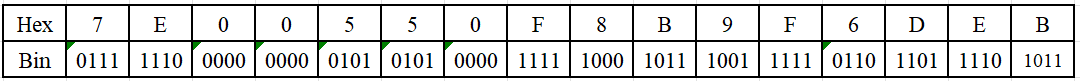
**Bài tập số 3\_ Đề 38**

Key: 7E00550F8B9F6DEB

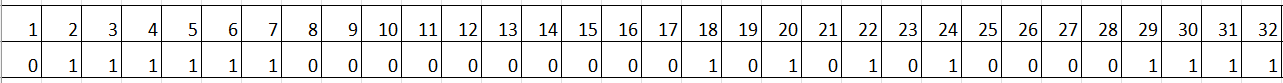
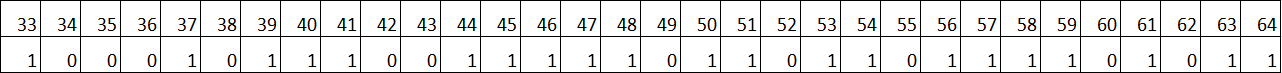
Plantext: 33B6473104DF7E84

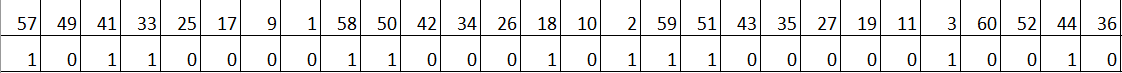
Bài làm

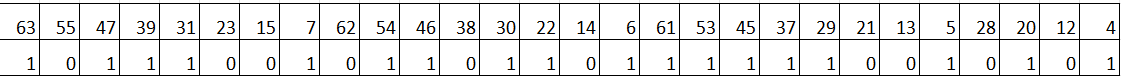
1. Sinh khóa con

- Ta có key: 7E00550F8B9F6DEB

- Hoán vị PC-1:

+ Ta có bảng:

+ Hoán vị:



- Dịch vòng trái: sinh 16 hoán vị

|  |  |  |  |
| --- | --- | --- | --- |
| Round Number | Bits Rotated | Ci | Di |
| 0 |  | 1011000011000101110000010010 | 1011100101101101111110010101 |
| 1 | 1 | 0110000110001011100000100101 | 0111001011011011111100101011 |
| 2 | 1 | 1100001100010111000001001010 | 1110010110110111111001010110 |
| 3 | 2 | 0000110001011100000100101011 | 1001011011011111100101011011 |
| 4 | 2 | 0011000101110000010010101100 | 0101101101111110010101101110 |
| 5 | 2 | 1100010111000001001010110000 | 0110110111111001010110111001 |
| 6 | 2 | 0001011100000100101011000011 | 1011011111100101011011100101 |
| 7 | 2 | 0101110000010010101100001100 | 1101111110010101101110010110 |
| 8 | 2 | 0111000001001010110000110001 | 0111111001010110111001011011 |
| 9 | 1 | 1110000010010101100001100010 | 1111110010101101110010110110 |
| 10 | 2 | 1000001001010110000110001011 | 1111001010110111001011011011 |
| 11 | 2 | 0000100101011000011000101110 | 1100101011011100101101101111 |
| 12 | 2 | 0010010101100001100010111000 | 0010101101110010110110111111 |
| 13 | 2 | 1001010110000110001011100000 | 1010110111001011011011111100 |
| 14 | 2 | 0101011000011000101110000010 | 1011011100101101101111110010 |
| 15 | 2 | 0101100001100010111000001001 | 1101110010110110111111001010 |
| 16 | 1 | 1011000011000101110000010010 | 1011100101101101111110010101 |

- PC-2: Với round number 1 ta có pc-2 như sau:

A picture containing chart

Description automatically generated

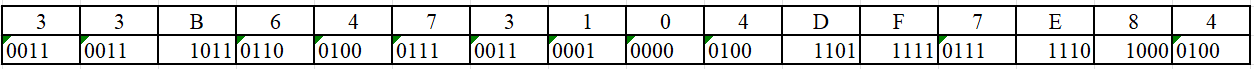
Ghép lại ta sẽ được khóa:

010000111000100011100011101111111101100101100001 :

