AN TOÀN THÔNG TIN

DES & DES3

Nhóm 8

Lê Minh Tuấn	20203916
Nguyễn Huy Toàn	20203890
Trần Duy Anh	20203872
Ngô Thị Thu Thủy	20203888
Bùi Vũ Bình Giang	20203897
Đào Thị Hồng Loan	20203903

1 Giới thiệu về DES và 3DES

2 Thuật toán DES

3 Thuật toán 3DES

4 So sánh DES và 3DES

5 Kết luận

Giới thiệu về DES và 3DES

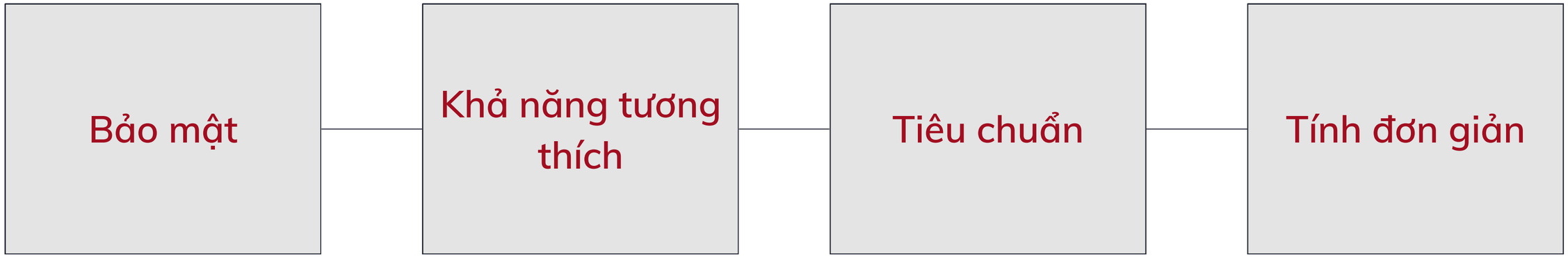
Lịch sử phát triển của DES và 3DES

- Tiền thân của DES là Lucifer, một thuật toán do IBM phát triển.

- 3DES sử dụng cùng một cấu trúc với DES, tuy nhiên nó sử dụng ba lần mã hóa với ba khóa khác nhau để tăng độ bảo mật.

