1.ECC

Per a la realització d'aquesta secció s'ha fet ús del fitxer *Wikipedia.org.pcpapng,* el qual conté la informació de totes les connexions en el moment d'establir contacte amb Wikipedia.org.

Les claus generades per *Firefox* que permeten llegir les seccions encriptades del protocol TCLS es poden trobar en l'arxiu *Keys.txt.*

Els paquets utilitzats per a la realització de la pràctica han estat els següents:

- **[170] Client Hello**
- **[172] Server Hello, Change Cipher Spec, Encrypted extensions**
- **[174] Certificate, Certificate Verify, Finished**

De *Server Hello* podem extreure que el *Cipher Suite* és **TLS_AES_256_GCM_SHA384.**

De *Certificate* obtenim la clau pública de wikipedia (punt de la corba elíptica).

04 e8 50 2c d0 d2 4e a2 b1 92 aa b6 73 0f cf a0 b4 57 e5 c2 c0 7c ae 6e 55 91 4a a6 94
67 fa a5 f8 b0 3f 46 ac 23 52 b4 48 3b 64 64 fb ea cd e9 e4 fb 8f 10 a7 f4 e8 23 ba 95 29 6e ef ca 72 bb 83

De *Certificate Verify* obtenim l'algoritme de signatura: *edcsa_secp256r1_sha256.* Per tant, estem utilitzant la corba p-256.

Les característiques de la mateixa han estat consultades en el següent document publicat pel NIST: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

L'arxiu *ecc.py* conté el codi necessari per a respondre les preguntes proposades en aquest apartat.

Amb l'objectiu de facilitar la consulta de les mateixes, adjunto en aquest document les respostes obtingudes:

a) L'ordre de la curva és primer.
b) El punt utilitzat com a clau publica per *Wikipedia.org* és un punt de la corba *secp256r1.*
c) L'ordre del punt será igual a l'ordre de la corba. Com ja sabem, l'ordre d'un punt és divisor de l'ordre de la corba. Degut a que en l'apartat a) hem comprovat que aquest valor es un número primer, els dos únics divisors possibles són 1 y ell mateix. Per tant, degut a que el punt proporcionat no és el punt de l'infinit, aquest disposar del

mateix ordre que el mencionat anteriorment. Aquest raonament pot ser comprovat realitzant el càlcul utilitzant *SageMath:*

```
In [14]: p256  = 115792089210356248762697446949407573530086143415290314195533631308867097853951
         FF = GF(p256)
         a256 = p256-3
         b256 = 0x5AC635D8AA3A93E7B3EBBD55769886BC651D06B0CC53B0F63BCE3C3E27D2604B
         EC = EllipticCurve([FF(a256), FF(b256)])
         Qx = 0xe8502cd0d24ea2b192aab6730fcfa0b457e5c2c07cae6e55914aa69467faa5f8
         Qy = 0xb03f46ac2352b4483b6464fbeacde9e4fb8f10a7f4e823ba95296eefca72bb83

In [15]: P = EC(Qx,Qy)

In [18]: P.order()

Out[18]: 115792089210356248762697446949407573529996955224135760342422259061068512044369
```

d) La signatura és correcta.

2. Certificats digitals

Per realitzar aquesta secció he obtingut, fent ús del navegador *Firefox*, els següents arxius:

- TERENASSLCA3.crl
- DigiCertAssuredIDRootCA.crt
- TERENASSLCA3.crt

a) Per poder veure el nombre de certificats revocats que conté la CRL, en primer lloc he convertit l'arxiu original a un document de text, fent ús *OpenSSL:*
openssl crl -inform DER -text -in TERENASSLCA3.crl -out TERENASSLCA3.txt

Disposant de *TERENASSLCA3.txt,* podem contar la quantitat de *Revoked certificates*, sent aquesta 2158.

b) Per poder realitzar aquesta secció en primer lloc hem de convertir els dos certificats a format *.pem*. Aquesta operació s'ha realitzat amb *OpenSSL* utilitzant les següents comandes:

openssl x509 -inform DER -in DigiCertAssuredIDRootCA.crt -out DigiCertAssuredIDRootCA.pem -text

openssl x509 -inform DER -in TERENASSLCA3.crt -out TERENASSLCA3.pem -text

Per obtenir l'estat del certificat a la OCSP, sent aquesta http://ocsp.digicert.com, tal i com es mostra en el certificat, podem fer ús de la següent comanda:

openssl ocsp -issuer DigiCertAssuredIDRootCA.pem -cert TERENASSLCA3.pem -url http://ocsp.digicert.com

Obtenint la següent resposta:

WARNING: no nonce in response
Response verify OK
TERENASSLCA3.pem: good
This Update: Dec 24 19:02:08 2021 GMT
Next Update: Dec 31 19:02:08 2021 GMT

Com podem comprovar, actualment l'estat del certificat és **good** i aquest, com a mínim, es mantindrà fins a la següent actualització, que es realitzarà el 31-12-2021.