NHÓM 1

BÀI TẬP MÃ HÓA DES

INPUT: K (là input bài 1) = 3FF81CDA5F417784;

M (là input bài 4) = FF1C9CA3596B7D48;

OUTPUT: Tìm C (kết quả bài 11) = C727541BBA49D95D

HÃY THỰC HIỆN CÁC BÀI TOÁN CHI TIẾT TỪ Bài 1 đến Bài 9, và Bài 11

(XEM THÊM YÊU CẦU PHẦN THỰC HÀNH)

PHẦN 1: SINH KHÓA Ki từ khóa K (input)

1. **Tính hoán vị PC1 đối với khóa K:**
   Input: K = (input) = , PC1 (xem tài liệu mục 3.2 DES)
   Output: C_0 = , D_0 =

2. **Tính các giá trị dịch vòng Ci, Di:**
   Input: C_0 = , D_0 = (kết quả bài 1), s_i (xem tài liệu mục 3.2 DES)
   Output: C_i = , D_i =

3. **Tính khóa K_i cho vòng lặp thứ i**
   Input: C_i = , D_i = (kết quả bài 2), **PC2** (xem tài liệu mục 3.2 DES)
   Output: **K_i** = .

PHẦN 2: MÃ HÓA

4. **Tính hoán vị IP đối với bản tin M**
   Input: M = (input) = , IP (xem tài liệu mục 3.2 DES)
   Output: L_0 = , R_0 =

   ========== CHI TIẾT VÒNG LẶP THỨ NHẤT ==========

5. **Tính hàm mở rộng nửa phải E[R_0]**
   Input: R_0 = (kết quả bài 4), E (xem tài liệu mục 3.2 DES)
   Output: ER_0 =

6. **Thực hiên XOR ER_0 với khóa K_1**
   Input: ER_0 (kết quả bài 5) , K_1 (kết quả bài 3)
   Output: A =

7. Thực hiện phép thế S-box đối với B
   Input: A (kết quả bài 6), 8 bảng S_i, i = 1, 2, ..., 8; (xem tài liệu mục 3.2 DES)
   Output: B = S(A) =

8. Thực hiện hoán vị P đối với SB
   Input: B (kết quả bài 7), P (xem tài liệu mục 3.2 DES)
   Output: F =
   ========= THỰC HIỆN VÒNG LẶP THỨ NHẤT ==========

9. Thực hiện vòng lặp thứ nhất
   Input: L_0 = ; R_0 = , (kết quả bài 4), F (kết quả bài 8)
   Output: $L_1 = R_0$ = ; $R_1 = L_0 \oplus F$ =
   ========= THỰC HIỆN VÒNG LẶP THỨ i, i = 2, 3, ..., 16 ==========

10. Thực hiện vòng lặp thứ i, i = 2, 3, ..., 16
    Input: L_{i-1} = ; R_{i-1} = , (kết quả bài 9 hoặc bài 10)
    Output: $L_i = R_{i-1}$ = ; $R_i = L_{i-1} \oplus f(R_{i-1},K_i)$ =
    ========= KẾT THÚC VÒNG LẶP THỨ 16 ==========

11. **Thực hiện hoán vị cuối cùng IP^{-1}**
    Input: L_{16} = ; R_{16} = , (kết quả bài 10); **IP^{-1}** (xem tài liệu mục 3.2 DES)
    Output: C = ;**(bản mã cần tìm)**
    ========== KẾT QUẢ MÃ HÓA ==========

NHÓM 2

BÀI TẬP MÃ HÓA DES

INPUT: K (là input bài 1) = 17FFCC5ADBF3EA87;

M (là input bài 4) = E36B4C92DE9AD726;

OUTPUT: Tìm C (kết quả bài 11) = 01A0C50A7FA4CF5A

HÃY THỰC HIỆN CÁC BÀI TOÁN CHI TIẾT TỪ Bài 1 đến Bài 9, và Bài 11

(XEM THÊM YÊU CẦU PHẦN THỰC HÀNH)

PHẦN 1: SINH KHÓA Ki từ khóa K (input)

1. **Tính hoán vị PC1 đối với khóa K:**
   Input: K = (input) = , PC1 (xem tài liệu mục 3.2 DES)
   Output: C_0 = , D_0 =

2. **Tính các giá trị dịch vòng Ci, Di:**
   Input: C_0 = , D_0 = (kết quả bài 1), s_i (xem tài liệu mục 3.2 DES)
   Output: C_i = , D_i =

3. **Tính khóa K_i cho vòng lặp thứ i**
   Input: C_i = , D_i = (kết quả bài 2), **PC2** (xem tài liệu mục 3.2 DES)
   Output: **K_i** = .

