Q1. What type of cipher is the Vigenère cipher?

- Substitution cipher
- Transposition cipher
- Polyalphabetic substitution cipher
- Stream cipher

  Answer: Polyalphabetic substitution cipher
  Explanation: Vigenère cipher uses multiple Caesar ciphers with different shift values based on a keyword.

Q2. How is the key used in the Vigenère cipher?

- Repeated cyclically to match plaintext length
- Used once and discarded
- Added to the plaintext
- Multiplied with plaintext

  Answer: Repeated cyclically to match plaintext length
  Explanation: The key is repeated to match the length of the plaintext for encryption.

Q3. Which of these is the main weakness of the Vigenère cipher?

- Key length is too long
- Key is reused and can be detected
- Only works with numbers
- It's a symmetric cipher

  Answer: Key is reused and can be detected
  Explanation: Repeated keys can be detected via frequency analysis, making Vigenère vulnerable.

Q4. Which method is commonly used to attack the Vigenère cipher?

- Brute force
- Frequency analysis
- Kasiski examination
- Chosen plaintext attack

  Answer: Kasiski examination
  Explanation: Kasiski examination finds repeated sequences to guess key length.

Q5. In the Vigenère cipher, encryption of a letter involves:

- Adding key letter shift mod 26
- XORing with key letter
- Multiplying ASCII codes
- Reversing plaintext

  Answer: Adding key letter shift mod 26
  Explanation: Each plaintext letter is shifted by the key letter's position in the alphabet.

Q6. If the key length equals the plaintext length and key is random, the Vigenère cipher becomes:

- Caesar cipher
- One-Time Pad
- Hill cipher
- Transposition cipher

  Answer: One-Time Pad
  Explanation: A Vigenère cipher with a truly random key as long as plaintext is effectively a One-Time Pad.

Q7. What alphabet does the classic Vigenère cipher use?

- Binary digits
- English alphabet (A-Z)
- ASCII characters
- Unicode characters

  Answer: English alphabet (A-Z)
  Explanation: It typically uses the 26 letters A-Z.

Q8. Which of the following best describes the key in the Vigenère cipher?

- Numeric string
- Alphabetic string
- Random binary string
- Matrix

  Answer: Alphabetic string
  Explanation: The key is an alphabetic string repeated for encryption.

Q9. What does the Vigenère square or table contain?

- Rows of shifted alphabets
- Random numbers
- XOR operations
- Matrices

  Answer: Rows of shifted alphabets
  Explanation: Each row is a Caesar shifted alphabet used to encrypt letters.

Q10. Vigenère cipher was considered unbreakable for:

- Thousands of years
- About 300 years
- Almost a century
- Until computers were invented

  Answer: Almost a century
  Explanation: It was called "le chiffre indéchiffrable" for a long time before attacks like Kasiski's were found.

Q11. What is the main difference between the Caesar cipher and the Vigenère cipher?

- Vigenère uses multiple keys, Caesar uses one
- Caesar uses multiple keys, Vigenère uses one
- Both use same key length
- Caesar cipher is polyalphabetic

  Answer: Vigenère uses multiple keys, Caesar uses one
  Explanation: Vigenère uses a keyword to shift letters differently, unlike Caesar's single fixed shift.

Q12. How do you decrypt a Vigenère ciphertext?

- Add the key letters modulo 26
- Subtract the key letters modulo 26
- XOR with key letters
- Multiply by inverse matrix

  Answer: Subtract the key letters modulo 26
  Explanation: Decryption is done by subtracting the key's letter values from the ciphertext letters.

Q13. Which modern cryptography concept was inspired by the polyalphabetic idea in Vigenère?

- Public key cryptography
- Block cipher
- Stream cipher
- Quantum cryptography

  Answer: Stream cipher

  Explanation: Stream ciphers use varying keys like polyalphabetic ciphers to increase security.

Q14. What is the complexity of brute forcing a Vigenère cipher dependent on?

- Size of the alphabet
- Length of the key
- Length of plaintext
- Speed of computer

  Answer: Length of the key

  Explanation: Longer keys increase the complexity of brute force attacks exponentially.

Q15. In the Vigenère cipher, what happens if the key is the letter 'A' repeated?

- No encryption happens
- Plaintext shifts by 1
- Ciphertext is reversed
- Encryption is strongest

  Answer: No encryption happens

  Explanation: 'A' corresponds to zero shift, so plaintext remains unchanged.