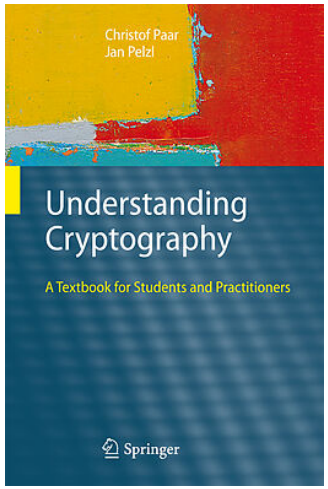
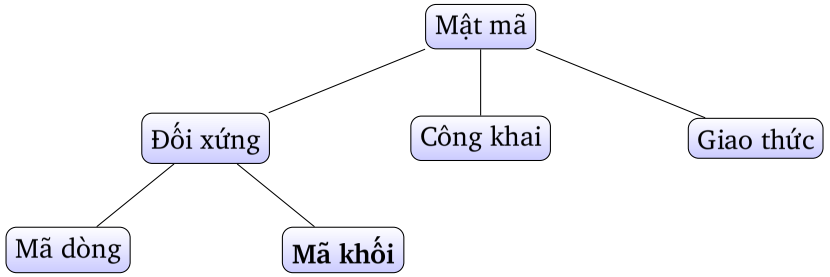
Tài liệu

https://www.crypto-textbook.com



Mật mã

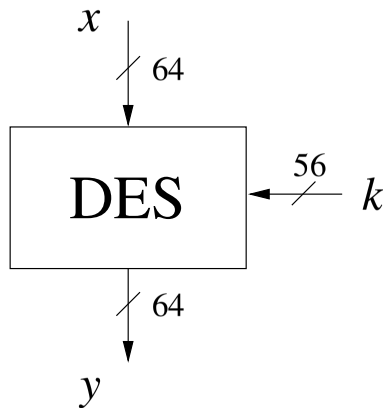


ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

Nhập môn An toàn Thông tin

Data Encryption Standard (DES) và một số biến thể

Nội dung



- Hiện nay, DES không còn an toàn do kích thước khoá ngắn.
- Nhưng 3DES thì rất an toàn.

Lịch sử

- Đề xuất bởi IBM năm 1974 dựa trên hệ Lucifer.

  Lucifer là họ hệ mật phát triển bởi Horst Feistel cuối những năm 1960. Lucifer có kích thước khối 64 bit và khoá 128 bit.

- National Security Agency (NSA) đã sửa đổi và đặt tên là DES.
- Sửa đổi này cho phép chống lại kiểu thám mã vi phân. Kiểu tấn công này chưa được biết đến trước năm 1990.
- Tuy nhiên, NSA lại sửa đổi kích thước khoá từ 128 bit xuống còn 56 bit!

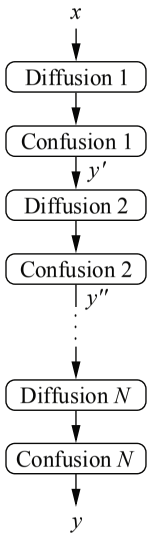
  $\Rightarrow$ Có thể tấn công vét cạn.
- Nhiều người giả thuyết rằng NSA có thể tìm kiếm khoá trong không gian 2^{56}.
- Năm 1977, công bố chuẩn mã hoá dữ liệu DES.

Nguyên lý xây dựng mã khối

theo Claude Shannon

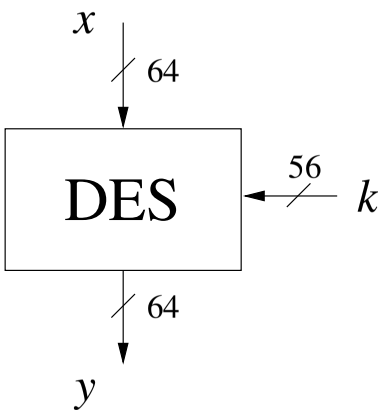
- Làm hỗn loạn (Confusion) là phép toán mã hoá nhằm che giấu liên hệ giữa khoá và bản mã.
- Khuếch tán (Diffusion) là phép toán mã hoá làm cho việc sửa một bit ở bản rõ sẽ ảnh hưởng rộng đến nhiều bit của bản mã. Mục tiêu là giấu tính chất thống kê của bản rõ.

