# Cryptography Foundations

Cryptography · Answer Key · 10 Questions

**1. Which mathematical problem forms the basis of the security for the RSA algorithm?**

A) Discrete logarithm problem
**B) Integer factorization**
C) Elliptic curve inversion
D) Subset sum problem

**2. What is the primary function of a cryptographic hash function like SHA-256?**

A) To reversibly encrypt data
B) To compress data without losing information
**C) To generate a fixed-size unique digital fingerprint**
D) To increase the entropy of a random number generator

**3. In symmetric-key cryptography, what is the main requirement for secure communication?**

A) The public key must be known to everyone
**B) Both parties must share the same secret key**
C) The private key must be derived from the public key
D) The algorithm must use a different key for every block

**4. Which of the following is a symmetric block cipher standard approved by NIST in 2001?**

**A) AES**
B) RSA
C) DSA
D) ECC

**5. What property ensures that a digital signature proves the sender actually sent the message?**

A) Confidentiality
**B) Non-repudiation**
C) Data freshness
D) Perfect forward secrecy

**6. Diffie-Hellman is a protocol primarily designed for what purpose?**

A) Digital signatures
**B) Key exchange**
C) Message authentication
D) Data compression

**7. Which attack attempts to find two different inputs that produce the same hash output?**

A) Brute-force attack
**B) Birthday attack**
C) Man-in-the-middle attack
D) Side-channel attack

**8. What is the length of the initialization vector (IV) in standard AES-GCM operations?**

A) 64 bits
**B) 96 bits**
C) 128 bits
D) 256 bits

**9. Which elliptic curve is widely used in the EdDSA signature scheme?**

**A) Curve25519**
B) secp256k1
C) NIST P-256
D) BrainpoolP512r1

**10. What does the 'P' in PGP (Pretty Good Privacy) refer to regarding its cryptographic nature?**

A) Private key encryption
**B) Public key encryption**
C) Password-based encryption
D) Protocol-based encryption