CMR

Internal Assessment-1.

1) Short notes on:-

a) Active attacks:

→ Active attacks are attacks on information transmission or any other authenticated transmission where the opponent alters the contents of the information and can become a threat to the system resources. It affects the system resources by means of modification, inserting, deletion, editing, replaying, preventing acces to network etc.

There are 4 types of active attacks:-

a) Masquerade:

→ Here the attacher or opponent tries to be an entity in the communition by an authorized perspective. The receiver thinks the information is coming from an authorized sender but, actually, the attacher will be sending.

b)

b) Replaying: / Replay attacks.

→ In replaying, the attacher gains information from the sender. The sender sends the data to receiver but the attacher modifies it and replays or resends modified information to the receiver.

c) Modification of messages.

→ modification or changes done to the actual information.

d) Denial of service.

→ The service for actual transmission is denie or the network is blocked.

1b) Passive attacks.

→ Passive attacks are attacks where the informa or data is monitored, the transmission of data is monitored between senders & receiv There is no attack or modification of system resources. Just the information is achieved from a third party.

→ There are 2 types of passive attacks.

i) Revealing the menage

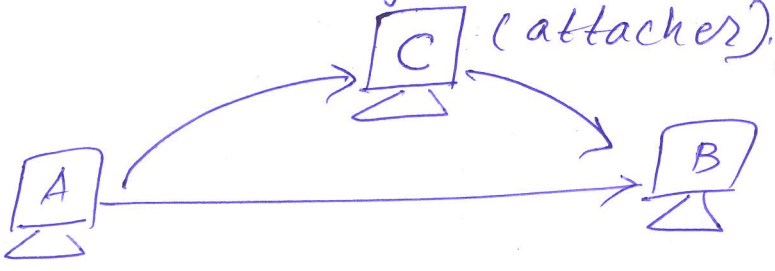
ii) Traffic analysis.

In first types, the information is known by the attacker. If there is any authenticated data being sent between the hosts, the third party achieves the information by hacking

In second type, the attacker monitors the length and frequency of the menage and ge to know the hosts.

1)c) Replay attacks.

→ Replay attack is a type of active attack.



→ The information is sent from the source host A to destination host B. But the attacker still captures the information from A, modifies it and resends/replays the information again to B as an entity (authorized)

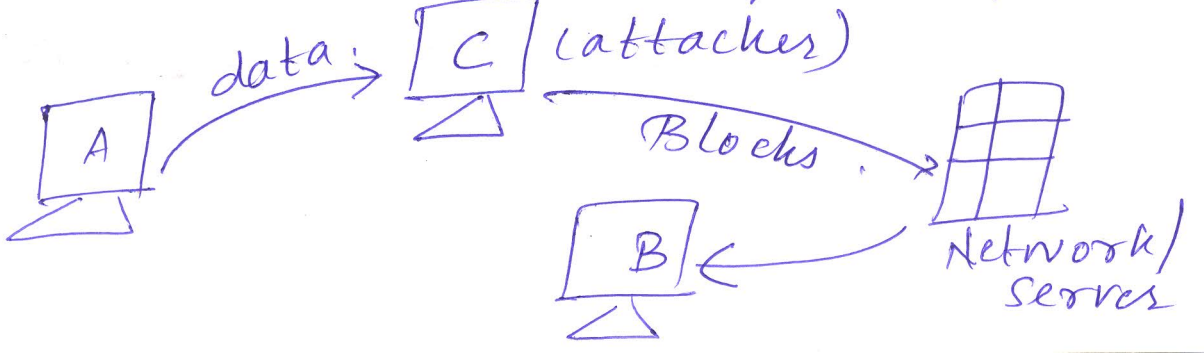
→ Misunderstanding arises between the 2 hosts as the host B might take in wrong information not sent by an authorized host A.

1)d) Denial of service.

→ Denial of service is an active attack.

→ Here the service or the transmission of data from host A is not sent to host B.