Giới thiệu về DES và 3DES

Tầm quan trọng của DES và 3DES trong lĩnh vực bảo mật thông tin



Giới thiệu về DES và 3DES

Tầm quan trọng của DES và 3DES trong lĩnh vực bảo mật thông tin

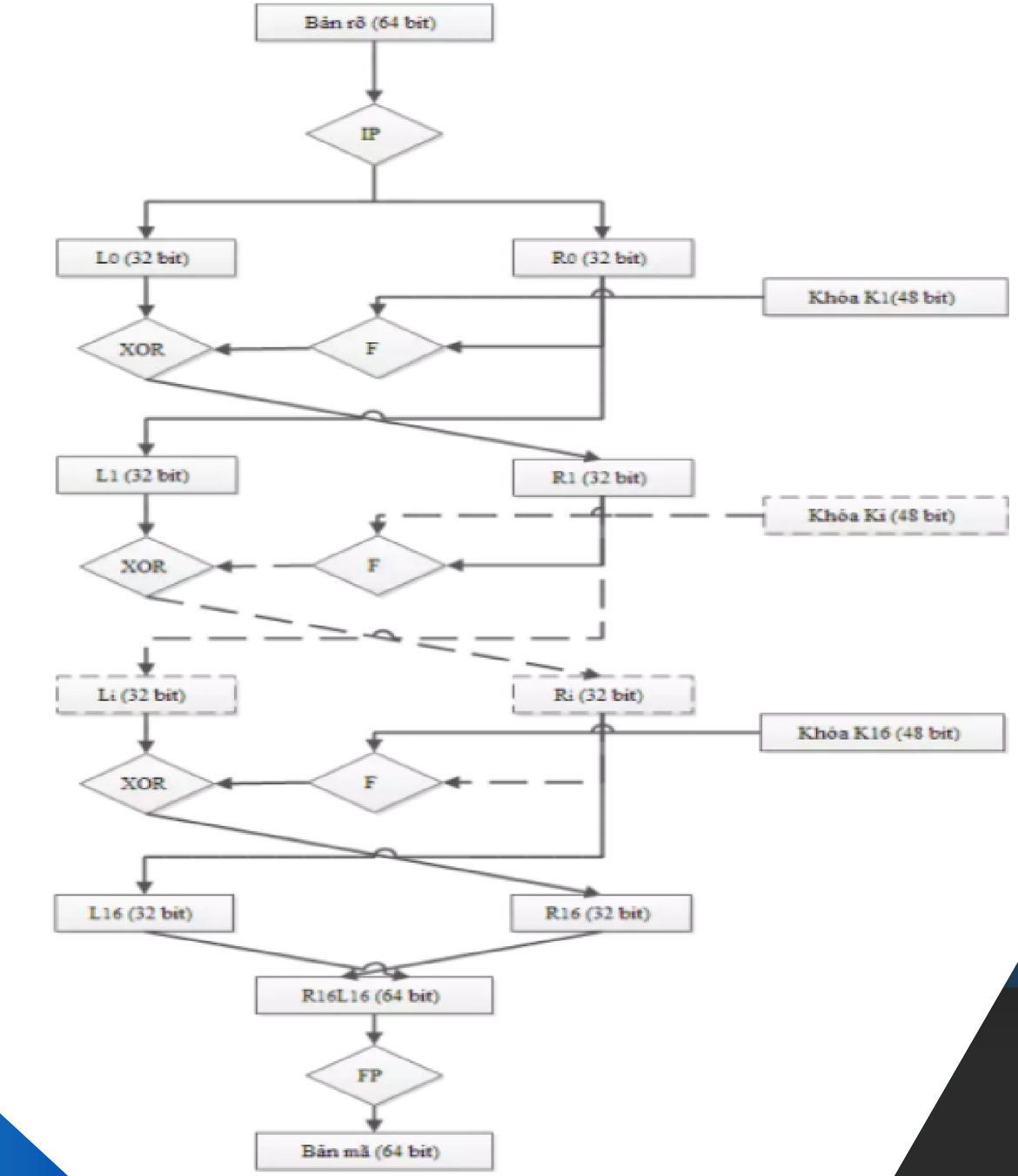
DES và 3DES đóng một vai trò quan trọng trong việc bảo mật dữ liệu

Tuy nhiên đã lỗi thời và phần lớn đã được thay thế bằng các công nghệ mã hóa mới hơn, tiên tiến hơn như AES

