ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI

Lớp KHMT3-K3

DES

Thực hiện:

Nguyễn Đình Mạnh

Dương Văn Minh

Trần Anh Nam (Team Header)

Nguyễn Danh Nam

Trần Tuấn Nghĩa

Nguyễn Thị Nhài

Hoàng Ninh Nhật

Mô hình về DES
Hoán Vị Khởi Đầu
Mô Tả Thuật Toán
Hàm *f*
Khóa Chuyển Đổi
Giải Mã DES

DES

- Giới thiệu về DES
- Hoán Vị Khởi Đầu
- Mô Tả Thuật Toán
- Hàm ***f***
- Khóa Chuyển Đổi
- Giải Mã DES

Mô hình về DES
Hoán Vị Khởi Đầu
Mô Tả Thuật Toán
Hàm *f*
Khóa Chuyển Đổi
Giải Mã DES

Giới thiệu về DES

- Ngày 13/5/1973 ủy ban quốc gia về tiêu chuẩn của Mỹ công bố yêu cầu về hệ mật mã áp dụng cho toàn quốc.
- Des được công ty IBM công bố vào năm 1975.

Mô hình về DES

Hoán Vị Khởi Đầu

Mô Tả Thuật Toán

Hàm *f*

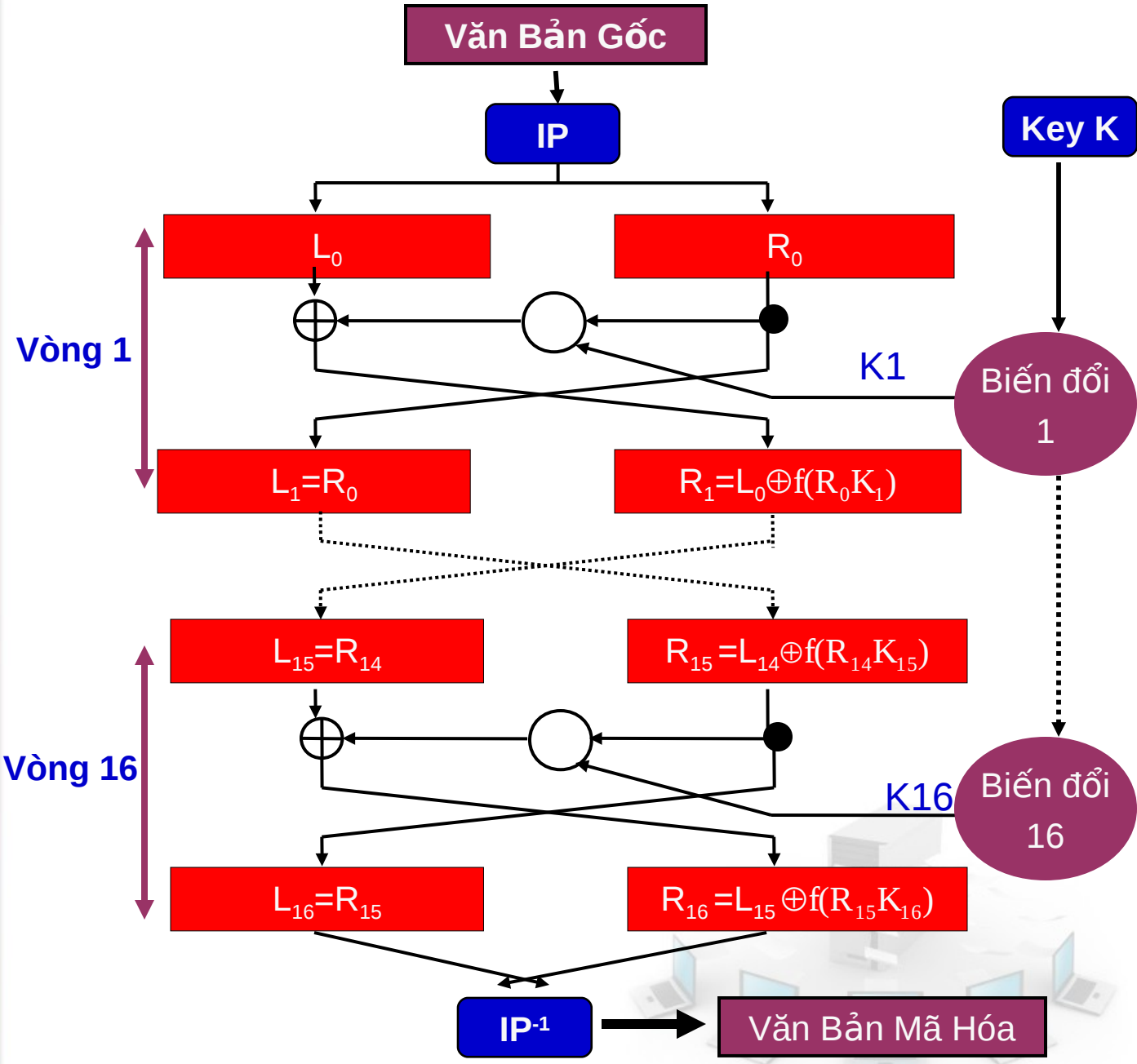
Khóa Chuyển Đổi

Giải Mã DES

Giới thiệu về DES

- DES là thuật toán mã hóa khối, độ dài mỗi khối là **64** bit .
- Khóa dùng trong DES có độ dài toàn bộ là **64** bit. Tuy nhiên chỉ có **56** bit thực sự được sử dụng; **8** bit còn lại chỉ dùng cho việc kiểm tra.
