March 5, 2024, Part 3, Computer & Network Security

SURNAME:_____ NAME: _____ MATRICOLA:_____

Q1: Multiple answer questions

In a (3,3) trivial secret sharing based on the XOR the three shares are 0110, 1110, 1000. What is the secret?	
Why Shamir Secret Sharing requires prime fields?	1. To guarantee forward secrecy 2. To guarantee unconditional security 3. To guarantee reconstruction of secret 4. To guarantee linearity
Given g and h public values, arithmetics modulo prime, e(G,G) a bilinear pairing, and s a secret, which of these constructions is a Pedersen commitment for the secret s?	1. Commit(r,s) = g^{rs} 2. Commit(r,s) = $e(g^r,h^s)$ 3. Commit(r,s) = $h^r g^s$ 4. None of the above
In an El Gamal encryption using a 1024 bit prime modulus, the size of the ciphertext is	1. 1024 bit 2. 2048 bit 3. 4096 bit 4. Variable, depends on the size of the plaintext
Being a an EC point, e(G,G) a bilinear pairing, g a generator of G, and b, c numerical coefficients, simplify the following expression: $e(a \times g^b, g^c)$	
How is the private key SK of an user named "bob" constructed in the Boneh-Franklin's Identity Based Encryption scheme? (notation: s, g^s = PKG key pair, H() = hash function which maps a string into an EC point)	1. SK = g^H(bob) 2. SK = H(bob^s) 3. SK = bob^s 4. SK = H(bob)^s

Q2: For the Pedersen Verifiable Secret Sharing scheme describe: i) how shares are assigned to each party, ii) how a party's share, once revealed, can be verified

March 5, 2024, Part 3, Computer & Network Security

SURNAME:_____ NAME: _____ MATRICOLA:_____

Q3: Consider the Elliptic curve $y^2 = x^3 + x + -1$ defined over the modular integer field Z_5.

A. find all the points EC(Z_5)

$$P = (x_1, y_1)$$
$$Q = (x_2, y_2)$$
$$R = P + Q = (x_3, y_3)$$
$$x_3 = \lambda^2 - x_1 - x_2$$
$$y_3 = \lambda(x_1 - x_3) - y_1$$
$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & P = Q \end{cases}$$

B. State what is the order of the corresponding group

C. Compute [4](0,2) using the minimum number of operations
[HELP: possibly useful mnemonic hints reported here on the right;
MUST-DO: show step-by-step detailed computations]

March 5, 2024, Part 3, Computer & Network Security

SURNAME:_____ NAME: _____ MATRICOLA:_____

Q4: In ECDSA, we decide to sign two messages m1 and m2 using as nonces r1=[k]P and r2=[2k]P. Is this harmful? And if this is the case, demonstrate why.

Q5: **Assume arithmetic modulus 101.** A Linear secret sharing scheme involving 3 parties is described by the following access control matrix:

A:	1	1	1
B:	0	1	-1
C:	0	0	1

A. Assume that the following shares are revealed:

A → 88

B → 12

C → 51

What is the secret? (explain how you arrived to the result, otherwise the answer is not considered valid)

March 5, 2024, Part 3, Computer & Network Security

SURNAME:_____ NAME: _____ MATRICOLA:_____

Q6. A same message M is RSA-encrypted using two different public keys e1 = 3 and e2 = 11, but same RSA modulus n=319. The two resulting ciphertexts are: c1=10 and c2=142. Decrypt the message applying the Common Modulus Attack (show the detailed computations required).

Mod 319 inverses that might be useful to speed up computation: $10^{-1} = 32$; $142^{-1} = 164$