CAE-1

Name: Mohnish Devaraj

Subject Name: Network security

Reg NO: 39110636

Subject Code: SCSA1602

Roll NO: 19S115398

Total pages: 8

Date: 31 Jan 2022

PART - B

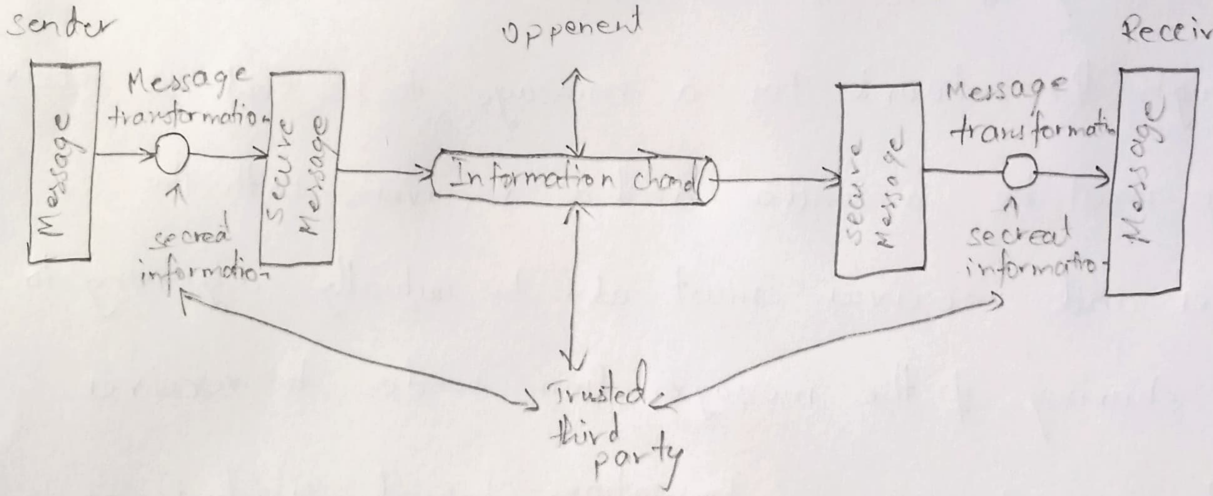
(6) A Network security model Exhibits how the security service has been designed over the network to prevent the oppenent from causing a threat to the confidentiality or authenticity of the ~~of~~ information that is being transmitted through the network. For a message to be sent or receive there must be a sender and a receiver. Both the sender and receiver must also be mutually agreeing to the sharing of the messages from sender to receiver needs a medium i.e., information channel which is an internet service

Any security service would have three components.

1. Transformation of the information which has to be sent to the receiver. So, that any opponent present at the information chanael is unable to read the message. This indicate the encryption of the message.

2. Sharing of the secreat information between sender and receiver of which the opponent must not any clue.

3. There must be a trusted third party which should take the responsibility of distributing the secreat information to both the communication parties and also prevent it from any opponent.



The network security model present two communicating parties sender and receiver who mutually aggrees to exchange the information. The sender has information to share with their receiver. But sender cannot send the message on the information cannel in the readable form as it will have a threat of being attacked by the opponent. so, before sending the message through the information channel, it should be transformed into an unreadable format. secret information is used while transforming the message which will also be required when the message will be retransformed at the recipient side. that's why a trusted third party is required which would take the responsibility of disturbing the secret information to both the parties involved in communication. ~~So, consid~~

To transform a readable message at the sender side into an unreadable format, an appropriate algorithm should be designed such that it should be difficult for an oppenent to crack that security algorithm. Next, the network security model designer is concerned about the generation of secret information which is known as key. this secret information is used in conjunction with the security algorithm in order to transform the message.

9 Random numbers are fondamental building blocks of cryptographic system s and as such , play a key role in each of these elements.

Randomness involves information or the lack of it. The random module provides function for generating random number..

Types of RNG

RRNG - Pseudo random number generator

TRNG - True random number generator

PRF - Pseudo random function.

Blum Blum shub Generator

A popular approach to generating secure pseudo random number is known as the Blum Blum shub (BBS) generator. It has perhaps the strongest public proof of it's cryptographic strength. Blum Blum shub is used as a pseudo random number generator. It is pseudo as it is not a truly random number, and where its randomisation depends on a random seed. It was created by Lenore Blum, Maneul Blum and Michael shub in 1968.

choose two large prime numbers p and q that have a remainder of 3 when divided by 4.

$$p \equiv q \equiv 3 \pmod 4$$

Let $n = pq$

choose a random number s that is relatively prime to n

```
$X_0 = s^2 \bmod n$
for $i = 1$ to $\infty$
    $x_i = (X_{i-1})^2 \bmod n$
    $B_i = X_i \bmod 2$
```

$x_{n+1} = x_n^2 \bmod n$

given $x_0 = 5$, $p = 7$, $q = 11$

$m = p * q$

$= 7 * 11 = 77$

$x_0 = 5^2 \bmod 77$ $= 25$

$x_1 = 25^2 \bmod 77$, $x_1 = 9$

$x_2 = 9^2 \bmod 77$, $x_2 = 4$

$$x_{n+1} = x_n^2 \text{ Mod } n$$

where m, is the product of two larg dictinct primes, the output is least significant bit of x_{n+1} or the parity of x_{n+1}.