- Des xuất ra bãn mã **64** bit.

Mô hình về DES
Hoán Vị Khởi Đầu
Mô Tả Thuật Toán
Hàm *f*
Khóa Chuyển Đổi
Giải Mã DES



Mô hình về DES

Hoán Vị Khởi Đầu

Mô Tả Thuật Toán

Hàm *f*

Khóa Chuyển Đổi

Giải Mã DES

Hoán vị khởi đầu

Hoán vị khởi đầu (Kí hiệu là **IP**) đổi chỗ khối dữ liệu vào, thay đổi vị trí các bit trong khối dữ liệu vào. Tất cả các bảng hoán vị khởi đầu được đọc từ trái qua phải từ trên xuống dưới.

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

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

Mô hình về DES

Hoán Vị Khởi Đầu

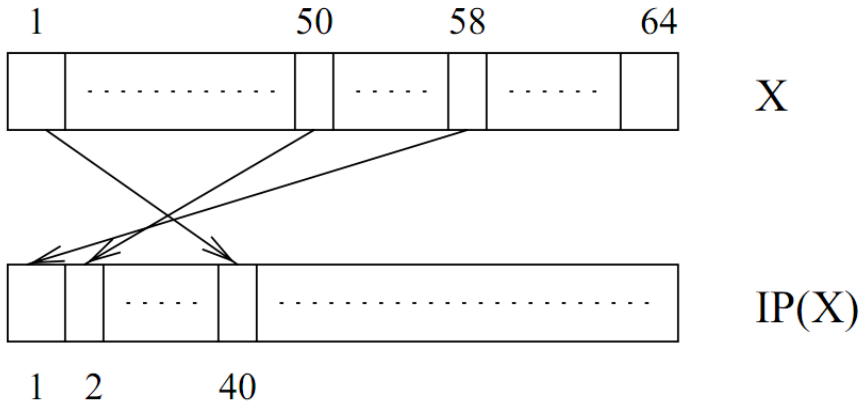
Mô Tả Thuật Toán

Hàm *f*

Khóa Chuyển Đổi

Giải Mã DES

Hoán vị khởi đầu



Mô hình về DES

Hoán Vị Khởi Đầu

Mô Tả Thuật Toán

Hàm *f*

Khóa Chuyển Đổi

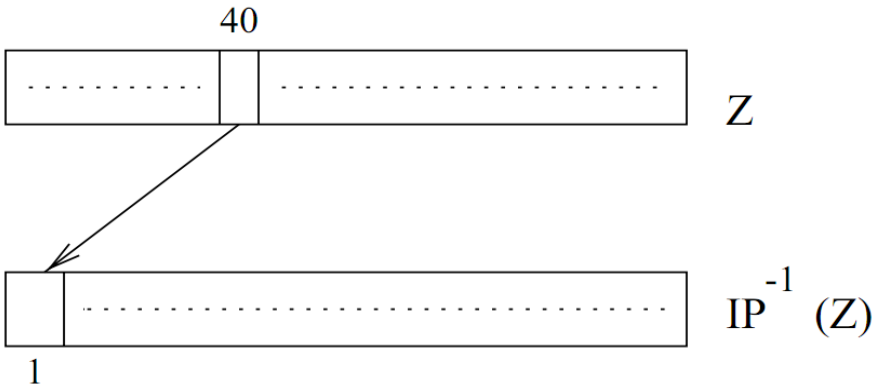
Giải Mã DES

Hoán Vị Cuối Cùng

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

Mô hình về DES
Hoán Vị Khởi Đầu
Mô Tả Thuật Toán
Hàm *f*
Khóa Chuyển Đổi
Giải Mã DES

