Mật mã & Ứng dụng

Trần Đức Khánh
Bộ môn HTTT – Viện CNTT&TT
ĐH BKHN

Mật mã học

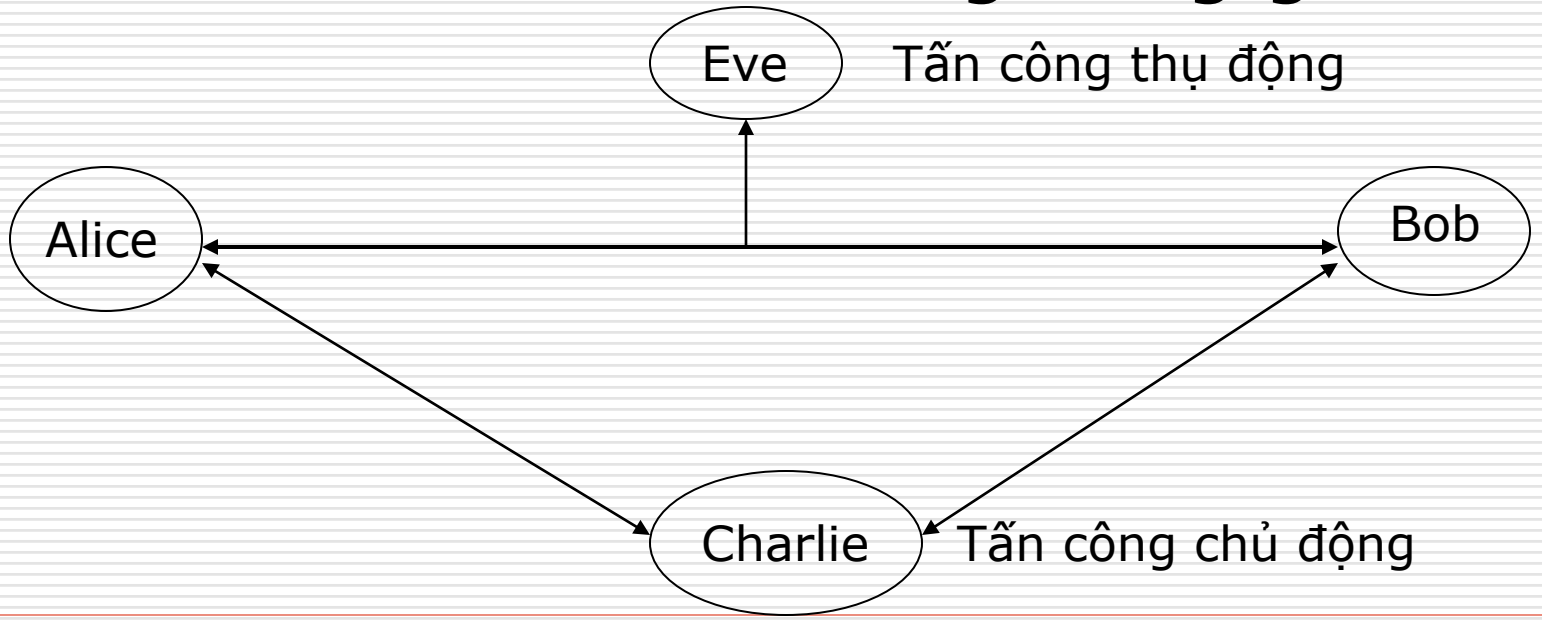
- Mật mã học (Cryptology)
  - Mật mã (Cryptography)
  - Mã thám (Cryptanalysis)
- Mật mã
  - Tăng cường các tính chất *Bí mật* và *Toàn vẹn* thông tin: các phép mã hóa
  - Xây dựng các kỹ thuật trao đổi thông tin bí mật: các giao thức mật mã
- Mã thám
  - Phá mã

