Universitat Politècnica de Catalunya

Criptografia

Segona entrega: Clau secreta

Mario Fernández Villalba

Grup 11

Q1 2017-2018

Contents

1 El cos finit $GF\ 2^8$

Per fer la comparativa de l'eficiència de les funcions *GF_product_p* i *GF_product_t* he realitzat 10000 experiments agafant valors aleatoris per a a.

Després de realitzar aquests experiments, he comprovat que en el 100% dels casos el producte mitjançant taules és molt superior en eficiència al producte estàndard.

2 Advanced Encryption Standard (AES)

Per resoldre els problemes plantejats en aquesta secció he implementat la meva pròpia versió de l'algoritme AES i del xifratge de blocs ECB.

2.1 Efectes de les funcions elementals

1. Per comprovar que es compleix la igualtat $C = C_i \oplus C_j \oplus C_{ij}$ he realitzat 1000 experiments. En aquests experiments he generat una clau aleatòria K de 128 bits i un text aleatori M de longitud entre 1 i 128 bits. Seguidament els he xifrat utilitzant ECB, i a continuació he agafat valors aleatoris per a i i j. Un cop fet tot això he xifrat M, M_i, M_j i M_{ij} i he comprovat que es complís la igualtat per a la versió de l'AES amb la funció $ByteSubIdentitat$ però que no es complís per a la versió de l'AES estàndard.

   Els resultats han sigut els esperats amb un cas especial a destacar: quan $i == j$, tenim que $C_i = C_j$ i que $C_{ij} = C$. Aleshores en ambdues versions la igualtat es complirà.

2. Per observar les diferències entre la versió de l'AES estàndard i la versió amb la funció $ShiftRowIdentitat$ he realitzat 10 experiments. En aquests experiments he generat una clau aleatòria K de 128 bits i un text aleatori M de 128 bits. Seguidament els he xifrat utilitzant ECB, i a continuació he agafat valors aleatoris per a i. Un cop fet tot això he xifrat M i M_i, i he observat les diferències entre C i C_i.

   La conclusió més destacable és que els 4 primers bytes del bloc no canvien, mentre que la resta sí.

3. Per observar les diferències entre la versió de l'AES estàndard i la versió amb la funció $MixColumnIdentitat$ he realitzat 10 experiments. En aquests experiments he generat una clau aleatòria K de 128 bits i un text aleatori M de 128 bits. Seguidament els he xifrat utilitzant ECB, i a continuació he agafat valors aleatoris per a i. Un cop fet tot això he xifrat M i M_i, i he observat les diferències entre C i C_i.

   La conclusió més destacable és que només canvien 4 bytes consecutius del bloc, depenent de la i utilitzada.

2.2 Propagació de petits canvis

Canvis a M:

1. A la Figura 1 podem observar l'histograma del nombre total de bits que canvien amb cada modificació de M. Observem que el nombre total de bits modificats sembla ser en mitjana la meitat de la mida de bloc, és a dir, 64 bits.

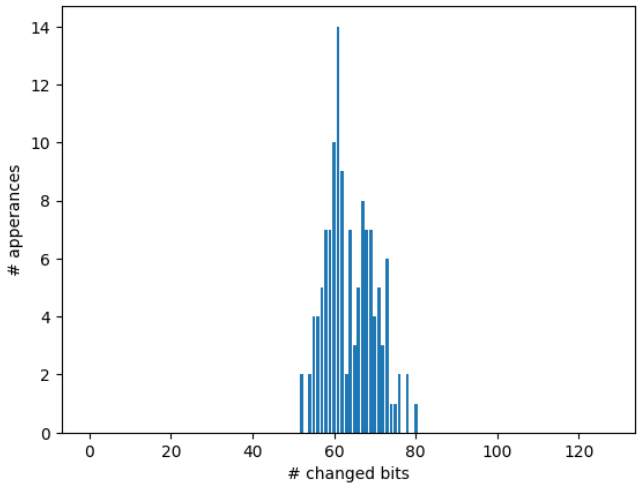

Figure 1: Histograma del nombre total de bits que canvien amb cada modificació de M.

2. A la Figura 1 podem observar l'histograma de les posicions que canvien amb cada modificació de M. Observem que totes les posicions es modifiquen aproximadament en la mateixa magnitud.

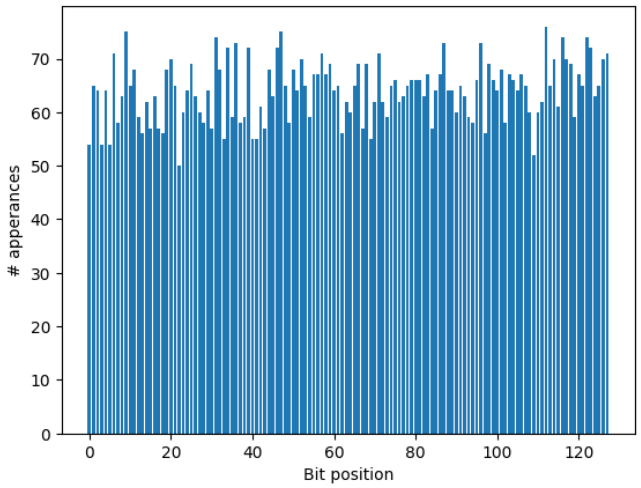

Figure 2: Histograma de les posicions que canvien amb cada modificació de M.

