Q1. What type of cipher is the Vernam cipher?

- Polyalphabetic substitution cipher
- One-Time Pad (OTP)
- Transposition cipher
- Stream cipher

  Answer: One-Time Pad (OTP)

  Explanation: The Vernam cipher is a type of One-Time Pad cipher using XOR operation.

Q2. What operation is used in Vernam cipher encryption?

- Modular addition
- XOR (exclusive OR)
- Matrix multiplication
- Caesar shift

  Answer: XOR (exclusive OR)

  Explanation: Vernam cipher uses XOR between plaintext and key bits for encryption.

Q3. What is the key requirement for the Vernam cipher to be perfectly secure?

- Key must be shorter than plaintext
- Key must be reused multiple times
- Key must be truly random and as long as the plaintext
- Key can be any string

  Answer: Key must be truly random and as long as the plaintext

  Explanation: Security depends on using a random key of the same length as plaintext, used only once.

Q4. What happens if the Vernam key is reused?

- Encryption becomes more secure
- The cipher can be broken easily
- The key resets automatically
- Nothing changes

  Answer: The cipher can be broken easily

  Explanation: Reusing key compromises security and allows attackers to find

plaintext.

Q5. What is the main advantage of the Vernam cipher?

- Simple to implement and perfectly secure with right key
- Works with any length key
- No need to share the key
- Based on prime numbers

Answer: Simple to implement and perfectly secure with right key
Explanation: With a truly random key used once, Vernam cipher is theoretically unbreakable.

Q6. What is the output if you XOR a bit with itself in Vernam cipher?

- 1
- 0
- Same bit
- Depends on bit

Answer: 0
Explanation: XOR of a bit with itself is always 0.

Q7. How is decryption done in Vernam cipher?

- Using modular subtraction
- Using XOR of ciphertext with the key
- Reversing ciphertext
- Applying matrix inverse

Answer: Using XOR of ciphertext with the key
Explanation: Decryption is identical to encryption: ciphertext XOR key yields plaintext.

Q8. Which historical figure is associated with the invention of the Vernam cipher?

- Claude Shannon
- Gilbert Vernam
- Alan Turing
- August Kerckhoffs

Answer: Gilbert Vernam

Explanation: Gilbert Vernam invented the cipher in 1917.

Q9. The Vernam cipher is best classified as:

- Symmetric key cipher
- Asymmetric key cipher
- Hash function
- Public key algorithm

Answer: Symmetric key cipher
Explanation: The same key is used for both encryption and decryption.

Q10. If the key in Vernam cipher is all zeros, what is the ciphertext?

- All ones
- Same as plaintext
- Random
- All zeros

Answer: Same as plaintext
Explanation: XOR with zero leaves plaintext unchanged.

Q11. Why is key distribution a major challenge for Vernam cipher?

- Keys are too short
- Keys must be securely shared and as long as plaintext
- Keys are public
- No keys are required

Answer: Keys must be securely shared and as long as plaintext
Explanation: Securely distributing long random keys is difficult in practice.

Q12. Which modern technique is similar in principle to Vernam cipher?

- AES encryption
- Stream ciphers using XOR
- RSA algorithm
- Hashing

Answer: Stream ciphers using XOR
Explanation: Many stream ciphers XOR plaintext with a pseudorandom keystream.

Q13. What happens to ciphertext if the key bit is flipped in Vernam cipher?

- Corresponding ciphertext bit flips
- No change
- All ciphertext bits change
- Only first bit changes

Answer: Corresponding ciphertext bit flips
Explanation: XOR changes bit only at positions where key bit is flipped.

Q14. Which of these is NOT true about Vernam cipher?

- Key must never be reused
- Perfect secrecy is guaranteed with random key
- Ciphertext length equals plaintext length
- Uses modular addition for encryption

Answer: Uses modular addition for encryption
Explanation: Vernam cipher uses XOR, not modular addition.

Q15. Vernam cipher encryption and decryption can be performed efficiently on computers because:

- XOR operation is fast and simple
- It requires complex math
- It uses large prime numbers
- It needs quantum computers

Answer: XOR operation is fast and simple
Explanation: XOR is a simple bitwise operation, very efficient to compute.