Cryptography Essentials for Students

Cryptography · Practice Test · 18 Questions

1. Which ancient cipher method involves shifting each letter in a message by a fixed number of positions down the alphabet?

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

2. What is the primary difference between symmetric and asymmetric encryption?

A) Symmetric uses two keys, asymmetric uses one
B) Symmetric is always slower than asymmetric
C) Symmetric uses one key for both encryption and decryption
D) Asymmetric is only used for image files

3. In the context of public-key cryptography, what is the 'public key' used for?

A) Decrypting messages received by the owner
B) Signing digital documents
C) Encrypting messages intended for the owner
D) Generating the private key

4. Which of the following is a common hashing algorithm used to verify data integrity?

A) AES
B) RSA
C) SHA-256
D) Diffie-Hellman

5. What does the term 'plaintext' refer to in cryptography?

A) An encrypted message that is easy to read
B) The original, unencrypted message
C) A message with no security
D) The code used to break a cipher

6. Who is often credited with breaking the German Enigma machine during World War II at Bletchley Park?

A) Charles Babbage
B) Alan Turing
C) Ada Lovelace
D) Claude Shannon

7. What is the main purpose of a 'digital signature'?

A) To compress files for faster transfer
B) To prove the authenticity and integrity of a message
C) To hide the identity of the sender completely
D) To encrypt the entire hard drive

8. Which encryption standard is widely considered the global benchmark for securing sensitive electronic data?

A) DES
B) AES
C) ROT13
D) Blowfish

9. What is 'steganography'?

A) The science of hiding messages within other non-secret data
B) The study of cracking passwords
C) A method of encrypting audio files
D) The process of converting binary to text

10. What does 'RSA' stand for in the context of encryption algorithms?

A) Rivest, Shamir, and Adleman
B) Reliable Security Algorithm
C) Rapid Secure Access
D) Remote System Authentication

11. What happens if the 'key' is lost in symmetric encryption?

A) The data can be recovered by brute force
B) The data remains encrypted and inaccessible
C) The encryption algorithm changes automatically
D) The public key can still decrypt the data

12. Which of these is considered a 'cryptographic hash function' property?

A) It must be easily reversible
B) It should produce the same output for different inputs
C) It should be computationally infeasible to find the original input from the output
D) It can only be used with text files

13. What is the term for a computer program that automatically tries every possible password combination?

A) Man-in-the-middle attack
B) Phishing
C) Brute-force attack
D) Social engineering

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

A) HTTPS
B) FTP
C) HTML
D) SMTP

15. What does 'cryptanalysis' focus on?

A) Creating new, stronger ciphers
B) The study and practice of breaking codes and ciphers
C) Storing sensitive keys in hardware
D) Developing new hardware for encryption

16. What is the main limitation of the Vigenère cipher?

A) It uses too few letters
B) It is vulnerable to frequency analysis when the key length is known
C) It requires a quantum computer to solve
D) It cannot be written down

17. Which key length in bits is commonly associated with the standard AES encryption?

A) 8-bit
B) 128-bit
C) 10-bit
D) 4-bit

18. In cryptography, what does the term 'entropy' refer to?

A) The speed of the processor
B) The randomness of the cryptographic key
C) The length of the message
D) The cost of the encryption software