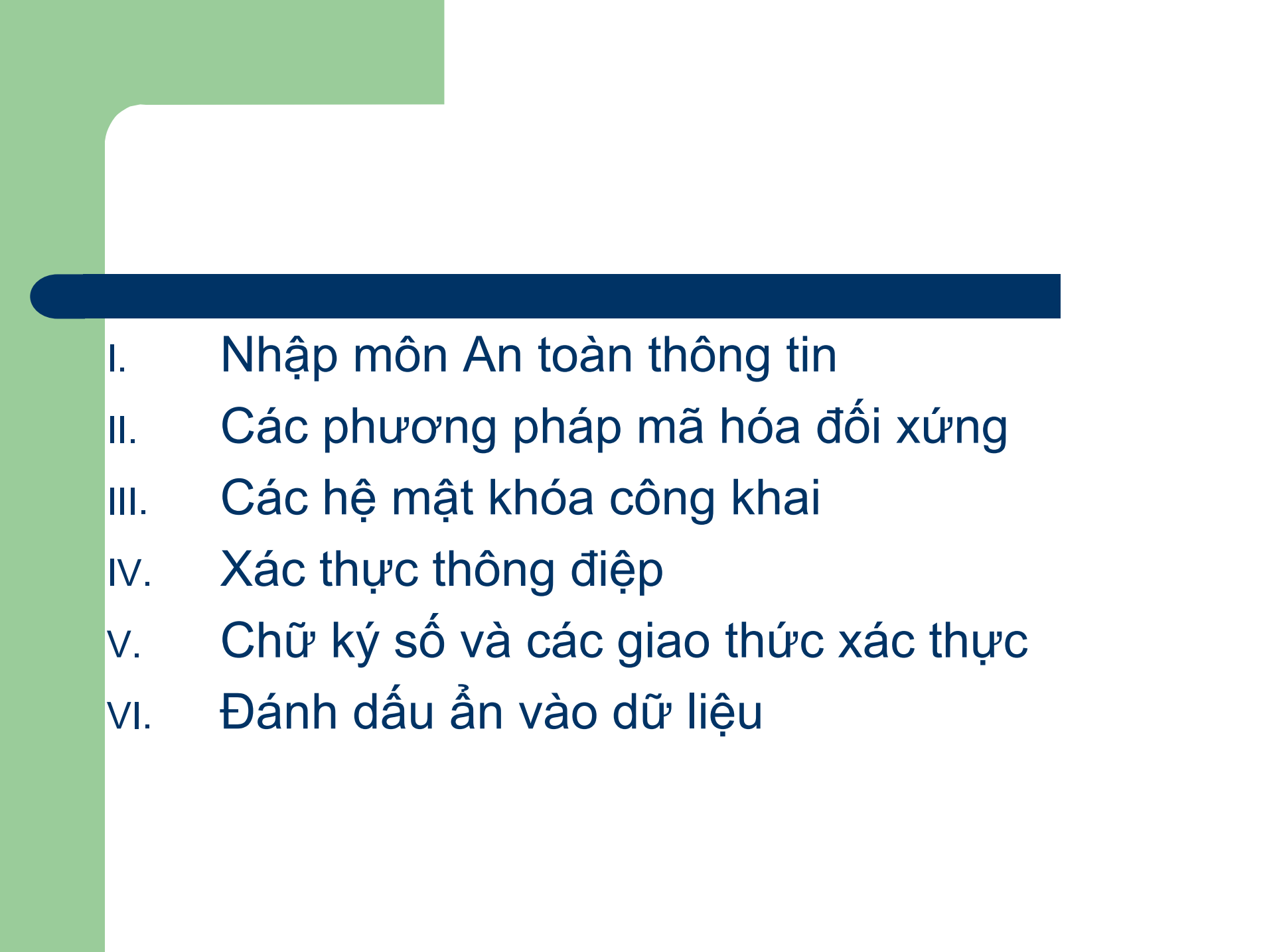


An toàn và An ninh thông tin

Nguyễn Linh Giang
Bộ môn Truyền thông
và Mạng máy tính



- 
- I. Nhập môn An toàn thông tin
 - II. Các phương pháp mã hóa đối xứng
 - III. Các hệ mật khóa công khai
 - IV. Xác thực thông điệp
 - V. Chữ ký số và các giao thức xác thực
 - VI. Đánh dấu ẩn vào dữ liệu

Chương II.

