ECC y certificados digitales

Criptografía

Sergi Guimerà

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

Los ficheros de este apartado se encuentran en la carpeta "*wikipedia*".

Los datos de la conexión con Wikipedia usados pertenecen a los paquetes:

- Client Hello: 107
- Server Hello: 109
- Certificate ... : 111

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

El orden de la curva (115792089210356248762697446949407573529996955224135760342422259061068512044369) es primo.

(b) Comprobad que la clave pública P de www.wikipedia.org es realmente un punto de la curva.

Si.

(c) Calculad el orden del punto P.

El orden de la curva es primo, como solo tenemos que comprobar los divisores del orden de la curva para el punto, solo puede ser 1 o el orden de la curva.
El orden de la curva es el mismo que el del punto: 115792089210356248762697446949407573529996955224135760342422259061068512044369.

(d) Comprobad que la firma ECDSA es correcta.

Si

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

Los ficheros de este apartado se encuentran en la carpeta "*certificados*".

(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?

Válido desde: jueves, 5 de diciembre de 2024 1:00:00
Válido hasta: sábado, 6 de diciembre de 2025 0:59:59

Llave pública FIB (base 10) es un RSA de 3072 bits:
Módulo:
52167516300766336280163777960030409098930287422679219566162187134431416668
49723694405344975720215391610437463462260975027528422793819426704394955181
37525355949094874767784366631851625200653171044527930288610627499189897105
71556569322225773995048901717562578892324203218608201662169269772925678 9
25729920902396688727219386745608997719575194678895151465806912889175721806
27090406524921017708728620510652128053214156867479559640742961541834241840
99345061361380835106772819091711055779223799306309608122528242322765146684
04401814100225800468507435857576626933245880174611519565009397112237868957
30981753895688829350297918360690849713505361518087076239771921504177017051 7
47907658654063976142839624355017876869081801477387388025737327321341088003
91018615830271209964287064021108018953096224215212534727431066880107424040 4
39885682937028168246483584371313651019664477173260078654151672684875922173 5
00473841795229538430756850287739803

Exponente público: 65537

El módulo tiene 925 dígitos en base 10 o 3072 en base 2.

(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?

Encontramos un enlace de ***sectigo*** donde después podemos encontrar el siguiente pdf con la información necesaria:
https://www.sectigo.com/uploads/files/Sectigo_WebPKI_CP_v1_3_4.pdf
donde podemos ver:
""""

6.1.5 Key sizes
(...) Certificates issued under this policy SHOULD contain RSA or elliptic curve Public Keys. (...)

All Certificates that expire on or before December 31, 2030 SHOULD contain subject Public Keys of at least 2048 bits for RSA/DSA, at least 256 bits for elliptic curve, and be signed with the corresponding Private Key.

All Certificates that expire after December 31, 2030 SHOULD contain subject Public Keys of at least 3072 bits for RSA/DSA, at least 256 bits for elliptic curve, and be signed with the corresponding Private Key.
”””
Así que admite RSA y curvas elípticas de tamaño mínimo 2048 y 256 bits respectivamente.

(c) En el certificado encontraréis un enlace un punto de distribución de la CRL de la autoridad certificadora. ¿Cuántos certificados revocados contiene la CRL?

Con el siguiente comando leemos el fichero y contamos cuántas veces aparece ‘Serial Number’, con esto obtenemos cuantos certificados revocados contiene (**22307**).

```
Unset
openssl crl -in .\GEANTOVRSACA4.crl -text -noout | grep 'Serial
Number:' | wc -l
```

(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?

Comprobamos con el siguiente prompt de OpenSSL:

```
Unset
openssl ocsp -issuer .\GEANTOVRSACA4.crt -cert .\www.fib.upc.edu.crt -url
http://GEANT.ocsp.sectigo.com -resp_text
```

Obtenemos que el certificado es “good”, así que no ha sido revocado. Este estatus es válido hasta el 24 de diciembre a las 16:31:33 GMT como muy tarde.

```
Unset
Response verify OK
.\www.fib.upc.edu.crt: good
        This Update: Dec 17 16:31:34 2024 GMT
        Next Update: Dec 24 16:31:33 2024 GMT
```

De hecho, he vuelto a ejecutar y ahora la data de validez del *status* ya ha cambiado ni que aun no estamos en 24:

```
Unset
Response verify OK
.\www.fib.upc.edu.crt: good
        This Update: Dec 21 04:31:37 2024 GMT
```

```
        Next Update: Dec 28 04:31:36 2024 GMT
```