**Caesar Cipher Quiz**

**Q1. What is the Caesar Cipher primarily used for?**

- Data compression
- Encrypting text
- Sorting data
- Decoding barcodes

  **Answer:** Encrypting text

  **Explanation:** The Caesar Cipher is a type of substitution cipher used mainly for encrypting text by shifting letters.

**Q2. If 'A' becomes 'D', what is the shift key?**

- 2
- 3
- 4
- 5

  **Answer:** 3

  **Explanation:** Since A shifted to D is a shift of 3 letters forward, the key is 3.

**Q3. What happens if you apply Caesar Cipher twice with key 13?**

- You get the original text
- It becomes undecipherable
- It's encrypted stronger
- It loops endlessly

  **Answer:** You get the original text

  **Explanation:** Applying the cipher twice with a key of 13 returns you to the original text because 13 is half the alphabet length.

**Q4. Which of these letters does NOT change with a Caesar Cipher key of 0?**

- A
- M
- Z
- All of them

  **Answer:** All of them

  **Explanation:** A shift key of 0 means no change; all letters remain the same.

**Q5. Why is the Caesar Cipher considered a weak encryption method?**

- It uses complex mathematical functions
- It can be easily broken by frequency analysis
- It requires a large key
- It encrypts binary data only

  **Answer:** It can be easily broken by frequency analysis

  **Explanation:** Caesar Cipher shifts letters uniformly and does not disguise letter frequency, making it vulnerable to simple frequency analysis.

**Q6. What is the size of the key space for a Caesar Cipher applied to the English alphabet?**

- 26
- 25
- 128
- 256

  **Answer:** 25

  **Explanation:** Because a shift of 0 or 26 results in the original text, there are only 25 meaningful keys.

**Q7. How does the Caesar Cipher handle non-alphabetic characters like numbers or punctuation?**

- Encrypts them the same way as letters
- Leaves them unchanged
- Removes them
- Converts them to letters before encrypting

  **Answer:** Leaves them unchanged

  **Explanation:** Typically, Caesar Cipher only shifts alphabetic characters and leaves others like numbers and punctuation unchanged.

**Q8. Explain how to decrypt a message encoded with a Caesar Cipher if the key is unknown.**

- Try all possible shifts (brute force)
- Use a one-time pad
- Apply the same key twice

- Use a hash function
  **Answer:** Try all possible shifts (brute force)
  **Explanation:** Since the key space is small, one can try all 25 possible shifts and check which one produces meaningful text.

**Q9. Is the Caesar Cipher symmetric or asymmetric encryption? Why?**

- Symmetric, because the same key is used for encryption and decryption
- Asymmetric, because it uses two different keys
- Symmetric, because it uses public keys
- Asymmetric, because it uses private keys
  **Answer:** Symmetric, because the same key is used for encryption and decryption
  **Explanation:** Caesar Cipher uses the same key (the shift value) for both encrypting and decrypting, making it symmetric encryption.

**Q10. Can the Caesar Cipher be used securely for modern communication? Explain.**

- Yes, because it's very complex
- No, because it's easily broken
- Yes, if the key is very large
- No, because it only encrypts numbers
  **Answer:** No, because it's easily broken
  **Explanation:** The Caesar Cipher is too simple and vulnerable to attacks, so it's not suitable for secure modern communication.

**Q11. What is the relationship between Caesar Cipher and ROT13?**

- ROT13 is a Caesar Cipher with a shift of 13
- ROT13 is a type of hash function
- ROT13 doubles the shift each time
- ROT13 is unrelated to Caesar Cipher
  **Answer:** ROT13 is a Caesar Cipher with a shift of 13
  **Explanation:** ROT13 is a special case of Caesar Cipher where the shift key is fixed at 13.

**Q12. If you apply the Caesar Cipher with a shift of 26 to any text, what is the result?**

- The original text
- The text is fully scrambled
- Only vowels are shifted
- An error occurs

  **Answer:** The original text

  **Explanation:** A shift of 26 equals the alphabet length, so the text remains unchanged.

**Q13. Can the Caesar Cipher be combined with other ciphers for better security? Give an example.**

- Yes, for example combining with Vigenère Cipher
- No, it cannot be combined
- Yes, it encrypts images better
- No, it's a hashing algorithm

  **Answer:** Yes, for example combining with Vigenère Cipher

  **Explanation:** Caesar Cipher can be part of a multi-layer encryption system to increase security, such as in polyalphabetic ciphers like Vigenère.