Segona entrega: Clau secreta

Albert López Alcácer

November 6, 2017

1 Introducció

Aquest document té l'objectiu de donar algunes explicacions sobre la segona entrega, en les seccions en les que calgui especificar alguna cosa més apart del codi en Python.

2 Definició de funcions utils i comparació de temps

2.1 El codi

Al fitxer GFHelpers.py hi han les diferents funcions:

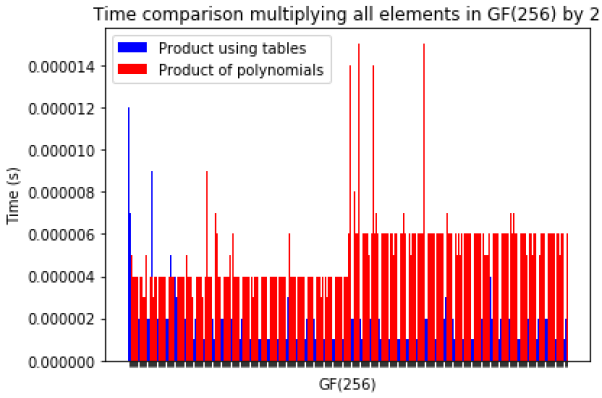
- GF_product_p(byte a, byte b)
- GF_tables()
- GF_product_t(byte a, byte b)
- GF_generador()
- GF_invers(byte a)

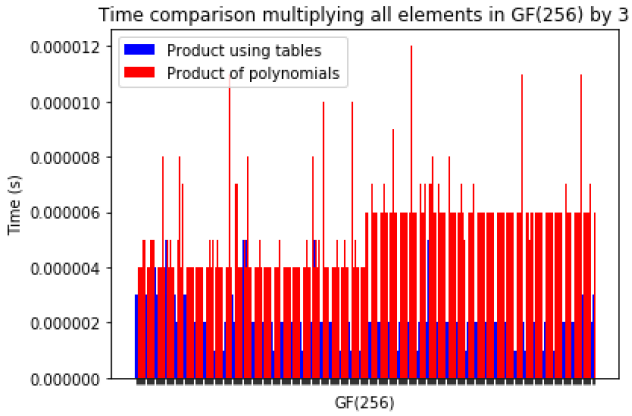
El codi que calcula els diferents temps d'execució per a comparar la multiplicació amb polinomis i accedint a les taules està a ProductTimeReport.py. En aquest codi hi han les funcions:

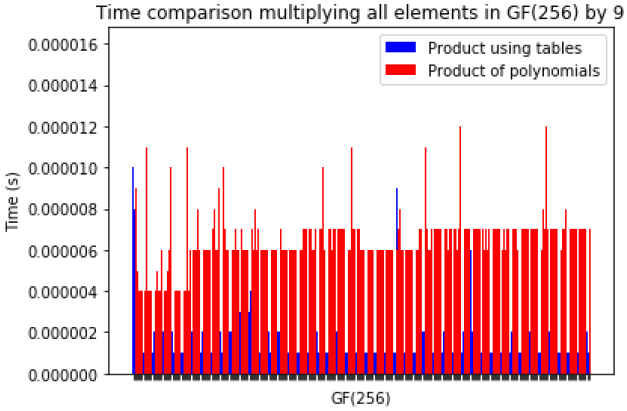
- timeForGF_product_T(a, b)
  Que, una vegada ha obtingut les taules exponencial i logarítmiques, fa servir la llibreria time per calcular la diferència de temps (process_time) en fer la multiplicació amb aquestes taules de a i b.
- timeForGF_product_P(a, b)
  Que calcula la diferència de temps fent servir la multiplicació de polinòmis.
- GF_product_TvsGF_productP(n_runs, b)
  Que fa la mediana per descartar resultats frontera dels n_runs execucions. Per a cada valor b dels [0x02, 0x03, 0x09, 0x0B, 0x0D, 0x0E] de l'enunciat es realitzarà la multiplicació amb tots els valors del cos finit GF(256). Fa servir les funcions anteriors.

