(Applied) Cryptography Tutorial #10

Bernardo Portela (bernardo.portela@fc.up.pt) Rogério Reis (rogerio.reis@fc.up.pt) November 29, 2024

- 1. Is (4,7) a point in the elliptic curve $y^2 = x^3 5x + 5$ over \mathbb{Z}_{23} ? And over \mathbb{R} ?
- 2. On the elliptic curve real numbers $y^2 = x^3 6x$, let P = (-2, 2) and Q = (3, 3). Find P + Q and 2P.
- 3. Consider the elliptic curve defined by $y^2 = x^3 + x + 6$ over \mathbb{Z}_{11} . Determine all of the points of the curve.
- 4. For the curve defined in the previous question, consider the point G = (2,7). Compute the multiples of G from 2G through 13G.
- 5. Write python/SageMath programs that for $\rm P{-}192^1$ and ECDSA
 - (a) Generates a pair of private/public keys.
 - (b) Sign a text using a private key.
 - (c) Verifies a signature using a public key.

¹https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf