Ramos Magaña Miguel Angel 6CM2

Franco Olvera Deman Oder

2.- Let Mix(P)

1	2	3	4	5	6	7	8
6	8	12	10	13	16	11	15
4	2	1	9	3	5	7	14
9	10	11	12	13	14	15	16

P^{-1}

11	10	13	9	14	1	15	2
12	4	7	3	5	16	8	6

1.- M = 11111....1111

K = 0000...000

La tabla M es igual a la tabla IP, lo cual nos deja con R0 = 11111...1111 y E(R0) = 11111...111

Como K = 00000....0000 entonces PC-1 es igual. Por lo tanto, al calcular K_1 entonces será K_1 = 000000000000.

E(R0) ⊕ k1 =

```
E(R0)    1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111
XOR K1   0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
         1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111
```

11 = 3 fila

111111

F = 15 columna

```
1 1 1 1 1 1   1 1 1 1 1 1   1 1 1 1 1 1   1 1 1 1 1 1   1 1 1 1 1 1
    S1 13         S2 9          S3 12         S4 14         S5 3
 1 1 0 1 -> d   1 0 0 1 -> 9   1 1 0 0 -> c   1 1 1 0 -> e   0 0 1 1 -> 3

        1 1 1 1 1 1, 1 1 1 1 1 1, 1 1 1 1 1 1,
            S6 13         S7 12         S8 11
        1 1 0 1 -> d   1 1 0 0 -> c   1 0 1 1 -> b
```

P

16	7	20	21	29	12	28	17
0	0	1	1	1	0	0	0
1	15	23	26	5	18	31	10
1	1	0	1	1	0	1	1
2	8	24	14	32	27	3	9
1	1	1	1	1	0	0	1
19	13	30	6	22	11	4	25
1	1	0	0	1	0	1	1

```
L0      1111 1111 1111 1111 1111 1111 1111 1111
XOR F   0011 1000 1101 1011 1111 1001 1100 1011
        1100 0111 0010 0100 0000 0110 0011 0100
0x       c    7    2    4    0    6    3    4
```

R_1 = 0x c7240634

L_1 = 0x FFFFFFFF

3.- X1 = 0x 0eba1123947c

x2 = 0x1afc492f991f

a)

$$X_1 = \underbrace{0000\,11}_{8}\underbrace{10\,1011}_{1}\ \underbrace{1010\,00}_{12}\underbrace{01\,0001}_{4}\underbrace{0010\,00}_{0}\underbrace{11\ 1001}_{12}\ \underbrace{0100\,01}_{4}\underbrace{11\,1100}_{8}$$

S4 →

$$X_2 = \underbrace{0001\,10}_{3}\underbrace{10\ 1111}_{8}\ \underbrace{1100\,01}_{9}\underbrace{00\ 1001}_{6}\underbrace{0010\,11}_{15}\underbrace{11\,1001}_{12}\ \underbrace{1001\ 00}_{9}\underbrace{01\ 1111}_{9}$$

$S_4(X_1)$ → 1000 0001 1100 0100 0000 1100 0100 1000

XOR $S_4(X_2)$ → 0011 1000 1001 0110 1111 1100 1001 1001

1011 1001 0101 0010 1111 0000 1101 0001

0x b 9 5 2 F 0 d 1 <—

∴ 0xB952F0D1

≠

0xBE1B875F

b) X_1 = 0000 1110 1011 1010 0001 0001 0010 0011 1001 0100 0111 1100

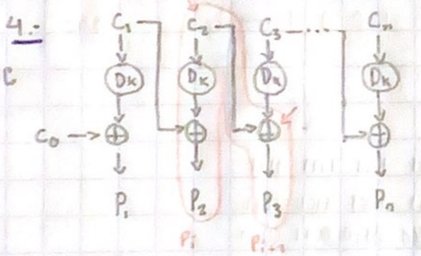
XOR X_2 = 0001 1010 1111 1100 0100 1001 0010 1111 1001 1001 0001 1111

$$\underbrace{0001\,0100}_{11}\ \underbrace{0100}_{14}\ \underbrace{0110}_{1}\ \underbrace{0101\,1000}_{11}\ \underbrace{0000\ \ 1100}_{8}\ \underbrace{0000}_{7}\ \underbrace{1101\ \ 0110}_{5}\ \underbrace{0011}_{15}$$

0x b e 1 b 8 7 5 F <—

4.-

CBC



Observamos que si se afecta o algún bloque Ci tiene un error, la información correspondiente al bloque de texto plano (pi) se verá igualmente afectada, así como el siguiente bloque de texto plano (pi+1) pues se está realizando un XOR con el Ci dañado para obtenerla.

