

AN TOÀN VÀ BẢO MẬT HỆ THÔNG THÔNG TIN

Giáo viên: Trần Hồng Diệp

Bộ môn: Tin học

Email: diepth18@yahoo.com
diepth18@gmail.com



Các hệ mật mã khóa bí mật

- Mã luồng
 - Mã Ceasar
 - Mã Vigenere
 - Mã Vernam
- Mã khối
 - **DES**
 - AES
 - Bài tập (DES)

Mã khối

- Đơn vị mã hóa cơ bản là các khối ký tự
- Các tham số bao gồm: kích thước khối và chiều dài khóa
 - Kích thước khối lớn để chống tấn công bằng thống kê
 - Chiều dài khóa lớn để chống tấn công vét cạn

Hệ mật mã Data Encryption Standard (DES)

□ Lịch sử

- 1970, NIST kêu gọi xây dựng hệ mật mã dành cho công chúng
- 1974, IBM xây dựng DES trên nền tảng hệ Lucifer
- 1979, chuẩn hóa

□ Mục tiêu

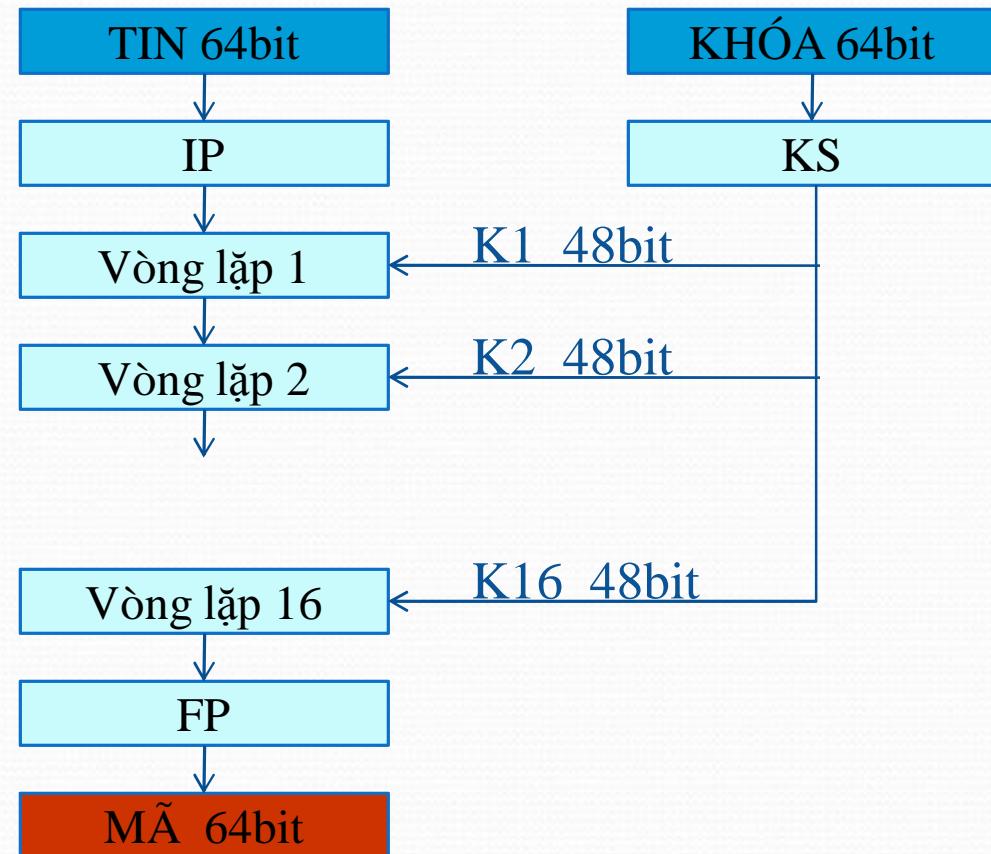
- Sử dụng rộng rãi
- Độ an toàn cao
- Không phụ thuộc vào tính bí mật của thuật toán

□ Ứng dụng

- ATM
- Truy nhập từ xa
- ...