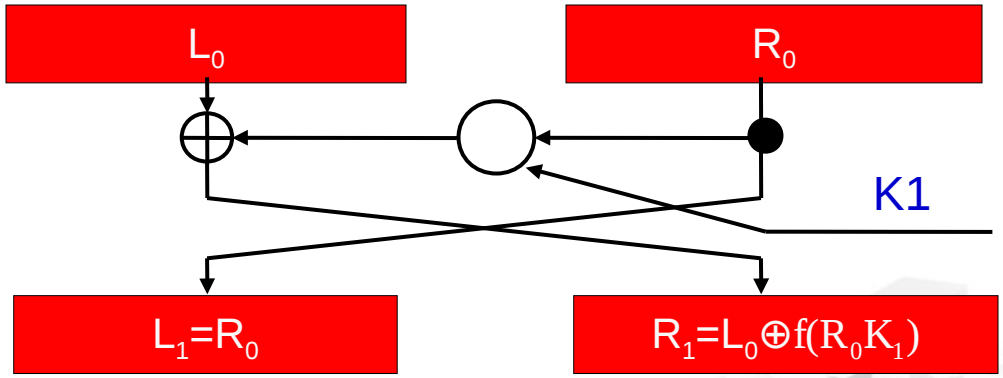
Hoán Vị Cuối Cùng



$IP^{-1}(IP(X))=X$

Mô hình về DES
Hoán Vị Khởi Đầu
Mô Tả Thuật Toán
Hàm *f*
Khóa Chuyển Đổi
Giải Mã DES

Hàm f



Mô hình về DES
Hoán Vị Khởi Đầu
Mô Tả Thuật Toán
Hàm *f*
Khóa Chuyển Đổi
Giải Mã DES

Mô Tả Thuật Toán

Với 1<=i<=16. Theo qui tắc:

for(i=1;i<=16,i++){

$L_i=R_{i-1}$

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

}

$\oplus$ là phép XOR của hai xâu bit:

$0 \oplus 0=0$, $1 \oplus 1=0$

$1 \oplus 0=1$, $0 \oplus 1=1$

f là hàm mà ta sẽ mô tả sau.

K_i là các xâu có độ dài 48 bit được tính như là các hàm của khóa K.

K_1 đến K_{16} lập nên một lịch khóa.

Mô hình về DES

Hoán Vị Khởi Đầu

Mô Tả Thuật Toán

Hàm *f*

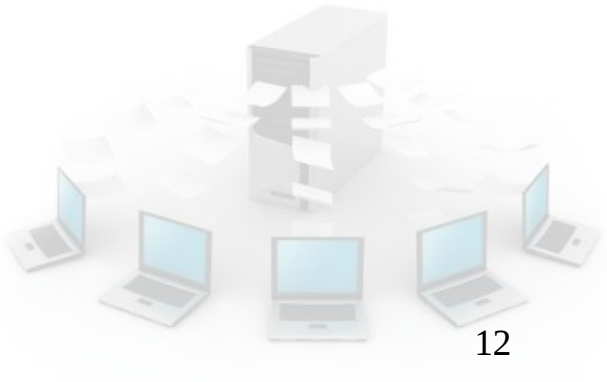
Khóa Chuyển Đổi

Giải Mã DES

Hàm **f**

mở

rộng



Mô hình về DES

Hoán Vị Khởi Đầu

Mô Tả Thuật Toán

Hàm *f*

Khóa Chuyển Đổi

Giải Mã DES

Hàm **f**

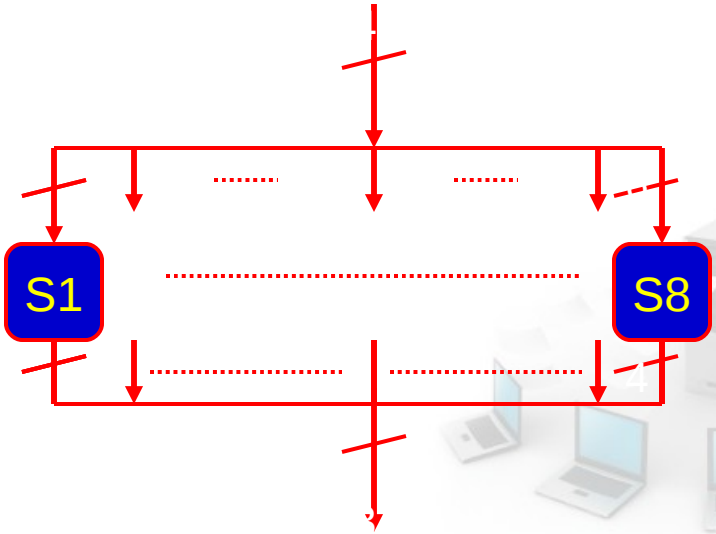
Dữ liệu vào			
1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16
17	18	19	20
21	22	23	24
25	26	27	28
29	30	31	32