Các phương pháp mã hóa đối xứng

1. Sơ đồ chung của phương pháp mã hóa đối xứng
2. Một số phương pháp mã hóa đối xứng kinh điển
3. **Phương pháp DES**
4. Quản trị và phân phối khóa

Phương pháp mật mã DES

- Văn bản gốc X , văn bản mã mật Y là các chuỗi nhị phân độ dài 64 bit.
- Khóa K có độ dài 56 bit.
- Từng khối 64 bit được mã hóa độc lập sử dụng chung một khóa.

Phương pháp mật mã DES

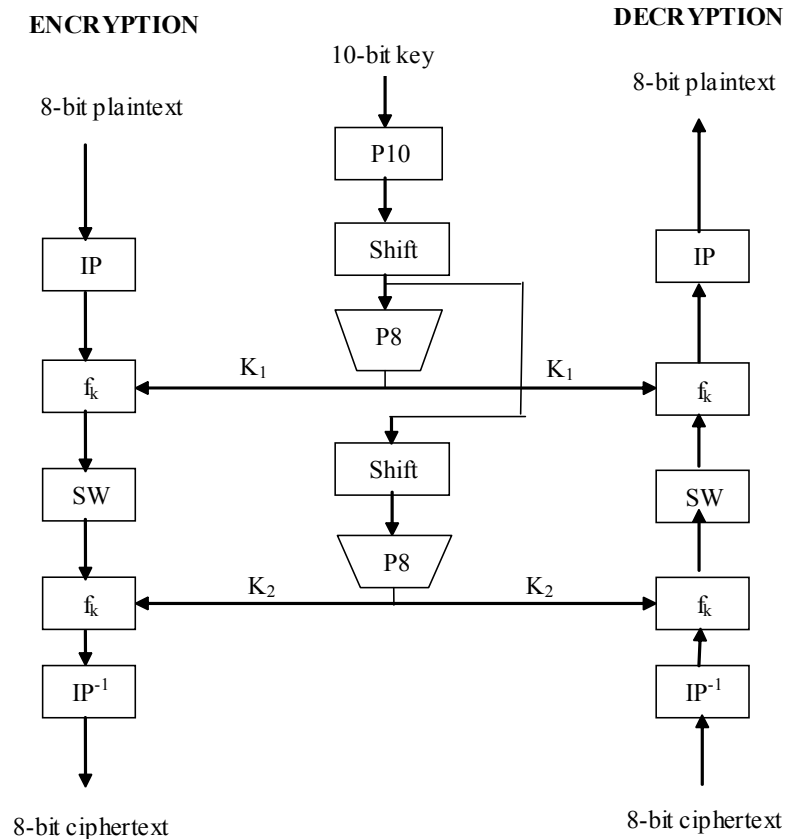
- Phương pháp S-DES(DES giản lược)
- Phương pháp mật mã DES

S- DES

(Simplified data encryption standard)

- Cấu trúc của DES là rất phức tạp
 - S-DES - phiên bản đơn giản của DES;
 - Cho phép:
 - Mã hoá và giải mã bằng tay;
 - Hiểu biết sâu về hoạt động chi tiết của giải thuật DES.
- S-DES đơn giản hơn nhiều so với DES
 - Các tham số của S-DES nhỏ hơn trong DES;
 - Do giáo sư Edward Schaefer thuộc trường đại học Santa Clara phát triển

Giải thuật S-DES(Simplified DES):



Hình 1:Sơ đồ mã hoá và giải mã S-DES

Giải thuật S-DES

- Giải thuật mã hoá S-DES sử dụng phương pháp mã hoá theo khối
- Đầu vào:
 - 8-bit block của bản rõ
 - 10-bit khoá
- Đầu ra:
 - 8-bit của bản mã

Giải thuật S-DES

- Giải thuật mã hoá bao gồm 4 hàm:
 - Hàm IP(Initial Permutation)
 - Hàm f_k
 - Hàm SW (Switch)
 - Hàm IP^{-1}
- Giải thuật mã hoá có thể biểu diễn như một hàm sau đây:
$$\text{ciphertext} = IP^{-1}(f(SW(f(IP(\text{plaintext}))))))$$
- Tương tự giải thuật giải mã có thể biểu diễn như hàm sau:
$$\text{plaintext} = IP(f(SW(f(IP^{-1}(\text{ciphertext}))))))$$

© 2015 Pearson Education, Inc. or its affiliate(s). All rights reserved.



