Oscar Mañas, grup 10

Advanced Encryption Standard (AES)

1. Efectes de les funcions elementals:

   (a) Canviem la funció **ByteSub** per la identitat, i.e. **ByteSub(x)=x**.

   Comentem la línia 211 del fitxer *aes.py* per tal de canviar la funció ByteSub per la identitat. Descomentem la línia 208 del fitxer *entrega3.py* per tal de cridar a la funció *exercici_1a()*.

   Dins la funció generem una clau aleatòria K i fem 100 iteracions, on a cada iteració generem un missatge aleatori M i les seves variacions amb bits canviats M_i, M_j, M_k, M_l, M_{ij}, M_{ijkl}. Encriptem els missatges i finalment comprovem que es compleix $C = C_i \wedge C_j \wedge C_{ij}$ i $C_{ijkl} = C_i \wedge C_j \wedge C_k \wedge C_l$ fent un *assert*.

   (b) Canviem la funció **ShiftRows** per la identitat. Quins efectes té aquest canvi al xifrar un bloc?

   Comentem les línies 216 i 217 del fitxer *aes.py* per tal de canviar la funció *ShiftRows* per la identitat. Descomentem la línia 209 del fitxer *entrega3.py* per tal de cridar a la funció *exercici_1b()*.

   Dins la funció generem una clau aleatòria K i diversos missatges M amb les seves variacions M_i corresponents. Encriptem els missatges i, en comparar-los, observem que els xifrats C i C_i són idèntics excepte en una fila.

   (c) Canviem la funció **MixColumns** per la identitat. Quins efectes té aquest canvi al xifrar un bloc?

   Comentem les línies 236-242 del fitxer *aes.py* per tal de canviar la funció *MixColumns* per la identitat. Descomentem la línia 210 del fitxer *entrega3.py* per tal de cridar a la funció *exercici_1c()*.

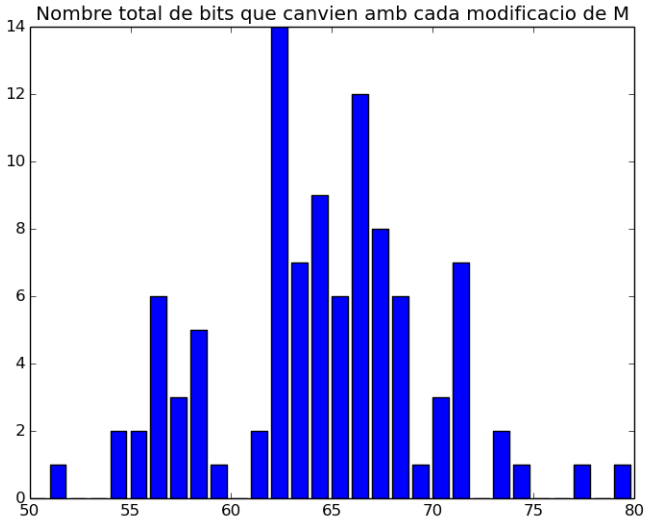
   Dins la funció generem una clau aleatòria K i diversos missatges M amb les seves variacions M_i corresponents. Encriptem els missatges i, en comparar-los, observem que els xifrats C i C_i són idèntics excepte en un byte.

2. Propagació de canvis: Amb un missatge M de 128 bits i una clau K de 128 bits qualssevol feu una estadística dels bits que canvien a la sortida quan modifiqueu un bit de M :

   (a) Histograma del nombre total de bits que canvien amb cada modificació.

