ĐẠI NAM
UNIVERSITY

CHƯƠNG 2: MÃ KHÓA BÍ MẬT

Giảng viên: Nguyễn Văn Nhân

Điện thoại: 0346542854

Email: nhannv@dainam.edu.vn

Symmetric encryption

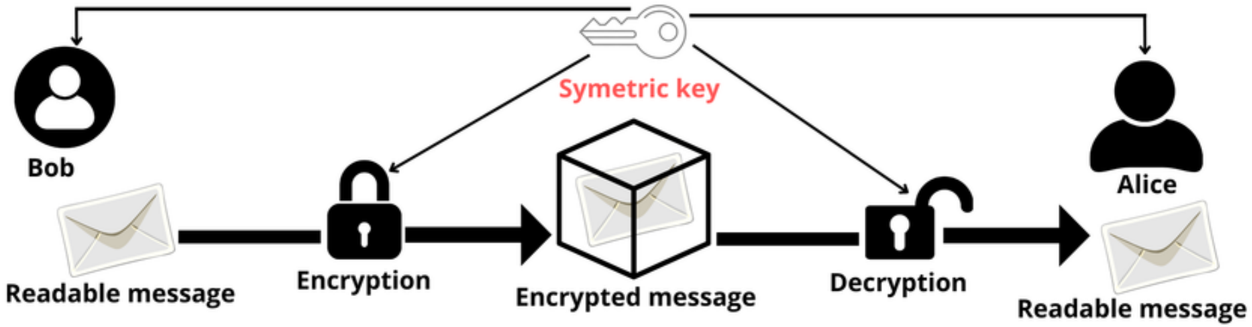
Secret key

Nội dung Chương 2: Mã hóa đối xứng

1. Kỹ thuật mã cổ điển

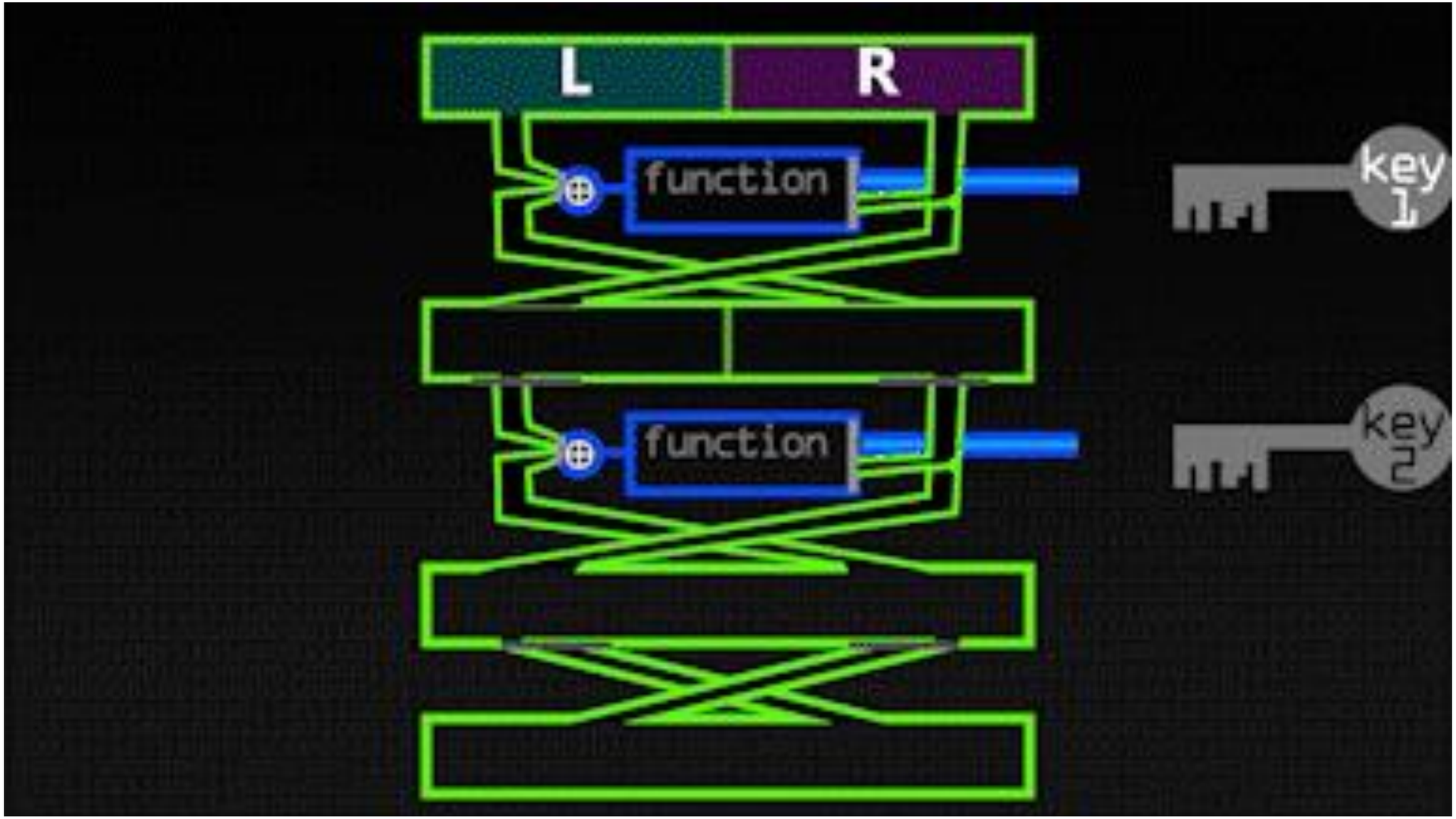
2. Mã khối DES

3. Mã khối AES



ÔN TẬP

Mã khối Feistel

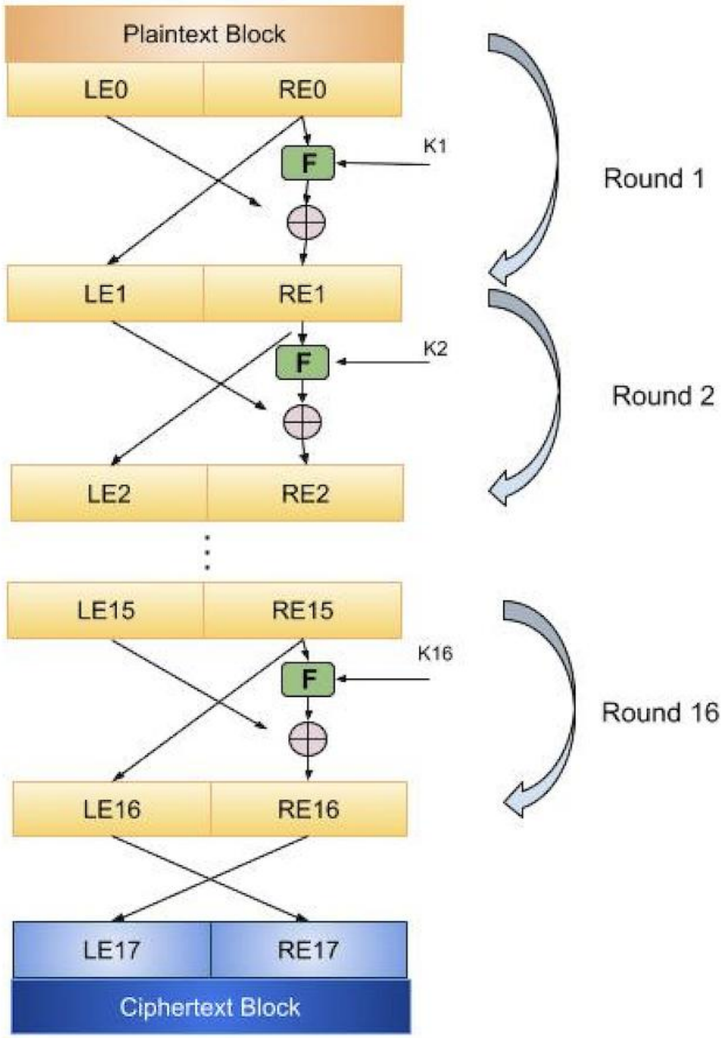


ĐẠI NAM
UNIVERSITY

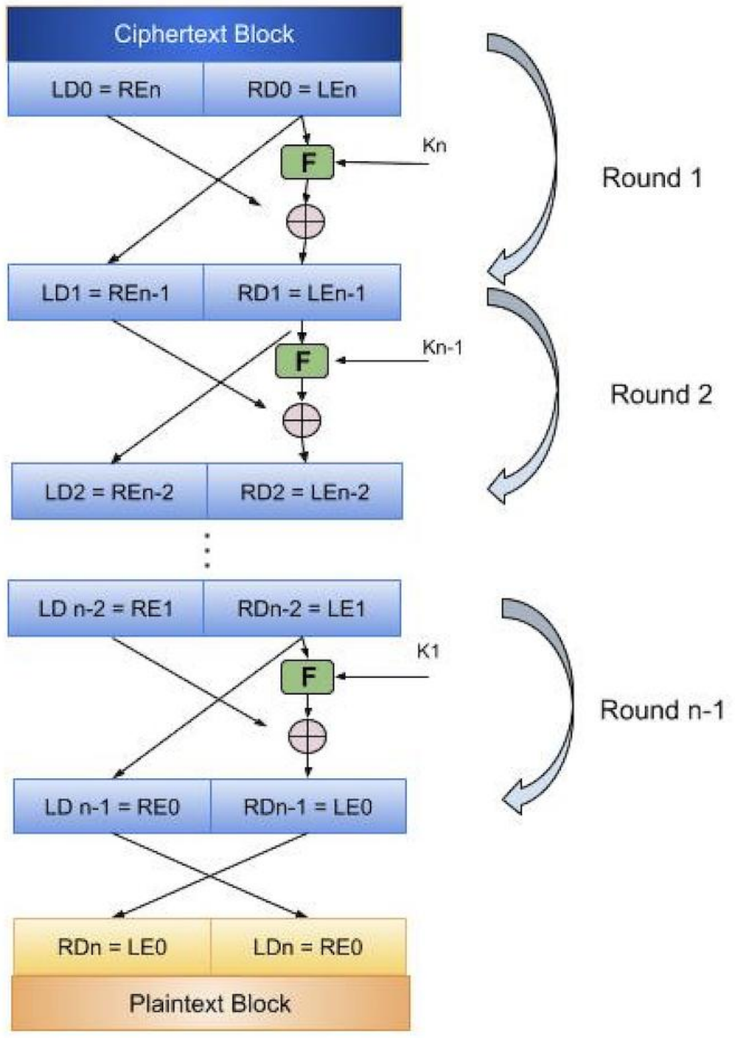
Bài 5

DES và Triple DES

Giới Thiệu Chung về DES (Data Encryption Standard)



Mã khối Feistel



Nội dung DES

1. Giới thiệu

2. Thuật toán DES

3. Thuật toán Triple DES

4. Luyện tập

Giới thiệu

Thuật toán mã DES (Data Encryption Standard):

- **Là một phương pháp mã khối, đối xứng, được phát triển vào đầu năm 1970**
- **IBM và được Cơ quan An ninh Quốc gia Mỹ (NSA) sửa đổi và công nhận là tiêu chuẩn mã hóa dữ liệu vào năm 1977.**

Giới thiệu

Năm 2000:

- **DES không còn đủ mạnh để bảo vệ thông tin nhạy cảm**

=> AES (Advanced Encryption Standard).

DES là gì?

- DES là một thuật toán mã hóa khối, nó mã hóa dữ liệu theo từng khối có kích thước cố định (64-bit).

- DES sử dụng cấu trúc Feistel(16 round) mỗi vòng sử dụng một phiên bản của khóa mã hóa để thực hiện các phép toán trên dữ liệu.

