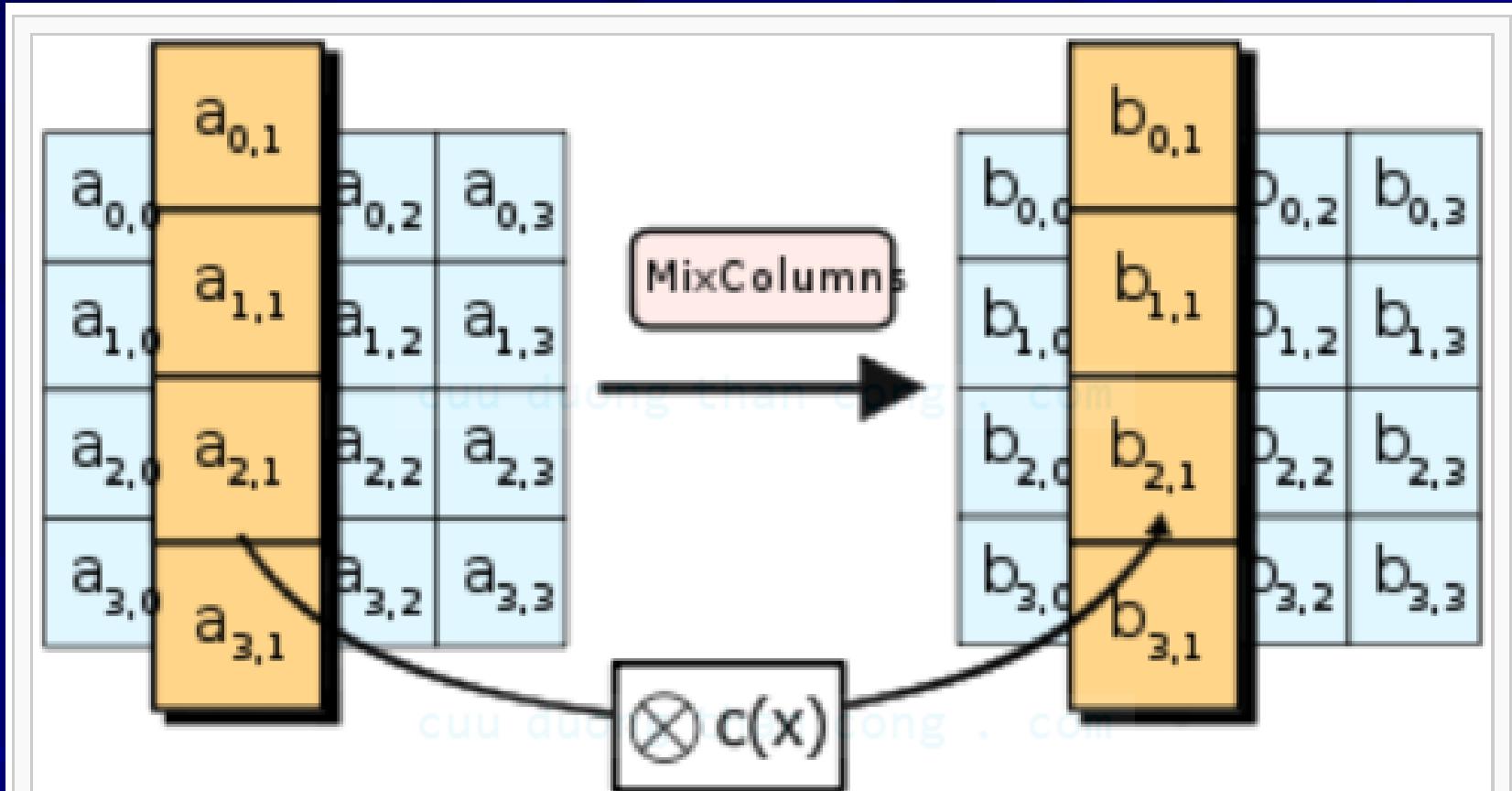
3. Tiêu chuẩn mã hoá tiên tiến AES



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



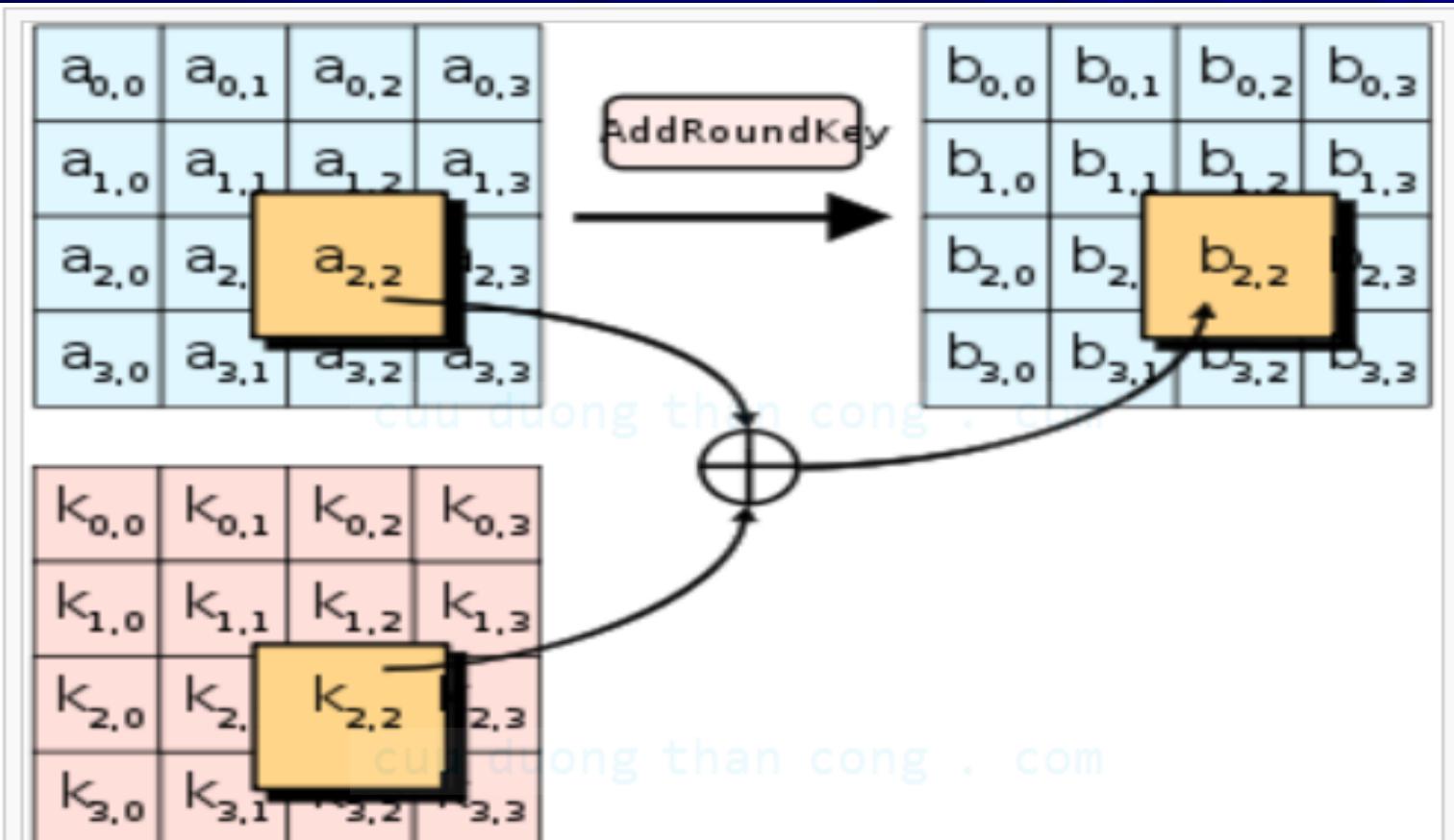
3. Tiêu chuẩn mã hoá tiên tiến AES



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



