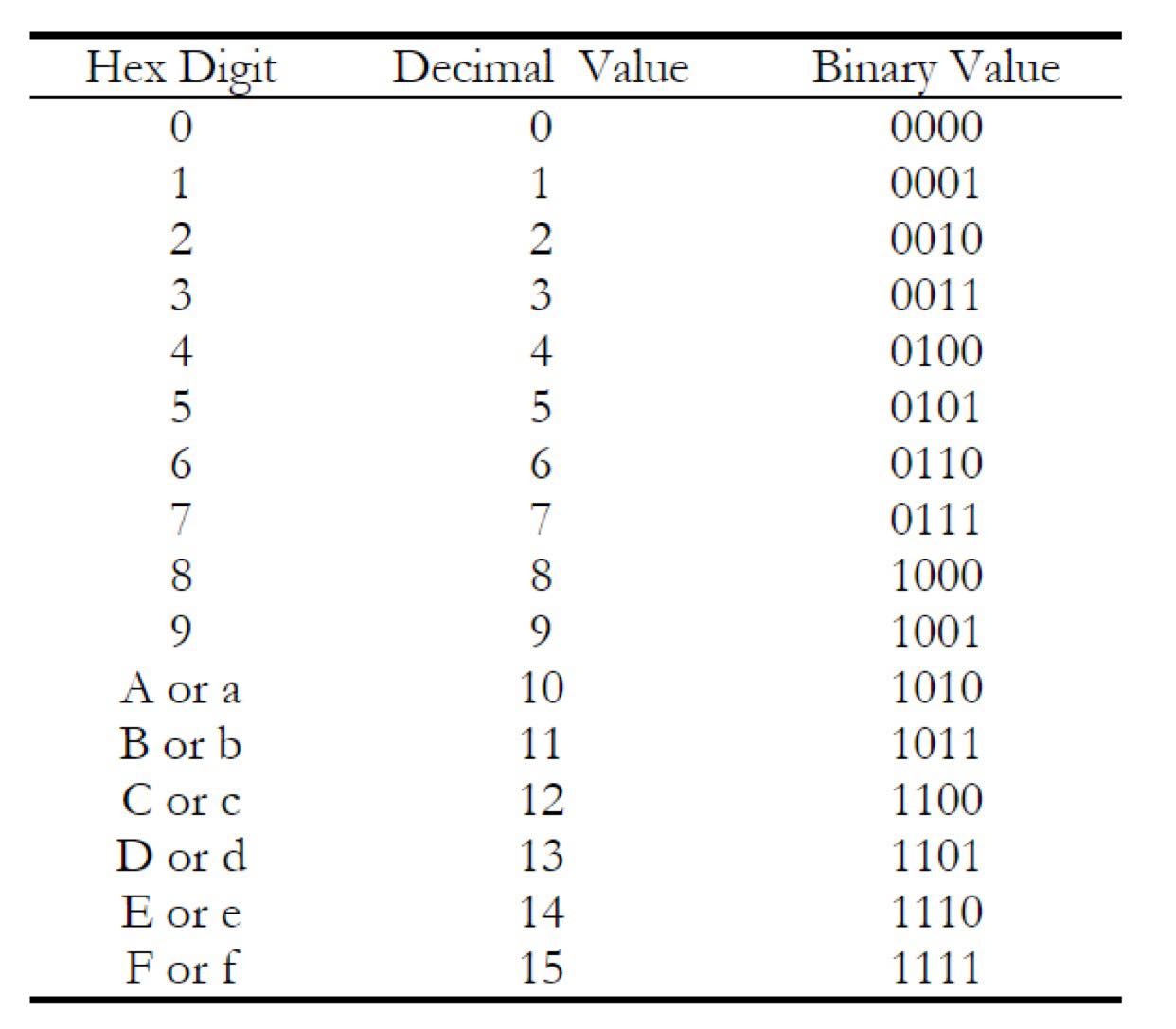
c

**Li = Ri -1**

**Ri = (Li-1) + F(Ri -1 , ki)**

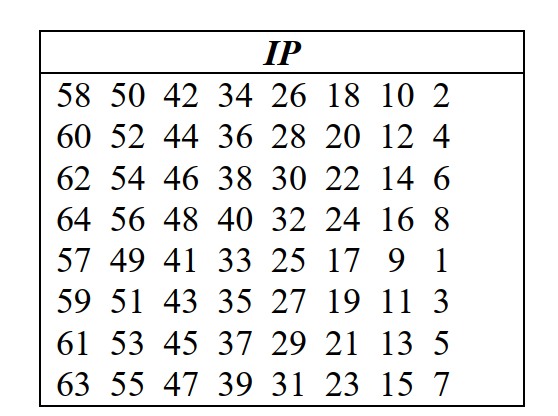
R1 = l0 + f (r0, k1)

Input: M , K0

B1: IP(X) - > L0 ( 32 Bit đầu) , RO ( 32 bit còn lại)

K0 = 0001001

0011010 0101011 0111100 1001101 1011110 1101111 1111000

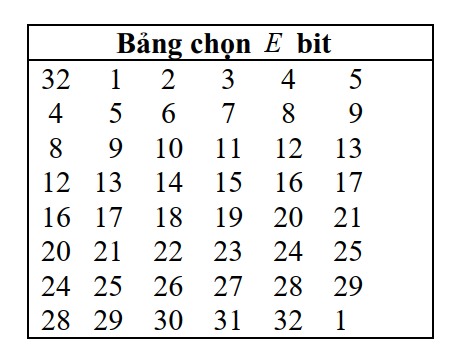


Cthuc : 1357 , 0246 từ dưới lên

L0 ( 32 Bit đầu) , RO ( 32 bit còn lại)

B2: MỞ RỘNG E(r0) 32 bit sau -> 48 bit

So sanhs với bảng e