PHẦN 2: MÃ HÓA

4. **Tính hoán vị IP đối với bản tin M**
   Input: M = (input) = , IP (xem tài liệu mục 3.2 DES)
   Output: L_0 = , R_0 =

   ========== CHI TIẾT VÒNG LẶP THỨ NHẤT ==========

5. **Tính hàm mở rộng nửa phải E[R_0]**
   Input: R_0 = (kết quả bài 4), E (xem tài liệu mục 3.2 DES)
   Output: ER_0 =

6. **Thực hiên XOR ER_0 với khóa K_1**
   Input: ER_0 (kết quả bài 5) , K_1 (kết quả bài 3)
   Output: A =

7. Thực hiện phép thế S-box đối với B
   Input: A (kết quả bài 6), 8 bảng S_i, i = 1, 2, ..., 8; (xem tài liệu mục 3.2 DES)
   Output: B = S(A) =

8. Thực hiện hoán vị P đối với SB
   Input: B (kết quả bài 7), P (xem tài liệu mục 3.2 DES)
   Output: F =
   ========= THỰC HIỆN VÒNG LẶP THỨ NHẤT ==========
9. Thực hiện vòng lặp thứ nhất
   Input: L_0 = ; R_0 = , (kết quả bài 4), F (kết quả bài 8)
   Output: $L_1 = R_0$ = ; $R_1 = L_0 \oplus F$ =
   ========= THỰC HIỆN VÒNG LẶP THỨ i, i = 2, 3, ..., 16 ==========
10. Thực hiện vòng lặp thứ i, i = 2, 3, ..., 16
    Input: L_{i-1} = ; R_{i-1} = , (kết quả bài 9 hoặc bài 10)
    Output: $L_i = R_{i-1}$ = ; $R_i = L_{i-1} \oplus f(R_{i-1},K_i)$ =
    ========= KẾT THÚC VÒNG LẶP THỨ 16 ==========
11. **Thực hiện hoán vị cuối cùng IP^{-1}**
    Input: L_{16} = ; R_{16} = , (kết quả bài 10); **IP^{-1}** (xem tài liệu mục 3.2 DES)
    Output: C = ;**(bản mã cần tìm)**
    ========== KẾT QUẢ MÃ HÓA ==========

NHÓM 3

BÀI TẬP MÃ HÓA DES

INPUT: K (là input bài 1) = B35F59255E3BCB54;

M (là input bài 4) = 32D604E6C4504149;

OUTPUT: Tìm C (kết quả bài 11) = 056546D954490960

HÃY THỰC HIỆN CÁC BÀI TOÁN CHI TIẾT TỪ Bài 1 đến Bài 9, và Bài 11

(XEM THÊM YÊU CẦU PHẦN THỰC HÀNH)

PHẦN 1: SINH KHÓA Ki từ khóa K (input)

1. **Tính hoán vị PC1 đối với khóa K:**
   Input: K = (input) = , PC1 (xem tài liệu mục 3.2 DES)
   Output: C_0 = , D_0 =

2. **Tính các giá trị dịch vòng Ci, Di:**
   Input: C_0 = , D_0 = (kết quả bài 1), s_i (xem tài liệu mục 3.2 DES)
   Output: C_i = , D_i =

3. **Tính khóa K_i cho vòng lặp thứ i**
   Input: C_i = , D_i = (kết quả bài 2), **PC2** (xem tài liệu mục 3.2 DES)
   Output: **K_i** = .