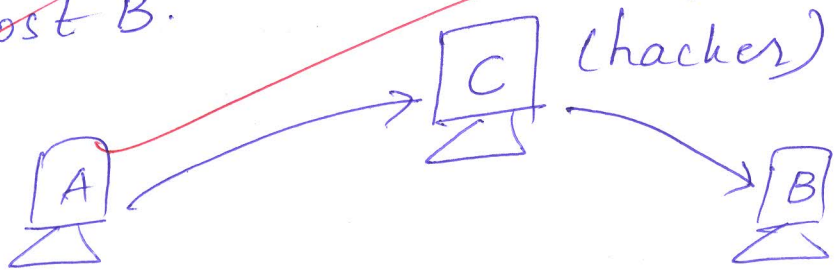
→ Either the network is blocked or hacked or the network is flooded by messages to block the actual transmission of data.



1)e) Modification of messages.

→ Modification of message is an active attack where the attacker/hacker modifies by the real/authenticated data by editing, insertion replaying etc techniques.

→ Due to modification, wrong message is sent to host B.



IAT-1

NETWORK SECURITY – SOLUTION TO PROBLEMS

2) C: BUAYPWBQUAJG | Hill cipher technique

Soln

$$K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \qquad P = D_K(C) = K^{-1}C \bmod 26$$

→ Find K^{-1} $\quad K^{-1} = \frac{adj\ k}{|k|}$ $\quad adj\ k = Trn$ (co-factor matrix)

Cofactors $\quad K_{11} = 300 \quad K_{21} = -313 \quad K_{31} = 267$

$K_{12} = -357 \quad K_{22} = 313 \quad K_{32} = -252$

$K_{13} = 6 \quad K_{23} = 0 \quad K_{33} = -51$

$$CF\ matrix = \begin{bmatrix} 300 & -357 & 6 \\ -315 & 313 & 0 \\ 267 & -252 & -51 \end{bmatrix} \qquad adj\ k = \begin{bmatrix} 300 & -313 & 267 \\ -357 & 313 & -252 \\ 6 & 0 & -51 \end{bmatrix}$$

$|k| = -939 \qquad -939 \bmod 26 = 23$

$$K^{-1} = \begin{bmatrix} 300/23 & -313/23 & 267/23 \\ -357/23 & 313/23 & -252/23 \\ 6/23 & 0 & -51/23 \end{bmatrix}$$

multiplicative inverse of 23 in $Z_{26} = -9$

$$K^{-1} = \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix}$$

$P = K^{-1}C \bmod 26$

$$P = \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix} \quad \begin{matrix} [BUA & YPW & BQU & AJG] \end{matrix} \quad \begin{bmatrix} 1 & 24 & 1 & 0 \\ 20 & 15 & 16 & 19 \\ 0 & 22 & 20 & 6 \end{bmatrix} \bmod 26$$

$$P = \begin{bmatrix} 2 & 15 & 6 & 15 \\ 17 & 19 & 17 & 7 \\ 24 & 14 & 0 & 24 \end{bmatrix} = \begin{bmatrix} C & P & g & P \\ r & t & r & h \\ y & o & a & y \end{bmatrix}$$

P = Cryptography

3) Playfair technique

PT: we are the students of network security

CT: UH LB MN KG TN ZI/J NU NT TL UN QZ VG SX KI VI DN CY

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

5) a) god is nowhere → Plaintext

6 14 3 8 18 13 14 22 7 4 17 4

$C = (P+k) \bmod 26$

$K = 3$

$g \rightarrow (6+3) \bmod 26 = 9 = J$

$o \rightarrow (14+3) \bmod 26 = 17 = R$

$d \rightarrow G$

$i \rightarrow L$

$s \rightarrow V$

$n \rightarrow Q$

$o \rightarrow R$

$w \rightarrow Z$

$h \rightarrow K$

$e \rightarrow H$

$r \rightarrow U$

$e \rightarrow H$

CT:

JRGLVQRZKHUH

b)

