Fundamentals of Cryptography

Cryptography · Answer Key · 20 Questions

1. Which classical cipher works by shifting each letter of the plaintext by a fixed number of positions down the alphabet?

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

2. What does the acronym AES stand for in modern symmetric encryption?

A) Advanced Encryption Standard
B) Automated Encoding System
C) Applied Electronic Security
D) Algorithmic Encryption Suite

3. In public-key cryptography, which key is typically made available to the public to encrypt messages?

A) Private key
B) Secret key
C) Public key
D) Session key

4. Who are the three individuals associated with the invention of the RSA algorithm?

A) Diffie, Hellman, and Merkle
B) Rivest, Shamir, and Adleman
C) Shannon, Turing, and Von Neumann
D) Kahn, Massey, and Knudsen

5. What is the primary purpose of a cryptographic hash function?

A) To encrypt sensitive data
B) To verify data integrity
C) To compress large files
D) To generate random numbers

6. Which of the following is considered a symmetric-key encryption algorithm?

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

7. The Enigma machine, used extensively during World War II, was primarily employed by which military force?

A) United States Navy
B) Imperial Japanese Army
C) Nazi Germany
D) Royal Air Force

8. What is the term for the process of converting ciphertext back into plaintext?

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

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

A) Discrete logarithm problem
B) Integer factorization
C) Elliptic curve mapping
D) Knapsack problem

10. What does a digital signature primarily provide to a recipient?

A) Message encryption
B) Data compression
C) Authenticity and integrity
D) Anonymity

11. The Vigenere cipher is categorized as what type of cipher?

A) Transposition cipher
B) Polyalphabetic substitution cipher
C) Monoalphabetic substitution cipher
D) Stream cipher

12. Which protocol is widely used to provide secure communication over a computer network, such as the internet?

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

13. What is the name of the 'one-time pad' property that makes it theoretically unbreakable if used correctly?

A) Computational hardness
B) Perfect secrecy
C) Prime factorization
D) Substitution parity

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

A) To encrypt the main key
B) To prevent rainbow table attacks on hashes
C) To increase the length of a password
D) To hide the algorithm type

15. Which of these is a widely used elliptic curve standard?

A) Curve25519
B) RSA-4096
C) DES-CBC
D) SHA-3

16. What is the definition of a 'brute-force attack'?

A) Exploiting a software vulnerability
B) Guessing every possible key until the correct one is found
C) Intercepting data in transit
D) Modifying the plaintext directly

17. Which organization is responsible for publishing many of the standards used in modern cryptography, such as FIPS?

A) NIST
B) IEEE
C) ISO
D) W3C

18. What is the function of a 'Nonce' in cryptographic protocols?

A) To identify the user
B) To provide a unique value for a single communication session
C) To compress the message
D) To provide long-term key storage

19. Which of these is a stream cipher?

A) AES

B) ChaCha20

C) RSA

D) Twofish

20. What does 'Diffie-Hellman' allow two parties to achieve over an insecure channel?

A) Data encryption

B) Shared secret key exchange

C) Digital document signing

D) Message authentication