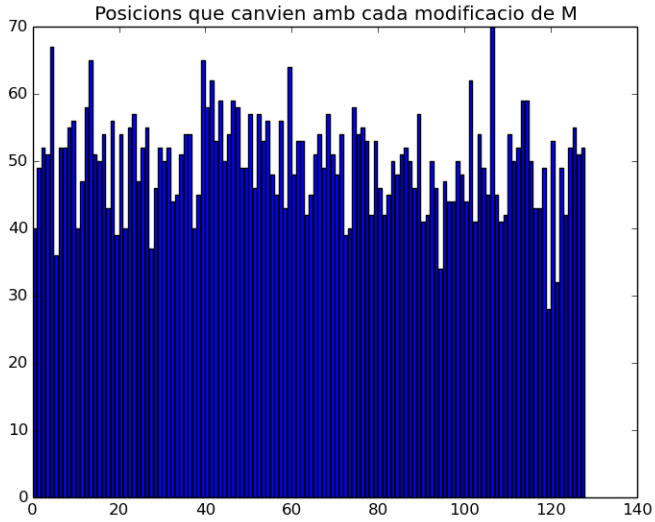
   Descomentem la línia 211 del fitxer *entrega3.py* per tal de cridar a la funció *exercici_2a()*.

   Observem que el més comú és que canviïn aproximadament la meitat dels bits.



(b) Histograma de les posicions que canvien amb cada modificació.

Descomentem la línia 212 del fitxer *entrega3.py* per tal de cridar a la funció *exercici_2b()*.

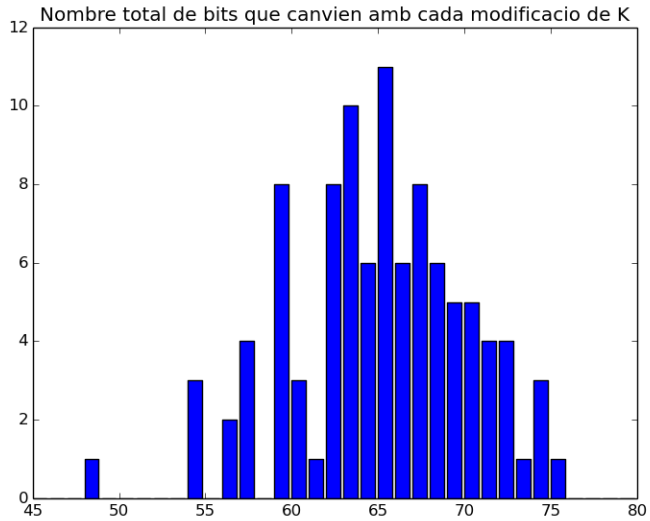


Observem que totes les posicions canvien gairebé amb la mateixa probabilitat.

Feu el mateix si modifiqueu un bit de *K*.

(c) Histograma del nombre total de bits que canvien amb cada modificació.

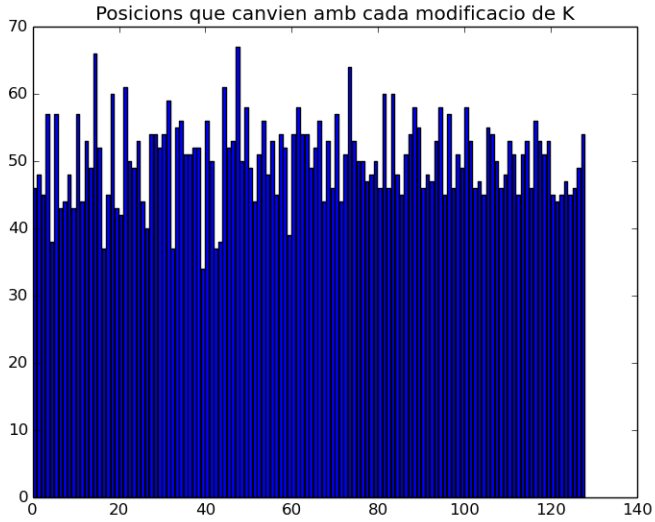
Descomentem la línia 213 del fitxer *entrega3.py* per tal de cridar a la funció *exercici_2c()*.



Observem que el més comú és que canviïn aproximadament la meitat dels bits.

(d) Histograma de les posicions que canvien amb cada modificació.

Descomentem la línia 214 del fitxer *entrega3.py* per tal de cridar a la funció *exercici_2d()*.



Observem que totes les posicions canvien gairebé amb la mateixa probabilitat.