



Q1. input plain text: A7E2BC3FD4C896D2
in binary format: ~~00010100000011~~

1010 0111 1110 0010
1011 1100 0011 1111
1101 0100 1100 1000
1001 0110 1101 0010

Apply input permutation:

$L_0 = \begin{cases} 1011 & 0010 & 1101 & 1100 \\ 0101 & 1101 & 0000 & 1001 \end{cases}$
 $R_0 = \begin{cases} 1111 & 0111 & 0000 & 1111 \\ 0010 & 1100 & 1100 & 1011 \end{cases}$

The encryption key is: 1A5D6D895B4B66DB
in binary format: 0001 1010 0101 1101
0110 1101 1000 1001
0101 1011 0100 1011
0110 0110 1101 1011

After Key transform:

$\begin{bmatrix} 1000 & 1000 & 1111 & 0110 \\ 0100 & 0100 & 1001 & 1111 \\ 0001 & 0100 & 0110 & 1011 \\ 1111 & 0011 & & \end{bmatrix}$

In round 1, shift left 1 bit. have:

~~00010100000011~~ 0001000 1111 0110 0100 0100 0011

~~001~~

111 000 0100 0110 1011 1111 0011

Permut choice 2: 1111 0001 0011 0001 0100 0101
1011 1110 1001 1101 0110 1010

R_0 After expansion permutation:

1111 0101 1110 1000 0101 1110 1001 0101 1001 0110 0101 0111

after \oplus permut choice 2: 0000 1011 1101 1001 0001 0100 0010 1011 0000 1011 0110 1101

0,1 3,14 2,2 0,10 0,5 2,8 3,6 3,6
4 14 4 8 10 7 10 8

S.Box result: 0100 1110 0100 1000 1010 0111 1010 1000

permute with P Box: 0100 1001 0010 1001 1010 0100 1101 1001

$R_1 = \text{Xor with } L_0: 1111 1011 1111 0101 1111 1001 1101 0000$

$L_1 = R_0 = 1111 0111 0000 1111 0010 1100 1100 1011$

In hex: $L_1: F70F2CCB$ $R_1: FBFSF9D0$