Canvis a K:

A la Figura 3 podem observar l'histograma del nombre total de bits que canvien amb cada modificació de K. Observem que un altre cop, el nombre total de bits modificats sembla ser en mitjana la meitat de la mida de bloc, és a dir, 64 bits.

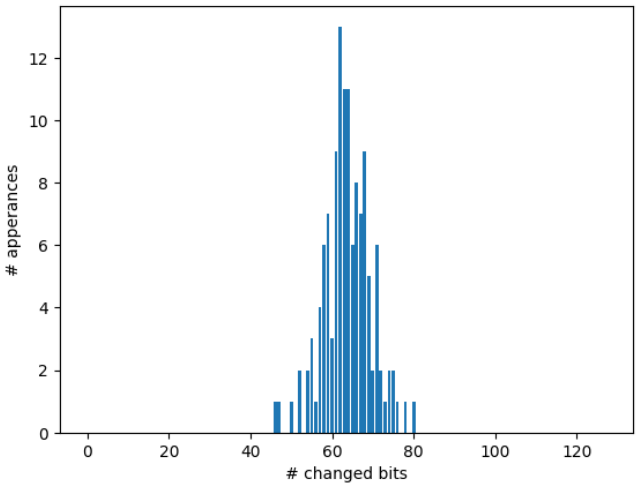

Figure 3: Histograma del nombre total de bits que canvien amb cada modificació de K.

A la Figura 4 podem observar l'histograma de les posicions que canvien amb cada modificació de K. Observem que de nou, totes les posicions es modifiquen aproximadament en la mateixa magnitud.

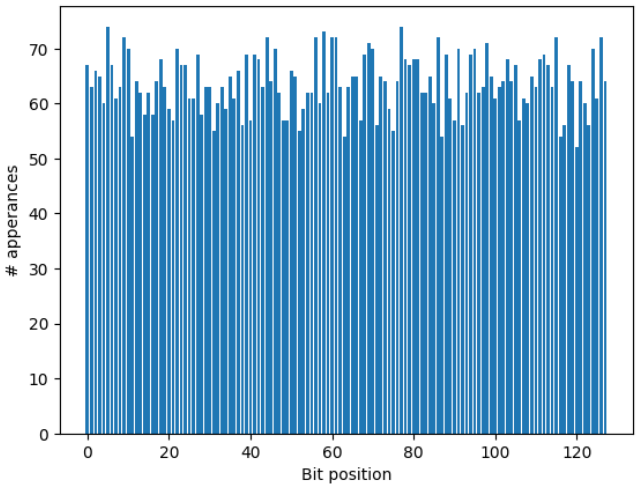

Figure 4: Histograma de les posicions que canvien amb cada modificació de K.

Per tant, podem concloure que és irrellevant quin bit és canviï, si un de M o un de K.

3 Criptografia de clau secreta

1. Per desencriptar el fitxer enviat he implementat la meva pròpia versió de desencriptació de l'AES. El resultat de desencriptar el fitxer enviat és visible a la Figura 5.

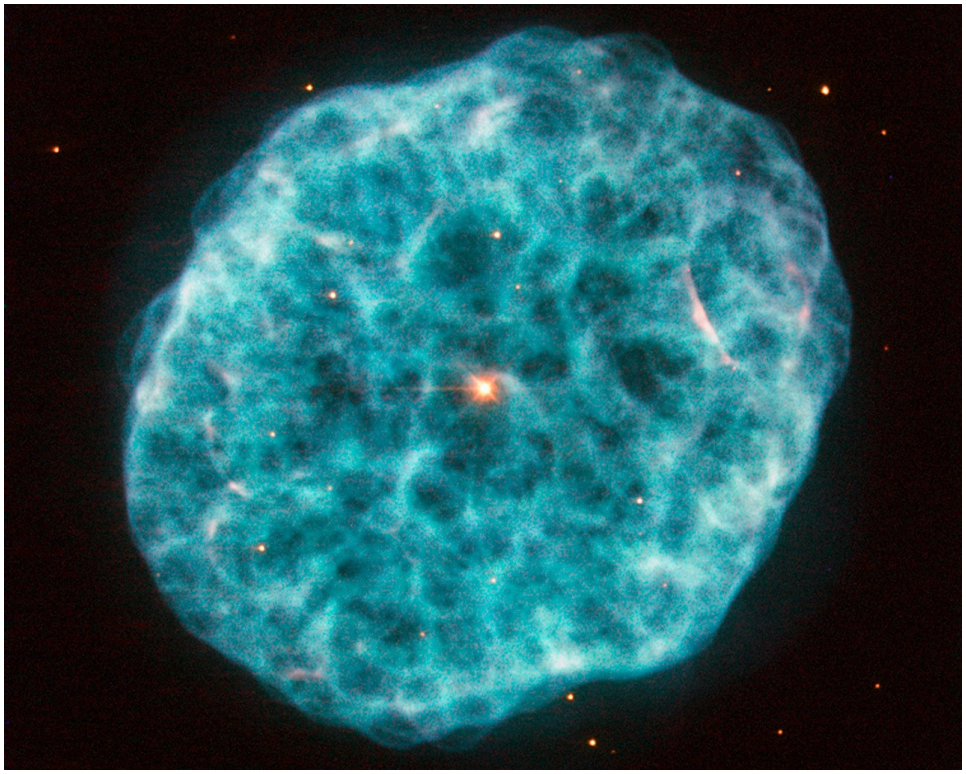

Figure 5: 2017_09_26_13_22_54_mario_fernandez.enc desencriptat.

2.