

## Assignment - I

Date \_\_\_\_\_  
Page \_\_\_\_\_

Q-1 Explain various type of Attack on Computer System

## (i) Passive Attack

→ The attacker only monitors the traffic attacking the confidentiality of the data. It contains release of message contents and traffic analysis.

## (1) Release of message contents

→ The release of message contents is easily understood.

→ A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information.

→ We would like to prevent an opponent from learning the contents of these transmissions.

## (2) Traffic analysis

→ A second type of passive attack, traffic analysis is

→ Suppose that we had a way of masking the contents of message or other information.

→ Even if they captured the message, could not extract the information from the message.



- Even if they captured the message, could not extract the information from the message
- The common technique for masking contents is encryption
- If we had encryption protection in place, an opponent might still be able to observe the pattern of these messages
- Passive attacks are very difficult to detect because they do not involve any alteration of the data
- Typically, the message traffic is sent and received in an apparently normal fashion and the sender nor receiver is aware that a third party has read the messages nor observed the traffic pattern

## (ii) Active attack

- Attacker tries to alter transmitted data. It includes masquerade, modification, replay and denial of service.

### (1) Masquerade

- A masquerade takes place when one entity pretends to be a different entity. A masquerade attack usually includes



one of the other forms of active attack

## (2) Replay:

→ Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect

## (3) Modification of message

→ Modification of message simply means that some portion of a legitimate message is altered, or that message is delayed or retransmitted, to produce an unauthorized effect

→ For example, a message meaning "Allow John Smith to send confidential file accounts" is modified to mean "Allow Fred Brown to send confidential file accounts"

## (4) Denial of service

→ The denial of service or inhibits the normal use or management of communications facilities

→ This attack may have a specific target for example, an entity may suppress all messages directed to a particular destination

→ Another form of service is the disruption of an entire network, either by



disabling the network or by overloading it with messages leads to degradable performance

2-2) Define terms cryptanalysis. Explain various types of cryptanalytic attacks

- Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some simple plaintext-ciphertext pairs. This type of attack finds characteristic of the algorithm to find a specific plaintext or to find key.
- Based on the amount of information known to the cryptanalyst cryptanalytic attacks can be categorized as

(i) Ciphertext only Attack:-

The attacker knows only ciphertext only. It is easiest to defend.

(ii) Known Plaintext Attack:-

In this type of attack, the opponent has some plaintext-ciphertext



pairs, or the analyst may know that certain plaintext patterns will appear in a message. For example, there may be a standardized header or banner to a electronic funds transfer message and the attacker can use that for generating plaintext-cipher text pairs.

### (iii) Chosen plaintext :-

If the analyst is able somehow to get the source system to insert into the system a message chosen by the analyst, then a chosen-plaintext attack is possible.

### (iv) Chosen cipher text :-

In this attack, the analyst has cipher text and some plaintext-cipher text pairs where cipher text has been chosen by the analyst.

### (v) Chosen Text :-

Here, the attacker has got cipher text, chosen plaintext-cipher text pairs and chosen cipher text-plaintext pairs.



Q-3

What is Play fair cipher with suitable example

→ In this technique multiple letters are encrypted at a time

→ This technique uses  $5 \times 5$  matrix which is also called key matrix

M	O	N	A	R
C	H	X	B	D
E	F	G	I	K
L	P	Q	S	T
V	W	Y	Z	

→ The Plaintext is encrypted two letters at a time

→ Break the plaintext into pairs of two consecutive letters

→ If pair is repeated letter, insert a filler like x in the plaintext eg.

Balloon is created as "bo lx lo on"

→ If both letters fall in the same row of the key matrix, replace each with the letter to its right eg. "AR" encrypts as "RM".



→ If both letters fall in same column, replace each with the letter below it.  
eg. "MV" encrypts to "CM"

→ otherwise each letter is replaced by the one in its row in the column of the other letter of the pair eg. "HS" encrypts to "BP" and "EA" to "JM"

→ Security is much improved over monoalphabetic as here two letters are encrypted at a time and hence there are  $26 \times 26 = 676$  diagrams and hence it needs a 676 entry frequency table.

→ However it can be broken even if a few hundred letters are known as much of plaintext structure is retained in cipher text.

→ Example

Key: monarchy

Plaintext: instruments

M	O	N	A	R
C	H	X	B	D
F	F	Q	I	K
L	P	Q	S	T
U	V	W	X	Z



Plan Text : "instruments"

After split : 'in' 'st' 'eu' 'mc' 'nt' 'sz'

Encryption

"in" → g

"st" → a

s → t

t → l

eu → m

mc → z

nt → c

c → o

n → z

t → g

s → t

z → x

Encrypted Text : gatlmczdgtx

Explain data confidentiality, data authentication and data integrity

→ The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system security



## (1) Confidentiality

⇒ Data Confidentiality :- Assume that

Private or confidential information is not made available or disclosed to unauthorized individuals

⇒ Privacy :-

Assume that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

## (2) Integrity

⇒ Data Integrity :-

Assumes that information and programs are changed only in a specified and authorized manner

⇒ System Integrity :-

Assume that a system performs its intended function in an unimpaired



manner, free from deliberate or inadvertent unauthorized manipulation of the system.

### (3) Availability

→ Assume that system's logic, prompt and service is not denied to authorize user

Q-5

Differences between substitution techniques and transposition. Explain transposition techniques

Substitution cipher  
Technique

Transposition cipher  
Technique

→

In this technique, plain text characters are replaced with other characters, numbers and symbols

In this technique, plain text characters are rearranged with respect to the position

→

This form use mono alphabetic substitution cipher and poly alphabetic substitution cipher

This form use key less transposition cipher and keyed transposition cipher



→ In this technique character's identity is changed while its position remains unchanged

In this technique, the position of the character is changed but character's identity is not changed

→ In this technique the letter with low frequency can detect plain text

In this technique the keys which are needed to correct key can disclose plain text

→ The example of this technique is Caesar cipher

The example of this technique is Rail Fence cipher

## ⇒ Transposition Techniques

→ A very different kind of mapping is achieved by performing some sort of permutation on the plain text letters. This technique is referred to as a transposition cipher.

→ The simplest such cipher is the Rail fence technique



## \* Rail Fence Technique

→ Encryption involves writing plaintext letters diagonally over a number of rows, then read off cipher row by row.

→ For example, the text "meet me after the party" can be written as:

m e m a t h n p s y  
e t e f e t e a t

→ ciphertext is read from the above row by row

ME MATHN PRY E T F E T E A T

→ This is very easy to cryptanalyze as no key involved

→ Transposition cipher can be made significantly more secure by performing more than one stage of transposition. The result is a more complex permutation that is not easily reconstructed.