Nguyên lý xây dựng mã khối



Kết hợp Confusion và Diffusion để xây dựng hệ mã khối mạnh.

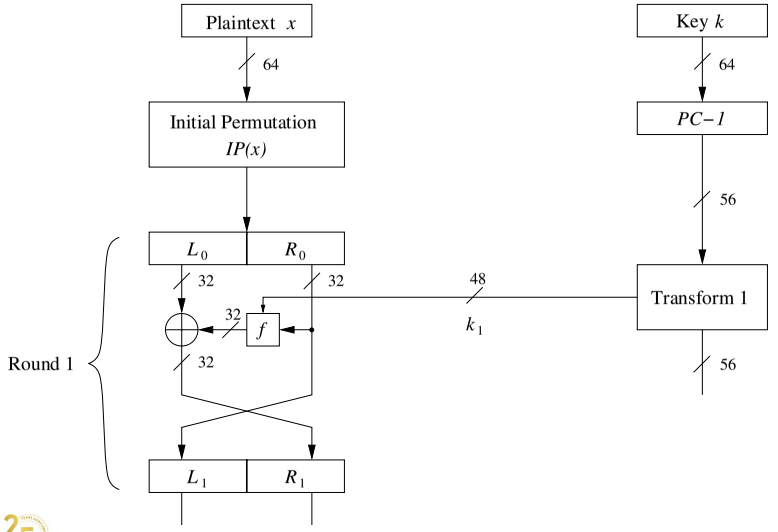
DES

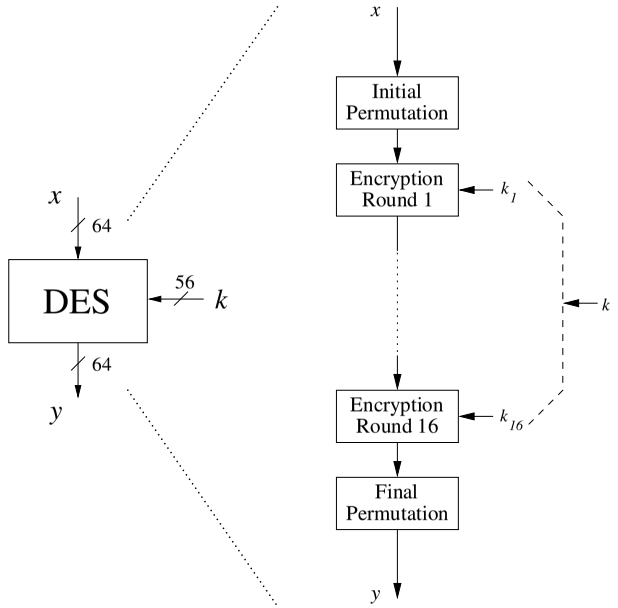


- Khoá 56 bit
- Khối 64 bit.