Hình2: Sơ đồ tạo khóa của thuật toán S-DES

Các hàm sinh khoá:

- P10: Đây là hàm hoán vị tuần theo luật như trong bảng

P10									
3	5	2	7	4	10	1	9	8	6

- LS-1: Là hàm dịch vòng 1 bit
- LS-2: Là hàm dịch vòng 2 bit
- P8: Là hàm hoán vị tuần theo luật như trong bảng

P8							
6	3	7	4	8	5	10	9

Mã hoá S-DES:

Hàm IP và hàm IP^{-1} :

+ Hàm IP tuân theo luật sau:

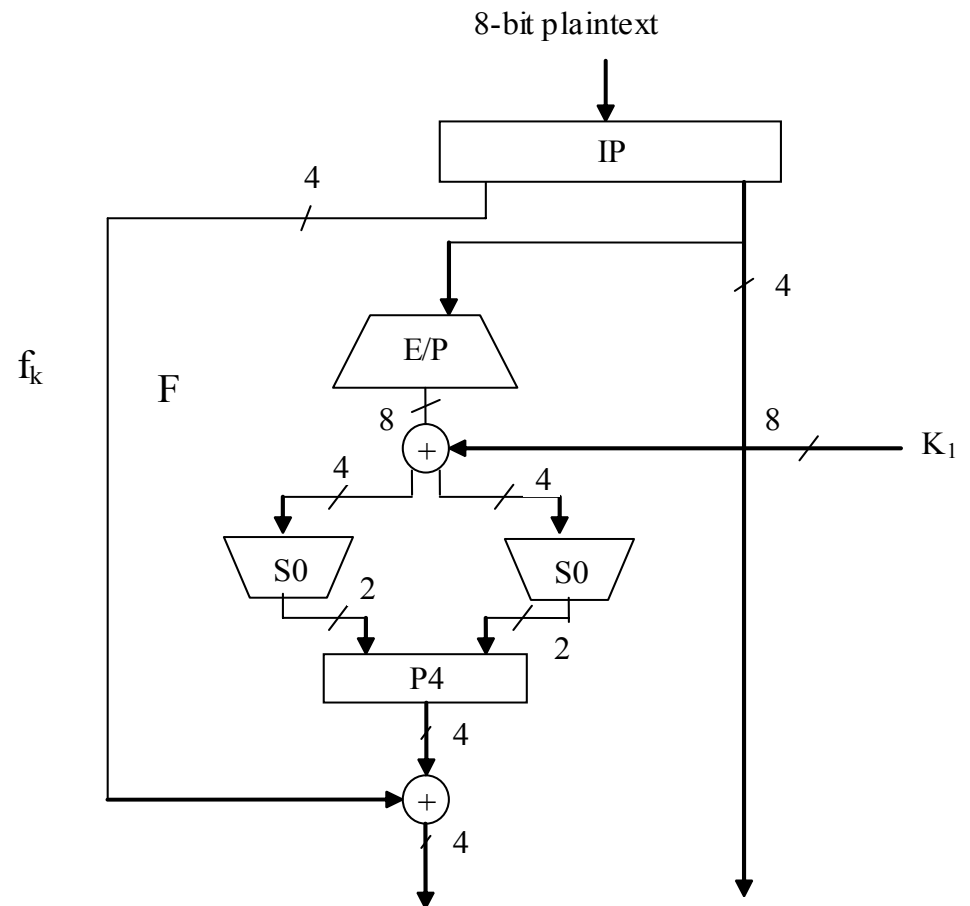
IP							
2	6	3	1	4	8	5	7

+ Hàm IP^{-1} tuân theo luật sau:

IP^{-1}							
4	1	3	5	7	2	8	6

Hàm f_k :