PHẦN 2: MÃ HÓA

4. **Tính hoán vị IP đối với bản tin M**
   Input: M = (input) = , IP (xem tài liệu mục 3.2 DES)
   Output: L_0 = , R_0 =

   ========== CHI TIẾT VÒNG LẶP THỨ NHẤT ==========

5. **Tính hàm mở rộng nửa phải E[R_0]**
   Input: R_0 = (kết quả bài 4), E (xem tài liệu mục 3.2 DES)
   Output: ER_0 =

6. **Thực hiên XOR ER_0 với khóa K_1**
   Input: ER_0 (kết quả bài 5) , K_1 (kết quả bài 3)
   Output: A =

7. Thực hiện phép thế S-box đối với B
   Input: A (kết quả bài 6), 8 bảng S_i, i = 1, 2, ..., 8; (xem tài liệu mục 3.2 DES)
   Output: B = S(A) =

8. Thực hiện hoán vị P đối với SB
   Input: B (kết quả bài 7), P (xem tài liệu mục 3.2 DES)
   Output: F =
   ========= THỰC HIỆN VÒNG LẶP THỨ NHẤT ==========
9. Thực hiện vòng lặp thứ nhất
   Input: L_0 = ; R_0 = , (kết quả bài 4), F (kết quả bài 8)
   Output: $L_1 = R_0$ = ; $R_1 = L_0 \oplus F$ =
   ========= THỰC HIỆN VÒNG LẶP THỨ i, i = 2, 3, ..., 16 ==========
10. Thực hiện vòng lặp thứ i, i = 2, 3, ..., 16
    Input: L_{i-1} = ; R_{i-1} = , (kết quả bài 9 hoặc bài 10)
    Output: $L_i = R_{i-1}$ = ; $R_i = L_{i-1} \oplus f(R_{i-1},K_i)$ =
    ========= KẾT THÚC VÒNG LẶP THỨ 16 ==========
11. **Thực hiện hoán vị cuối cùng IP^{-1}**
    Input: L_{16} = ; R_{16} = , (kết quả bài 10); **IP^{-1}** (xem tài liệu mục 3.2 DES)
    Output: C = ;**(bản mã cần tìm)**
    ========== KẾT QUẢ MÃ HÓA ==========

NHÓM 4

BÀI TẬP MÃ HÓA DES

INPUT: K (là input bài 1) = F35D514714F45A8A;

M (là input bài 4) = 1EDE3CBCAF288822;

OUTPUT: Tìm C (kết quả bài 11) = C9465DCEBC57ECE6

HÃY THỰC HIỆN CÁC BÀI TOÁN CHI TIẾT TỪ Bài 1 đến Bài 9, và Bài 11

(XEM THÊM YÊU CẦU PHẦN THỰC HÀNH)

PHẦN 1: SINH KHÓA Ki từ khóa K (input)

1. **Tính hoán vị PC1 đối với khóa K:**
   Input: K = (input) = , PC1 (xem tài liệu mục 3.2 DES)
   Output: C_0 = , D_0 =

2. **Tính các giá trị dịch vòng Ci, Di:**
   Input: C_0 = , D_0 = (kết quả bài 1), s_i (xem tài liệu mục 3.2 DES)
   Output: C_i = , D_i =

3. **Tính khóa K_i cho vòng lặp thứ i**
   Input: C_i = , D_i = (kết quả bài 2), **PC2** (xem tài liệu mục 3.2 DES)
   Output: **K_i** = .

PHẦN 2: MÃ HÓA

4. **Tính hoán vị IP đối với bản tin M**
   Input: M = (input) = , IP (xem tài liệu mục 3.2 DES)
   Output: L_0 = , R_0 =

   ========== CHI TIẾT VÒNG LẶP THỨ NHẤT ==========

5. **Tính hàm mở rộng nửa phải E[R_0]**
   Input: R_0 = (kết quả bài 4), E (xem tài liệu mục 3.2 DES)
   Output: ER_0 =

6. **Thực hiên XOR ER_0 với khóa K_1**
   Input: ER_0 (kết quả bài 5) , K_1 (kết quả bài 3)
   Output: A =

7. Thực hiện phép thế S-box đối với B
   Input: A (kết quả bài 6), 8 bảng S_i, i = 1, 2, ..., 8; (xem tài liệu mục 3.2 DES)
   Output: B = S(A) =

8. Thực hiện hoán vị P đối với SB
   Input: B (kết quả bài 7), P (xem tài liệu mục 3.2 DES)
   Output: F =
   ========= THỰC HIỆN VÒNG LẶP THỨ NHẤT ==========

9. Thực hiện vòng lặp thứ nhất
   Input: L_0 = ; R_0 = , (kết quả bài 4), F (kết quả bài 8)
   Output: $L_1 = R_0$ = ; $R_1 = L_0 \oplus F$ =
   ========= THỰC HIỆN VÒNG LẶP THỨ i, i = 2, 3, ..., 16 ==========