E bit 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

Mô hình về DES
Hoán Vị Khởi Đầu
Mô Tả Thuật Toán
Hàm *f*
Khóa Chuyển Đổi
Giải Mã DES

Hộp Thay Thế - **S**

- Sau khi được nén khóa XOR với khối mở rộng , 48 bit kết quả được chuyển sang giai đoạn thay thế. Sự thay thế được thực hiện bởi 8 hộp thay thế. Khối 48 bit được chia thành 8 khối 6 bit. Mỗi khối được thực hiện trên 1 hộp S riêng biệt: khối 1 được thực hiện trên hộp S1, khối 2 được thực hiện trên hộp S2, ……, khối 8 được thực hiện trên hộp S8



Mô hình về DES

Hoán Vị Khởi Đầu

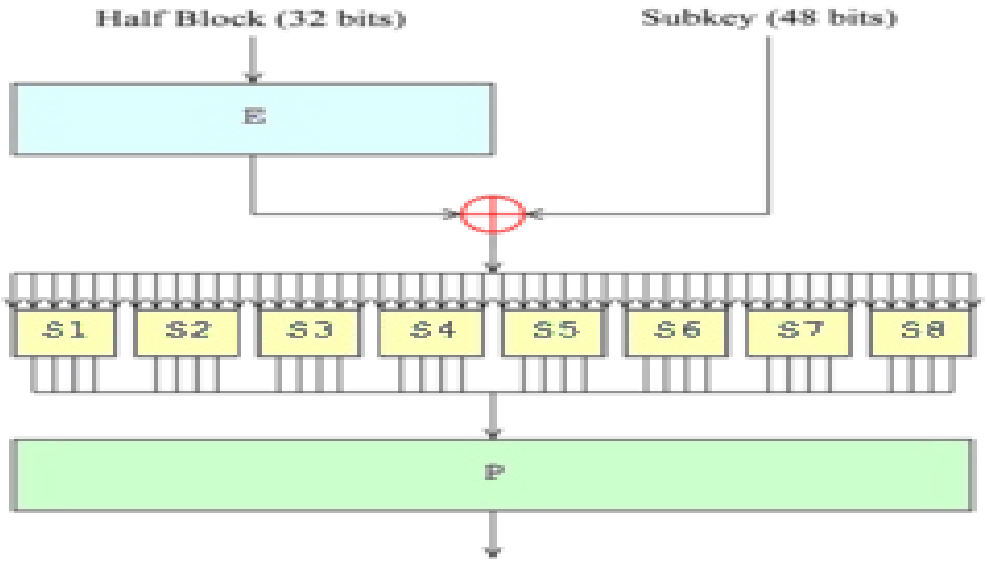
Mô Tả Thuật Toán

Hàm *f*

Khóa Chuyển Đổi

Giải Mã DES

Hộp Thay Thế - **S**



Mô hình về DES
Hoán Vị Khởi Đầu
Mô Tả Thuật Toán
Hàm *f*
Khóa Chuyển Đổi
Giải Mã DES

