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

1. **Tính hoán vị PC1 đối với khóa K:**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 7 | 6 | 9 | 3 | 4 | F | 9 | 5 | E | 9 | D | F | 2 | A | C | A |
| 0111 | 0110 | 1001 | 0011 | 0100 | 1111 | 1001 | 0101 | 1110 | 1001 | 1101 | 1111 | 0010 | 1010 | 1100 | 1010 |

K = 0111 0110 1001 0011 0100 1111 1001 0101 1110 1001 1101 1111 0010 1010 1100 1010

Table

Description automatically generated

PC1 = 1011 1010 1011 0101 0101 0001 0010 1110 0111 0010 1101 1111 0100 1011

C0 = 1011 1010 1011 0101 0101 0001 0010

D0 = 1110 0111 0010 1101 1111 0100 1011

**2. Tính các giá trị dịch vòng Ci, Di:**

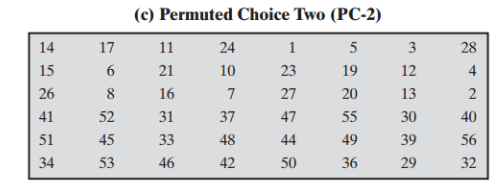
|  |  |  |  |
| --- | --- | --- | --- |
| i | Si | PC1K | |
| Ci | Di |
| 0 |  | 1 011 1010 1011 0101 0101 0001 0010 | 1110 0111 0010 1101 1111 0100 1011 |
| 1 | 1 | 0111 0101 0110 1010 1010 0010 0101 | 1100 1110 0101 1011 1110 1001 0111 |
| 2 | 1 | 1110 1010 1101 0101 0100 0100 1010 | 1001 1100 1011 0111 1101 0010 1111 |
| 3 | 2 | 1010 1011 0101 0101 0001 0010 1011 | 0111 0010 1101 1111 0100 1011 1110 |
| 4 | 2 | 1010 1101 0101 0100 0100 1010 1110 | 1100 1011 0111 1101 0010 1111 1001 |
| 5 | 2 | 1011 0101 0101 0001 0010 1011 1010 | 0010 1101 1111 0100 1011 1110 0111 |
| 6 | 2 | 1101 0101 0100 0100 1010 1110 1010 | 1011 0111 1101 0010 1111 1001 1100 |
| 7 | 2 | 0101 0101 0001 0010 1011 1010 1011 | 1101 1111 0100 1011 1110 0111 0010 |
| 8 | 2 | 0101 0100 0100 1010 1110 1010 1101 | 0111 1101 0010 1111 1001 1100 1011 |
| 9 | 1 | 1010 1000 1001 0101 1101 0101 1010 | 1111 1010 0101 1111 0011 1001 0110 |
| 10 | 2 | 1010 0010 0101 0111 0101 0110 1010 | 1110 1001 0111 1100 1110 0101 1011 |
| 11 | 2 | 1000 1001 0101 1101 0101 1010 1010 | 1010 0101 1111 0011 1001 0110 1111 |
| 12 | 2 | 0010 0101 0111 0101 0110 1010 1010 | 1001 0111 1100 1110 0101 1011 1110 |
| 13 | 2 | 1001 0101 1101 0101 1010 1010 1000 | 0101 1111 0011 1001 0110 1111 1010 |
| 14 | 2 | 0101 0111 0101 0110 1010 1010 0010 | 0111 1100 1110 0101 1011 1110 1001 |
| 15 | 2 | 0101 1101 0101 1010 1010 1000 1001 | 1111 0011 1001 0110 1111 1010 0101 |
| 16 | 1 | 1011 1010 1011 0101 0101 0001 0010 | 1110 0111 0010 1101 1111 0100 1011 |