Hình 3: Mô hình chi tiết f_k

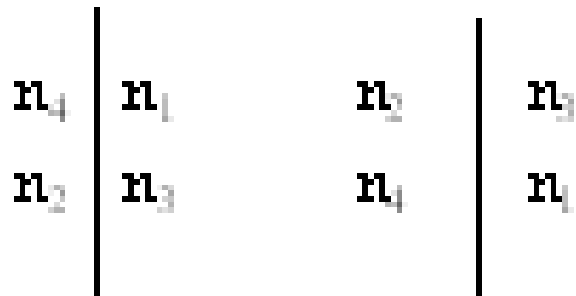


E/P(expension/permutation):

- Hàm E/P tuân theo luật sau:

E/P							
4	1	2	3	2	3	4	1

- Nếu gọi 4 bit đầu vào là (n_1, n_2, n_3, n_4) thì E/P được biểu diễn chi tiết như sau:



Khối thay thế S-box

- Tại đầu vào S-box một khối 8 bit được chia thành hai khối 4 bit;
- Mỗi khối 4 bit được đưa vào S_0 và S_1
- Thay thế mỗi khối 4 bit bằng khối 2 bit;
- Các khối S_0 và S_1 được định nghĩa như sau:

S_0 :

1	0	3	2
3	2	1	0
0	2	1	3
3	1	3	2

S_1 :

0	1	2	3
2	0	1	3
3	0	1	2
2	1	0	3

Khối thay thế S-box

- Phần tử trong khối S-box có độ dài 2 bit;
- Quá trình thay thế trong S-box:
 - Với 4 bit đầu vào là (b_1, b_2, b_3, b_4) ;
 - b_1 và b_4 kết hợp thành một số chỉ ra hàng của S box,
 - b_2 và b_3 tạo thành số chỉ ra cột trong S box;
 - Phần tử được chỉ ra bởi hàng và cột được thay thế cho 4 bit đầu vào hộp đó.

Hàm P4

- Hàm hoán vị P4 tuân theo luật sau:

P4			
2	4	3	1

Hàm SW

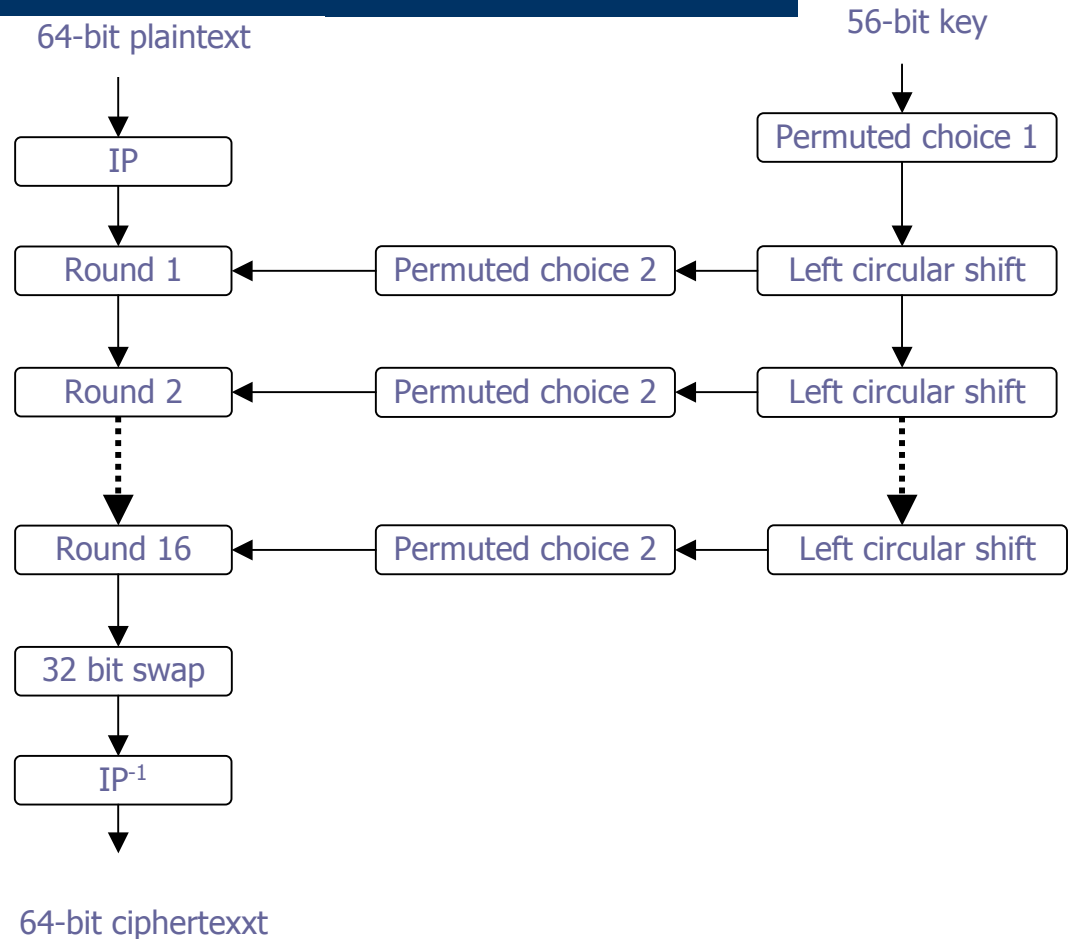
- Hàm f_k chỉ thay đổi 4 bit trái của đầu vào vì vậy
- Hàm SW đổi 4 bit phải và 4 bit trái để khi thực hiện hàm f_k lần sau sẽ thực hiện thay đổi 4 bit khác.
- Hàm f_k thực hiện lần 2 thực hiện các hàm E/P, $S_0, S_1, P4$ như trên.