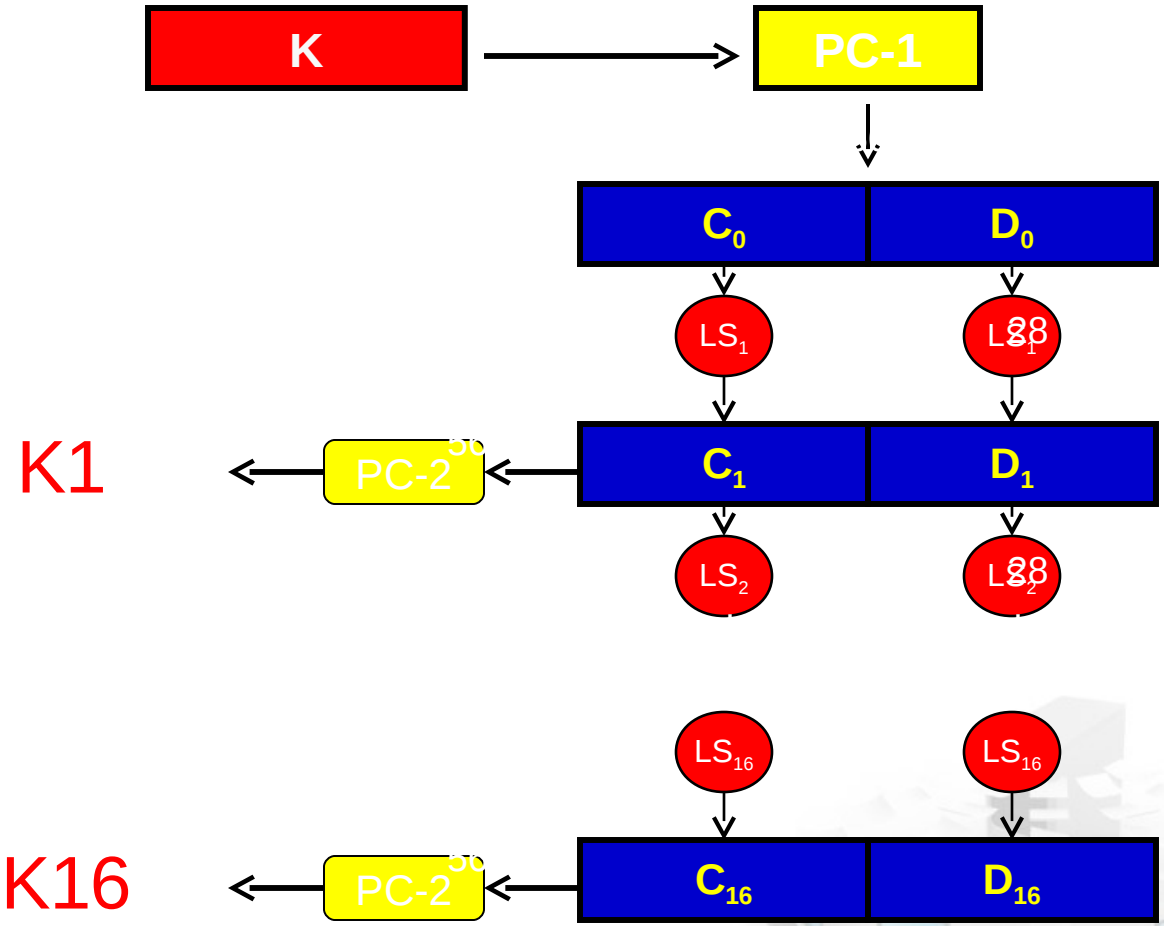
Khóa Chuyển Đổi

- K là một xâu có độ dài 64 bit trong đó 56 bit dùng làm khóa và 8 bit dùng để kiểm tra lỗi.

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

Mô hình về DES
Hoán Vị Khởi Đầu
Mô Tả Thuật Toán
Hàm *f*
Khóa Chuyển Đổi
Giải Mã DES

Khóa Chuyển Đổi

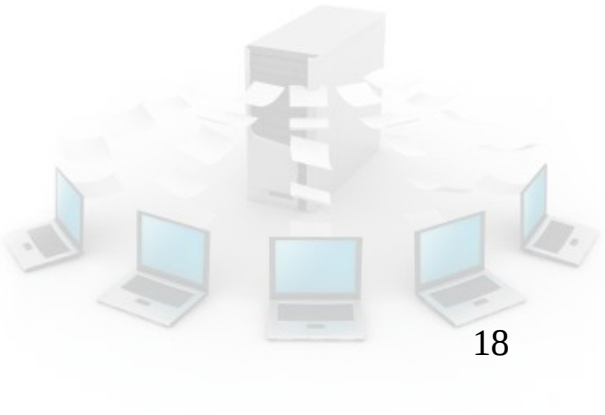


Mô hình về DES
Hoán Vị Khởi Đầu
Mô Tả Thuật Toán
Hàm *f*
Khóa Chuyển Đổi
Giải Mã DES

Khóa Chuyển Đổi

Quá trình tạo các khóa con (subkeys) từ khóa K

1.