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

E I F U S L P O → C.T

th an ky ou → P.T

PT: thankyou

6) PT = 01000001 (1 2 3 4 5 6 7 8)

K = 1010000010 (1 2 3 4 5 6 7 8 9 10)

Key generation

$K_1 = 10100100$

$K_2 = 01000011$

Encryption

P.T = 01000001 (1 2 3 4 5 6 7 8)

i) IP = 1000 0100 (L | R)

ii) $f_{k_1}(L, R) = [L \oplus F(R, K_1), R]$ ——— (1)

$L = 1000$ $R = 0100$ ($n_1 n_2 n_3 n_4$) $k_1 = 10100100$ (1 2 3 4 5 6 7 8)

$$\begin{array}{|c|c|c|} \hline n_4 \oplus k_{11} & n_1 \oplus k_{12} \quad n_2 \oplus k_{13} & n_3 \oplus k_{14} \\ \hline n_2 \oplus k_{15} & n_3 \oplus k_{16} \quad n_4 \oplus k_{17} & n_1 \oplus k_{17} \\ \hline \end{array} \Rightarrow \begin{array}{|c|c|c|} \hline 0 \oplus 1 & 0 \oplus 0 \quad 1 \oplus 1 & 0 \oplus 0 \\ \hline 1 \oplus 0 & 0 \oplus 1 \quad 0 \oplus 0 & 0 \oplus 0 \\ \hline \end{array}$$

$$\begin{array}{|c|c|c|} \hline 1 & 0 \quad 0 & 0 \rightarrow S_0 \\ \hline 1 & 1 \quad 0 & 0 \rightarrow S_1 \\ \hline \end{array}$$

