Survey n° 3

Cryptography and Security 2025

Full Name: _____

SCIPER: _____

C

1. Which of the following statements about primality testing is **true**?

   - ☐ If Fermat test claims n is composite, then n can still be prime with small probability.
   - ☐ If Miller-Rabin test claims n is composite, then n can still be prime with small probability.
   - ■ Given an input composite number n, both Fermat and Miller-Rabin tests may claim n is prime.
   - ☐ Both Fermat and Miller-Rabin tests run in complexity $\mathcal{O}(l^2)$ for a number of l bits.

2. Which of the following is **true** about ElGamal and plain RSA?

   - ☐ RSA key generation has lower complexity than ElGamal.
   - ■ RSA has lower encryption complexity than ElGamal.
   - ☐ Both RSA and ElGamal can be easily adapted to elliptic curves.
   - ☐ Both plain RSA and ElGamal are deterministic.

3. Let p be an odd prime, and $a \in \mathbb{Z}_p^*$. Then a is a quadratic residue iff ...

   - ☐ $\ldots a^{p-1} \equiv 1 \mod p$.
   - ■ $\ldots a^{\frac{p-1}{2}} \equiv 1 \mod p$.
   - ☐ $\ldots a^{\frac{p+1}{2}} \equiv 1 \mod p$.
   - ☐ $\ldots a^{\frac{p-1}{2}} \equiv a \mod p$.

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

   - ☐ If two elliptic curves share the same j-invariant, they are isomorphic over a field extension.
   - ■ All curves defined by the equation $y^2 = x^3 + Ax + B$ have an Abelian group structure.
   - ☐ The DL problem is easy on supersingular elliptic curves.
   - ☐ The x-coordinate of a point $P \neq \infty$ on an elliptic curve defined by the equation $y^2 = x^3 + Ax + B$ determines this point up to sign.

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

   - ☐ On $\mathbb{F}_{401}$, there exists a curve E such that $\#E = 380$.
   - ☐ On $\mathbb{F}_{401}$, there exists a curve E such that $\#E = 430$.
   - ■ On $\mathbb{F}_{223}$, there exists a curve E such that $\#E = 400$.
   - ☐ On $\mathbb{F}_{223}$, there exists a curve E such that $\#E = 245$.