

Cryptography Foundations

Cryptography · Practice Test · 10 Questions

1. Which ancient Roman leader is credited with creating a simple substitution cipher where each letter is shifted three positions down the alphabet?

- A) Julius Caesar
- B) Augustus Caesar
- C) Marcus Aurelius
- D) Nero

2. What is the specific name for a cryptographic tool consisting of two concentric disks with alphabets used to simplify polyalphabetic substitution?

- A) The Enigma Machine
- B) The Alberti Cipher Disk
- C) The Vigenere Square
- D) The Scytale

3. During World War II, what was the primary purpose of the 'Bombe' machine developed by Alan Turing and his team?

- A) To send secret radio signals
- B) To calculate artillery trajectories
- C) To decrypt Enigma-encrypted messages
- D) To jam enemy radar frequencies

4. In cryptography, what is the term for the original, readable message before it has been transformed into a secret code?

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

5. What is a 'frequency analysis' technique used by cryptanalysts to break simple substitution ciphers?

- A) Measuring the speed of encryption
- B) Counting how often each letter appears
- C) Testing every possible password
- D) Using light to scan codes

6. Which famous 19th-century author and poet wrote a short story titled 'The Gold-Bug' which features a plot centered on solving a complex substitution cipher?

- A) Edgar Allan Poe
- B) Mark Twain
- C) Charles Dickens
- D) Lewis Carroll

7. What type of cryptographic system uses two different keys--one for encryption and one for decryption--known as a public and private key?

- A) Symmetric encryption
- B) Asymmetric encryption
- C) Steganography
- D) Polyalphabetic cipher

8. The 'Scytale' was an ancient Greek device used for encryption. How did it work?

- A) By rotating a hidden inner wheel
- B) By wrapping a strip of parchment around a rod
- C) By using invisible ink that required heat
- D) By substituting letters based on a grid

9. What is the field of hiding a secret message inside a non-secret file, such as embedding text inside an image, called?

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

10. Which mechanical device used during the 1920s to 1940s utilized a series of rotating rotors to scramble letters into a complex ciphertext?

- A) The Enigma Machine
- B) The Abacus
- C) The Telegraph
- D) The Typewriter