Fundamentals of Cryptography

Cryptography · Answer Key · 12 Questions

1. Which ancient cipher involves replacing each letter in a plaintext with a letter a fixed number of positions down the alphabet?

A) Vigenère cipher
B) Caesar cipher
C) Playfair cipher
D) Rail fence cipher

2. What is the primary function of a cryptographic hash function?

A) To encrypt sensitive data
B) To compress data for storage
C) To map data of arbitrary size to a fixed-size bit string
D) To provide non-repudiation for financial transactions

3. In RSA cryptography, what type of keys are used to encrypt and decrypt messages?

A) A single shared symmetric key
B) A public key and a private key
C) Two identical private keys
D) A rotating password key

4. Which of the following is a symmetric-key block cipher standardized by the U.S. government in 2001?

A) AES
B) DES
C) RSA
D) ECC

5. What does the acronym 'PGP' stand for in the context of email encryption?

A) Private Group Protocol
B) Public Gateway Protection
C) Pretty Good Privacy
D) Personal General Password

6. Which mathematical problem forms the basis of the security of the RSA algorithm?

A) Discrete logarithm problem
B) Integer factorization
C) Elliptic curve point multiplication
D) Shortest vector problem

Quixly | This material was auto-generated. Quixly is not liable for errors or omissions. Visit quixlylearn.com to report corrections.

7. What is the core purpose of a Digital Signature?

A) To hide the content of a message from unauthorized users
B) To verify the authenticity and integrity of a digital document
C) To replace traditional passwords for login systems
D) To compress files to save bandwidth

8. Which cryptographic protocol is the successor to SSL (Secure Sockets Layer) for securing internet communications?

A) TLS
B) HTTP
C) FTP
D) SMTP

9. In cryptography, what is 'salt' used for?

A) To randomize hash outputs to protect against rainbow table attacks
B) To encrypt the metadata of a file
C) To speed up the decryption process
D) To ensure the message length remains constant

10. What term describes the process of converting ciphertext back into plaintext?

A) Encoding
B) Decoding
C) Decryption
D) Hashing

11. Which of these is considered a 'stream cipher'?

A) AES
B) RC4
C) DES
D) Blowfish

12. What is the main advantage of Elliptic Curve Cryptography (ECC) compared to RSA?

A) It is easier to implement
B) It requires smaller key sizes for equivalent security
C) It does not require public keys
D) It is immune to quantum computing

Quixly | This material was auto-generated. Quixly is not liable for errors or omissions. Visit quixlylearn.com to report corrections.