0 Introducció

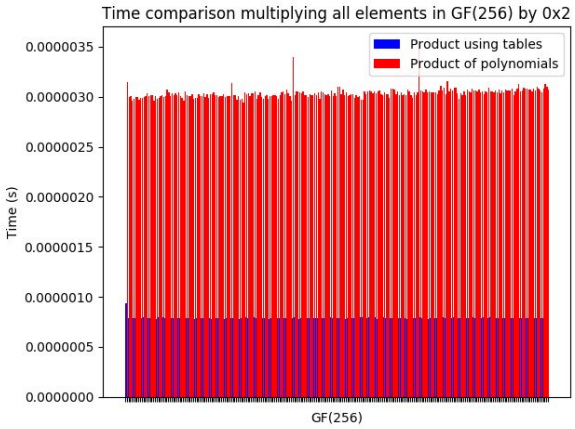
Aquesta pràctica ha sigut realitzada per Héctor Baiges Sánchez i Rubén González López. Aquest document pretén resumir els punts més importants de la pràctica.

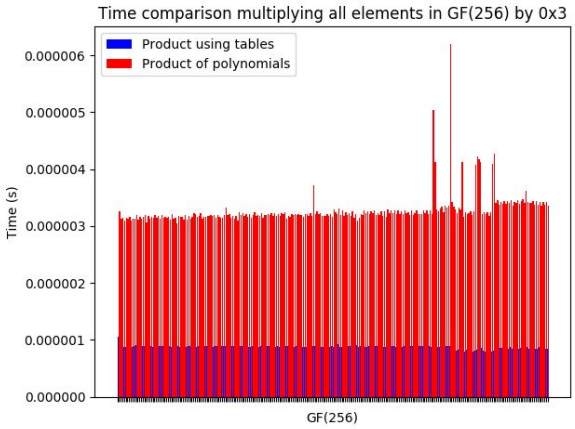
1 El cos finit GF (256)

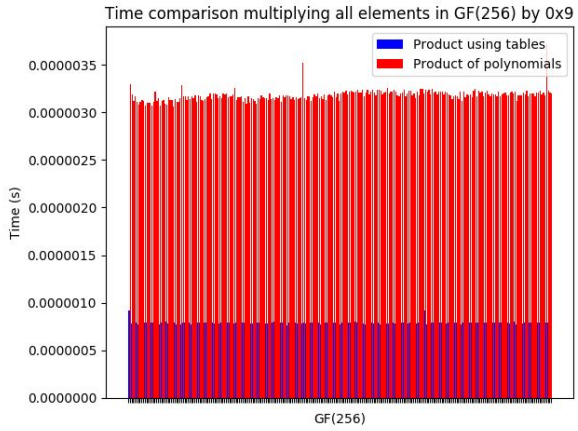
En el arxiu GF256.py estan definides les següents funcions:

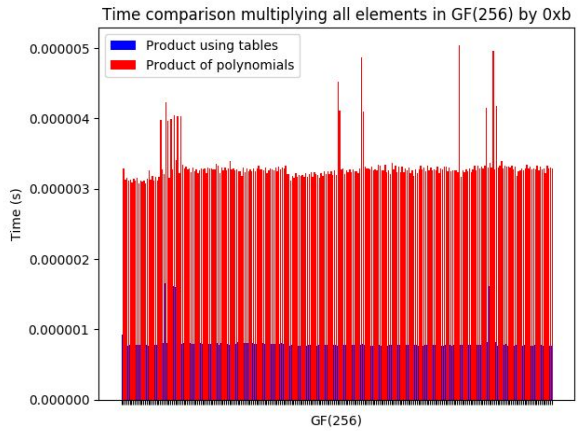
- GF_product_p(a, b)
- GF_es_generador(a)
- GF_tables()
- GF_product_t(a, b)
- GF_invers(a)

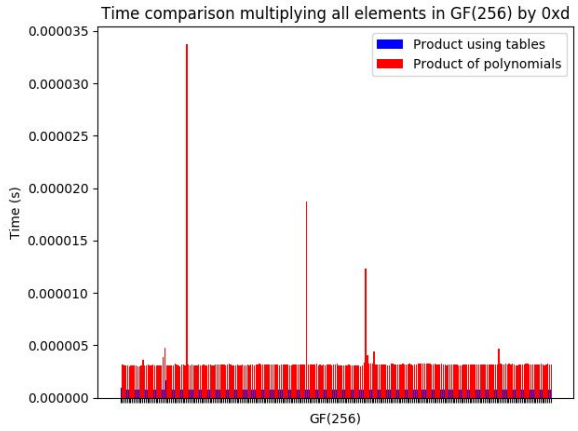
Per tal de mesurar el temps de les funcions de productes, hem utilitzat les llibreries de *time*, per tal de saber el temps d'execució de GF_product_p(a, b) i GF_product_t(a, b); *numpy* i *matplotlib* per visualitzar els temps en les gràfiques següents.

