CRIPTOGRAFIA

MAT - FIB

ECC i certificats digitals

1. Enregistreu una connexió **TLS 1.3** amb www.wikipedia.org que faci servir un certificat amb una clau pública EC (Elliptic Curve).
   (a) Comproveu que el nombre de punts (ordre) de la corba que es fa servir al certificat és primer.
   (b) Comproveu que la clau pública P de www.wikipedia.org és realment un punt de la corba.
   (c) Calculeu l'ordre del punt P.
   (d) Comproveu que la signatura ECDSA és correcta.

   Pels càlculs podeu fer servir *SAGE*.
2. Connecteu-vos amb www.fib.upc.edu. En aquesta connexió us faran arribar el certificat del servidor de la FIB.
   (a) En el certificat trobareu un punt de distribució de la CRL de l'autoritat certificadora. Quants certificats revocats conté la CRL?
   (b) En el certificat trobareu l'adreça OCSP (Online Certificate Status Protocol) on preguntar per l'estatus del certificat. Quin és l'estatus del certificat i fins quan és vàlid aquest estatus?

Entrega

1. El fitxers amb les captures de les connexions i els fitxers adicionals necesaris per desxifrar els paquets xifrats i comprovar la signatura. S'ha de explicitar clarament quins són els paquets involucrats en la connexió amb www.wikipedia.org.
2. Els càlculs i les comprovacions demanades al primer punt. Podeu fer servir `https://pypi.org/project/ECPy` y `https://docs.sympy.org/latest/modules/ntheory.html`
3. La CRL de l'últim punt i les respostes a les dues preguntes.

Referències

- Wireshark network protocol analyzer
- Wireshark: Using the (Pre)-Master-Secret in TLS
- The New Illustrated TLS Connection
- The Transport Layer Security (TLS) Protocol Version 1.3, https://tools.ietf.org/html/rfc8446
- TLS 1.3: `Certificate Verify` message
- FIPS 186-4 Digital Signature Standard, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
- 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
- Openssl ocsp - Online Certificate Status Protocol utility, https://www.openssl.org/docs/manmaster/man1/ocsp.html