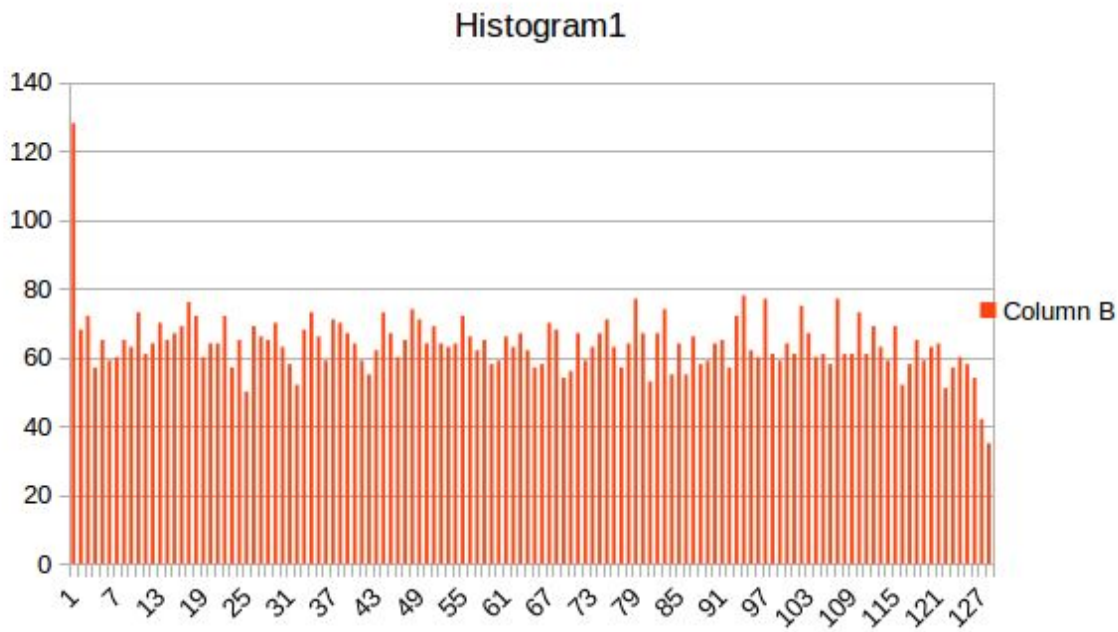
Practica 3 - AES

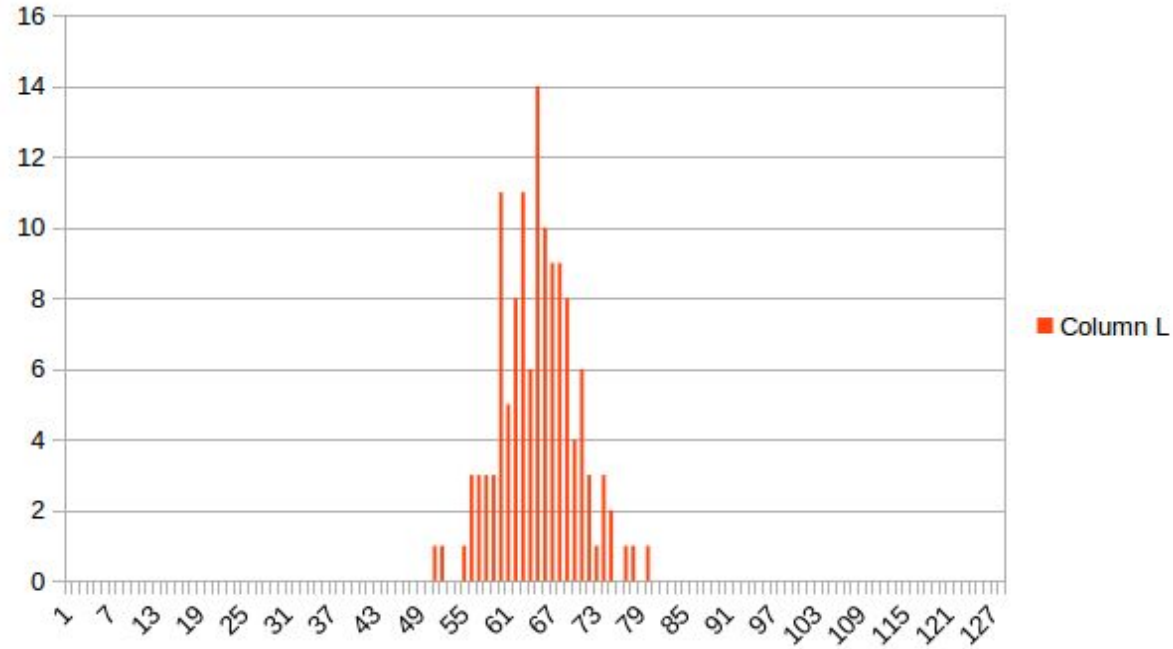
1) Para comprobar que efectivamente, si cuando tenemos la función subBytes como la identidad, podemos conseguir el mensaje codificado de M : (C),a partir de C = Ci ^ Cj^ Cij He crado 100 Mensajes M aleatorios con sus respectivos Mi,Mj i Mij, codificandolos y comprobando si la formula era cierta. Efectivamente, al ejecutarlos comprobamos por medio del script que todos los 100 casos cumplen la formula i que si usamos la función original, no.
2) Podemos observar que, si shift rows corresponde a la identidad, el bloque resultante solo cambia en la fila donde el bit i ha sido modificado, en cambio, si usamos el shiftrows original, podemos observar que el cambio se ha propagado por varios bits del bloque.
3) Si utilizamos el mixing row original podemos observar que al cambiar un bit del mensaje original, esto hace que en el mensaje cifrado haya mas de un byte modificado, No obstante si decidimos utilizar la identidad para esta funcion, nos encontramos que solamente cambia el byte que hemos alterado al producir Mi

Histogramas

(1)



(2)


16
14
12
10
8
6
4
2
0
1
7
13
19
25
31
37
43
49
55
61
67
73
79
85
91
97
103
109
115
121
127
Column L