6.- Sabemos que:

$$K=\begin{pmatrix}1&2&3\\4&5&6\\11&9&8\end{pmatrix}.$$ Sabemos por el programa que $K^{-1} \bmod 256 = \begin{pmatrix}90&167&1\\74&179&254\\177&81&1\end{pmatrix}$

Necesitamos P_2; de acuerdo con el diagrama de descifrado en CBC, sabemos que:

$$\underline{P_2 = D_K(C_2) \oplus C_1}$$

Sabemos también que:

$$\underline{C_1 = (40, 171, 36)} \;\&\; \underline{C_2 = (236, 184, 95)}$$

Hacemos $D_K(C_2) = (236, 184, 95) \cdot \begin{pmatrix}90&167&1\\74&179&254\\177&81&1\end{pmatrix} = \underline{(215, 171, 219)}$

$a = 236(90) + 184(74) + 95(177) = 51671 \bmod 256 = 215$

$b = 236(167) + 184(179) + 95(81) = 80043 \bmod 256 = 171$

$c = 236(1) + 184(254) + 95(1) = 47067 \bmod 256 = 219$

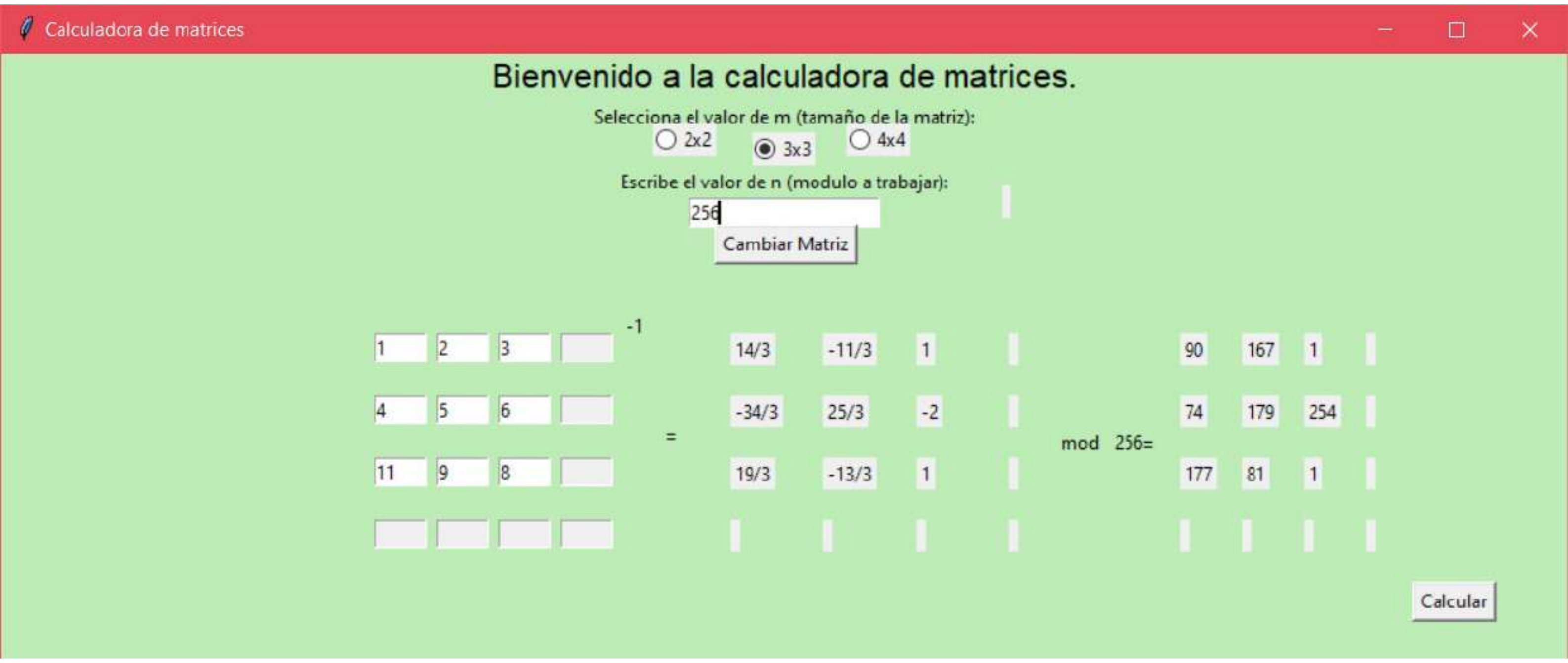
Tenemas:

40 ~ 10 1000 | 215 ~ 1101 0111
171 ~ 1010 1011 | 171 ~ 1010 1011
36 ~ 10 0100 | 219 ~ 1101 1011

$$\begin{array}{r}0010\ 1000\\ 1101\ 0111\\ \hline 1111\ 1111\end{array}\sim 255 \qquad \begin{array}{r}1010\ 1011\\ 1010\ 1011\\ \hline 0000\ 0000\end{array}\sim 0 \qquad \begin{array}{r}0010\ 0100\\ 1101\ 1011\\ \hline 1111\ 1111\end{array}\sim 255$$

Finalmate: $\underline{P_2 = (255, 0, 255)}$

P_2	255	0	255



Bienvenido a la calculadora de matrices.

Selecciona el valor de m (tamaño de la matriz):

○ 2x2 ● 3x3 ○ 4x4

Escribe el valor de n (modulo a trabajar): 256

$$\begin{pmatrix}1 & 2 & 3\\ 4 & 5 & 6\\ 11 & 9 & 8\end{pmatrix}^{-1} = \begin{pmatrix}14/3 & -11/3 & 1\\ -34/3 & 25/3 & -2\\ 19/3 & -13/3 & 1\end{pmatrix} \bmod 256 = \begin{pmatrix}90 & 167 & 1\\ 74 & 179 & 254\\ 177 & 81 & 1\end{pmatrix}$$