Lịch sử ngành Mật mã

- Giai đoạn "Tiền sử" (~ 2000, TCN)
  - Những dấu hiệu đầu tiên của Mật mã xuất hiện ở bên bờ sông Nile, Ai Cập
- Giai đoạn "Mật mã thủ công" (~ 50, TCN)
  - Phép mã hóa Ceasar
- Giai đoạn "Mật mã cơ học" (cho đến Thế chiến 2)
  - Máy Enigma ở Đức
  - Các nghiên cứu về Mã thám ở Anh
- Giai đoạn "Mật mã điện tử"
  - Dựa vào Toán học và Tin học
  - Được đặt nền móng bởi Shanon, Diffie và Hellman
  - Khóa bí mật (DES, AES,…), Khóa công khai (RSA, ElGamal, …)

Trao đổi thông tin bí mật

- Alice và Bob trao đổi thông tin bí mật, được mã hóa
- Eve và Charlie tấn công bằng giải mã



Mục tiêu An toàn

- Bí mật (Confidentiality)
- Toàn vẹn (Integrity)
- Xác thực (Authentication)
- Chống phủ nhận (Non-repudiation)
- …

Chủ đề

- Hệ mật mã cổ điển
- Hệ mật mã khóa bí mật (đối xứng)
- Hệ mật mã khóa công khai (bất đối xứng)
- Hàm băm, chữ ký số
- Quản lý khóa, giao thức mật mã,…

Hệ mật mã

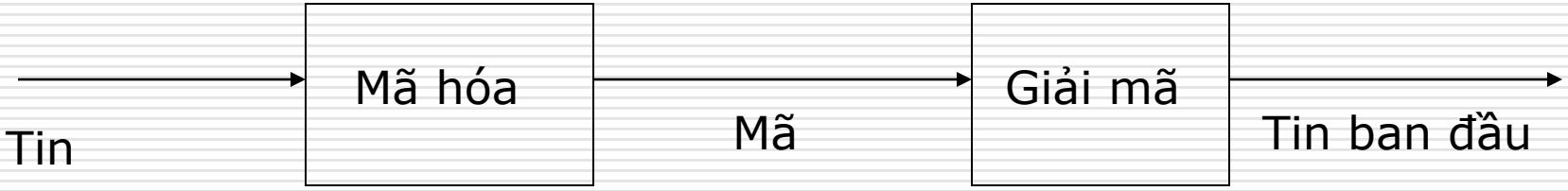
Hệ Mật mã = Bộ 5 (*K,M,C,E,D*)

- Không gian Khóa (Key): *K*
- Không gian Tin (Message/Plaintext): *M*
- Không gian Mã (Cipher): *C*
- Hàm mã hóa (Encryption)
  - *E: K x M -> C*
- Hàm giải mã (Decryption)
  - *D: K x C -> M*

Chủ đề

- Hệ mật mã cổ điển
- Hệ mật mã khóa bí mật (đối xứng)
- Hệ mật mã khóa công khai (bất đối xứng)
- Hàm băm, chữ ký số
- Quản lý khóa, giao thức mật mã,…

Hệ mật mã cổ điển



Hệ mật mã cổ điển

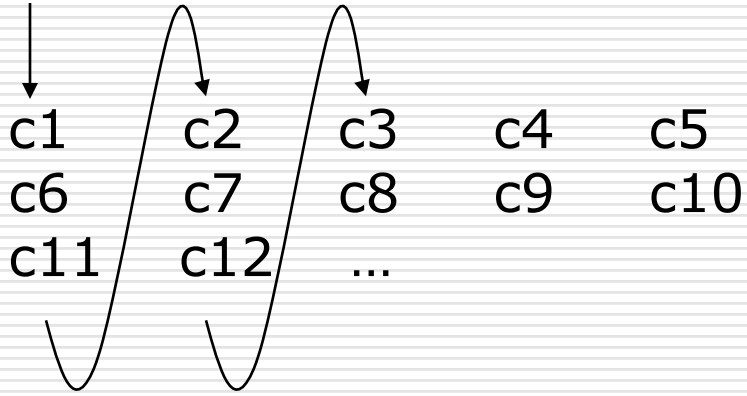
- Mã hoán vị
- Mã đơn thế

Mã hoán vị

- Các ký tự trong Tin được hoán vị cho nhau

Mã hoán vị

Hoán vị cột



chuyển thành

c1	c6	c11	c2	c7
c12	c3	c8	….	….
…..	….	….		

