Quarta entrega: ECC

Albert López Alcácer

14 de gener de 2018

1 Entrega

1. **(a)** x25519 i P-256

   (b)

2. Per al lloc web: www.forocoches.com
   "openssl x509 -inform der -in forocochescrt.bin -text"

   Punt: (0x88f64e14f9ea807c0e85449f42bdda34ff9f27e229dc55f560df93d7d92983cd,
   0x5e0289a5c390c58149baa7bc876da634cb955173b037366fc527191a71a1aba2)
   Corva: P-256

   (a) Clau pública:
   (109098897891037053549335793542440777622043143433545907047064257686176197056844
   : 261059260776451928264983731048286505946989915442306126131881936621517605835 91
   : 1)

   (b)

3. Adreça de la CRL: http://crl.comodoca4.com/COMODOECCDomainValidationSecureServerCA2.crl

   (a) Número de certificats revocats: 77

   (b) Estat del certificat:
   "openssl ocsp -issuer COMODOECCDomainValidationSecureServerCA2.crt -cert forocochescrt.pem -url http://ocsp.comodoca4.com -text"

   forocochescrt.pem: good
   This Update: Jan 13 13:05:16 2018 GMT
   Next Update: Jan 20 13:05:16 2018 GMT