THUẬT TOÁN MÃ HÓA DES

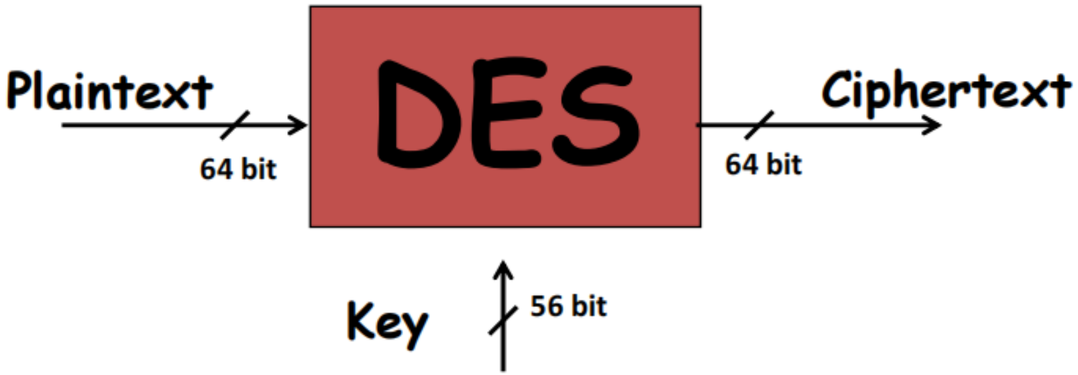
DES

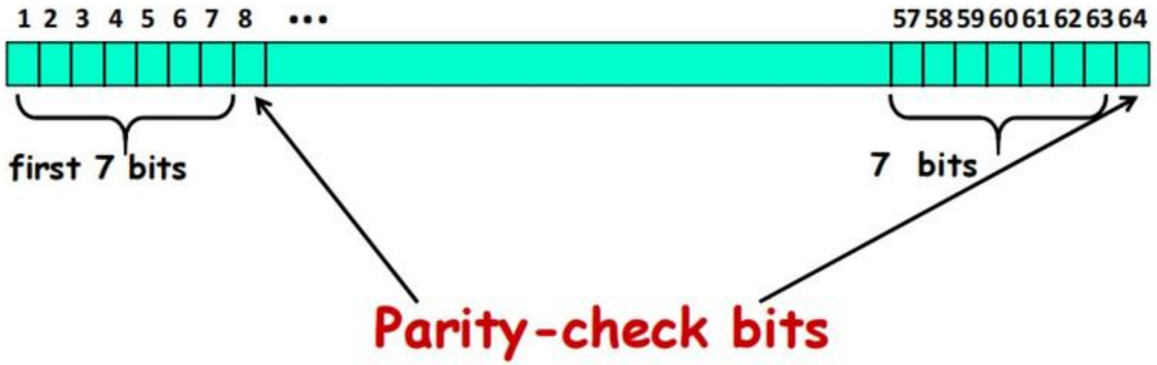
Demonstration

https://simewu.com/des/

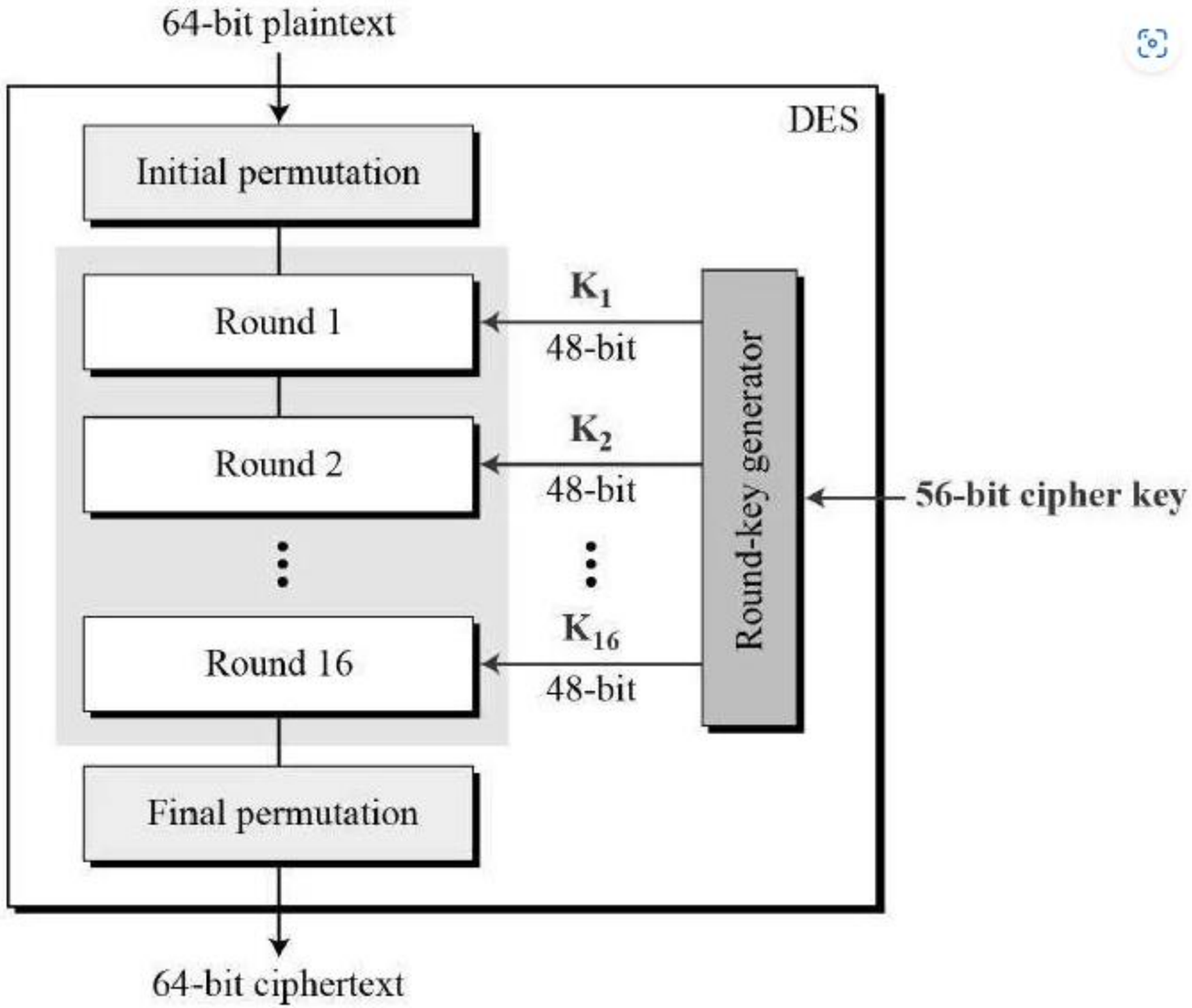
THUẬT TOÁN MÃ HÓA DES

- Block size = 64 bits
- Key size = 56 bits (64 bits, 8 are used as parity-check bits for error control)
- Number of rounds = 16





CÁC THÀNH PHẦN VÀ HOẠT ĐỘNG CỦA DES



- Kích thước mỗi khối là 64 bits, kích thước khóa là 56 bits
- Tương tự Feistel, DES sử dụng một hàm F chung trong khi mỗi round lại sử dụng một sub-key riêng (được sinh từ master key).