**B3**: E® + K1 = B1-> B8 ( 6bit\*8) = 48 bit ( 6 bit là 1b)

E(r0) + k1 = (xor : cộng không nhớ )

**B4**: B1->B8 -> Sbox 8 bảng ( s1 -> s8)

Bi so với bảng Si

b1 : B1b2b3b4b5b6

( R = B1B6 : hàng , S = B2B3B4B5 : cột )

B5: **Ri = (Li-1) + F(Ri -1 , ki)**

VÍ DỤ:

B1 = 000011

R =01(dec) = 1 ( bin) -> hàng 1

**( 00 =0 , 01=1, 10 =2, 11 = 3)**

S = 0001 ( bin) = 1 ( dec) -> cột 1

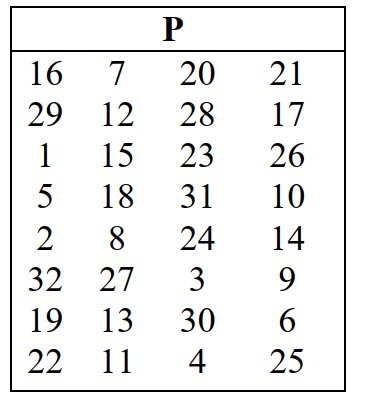
11 -> so với bảng sbox s1 = 15 (dec) -> (1111)2

output: s1 = 1111 (4 bit ) \*8 = 32 bit

s2 -> s8 :