Hoán vị cột

Tin

T H I S I
S A M E S
S A G E T
O S H O W
H O W A C
O L U M N
A R T R A
N S P O S
I T I O N
W O R K S

Hoán vị cột

Tin	Mã
T H I S I	t s s o h
S A M E S	o a n i w
S A G E T	h a a s o
O S H O W	l r s t o
H O W A C	i m g h w
O L U M N	u t p i r
A R T R A	s e e o a
N S P O S	m r o o k
I T I O N	i s t w c
W O R K S	n a s n s

Mã đơn thế

- Mỗi ký tự được thay thế bằng một ký tự khác

Mã đơn thế

Mã Ceasar: $c = m + n$

- m: ký tự trong Tin
- c: ký tự tương ứng trong Mã
- n: độ dịch chuyển
- +: phép cộng modulo 26

Ví dụ: $n = 3$

Tin: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Mã: defghijklmnopqrstuvwxyzabc

Mã Ceasar

Tin

T R E A T Y

I M P O S S I B L E

Mã Ceasar

Tin	Mã
T R E A T Y	W U H D W B
I M P O S S I B L E	L P S R V V L E O H

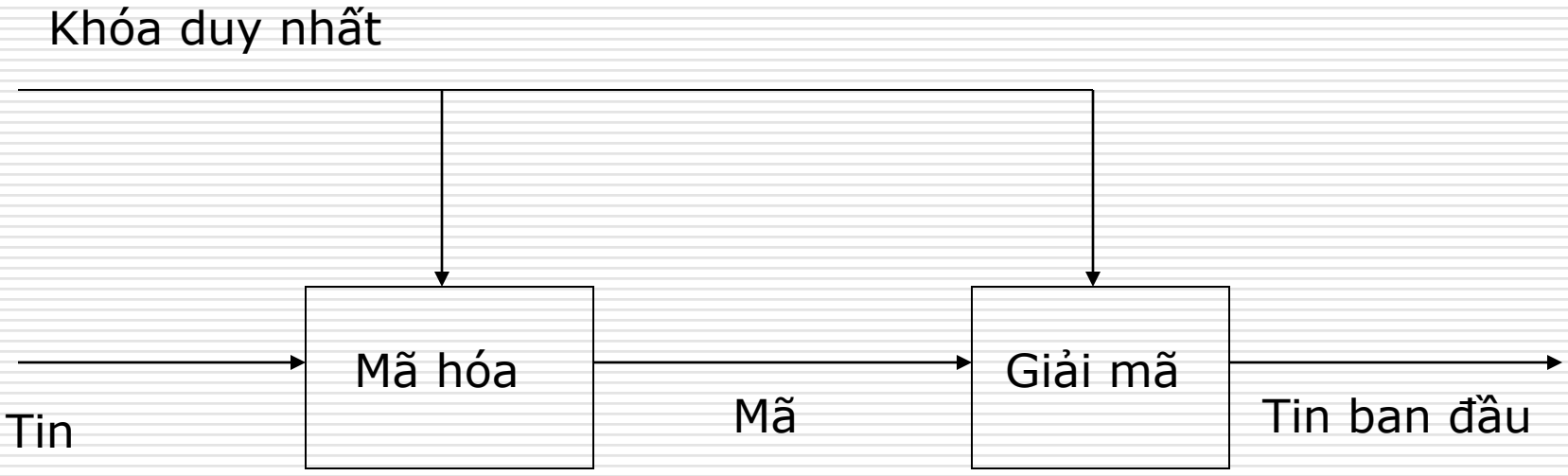
Chủ đề

- Hệ mật mã cổ điển
- Hệ mật mã khóa bí mật (đối xứng)
- Hệ mật mã khóa công khai (bất đối xứng)
- Hàm băm, chữ ký số
- Quản lý khóa, giao thức mật mã,…