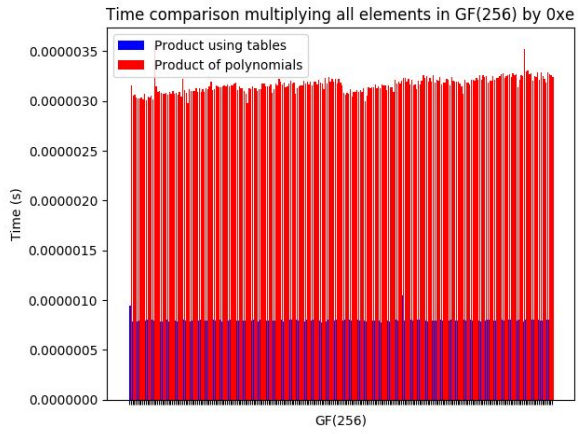












Com podem observar, el producte amb taules és molt més ràpid que el producte polinòmic.

2 Advanced Encryption Standard (AES)

2.1 Efectes de les funcions elementals

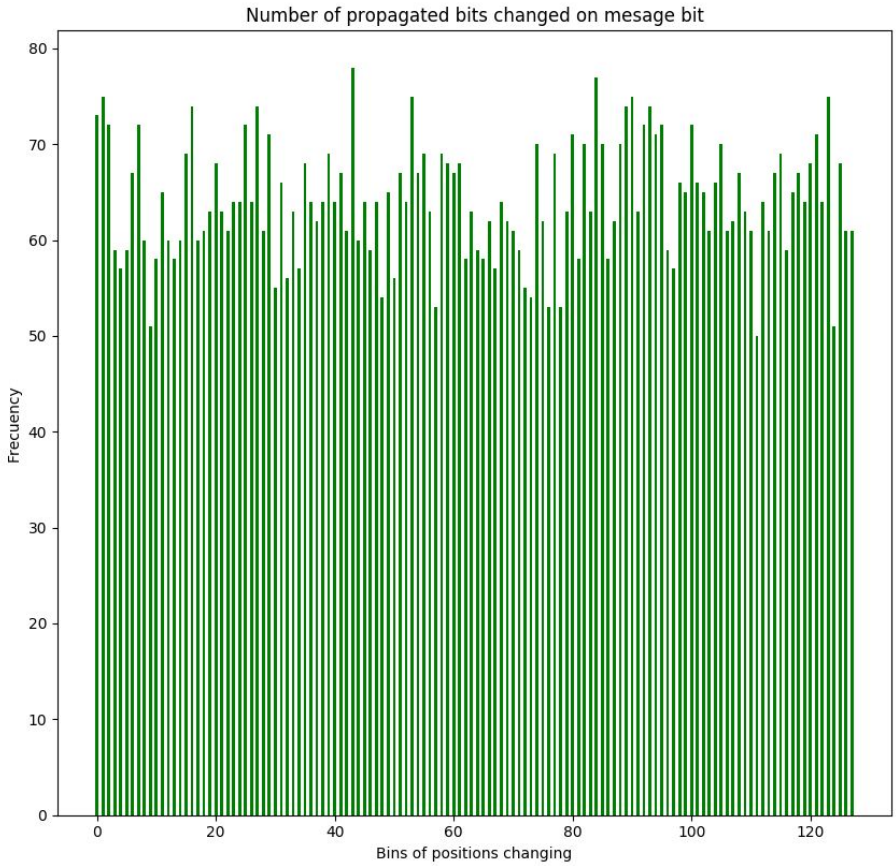
El programa que s'encarrega de comprovar els efectes de canviar les funcions demanades de l'AES per la identitat es troba en ExerciciAES_2.1.py, en el que s'executen les següents funcions:

