# January 29, 2025, final midterm, Computer & Network Security

**SURNAME:_____ NAME: _____ MATRICOLA:_____**

**Q1**: Multiple answer questions / short answer questions

| | |
|---|---|
| In a (5,7) Shamir Secret Sharing what is the order of the polynomial to use? | • 4<br>• 5<br>• 6<br>• 7<br>• 8 |
| Is g=3 a generator for the $Z_{23}^{\epsilon}$ group? Please motivate the answer stating which computation you did, for verifying this (or, if no computation is necessary to provide the answer, state why) | |
| Write all the points of the EC curve $y^2 = x^3 + 1$ defined over the modular integer field $Z_5$. | |
| **Let G and $G_t$ be groups with generators** g and $g_t$ respectively, assume a **Bilinear Pairing** $e(G,G) \rightarrow G_t$. Simplify the expression $e(a \times g^b, g^{c+d})$ | |
| Consider a vanilla El Gamal Encryption scheme based on a prime modulus of 2048 bits. Assume you encrypt a message of 1024 bits. The size of the ciphertext (all included) is… | • 1024 bit<br>• 1024 bit + the size of the chosen IV<br>• 2048 bit<br>• 2048 bit + the size of the chosen IV<br>• 3072 bit<br>• 4096 bit |
| Write the access control matrix for the policy<br><br>(A and B) or (C and D) | |
| The Pedersen Commitment is | • Computationally hiding & computationally binding<br>• Unconditionally hiding & computationally binding<br>• Computationally hiding & Unconditionally binding<br>• Unconditionally hiding & Unconditionally binding |
| In the ECDSA signature, being PK the public key and SK the secret key, | • Both PK and SK are EC points<br>• PK is an EC point, SK is an integer<br>• PK is an integer, SK is an EC point<br>• Both PK and SK are integers |

# January 29, 2025, final midterm, Computer & Network Security

**SURNAME:_____ NAME: _____ MATRICOLA:_____**

**Q2**: In a DKG system based on a (3,3) secret sharing scheme, the private key s associated to the public key $g^s$ mod p is shared by three parties A, B and C, each having a share $\sigma_x$ so that $s= \sigma_a+\sigma_c+\sigma_c$. Assume that, <u>at a subsequent time</u>, party D wants to be included as fourth party, BUT without re-running the entire DKG scheme. Please propose a possible approach to:

1) (trivial case) include the new partner in the group, suitably modifying the overall public key

2) +

**Q3**:Describe the Boneh-Franklin Identity Based Encryption scheme

# January 29, 2025, final midterm, Computer & Network Security

**SURNAME:_____ NAME: _____ MATRICOLA:_____**

**Q4**: A Shamir Secret Sharing scheme uses a non-prime modulus p=33 (if you need modular inverses see table on the right). Three participants, having x coordinates $x_i$ = {1, 3, 5}, aim at reconstructing the secret.

a) compute the Lagrange Interpolation coefficients for each of these three parties 1, 3, 5.

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

P1 → 20
P3 → 4
P5 → 28

c) Does the knowledge of the two shares P3 and P5 leak information about the secret?

| n | $n^{-1}$ |
|---|---|
| 1 | 1 |
| 2 | 17 |
| 4 | 25 |
| 5 | 20 |
| 7 | 19 |
| 8 | 29 |
| 10 | 10 |
| 13 | 28 |
| 14 | 26 |
| 16 | 31 |
| 17 | 2 |
| 19 | 7 |
| 20 | 5 |
| 23 | 23 |
| 25 | 4 |
| 26 | 14 |
| 28 | 13 |
| 29 | 8 |
| 31 | 16 |
| 32 | 32 |

# January 29, 2025, final midterm, Computer & Network Security

**SURNAME:_____ NAME: _____ MATRICOLA:_____**

**Q5**: A same message M is RSA-encrypted using two different public keys e1 = 3 and e2 = 23, but same RSA modulus n=253. The two resulting ciphertexts are: c1=173 and c2=151. Decrypt the message applying the Common Modulus Attack (show the detailed computations required).

**Q6**: MOV reduction: Prove that if a group G admits a bilinear pairing e(G,G)→Gt, then the DLOG problem cannot be harder than the corresponding DLOG problem in Gt.