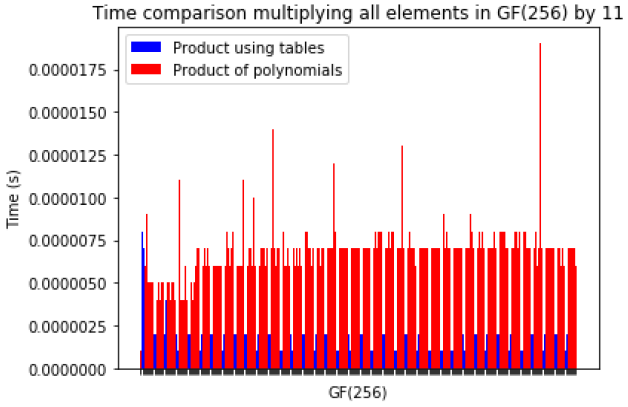
2.2 Taules comparatives

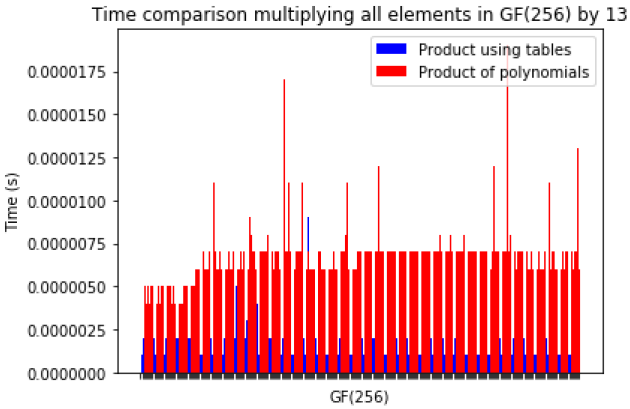
Per a mostrar les diferencies de temps que hi han realitzant la multiplicació de dos elements del cos finit fent servir les taules logarítmiques i exponencials o fent la multiplicació en representació polinómica, mostro un bar chart per a cada valor dels [0x02, 0x03, 0x09, 0x0B, 0x0D, 0x0E] de l'enunciat. En cada gràfic es multiplica el valor per tots els del cos finit per visualitzar la diferència de temps:

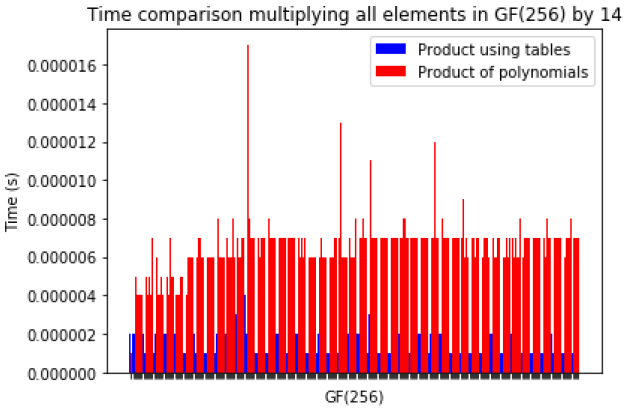
1. 

2. 

3. 

4. 

5. 

6. 

3 Advanced Encryption Standard

S'ha fet servir la implementació del AES:
GitHub bozhu/AES-Python

3.1 Efectes de les funcions elementals

El fitxer CSecreteAes.py fa servir la implementació del AES per a observar els efectes de les diferents funcions elementals.
S'ha fet una subclasse per a cada funció, en la que aquesta es sobreescriu la funció elemental corresponent per a no fer res.