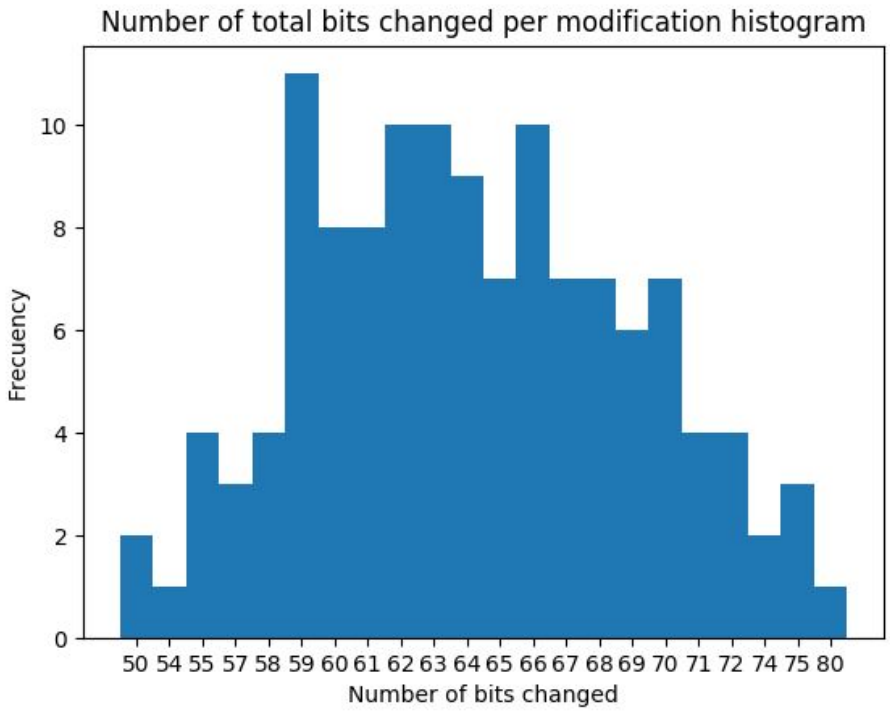
- subByteTest_identidad(): fitxats M, K i canviant la funció de subByte per l'identitat, comprova que C **=** Ci ⊕ Cj ⊕ Cij per tot i, j.
- subByteTest(): fitxats M ,K i deixant la funcio de subByte, comprova que C **!=** Ci ⊕ Cj ⊕ Cij per tot i, j.

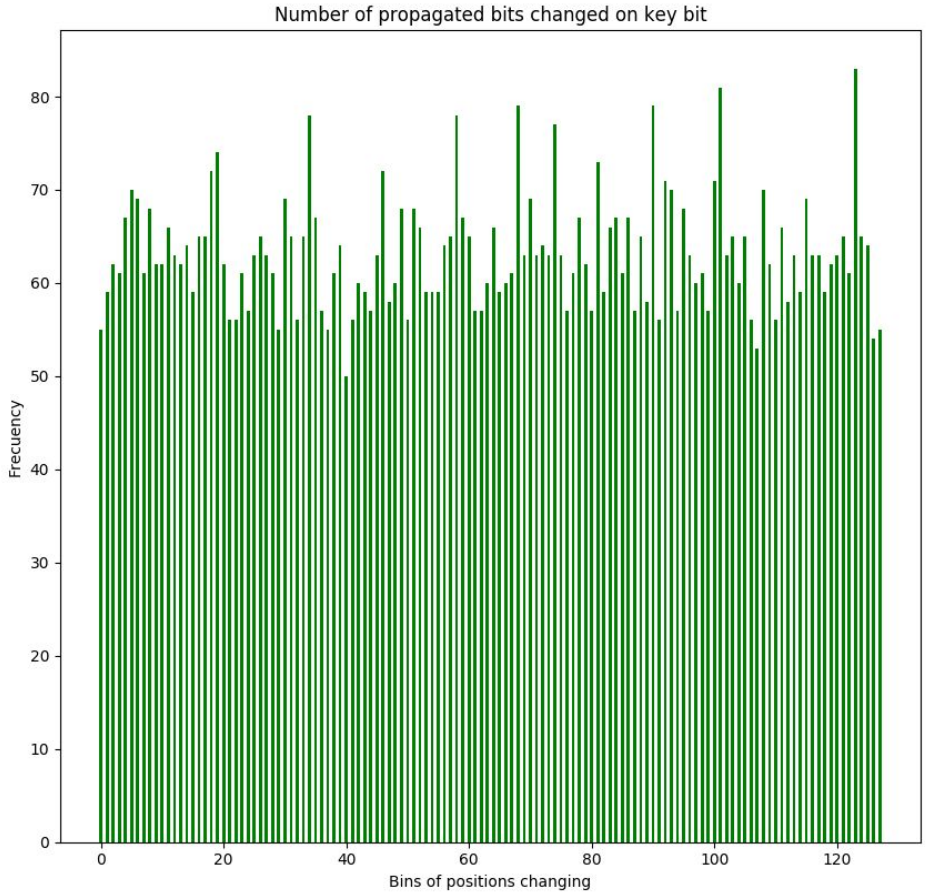
- shiftRowsTest_identidad(): Al canviar la funció de shiftRows per l'identitat, veiem que els canvis només es manifesten en la columna del canvi.
- mixColumnsTest_identidad():Al canviar la funció de mixColumns per l'identitat, veiem que els canvis només es manifesten en un únic byte.