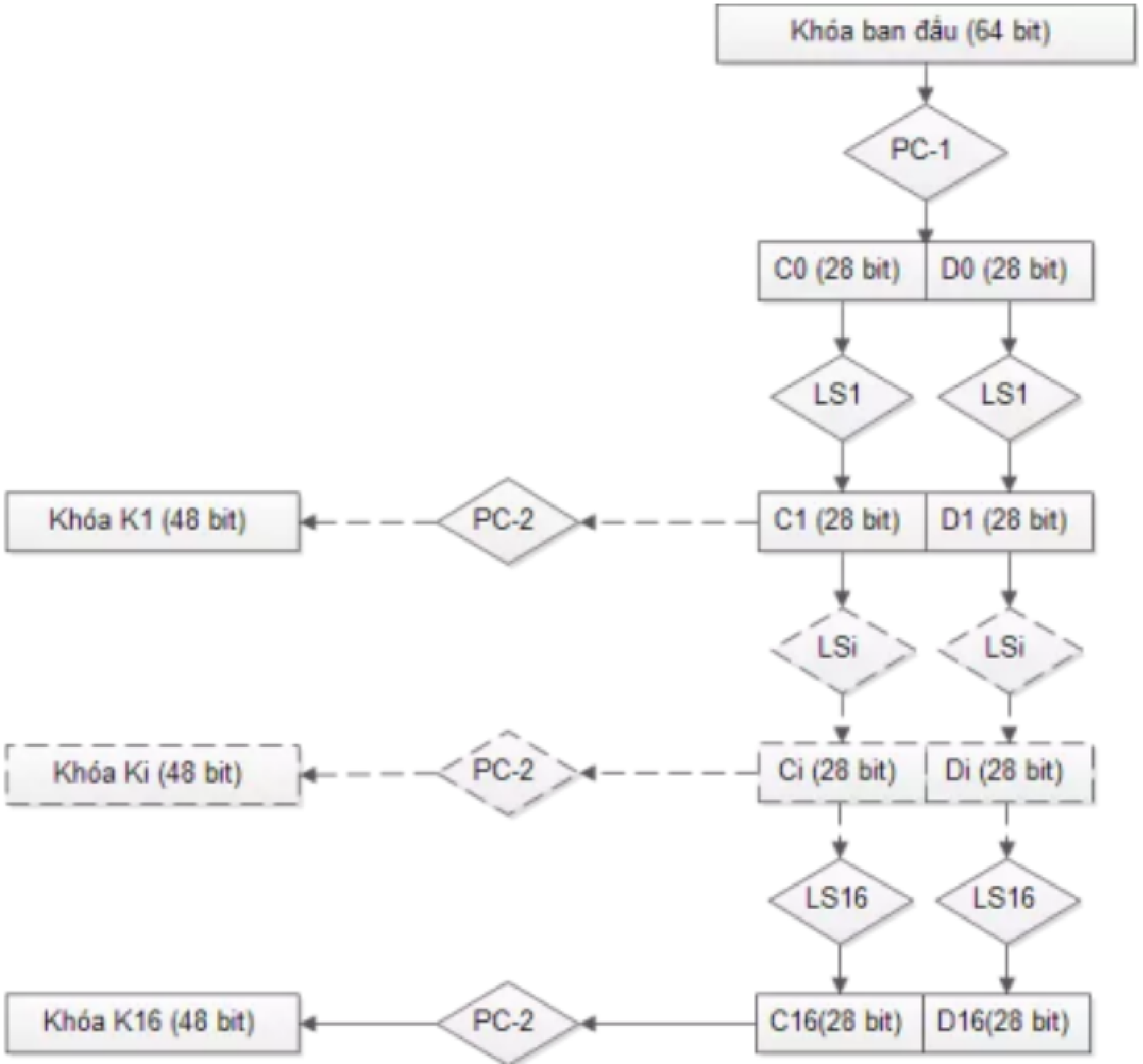
Thuật toán

DES là thuật toán mã hóa theo khối, nó xử lý từng khối thông tin của bản rõ có độ dài xác định là 64 bit.

1	Sinh khóa con
2	Sử dụng phép hóa vị khỏi đầu
3	Với i chạy từ i = 1 đến 16 thực hiện
4	Đổi vị trí khối L16, R16
5	Sử dụng phép hoán vị kết thúc FP(Final Permutation – nghịch đảo với hoán vị khởi đầu IP)


Bản rõ (64 bit)
IP
L0 (32 bit)
R0 (32 bit)
Khóa K1(48 bit)
XOR
F
L1 (32 bit)
R1 (32 bit)
Khóa Ki (48 bit)
XOR
F
Li (32 bit)
Ri (32 bit)
Khóa K16 (48 bit)
XOR
F
L16 (32 bit)
R16 (32 bit)
R16L16 (64 bit)
FP
Bản mã (64 bit)

Quá trình sinh khóa con



16 vòng lặp của DES chạy cùng thuật toán như nhau nhưng với 16 khóa con khác nhau. Các khóa con đều được sinh ra từ khóa chính của DES bằng thuật toán sinh khóa con.