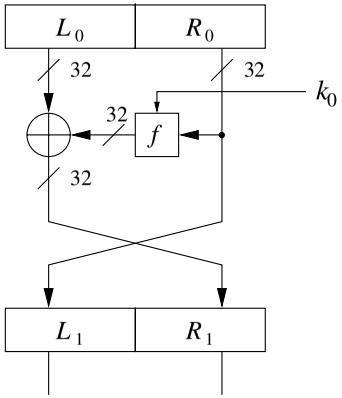
Nội dung

Mạng Feistel: Vòng 1





Cấu trúc mạng Feistel

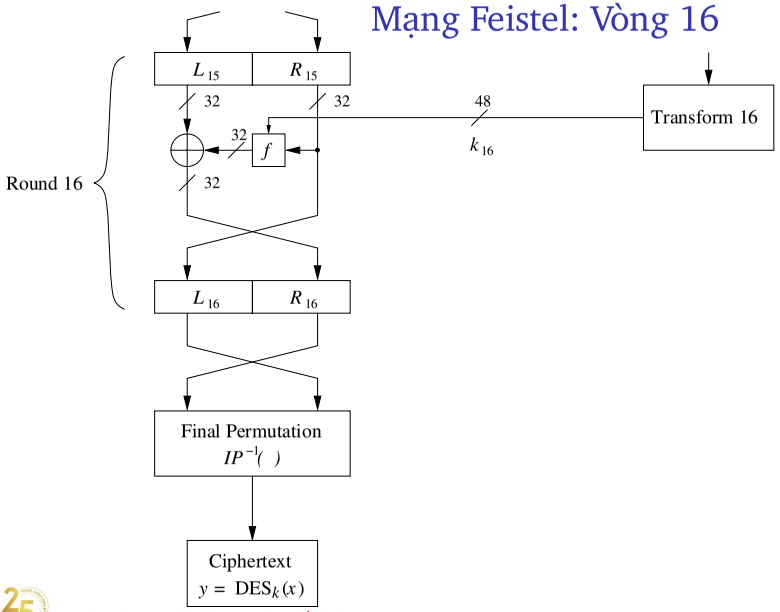


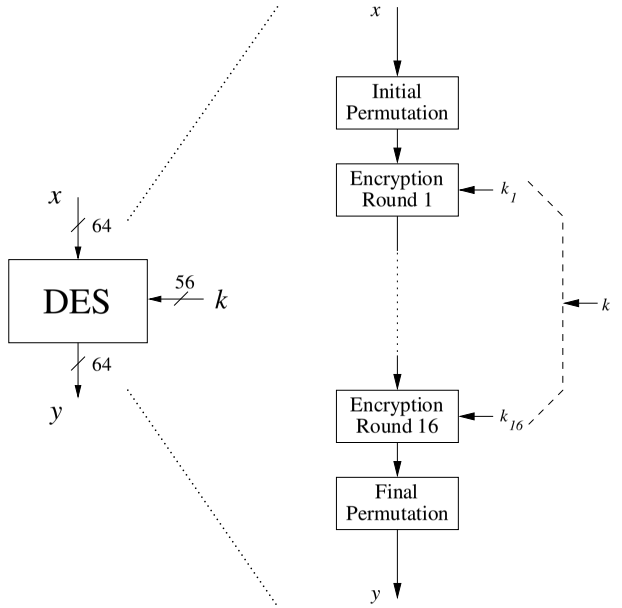
- Công thức tổng quát:

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

- Làm thế nào để tính ngược lại L_{i-1} và R_{i-1}?

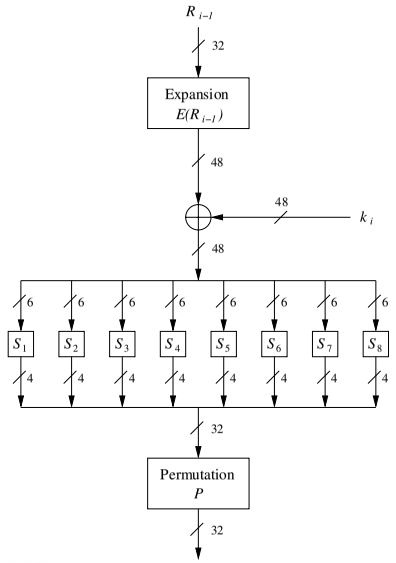
Mạng Feistel: Vòng 16





Nội dung

Hàm f



- Mở rộng đầu vào $E(R_{i+1})$
- XOR với khoá vòng i
- Bảng thay thế S-box
- Hoán vị P

