

Introduction to Cryptography

Cryptography · Practice Test · 15 Questions

1. What is the term for the process of converting readable information into an unreadable format?

- A) Decryption
- B) Encryption
- C) Hashing
- D) Authentication

2. Which historical cipher involves shifting letters of the alphabet by a fixed number of positions?

- A) Caesar cipher
- B) Vigenère cipher
- C) RSA algorithm
- D) AES

3. What is the original, readable message before it is encrypted called?

- A) Ciphertext
- B) Key
- C) Plaintext
- D) Metadata

4. In symmetric-key cryptography, how many keys are used to both encrypt and decrypt the data?

- A) Zero
- B) One
- C) Two
- D) Three

5. What is the primary purpose of a digital signature in network security?

- A) To hide the message content
- B) To speed up data transmission
- C) To verify the authenticity and integrity of a message
- D) To compress large files

6. Which of these is a widely used symmetric encryption algorithm?

- A) RSA
- B) AES
- C) Diffie-Hellman
- D) ECC

7. What does the 'A' in the RSA encryption algorithm stand for?

- A) Adleman
- B) Algorithm
- C) Advanced
- D) Authentication

8. Which type of cryptography uses a public key for encryption and a private key for decryption?

- A) Symmetric cryptography
- B) Asymmetric cryptography
- C) Hash-based cryptography
- D) Steganography

9. What is the main goal of a 'hash function' in data security?

- A) To reverse encrypted data
- B) To provide a unique fixed-length string representation of data
- C) To compress images
- D) To translate languages

10. What is 'ciphertext' in the context of cryptography?

- A) The raw data input
- B) The encoded or encrypted version of the data
- C) The key used to unlock a file
- D) A secure network protocol

11. Which of these is a common weakness of a simple Caesar cipher?

- A) It requires very long keys
- B) It is immune to frequency analysis
- C) It has a very small number of possible keys
- D) It uses too much memory

12. What is the practice of hiding information within other non-secret data, such as an image?

- A) Steganography
- B) Decryption
- C) Encryption
- D) Hashing

13. Which cryptographic technique is used to ensure data has not been altered during transmission?

- A) Data compression
- B) Integrity checking (Hashing)
- C) Data masking
- D) Key rotation

14. Who is meant to have access to a private key in an asymmetric system?

- A) The general public
- B) Only the recipient of the message
- C) Everyone on the network
- D) The network administrator only

15. What is the definition of a 'cryptographic key'?

- A) A physical key for a server room
- B) A piece of information used to control the encryption and decryption process
- C) A password for a user account
- D) A hardware firewall