Quá trình sinh khóa con

57	49	41	33	25	17	9	1
58	50	42	34	25	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

Mỗi phần sẽ được xử lý 1 cách độc lập. $C_i = LS_i(C_{i-1})$ $D_i = LS_i(C_{i-1})$ với $1 \leq i \leq 16$.

Quá trình sinh khóa con

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

Cuối cùng sử dụng hoán vị cố định PC-2 (Permuted choice 2) để hoán vị chuỗi CiDi 56 bit tạo thành khóa Ki với 48 bit.

Quá trình mã hóa DES

Giai đoạn 1:

- 1 xâu x’ sẽ được tạo ra bằng cách hoán vị các bit của x theo hoán vị ban đầu IP
- x’ sẽ được chia thành 2 phần L0,R0. x’ = IP(x) = L0R0 Trong đó L0 là 32 bit đầu, R0 là 32 bit cuối.

Giai đoạn 2

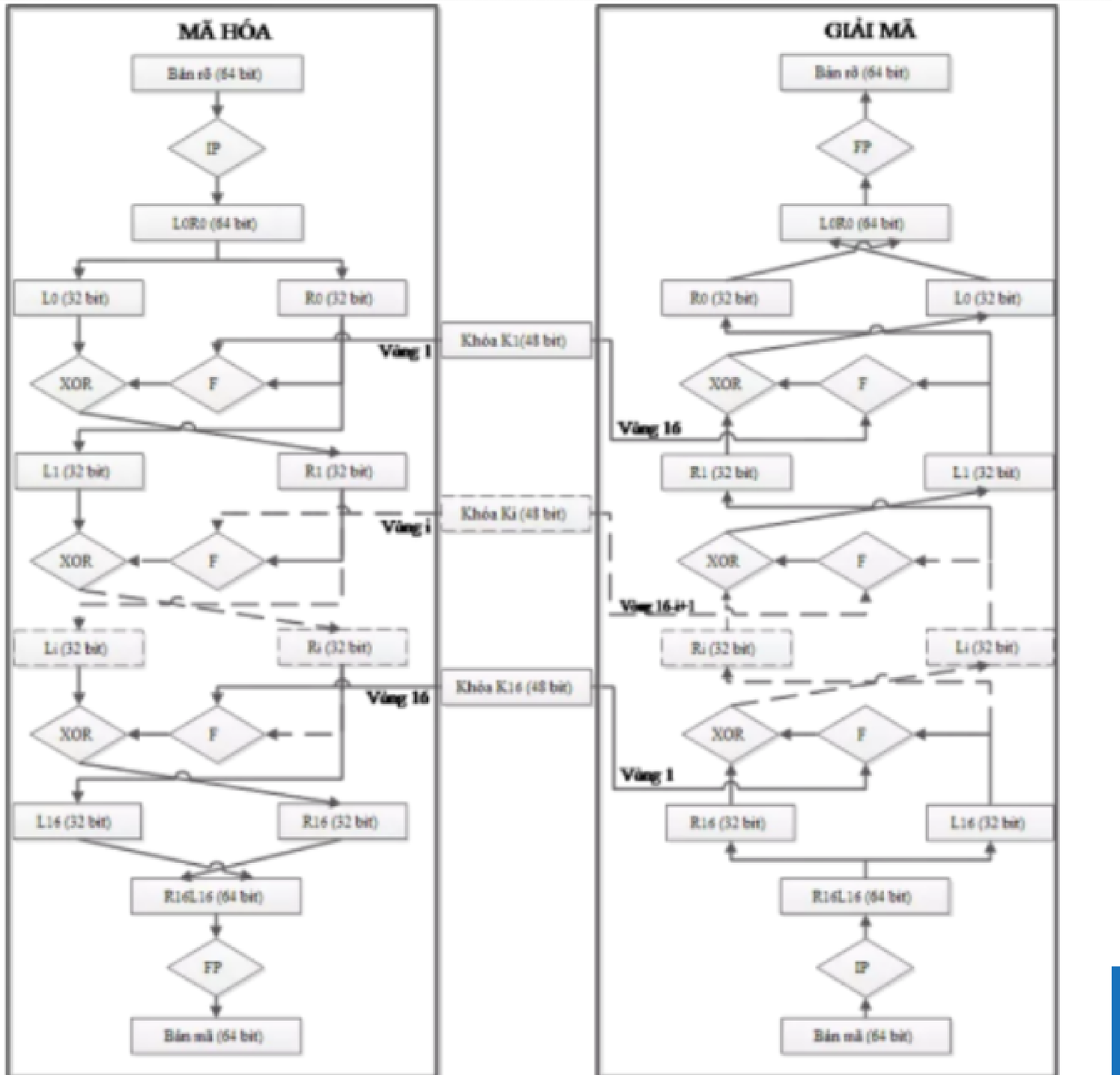
- Tính bằng hàm Li = Ri-1. Ri = Li-1 XOR f(Ri-1, Ki).

