PRACTICAL FILE

Name : Ujjawal kumar

College roll no. :20201441

Exam roll no. :20020570038

Subject : Information Security

Course : BSc. (H) Computer Science

Semester : 6th Sem, 3rd Year

Submitted to :Mr. Sahil Sir

Date :30thApril,2023

(Ramanujan College)

Q10) Illustrate the Ciphertext only and Known Plaintext attacks.

Illustration:

Ciphertext

Ciphertext-only attack:

In a ciphertext-only attack, an attacker has access only to the encrypted data, without any knowledge of the plaintext or the encryption key. The attacker's goal is to recover the original plaintext or the encryption key. Ciphertext-only attacks are difficult to carry out because the attacker has no information to work with except the ciphertext. The attacker needs to analyze the patterns and properties of the ciphertext to gain insight into the encryption algorithm and then use this information to try to decrypt the message. Ciphertext-only attacks are typically successful against weak encryption algorithms and short keys.

Ciphertext-only attack example:

Suppose an attacker intercepts a series of encrypted messages that were encrypted using a simple substitution cipher. The attacker doesn't know the original plaintext or the encryption key, but they do know that the messages are in English. The attacker could use frequency analysis to analyze the frequency of each letter in the ciphertext and try to infer the most likely mapping between the ciphertext letters and the original plaintext letters. With enough ciphertext samples, the attacker could eventually crack the encryption key and decrypt the messages.

Ciphertext-only attack algorithm:

1. Collect a sufficient amount of ciphertext samples.
2. Analyze the frequency of each letter in the ciphertext.

3. Identify the most frequently occurring ciphertext letters and try to map them to the most frequently occurring letters in the original language.
4. Use the identified mappings to infer additional mappings between other ciphertext and plaintext letters.
5. Test the inferred mappings by decrypting a subset of the ciphertext and checking if the resulting plaintext is meaningful.
6. Iterate steps 3-5 until the entire message is decrypted.

Plaintext

Known plaintext attack:

In a known plaintext attack, an attacker has access to both the plaintext and the corresponding ciphertext. The attacker's goal is to recover the encryption key. Known plaintext attacks are easier to carry out than ciphertext-only attacks because the attacker has some knowledge of the plaintext and can use this to infer information about the encryption key. The attacker needs to analyze the patterns and properties of the plaintext and the corresponding ciphertext to gain insight into the encryption algorithm and then use this information to try to decrypt the message. Known plaintext attacks are typically successful against weak encryption algorithms and short keys, and are sometimes used to break historical ciphers that are no longer in use.

Known plaintext attack example:

Suppose an attacker intercepts an encrypted message and also knows the corresponding plaintext message. The attacker could use this knowledge to infer information about the encryption algorithm and the encryption key. For example,

if the attacker knows that the plaintext message contains a specific word or phrase, they could look for patterns in the ciphertext that correspond to that word or phrase. With enough known plaintext samples, the attacker could eventually deduce the encryption key and decrypt other messages that were encrypted using the same key.

Known plaintext attack algorithm:

1. Collect a sufficient amount of known plaintext and corresponding ciphertext samples.
2. Look for patterns in the ciphertext that correspond to the known plaintext.
3. Use the patterns to infer information about the encryption algorithm and the encryption key.
4. Test the inferred encryption key by decrypting a subset of the ciphertext and checking if the resulting plaintext is meaningful.
5. If the encryption key is incorrect, adjust the inferred key and repeat step 4.
6. Once the entire message is decrypted, verify the accuracy of the decrypted plaintext.