Mô hình về DES
Hoán Vị Khởi Đầu
Mô Tả Thuật Toán
Hàm *f*
Khóa Chuyển Đổi
Giải Mã DES

Khóa Chuyển Đổi

- Hoán vị cố định PC1

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

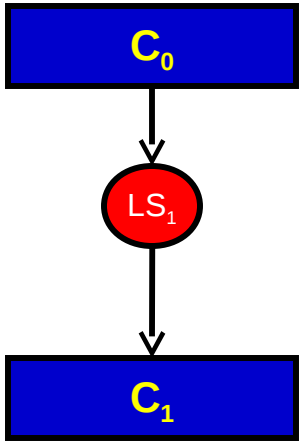
Mô hình về DES
Hoán Vị Khởi Đầu
Mô Tả Thuật Toán
Hàm *f*
Khóa Chuyển Đổi
Giải Mã DES

Khóa Chuyển Đổi

Thuật toán tính C_i, D_i như sau:

```
for(i=1;i<=16;i++){
        Ci = LSi(Ci-1)
        Di = LSi(Di-1)
}
```

$K_i = PC\text{-}2(C_iD_i)$.



Mô hình về DES
Hoán Vị Khởi Đầu
Mô Tả Thuật Toán
Hàm *f*
Khóa Chuyển Đổi
Giải Mã DES

Khóa Chuyển Đổi

Sang 1 vị trí	1	2	9	16		
Sang 2 vị trí	3	4	5	6	7	8
	10	11	12	13	14	15

Mô hình về DES
Hoán Vị Khởi Đầu
Mô Tả Thuật Toán
Hàm *f*
Khóa Chuyển Đổi
Giải Mã DES

Khóa Chuyển Đổi

Sau khi được dịch chuyển vị trí, 48 bít được lựa chọn ra từ 56 bít. Thực hiện này đổi chỗ thứ tự các bít như lựa chọn một tập con các bít, nó được gọi là hoán vị nén hoặc hoán vị lựa chọn (PC-2).