**output : 32 bit**

B5: đủ b1, b8 output -> đưa vào hàm P -> hàm F



----

K0= 0001001

0011010

0101011

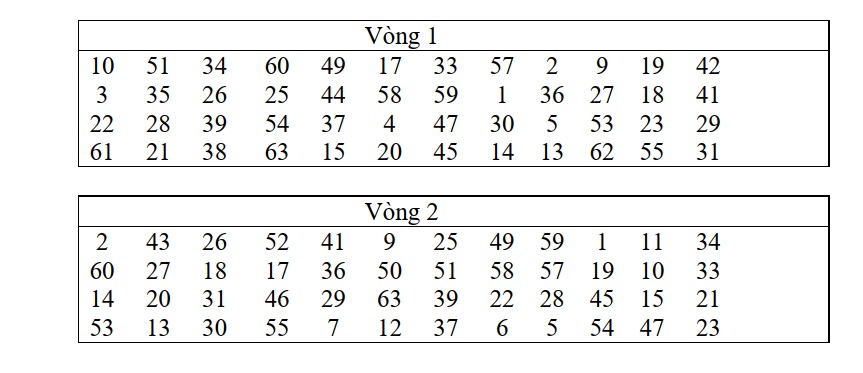
0111100

1001101

1011110

1101111

1111000



K1 = 0001101

K2 = k1 so với vòng 2 ………

Đề bài:

Xét việc mã hoá bản rõ (ở dạng mã hexa):

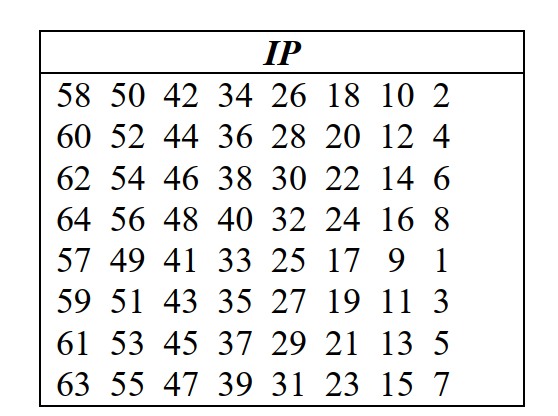
M = 0 1 2 3 4 5 6 7 8 9 A B C D E F

bằng cách dùng khoá

K0 = 1 2 3 4 5 7 7 9 9 B B C D F F 1

Khoá ở dạng nhị phân (không chứa các bit kiểm tra –bit 8,16,...) là: 0001001 0011010 0101011 0111100 1001101 1011110 1101111 1111000 (chỗ cách là chỗ các bit 8,16,... bị bỏ qua).

B1: dùng bảng IP, để tính L0 và R0 (dạng nhỉ phân)

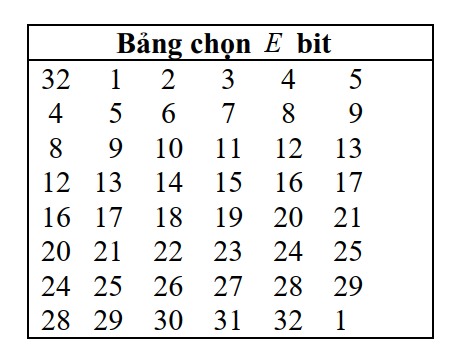


L0 = 32 bit đầu

R0 = 32 bit cuối

B2: MỞ RỘNG E(R0) 32 bit sau -> 48 bit

So sánh với bảng E



**B3**: E® + K1 = B1-> B8 ( 6bit\*8) = 48 bit ( 6 bit là 1b)

E(r0) + k1 = (xor : cộng không nhớ )

**B4**: tìm hộp S

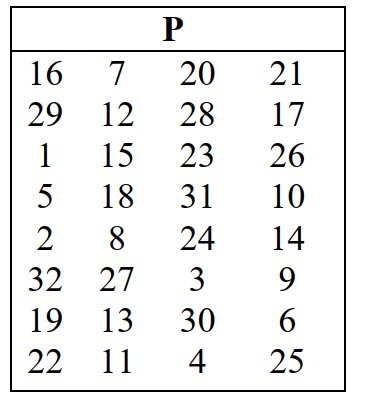
B1->B8 -> Sbox 8 bảng ( s1 -> s8)

Bi so với bảng Si

b1 : B1b2b3b4b5b6

( R = B1B6 : hàng , S = B2B3B4B5 : cột )

**B5**: đủ b1, b8 output -> đưa vào hàm P -> hàm F



**B6**: R1 là = L0 + f(r0,k1)