10. Thực hiện vòng lặp thứ i, i = 2, 3, ..., 16
    Input: L_{i-1} = ; R_{i-1} = , (kết quả bài 9 hoặc bài 10)
    Output: $L_i = R_{i-1}$ = ; $R_i = L_{i-1} \oplus f(R_{i-1},K_i)$ =
    ========= KẾT THÚC VÒNG LẶP THỨ 16 ==========

11. **Thực hiện hoán vị cuối cùng IP^{-1}**
    Input: L_{16} = ; R_{16} = , (kết quả bài 10); **IP^{-1}** (xem tài liệu mục 3.2 DES)
    Output: C = ;**(bản mã cần tìm)**
    ========== KẾT QUẢ MÃ HÓA ==========

NHÓM 5

BÀI TẬP MÃ HÓA DES

INPUT: K (là input bài 1) = F7918DFD6815020C;

M (là input bài 4) = D8B8217DA16D5B5F;

OUTPUT: Tìm C (kết quả bài 11) = BD9B0A1452DC4028

HÃY THỰC HIỆN CÁC BÀI TOÁN CHI TIẾT TỪ Bài 1 đến Bài 9, và Bài 11

(XEM THÊM YÊU CẦU PHẦN THỰC HÀNH)

PHẦN 1: SINH KHÓA Ki từ khóa K (input)

1. **Tính hoán vị PC1 đối với khóa K:**
   Input: K = (input) = , PC1 (xem tài liệu mục 3.2 DES)
   Output: C_0 = , D_0 =

2. **Tính các giá trị dịch vòng Ci, Di:**
   Input: C_0 = , D_0 = (kết quả bài 1), s_i (xem tài liệu mục 3.2 DES)
   Output: C_i = , D_i =

3. **Tính khóa K_i cho vòng lặp thứ i**
   Input: C_i = , D_i = (kết quả bài 2), **PC2** (xem tài liệu mục 3.2 DES)
   Output: K_i = .

PHẦN 2: MÃ HÓA

4. **Tính hoán vị IP đối với bản tin M**
   Input: M = (input) = , IP (xem tài liệu mục 3.2 DES)
   Output: L_0 = , R_0 =

   ========== CHI TIẾT VÒNG LẶP THỨ NHẤT ==========

5. **Tính hàm mở rộng nửa phải E[R_0]**
   Input: R_0 = (kết quả bài 4), E (xem tài liệu mục 3.2 DES)
   Output: ER_0 =

6. **Thực hiên XOR ER_0 với khóa K_1**
   Input: ER_0 (kết quả bài 5) , K_1 (kết quả bài 3)
   Output: A =

7. Thực hiện phép thế S-box đối với B
   Input: A (kết quả bài 6), 8 bảng S_i, i = 1, 2, ..., 8; (xem tài liệu mục 3.2 DES)
   Output: B = S(A) =

8. Thực hiện hoán vị P đối với SB
   Input: B (kết quả bài 7), P (xem tài liệu mục 3.2 DES)
   Output: F =
   ========= THỰC HIỆN VÒNG LẶP THỨ NHẤT ==========

9. Thực hiện vòng lặp thứ nhất
   Input: L_0 = ; R_0 = , (kết quả bài 4), F (kết quả bài 8)
   Output: $L_1 = R_0$ = ; $R_1 = L_0 \oplus F$ =
   ========= THỰC HIỆN VÒNG LẶP THỨ i, i = 2, 3, ..., 16 ==========

10. Thực hiện vòng lặp thứ i, i = 2, 3, ..., 16
    Input: L_{i-1} = ; R_{i-1} = , (kết quả bài 9 hoặc bài 10)
    Output: $L_i = R_{i-1}$ = ; $R_i = L_{i-1} \oplus f(R_{i-1},K_i)$ =
    ========= KẾT THÚC VÒNG LẶP THỨ 16 ==========

11. **Thực hiện hoán vị cuối cùng IP^{-1}**
    Input: L_{16} = ; R_{16} = , (kết quả bài 10); **IP^{-1}** (xem tài liệu mục 3.2 DES)
    Output: C = ;**(bản mã cần tìm)**
    ========== KẾT QUẢ MÃ HÓA ==========