Hệ mật mã khóa đối xứng

- Duy nhất một khóa cho quá trình mã hóa và giải mã
  - $C = E(K,M)$
  - $M = D(K,C)$
- Khóa phải được giữ bí mật

Hệ mật mã khóa đối xứng



Các Hệ mật mã khóa đối xứng

- Mã luồng
  - Mã Vigenère
  - Mã Vernam
- Mã khối
  - DES
  - AES

Mã luồng

- Đơn vị mã hóa cơ bản là các ký tự
  - Các ký tự trong Tin được mã hóa tách biệt

Mã Vigenère

Khóa

Tin

Mã Vigenère

- Khóa
  - BENCH
- Tin
  - A LIMERICK PACKS LAUGHS ANATOMICAL
- Nối dài Khóa
  - B ENCHBENC HBENC HBENCH BENCHBENCH
- Mã hóa
  - Khóa: B ENCHBENC HBENC HBENCH BENCHBENCH
  - Tin: A LIMERICK PACKS LAUGHS ANATOMICAL
  - Mã: B PVOLSMPM WBGXU SBYTJZ BRNVVNMPCS

Mã Vernam

- Ký tự là các bit
- Khóa
  - K = K1K2K3…Kn
  - Số ngẫu nhiên
- Tin
  - M = M1M2M3…Mn
- Mã
  - C = C1C2C3…Cn

trong đó *Ci = Ki xor Mi*

Ki	*Mi*	*Ci = Ki xor Mi*
0	0	0
0	1	1
1	0	1
1	1	0

Mã khối

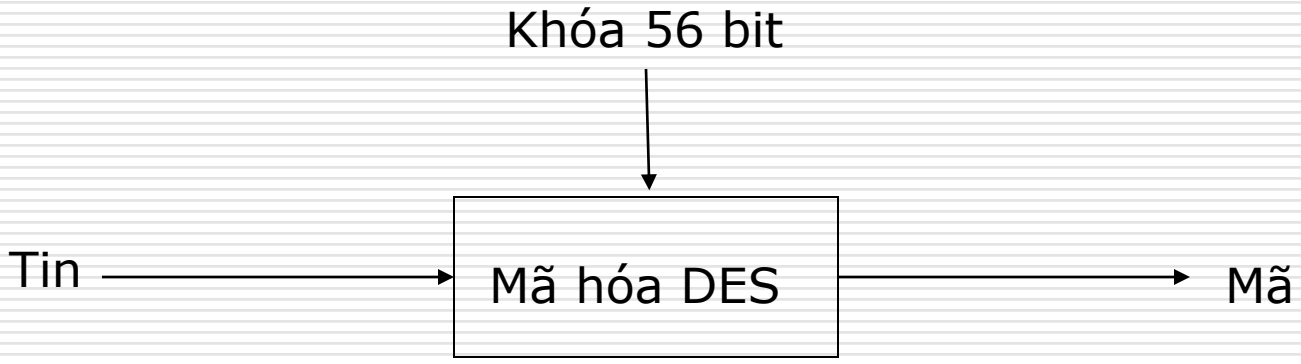
- Đơn vị mã hóa cơ bản là các khối ký tự
- Các tham số bao gồm kích thước khối và chiều dài khóa
  - Kích thước khối lớn để chống tấn công bằng thống kê
  - Chiều dài khóa lớn để chống tấn công vét cạn

Data Encryption Standard (DES)

