

Fundamentals of Cryptography

Cryptography · Answer Key · 18 Questions

1. Which type of cipher replaces each letter in the plaintext with a fixed letter a certain number of positions down the alphabet?

- A) Caesar cipher**
- B) Vigenère cipher
- C) Transposition cipher
- D) Rail fence cipher

2. What is the term for the original, readable message before it is encrypted?

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

3. The Enigma machine, used for encryption during World War II, was primarily operated by which nation?

- A) United Kingdom
- B) United States
- C) Germany**
- D) Japan

4. Which classic cipher uses a keyword to determine a series of different Caesar ciphers based on the letters of the keyword?

- A) Atbash cipher
- B) Vigenère cipher**
- C) Playfair cipher
- D) Scytale cipher

5. In cryptography, what is a 'key'?

- A) A physical metal object
- B) A piece of information that controls the encryption process**
- C) A type of computer virus
- D) The final encrypted message

6. Which ancient Greek device consisted of a cylinder wrapped with a strip of parchment to encrypt messages?

- A) Abacus
- B) Astrolabe
- C) Scytale**
- D) Antikythera mechanism

7. What is the process of converting encrypted data back into its original, readable form?

- A) Encoding
- B) Decoding
- C) Decryption**
- D) Transposition

8. The 'Atbash' cipher is a simple substitution cipher that works by reversing which of the following?

- A) The entire alphabet**
- B) The word order
- C) The sentence structure
- D) The frequency of vowels

9. Which field of study involves the practice and study of techniques for secure communication in the presence of third-party adversaries?

- A) Cryptography**
- B) Calligraphy
- C) Cartography
- D) Cryptology

10. In the context of the World War II era, who led the team at Bletchley Park that successfully cracked the Enigma code?

- A) Charles Babbage
- B) Alan Turing**
- C) Ada Lovelace
- D) John von Neumann

11. What is a cipher called if it changes the position of the letters in the message rather than substituting them for other letters?

- A) Substitution cipher
- B) Transposition cipher**
- C) Polyalphabetic cipher
- D) Monoalphabetic cipher

12. Which technique involves analyzing the frequency of letters in a ciphertext to break simple substitution ciphers?

- A) Frequency analysis**
- B) Brute force
- C) Key exchange
- D) Steganography

13. What term describes the practice of hiding a secret message within a non-secret file, such as an image or audio track?

- A) Encryption
- B) Cryptography
- C) Steganography**
- D) Hashing

14. Which of the following is an example of a symmetric-key algorithm?

- A) RSA
- B) AES**
- C) Diffie-Hellman
- D) ECC

15. What is the primary vulnerability of a simple Caesar cipher?

- A) It requires a computer
- B) It has a very small number of possible keys**
- C) It cannot be written down
- D) It only works on vowels

16. During World War I, the Zimmermann Telegram was an intercepted message that influenced which country to join the war?

- A) Australia
- B) Canada
- C) United States**
- D) France

17. A 'Polyalphabetic' cipher is one that uses:

- A) Only one substitution alphabet
- B) Multiple substitution alphabets**
- C) No alphabet at all
- D) Only prime numbers

18. What is 'brute force' in the context of cracking a code?

- A) Using physical force to open a safe
- B) Trying every possible key until the correct one is found**
- C) Using a supercomputer to analyze language patterns
- D) Stealing the key from the sender