NHÓM 6

BÀI TẬP MÃ HÓA DES

INPUT: K (là input bài 1) = E35CB18E63EEED18;

M (là input bài 4) = B71127D233E316C3;

OUTPUT: Tìm C (kết quả bài 11) = 1E543DD140CBA51F

HÃY THỰC HIỆN CÁC BÀI TOÁN CHI TIẾT TỪ Bài 1 đến Bài 9, và Bài 11

(XEM THÊM YÊU CẦU PHẦN THỰC HÀNH)

PHẦN 1: SINH KHÓA Ki từ khóa K (input)

1. **Tính hoán vị PC1 đối với khóa K:**
   Input: K = (input) = , PC1 (xem tài liệu mục 3.2 DES)
   Output: C_0 = , D_0 =

2. **Tính các giá trị dịch vòng Ci, Di:**
   Input: C_0 = , D_0 = (kết quả bài 1), s_i (xem tài liệu mục 3.2 DES)
   Output: C_i = , D_i =

3. **Tính khóa K_i cho vòng lặp thứ i**
   Input: C_i = , D_i = (kết quả bài 2), **PC2** (xem tài liệu mục 3.2 DES)
   Output: **K_i** = .

PHẦN 2: MÃ HÓA

4. **Tính hoán vị IP đối với bản tin M**
   Input: M = (input) = , IP (xem tài liệu mục 3.2 DES)
   Output: L_0 = , R_0 =

   ========== CHI TIẾT VÒNG LẶP THỨ NHẤT ==========

5. **Tính hàm mở rộng nửa phải E[R_0]**
   Input: R_0 = (kết quả bài 4), E (xem tài liệu mục 3.2 DES)
   Output: ER_0 =

6. **Thực hiên XOR ER_0 với khóa K_1**
   Input: ER_0 (kết quả bài 5) , K_1 (kết quả bài 3)
   Output: A =

7. Thực hiện phép thế S-box đối với B
   Input: A (kết quả bài 6), 8 bảng S_i, i = 1, 2, ..., 8; (xem tài liệu mục 3.2 DES)
   Output: B = S(A) =

8. Thực hiện hoán vị P đối với SB
   Input: B (kết quả bài 7), P (xem tài liệu mục 3.2 DES)
   Output: F =
   ========= THỰC HIỆN VÒNG LẶP THỨ NHẤT ==========
9. Thực hiện vòng lặp thứ nhất
   Input: L_0 = ; R_0 = , (kết quả bài 4), F (kết quả bài 8)
   Output: $L_1 = R_0$ = ; $R_1 = L_0 \oplus F$ =
   ========= THỰC HIỆN VÒNG LẶP THỨ i, i = 2, 3, ..., 16 ==========
10. Thực hiện vòng lặp thứ i, i = 2, 3, ..., 16
    Input: L_{i-1} = ; R_{i-1} = , (kết quả bài 9 hoặc bài 10)
    Output: $L_i = R_{i-1}$ = ; $R_i = L_{i-1} \oplus f(R_{i-1},K_i)$ =
    ========= KẾT THÚC VÒNG LẶP THỨ 16 ==========
11. **Thực hiện hoán vị cuối cùng IP^{-1}**
    Input: L_{16} = ; R_{16} = , (kết quả bài 10); **IP^{-1}** (xem tài liệu mục 3.2 DES)
    Output: C = ;**(bản mã cần tìm)**
    ========== KẾT QUẢ MÃ HÓA ==========

NHÓM 7

BÀI TẬP MÃ HÓA DES

INPUT: K (là input bài 1) = F90C3770C45B6CD9;

M (là input bài 4) = 25EA45B3FBFBAE3E;

OUTPUT: Tìm C (kết quả bài 11) = B8AF288D923F3974

HÃY THỰC HIỆN CÁC BÀI TOÁN CHI TIẾT TỪ Bài 1 đến Bài 9, và Bài 11

(XEM THÊM YÊU CẦU PHẦN THỰC HÀNH)

PHẦN 1: SINH KHÓA Ki từ khóa K (input)

1. **Tính hoán vị PC1 đối với khóa K:**
   Input: K = (input) = , PC1 (xem tài liệu mục 3.2 DES)
   Output: C_0 = , D_0 =

2. **Tính các giá trị dịch vòng Ci, Di:**
   Input: C_0 = , D_0 = (kết quả bài 1), s_i (xem tài liệu mục 3.2 DES)
   Output: C_i = , D_i =

3. **Tính khóa K_i cho vòng lặp thứ i**
   Input: C_i = , D_i = (kết quả bài 2), **PC2** (xem tài liệu mục 3.2 DES)
   Output: **K_i** = .