- AesWoByteSub(aes.AES)
- AesWoShiftRows(aes.AES)
- AesWoMixColumns(aes.AES)

Els diferents tests per veure els efectes son:

- byteSubEffectTest()
  En el que s'observa com substituir els bytes de les columnes de l'estat del AES per els de la S-Box permet que no existeixi la linearietat del "assert" del codi. A la construcció de la S-Box, la inversa en el cos finit GF(256) treu linearietat i la multiplicació afí trenca l'estructura algebràica d'aquest cos.
- shiftRowsEffectTest()
  En el que modifiquem un bit respecte al missatge original per a veure que al text xifrat la única columna diferent es la mateixa on s'ha modificat el bit. Així doncs, shift rows serveix per a introduir difussió a l'AES fent que en cada ronda l'input de mix columns siguin grups de bytes diferents.
- mixColumnsEffectTest()
  En el que en modificar un bit al missatge, fa que nomes en depengui un byte d'aquesta modificació. (Encara menys propagació de canvis)

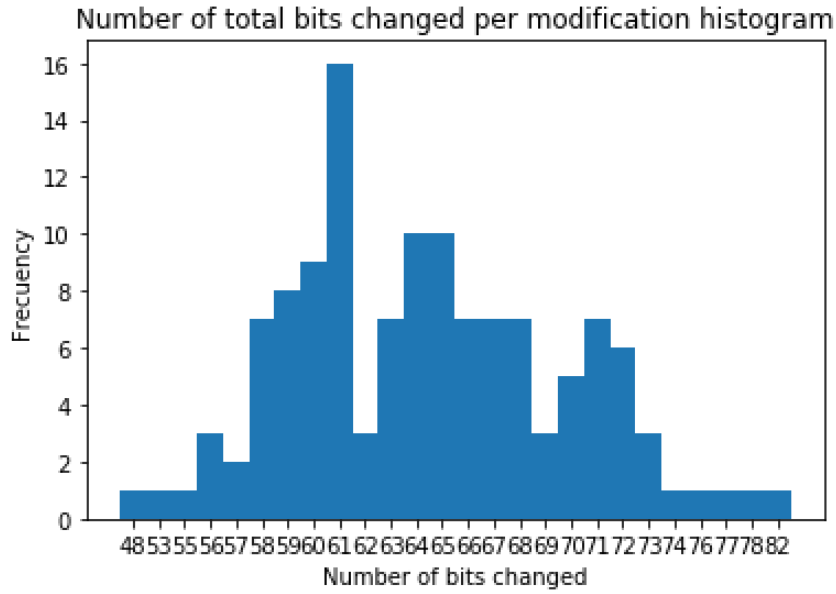
En general doncs, mixColumns juntament amb shiftRows fan que cada byte de la matriu obtinguda de xifrar el missatge depengui dels 16 bytes d'aquest.