Chuẩn mã hóa dữ liệu DES (Data Encryption Standard)

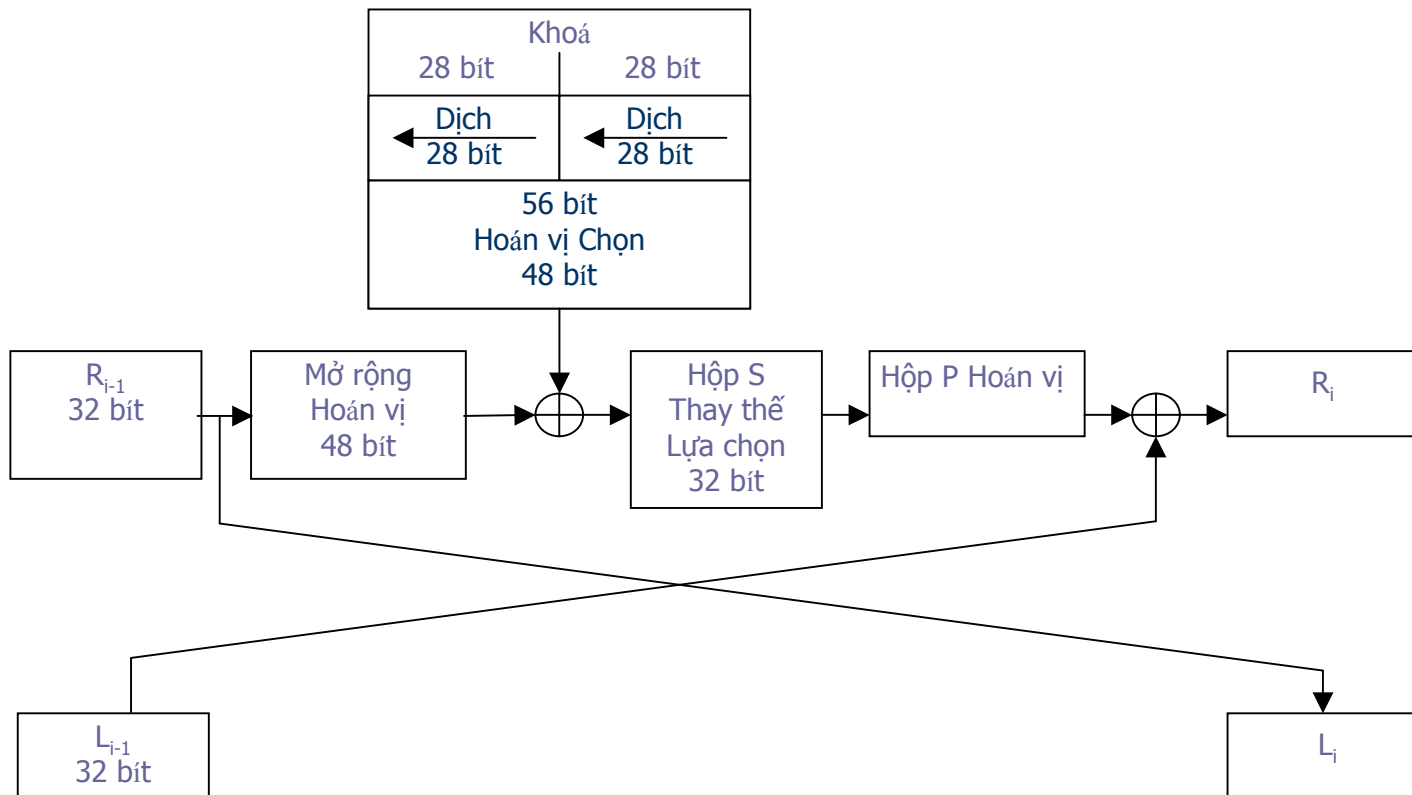
- Chuẩn mã hoá dữ liệu DES được Văn phòng tiêu chuẩn của Mỹ (U.S National Bureau for Standards) công bố năm 1971 để sử dụng trong các cơ quan chính phủ liên bang. Giải thuật được phát triển tại Công ty IBM.
- DES có một số đặc điểm sau:
 - Sử dụng khoá 56 bit.
 - Xử lý khối vào 64 bit, biến đổi khối vào thành khối ra 64 bit.
 - Mã hoá và giải mã được sử dụng cùng một khoá.
 - DES được thiết kế để chạy trên phần cứng.
 - DES thường được sử dụng để mã hoá các dòng dữ liệu mạng và mã hoá dữ liệu được lưu trữ trên đĩa.