Giai đoạn 3

- Áp dụng hoán vị kết thúc FP cho xâu bit R16L16
- thu được bản mã y: y = FP(R16L16).

Giải mã DES

- Tương tự quá trình mã hóa.
- Khác nhau ở: Li = Ri-1. Ri = Li-1 XOR f(Ri-1, K16-i+1). Như vậy khóa K của hàm F sẽ đi từ khóa K16 đến khóa K1.



שורה	מס' עמודה															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	S_1															
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	3	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	13	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
	S_2															
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
	S_3															
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
	S_4															
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
	S_5															
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
	S_6															
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
	S_7															
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
	S_8															
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1									12	5	6	11	0	14	9	2
2									0	6	10	13	15	3	5	8
3										12	9	0	3	5	6	11

Thuật toán 3DES

1. Cơ chế hoạt động của 3DES

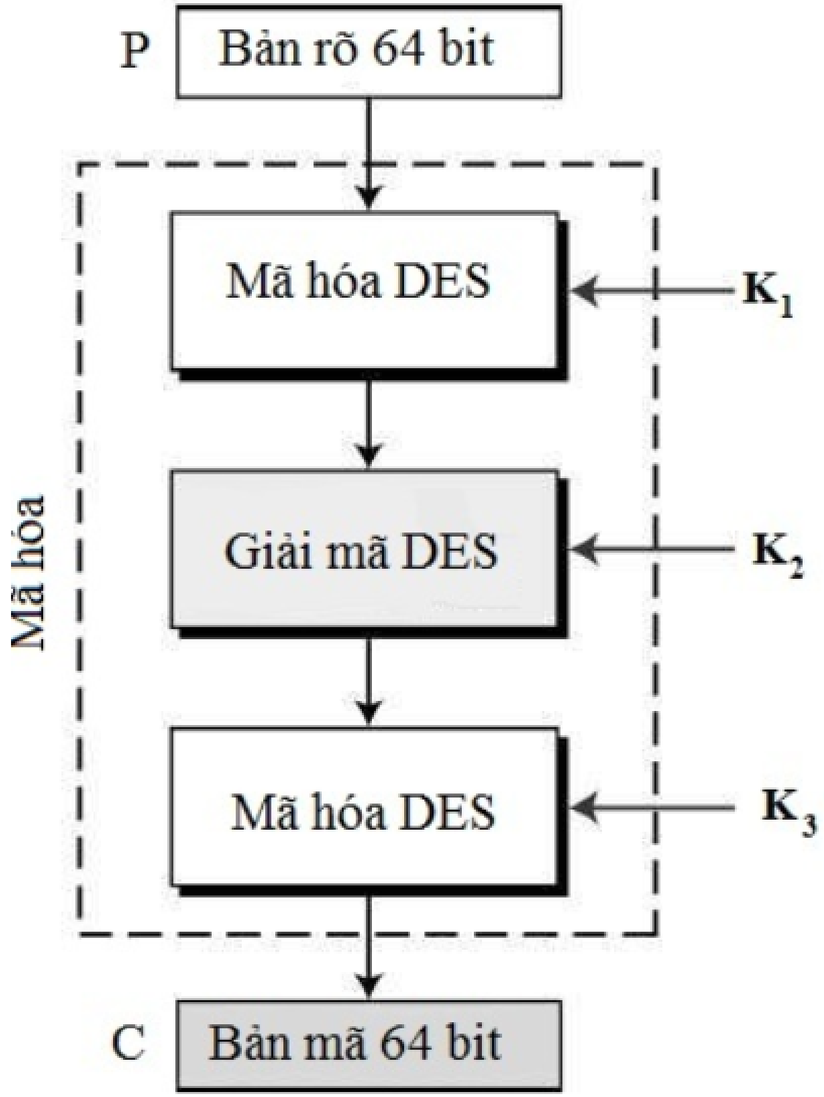
- Nguyên lý của thuật toán khóa đối xứng.
- DES sử dụng 2 khóa, mã hóa mỗi khối 2 lần: EK2(EK1(plaintext)).
- Thuật toán 3DES sử dụng một nhóm khóa bao gồm 3 khóa DES là K1, K2 và K3, mỗi khóa có giá trị 56 bit (trừ 8 bit kiểm tra phát hiện lỗi - parity bits)

