Practical No. 1

Aim:— To study cryptography and network security.

Theory:—

Cryptography is techique of securing information and communication through use of codes so that only those person for whom the information is intended can understand it and process it. The preventing unalthorized access to information. The prefix "crypt" means hidden and suffix "graphy" means writing. In the cryptography, the ~~thee~~ techique which are used to protect information are obtained from mathematical concepts and a set of rules based calculations known as algorithms to convert messages in a way that make it hard to decode it. Those algorithm are used for cryptography key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transaction such as credit card and debit card transaction.

Technique used for cryptography:—

In today's age of computers, cryptography is often associated with the process where an ordinary plaintext is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption.

The process of conversion of cipher text to plaintext is known as decryption.

Features of Cryptography:—

(i) Confidentiality

Information can only be accessed by the person for whom it is intended for and no other person except him can access ~~the~~ it.

(ii) Integrity

Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.

(iii) Authentication

The identities of sender and receiver are conformed as well as destination of information is conformed.

What are cryptography attack:—

A cryptography attack is a method used by hackers to target cryptographic solution like cipher text, encryption keys, etc. Those attacks aim to retrieve the plain text from the cipher text or decodes the encrypted data. Hackers may attempt to bypass the security of a cryptographic system by discovering weaknesses and flaws in cryptography technique, cryptography protocols, encryption algorithms or key management strategies.

Passive and Active attacks:—

1) Passive attack:—

Passive cryptography ~~to~~ attack intend to obtain unauthorized access to sensitive data or information by incepting or eavesdropping or generating communication. In this situation, the data and the commuation remain intact and not tempered with.

2) Active attack:—

On the other hand, active cryptography attack involves some kind of modification of the data or communication. In this case, the attackers not only gain access to data but also tempers with it.

Type of cryptographic attacks :—

1) Brute force attack :—

Public and private key play a significant role in encrypting and decrypting ~~tha~~ the data in a cryptographic system. In brute force attack, the attacker tries various private keys to decipher the encrypted message or data. If the key size is 8-bit, the possible key will be 256.

2) Cipher text only attack

In this attack, the attacker gain access to a collection of cipher text. Through the ~~con~~ collection through this attack technique, the attacker can occasionally determine the key.

3) Chosen plaintext attack

In this type, the cyber criminal can choose arbitrary plaintext data to obtain the cipher text. It simplifies the attacker task of resolving the encryption keys.

4) Chosen ciphertext attack

In this attack, the ~~cyr~~ cyber criminal ~~and~~ a chosen ciphertext corresponding to its plaintext. The attacker tries to obtain a secret key or the details about the system. By analyzing the chosen cipher text and relating it to the plaintext the attacker attempts to guess the key.

5) Known plaintext attack

In this attack technique, the cyber criminal finds knows the plaintext of some portions of the cipher text using information gathering technique.

Conclusion: —

Cryptography and network security has been studied successfully.

Ashahakar
A