Hoán vị ban đầu IP và kết thúc IP^{-1}

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

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

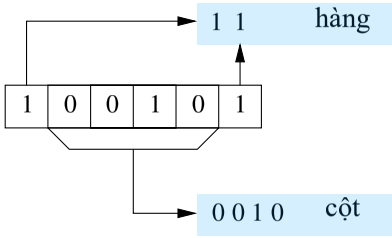
S-Box

- S-box là hàm $\{0,1\}^6 \to \{0,1\}^4$; 6 bit input và 4 bit output.
- Gồm 8 S-box được thiết kế phi tuyến

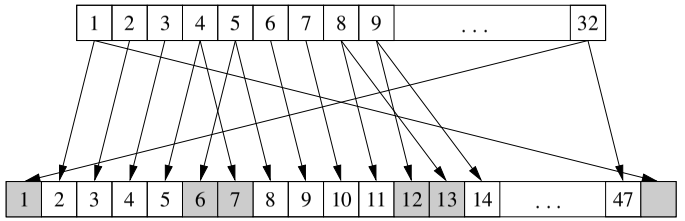
$$S(a) \oplus S(b) \neq S(a \oplus b)$$

để chống lại thám mã vi phân.

- Bảng S-box được giải mã theo cách đặc biệt:



Hàm mở rộng đầu vào E



E

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

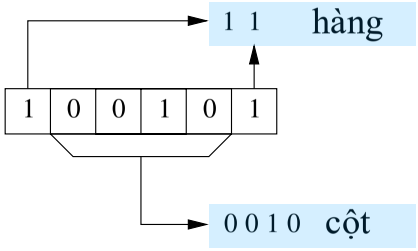
Hoán vị P

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

Hình: Hoán vị P là phép khuếch tán, gây ảnh hưởng đến nhiều S box khác trong vòng tiếp theo.

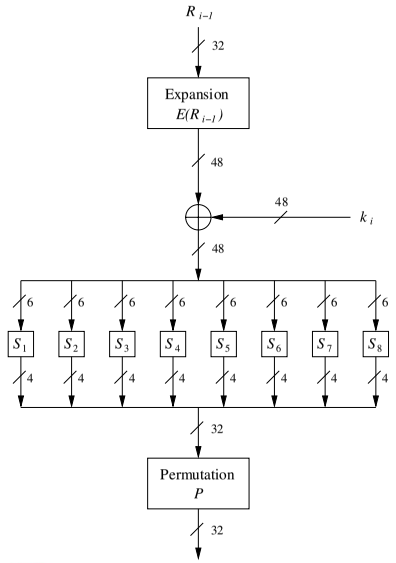
Nội dung

S-box



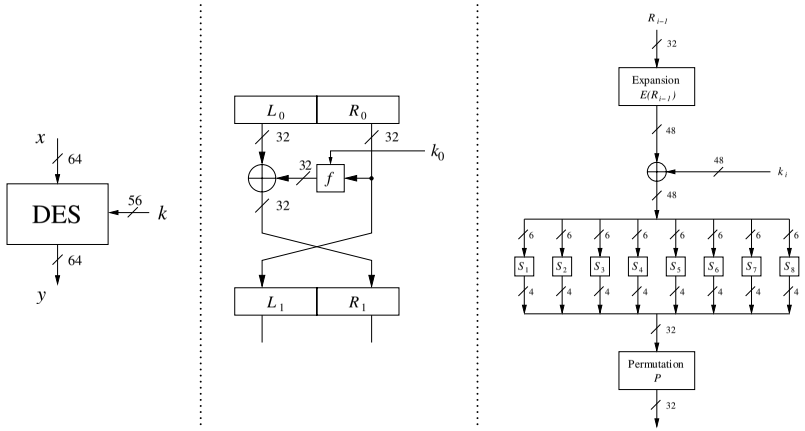
S_1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	01	10	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