Các bước thực hiện thuật toán 3DES

Mã hóa 3DES

Giải mã 3DES

Lựa chọn nhóm khóa



Mức độ bảo mật của 3DES

- Tính chất dễ bị tấn công bởi meet-in-the-middle attack (MITM), mức hiệu quả bảo mật nó đem lại chỉ là 112 bit
- Dễ bị tấn công bằng tấn công với văn bản thuần túy chọn trước, văn bản thuần túy biết trước

✓ *Không an toàn*

✓ *3DES đã bị NIST ngừng sử dụng vào năm 2017.*

So sánh DES & 3 DES

DES là một thuật toán mã hóa đối xứng đơn giản và nhanh nhưng mức độ bảo mật thấp, trong khi 3DES là phiên bản cải tiến của DES với độ an toàn cao hơn nhưng tốc độ xử lý chậm hơn và khóa lớn hơn

Mức độ bảo	3DES mức độ bảo mật cao hơn nhiều so với DES.
Tốc độ xử lý	DES có tốc độ xử lý nhanh hơn so với 3DES
Khóa	3DES sử dụng khóa lớn hơn so với DES, tăng cường độ an toàn
Sử dụng	DES và 3DES đều được sử dụng để bảo vệ dữ liệu truyền qua mạng

So sánh DES & 3 DES

Cả DES và 3DES đều đã lỗi thời và thường được thay thế bằng các thuật toán mã hóa hiện đại hơn như AES.

Mức độ bảo	3DES mức độ bảo mật cao hơn nhiều so với DES.
Tốc độ xử lý	DES có tốc độ xử lý nhanh hơn so với 3DES
Khóa	3DES sử dụng khóa lớn hơn so với DES, tăng cường độ an toàn
Sử dụng	DES và 3DES đều được sử dụng để bảo vệ dữ liệu truyền qua mạng

Tầm quan trọng của DES và 3DES

Khả năng cung cấp
tính bảo mật và tính toàn vẹn
của dữ liệu nhạy cảm.

Được sử dụng rộng rãi
trong các ứng dụng như giao dịch
trực tuyến, mạng riêng ảo (VPN)
và mã hóa email.

Các thuật toán này đảm bảo
dữ liệu không thể bị chặn,
giả mạo hoặc đọc bởi các bên trái phép.

Tuy nhiên, phần lớn DES và 3DES
bị thay thế bởi các thuật toán mã hóa
mới hơn và tiên tiến hơn


Thank you