Tương tự với các round còn lại ta sẽ xó bảng sau:

|  |  |  |
| --- | --- | --- |
| Round Number | Ki(bin) | Key(hex) |
| 1 | 010000111000100011100011101111111101100101100001 | 4388E3BFD961 |
| 2 | 100010001000001001111001011111110100101010111110 | 8882797F4ABE |
| 3 | 100001010101101000001110110101010101100111011011 | 855A0ED559DB |
| 4 | 001000100011101111000000100001111011001001111101 | 223BC087B27D |
| 5 | 000110000111110001100001111100111011111111100100 | 187C61F3BFE4 |
| 6 | 110000010110010101011000001110001000111110111111 | C16558388FBF |
| 7 | 010001001100011110000101010111110111110010010111 | 44C7855F7C97 |
| 8 | 010100111001100100000011011011110110000111111001 | 5399036F61F9 |
| 9 | 110010100000101000101001111101101110111010110011 | CA0A29F6EEB3 |
| 10 | 100010011011001000011100011111110000111101011011 | 89B21C7F0F5B |
| 11 | 000001000001111011001010100111111111000101011010 | 041ECA9FF15A |
| 12 | 011100100111100001100000011001011111011101100100 | 72786065F764 |
| 13 | 100010001110110101000000111110001010110011101110 | 88ED40F8ACEE |
| 14 | 010000000110011100011111111011001101111010011111 | 40671FECDE9F |
| 15 | 011001011001010100000001000111110111011011111011 | 6595011F76FB |
| 16 | 110110100001000100101000111010000111111100110111 | DA1128E87F37 |

2. Mã hóa plantext

- Ta có plantext : 33B6473104DF7E84. Chuyển plantext từ hệ hex sang hệ nhị phân

- Hoán vị IP: Dựa vào bảng ta sẽ có hoán vị:

Table

Description automatically generated

A picture containing calendar

Description automatically generated

A picture containing table

Description automatically generated

=> Kết quả hoán vị là:

0110010001101011111101100010110110100010010010110110000001100111

- Round 1:

Ta có L0: 01100100011010111111011000101101 => 646BF62D

R0: 10100010010010110110000001100111 => A24B6067

- Mở rộng hoán vị R0: Dự vào bảng sau để mở rộng ta sẽ có bảng dưới

Table

Description automatically generated



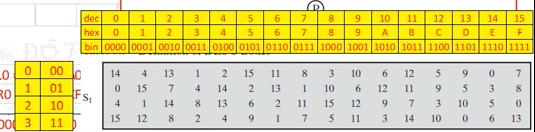
=> E(R0): 110100000100001001010110101100000000001100001111 =>

Thực hiện XOR với K1 = 010000111000100011100011101111111101100101100001

Nếu 2 bit giống nhau là 0, khác nhau là 1. Ta được kết quả:

XOR = 110100111100101010110101000011111101101001101110 => D3CAB50FDA6E

- Thay thế qua bảng S-box:



Table

Description automatically generated

Tách XOR thành các cặp 6 bit, rồi tra bảng, cột 1 tra bảng 1, cột 2 tra bảng 2, ... đến hết. Ta sẽ được kết quả như sau:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 6 bit | 110100 | 111100 | 101010 | 110101 | 000011 | 111101 | 101001 | 101110 |
| Row | 10 | 10 | 10 | 11 | 01 | 11 | 11 | 10 |
| Col | 1010 | 1110 | 0101 | 1010 | 0001 | 1110 | 0100 | 0111 |
| S\_box | 9 | 5 | 15 | 5 | 11 | 8 | 11 | 2 |
| Bin | 1001 | 0101 | 1111 | 0101 | 1011 | 1000 | 1011 | 0010 |

=> Sbox = 10010101111101011011100010110010=> 95F5B8B2

- Tiếp theo là hoán vị Permutation. Hoán vị P được cho bởi bảng: Table

Description automatically generated

Ta được bảng sau:

A picture containing calendar

Description automatically generated

=> P = 10100010000100001000110000100101 => A2108C25

- Thực hiện phép Xor P với L0:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| i | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| L0 | 1010 | 0010 | 0001 | 0000 | 1000 | 1100 | 0010 | 0101 |
| P | 0110 | 0100 | 0110 | 1011 | 1111 | 0110 | 0010 | 1101 |
| Xor | 1100 | 0110 | 0111 | 1011 | 0111 | 1010 | 0000 | 1000 |

=> Ta được R1: 11000110011110110111101000001000 => C67B7A08

Ta thu được bảng sau với K1. Các key sau làm tương tự.

Table

Description automatically generated