Pre Lab:-

1. What is the one-time pad encryption technique?
The one-time pad is a symmetric encryption technique where a random key, as long as the plaintext, is used to encrypt the message, and the same key is used for decryption.

2. What are the key characteristics of a one-time pad?
The key must be completely random, as long as the message, used only once, and securely shared between the sender and receiver.

3. Why is the one-time pad considered a perfect encryption technique?
It offers theoretically perfect security because the ciphertext reveals no information about the plaintext if the key is random and used only once.

4. What are the main vulnerabilities or limitations of the one-time pad?
The key distribution is challenging, and the system is only secure if the key is truly random, as long as the message, and never reused.

5. How does the security of the one-time pad compare to other encryption techniques?
The one-time pad is the most secure encryption method but impractical for large-scale use due to key management, whereas modern techniques like AES balance security and practicality.

VIVA:-

1. Can the one-time pad be vulnerable to known-plaintext attacks or chosen-plaintext attacks?
No, the one-time pad is theoretically immune to known-plaintext or chosen-plaintext attacks when properly implemented, as the ciphertext reveals no information about the plaintext.

2. What are some practical applications or historical uses of the one-time pad?
It was historically used in military and diplomatic communications, such as during World War II and the Cold War, for secure communication between high-level officials.

3. What are some examples of errors in implementing the one-time pad that could compromise its security?
Reusing a key or failing to generate truly random keys can lead to vulnerabilities, allowing attackers to potentially recover the plaintext through cryptanalysis.

4. How does the XOR operation play a crucial role in the one-time pad encryption?
The XOR operation combines each bit of the plaintext with the corresponding bit of the key, making it simple to both encrypt and decrypt messages using the same operation.

5. What are some modern alternatives to the one-time pad that address its limitations?
Modern encryption algorithms like AES and RSA are more practical, offering strong security without requiring keys as long as the message or the need for perfect randomness.