Mô tả thuật toán

Hình 4: Mô tả chung của giải thuật DES



Chi tiết một vòng lặp



Hoán vị khởi đầu

Hoán vị khởi đầu đổi chỗ khối dữ liệu vào, thay đổi vị trí của các bit trong khối dữ liệu vào, như được mô tả trong bảng

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

Khoá chuyển đổi

Đầu tiên 56 bit khoá thực hiện hoán vị chọn lựa 1 theo bảng

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

Hoán vị khởi đầu

- Sau khi khoá 56 bit được chuyển đổi, một khoá khác 48 bit được sinh ra cho mỗi vòng của DES. Những khoá này, k_i , được xác định bằng cách:
 - + Đầu tiên, khoá 56 bit được chia làm hai phần mỗi phần 28 bit. Sau đó, các phần này được dịch trái một hoặc hai bit, phụ thuộc vào vòng đó. Số bit được dịch được cho trong bảng .

Vòng	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Số bit dịch	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Sau khi được dịch, 48 bit được lựa chọn ra từ 56 bit. Bởi vì sự thực hiện này đổi chỗ thứ tự các bit như là sự lựa chọn một tập con các bit, nó được gọi là hoán vị nén (compression permutation), hoặc hoán vị lựa chọn2 (permuted choice 2)

Bảng định nghĩa hoán vị nén

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

. Hoán vị mở rộng

Ở thao tác này, nửa phải của dữ liệu, R_i , được mở rộng từ 32 bit thành 48 bit. Bởi vì sự thực hiện này thay đổi thứ tự của các bit bằng cách lặp lại một bit nào đó, nó được hiểu như là một sự hoán vị mở rộng.