CÁC THÀNH PHẦN CỦA DES

- Hoán Vị Ban Đầu (Initial Permutation)
- 16 vòng lặp: Khóa, bảng S-box, hàm mở rộng (Expansion Function), P, Sinh khóa.
- Hoán vị cuối (Final Permutation)

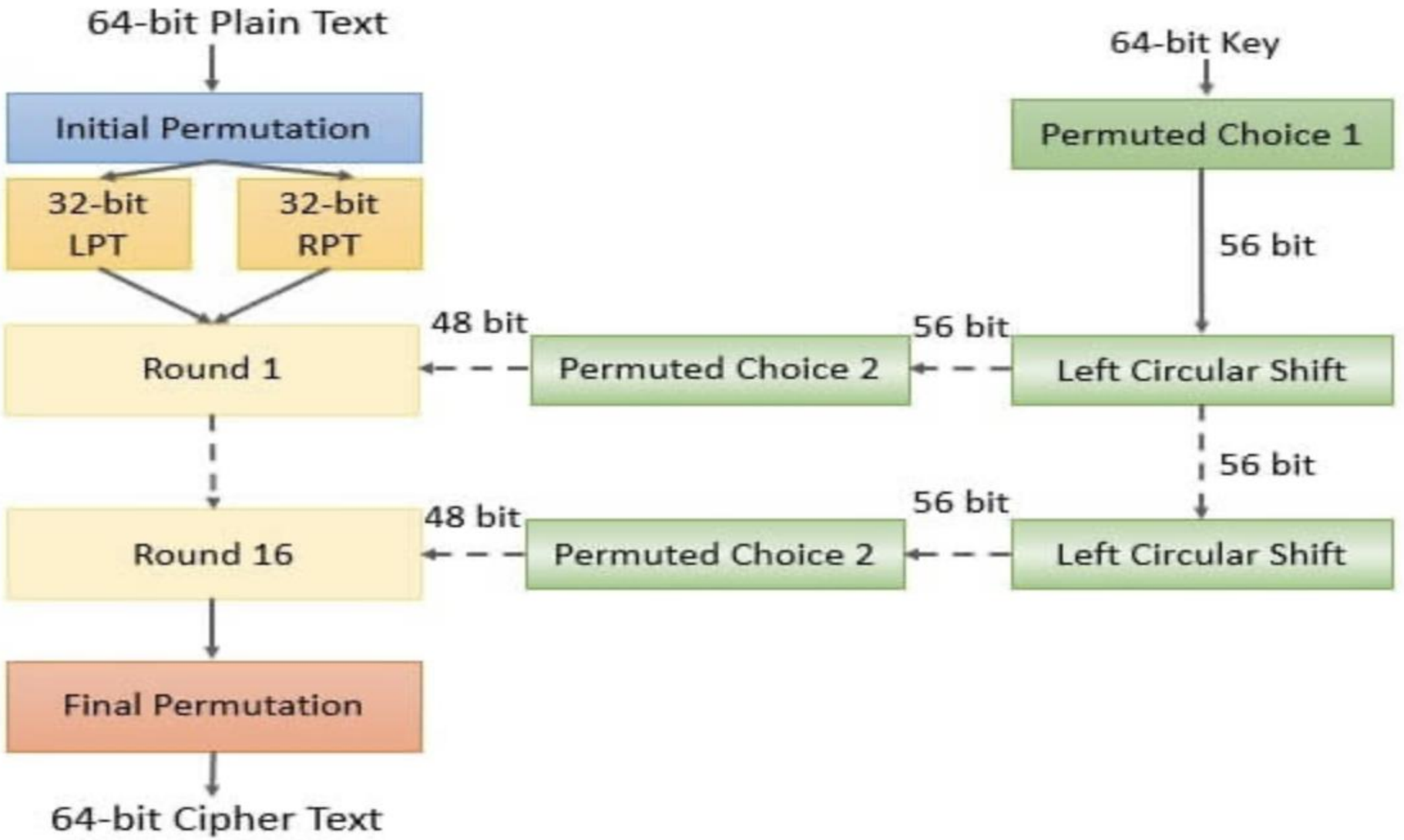
HOẠT ĐỘNG THUẬT TOÁN CỦA DES

B1: Đầu tiên, khối plaintext (64 bits) được đưa qua bước Initial permutation để thực hiện hoán vị các bit data (Quy tắc hoán vị được định nghĩa trong một bảng gọi là Inital permutaion table).

B2: Sau đó, cho khối chạy 16 rounds để mã hóa, các bước chạy giống như Feistel đã trình bày ở trên.

B3: Cuối cùng, thực hiện bước Final permutation để thu ciphertext (bước này thực chất là đảo ngược của quá trình Initial permutation).

HOẠT ĐỘNG CỦA THUẬT TOÁN DES

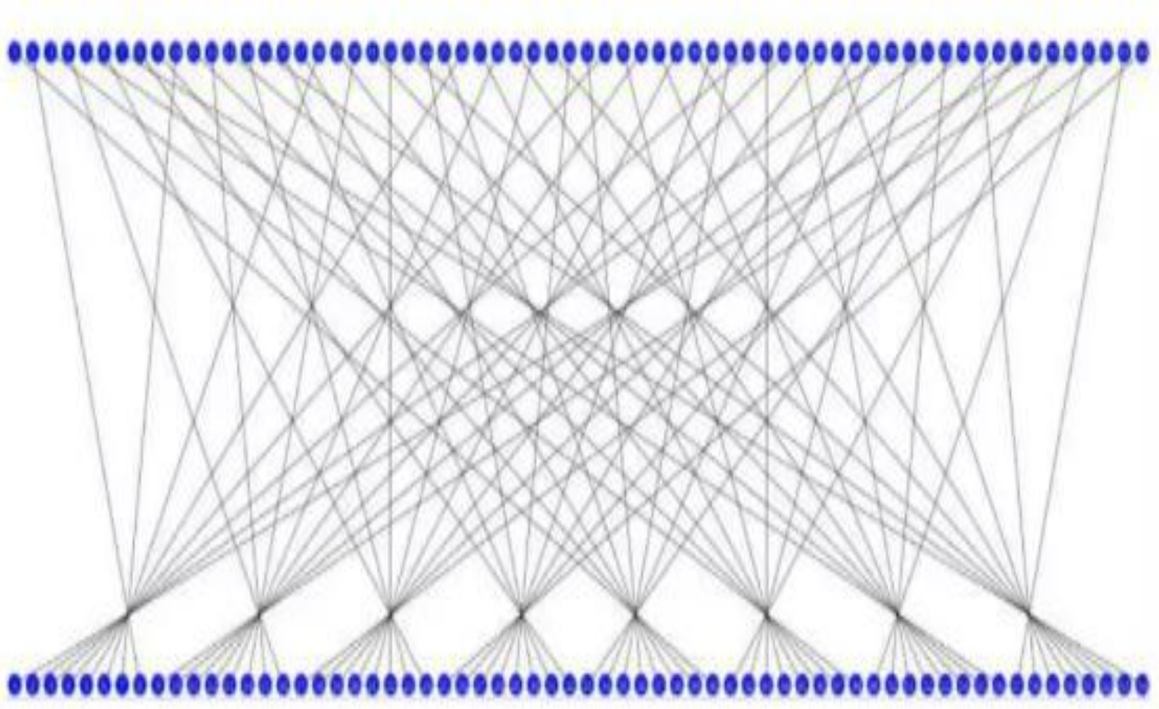


HOẠT ĐỘNG CỦA THUẬT TOÁN DES

Hoán vị khởi tạo (Initial Permutation) Block 64 bits

58	50	42	34	26	18	10	02
60	52	44	36	28	20	12	04
62	54	46	38	30	22	14	06
64	56	48	40	32	24	16	08
57	49	41	33	25	17	09	01
59	51	43	35	27	19	11	03
61	53	45	37	29	21	13	05
63	55	47	39	31	23	15	07

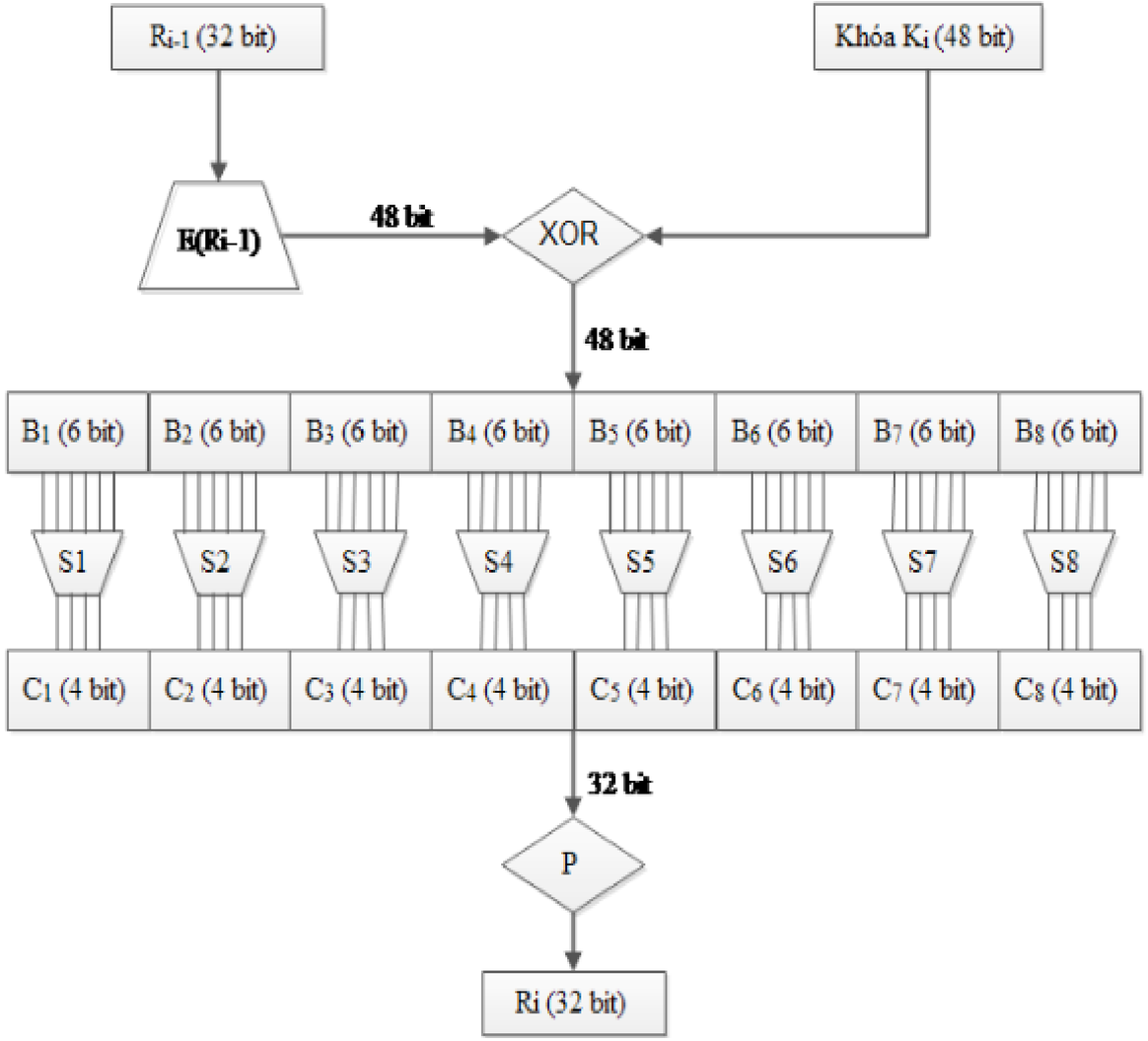
Initial Permutation Table



HOẠT ĐỘNG CỦA THUẬT TOÁN DES

Hàm sinh khóa f(•):

- Hoán vị mở rộng E (Expansion Permuatation): 32 bit -> 48 bit
- Trộn khoá ⊕ (Key mixing): Áp dụng phép XOR dữ liệu với khoá con
- Thay thế S-box (Substitution S1, S2, ..., S8): 48 bit -> 32 bit
- Hoán vị P (Permutation): sắp xếp lại 32 bit
- XOR với Left



SINGLE ROUND OF DES

Hoán vị mở rộng E

- Mở rộng 32 bit thành 48 bit để phù hợp với kích thước của khoá con
- 32 bit đầu vào được chia thành 8 khối 4 bit
- Mỗi khối 4 bit được mở rộng thành 6 bit bằng cách lấy thêm 2 bit từ các khối liền kề

32	01	02	03	04	05
04	05	06	07	08	09
08	09	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	01

E

Thay thế S-box

	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	4	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

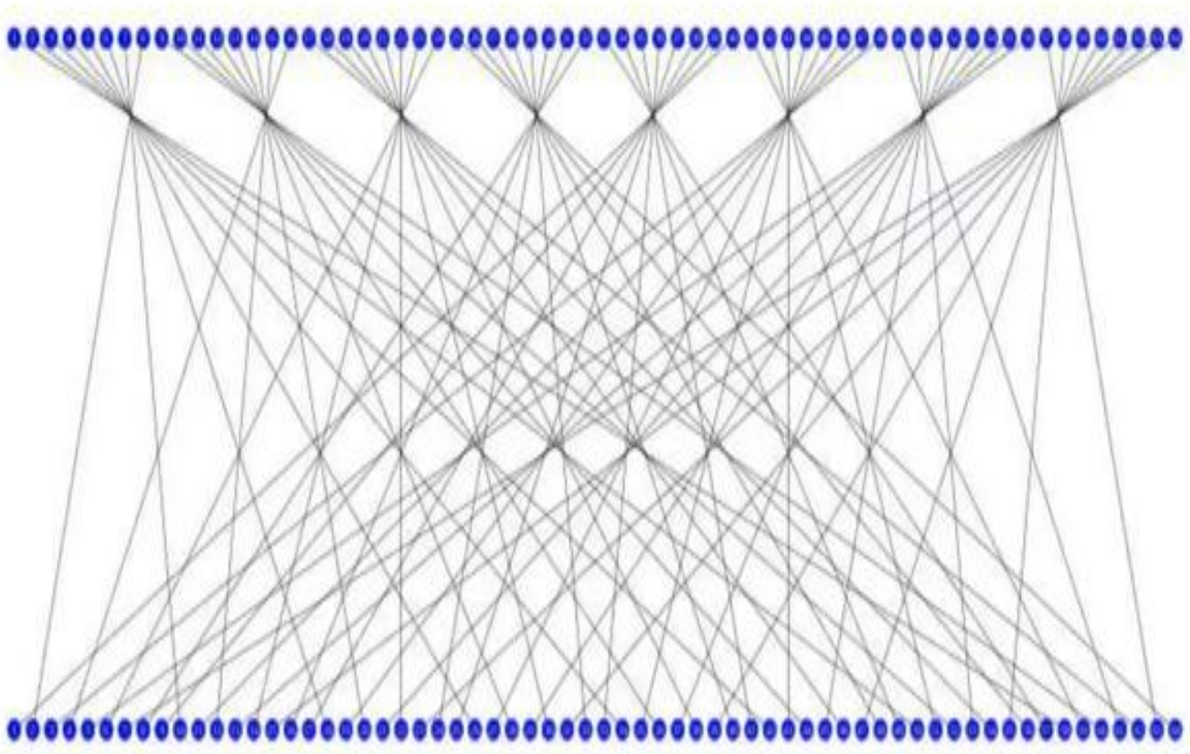
S_8

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

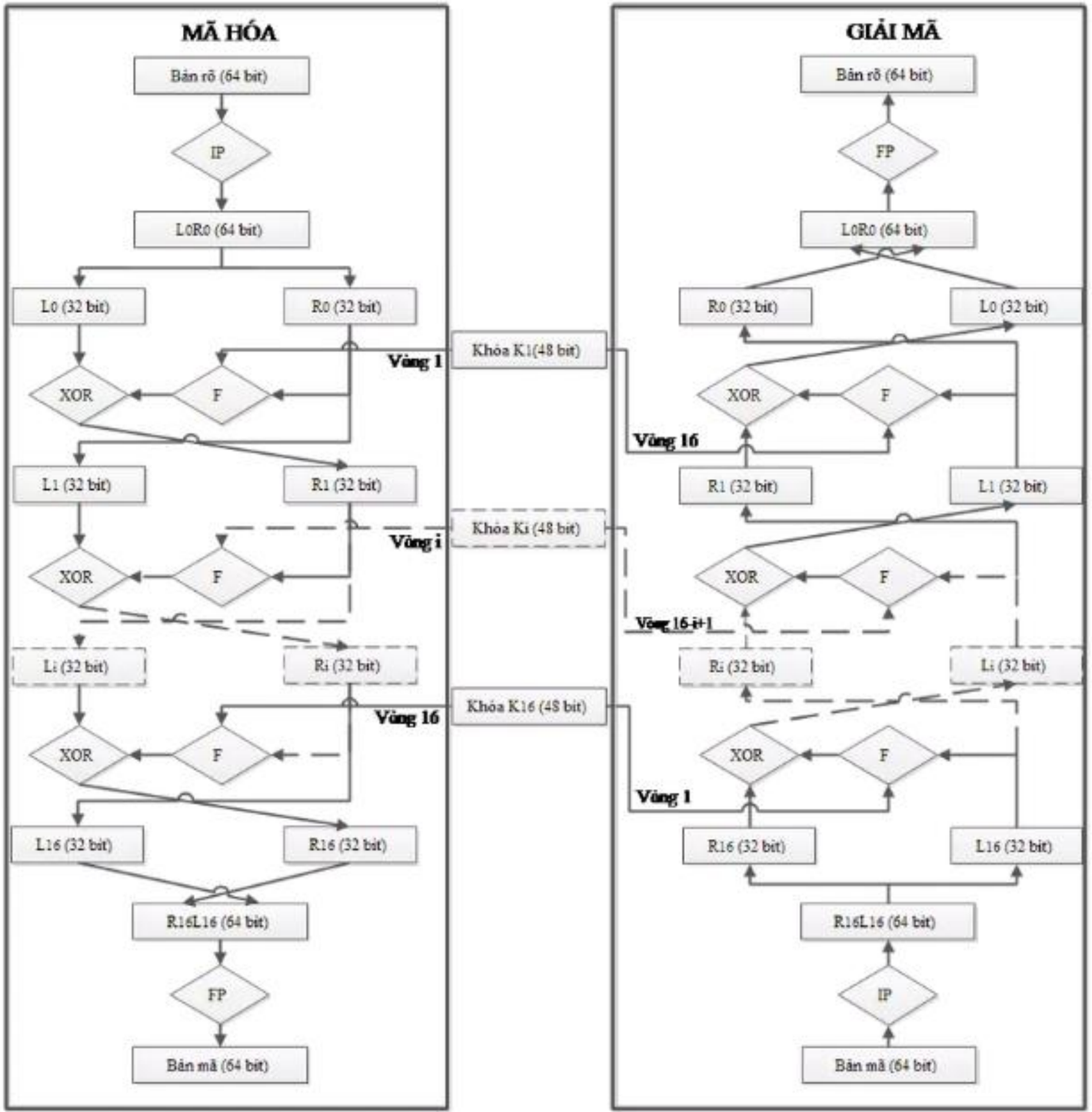
Hoán vị kết thúc (Final Permutation)

