Q1. What type of cipher is the Railfence cipher?

- Substitution cipher
- Transposition cipher
- Stream cipher
- Block cipher

  Answer: Transposition cipher

  Explanation: Railfence is a transposition cipher that rearranges letters.

Q2. How does the Railfence cipher encrypt a message?

- By substituting letters with others
- By writing letters diagonally over rails and reading row-wise
- By XORing letters with a key
- By shifting letters by a fixed number

  Answer: By writing letters diagonally over rails and reading row-wise

  Explanation: Plaintext is written in zigzag across rails, then read line by line.

Q3. What is the key in the Railfence cipher?

- A numeric shift value
- The number of rails
- A substitution alphabet
- A random key string

  Answer: The number of rails

  Explanation: The key is the number of rails (rows) used in zigzag writing.

Q4. For the plaintext 'HELLO' and 2 rails, what is the ciphertext?

- HLOEL
- HOELL
- HELLO
- HLLOE

  Answer: HLOEL

  Explanation: Zigzag: H L O (top), E L (bottom), read rows: H L O E L.

Q5. What happens if you use only 1 rail in Railfence cipher?

- It becomes a substitution cipher

- Ciphertext equals plaintext
- Encryption fails
- Text is reversed

  Answer: Ciphertext equals plaintext
  Explanation: With 1 rail, letters stay in order, no change occurs.

Q6. How is decryption performed in Railfence cipher?

- Reversing the zigzag pattern based on key
- Using modular arithmetic
- Applying XOR with the key
- Shifting letters backward

  Answer: Reversing the zigzag pattern based on key
  Explanation: Decryption reconstructs the zigzag shape to read plaintext.

Q7. Which of these best describes Railfence cipher security?

- Very strong and unbreakable
- Weak, vulnerable to frequency analysis
- Moderate, vulnerable to brute force
- Perfect secrecy

  Answer: Moderate, vulnerable to brute force
  Explanation: Simple transposition can be brute forced easily with small keys.

Q8. If the key (number of rails) is 3, how are letters arranged?

- In three horizontal rows with zigzag pattern
- In a single row
- Randomly distributed
- Only in two rows

  Answer: In three horizontal rows with zigzag pattern
  Explanation: Letters placed diagonally across 3 rails forming zigzag.

Q9. Railfence cipher is a type of:

- Monoalphabetic cipher
- Polyalphabetic cipher
- Permutation cipher

- Steganographic technique
  Answer: Permutation cipher
  Explanation: It permutes (rearranges) the letters without substitution.

Q10. What is the ciphertext of 'WEAREDISCOVERED' with 2 rails?

- WRSOEVEAEDCIRD
- WESVDEAECRRDIO
- WECRLTEERDSOEEFEAOCVDE
- WAEICDRSDVOREE
  Answer: WRSOEVEAEDCIRD
  Explanation: Letters written in zigzag across 2 rails and read row-wise.

Q11. Which property does Railfence NOT possess?

- Substitution of letters
- Rearrangement of letters
- Uses key as number of rails
- Can be decrypted with key
  Answer: Substitution of letters
  Explanation: Railfence does not substitute letters, only reorders them.

Q12. Railfence cipher can be combined with which cipher to increase security?

- Caesar cipher
- Vigenère cipher
- Hill cipher
- Any substitution cipher
  Answer: Any substitution cipher
  Explanation: Combining transposition with substitution ciphers improves security.

Q13. Why is Railfence cipher considered a classical cipher?

- It uses modern encryption techniques
- It is simple and was used historically
- It is based on quantum principles
- It requires computers
  Answer: It is simple and was used historically

Explanation: Railfence is one of the earliest ciphers, simple and manual.

Q14. The zigzag pattern in Railfence cipher means:

- Letters are written diagonally down and up across rails
- Letters are shifted by key
- Letters are replaced by numbers
- Letters are sorted alphabetically

Answer: Letters are written diagonally down and up across rails
Explanation: Zigzag means moving down and up over rails while writing letters.

Q15. What is a major weakness of Railfence cipher?

- The key space is very small
- It uses complex mathematics
- It needs large keys
- It is computationally expensive

Answer: The key space is very small
Explanation: Number of rails is usually small, making brute force easy.