Advanced Cryptology and Cryptanalysis

Cryptography · Practice Test · 18 Questions

1. Which mathematical property serves as the fundamental security basis for the RSA algorithm?

A) Integer factorization of large semiprimes
B) Discrete logarithm problems in finite fields
C) Elliptic curve scalar multiplication
D) Modular square roots of quadratic residues

2. In the context of the Enigma machine, what specific mechanical component prevented the simple substitution cipher from being trivial to solve?

A) The plugboard (Steckerbrett)
B) The reflector (Umkehrwalze)
C) The variable-speed motor
D) The paper tape perforator

3. What is the primary scientific reason that a One-Time Pad (OTP) cipher is theoretically unbreakable?

A) Infinite key length
B) Perfect secrecy defined by information theory
C) Quantum key distribution necessity
D) Complexity of polynomial-time algorithms

4. Alan Turing's 'Bombe' machine was designed to exploit which specific weakness in German Enigma traffic?

A) The use of non-repeating keys
B) The fact that a letter could never be encrypted as itself
C) The predictable sequence of rotor movements
D) The limited number of available plugboard combinations

5. Which cipher technique relies on the frequency analysis of letter combinations to overcome polyalphabetic substitution?

A) Kasiski examination
B) Vigenère square rotation
C) Playfair matrix transformation
D) Scytale transposition

6. The 'Lorenz cipher' used during WWII was a rotor machine that operated on which type of data stream?

A) Morse code dots and dashes
B) Baudot code (5-bit teleprinter code)
C) ASCII character encoding
D) Binary phase-shift keying

7. In modern cryptography, what does the 'Avalanche Effect' describe in block ciphers?

A) The rapid increase in computational cost with key length
B) A significant change in output after a minor change in input
C) The collapse of ciphertext under differential analysis
D) The process of generating high-entropy random numbers

8. Which of the following is classified as a 'Stream Cipher' rather than a 'Block Cipher'?

A) AES
B) DES
C) RC4
D) Blowfish

9. What was the primary method used by the U.S. Army's Signal Intelligence Service to solve the Japanese 'Purple' code?

A) Analog replication of the machine's stepping switches
B) Manual codebook recovery from a crashed aircraft
C) High-speed brute force using early vacuum tubes
D) Cryptanalysis of the Diplomatic 'Red' code

10. What is a 'meet-in-the-middle' attack primarily used to break?

A) Double encryption schemes
B) Public key exchange protocols
C) Diffie-Hellman key agreement
D) Hash functions with short output lengths

11. In elliptic curve cryptography (ECC), which problem provides the security?

A) The difficulty of finding the order of the group
B) The elliptic curve discrete logarithm problem
C) The difficulty of polynomial interpolation
D) The prime factorization of large curves

12. What was the 'Zimmermann Telegram' notable for in the history of cryptanalysis?

A) It was the first encrypted radio transmission
B) It utilized a transposition cipher that was broken by British Room 40
C) It was the first instance of quantum-resistant encryption
D) It proved the futility of the Playfair cipher

13. Which of these describes the 'Birthday Attack' in the context of hash functions?

A) Searching for two different inputs that produce the same hash
B) Predicting the output based on the user's birthdate
C) A brute force attack on key schedules
D) Exploiting the lack of randomness in salts

14. In the context of the Caesar cipher, what is the maximum number of distinct keys possible?

A) 25
B) 26
C) 127
D) 256

15. What type of cryptographic primitive is used to ensure data integrity without providing confidentiality?

A) Symmetric key
B) Digital signature
C) Cryptographic hash function
D) Homomorphic encryption

16. Which early 20th-century cipher machine was famous for using a system of interlocking rotors with multiple contact points?

A) The Enigma
B) The Sigaba
C) The M-209
D) The Hagelin C-36

17. What does 'Forward Secrecy' guarantee in an encrypted communication session?

A) That keys are changed for every packet
B) That compromised long-term keys do not compromise past session keys
C) That the message cannot be read before decryption
D) That the key remains valid for future sessions

18. Which of the following is a common transposition cipher that rearranges columns based on a keyword?

A) Columnar Transposition
B) Rail Fence Cipher
C) Atbash Cipher
D) Affine Cipher