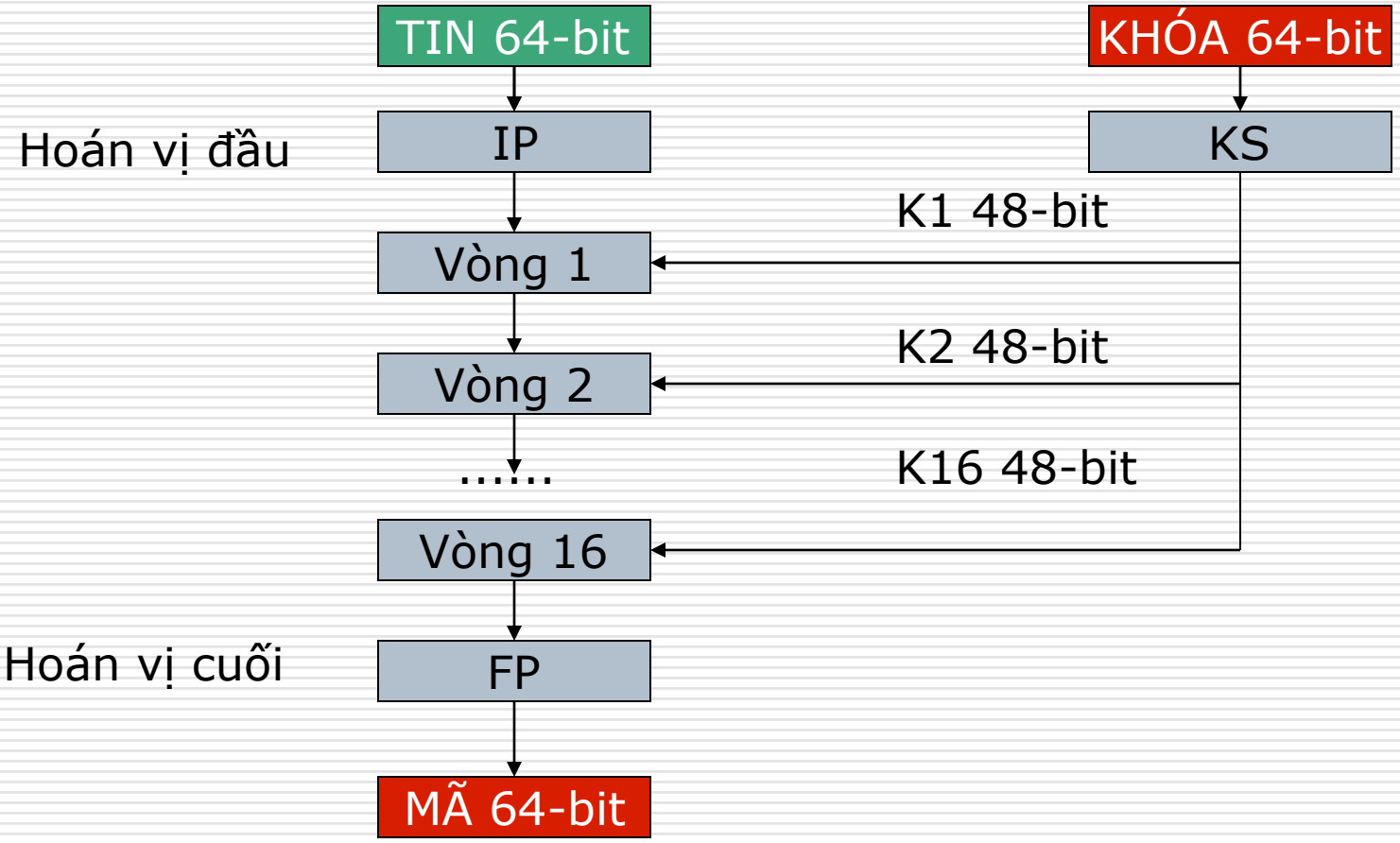
- Lịch sử
  - ~ 1970, NIST kêu gọi xây dựng hệ mật mã dành cho công chúng
  - 1974, IBM xây dựng DES trên nền tảng của hệ Lucifer
  - 1979, chuẩn hóa
- Mục tiêu
  - Mục đích sử dụng rộng rãi
  - Độ an toàn cao
  - Không phụ thuộc vào tính bí mật của thuật toán
- Ứng dụng
  - ATM
  - Truy nhập từ xa
  - …

Data Encryption Standard (DES)

- DES
  - Khối 64 bit
  - Khóa 56 bit
  - 16 vòng lặp mã hóa
  - Mỗi vòng kết hợp Hoán vị + Đơn thế



