# Survey n° 2

*Cryptography and Security 2025*

Full Name: _____

SCIPER: _____

1. Let $a$ and $n$ be integers. The Euclidean Algorithm can be used to ... C

   - ☐ ... compute the additive inverse of $a$ in $\mathbb{Z}_n^*$.
   - ■ ... compute the gcd of $a$ and $n$ in $\mathbb{Z}$.
   - ☐ ... factor $n$ into its prime components.
   - ☐ ... compute the inner product of two vectors over $\mathbb{Z}_n^*$.

2. Let $n$ be an integer. Which of the following is **false**.

   - ☐ If $n$ is prime, then $\mathbb{Z}_n$ is cyclic.
   - ■ $\forall m \in \mathbb{Z}_n$, $m^{\varphi(n)} = 1 \pmod{n}$.
   - ☐ If $n$ is prime, then $\mathbb{Z}_n^*$ is cyclic.
   - ☐ If all elements in $\mathbb{Z}_n \setminus \{0\}$ are generators of $\mathbb{Z}_n$, then $n$ is prime.

3. Which of the following is **false**.

   - ☐ The Discrete Logarithm Problem is at least as hard as the Computational Diffie-Hellman Problem.
   - ☐ The Computational Diffie-Hellman Problem is easy if one can solve the ElGamal Key Recovery Problem.
   - ☐ The Decisional Diffie-Hellman Problem can still be hard even if we know all prime factors of the group order.
   - ■ The Computational Diffie-Hellman Problem can still be hard even if we can solve the ElGamal Decryption Problem.

4. Which of the following is **false**. The Discrete Logarithm Problem ...

   - ■ is believed to be hard in any group of size $2^\lambda$, where $\lambda$ is the security parameter.
   - ☐ can be solved by the baby step - giant step algorithm.
   - ☐ is easy if the group order is smooth.
   - ☐ is easy for a large-scaled quantum computer using Shor's algorithm.

5. Which of the following statements is **false**?

   - ☐ The Diffie–Hellman key exchange produces shared-keys as long as the public key.
   - ☐ Decryption resistance of the ElGamal encryption scheme is equivalent to the CDH.
   - ☐ INDCPA security of the Diffie–Hellman key exchange is equivalent to the DDH.
   - ■ The ElGamal encryption scheme produces ciphertexts as long as the plaintexts.