3. Tiêu chuẩn mã hoá tiên tiến 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. Hệ mã hoá khoá công khai RSA

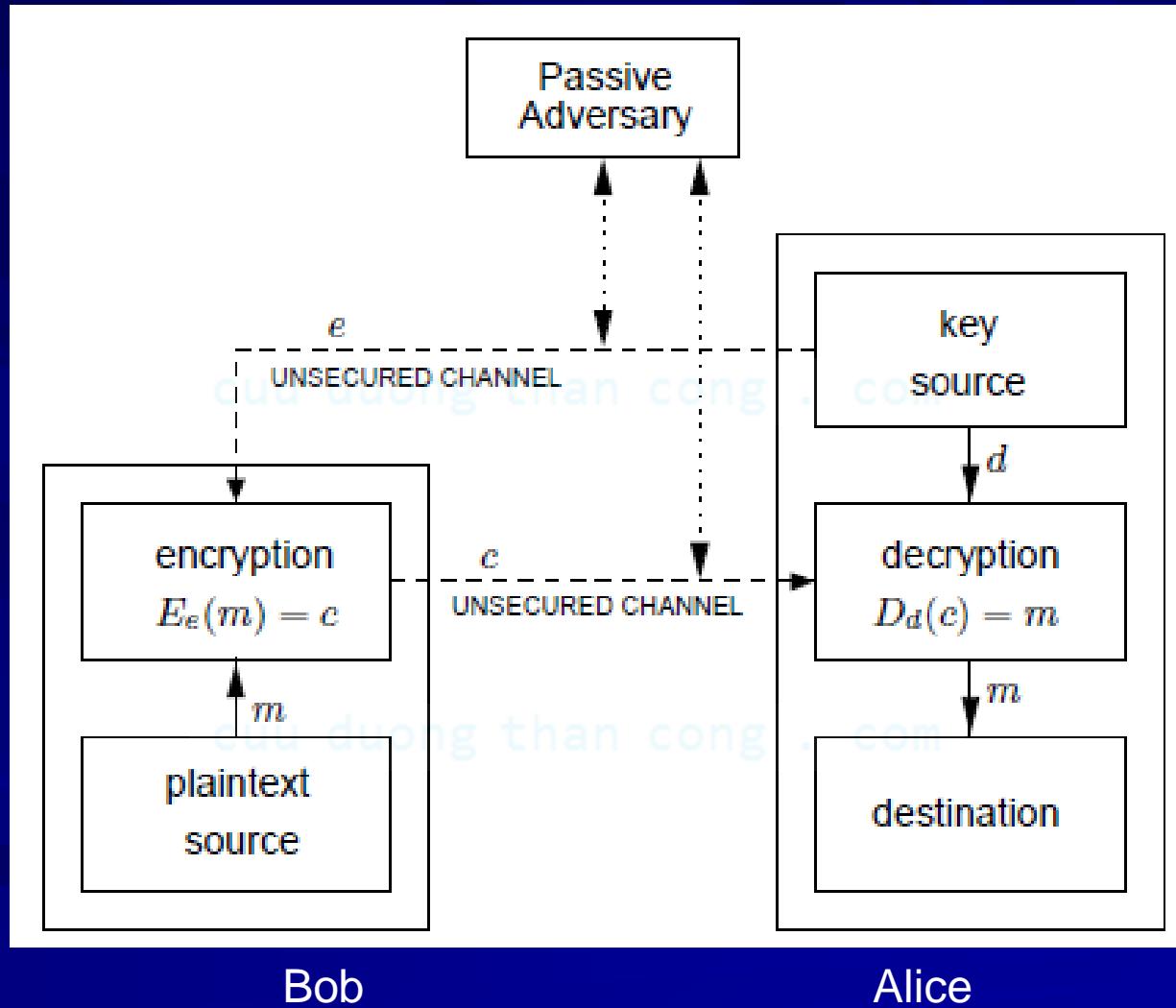
- Được sử dụng phổ biến trong thương mại điện tử
- Đảm bảo an toàn với điều kiện độ dài khóa đủ lớn.
- Thuật toán RSA có hai khóa:
 - khóa công khai (hay khóa công cộng)
 - khóa bí mật (hay khóa cá nhân).
- Mỗi khóa là những số cố định sử dụng trong quá trình mã hóa và giải mã.
- Khóa công khai được 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. Hệ mã hoá khoá 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.

