The World of Cryptography

Cryptography · Practice Test · 15 Questions

1. Which ancient cipher involves shifting the letters of the alphabet by a fixed number of positions?

A) Vigenère Cipher
B) Atbash Cipher
C) Caesar Cipher
D) Playfair Cipher

2. The Enigma machine, used for encrypting messages during World War II, was primarily used by which country?

A) Germany
B) Great Britain
C) Japan
D) United States

3. In asymmetric encryption, if a message is encrypted with a Public Key, which key is required to decrypt it?

A) The same Public Key
B) A Symmetric Key
C) The corresponding Private Key
D) A Master Key

4. What is the term for a cryptographic function that converts an input into a fixed-size string of characters and cannot be reversed?

A) Hash function
B) Transposition
C) Substitution
D) Salting

5. The security of the RSA encryption algorithm relies heavily on the mathematical difficulty of which task?

A) Calculating square roots
B) Factoring large prime numbers
C) Solving linear equations
D) Dividing by zero

6. What is the practice of hiding a secret message inside a non-secret file, such as an image or audio clip?

A) Cryptanalysis
B) Steganography
C) Encoding
D) Obfuscation

7. Which famous British mathematician led the team at Bletchley Park that cracked the Enigma code?

A) Isaac Newton
B) Charles Babbage
C) Alan Turing
D) Ada Lovelace

8. A 'Symmetric Key' algorithm is defined by using how many keys for both encryption and decryption?

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

9. The Vigenère cipher is an improvement over the Caesar cipher because it uses which of the following?

A) A keyword to change shifts
B) Binary code
C) Electric rotors
D) Random number generators

10. What is the name of the ancient Greek device consisting of a parchment strip wrapped around a wooden rod?

A) Abacus
B) Scytale
C) Astrolabe
D) Cipher Disk

11. Which protocol allows two parties to establish a shared secret key over an insecure communication channel?

A) MD5
B) SHA-1
C) Diffie-Hellman
D) ROT13

12. In cryptography, what is 'Frequency Analysis' used for?

A) Breaking ciphers by counting letter occurrences
B) Speeding up data transmission
C) Generating random numbers
D) Hiding IP addresses

13. Which of these is a widely used cryptographic hash function often associated with Bitcoin?

A) AES-128
B) SHA-256
C) RSA-2048
D) DES

14. A 'Transposition Cipher' works by doing what to the plaintext?

A) Replacing letters with numbers
B) Replacing letters with different letters
C) Rearranging the order of the letters
D) Changing the font of the letters

15. What is the main purpose of a 'Digital Signature' in electronic communication?

A) To verify the sender's identity and message integrity
B) To hide the contents of the message
C) To speed up the delivery of the email
D) To compress the file size