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

Mô hình về DES

Hoán Vị Khởi Đầu

Mô Tả Thuật Toán

Hàm *f*

Khóa Chuyển Đổi

Giải Mã DES

Giải Mã DES

Mô hình về DES

Hoán Vị Khởi Đầu

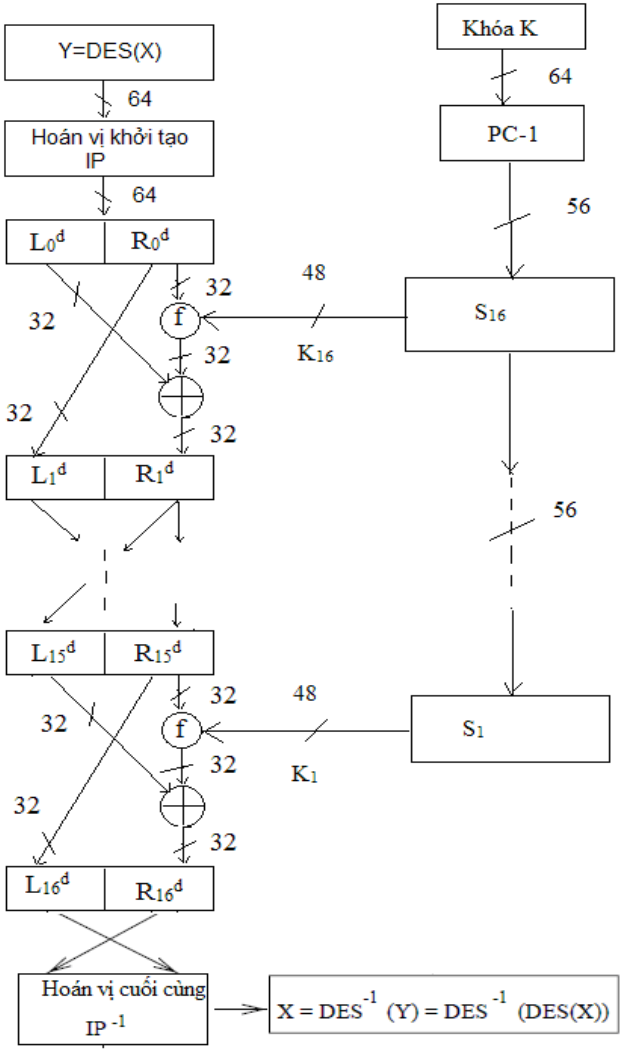
Mô Tả Thuật Toán

Hàm *f*

Khóa Chuyển Đổi

Giải Mã DES

Giải Mã DES



Mô hình về DES

Hoán Vị Khởi Đầu

Mô Tả Thuật Toán

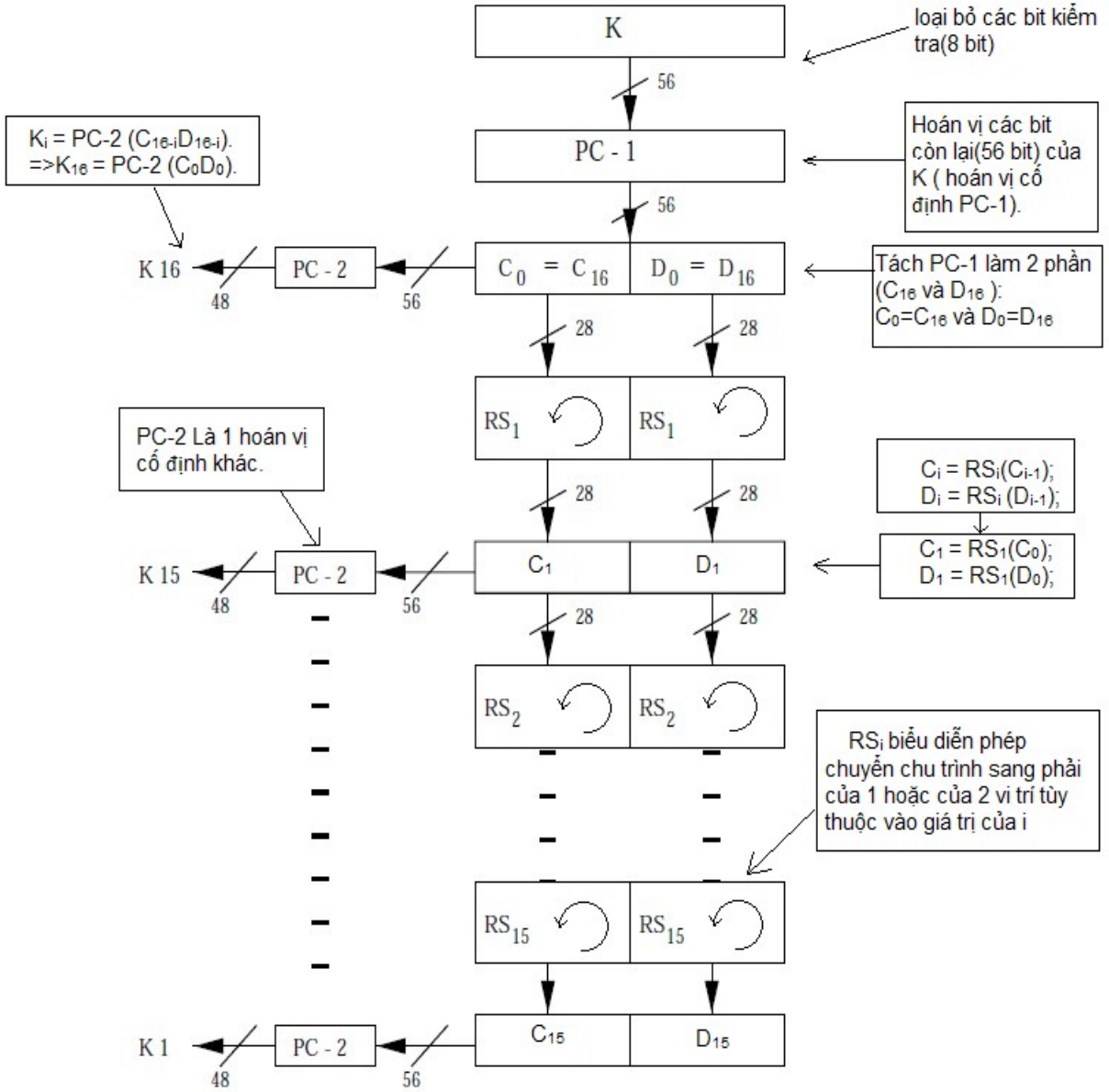
Hàm *f*

Khóa Chuyển Đổi

Giải Mã DES

Đặc Điểm Mã Des

- Mô hình về DES
- Hoán Vị Khởi Đầu
- Mô Tả Thuật Toán
- Hàm *f*
- Khóa Chuyển Đổi
- Giải Mã DES

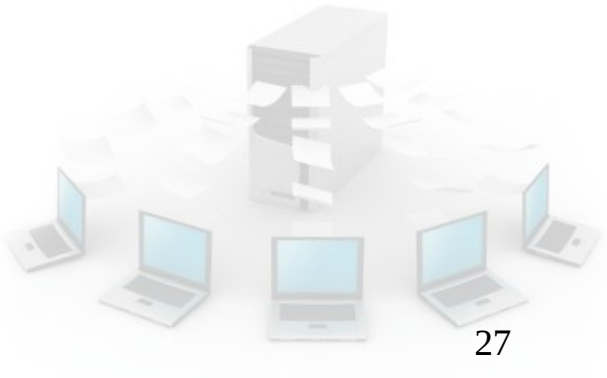


Mô hình về DES
Hoán Vị Khởi Đầu
Mô Tả Thuật Toán
Hàm *f*
Khóa Chuyển Đổi
Giải Mã DES

Tấn Công

Có hai điểm chỉ trích nghiêm trọng về DES từ phần đầu:

- Kích cỡ khóa quá nhỏ
- S-boxes chứa chuẩn thiết kế không công khai.



