Cryptography Basics for Young Minds

Cryptography · Practice Test · 15 Questions

1. What is the primary purpose of encryption?

A) To make data unreadable to unauthorized individuals.
B) To speed up data transmission.
C) To compress data for storage.
D) To create digital art.

2. In symmetric encryption, how many keys are typically used for both encryption and decryption?

A) One
B) Two
C) Three
D) Four

3. Which of the following is a common example of a symmetric encryption algorithm?

A) AES (Advanced Encryption Standard)
B) RSA
C) ECC (Elliptic Curve Cryptography)
D) SHA-256

4. What is a 'key' in cryptography?

A) A piece of information used to encrypt or decrypt data.
B) A type of digital lock.
C) A secret password for a website.
D) A unique identifier for a file.

5. In asymmetric encryption (also known as public-key cryptography), how many keys are used?

A) Two (a public key and a private key)
B) One
C) Three
D) A variable number depending on the message size

6. What is the function of a 'hash function' in cryptography?

A) To create a fixed-size string of characters (a hash) from any input data.
B) To encrypt messages for secure communication.
C) To generate random numbers for security purposes.
D) To digitally sign documents to verify authenticity.

7. Which of the following is NOT a characteristic of a good cryptographic hash function?

A) It is easy to reverse engineer the original data from the hash.
B) It is computationally infeasible to find two different inputs that produce the same hash.
C) It is computationally infeasible to find an input that produces a given hash.
D) A small change in the input produces a significantly different hash.

8. What does 'plaintext' refer to in cryptography?

A) Unencrypted, readable data.
B) Encrypted, unreadable data.
C) The key used for encryption.
D) A secret code word.

9. What is 'ciphertext'?

A) Encrypted data that is unreadable without the correct key.
B) The original, readable message.
C) A type of digital signature.
D) A secure communication channel.

10. Which of these is a common use case for asymmetric encryption?

A) Securely exchanging keys for symmetric encryption.
B) Encrypting large amounts of data for fast transmission.
C) Compressing files to save storage space.
D) Creating watermarks on images.

11. What is a 'digital signature' primarily used for?

A) To verify the authenticity and integrity of a digital message or document.
B) To encrypt sensitive information.
C) To speed up internet connections.
D) To track the location of devices.

12. Why is it important for cryptographic keys to be kept secret, especially private keys?

A) If a private key is compromised, the encrypted data can be decrypted by attackers.
B) Secret keys make the encryption process faster.
C) Secret keys are needed to create new encryption algorithms.
D) Keeping keys secret prevents the creation of digital signatures.

13. What does 'cryptanalysis' refer to?

A) The study and practice of breaking or bypassing encryption and security systems.
B) The development of new encryption algorithms.
C) The secure storage of cryptographic keys.
D) The process of encrypting and decrypting data.

14. Which historical figure is often credited with using a simple substitution cipher for his military communications?

A) Julius Caesar
B) Albert Einstein
C) Isaac Newton
D) Leonardo da Vinci

15. What is the main difference between a cipher and a code?

A) A cipher substitutes letters or symbols, while a code substitutes entire words or phrases.
B) A code uses a key, while a cipher does not.
C) A cipher is always symmetric, while a code is always asymmetric.
D) A code is used for encryption, while a cipher is used for decryption.