



## Selected Topics in Cryptography

### Guía de estudio para el ETS

1. Find a non-singular elliptic curve over the  $\mathbb{Z}_5$ . Justify why is it non-singular. **(2 points)**
2. Let  $E$  be an elliptic curve defined over  $\mathbb{Z}_5$ :  $y^2 = x^3 + 3x + 3$ 
  - a) Compute all points on  $E$  over  $\mathbb{Z}_5$ .
  - b) How many points does  $E$  have?
  - c) Find a generator point for this elliptic curve. Justify why it is a generator point.
3. Given the elliptic curve  $y^2 = x^3 + x + 3 \pmod{7}$  with the points, compute the following operations
  - a) Verify that  $P = (4, 1) \in E(1, 3)$ . If your answer is positive, compute  $-P$  and  $2P$
  - b) if  $P = (6, 6)$  calculate  $P + \mathcal{O}$
  - c)  $(6, 1) + (6, 6)$
  - d)  $(5, 0) + (4, 1)$
4. Compute a session key between two entities Alice and Bob, in a ECDH protocol. Your secret vale is  $a = 5$ . You receive from Bob  $B = (3, 2)$ . The elliptic curve being used is defined by  $y^2 = x^3 + x + 4 \pmod{5}$ .

$G$	$=$	$(2, 2)$
$2G$	$=$	$(0, 2)$
$3G$	$=$	$(3, 3)$
$4G$	$=$	$(1, 4)$
$5G$	$=$	$(1, 1)$
$6G$	$=$	$(3, 2)$
$7G$	$=$	$(0, 3)$
$8G$	$=$	$(2, 3)$
$9G$	$=$	$\mathcal{O}$
5. Consider the public key  $K_{pb} = (p, a, b, q, A, B) = (7, 1, 1, 5, (2, 5), (0, 6))$  for ECDSA:, if  $h(x) = 4$ , verify the signature  $(r, s) = (0, 3)$
6. Consider ECDSA, show why the signature  $(r, s)$  satisfies the condition  $r = x_p \pmod{q}$  where  $x_p$  is the x coordinate of  $P = u_1A + u_2B$ ,  $A$  is generator and  $B$  is the public key.
7. An RSA encryption scheme has the set-up parameters  $p = 17$  and  $q = 19$ . The public key is  $e = 5$ 
  - a) Decrypt the ciphertext  $y = 2$  using Chinese Remainder Theorem (CRT).
  - b) Verify your result by encrypting the plaintext without using the CRT.

8. What is the purpose of RSA-PSS? Please list the differences between schoolbook RSA and RSA-PSS?
9. Considering EdDSA answer the following questions:
  - a) Which cryptographic service provide EdDSA?
  - b) Why is this cryptographic algorithm secure? Please describe the intractable mathematical problem that provide security to EdDSA.
  - c) List the differences between the parameters (elliptic curve, finite field, etc) used for ECDSA and the parameters used for EdDSA.
10. The protocol TLS 1.3 provides security over a computer network. To do this it uses several cryptographic algorithms.
  - a) List the cryptographic algorithms used in this protocol to provide integrity.
  - b) Why TLS 1.3 provide perfect forward secrecy (PFS)? Which cryptographic mechanism provide PFS and why?
  - c) Which cryptographic algorithms are used for key exchange in TLS 1.3?
  - d) What would happen if we do not use digital certificates in TLS?
  - e) What is the purpose of a certificate authority?