PHẦN 2: MÃ HÓA

4. **Tính hoán vị IP đối với bản tin M**
   Input: M = (input) = , IP (xem tài liệu mục 3.2 DES)
   Output: L_0 = , R_0 =

   ========== CHI TIẾT VÒNG LẶP THỨ NHẤT ==========

5. **Tính hàm mở rộng nửa phải E[R_0]**
   Input: R_0 = (kết quả bài 4), E (xem tài liệu mục 3.2 DES)
   Output: ER_0 =

6. **Thực hiên XOR ER_0 với khóa K_1**
   Input: ER_0 (kết quả bài 5) , K_1 (kết quả bài 3)
   Output: A =

7. Thực hiện phép thế S-box đối với B
   Input: A (kết quả bài 6), 8 bảng S_i, i = 1, 2, ..., 8; (xem tài liệu mục 3.2 DES)
   Output: B = S(A) =

8. Thực hiện hoán vị P đối với SB
   Input: B (kết quả bài 7), P (xem tài liệu mục 3.2 DES)
   Output: F =
   ========= THỰC HIỆN VÒNG LẶP THỨ NHẤT ==========
9. Thực hiện vòng lặp thứ nhất
   Input: L_0 = ; R_0 = , (kết quả bài 4), F (kết quả bài 8)
   Output: $L_1 = R_0$ = ; $R_1 = L_0 \oplus F$ =
   ========= THỰC HIỆN VÒNG LẶP THỨ i, i = 2, 3, ..., 16 ==========
10. Thực hiện vòng lặp thứ i, i = 2, 3, ..., 16
    Input: L_{i-1} = ; R_{i-1} = , (kết quả bài 9 hoặc bài 10)
    Output: $L_i = R_{i-1}$ = ; $R_i = L_{i-1} \oplus f(R_{i-1},K_i)$ =
    ========= KẾT THÚC VÒNG LẶP THỨ 16 ==========
11. **Thực hiện hoán vị cuối cùng IP^{-1}**
    Input: L_{16} = ; R_{16} = , (kết quả bài 10); **IP^{-1}** (xem tài liệu mục 3.2 DES)
    Output: C = ;**(bản mã cần tìm)**
    ========== KẾT QUẢ MÃ HÓA ==========

NHÓM 8

BÀI TẬP MÃ HÓA DES

INPUT: K (là input bài 1) = 3513784465A003DD;

M (là input bài 4) = 950FB522A6E2B1DB;

OUTPUT: Tìm C (kết quả bài 11) = E884DE129C8D5B25

HÃY THỰC HIỆN CÁC BÀI TOÁN CHI TIẾT TỪ Bài 1 đến Bài 9, và Bài 11

(XEM THÊM YÊU CẦU PHẦN THỰC HÀNH)

PHẦN 1: SINH KHÓA Ki từ khóa K (input)

1. **Tính hoán vị PC1 đối với khóa K:**
   Input: K = (input) = , PC1 (xem tài liệu mục 3.2 DES)
   Output: C_0 = , D_0 =

2. **Tính các giá trị dịch vòng Ci, Di:**
   Input: C_0 = , D_0 = (kết quả bài 1), s_i (xem tài liệu mục 3.2 DES)
   Output: C_i = , D_i =

3. **Tính khóa K_i cho vòng lặp thứ i**
   Input: C_i = , D_i = (kết quả bài 2), **PC2** (xem tài liệu mục 3.2 DES)
   Output: **K_i** = .

