**Information Security Practicals**

1. Implement the error correcting code.

2. Implement the error detecting code.

3. Implement caesar cipher substitution operation.

4. Implement monoalphabetic and polyalphabetic cipher substitution operation.

5. Implement playfair cipher substitution operation.

6. Implement hill cipher substitution operation.

7. Implement rail fence cipher transposition operation.

8. Implement row transposition cipher transposition operation.

9. Implement product cipher transposition operation.

10. Illustrate the Ciphertext only and Known Plaintext attacks.

11. Implement a stream cipher technique.

**ANSWER 10**

**CipherText-only Attack**

A ciphertext-only attack is an attack in which an attacker only has access to the ciphertext, the encrypted version of a message, and does not have any knowledge about the plaintext or the encryption algorithm used. The goal of a ciphertext-only attack is to try and recover the plaintext message or the encryption key that was used to encrypt the message. The attacker typically uses various cryptanalysis techniques like frequency analysis, statistical analysis, and pattern recognition to try and break the encryption.

* Frequency analysis: In this technique, the attacker analyses the frequency of each character or symbol in the ciphertext to try and identify patterns that can reveal information about the underlying language used in the plaintext. For example, in English language text, the letter 'e' appears more frequently than other letters, so the attacker can try to identify the most frequent characters in the ciphertext and guess that they correspond to the letter 'e'.
* Statistical analysis: This technique involves analysing the statistical properties of the ciphertext, such as its entropy or randomness. The attacker may try to identify any biases or patterns in the ciphertext that can reveal information about the encryption algorithm or key.
* Pattern recognition: In this technique, the attacker looks for repeating patterns or sequences in the ciphertext that can reveal information about the plaintext or the encryption algorithm. For example, if the attacker notices that a certain sequence of characters in the ciphertext is always followed by another specific sequence, they may be able to deduce some information about the plaintext or the encryption algorithm.

Ciphertext only attacks can be very difficult to perform successfully, especially if the encryption algorithm and key are strong and the attacker does not have any additional information or context about the message or the encryption process.

**Known Plaintext Attack**

A known plaintext attack is an attack in which an attacker has access to both the plaintext message and its corresponding ciphertext. The goal of a known plaintext attack is to determine the encryption key that was used to encrypt the message. The attacker can use the known plaintext and its corresponding ciphertext to deduce information about the encryption algorithm and its parameters. The attacker may also use cryptanalysis techniques like differential cryptanalysis, linear cryptanalysis, and algebraic attacks to try and break the encryption.

For example, suppose Alice wants to send a secret message to Bob. Alice encrypts the message using a secret key and sends the ciphertext to Bob. An attacker who intercepts the ciphertext can launch a ciphertext-only attack to try and recover the plaintext message or the encryption key. However, if the attacker knows the plaintext of the message, they can launch a known plaintext attack to try and deduce the encryption key.

Overall, both ciphertext only attacks and known plaintext attacks are important cryptanalysis techniques that can be used to try and break encryption. It's important for cryptographers and security professionals to be aware of these attacks and to design strong encryption algorithms and keys that can withstand them.