Mã hóa DES


TIN 64-bit
KHÓA 64-bit
Hoán vị đầu
IP
KS
K1 48-bit
Vòng 1
K2 48-bit
Vòng 2
.....
K16 48-bit
Vòng 16
Hoán vị cuối
FP
MÃ 64-bit

IP, FP

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

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

- $IP(b1b2…b64) = b58b50…b7$
- $FP(b1b2…b64) = b40b8…b25$

KS

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

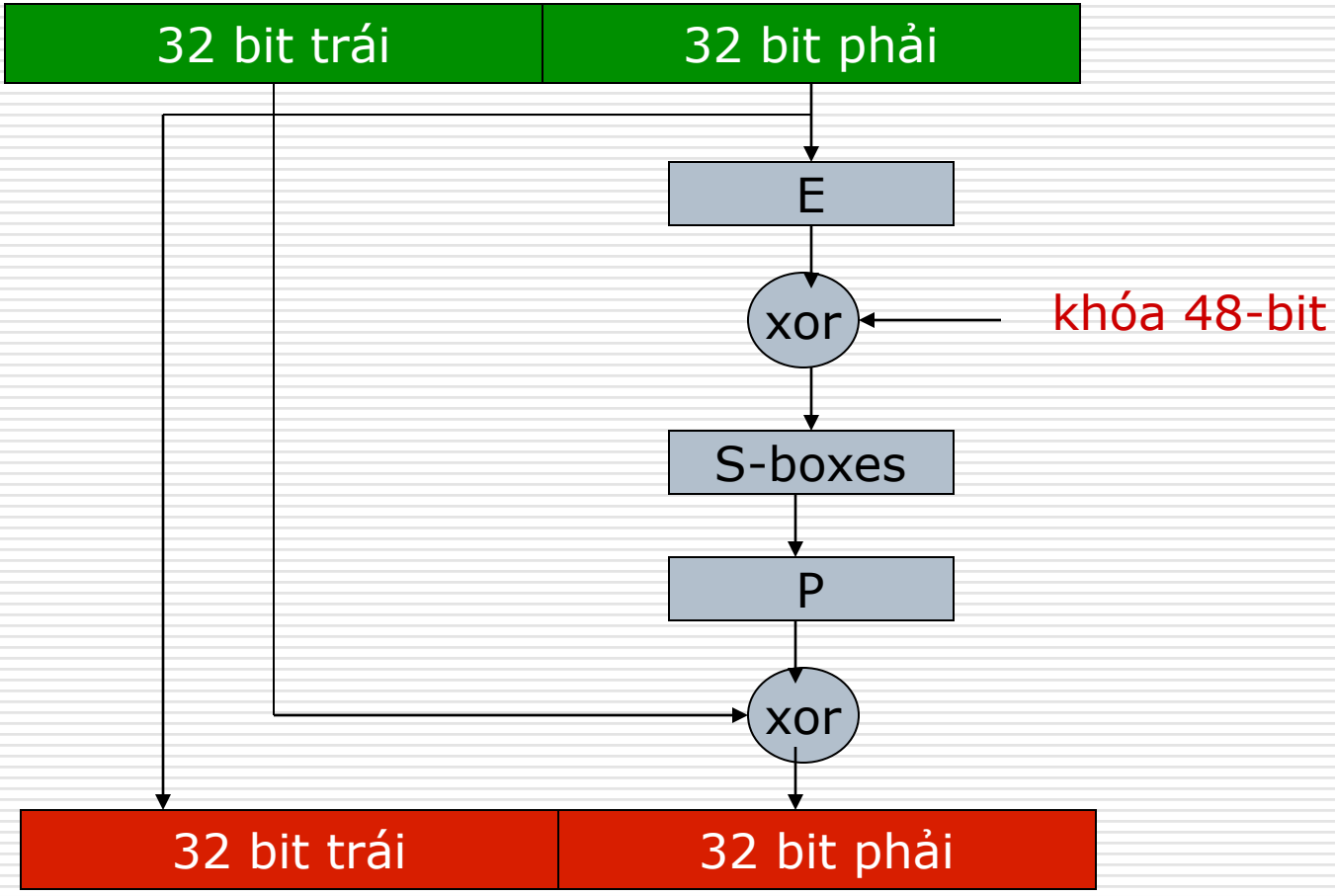
KS2					
14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