3.2 Propagació de petits canvis

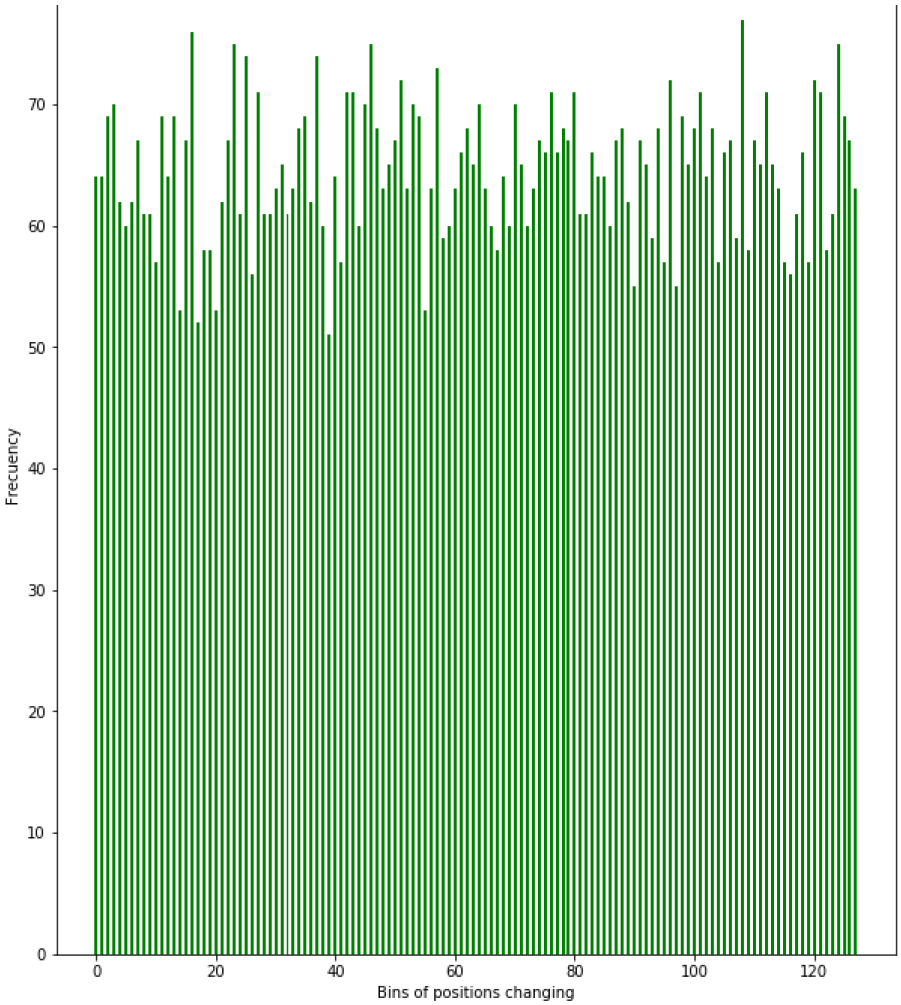
La estadística de la propagació de canvis esta al fitxer PropagationHistograms.py

3.2.1 Al missatge

- Histograma del nombre total de bits que canvien amb cada modificació:

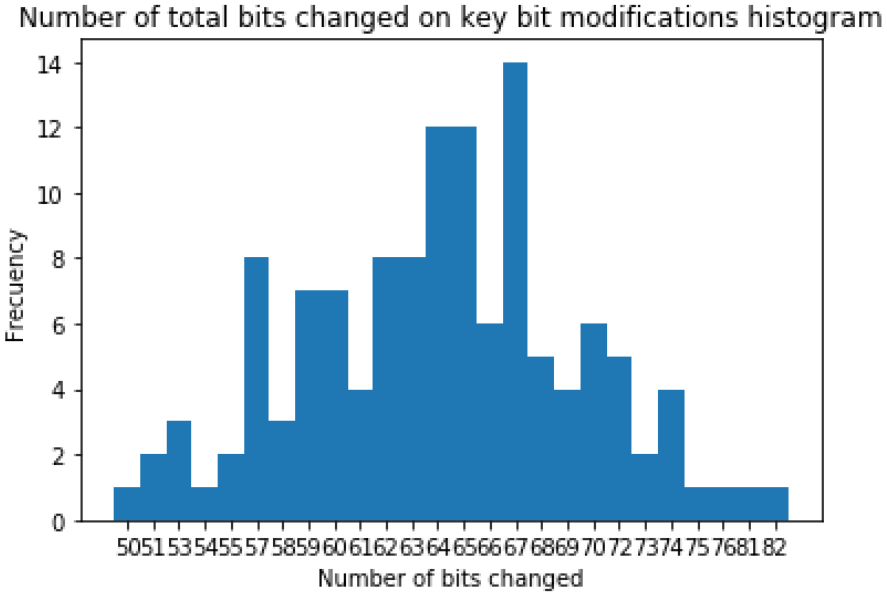


- Histograma de les posicions que canvien amb cada modificació:

