Network Security

- SCSA1602

Name: Mohnish Devaraj

Reg No: 39110636

Section: C1

Assignment-1

PART-A

1. Active attacks
2. Encipherment
3. Non-repudiation
4. Cryptanalysis
5. Known Plaintext Attack (KPA)

PART-B

6. **Caesar Cipher**

The Caesar Cipher technique is one of the earliest and simplest method of encryption technique. It's simple a type of substitution cipher, i.e., each letter of a given text is replaced by a letter some fixed number of positions down the alphabet.

⑦ Brute force Attack

A brute force attack is a category of attack that leverages computers power to rapidly perform the same action millions of times to "guess" passwords, discover hidden URLs, or expose encrypted or hashed password. While there are easy and common ways to defend oganist this attacks, it's a low effort attack on the part of hackers, making it easy to find a vulnerability within a company's site.

⑨ Integrity

Integrity measures protect information from unauthorized alteration. These measures provide assurance in the accuracy and completeness of Data. The need to protect information includes both data that is stored on systems and data that is transmitted between system such as email.

Confidentiality

Confidentiality measures protect information from unauthorized access and ~~mine~~ misuse. Most information systems house information that has some degree

of sensitivity. It might be proprietary business information that competitors could use to their advantage or personal information regarding an organization's employee's, customers or clients.

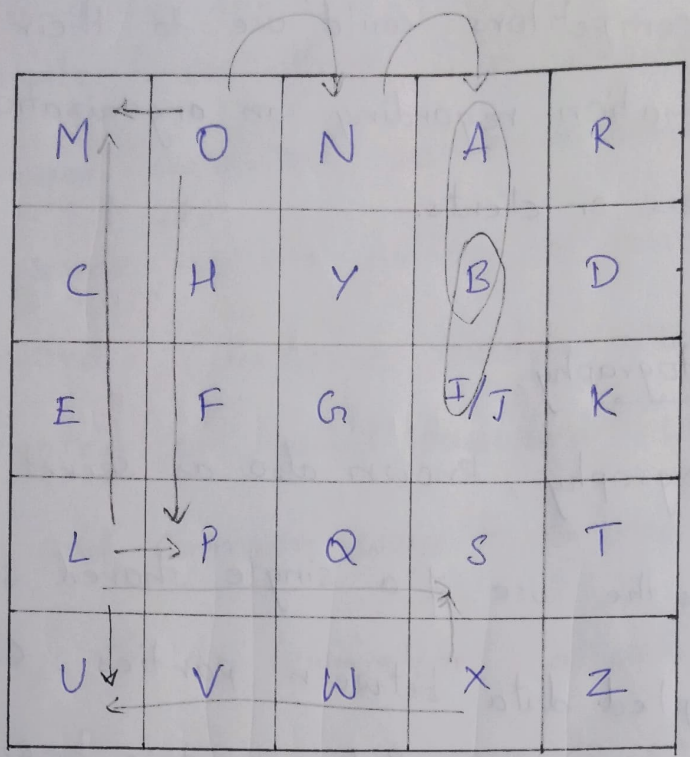
(10) Symmetric Cryptography

Symmetric cryptography, known also as secret key cryptography, is the use of a single shared secret to share encrypted data between parties. Ciphers in this category are also called symmetric because it use the same key to encrypt and to decrypt the data. In simple terms, the sender encrypts data using a password, and the recipient must known that password to access the data.

(8)

Plain text : "ballon"

key word : "Monarchy"



Plain text : Ballon

By making it Pairs

ba lx lo on
↓ ↓ ↓ ↓
IB SU PM NA

IBSUPMNA is the Encrypted ~~message~~ text.

PART - C

(11) Hill Cipher

Hill Cipher is a polygraphic substitution cipher based on linear algebra. Each letter is represented

by a number modulo 26. often the simple scheme A=0, B=1, ..., Z=25 is used, but this is not an essential features of the cipher. To encrypt a message, each block of n letters (considered as an n-component vector) is multiplied by an invertible nxn matrix, against modulus 26. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption. The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible nxn matrices (modulo 26).

Example

Plaintext : ACT

Key word : GYBNQKURP

Encryption

We have the Encrypt the message "ACT" (n=3). The Keyword can be written in the nxn matrix.

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

The message 'ACT' is written as vector:

$$\begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

The enciphered vector is given as:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 9 \end{bmatrix} \Rightarrow \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \Rightarrow \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \pmod{26}$$

which corresponds to ciphertext of 'POH'.

Decryption

To decrypt the message, we turn the ciphertext back into a vector, then simply multiply by the inverse matrix of the key matrix (IFKVIVVMI in letters).

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}^{-1} \Rightarrow \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \pmod{26}$$

For the previous Ciphertext 'POH':

$$\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \Rightarrow \begin{bmatrix} 260 \\ 574 \\ 539 \end{bmatrix} \Rightarrow \begin{bmatrix} 0 \\ 2 \\ 9 \end{bmatrix} \pmod{26}$$

which gives us back "ACT".

Assume that all the alphabets are in upper case