3. **Tính khóa Ki cho vòng lặp thứ I   
Input:**

|  |  |
| --- | --- |
| C1 = | 0111 0101 0110 1010 1010 0010 0101 |

|  |  |
| --- | --- |
| D1 = | 1100 1110 0101 1011 1110 1001 0111 |

(kết quả bài 2), **PC2** (xem tài liệu mục 3.2 DES) **Output: Ki** = .3

****

K1 = 0110 0011 1101 1101 1100 0011 1100 1111 0110 1101 10100010

**PHẦN 2: MÃ HÓA  
4. Tính hoán vị IP đối với bản tin M  
Input:** M = 81793427080B49CF = , IP (xem tài liệu mục 3.2 DES)  
**Output:** L0 = , R0 =

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 1 | 7 | 9 | 3 | 4 | 2 | 7 | 0 | 8 | 0 | B | 4 | 9 | C | F |
| 1000 | 0001 | 0111 | 1001 | 0011 | 0100 | 0010 | 0111 | 0000 | 1000 | 0000 | 1011 | 0100 | 1001 | 1100 | 1111 |

M =1000 0001 0111 1001 0011 0100 0010 0111 0000 1000 0000 1011 0100 1001 1100 1111

IP(M) = 1100 0010 0000 0110 1000 1100 1110 1011 1000 0001 0000 1110 1111 0010 1010 1000

L0=C2 06 8C EB

R0=81 0E F2 A8

|  |
| --- |
| 10000001000011101111001010101000 |

**========== CHI TIẾT VÒNG LẶP THỨ NHẤT ==============  
5. Tính hàm mở rộng nửa phải E[*R0*]  
Input:** R0 =81 0E F2 A8 (kết quả bài 4), E (xem tài liệu mục 3.2 DES)  
**Output:** ER0 =

R0=

ER0= 010000000010100001011101011110100101010101010001

**6. Thực hiên XOR ER0 với khóa K1  
Input:** ER0 = 010000000010100001011101011110100101010101010001 (kết quả bài 5) ,

K1=011000111101110111000011110011110110110110100010 (kết quả bài 3) **Output:** A =

A= 001000111111010110011110101101010011100011110011

A=23F59EB538F3

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

A=001000 111111 010110 011110 101101 456 100011 110011

• 6-bit input qua mỗi Si ->cho ra 4-bit output

(Hàng = bit đầu + bit cuối , Cột = 4 bit giữa)

* 6 bit đầu qua bảng S1 ta có:

001000=> lấy hàng 00 = 0 , lấy cột 0100= 4

=> được 2 =0010

Tương tự ta có:

+ 9 = 1001 (hàng 3 cột 15 bảng S2)

+ 7 = 0111 (hàng 0 cột 11 bảng S3)

+ 15 = 1111 (hàng 0 cột 15 bảng S4)

+ 2 = 0010 (hàng 3 cột 6 bảng S5)

+ 1 = 0001 (hàng 1 cột 9 bảng S6)

+ 11 =1011 (hàng 3 cột 1 bảng S7)

+ 12 =1100 (hàng 3 cột 9 bảng S8)

B = 00101001011111110010000110111100 =297F21BC

**8. Thực hiện hoán vị P đối với SB  
Input:** B = 00101001011111110010000110111100

(kết quả bài 7), P (xem tài liệu mục 3.2 DES)  
**Output:** F =

A picture containing text, electronics, telephone

Description automatically generated

F = 10001110010010010111011011100101 = 8E 49 76 E5

**========= THỰC HIỆN VÒNG LẶP THỨ NHẤT =================  
9. Thực hiện vòng lặp thứ nhất  
Input:** L0 =11000010000001101000110011101011;

R0 =10000001000011101111001010101000, (kết quả bài 4),

F =10001110010010010111011011100101

(kết quả bài 8) **Output:** L1 = R0 = ; R1 = L0 ⊕ F =

L1 = R0 = 81 0E F2 A8

R1 = L0 ⊕ F = 4C 4F FA0E

========= THỰC HIỆN VÒNG LẶP THỨ i, i = 2, 3, ..., 16 ==========

10. Thực hiện vòng lặp thứ i, i = 2, 3, ..., 16

Input: Li-1 = ; Ri-1 = , (kết quả bài 9 hoặc bài 10)

Output: Li = Ri-1 = ; Ri = Li-1 ⊕ f(Ri-1,Ki) =