Bảng hoán vị mở rộng

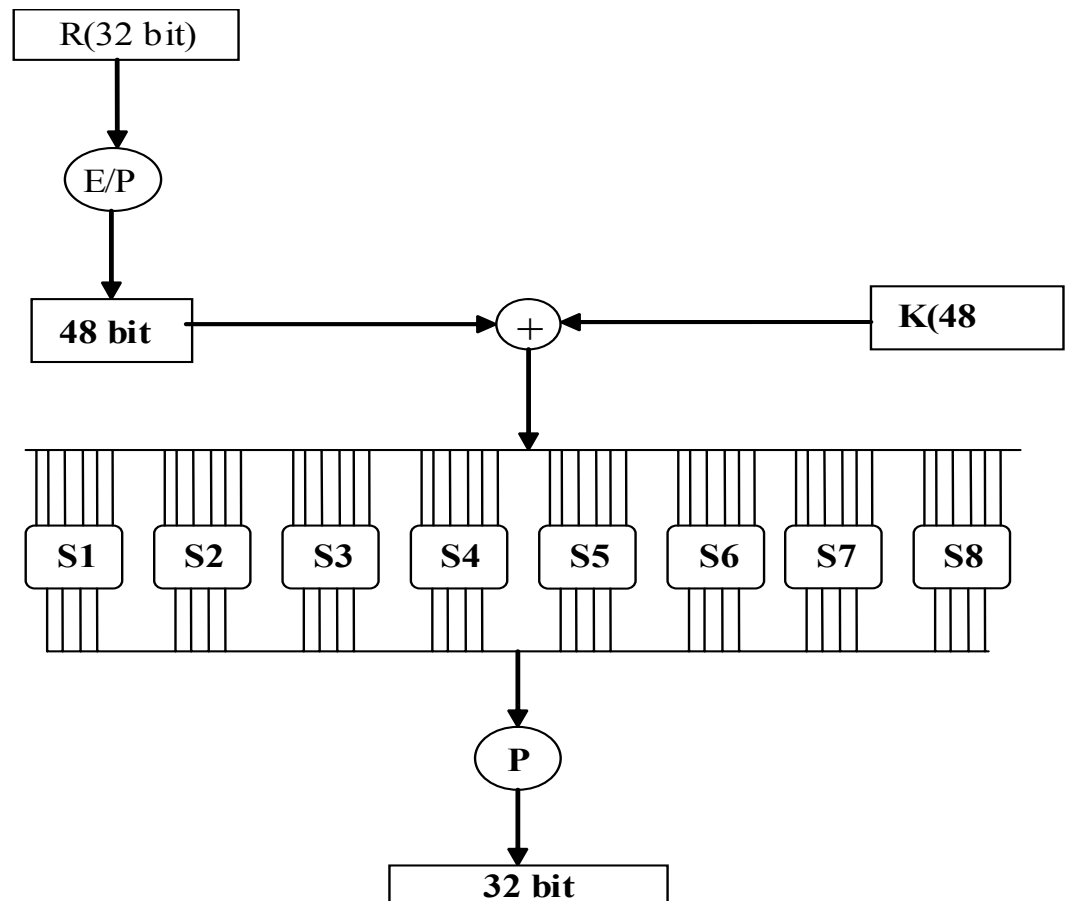
32	1	2	3	4	5	4	5	6	7	8	9
8	9	10	11	12	12	12	13	14	15	16	17
16	17	18	19	20	21	20	21	22	23	24	25
24	25	26	27	28	29	28	29	30	31	32	1

Hộp thay thế S

- Sau khi được nén, khoá được 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 (substitution boxes, S-boxes). Khối 48 bit được chia thành 8 khối 6 bit. Mỗi khối được thực hiện trên một hộp S riêng biệt (separate S-box): khối 1 được thực hiện trên hộp S1, khối 2 được thực hiện trên hộp S2,... , khối 8 được thực hiện trên hộp S8.
- Mỗi hộp S là một bảng gồm 4 hàng và 16 cột. Mỗi phần tử của hộp là một số 4 bit. Sáu bit vào hộp S sẽ xác định số hàng và số cột để tìm kết quả ra. Các bảng sau biểu diễn 8 hộp S.

Các hộp S-box

Các hộp S



Các hộp S-box: các bảng biểu diễn

8 S-box

S1:

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

S2:

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

Các hộp S-box

S3:

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

S4:

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

Các hộp S-box

S5:

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

S6:

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

Các hộp S-box

S7:

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

S8:

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

Quá trình thay thế

- Những bit vào xác định một phần tử trong hộp S một cách riêng biệt. Sáu bit vào của hộp được ký hiệu là b_1, b_2, b_3, b_4, b_5 và b_6 . Bit b_1 và b_6 được kết hợp thành một số 2 bit, nhận giá trị từ 0 đến 3, tương ứng với một hàng trong bảng. Bốn bit ở giữa, từ b_2 tới b_5 , được kết hợp thành một số 4 bit, nhận giá trị từ 0 đến 15, tương ứng với một cột trong bảng.
- Ví dụ, giả sử ta đưa dữ liệu vào hộp S thứ 6 (bit 31 tới bit 36 của hàm XOR) là 110010. Bit đầu tiên và bit cuối cùng kết hợp thành 10, tương ứng với hàng thứ 2 của hộp S thứ 6. Bốn bit giữa kết hợp thành 1001, tương ứng với cột thứ 9 của hộp S thứ 6. Phần tử hàng 2 cột 9 của hộp S thứ 6 là 0. Giá trị 0000 được thay thế cho 110010.

