Facultat d'Informàtica de Barcelona

Quadrimestre de tardor, 2022/2023

Tercera pràctica de Criptografia

RSA

Guillem González Valdivia
(guillem.gonzalez.valdivia@Estudiantat.upc.edu)
Daniel Morón Roces
(daniel.moron.roces@Estudiantat.upc.edu)

Índex

1 BlockChain

A la primera part de la pràctica hem implementat una BlockChain simple per tal d'entendre millor el seu funcionament. Tots els codis i documents relacionats els adjuntem al fitxer comprimit final de l'entrega.

1.1 Taula amb temps per firmar amb diferents modes

Com es pot observar a la taula que hem generat a partir del codi rsa1.py, hem mesurat el temps de signatura per 100 missatges diferents variant la quantitat de bits de la clau i el fet d'utilitzar o no el teorema xinès del residu (TXR), el qual és un resultat d'aritmètica modular que tracta de la resolució de sistemes de congruències.

A l'hora de firmar un missatge, podem veure que la quantitat de temps emprat és directament proporcional a la quantitat de bits de la clau, la qual cosa té sentit, ja que és més difícil computacionalment elevar a un nombre molt gran que a un nombre més petit. Per poder firmar el missatge el que s'ha de fer és elevar el missatge a l'exponent privat d de la clau privada i això que sigui congruent mòdul n. Aquí mostrem els diferents resultats que hem obtingut:

Bits Modulo	Tiempo con TXR	Tiempo sin TXR
512	0.12321615219116211	0.29004955291748047
1024	0.6291553974151611	1.9852490425109863
2048	4.076637268066406	14.014976024627686
4096	28.417673587799072	97.55249547958374

Un altre factor important a tenir en compte és que si s'utilitza el teorema xinès del residu es redueix considerablement el temps necessari per firmar. L'objectiu principal al final és calcular el missatge elevat a l'exponent privat, concretament, volem calcular el següent: x = m$\hat{d}$ mod n

On n = p * q. Tenim: x és congruent amb a (mod p) i x és congruent amb b (mod q). Gràcies a l'identitat de Bezout, podem deduir que x = q*q' * a + p*p' * b, on q' és l'invers de q mod p i p' és l'invers de p mod q. D'aquesta manera, podem calcular a i b, ja que a seria d mod (p-1) i b seria d mod (q-1).

Tot i que sembli més costós, a l'hora de fer els càlculs és molt més efectiu utilitzar el TXR, ja que l'altra forma de calcular m$\hat{d}$ implica utilitzar la funció pow en python fent: pow(m,d mod phi_n, n), i aquesta opció consumeix molts més recursos. Per aquest mateix motiu, es pot analitzar veient les taules que és molt més ràpid firmar utilitzant el TXR.

2 RSA

Al fitxer comprimit de l'entrega adjuntem tots els documents esmentats a l'enunciat, concretament els fitxers desencriptats, els fitxers en format PEM i els fitxers amb les claus secretes que s'han utilitzat per l'AES.

3 Referències

https://www.dlitz.net/software/pycrypto/api/2.6/Crypto.Cipher.AES-module.html