PHẦN 2: MÃ HÓA

4. **Tính hoán vị IP đối với bản tin M**
   Input: M = (input) = , IP (xem tài liệu mục 3.2 DES)
   Output: L_0 = , R_0 =

   ========== CHI TIẾT VÒNG LẶP THỨ NHẤT ==========

5. **Tính hàm mở rộng nửa phải E[R_0]**
   Input: R_0 = (kết quả bài 4), E (xem tài liệu mục 3.2 DES)
   Output: ER_0 =

6. **Thực hiên XOR ER_0 với khóa K_1**
   Input: ER_0 (kết quả bài 5) , K_1 (kết quả bài 3)
   Output: A =

7. Thực hiện phép thế S-box đối với B
   Input: A (kết quả bài 6), 8 bảng S_i, i = 1, 2, ..., 8; (xem tài liệu mục 3.2 DES)
   Output: B = S(A) =

8. Thực hiện hoán vị P đối với SB
   Input: B (kết quả bài 7), P (xem tài liệu mục 3.2 DES)
   Output: F =
   ========= THỰC HIỆN VÒNG LẶP THỨ NHẤT ==========
9. Thực hiện vòng lặp thứ nhất
   Input: L_0 = ; R_0 = , (kết quả bài 4), F (kết quả bài 8)
   Output: $L_1 = R_0$ = ; $R_1 = L_0 \oplus F$ =
   ========= THỰC HIỆN VÒNG LẶP THỨ i, i = 2, 3, ..., 16 ==========
10. Thực hiện vòng lặp thứ i, i = 2, 3, ..., 16
    Input: L_{i-1} = ; R_{i-1} = , (kết quả bài 9 hoặc bài 10)
    Output: $L_i = R_{i-1}$ = ; $R_i = L_{i-1} \oplus f(R_{i-1},K_i)$ =
    ========= KẾT THÚC VÒNG LẶP THỨ 16 ==========
11. **Thực hiện hoán vị cuối cùng IP^{-1}**
    Input: L_{16} = ; R_{16} = , (kết quả bài 10); **IP^{-1}** (xem tài liệu mục 3.2 DES)
    Output: C = ;**(bản mã cần tìm)**
    ========== KẾT QUẢ MÃ HÓA ==========

NHÓM 9

BÀI TẬP MÃ HÓA DES

INPUT: K (là input bài 1) = 03756CD378146EC7;

M (là input bài 4) = 66581B2AE5B0BD6D;

OUTPUT: Tìm C (kết quả bài 11) = F20CA5AE288E3903

HÃY THỰC HIỆN CÁC BÀI TOÁN CHI TIẾT TỪ Bài 1 đến Bài 9, và Bài 11

(XEM THÊM YÊU CẦU PHẦN THỰC HÀNH)

PHẦN 1: SINH KHÓA Ki từ khóa K (input)

1. **Tính hoán vị PC1 đối với khóa K:**
   Input: K = (input) = , PC1 (xem tài liệu mục 3.2 DES)
   Output: C_0 = , D_0 =

2. **Tính các giá trị dịch vòng Ci, Di:**
   Input: C_0 = , D_0 = (kết quả bài 1), s_i (xem tài liệu mục 3.2 DES)
   Output: C_i = , D_i =

3. **Tính khóa K_i cho vòng lặp thứ i**
   Input: C_i = , D_i = (kết quả bài 2), **PC2** (xem tài liệu mục 3.2 DES)
   Output: **K_i** = .

PHẦN 2: MÃ HÓA

4. **Tính hoán vị IP đối với bản tin M**
   Input: M = (input) = , IP (xem tài liệu mục 3.2 DES)
   Output: L_0 = , R_0 =

   ========== CHI TIẾT VÒNG LẶP THỨ NHẤT ==========

5. **Tính hàm mở rộng nửa phải E[R_0]**
   Input: R_0 = (kết quả bài 4), E (xem tài liệu mục 3.2 DES)
   Output: ER_0 =

6. **Thực hiên XOR ER_0 với khóa K_1**
   Input: ER_0 (kết quả bài 5) , K_1 (kết quả bài 3)
   Output: A =

7. Thực hiện phép thế S-box đối với B
   Input: A (kết quả bài 6), 8 bảng S_i, i = 1, 2, ..., 8; (xem tài liệu mục 3.2 DES)
   Output: B = S(A) =

