

Fundamentals of Cryptography

Cryptography · Answer Key · 25 Questions

1. Which World War II German cipher machine used a series of rotating wheels to scramble messages?

- A) Enigma**
- B) Purple
- C) Lorenz
- D) Typex

2. What is the oldest known method of encryption, involving shifting letters in the alphabet by a set number of positions?

- A) Vigenere cipher
- B) Caesar cipher**
- C) Playfair cipher
- D) Rail fence cipher

3. Which polyalphabetic substitution cipher uses a keyword to determine the shift for each letter?

- A) Atbash cipher
- B) Vigenere cipher**
- C) Bacon's cipher
- D) ROT13

4. What was the primary goal of the 'SIGABA' machine used by the United States during World War II?

- A) Radio signal jamming
- B) Secret communication**
- C) Radar calibration
- D) Map encryption

5. The 'Zimmermann Telegram' was a decoded message sent by Germany to which country during World War I?

- A) France
- B) Russia
- C) Mexico**
- D) Japan

6. Which famous cryptanalyst led the team at Bletchley Park that cracked the Enigma code?

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

7. What type of cipher replaces each letter with its mirror image in the alphabet (A becomes Z, B becomes Y)?

- A) Affine cipher
- B) Atbash cipher**
- C) Beaufort cipher
- D) Null cipher

8. Which historical codebreaking device was the first electromechanical machine used to attack the Enigma?

- A) Colossus
- B) The Bombe**
- C) Differential Analyzer
- D) Difference Engine

9. What is the term for the process of converting plaintext into ciphertext?

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

10. Which American cryptographer is credited with coining the term 'information theory'?

- A) Bruce Schneier
- B) Claude Shannon**
- C) Whitfield Diffie
- D) Phil Zimmermann

11. The 'Great Cipher' was a highly secure system used by which French monarch?

- A) Louis XIV**
- B) Napoleon Bonaparte
- C) Charles X
- D) Francis I

12. What is the name of the modern cryptographic system that uses a pair of keys (public and private)?

- A) Symmetric key cryptography
- B) Asymmetric cryptography**
- C) Substitution cryptography
- D) Transposition cryptography

13. Which World War I cipher was famous for its use of a 5x5 grid of letters?

- A) Playfair cipher**
- B) Hill cipher
- C) Polybius square
- D) Bifid cipher

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

- A) Steganography**
- B) Cryptography
- C) Cryptanalysis
- D) Ciphertext

15. The 'Purple' code was a diplomatic cipher used by which country during the 1930s and 1940s?

- A) Italy
- B) Germany
- C) Japan**
- D) Spain

16. What is the primary function of a 'hash' function in computer security?

- A) Encryption of data
- B) Compression of files
- C) Verification of data integrity**
- D) Masking of IP addresses

17. Which historical cipher is based on the principle of writing a message in a zig-zag pattern?

- A) Rail fence cipher**
- B) Columnar transposition
- C) Scytale
- D) Book cipher

18. The 'Scytale' cipher, used by the ancient Spartans, relied on which object to read the message?

- A) A stone slab
- B) A rotating cylinder
- C) A wooden baton**
- D) A wax tablet

19. What is the standard length of an MD5 hash value in bits?

- A) 64 bits
- B) 128 bits**
- C) 256 bits
- D) 512 bits

20. Which historical group of people used a cipher based on the position of dots and dashes in a grid?

- A) Knights Templar
- B) Freemasons**
- C) Rosicrucians
- D) Carbonari

21. What does the acronym 'RSA' stand for in public-key cryptography?

- A) Rivest, Shamir, Adleman**
- B) Random Security Algorithm
- C) Robust Secure Architecture
- D) Remote System Access

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

- A) A physical lock
- B) A piece of information used by a cipher**
- C) A sequence of random numbers
- D) A protocol for communication

23. Which of these is a substitution cipher that uses a 2x2 matrix to transform pairs of letters?

- A) Hill cipher**
- B) Vigenere cipher
- C) Playfair cipher
- D) Baconian cipher

24. What was the name of the British codebreaking computer used to crack the Lorenz cipher?

- A) Enigma
- B) Colossus**
- C) Bombe
- D) Turing machine

25. What is the defining characteristic of a 'monoalphabetic' cipher?

- A) It uses a single key for all letters
- B) It uses multiple alphabets for encryption
- C) Each letter is replaced by a consistent substitute**
- D) It requires a computer to decode