CRIPTOGRAFIA

MAT - FIB

Entrega

Pels càlculs podeu fer servir *SAGE*.

1. Trobeu a la xarxa un lloc web que presenti un certificat amb una clau pública que sigui un punt d'una corba el.líptica. Doneu el punt i la corba que fa servir.

   Fent servir aquesta corba:

   (a) Trobeu la clau pública associada a la clau privada que és l'enter obtingut de concatenar 8 vegades les xifres del vostre DNI.

   (b) Trobeu, si existeix, una clau pública que tingui per primera component el vostre DNI. Podeu trobar la clau privada associada?

   Si no existeix, trobeu una clau pública que tingui per xifres més significatives el vostre DNI. Podeu trobar la clau privada associada?

   (c) Amb les claus trobades als apartats anteriors, signeu el missatge que, el seu hash en hexadecimal, coincideix amb el vostre DNI.

   (d) Amb les signatures trobades als apartats anteriors i el mateix missatge, calculeu la clau secreta que s'obtendria fent servir com a nombre aleatori s el que, en hexadecimal, coincideix amb el vostre DNI.

2. A https://www.bsi.bund.de/EN/Topics/ElectrIDDocuments/CSCAcertGermany/cscaGermany_node.html trobareu la clau pública de The German Country Signing CA (CSCA)Main Public Key Certificate Certificate 4[1].

   Doneu el punt i la corba que fa servir.

Referències

RFC 5480: Elliptic Curve Cryptography Subject Public Key Information

Standards for Efficient Cryptography Group (SECG), "SEC 1: Elliptic Curve Cryptography"

Per llegir

Sony PS3 Security Broken. PS3 Epic Fail, pàgines 122-133 Console Hacking 2010. 27th Chaos Communication Congress.

Un petit exemple en Sage

```
p=0x008cb91e82a3386d280f5d6f7e50e641df152f7109ed5456b412b1da197fb7...
  ...1123acd3a729901d1a71874700133107ec53

punto=(0x6bfbeec69de72c66a668ece1aaf1a264a3c9b288fb32d059e92c3e5d5...
```

[1]Si feu servir *openssl x509* per veure la clau pública he de dir-li que el certificat està en format DER

```
  ...bd4d7b5014878f4479c13c883d054555cd90ecd,
  0x136ec4cc346489cdd64e6943f333864ab9dfe442dcbf8f69c19e71d035ff31...
  ...7fc032fc2155caeaa65b493d191d399ac0)

a=0x7bc382c63d8c150c3c72080ace05afa0c2bea28e4fb22787139165efba91f9...
  ...0f8aa5814a503ad4eb04a8c7dd22ce2826

b=0x04a8c7dd22ce28268b39b55416f0447c2fb77de107dcd2a62e880ea53eeb62...
  ...d57cb4390295dbc9943ab78696fa504c11

Generador=(0x1d1c64f068cf45ffa2a63a81b7c13f6b8847a3e77ef14fe3db7fc...
  ...afe0cbd10e8e826e03436d646aaef87b2e247d4af1e,
  0x8abe1d7520f9c2a45cb1eb8e95cfd55262b70b29feec5864e19c054ff99129...
  ...280e4646217791811142820341263c5315)

orden=0x008cb91e82a3386d280f5d6f7e50e641df152f7109ed5456b31f166e6c...
  ...ac0425a7cf3ab6af6b7fc3103b883202e9046565

Px=punto[0]
Py=punto[1]
mod(Py**2,p)-mod(Px**3+a*Px+b,p)

Gx=Generador[0]
Gy=Generador[1]
mod(Gy**2,p)-mod(Gx**3+a*Gx+b,p)

# Defino la curva
Zp= Zmod(p)
E = EllipticCurve(Zp,[a,b]);

# Defino dos puntos
G = E([Gx,Gy])
P = E([Px,Py])

# Punto del infinito
orden*G
```

$$(0 : 1 : 0)$$

```
2*P+G
```

$$(344347803282129877776932428213988787461141815132564776123309564 2...$$
$$...4094413223261633561348476432661330719096979326126 28 :$$
$$1842107221448116526861623271245585862876778735571430832108887585...$$
$$...3613808852319731362989064276245464841666408395212922 : 1)$$