8. Thực hiện hoán vị P đối với SB
   Input: B (kết quả bài 7), P (xem tài liệu mục 3.2 DES)
   Output: F =
   ========= THỰC HIỆN VÒNG LẶP THỨ NHẤT ==========
9. Thực hiện vòng lặp thứ nhất
   Input: L_0 = ; R_0 = , (kết quả bài 4), F (kết quả bài 8)
   Output: $L_1 = R_0$ = ; $R_1 = L_0 \oplus F$ =
   ========= THỰC HIỆN VÒNG LẶP THỨ i, i = 2, 3, ..., 16 ==========
10. Thực hiện vòng lặp thứ i, i = 2, 3, ..., 16
    Input: L_{i-1} = ; R_{i-1} = , (kết quả bài 9 hoặc bài 10)
    Output: $L_i = R_{i-1}$ = ; $R_i = L_{i-1} \oplus f(R_{i-1},K_i)$ =
    ========= KẾT THÚC VÒNG LẶP THỨ 16 ==========
11. **Thực hiện hoán vị cuối cùng IP^{-1}**
    Input: L_{16} = ; R_{16} = , (kết quả bài 10); **IP^{-1}** (xem tài liệu mục 3.2 DES)
    Output: C = ;**(bản mã cần tìm)**
    ========== KẾT QUẢ MÃ HÓA ==========

NHÓM 10

BÀI TẬP MÃ HÓA DES

INPUT: K (là input bài 1) = 76934F95E9DF2ACA;

M (là input bài 4) = 81793427080B49CF;

OUTPUT: Tìm C (kết quả bài 11) = 3CBBDFB2686AABD6

HÃY THỰC HIỆN CÁC BÀI TOÁN CHI TIẾT TỪ Bài 1 đến Bài 9, và Bài 11

(XEM THÊM YÊU CẦU PHẦN THỰC HÀNH)

PHẦN 1: SINH KHÓA Ki từ khóa K (input)

1. **Tính hoán vị PC1 đối với khóa K:**
   Input: K = (input) = , PC1 (xem tài liệu mục 3.2 DES)
   Output: C_0 = , D_0 =

2. **Tính các giá trị dịch vòng Ci, Di:**
   Input: C_0 = , D_0 = (kết quả bài 1), s_i (xem tài liệu mục 3.2 DES)
   Output: C_i = , D_i =

3. **Tính khóa K_i cho vòng lặp thứ i**
   Input: C_i = , D_i = (kết quả bài 2), **PC2** (xem tài liệu mục 3.2 DES)
   Output: **K_i** = .

PHẦN 2: MÃ HÓA

4. **Tính hoán vị IP đối với bản tin M**
   Input: M = (input) = , IP (xem tài liệu mục 3.2 DES)
   Output: L_0 = , R_0 =

   ========== CHI TIẾT VÒNG LẶP THỨ NHẤT ==========

5. **Tính hàm mở rộng nửa phải E[R_0]**
   Input: R_0 = (kết quả bài 4), E (xem tài liệu mục 3.2 DES)
   Output: ER_0 =

6. **Thực hiên XOR ER_0 với khóa K_1**
   Input: ER_0 (kết quả bài 5) , K_1 (kết quả bài 3)
   Output: A =

7. Thực hiện phép thế S-box đối với B
   Input: A (kết quả bài 6), 8 bảng S_i, i = 1, 2, ..., 8; (xem tài liệu mục 3.2 DES)
   Output: B = S(A) =

8. Thực hiện hoán vị P đối với SB
   Input: B (kết quả bài 7), P (xem tài liệu mục 3.2 DES)
   Output: F =
   ========= THỰC HIỆN VÒNG LẶP THỨ NHẤT ==========
9. Thực hiện vòng lặp thứ nhất
   Input: L_0 = ; R_0 = , (kết quả bài 4), F (kết quả bài 8)
   Output: $L_1 = R_0$ = ; $R_1 = L_0 \oplus F$ =
   ========= THỰC HIỆN VÒNG LẶP THỨ i, i = 2, 3, ..., 16 ==========
10. Thực hiện vòng lặp thứ i, i = 2, 3, ..., 16
    Input: L_{i-1} = ; R_{i-1} = , (kết quả bài 9 hoặc bài 10)
    Output: $L_i = R_{i-1}$ = ; $R_i = L_{i-1} \oplus f(R_{i-1},K_i)$ =
    ========= KẾT THÚC VÒNG LẶP THỨ 16 ==========
11. **Thực hiện hoán vị cuối cùng IP^{-1}**
    Input: L_{16} = ; R_{16} = , (kết quả bài 10); **IP^{-1}** (xem tài liệu mục 3.2 DES)
    Output: C = ;**(bản mã cần tìm)**
    ========== KẾT QUẢ MÃ HÓA ==========