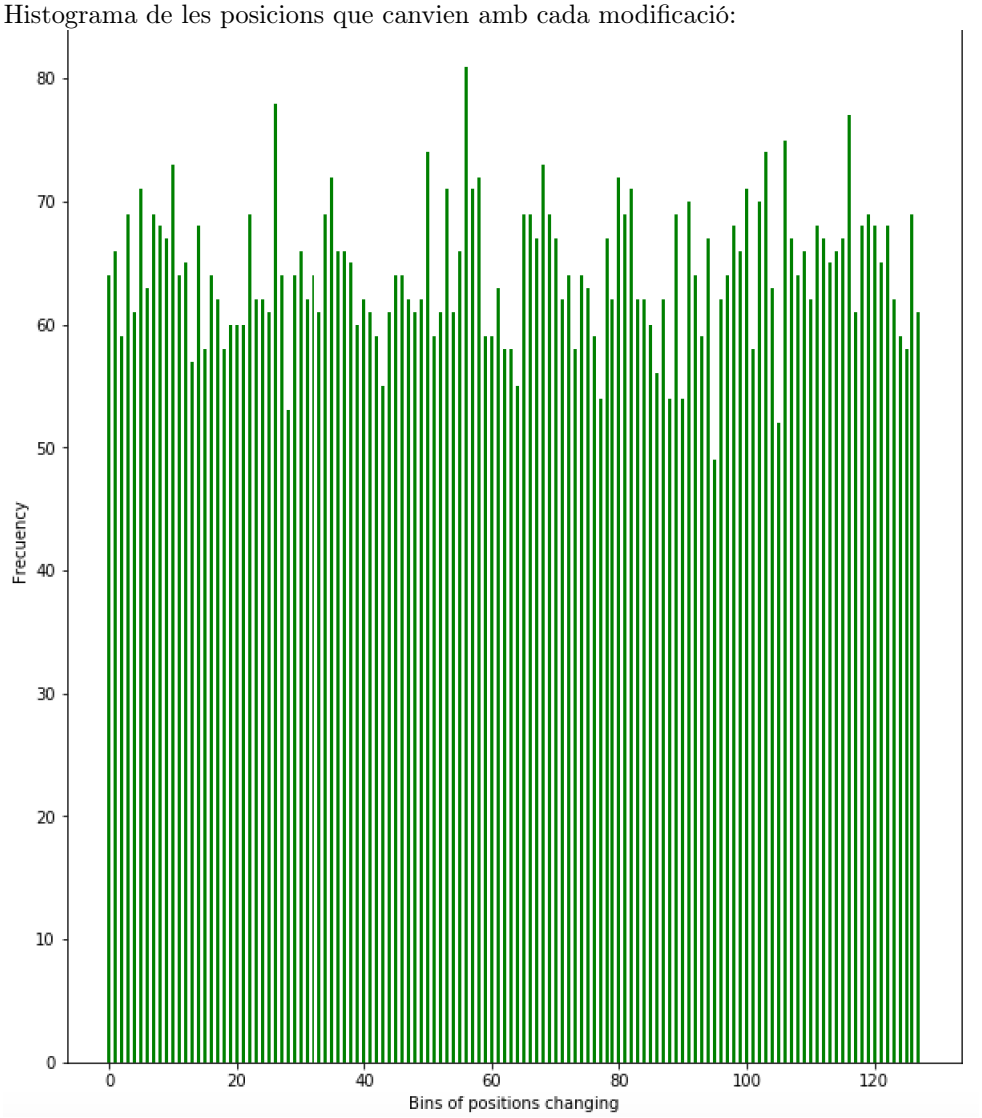


3.2.2 A la clau

- Histograma del nombre total de bits que canvien amb cada modificació:



- Histograma de les posicions que canvien amb cada modificació:



4 Criptografía de clau secreta

- El primer fitxer esta desxifrat i és:
  2017_09_26_13_22_04_albert.lopez.alcacer.dec: JPEG image data
- El segon ha estat desxifrat (fent força bruta del element "kiv") i és:
  2017_09_26_13_22_04_albert.lopez.alcacer.puerta_trasera.dec: JPEG image data