Jessica Braganza
BE comp 2
F17112151

PAGE NO :
DATE :

ICS Assignment 1.

1) Draw and explain operational model of network security.

Ans. 1) Consider a message or data is to be transferred from sender to receiver or from one party to another across internet.

2) During this data transmission process it is necessary to protect security aspects of this information from an opponent or attacker.

3) The technique used to provide security is as follows:

- The original message is encrypted with the help of a key, which scrambles the message so that it is not readable to any third party.
- An additional code can be attached to the encrypted data which is based on the contents of the message, which can be used to verify the identity of the sender.
- The message is now transmitting through an insecure channel such as internet. The message when received at the receiver side is unscrambled either using same or different key to obtain the original message.
- A trusted third party (such as Virtual Private Network) is required for secure transmission.
- The trusted third party is responsible to distribute the private key and secret information to the sender and receiver while keeping it away from any opponent or attacker.

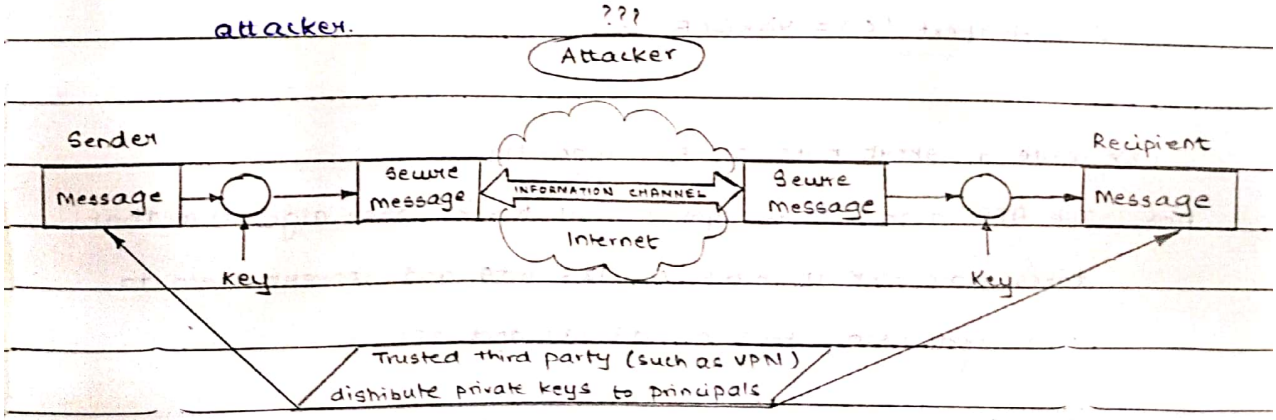

Fig: Model for network security

PAGE NO :
DATE :

2) Find out the ciphertext for plaintext "MESCOE" using Hill cipher with key as $K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$

Solution:

Key (K) = $\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$

Plaintext (Pi) = "MESCOE"

$C_i = KP_i \bmod 26$

Here, we have to encrypt the message 'MESCOE'. This message is written as vector:

$$\text{MESCOE} \rightarrow \begin{bmatrix} M \\ E \\ S \end{bmatrix}, \begin{bmatrix} C \\ O \\ E \end{bmatrix} \rightarrow \begin{bmatrix} 12 \\ 4 \\ 18 \end{bmatrix}, \begin{bmatrix} 2 \\ 14 \\ 4 \end{bmatrix}$$

Then we compute C_i:

$$\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 12 \\ 4 \\ 18 \end{bmatrix} \bmod 26 = \begin{bmatrix} 362 \\ 702 \\ 374 \end{bmatrix} \bmod 26 = \begin{bmatrix} 24 \\ 0 \\ 10 \end{bmatrix} = \begin{bmatrix} Y \\ A \\ K \end{bmatrix}$$

$$\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 2 \\ 14 \\ 4 \end{bmatrix} \bmod 26 = \begin{bmatrix} 292 \\ 378 \\ 108 \end{bmatrix} \bmod 26 = \begin{bmatrix} 6 \\ 14 \\ 4 \end{bmatrix} = \begin{bmatrix} G \\ O \\ E \end{bmatrix}$$

∴ Ciphertext (Ci) = YAKGOE

3) Write a short note on AES algorithm.

Ans. The AES algorithm is symmetrical block cipher algorithm that takes plain text in block of 128 bits and convert them to ciphertext using keys of 128, 192 and 256 bits.

PAGE NO :
DATE :

Since AES algorithm is considered secure, it is in world wide standard.

Working of AES :

- The AES algorithm uses a substitution-permutation or SP network with multiple rounds to produce ciphertext.
- The number of round depends upon the key size being used.
- A 128 bit key size dictates 10 round, a 192 bit key size dictates 12 rounds and 258 bit key size has 14 rounds.
- Each of these rounds requires a round key, but since only one key is given as an input to the algorithm, this key needs to be expanded to get the keys for each round, including round 0.

AES algorithm has 5 modes of operation :

i) Electronic Code Book (ECB) mode.

ii) Cipher Block Chaining (CBC) mode.

iii) Cipher Feedback (CFB) mode

iv) Output Feedback (OFB) mode

v) Counter (CTR) mode.