Foundations of Cryptography

Cryptography · Practice Test · 8 Questions

1. Which historical cipher method involves shifting each letter in the plaintext by a fixed number of positions down the alphabet?

A) Vigenère cipher
B) Caesar cipher
C) Playfair cipher
D) Rail fence cipher

2. What is the primary difference between symmetric and asymmetric encryption?

A) Symmetric uses a public key; asymmetric uses no key.
B) Symmetric uses the same key for encryption and decryption.
C) Asymmetric encryption is always faster than symmetric.
D) Symmetric encryption was invented after the internet.

3. During World War II, which electro-mechanical rotor machine was famously used by the German military to encrypt communications?

A) Enigma machine
B) Purple machine
C) SIGABA
D) Typex

4. What is a 'polyalphabetic' cipher?

A) A cipher that uses only one substitution alphabet.
B) A cipher that uses multiple substitution alphabets to obscure patterns.
C) A cipher that requires no key to decrypt.
D) A cipher that translates letters into binary code only.

5. In the context of the Vigenère cipher, what is the 'keyword' used for?

A) To determine the length of the message.
B) To dictate the repeating sequence of shifts applied to the plaintext.
C) To generate a random prime number for decryption.
D) To act as a digital signature for the sender.

6. Which of the following is considered a modern cryptographic hash function?

A) SHA-256
B) Caesar shift
C) Atbash
D) Morse code

7. What is the 'frequency analysis' technique primarily used for in classical cryptanalysis?

A) To crack codes by counting the occurrence of letters in a ciphertext.
B) To measure the speed of an encryption algorithm.
C) To determine the strength of a firewall.
D) To encrypt files using prime numbers.

8. Which classic cipher replaces pairs of letters (digraphs) rather than single letters?

A) Playfair cipher
B) Substitution cipher
C) ROT13
D) Book cipher