## **❓ Practice Q&A**

### **Multiple Choice Questions**

1. **Which of the following is a symmetric-key algorithm?**
   * A) RSA
   * B) ElGamal
   * C) AES
   * D) ECC
2. **Answer**: C) AES
3. **In RSA, what is the relationship between e and d?**
   * A) e \* d ≡ 1 mod n
   * B) e + d = n
   * C) e \* d ≡ 1 mod ϕ(n)
   * D) e = d
4. **Answer**: C) e \* d ≡ 1 mod ϕ(n)

### **Fill-in-the-Blanks**

1. **In a stream cipher, encryption is performed by computing ci = pi ⊕ ki, where pi is the plaintext bit and ki is the \_\_\_\_\_\_\_\_\_\_.** **Answer**: keystream bit
2. **The RSA algorithm relies on the difficulty of factoring large \_\_\_\_\_\_\_\_\_\_ numbers.** **Answer**: composite

### **Short Answer Questions**

1. **Explain the avalanche effect in block ciphers.** **Answer**: The avalanche effect refers to the property of block ciphers where a small change in the plaintext or key results in a significant and unpredictable change in the ciphertext, enhancing security by making patterns less discernible.
2. **Why is it important for e and ϕ(n) to be coprime in RSA?** **Answer**: e and ϕ(n) must be coprime to ensure that a modular inverse d exists, which is necessary for the decryption process in RSA.