Hàm f



- Mở rộng đầu vào $E(R_{i+1})$
- XOR với khoá vòng i
- Bảng thay thế S-box
- Hoán vị P

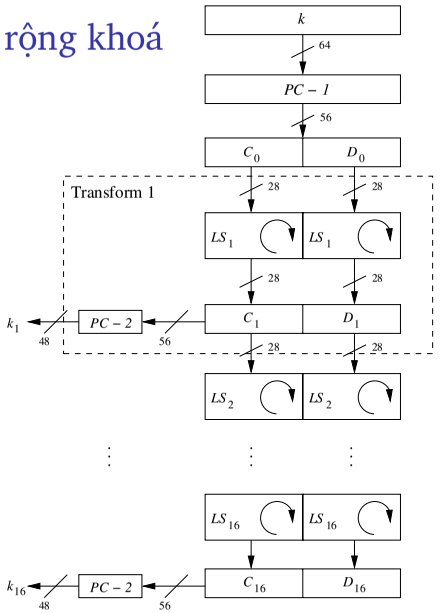
Nhắc lại: Thành phần của DES



Mở rộng khoá

- Câu hỏi: Làm thế nào để tính 16 khoá con $k_1, \ldots, k_{16}$?
- Mở rộng khoá chỉ gồm các phép toán đơn giản (hoán vị và xoay vòng trái) trên bit.

Mở rộng khoá



PC-1: Permuted Choice 1

- Loại bỏ các bit $8, 16, 24, \ldots, 64$ của khoá k kích thước 64 bit.
- Khoá thực sự của DES chỉ là $(64 - 8) = 56$ bit.

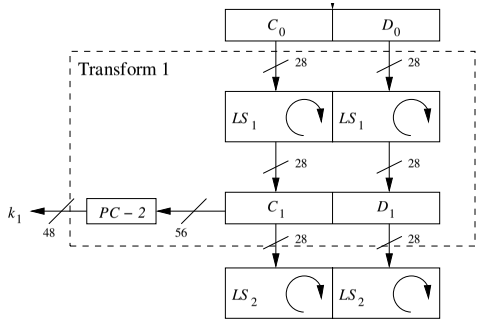
$PC-1$							
57	49	41	33	25	17	9	1
58	50	42	34	26	18	10	2
59	51	43	35	27	19	11	3
60	52	44	36	63	55	47	39
31	23	15	7	62	54	46	38
30	22	14	6	61	53	45	37
29	21	13	5	28	20	12	4

PC-2: Permuted Choice 2

- Loại bỏ 8 bit của $\boxed{C_i}\boxed{D_i}$;
- Số bit của khoá con k_i là $56-8=48$ bit

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

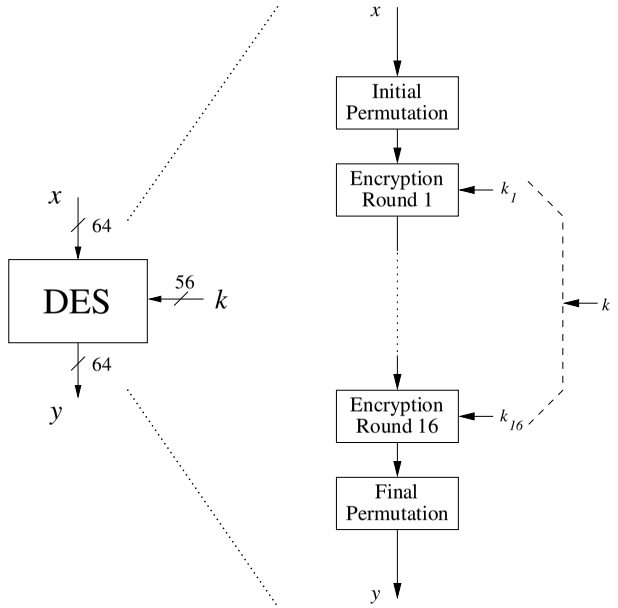
LS_i: Left shift (left rotate)



$$LS_i = \begin{cases} \text{Xoay vòng trái 1 vị trí} & \text{nếu } i = 1, 2, 9, 16 \\ \text{Xoay vòng trái 2 vị trí} & \text{trong trường hợp khác.} \end{cases}$$