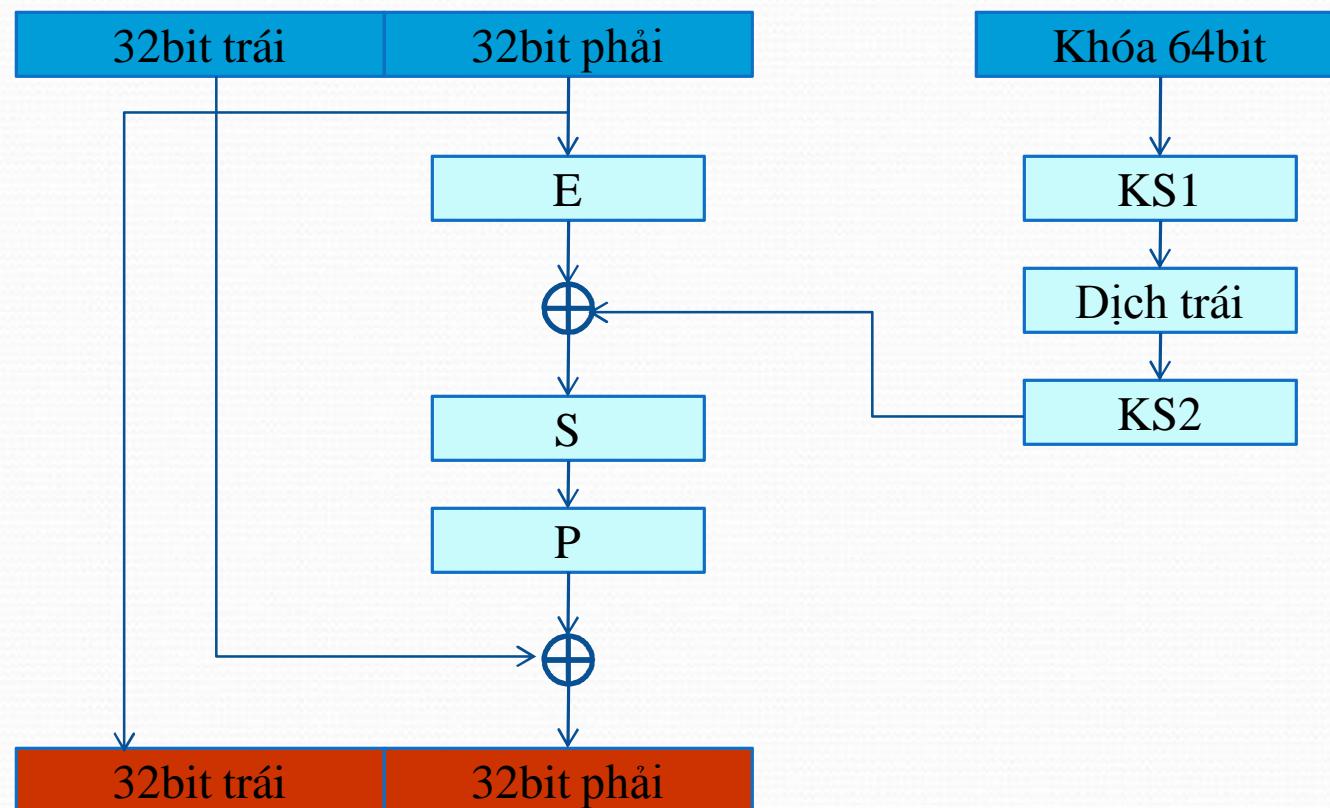
Mô hình mã hóa DES

- Tin được mã hóa theo từng khối 64 bit.
- Khóa 56 bit
- Có 16 vòng lặp mã hóa
- Mỗi vòng lặp, một khóa Ki được trích từ khóa 56bit ban đầu.



Một vòng lặp DES

- Vào và ra của mỗi vòng lặp đều là một khối 64 bit.
- Mỗi khối được phân biệt ra 2 phần: 32 bit trái và 32 bit phải



Hoán vị khởi đầu (IP)

- Đổi thứ tự các bít của khối dữ liệu vào:

$$IP(b_1b_2b_3\dots b_{63}b_{64}) = b_{58}b_{50}b_{42}\dots b_{15}b_7$$

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

Chuyển đổi khóa (KS1)

- Khóa 64 bit ban đầu được bỏ 8 bít chẵn lẻ và được xếp lại theo thứ tự cho trong bảng KS1:

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

- Thu được khóa 56 bit

Dịch trái khóa

- Khóa 56 bit được chia ra 2 nửa: nửa đầu và nửa sau, mỗi nửa 28 bit
- Mỗi nửa thực hiện việc dịch trái 1 hoặc 2 bit tùy thuộc vào số thứ tự của vòng lặp DES.
- Vòng lặp thứ 1, 2, 9 và 16 dịch trái 1, các vòng lặp còn lại dịch trái 2

Hoán vị nén (KS2)

- ❑ Còn được gọi là hoán vị lựa chọn
- ❑ Hai khối 28 bit được lựa chọn 48 bit và xếp lại theo thứ tự cho trong bảng KS2:

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 (E)

- ❑ Nửa phải 32 bit của khối dữ liệu vào trong mỗi vòng lặp DES được mở rộng thành 48 bit bằng cách lặp lại một số bit.
- ❑ Định nghĩa hoán vị mở rộng cho trong bảng E sau:

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

Hộp thay thế S

- **Nhiệm vụ**
 - Chuyển khối vào 48bit thành khối ra 32bit
- **Cách làm**
 - Chia khối vào 48bit ban đầu thành 8 khối nhỏ, lần lượt là: B1, B2, B3...B8. Mỗi khối Bi gồm 6bit.
 - Có 8 hộp thay thế S.
 - Mỗi khối Bi sử dụng hộp Si tương ứng để biến đổi thành khối 4bit

Hộp thay thế S

□ S1:

	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	13

□ S2:

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

Hộp thay thế S

□ S3:

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

□ S4:

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

Hộp thay thế S

□ S5:

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

□ S6:

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

Hộp thay thế S

□ S7:

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

□ S8:

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

Hộp thay thế S

□ Ví dụ:

Giả sử khối $B_6 = b_1 b_2 b_3 b_4 b_5 b_6 = 101100$

Chỉ số hàng $= b_1 b_6 = 10_2 = 2_{10}$

Chỉ số cột $= b_2 b_3 b_4 b_5 = 0110_2 = 6_{10}$

Tra bảng S6 được: $12_{10} = 1100_2$

□ S6:

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

Hộp hoán vị P

- Ánh xạ mỗi bit vào tới một bit ra

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 (FP)

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



Cảm ơn!