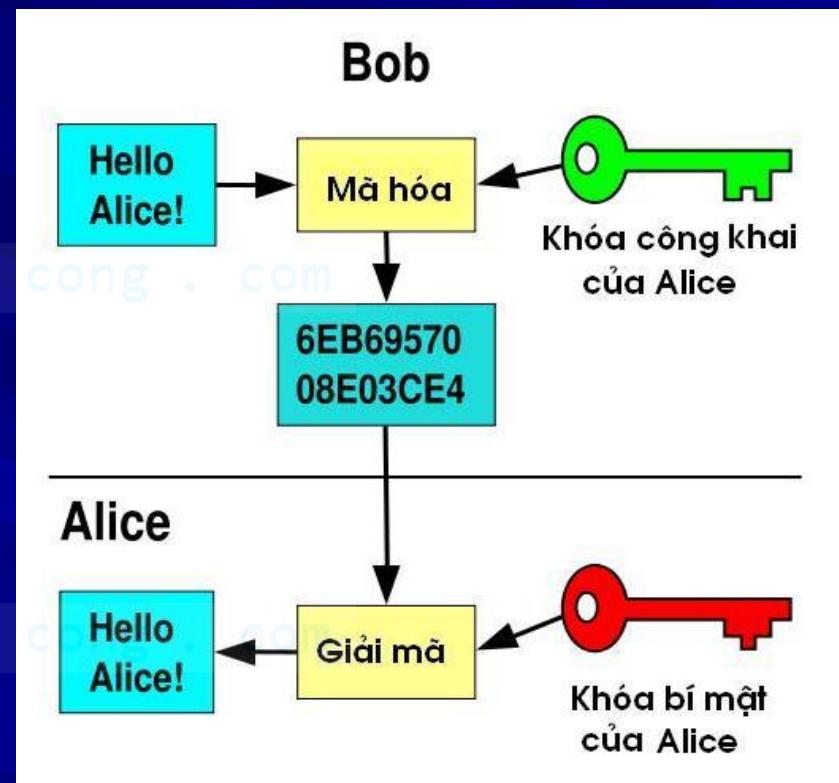
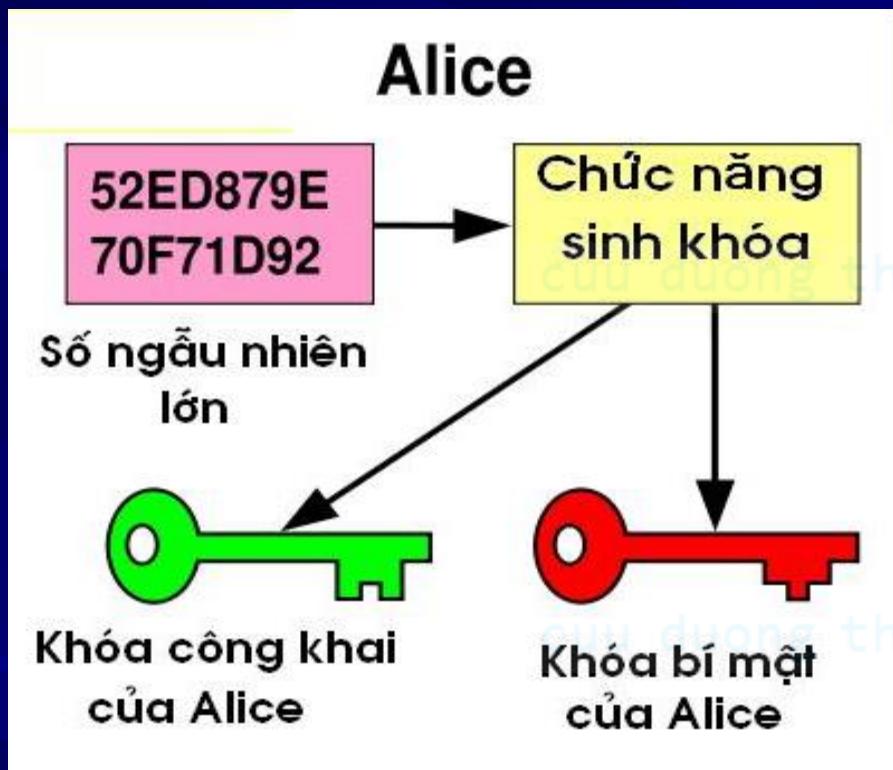
4. Hệ mã hoá khoá công khai RSA