Chú ý: Tổng số bit được xoay vòng $4 \times 1 + 12 \times 2 = 28$, do đó

$$C_{16} = C_0;\ D_{16} = D_0.$$



Nội dung

Nội dung

Bổ đề

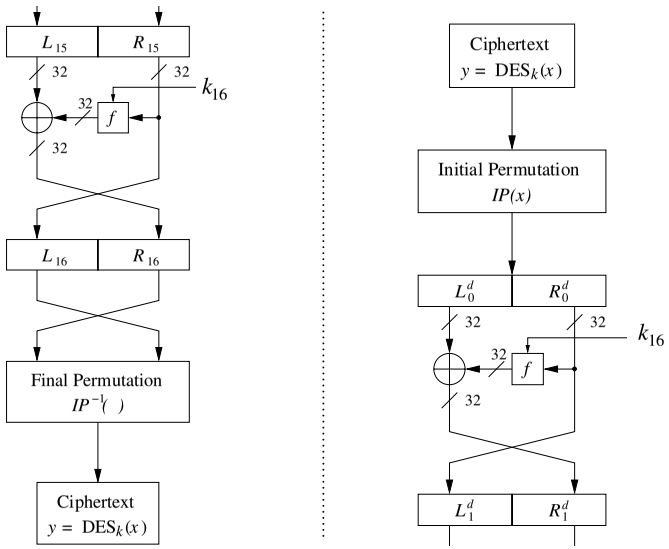
Giả sử DES là một hệ mã lý tưởng (2^{56} hàm khả nghịch ngẫu nhiên $\pi_i : \{0,1\}^{64} \to \{0,1\}^{64}$)

Vậy thì với mỗi cặp x, y có nhiều nhất một khóa k thỏa mãn

$$y = DES(k, x)$$

với xác suất $\geq 1 - 1/256 \approx 99.5\%$.

Giải mã mỗi vòng



Tấn công vét cạn để tìm khóa của mã khối

Bài toán

- Cho một số cặp input/output

$$(x_i, y_i = \mathrm{Enc}(k, x_i))$$

với $i = 1, 2, 3$.

- Hãy tìm khóa k.

Thử thách DES

Cho các cặp bản rõ và bản mã

```
msg = "The unknown messages is : XXXX ... "
CT  =      y1       y2       y3         y4
```

Hãy tìm khóa $k \in \{0,1\}^{56}$ thỏa mãn $DES(k, x_i) = y_i$ với $i = 1, 2, 3$.

- 1997: DESCHALL project với internet search – 96 ngày
- 1998: EFF dùng máy DeepCrack – 3 ngày (250K $)
- 1999: Kết hợp cả DeepCrack và internet search – 22 giờ
- 2006: COPACOBANA (120 FPGA) – 7 ngày (10K $).

Không nên dùng mã khối 56 bit khóa !!
128-bit khóa $\Rightarrow 2^{72}$ ngày.

Tìm kiếm vét cạn để tìm khóa cho mã khối

- Với hai cặp DES:

$$(x_1, y_1 = DES(k, x_1)) \text{ và } (x_2, y_2 = DES(k, x_2))$$

  xác suất để có k có duy nhất là $\approx 1 - 1/2^{71}$.
- Với AES-128: cho hai cặp input/output, xác suất có k duy nhất $\approx 1 - 1/2^{128}$
- Vậy hai cặp input/output là đủ thông tin để tìm kiếm vét cạn cho khóa.