*Cryptography*

*“Ejercicio DES*

**Grupo:** 3CM13

**Integrantes:**

* CHACON INOSTROSA JAIME ENRIQUE.
* RAMÍREZ OLVERA GUILLERMO.
* SÁNCHEZ MÉNDEZ EDMUNDO JOSUE.
* BERNAL RAMIREZ ANDRE
* CEDILLO HERNANDEZ JUAN DANIEL
* COVARRUBIAS SANCHEZ DANIEL

**Ejercicio DES**

**Instrucciones**

1. Let M= 11111….1111 and K=1111...1111 be the DES key. Show the output of the Sbox after the first round.

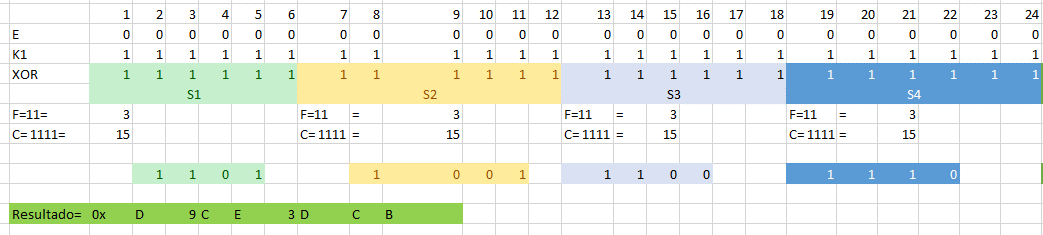
Aplicación, Tabla, Excel, Calendario

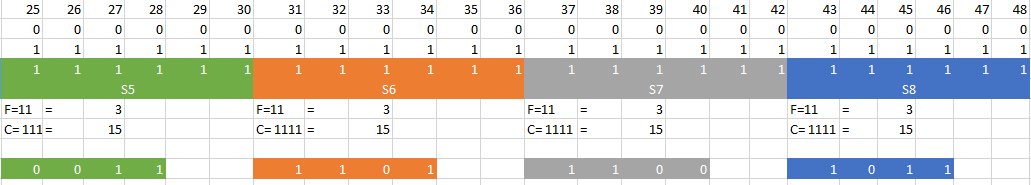
Descripción generada automáticamente

Interfaz de usuario gráfica, Aplicación, Tabla, Excel, Calendario

Descripción generada automáticamente

1. Let M= 0000...000 and K=1111…111 be the DES key. Show the output of the Sbox after the first round.





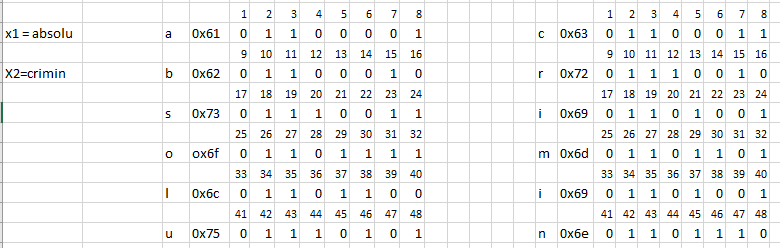
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Let Mix(p)   |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | 13 | 3 | 2 | 15 | 5 | 10 | 7 | 9 | | 16 | 1 | 14 | 4 | 12 | 6 | 11 | 8 | | Find the inverse Mix   |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | 10 | 3 | 2 | 12 | 5 | 14 | 7 | 16 | | 8 | 6 | 15 | 13 | 1 | 11 | 4 | 9 | |

