

## Entrega

1. Enregistreu una connexió segura amb [www.wikipedia.org](http://www.wikipedia.org) que faci servir ECDHE-ECDSA.
  - (a) Doneu els noms de les corbes que es fan servir per acordar la clau DH i per la clau pública del servidor.
  - (b) Comproveu que el nombre de punts (ordre) de la corba que es fa servir al certificat és primer.
  - (c) Comproveu que la clau pública  $P$  de [www.wikipedia.org](http://www.wikipedia.org), és realment un punt de la corba.
  - (d) Calculeu l'ordre del punt  $P$ .
  - (e) Comproveu que la signatura ECDSA és correcta.

Pels càlculs podeu fer servir *SAGE*.

2. Feu el mateix però amb una connexió amb [google.com](http://google.com).
3. Enregistreu una connexió segura amb [www.fib.upc.edu](http://www.fib.upc.edu). En aquesta connexió us faran arribar el certificat i el seu estatus.
  - (a) En el certificat es dona un punt de distribució de la CRL de l'autoritat certificadora. Quants certificats revocats conté la CRL?
  - (b) Quin és l'estatus del certificat i fins quan és vàlid aquest estatus?

## Entrega

1. Els tres fitxers amb les captures de les connexions.
2. Els càlculs i les comprovacions demanades als dos primers punts o, en el seu defecte, una explicació de perquè no s'han fet.
3. La CRL de l'últim punt i les respostes a les dues preguntes.

## Referències

FIPS 186-4 Digital Signature Standard, <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf>

The Transport Layer Security (TLS) Protocol Version 1.2, <https://tools.ietf.org/html/rfc5246>

The Transport Layer Security (TLS) Protocol Version 1.3, <https://tools.ietf.org/html/rfc8446>

Elliptic Curve Cryptography (ECC) Cipher Suites for TLS, <https://tools.ietf.org/search/rfc4492>

RFC 5480: Elliptic Curve Cryptography Subject Public Key Information, <https://tools.ietf.org/html/rfc5480#section-2.2>

Standards for Efficient Cryptography Group (SECG), "SEC 1: Elliptic Curve Cryptography", <http://www.secg.org/sec1-v2.pdf>

Openssl x509 - Certificate utility, <https://www.openssl.org/docs/manmaster/man1/x509.html>

Openssl crl - CRL utility, <https://www.openssl.org/docs/manmaster/man1/crl.html>

## Un petit exemple en Sage

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

```
punto=(0x6bfbeec69de72c66a668ece1aaf1a264a3c9b288fb32d059e92c3e5d5...
...bd4d7b5014878f4479c13c883d054555cd90ecd,
0x136ec4cc346489cdd64e6943f333864ab9dfe442dcbf8f69c19e71d035ff31...
...7fc032fc2155caaaa65b493d191d399ac0)
```

```
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

```
(3443478032821298777769324282139887874611418151325647761233095642...
...409441322326163356134847643266133071909697932612628 :
1842107221448116526861623271245585862876778735571430832108887585...
...3613808852319731362989064276245464841666408395212922 : 1)
```