ECC y certificados digitales

1. Capturad una conexión TLS 1.3 con www.wikipedia.org que use un certificado con una clave pública ECC (Elliptic Curve).

(a) Comprobad que el número de puntos (orden) de la curva usada en el certificado es primo.

In [3]:
```
p = 115792089210356248762697446949407573530086143415290314195533631308867097853951
n = 115792089210356248762697446949407573529996955224135760342422259061068512044369
a = -3
b =  0x5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
Gx = 0x6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
Gy = 0x4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5

# valores extraidos del campo subjectPublicKy con Wireshark
Qx = 0x3561f4211aff6ac43bfa0647c6196ebe7038f1dc16b1bc381412d4142b1c0b31
Qy = 0x8159f567f6e72ad13c1efaaea7ed065dd66f5d894c6bc8b0e00f83cff5d38ada
# valores extraidos del campo signature con Wireshark
F1=0x3aca1086dc42a307bd4bb18e7fb747631d3994ee17f10b2050f0257f6e84940a
F2=0x49e2cf69724f4b92bd5088a145fbdf9247e18638d233c95e94674a7c23ecadee
# 256 bits producto de la concatenación de los binarios
result = 0x835e7e10502008132404512b6a1274c6c41a7f2b2a563f6b209d2043ead3f4d5


EC = EllipticCurve(Zmod(p),[a,b])
if EC.cardinality().is_prime():
    print("El orden es primo")
```

Out[3]:
```
El orden es primo
```

(b)Comprobad que la clave pública P de www.wikipedia.org es realmente un punto de la curva. (c) Calculad el orden del punto P .

Al calcular el orden también verificamos que pertenezca a la curva.

In [4]:
```
p = 115792089210356248762697446949407573530086143415290314195533631308867097853951
n = 115792089210356248762697446949407573529996955224135760342422259061068512044369
a = -3
b =  0x5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
Gx = 0x6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
Gy = 0x4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5

# valores extraidos del campo subjectPublicKy con Wireshark
Qx = 0x3561f4211aff6ac43bfa0647c6196ebe7038f1dc16b1bc381412d4142b1c0b31
Qy = 0x8159f567f6e72ad13c1efaaea7ed065dd66f5d894c6bc8b0e00f83cff5d38ada
# valores extraidos del campo signature con Wireshark
F1=0x3aca1086dc42a307bd4bb18e7fb747631d3994ee17f10b2050f0257f6e84940a
F2=0x49e2cf69724f4b92bd5088a145fbdf9247e18638d233c95e94674a7c23ecadee
# 256 bits producto de la concatenación de los binarios
result = 0x835e7e10502008132404512b6a1274c6c41a7f2b2a563f6b209d2043ead3f4d5


EC = EllipticCurve(Zmod(p),[a,b])
if EC.cardinality().is_prime():
    print("El orden es primo")

Q = EC([Qx,Qy])
Q.order()
```

Out[4]:
```
El orden es primo
115792089210356248762697446949407573529996955224135760342422259061068512044369
```

(d) Comprobad que la firma ECDSA es correcta.

In [2]:
```
p = 115792089210356248762697446949407573530086143415290314195533631308867097853951
n = 115792089210356248762697446949407573529996955224135760342422259061068512044369
a = -3
b =  0x5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
Gx = 0x6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
Gy = 0x4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5

# valores extraidos del campo subjectPublicKy con Wireshark
Qx = 0x3561f4211aff6ac43bfa0647c6196ebe7038f1dc16b1bc381412d4142b1c0b31
Qy = 0x8159f567f6e72ad13c1efaaea7ed065dd66f5d894c6bc8b0e00f83cff5d38ada
# valores extraidos del campo signature con Wireshark
F1=0x3aca1086dc42a307bd4bb18e7fb747631d3994ee17f10b2050f0257f6e84940a
F2=0x49e2cf69724f4b92bd5088a145fbdf9247e18638d233c95e94674a7c23ecadee
# 256 bits producto de la concatenación de los binarios
result = 0x835e7e10502008132404512b6a1274c6c41a7f2b2a563f6b209d2043ead3f4d5

EC = EllipticCurve(Zmod(p),[a,b])
if EC.cardinality().is_prime():
    print("El orden es primo")

Q = EC([Qx,Qy])
# Q.order()

# Verificación firma
Punto = EC([Gx,Gy])
k = mod(result*F2^-1,n)
l = mod(F1*F2^-1,n)
verify = Integer(k)*Punto+Q*Integer(l)
if mod(verify[0],n) == F1:
    print("Firma válida")
else:
    print("Firma no válida")
```

Out[2]:
```
El orden es primo
Firma válida
```

Los valores utilizados para calcular Qx, Qy, F1 y F2 se han extraído de la captura wikipedia.pcapng y se pueden consultar en el archivo valores.txt. Por su parte, result sale de la concatenación de los 4 binarios, se crea usando el script ecc.py y su resultado se guarda en result.txt.

2. Conectaros con www.fib.upc.edu. En esta conexión os enviarán el certificado del servidor de la FIB.

(a) Obtened el periodo de validez del certificado y la clave pública (módulo y exponente, en base 10) del web de la FIB. ¿Cuántos dígitos tiene el módulo?

- **Periodo de validez:**
  Emitido en 2023-05-29 00:00:00 (UTC)
  Vencimiento en 2024-05-28 23:59:59 (UTC)
- **Exponente: 65537**
- **Módulo:**
  0x00c13bdd03c15ae7647867ef0ffa347807d43ee18a193977ae725d09fdf2ebd2c1a df4ceee06ea0b1891a198f1e9aaeebd9090f8ea5d268acdf1e9fdd2e88a6917a3ac7b 8e7198a0c7350cbc95636565c76afbd5b1b7992d6e31b0a3e8379b579183d3fbcf9a 10a0d7197f6b7241ee599a784c4e3e01e0ba5b7bb2ea95bd9f3af7553c8740544abd a939b2e3e81c7e1c9fcf96533c83ac1597787f1e0479de407ed76664c8eb4fb672164 c1e050316af9aa1ce9eada0ec7f3e6b5525ce070edeb0b6fc09c10ca29e4151ca366 ecd7e10bfed33ab63ae7279706ed43b8bbbadd9ca9c9830c67dd49579f168011f90 838ab881b06a0a0b93babf5c67a8f031ba13dd

En decimal son 617 dígitos.
El tamaño de la clave es de 4096 bits.

(b) En el certificado encontraréis un enlace a la política de certificados (CPS) de la autoridad certificadora firmante. ¿Qué tipo de claves públicas y tamaños admite?
RSA: 2048 bits, 3072 bits y 4096 bits.
ECDSA: 256 bits, 384 bits y 521 bits.

(c) En el certificado encontraréis un enlace un punto de distribución de la CRL de la autoridad certificadora. ¿Cuántos certificados revocados contiene la CRL?
Hay 18234 certificados revocados en la CRL. Se ha usado el comando:

```
Unset
openssl crl -inform DER -text -noout -in GEANTOVRSACA4.crl | grep -c -A1 "Serial Number"
```

(d) En el certificado encontraréis la dirección OCSP (Online Certificate Status Protocol) a la que se puede preguntar por el estatus del certificado. ¿Cuál es el estatus del certificado y hasta cuándo es válido dicho estatus?

- **Revocation status: good**
- **This Update: Dec 17 14:36:47 2023 GMT**
- **Next Update: Dec 24 14:36:46 2023 GMT**