April 22, 2024, Part 3, Computer & Network Security

SURNAME:_____ NAME: _____ MATRICOLA:_____

Q1: Multiple answer questions

A verifiable secret sharing schemes permits to catch	• A malicious dealer which deals invalid shares • A malicious party who modifies/spoof shares • Both a malicious dealer and a malicious party • As (3) but only if the dealer is centralized
In a (7,9) Shamir Secret Sharing what is the order of the polynomial to use?	• 6 • 7 • 8 • 9
For a Z_p^{ι} group with strong prime p, How can you assess whether an element x belongs to the QR subgroup?	• By checking if $x_{\square}^{(p-1)/2}=1$ • By checking if $x_{\square}^{(p-1)/2}=-1$ • By checking if $x_{\square}^{(p-1)/2}\neq 1$ • By checking if $x_{\square}^{(p-1)/2}\neq -1$
In a secret sharing scheme (SSS) the size of a share is X. If we transform it in a verifiable SSS using the Pedersen commitment, the size of the resulting share…	1. Remains X 2. Increases to 2X 3. Increases to 3X 4. Increases, but depends on the used DLOG group size
Write all the points of the EC curve $y^2 = x^3 - 2x + 1$ defined over the modular integer field Z_5.	
In the ECDSA signature, being PK the public key and SK the secret key,	1. Both PK and SK are EC points 2. PK is an EC point, SK is an integer 3. PK is an integer, SK is an EC point 4. Both PK and SK are integers

Q2: Describe the RSA common modulus attack, and “invent and solve” an example using small numbers.

April 22, 2024, Part 3, Computer & Network Security

SURNAME:_____ NAME: _____ MATRICOLA:_____

Q3: Discuss what may happen if a client consistently reuses the same constant term g^r (expected to be ephemeral, i.e. nonce) within subsequent El Gamal encryptions.

Q4(a): Derive the access control matrix which implements the monotone Access Control Policy

A AND ((B AND C) OR (D AND E)

Q4(b): For the above exercise, assuming arithmetic mod 101, deal the numerical shares to give to A, B, C, D and E under the assumption that the secret to hid is 10, and the random quantities to use are generated by the following PRNG pick the number of valies you need to solve this exercise:

{31, 22, 78, 07, 95, 81, 77, 11, 58, …}

[Note – if you cannot solve the exercise Q4(a), "invent" an "alternative/reasonable" binary matrix]