- *KS1* chuyển khối 64 bit thành khối 2 khối 28 bit
  - *KS1(b1b2…b64) = b57b49…b36 b63b55…b4*
- *KS2* chuyển 2 khối 28 bit thành khối 48 bit
  - *KS2 (b1b2…b56) = b14b17…b32*

KS

- Khóa ban đầu K
- *(C0,D0) = KS1(K)*
- *Ki = KS2 (Ci,Di)*
  - *Ci*
    - Dịch chuyển vòng tròn sang trái 1 bit *Ci-1* nếu i = 1,2,9,16
    - Dịch chuyển vòng tròn sang trái 2 bit *Ci-1* trong các trường hợp khác
  - Tương tự cho *Di*

Vòng lặp DES


32 bit trái
32 bit phải
E
xor
khóa 48-bit
S-boxes
P
xor
32 bit trái
32 bit phải

E, P

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

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

- *E(b1b2…b32) = b32b1…b1*
- *P(b1b2…b32) = b16b7…b25*

S-Boxes

- Chuyển khối 48 bit thành khối 32 bit
  - 8 khối 6 bit: S1, S2,…,S8 (b1b2b3b4b5b6)
  - Chuyển S1 thành khối 4 bit
    - b1b6 cho giá trị thập phân i
    - b2b3b4b5 cho giá trị thập phân j
    - kết quả tại dòng i cột j của bảng 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

  - Tương tự đối với S2,S3,…,S8 (có bảng riêng)

S-Boxes

- Chuyển S1 (110001) thành khối 4 bit
  - b1b6 (11) cho giá trị thập phân i (3)
  - b2b3b4b5 (1000) cho giá trị thập phân j (8):
  - kết quả (5) tại dòng i (3) cột j (8) của bảng 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

5 (Thập phân) = 0101 (Nhị phân)

Giải mã DES

- Sử dụng cùng một dãy khóa
- Thứ tự các khóa đảo ngược
- Hoán đổi 2 nửa trái, phải
- Thực hiện cùng số vòng lặp

Điểm yếu DES

- Tìm khóa bằng vét cạn
  - 2^{56} khả năng
- Sử dụng tính bù để loại trừ số khả năng khóa

$$c = DES(k, m) \Rightarrow \overline{c} = DES(\overline{k}, \overline{m})$$

Ví dụ

$$\overline{1011} = 0100$$

- Khóa yếu
  - *c = DES(k, m)* và *m = DES(k, c)*
  - *c = DES(k1,m)* và *c = DES(k2,m)*
- Mã thám
  - Vi sai
  - Tuyến tính
  - Davies

3DES

- Mã hóa
  - $c = E(k3,(D(k2,E(k1,m)))$
- Giải mã
  - $m = D(k1,(E(k2,D(k3,c)))$
- Lựa chọn khóa
  - *k1,k2,k3* độc lập
  - *k1,k2* độc lập và *k3* = *k1*
  - *k1=k2=k3*

Advanced Encryption Standard (AES)

- 1997, NIST kêu gọi xây dựng một hệ mật mã mới để thay thế DES
- Hệ Rijndael của Daemen và Rijmen được lựa chọn
- 2001, hệ Rijndael được chuẩn hóa thành AES
  - Dựa trên lý thuyết "Trường Galois"
  - Khối 128 bit
  - Khóa 128, 192, 256 bit
  - n vòng lặp mã hóa, phụ thuộc vào chiều dài khóa
    - Khóa 128 bit, n = 10
    - Khóa 192 bit, n = 12
    - Khóa 256 bit, n = 14
  - Mỗi vòng kết hợp Hoán vị + Đơn thế