Mô hình về DES
Hoán Vị Khởi Đầu
Mô Tả Thuật Toán
Hàm *f*
Khóa Chuyển Đổi
Giải Mã DES

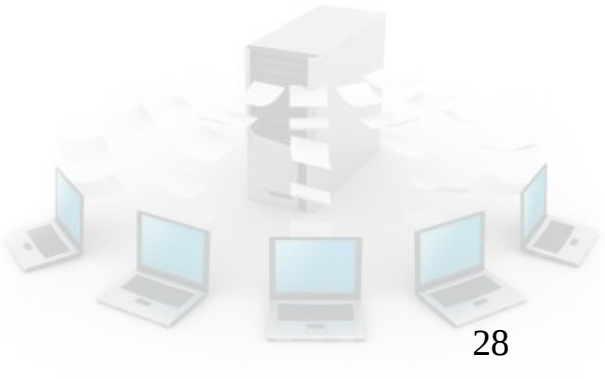
Tìm kiếm khóa đầy đủ

Tìm kiếm bản rõ :

Biết : X và Y .

Tìm K , sao cho $Y=DES_k(X)$.

Ý tưởng : kiểm tra tất cả 2^{56} trường hợp có thể là khóa



Tìm kiếm khóa đầy đủ

víi mét cÆp râ - m· cho tr-íc, h·y thö tÊt c¶ 2^{56} kho¸ cô thÓ. ®iÒu nµy kh«ng yªu cÇu bé nhí, nh-ng trung binh ph¶i thö 2^{55} kho¸ tr-íc khi tim ®-îc kho¸ ®óng.

MÆt kh¸c, víi mét b¶n râ x cho tr-íc, Oscar cã thÓ tÝnh tr-íc $y_K = e_K(x)$ ®èi víi toµn bé 2^{56} kho¸ K vµ x©y dùng mét b¶ng c¸c cÆp (y_K,K) ®-îc s¾p xÕp theo c¸c t¹o ®é ®Çu cña chóng. Sau ®ã khi Oscar thu ®-îc b¶n m· y (lµ kÕt qu¶ cña phÐp m· b¶n râ x), anh ta ph¶i nh×n vµo gi¸ trÞ y trong b¶ng vµ lËp tøc t×m ®-îc kho¸ K.

Mô hình về DES

Hoán Vị Khởi Đầu

Mô Tả Thuật Toán

Hàm *f*

Khóa Chuyển Đổi

Giải Mã DES

Thám mã vi sai

- Được đề xuất bởi Biham và Shamir năm 1990.
- Nguyên tắc : Đây là một kỹ thuật sử dụng những phỏng đoán khác nhau trong bản rõ để đưa ra những thông tin trong bản mã
- Phá mã vi sai là thuật toán xem xét những cặp mã hoá khác nhau, đây là những cặp mã hoá mà bản rõ của chúng là khác biệt. Người ta sẽ phân tích tiến trình biến đổi của những cặp mã này thông qua các vòng của DES khi chúng được mã hoá với cùng một khoá K. Sau đó sẽ chọn hai bản rõ khác nhau một cách ngẫu nhiên hợp lý nhất. Sử dụng sự khác nhau của kết quả mã hoá và gán cho những khoá khác nhau một cách phù hợp nhất. Khi phân tích nhiều hơn những cặp bản mã, chúng ta sẽ tìm ra một khoá được xem là đúng nhất

Mô hình về DES
Hoán Vị Khởi Đầu
Mô Tả Thuật Toán
Hàm *f*
Khóa Chuyển Đổi
Giải Mã DES

Thám mã vi sai

- Để phá mã DES với đầy đủ 16 chu trình :
  Phá mã vi sai cần đến 2^{47} cặp bản rõ (X,Y).
- Để hiểu được một văn bản đã được mã hóa cần 2^{55} cặp bản rõ (X,Y).
- Phải cần đến 2^{37} phép tính số học
- Mỗi cặp (X,Y) có độ dài là 128bit , cần lưu trữ lớn thì việc tấn công này là không thực tế