$$\mathbf{FP} = \mathbf{IP}^{-1}$$

40	08	48	16	56	24	64	32
39	07	47	15	55	23	63	31
38	06	46	14	54	22	62	30
37	05	45	13	53	21	61	29
36	04	44	12	52	20	60	28
35	03	43	11	51	19	59	27
34	02	42	10	50	18	58	26
33	01	41	09	49	17	57	25



Giải mã


MÃ HÓA
Bản rõ (64 bit)
IP
L0R0 (64 bit)
L0 (32 bit)
R0 (32 bit)
Vòng 1
XOR
F
L1 (32 bit)
R1 (32 bit)
Khóa K1(48 bit)
Vòng i
Khóa Ki (48 bit)
Li (32 bit)
Ri (32 bit)
Vòng 16
Khóa K16 (48 bit)
L16 (32 bit)
R16 (32 bit)
R16L16 (64 bit)
FP
Bản mã (64 bit)
GIẢI MÃ
Bản rõ (64 bit)
FP
L0R0 (64 bit)
R0 (32 bit)
L0 (32 bit)
Vòng 16
R1 (32 bit)
L1 (32 bit)
Vòng 16-i+1
Ri (32 bit)
Li (32 bit)
Vòng 1
R16 (32 bit)
L16 (32 bit)
R16L16 (64 bit)
IP
Bản mã (64 bit)

ĐÁNH GIÁ THUẬT TOÁN

Attack Method	Known	Chosen	Storage Complexity	Processing Complexity
Exhaustive precomputation	-	1	2^{56}	1
Exhaustive search	1	-	Negligible	2^{55}
Linear cryptanalysis	2^{43} 2^{38}	- -	For texts	2^{43} 2^{50}
Differential cryptanalysis	- 2^{55}	2^{47} -	For texts	2^{47} 2^{55}

The weakest point of DES remains the size of the key (56 bits)!

ĐÁNH GIÁ THUẬT TOÁN

Key Size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 Decryptions/s	Time Required at 10^{13} Decryptions/s
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	2^{55} ns = 1.125 years	1 hour
128	AES	$2^{128} \approx 3.4 \times 10^{38}$	2^{127} ns = 5.3×10^{21} years	5.3×10^{17} years
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	2^{167} ns = 5.8×10^{33} years	5.8×10^{29} years
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	2^{191} ns = 9.8×10^{40} years	9.8×10^{36} years
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	2^{255} ns = 1.8×10^{60} years	1.8×10^{56} years
26 characters (permutation)	Monoalphabetic	$2! = 4 \times 10^{26}$	2×10^{26} ns = 6.3×10^{9} years	6.3×10^{6} years

ĐÁNH GIÁ THUẬT TOÁN

Timing Attacks

We discuss timing attacks in more detail in Part Three, as they relate to public-key algorithms. However, the issue may also be relevant for symmetric ciphers. In essence, a timing attack is one in which information about the key or the plaintext is obtained by observing how long it takes a given implementation to perform decryptions on various ciphertexts. A timing attack exploits the fact that an encryption or decryption algorithm often takes slightly different amounts of time on different inputs. [HEVI99] reports on an approach that yields the Hamming weight (number of bits equal to one) of the secret key. This is a long way from knowing the actual key, but it is an intriguing first step. The authors conclude that DES appears to be fairly resistant to a successful timing attack but suggest some avenues to explore. Although this is an interesting line of attack, it so far appears unlikely that this technique will ever be successful against DES or more powerful symmetric ciphers such as triple DES and AES.