PART-A

① Passive Attacks

Passive Attacks are the type of attacks in which, the attacker obseres the content of messages or copy the content of messages. Passive attack is danger for confidentility. Due to passive attack, there is no any harm to the system. The most important thing is that in passive attack, Victim does not get informed about the attack.

Active Attacks

Active Attacks are the type of attacks ~~ina~~ which, the attacker efforts to change or mordify the content of message. Active attackers is danger for integrity as well as availability. Due to the ~~activeh~~ attack system is always damaged and system resources can be changed.

② Plain text : "instruments"

~~Encrypted text~~ : ~~ga~~

Key word : "monarchy

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

in st ru me nt sz
ga tl mz cl rq tx

Encrypted text : GATLMZCLRQTX

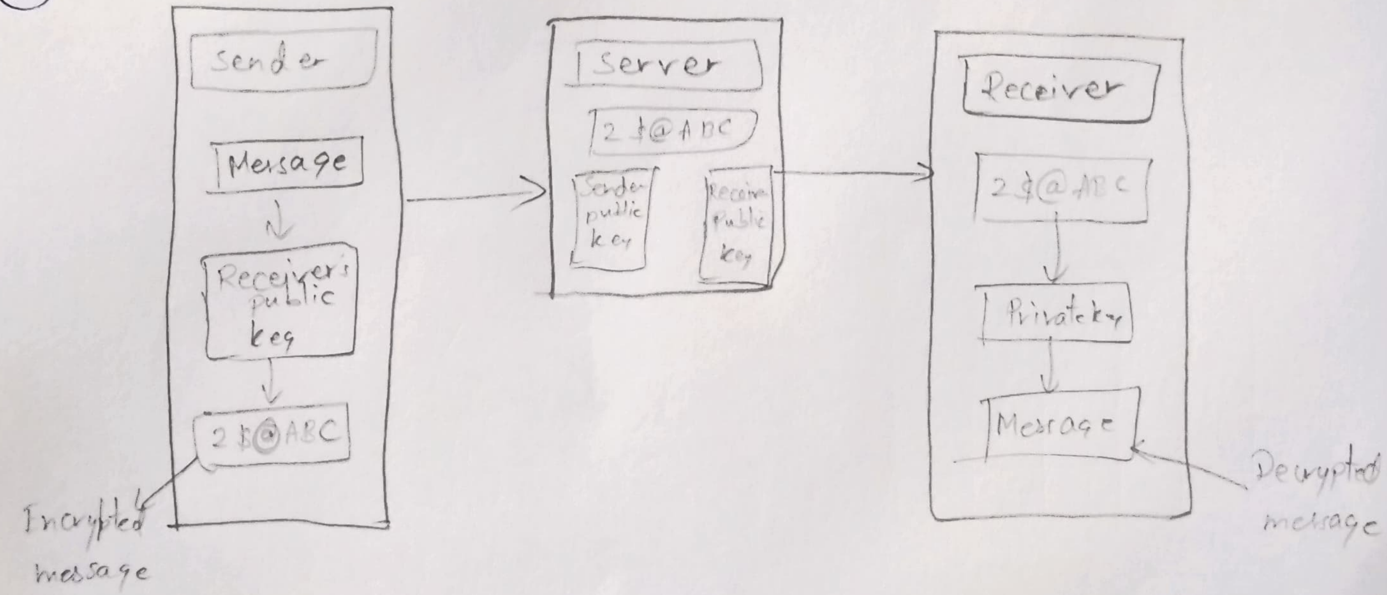
③ steganograph is the practice of hiding a secret message inside of something that is not secret. that something can be just about anything which is required. these days, many example of stegonargraphy involve embedding a secret pieee of text inside of a picture.

④ The strength of DES lies on two facts:

a) The use of 56-bit keys: 56-bit key is used in encyption there are 256 possible keys. A brute force attack on such number of keys is impractical.

b) the nature of alogorithm: Cryptoanalyst can perform crypto analysis by exploiting the characteristics of DES alogrithm but no one has succeeded in findingo out the weakness.

⑤



End to End Encryption refers to the process in which Encryption of data are being done at the end host. It is an implementation of Asymmetric encryption and hence ensures a secure way of data communication