$S_0 \rightarrow 00$

$S_1 \rightarrow 01$

$P_4 : 0100$

$P_4 : 0100 \Rightarrow F(R, K_1) = 0100$

(1) $\Rightarrow f_{K_1} = [1000 \oplus 0100, 0100]$

$$\boxed{f_{K_1} = [1100, 0100]}$$

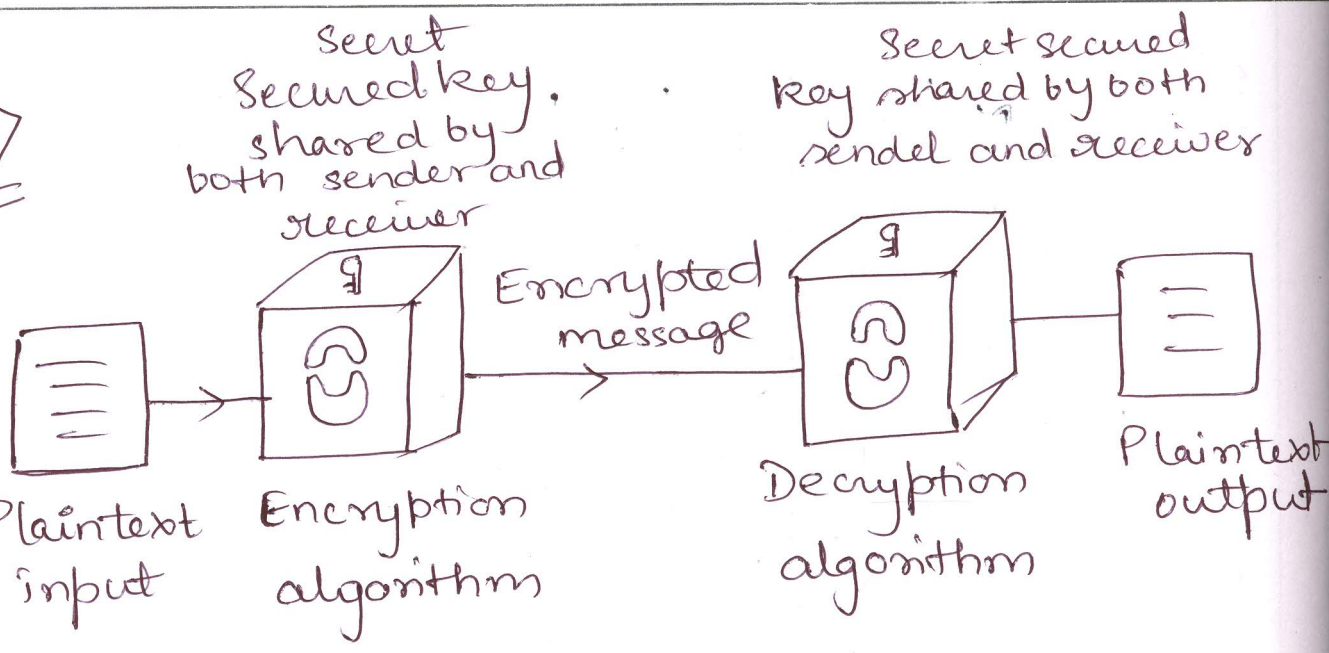
SWAP: $L_2 = 0100$ $R_2 = 1100$

$f_{K_2}(L_2, R_2) = [L_2 \oplus F(R_2, K_2), R_2]$

$$\boxed{f_{K_2} = [0100, 1100]} \quad (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8)$$

$$\boxed{IP^{-1} = 00010101 = BF}$$

7)



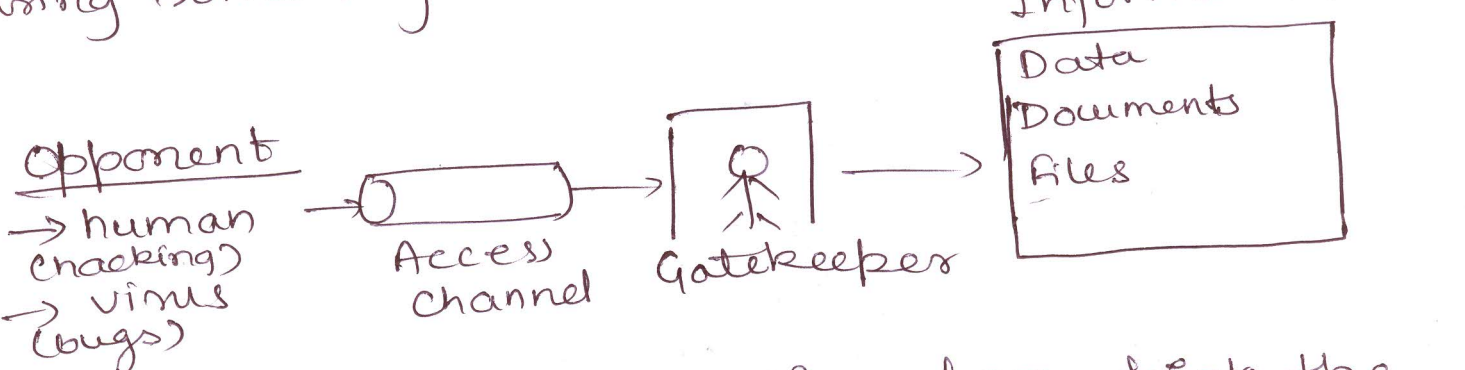
→ Plain-text is the message which has to be send after encryption or scrambling so that the message cannot get identified by others. Initial message send that needs encryption is plain text.

→ Encryption algorithm - The algorithm of twisting or scrambling the message so that it is safe from unwanted hackers it is done to maintain the authenticity of the message.

→ Secret key - This principal is made available to both sender and receiver through a third party so that the secracy of the message is maintained. With the help of secret key and encryption algorith it becomes easy for hackers to ~~get~~ decode the message.

→ Decryption - It is generally the inverse algorithm of encryption to get back the encrypted message with the help of key.

Cipher text - Encrypted message to prevent the confidentiality and authenticity of the message, It is the scrambled form of ~~encry~~ initial message using some algorithm



Opponent can be human or virus from which the data has to be protected.

Opponent needs access channel to reach to the data and attack it.