TRIPLE DES

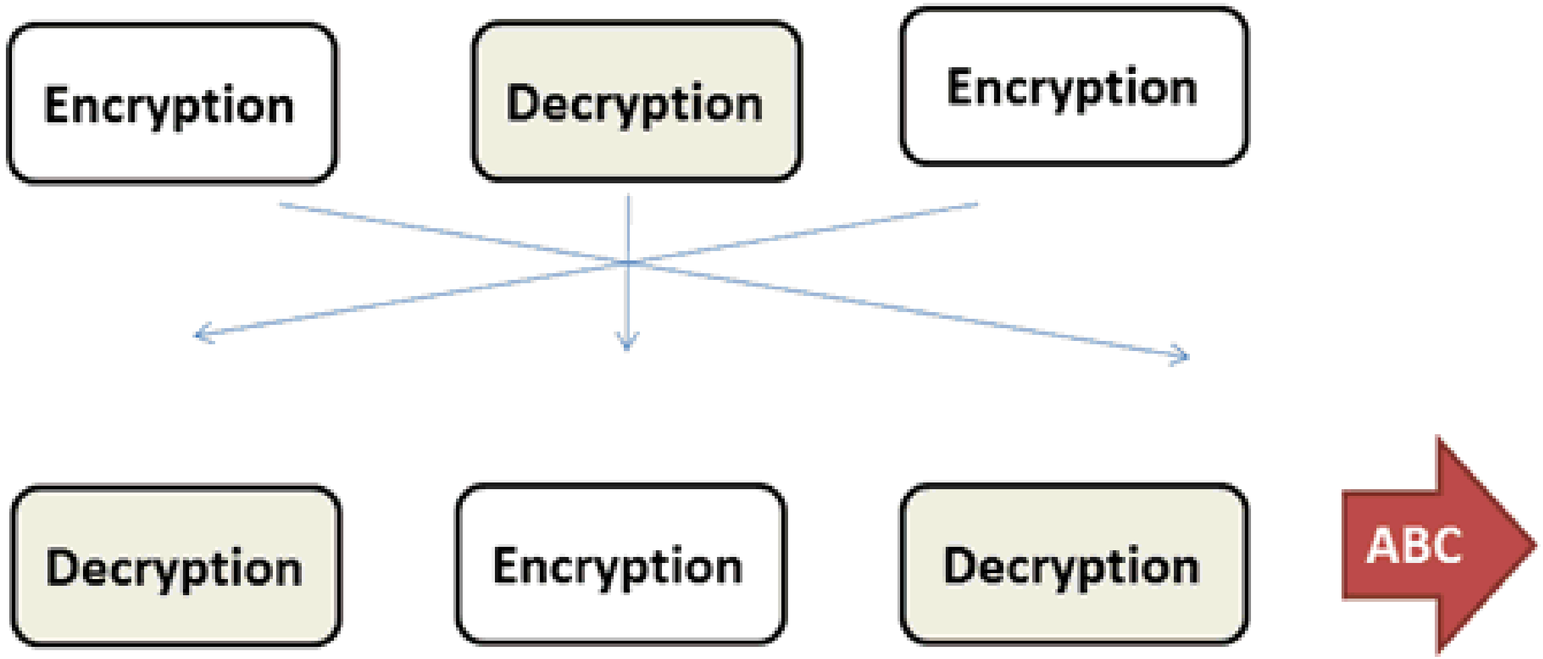
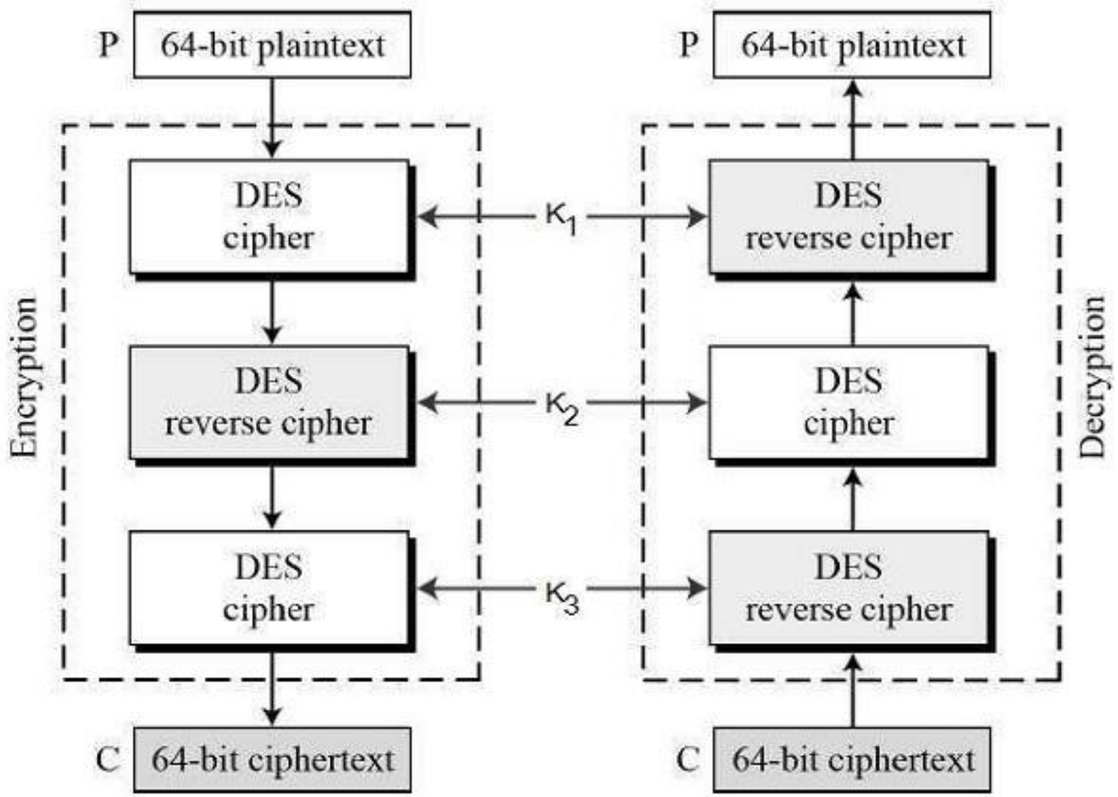


Fig : TripleDES Encryption

Các Biến Thể của DES

- Tổng quan về các biến thể (Triple DES).
- Mục đích và sự khác biệt so với DES gốc.
- Giới thiệu Triple DES: sử dụng ba khóa DES để cải thiện bảo mật.



- **Cơ chế**: Dữ liệu được mã hóa/giải mã qua 3 giai đoạn DES:
  - Mã hóa bằng khóa K1.
  - Giải mã bằng khóa K2.
  - Mã hóa lại bằng khóa K3.

$$C = E_{K3}(D_{K2}(E_{K1}(P)))$$

Khóa Key: Tổng cộng 168-bit (3 x 56-bit)

Tổng kết

- ✓ Cấu trúc của DES
- ✓ Hoạt động của DES
- ✓ Cơ chế sinh khóa
- ✓ Mở rộng với thuật toán Triple DES

ĐẠI NAM
UNIVERSITY

Thank You