Bob

Alice

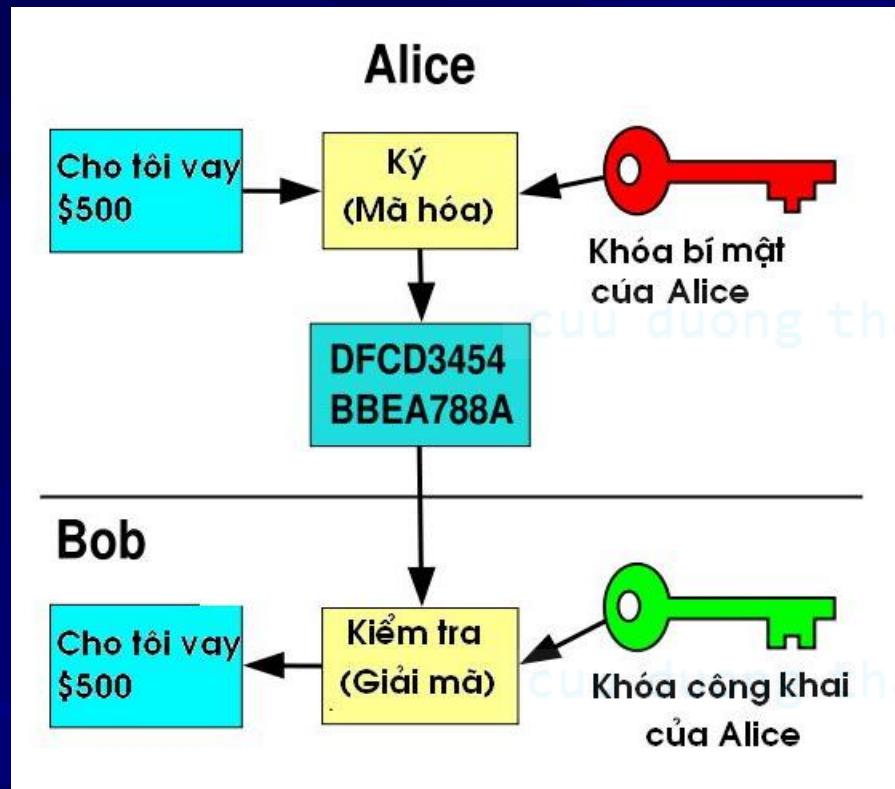
4. Hệ mã hoá khoá công khai RSA



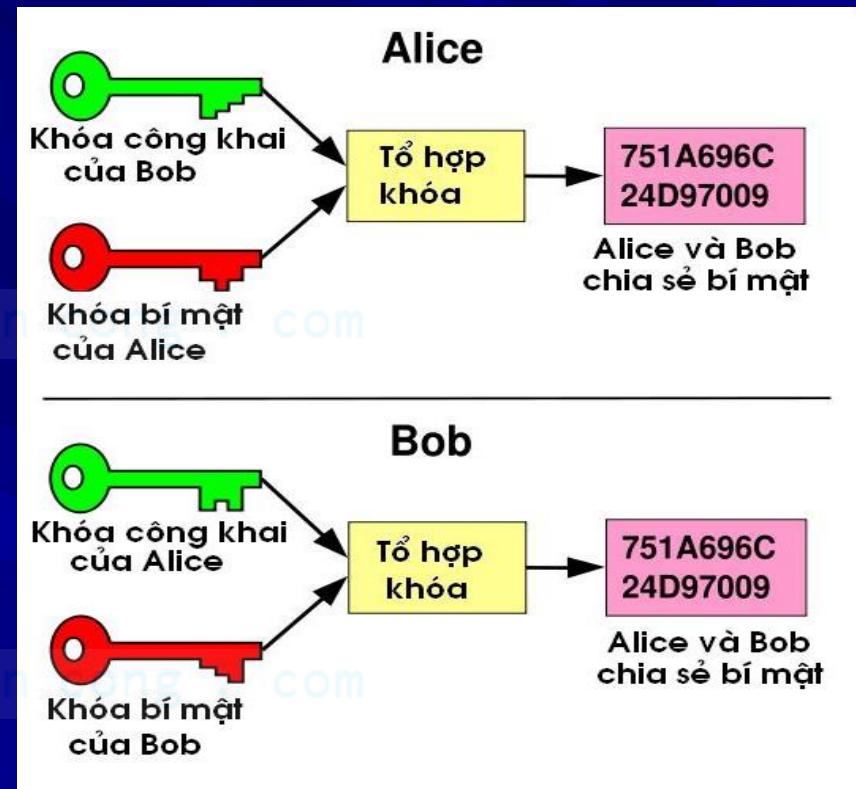
Chọn một số ngẫu nhiên lớn để sinh cặp khóa.