Hộp hoán vị P

- Khối dữ liệu 32 bit ra của hộp thay thế S được hoán vị tiếp trong hộp P. Sự hoán vị này ánh xạ mỗi bit dữ liệu vào tới một vị trí trong khối dữ liệu ra; không bit nào được sử dụng hai lần và cũng không bit nào bị bỏ qua. Nó được gọi là hoán vị trực tiếp (straight permutation). Bảng cho ta vị trí của mỗi bit cần chuyển. Ví dụ: bit 4 chuyển tới bit 21, trong khi bit 32 chuyển tới bit 4.

Bảng hoán vị P32:

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 cuối cùng

- Hoán vị cuối cùng là nghịch đảo của hoán vị khởi đầu, và nó được mô tả trong bảng dưới. Chú ý rằng nửa trái và nửa phải không được trao đổi sau vòng cuối cùng của DES; thay vào đó khối nội R16L16 được sử dụng như khối dữ liệu ra của hoán vị cuối cùng.

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

Giải mã DES

- Sau khi thay đổi, hoán vị, XOR, và dịch vòng, chúng ta có thể nghĩ rằng thuật toán giải mã phức tạp, khó hiểu như thuật toán mã hoá và hoàn toàn khác thuật toán mã hoá. Trái lại, sự hoạt động được lựa chọn để đưa ra một đặc tính hữu ích: cùng thuật toán làm việc cho cả mã hoá và giải mã.
- Với DES, có thể sử dụng cùng chức năng để giải mã hoặc mã hoá một khối. Chỉ có sự khác nhau đó là các khoá phải được sử dụng theo thứ tự ngược lại.

Độ an toàn của DES

- Tính bảo mật của một hệ mã hoá đối xứng là một hàm hai tham số: độ phức tạp của thuật toán và độ dài của khoá.
- Khoá có độ dài 56 bit, thì sẽ có 2^{56} khoá có thể sử dụng.
- Giả sử rằng tính bảo mật chỉ phụ thuộc vào độ phức tạp của thuật toán. Có nghĩa rằng sẽ không có phương pháp nào để phá vỡ hệ thống mật mã hơn là cố gắng thử mọi khoá có thể, phương pháp đó được gọi là brute-force attack. Giả sử một Suppercomputer có thể thử một triệu khoá trong một giây, thì nó sẽ cần 2000 năm để tìm ra khoá đúng.

Kết luận

- Có rất nhiều phương pháp mã hoá để đảm bảo an toàn dữ liệu. Để đánh giá tính ưu việt một giải thuật mã hoá người ta thường dựa vào các yếu tố: tính bảo mật, độ phức tạp, tốc độ thực hiện giải thuật và vấn đề phân phối khoá trong môi trường nhiều người sử dụng.
- Các phương pháp mã hoá cổ điển như phương pháp mã hoá thay thế, hoán vị còn đơn giản. Nhược điểm của chúng là độ an toàn không cao vì thường không đạt được độ phức tạp cần thiết và rất dễ bị lộ khoá do cả người gửi và người nhận đều sử dụng cùng một khoá.
- DES đã được phân tích kỹ lưỡng và công nhận là vững chắc. Các hạn chế của nó đã được hiểu rõ và có thể xem xét trong quá trình thiết kế. Và để tăng độ an toàn hơn, ngày nay các hệ thống mã hoá sử dụng DES mở rộng được ứng dụng rộng rãi. Với DES mở rộng khoá có thể là 128 bit, 192 bit,... độ lớn khối có thể là 128 bit. Do vậy, độ an toàn của DES mở rộng cao hơn rất nhiều.