1. Sinh Khóa con

Key: 992DCDBF953C4C5A

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1 | | 2 | | 3 | | 4 | | 5 | 6 | | 7 | | 8 | | 9 | | 10 | | 11 | 12 | | 13 | | 14 | | 15 | | 16 |
| Hex | 9 | | 9 | | 2 | | D | | C | D | | B | | F | | 9 | | 5 | | 3 | C | | 4 | | C | | 5 | | A |
| Bin | 1001 | | 1001 | | 0010 | | 1101 | | 1100 | 1101 | | 1011 | | 1111 | | 1001 | | 0101 | | 0011 | 1100 | | 0100 | | 1100 | | 0101 | | 1010 |
| Key | | 10011001 00101101 11001101 10111111 10010101 00111100 01001100 01011010 | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Số bit | | 64 | |  | |  | |  | | |  | |  | |  | |  | |  | | |  | |  | |  | |  | |

Permuted Choice One (PC-1)

|  |  |
| --- | --- |
| After PC1 | 00011101110001000010101010111000100001111110111011111001 |
| Len(PC1) | 56 |

Left Shift

|  |  |  |  |
| --- | --- | --- | --- |
| Round Number | Bits Rotated | Ci | Di |
| 0 |  | 0001110111000100001010101011 | 1000100001111110111011111001 |
| 1 | 1 | 0011101110001000010101010110 | 0001000011111101110111110011 |
| 2 | 1 | 0111011100010000101010101100 | 0010000111111011101111100110 |
| 3 | 2 | 1101110001000010101010110001 | 1000011111101110111110011000 |
| 4 | 2 | 0111000100001010101011000111 | 0001111110111011111001100010 |
| 5 | 2 | 1100010000101010101100011101 | 0111111011101111100110001000 |
| 6 | 2 | 0001000010101010110001110111 | 1111101110111110011000100001 |
| 7 | 2 | 0100001010101011000111011100 | 1110111011111001100010000111 |
| 8 | 2 | 0000101010101100011101110001 | 1011101111100110001000011111 |
| 9 | 1 | 0001010101011000111011100010 | 0111011111001100010000111111 |
| 10 | 2 | 0101010101100011101110001000 | 1101111100110001000011111101 |
| 11 | 2 | 0101010110001110111000100001 | 0111110011000100001111110111 |
| 12 | 2 | 0101011000111011100010000101 | 1111001100010000111111011101 |
| 13 | 2 | 0101100011101110001000010101 | 1100110001000011111101110111 |
| 14 | 2 | 0110001110111000100001010101 | 0011000100001111110111011111 |
| 15 | 2 | 1000111011100010000101010101 | 1100010000111111011101111100 |
| 16 | 1 | 0001110111000100001010101011 | 1000100001111110111011111001 |

Permuted Choice Two (PC-2)

|  |  |  |
| --- | --- | --- |
| Round Number | Ki | Key(Hex) |
| 1 | 000001100000000111011110110101011101110110111001 | 0601ded5ddb9 |
| 2 | 010100100110111111010001101111011101111000001100 | 526FD1BDDE0C |
| 3 | 010111011111110100000001110110000101011011110110 | 5DFD01D856F6 |
| 4 | 010100111010010111001011100111011110101000101101 | 53A5CB9DEA2D |
| 5 | 011010011100010010000111101100100111110011010001 | 69C487B27CD1 |
| 6 | 011000011000100110001010101110111010001110110111 | 61898ABBA3B7 |
| 7 | 001100001010000010110111101101110110110110000010 | 30A0B7B76D82 |
| 8 | 101001010000110000010110011111000010001111010111 | A50C167C23D7 |
| 9 | 010100000111111101001010111101101000001101110101 | 507F4AF68375 |
| 10 | 011100001111010101100101010000111010111101001111 | 70F56543AF4F |
| 11 | 110000011100110101000011011111101011010100011001 | C1CD437EB519 |
| 12 | 011100011110001110110011011010110101011101101111 | 71E3B36B576F |
| 13 | 101001011001010110000011010011101111100110101010 | A595834EF9AA |
| 14 | 011000110000001011010011111001000101111111111101 | 6302D3E45FFD |
| 15 | 001011011101000010010100110010111001100011111010 | 2DD094CB98FA |
| 16 | 100101010111110101001000110010011110010101111010 | 957D48C9E57A |

2. Mã hóa:

Plaintext: AB7A25DE0E01B093

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1 | |  | | 2 | | 3 | | 4 | | 5 | 6 | | 7 | | 8 | | 9 | | 10 | | 11 | 12 | | 13 | | 14 | | 15 | | 16 |
| Hex | A | |  | | B | | 7 | | A | | 2 | 5 | | D | | E | | 0 | | E | | 0 | 1 | | B | | 0 | | 9 | | 3 |
| Bin | 1010 | |  | | 1011 | | 0111 | | 1010 | | 0010 | 0101 | | 1101 | | 1110 | | 0000 | | 1110 | | 0000 | 0001 | | 1011 | | 0000 | | 1001 | | 0011 |
| Key | |  | | 1010101101111010001001011101111000001110000000011011000010010011 | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Số bit | |  | | 64 | |  | |  | |  | | |  | |  | |  | |  | |  | | |  | |  | |  | |  | |

Intial Permutation (IP)

|  |  |
| --- | --- |
| After ip | 0000101011001010000111001010010111001001010001110001101110011011 |
|  | 64 |

|  |  |  |
| --- | --- | --- |
| Vòng lặp | 1 |  |
| L0 | 00001010110010100001110010100101 | 0ACA1CA5 |
| R0 | 11001001010001110001101110011011 | C9471B9B |
| E(R0) | 100001011100000000000011110110100001010010100110 | 85C003DA14A6 |
| XOR K1 | 100000111100000111011101000011111100100100011111 | 83C1DD0FC91F |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 6 bit | 100000 | 111100 | 000111 | 011101 | 000011 | 111100 | 100100 | 011111 |
| Row | 10 | 10 | 01 | 01 | 01 | 10 | 10 | 01 |
| Col | 0000 | 1110 | 0011 | 1110 | 0001 | 1110 | 0010 | 1111 |
| S\_box | 4 | 2 | 9 | 14 | 11 | 11 | 11 | 2 |
| Bin | 0100 | 0010 | 1001 | 1110 | 1011 | 1011 | 1011 | 0010 |

=>Sbox: 01000010100111101011101110110010 => 429EBBB2

Hoán vị P:

=> P = 01110111011000101011010111000001 =>7762B5C1

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| i | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| L0 | 0000 | 1010 | 1100 | 1010 | 0001 | 1100 | 1010 | 0101 |
| P | 0111 | 0111 | 0110 | 0010 | 1011 | 0101 | 1100 | 0001 |
| Xor | 0111 | 1101 | 1010 | 1000 | 1010 | 1001 | 0110 | 0100 |

=>R1: 01111101101010001010100101100100 => 7DA8A964

Ta thu được:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Round | SubKey | Li | Ri | Ei | Xor(Ei,Ki) | S-box | P(S-box) | Xor(P,Li) |
| IP | 48bit |  |  | 48bit | 48bit | 32bit | 32bit | 32bit |
| 1 | 0601ded5ddb9 | 0ACA1CA5 | C9471B9B | 85C003DA14A6 | 83C1DD0FC91F | 429EBBB2 | 7762B5C1 | 7DA8A964 |