

Name+Surname: \_\_\_\_\_ Univ. Code: \_\_\_\_\_

**Q1.** Determine whether the following statements are true or false or Not-applicable/meaningless (i.e. the sentence is badly formulated or refers to something impossible/wrong).

In ECDSA, for providing IND-CPA (semantic) security, the nonce used must be always fresh	V	F	N/A
In ECIES, for providing IND-CPA (semantic) security, the nonce used must be always fresh	V	F	N/A
In El Gamal, for providing IND-CPA security, the nonce used must be always fresh	V	F	N/A
ECDSA security relies on the hardness of the factorization problem over elliptic curves	V	F	N/A
The order of an elliptic curve group built on $Z_p$ with $p$ prime is either $p$ or a multiple of $p$	V	F	N/A
In a (4,4) secret sharing scheme using arithmetic modulo $n$ , $n$ must be a prime number	V	F	N/A
The Shamir secret sharing is unconditionally secure	V	F	N/A
A verifiable secret sharing using the Pedersen Commitment is unconditionally secure	V	F	N/A
The Pedersen Commitment is perfectly hiding	V	F	N/A
Unlike Shamir, a trivial secret sharing scheme cannot be ideal	V	F	N/A

**Q2. Part 1:** Describe the Boneh-Franklin's Identity Based Encryption scheme

**Part 2:** Show how the user private key can be computed via a PKG system distributed among two parties so that neither party is able, alone, to know the users' private keys.

Name+Surname: \_\_\_\_\_ Univ. Code: \_\_\_\_\_

**Q3.** Let P be an EC point. What is the minimum number of EC sums/doubles necessary to compute  $[193]P$ ?

**Q4 Assume arithmetic modulus 100.** A Linear secret sharing scheme involving 4 parties is described by the following access control matrix:

A:	1	1	0	0
B:	0	1	1	0
C:	0	0	1	1
D:	0	0	0	1

Assume that the following shares are revealed: A → 15, B → 27, C → 33, D → 41  
What is the secret?

**Q5.** Consider the Elliptic curve EC( $Z_7$ ):  $y^2 = x^3 + x$  defined over the modular integer field  $Z_7$ .

- A. Verify that (0,0) is a point of the curve, and (*without any computation*) determine  $(0,0) + (0,0)$ .
- B. find all the remaining points of the curve.

Name+Surname: \_\_\_\_\_ Univ. Code: \_\_\_\_\_

**Q6.** A Shamir Secret Sharing scheme uses a non-prime modulus  $p=35$  (if you need modular inverses see table on the right). Of the 5 participating parties  $P_1, \dots, P_5$ , with respective  $x$  coordinates  $x_i = \{1,2,3,4,5\}$ , parties  $P_1, P_2$  and  $P_4$  aim at reconstructing the secret.

a) compute the Lagrange Interpolation coefficients for parties 1, 2, 4.

b) Reconstruct the secret, assuming that the shares are:

$$P_1 \rightarrow 33$$

$$P_2 \rightarrow 4$$

$$P_4 \rightarrow 21$$

c) Does the knowledge of the two shares  $P_1$  and  $P_2$  leak information about the secret?

x	1/x mod 35
1	1
2	18
3	12
4	9
6	6
8	22
9	4
11	16
12	3
13	27
16	11
17	33
18	2
19	24
22	8
23	32
24	19
26	31
27	13
29	29
31	26
32	23
33	17
34	34

Name+Surname: \_\_\_\_\_ Univ. Code: \_\_\_\_\_

**Q7** An RSA system has the following parameters: modulo  $n=253$ , public key  $e=3$ . Assume we are NOT able neither to factorize n nor gather or compute the corresponding private key d. Despite this, we wish to compute the RSA signature  $19^d \bmod n$  for message  $m=19$ .

- 1) Show how this is possible if we know that  $19^{5d} = 10 \bmod n$ , and
- 2) numerically compute the signature.

[here a few modular inverses with might (might not) be useful:  $\{3, 5, 10, 19, 100\}^{-1} \bmod n \rightarrow \{169, 152, 76, 40, 210\}$ ]