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

4. Hệ mã hoá khoá công khai RSA

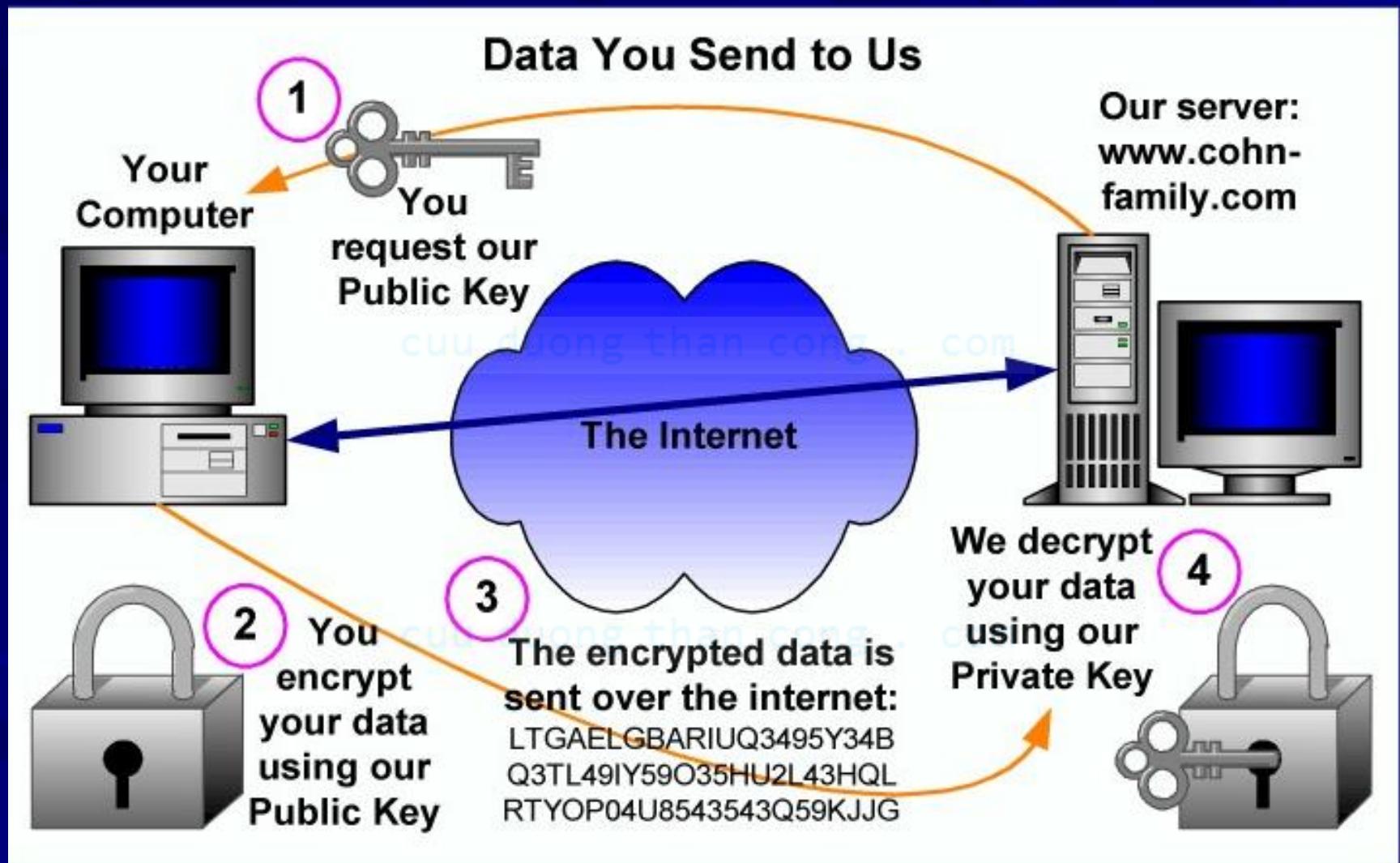


Dùng khoá bí mật để ký một thông báo; dùng khoá công khai để xác minh chữ ký.



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

4. Hệ mã hóa khoá công khai RSA



4. Hệ mã hóa khoá 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. Hệ mã hoá khoá 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. Bài tập

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

5. Bài tập

5. Viết ứng dụng mã hoá và giải mã cho một giải thuật mã hoá hiện đại sử dụng DES và AES.
6. Viết ứng dụng mô phỏng giải thuật mã hoá RSA.
7. Nêu cách sử dụng công cụ mã hoá TrueCrypt.
8. Thực hiện mã hoá và giải mã dữ liệu với công cụ EFS (Encrypt File System).