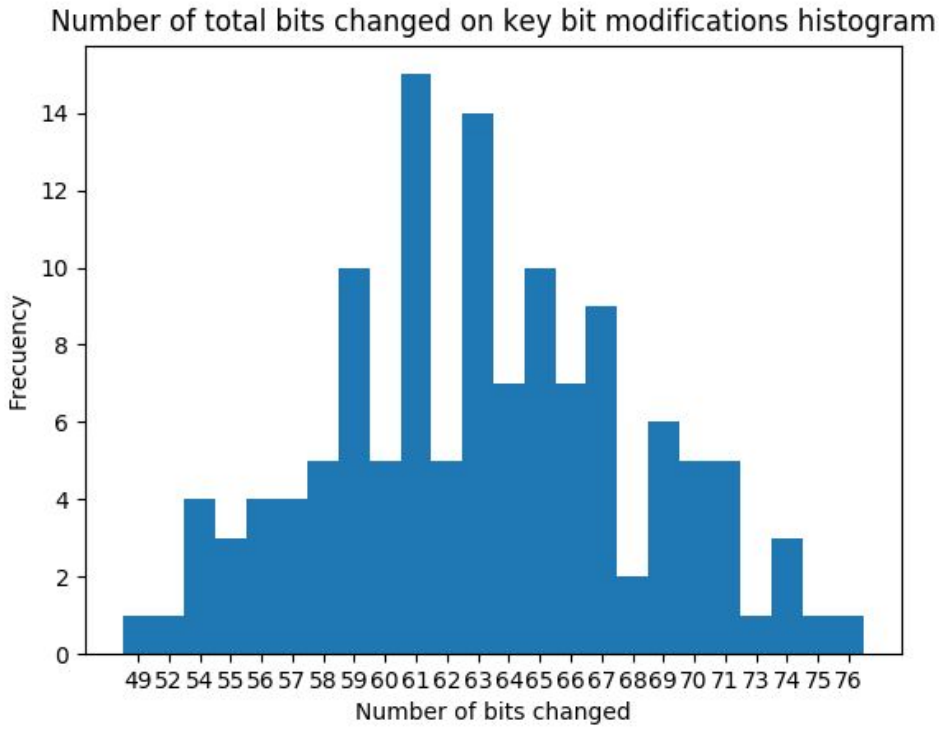
2.2 Propagació de petits canvis

En les següents gràfiques podem observar que la propagació dels bits, tant en el missatge com en la clau, segueixen més o menys freqüències semblants (si es realitzés el mateix gràfic amb la mitjana d'una multitud de missatges i claus diferents, la freqüència dels bits propagats seria la mateixa). Amb el nombre de bits canviats es pot veure que segueix aproximadament una normal (si es realitzés el mateix gràfic amb la mitjana d'una multitud de missatges i claus diferents, seguiria totalment una distribució normal).




Number of total bits changed per modification histogram
Frecuency
0
2
4
6
8
10
50 54 55 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 74 75 80
Number of bits changed


Number of propagated bits changed on key bit
Frecuency
0
10
20
30
40
50
60
70
80
0
20
40
60
80
100
120
Bins of positions changing



2.3 Ús com a funció unidireccional

- Quin és el màxim nombre de 0 inicials que heu trobat als diferents C? Doneu M i K en hexadecinal.

  El màxim nombre de 0 inicials a C ha sigut tot C a 0x0. S'ha trobat amb
  M=0XFE92EFBD3753A16437620860CEF11A25
  K=0xABABABABA19291879EDEDEDE09753883

- Quantes proves heu fet?

  Hem realitzat una prova, desxifrant un missatge C=0x0, am la key K=0xABABABABA19291879EDEDEDE09753883, i hem obtingut un missatge que al xifrar-ho obtenim el C=0x0

3 Criptografia de clau secreta

- El primer fitxer está desxifrat en el arxiu : 2019_09_25_17_00_56_hector.baiges.dec
- El segon fitxer, la "puerta trasera" está desxifrat en el arxiu : 2019_09_25_17_00_56_hector.baiges.puerta_trasera.dec