PRE LAB:-

1. What is the Vigenère cipher, and how does it differ from the Caesar cipher?

A polyalphabetic substitution cipher that uses a keyword to shift letters in the plaintext, differing from the Caesar cipher which uses a single fixed shift for all letters.

2. Explain the process of encryption using the Vigenère cipher.2.

Encrypt each letter of the plaintext by shifting it according to the corresponding letter of the keyword, repeating the keyword as needed.

3. How does the Vigenère cipher use a keyword or phrase as its key?

The Vigenère cipher uses a repeating keyword to determine shifting amounts for each letter in the plaintext, providing a variable shift for each position.

4. How does the Caesar cipher handle spaces and punctuation in the plaintext?

The key space is significantly larger than the Caesar cipher as it depends on the length and complexity of the keyword, making it more resistant to attacks.

5. What is the advantage of using the Vigenère cipher over the Caesar cipher?

The Vigenère cipher offers stronger security than the Caesar cipher by using multiple shifts based on the keyword, thus reducing predictability and vulnerability.

VIVA :-

1.How does the Vigenère cipher achieve polyalphabetic substitution, and why is it more resistant to frequency analysis?

The Vigenère cipher uses a keyword to determine multiple shift values for encryption, changing the substitution alphabet for each letter based on the keyword, which makes it more resistant to frequency analysis by varying the substitution patterns.

2. **Discuss the process of decrypting a message encrypted with the Vigenère cipher.**

Decrypt by reversing the encryption process—subtract the shift values determined by the keyword from each letter in the ciphertext and wrap around the alphabet as needed.

3. **What are some weaknesses of the Vigenère cipher, and how can they be exploited in cryptanalysis?**

The Vigenère cipher can be vulnerable to frequency analysis attacks, especially with short keywords. Methods like Kasiski examination and Friedman test can exploit repeating patterns and keyword length.

4. **How does the length of the keyword affect the security of the Vigenère cipher?**

Longer keywords provide better security as they make the repeating patterns less apparent, increasing resistance to frequency analysis and making the cipher harder to break.

5. **Compare the security and efficiency of the Vigenère cipher with modern encryption algorithms.**

Modern encryption algorithms like AES are far more secure and efficient than the Vigenère cipher due to their complex key management, resistance to various attacks, and advanced cryptographic techniques.