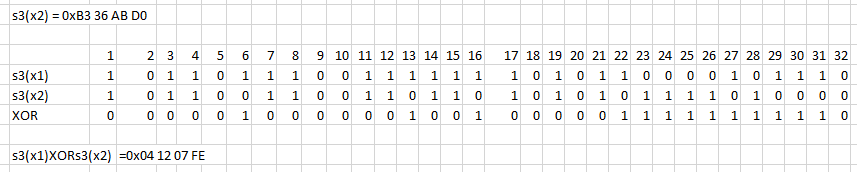
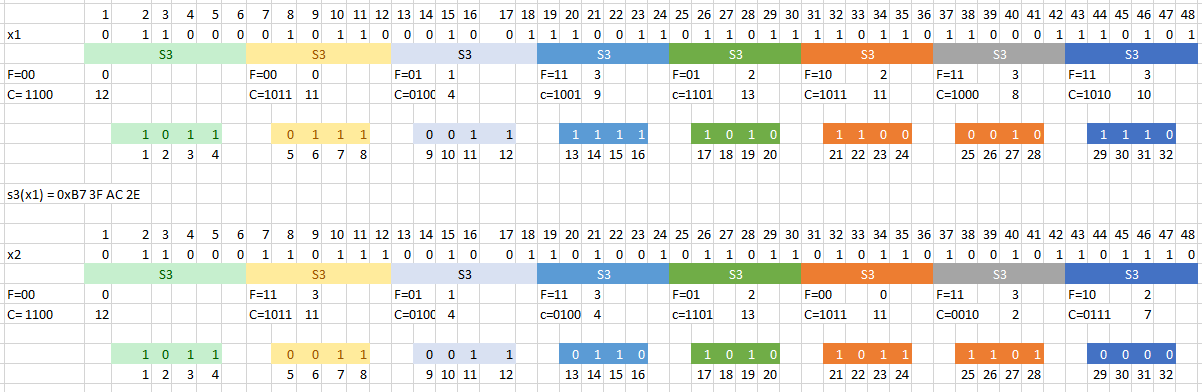
1. Show that in DES the S-boxes are nonlinear. Let the input to the S-box

X1 = absolu

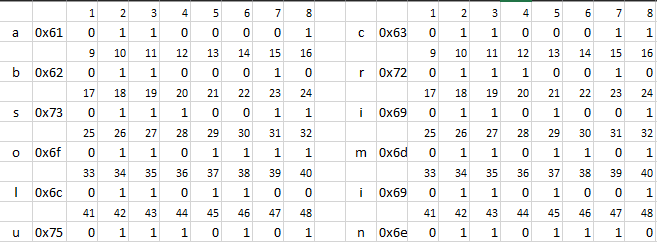
X2= crimin

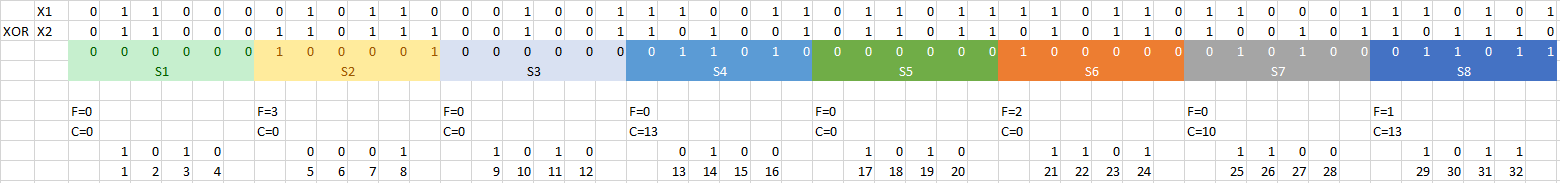
a)Find S3(x1) XOR S3(x2)



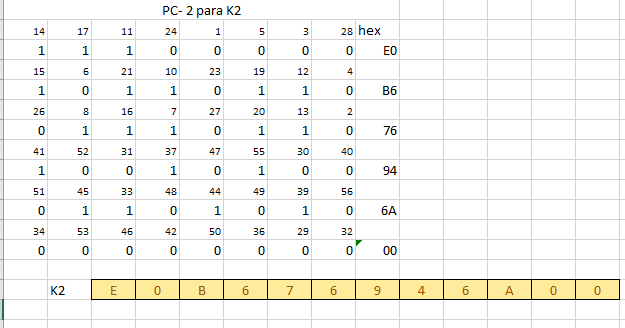


b)Find S3(x1 XOR x2)

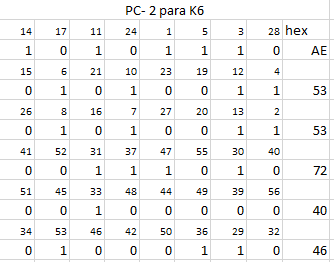




1. If the initial Key= **academic** calculate the K2 Using DES.



1. If the initial Key= **academic** calculate the K6 Using DES.





**Deadline**

[Capte la atención de los lectores mediante una cita importante extraída del documento o utilice este espacio para resaltar un punto clave. Para colocar el cuadro de texto en cualquier lugar de la página, solo tiene que arrastrarlo.]