Experiment - 01

Aim - Implementation of ceaser Cipher

Theory -

Q1 Explain CIA Security Model

→ CIA security model also known as CIA Triad is a fundamental frame work in iformation security. It stands for ~~confidentially~~ confidentiality, Integrity and Availablity.

Confidentiality - This ensures that sensitive information is accessed only by authorized individuals. Techniques like encryption, access control, and authentication mechanism are used to maintain confidentiality. For example, using HTTPS for secure web browsing it ensures that the data transmitted between your browser and server remain confident.

Integrity - This ensure that the data remains accurate and unalterade during storage or transmission Integrity is maintained through method like checksum, hashing, digital signatures.

Availablity - This ensures that information and resources are accessible to authorized user when needed. Avablity is maintain through redundancy, failover mechanisms, and regular maintainence. fore example, cloud services often uses multiple data centers to ensure that services remain available even if one data centre fails.

Q2 Explain different categories of attacks

→ There are 2 types of attacks

i. Active Attack-

Active attack are a type of cybersecurity attack in which an attacker attempts to alter, destroy, or disrupt the normal operation of system or network.

Active attacks involve the attacker taking direct action against the target system or network and can be more dangerous.

Types of active attack-

a. Masquerade
b. Modification of message
c. Repudiation
d. Replay
e. Denial of Service

ii. Passive attack-

A passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive attacks are in the nature of eavesdropping on or monitoring transmission. The goal of opponent is to obtain information that is being transmitted.

Types of passive attacks-

a. The release of message content
b. Traffic analysis.

Q3. Explain Substitution ~~Ceaser~~ Cipher Technique with modified Caesar Cipher Method as an Example

→ Substitution Cipher Method-

A substitution cipher method of encryption where each letter in the plaintext is replaced with another letter. The subsititution is based on fixed system, which is as simple as shifting letters by a ~~certain~~ 3 number of position in the alphabets.

Example

Plain Text → HELLO

Shift → 3

Cipher Text → KHOOR

To break/decrypt the cipher text we need to replace the characters of cipher text message by alphabet 3 places back

Modified Caesar Cipher-

To enhance the security of traditional ceaser Cipher In modified caesar cipher ~~the~~ an alphabet in the plain text will not necessarily shif forward by 3 positions. It can be replaced by any other alphabet. Once the replacement scheme is decided it will be constant and will be wed for all other alphabets in that message. There are 25 possiblity for each alphabet

Example

Plain Text → Hello

let Shift be 5

Cipher text

H shift by 5 → M
e shift by 5 → j
l shift by 5 → q
l shift by 5 → q
o shift by 5 → t

∴ Hello → Mjqqt

To decrypt the message we need to replace the characters of cipher text by alphabets backward the number of times we shif the ~~value~~ position (here 5 times backward).

Q4 Explain Transposition Techniques with Simple Columnar Method as an example

→ In ~~this~~ ~~category~~ Transposition technique, no replacement of plain text content is done, only the position of the content of the plain text message is changed.

Simple Columnar Method-

lets consider

Plain Text - Everything is nothing

Now write the plain text message row by row in a rectangle of pure defined size.

lets consider the rectangle of 6 colums.

The plain text will written as

1	2	3	4	5	6
E	v	e	r	y	t
h	i	n	g	i	s
n	o	t	h	i	n
g					

Now to encrypth this read the message column by column in a random order of column

Let's consider the order of column is - 2, 3, 6, 5, 4, 1

Our cipher text will be-

viоentt sn yii rgh ehng

everything is nothing → viоentt sn yii rgh ehng