Universitat Politècnica de Catalunya

Criptografia

Quarta entrega: ECC

Mario Fernández Villalba

Grup 11

Q1 2017-2018

1. Per establir una connexió segura amb `www.google.com` he utilitzat el navegador Chrome, i he capturat els paquets mitjançant Wireshark. La captura corresponent es troba al fitxer *paquetes.pcapng*.

   a) La clau DH s'acorda utilitzant la corba X25519 i la signatura amb la corba NIST P-256.

   b) Per comprovar el certificat d'una connexió segura amb Google he seguit el procés següent:

      - Primerament he exportat els bytes random dels missatges *HelloClient* i *HelloServer*; i els bytes dels camps *CurveType*, *NamedCurve*, *PubKeyLen* i *PubKey* del missatge d'intercanvi de certificats. Seguidament els he concatenat per aconseguir el missatge m que posteriorment he hashejat en *SHA256*.
      - A continuació he buscat els paràmetres a,b,p,n,P de la corba NIST P-256 en el DSS.
      - Seguidament he extret la clau publica utilitzada en la signatura del camp *subjectPublicKey* del certificat.
      - Finalment he passat a verificar la signatura amb totes les dades recol·lectades.

      Tot aquest procés es troba programat al directori *ex1.ipynb*. Efectivament, la verificació ha sigut positiva.

2. Utilitzant Chrome he comprovat que la connexio amb `www.facebook.com` utilitza per signar el certificat la corba NIST P-256, amb el punt:

   (61521275115279842049803341918794004729639400001015784075693632594254284814290 : 591746761607989203382562728503952926173653913652936183446140085388478102172 43 : 1)

   a) La clau privada associada amb el meu DNI es:
   (319414943592252434002570389751673588506177117713535384797979003498163107062 85 :
   49586235081845106080218621805866121073632073969038042121780860922539220854937 :
   1)

   b) He provat amb SAGE de trobar una clau pública que tingui per primera component el meu DNI i he comprovat que no existeix. També he fet una cerca exhaustiva per trobar una clau pública que tingui per xifres mes significatives el meu DNI i després de 5 min de cerca i no trobar-ne he parat el programa degut al cost computacional.

   Tot aquest procés es troba programat al directori *ex2.ipynb*.

3. El punt de distribució CRL es troba a `http://crl3.digicert.com/sha2-ha-server-g6.crl` i l'adreça de peticions OCSP és `https://www.digicert.com/CPS`.

   a) Mitjançant la comanda de PowerShell *certutil -dump ./sha2-ha-server-g6.crl* he comprovat que el CRL conté 637 certificats revocats.

   b) Per comprovar el estatus del certificat he usat la comanda *openssl ocsp -issuer DigiCertSHA2HighAssuranceServerCA.crt -cert facebook.crt -url https://www.digicert.com/CPS -text*.

   Els certificats corresponents es troben al directori ex3.