Study Material

On

Cryptography and Network Security

Department of Computer Science & Engineering

CAPITAL ENGINEERING COLLEGE

Mahatapalla, Khordha, Bhubaneswar, Odisha: 752060

(Affiliated to Biju Patnaik University of Technology, Odisha and SCTE & VT, Odisha, Approved by AICTE, New Delhi and Recognised by Govt. of Odisha)

1.1 The Need for Security

- The growing computer implies a need for automated tools for protecting files & other information.
- The use of network & communication facilities for carrying data between users & computers is also growing so network security measures are needed to protect data during transmission.
- To avoid data threat.
- To Avoid Denial of Service (DOS).
- To secure our data from hackers. To safeguard our data from traffic Analyzer.

1.2 Security Approach

Trusted System

- It is a computer system that can be trusted to a specified extend to enforce a specific policy.
- Trusted system where initially of primary interest to the military.
- However, these days the concept has spanned across various areas more permanently in the banking and financial community but the concept never caught on.
- Trusted system often use the term "Reference-Monitor" This is any entity i.e. logical heart of the computer system.

Dt-12.01.19

Security Models

- Security models an organisation can take several approaches to implement its security model & these approaches are

I) No Security

In this simplest case the approach could be a decision to implement no security at all.

II) Security through Obscurity

In this model a system is secured simply because nobody knows about its existance and contents. This approach cannot work for too long, as there are many ways an attacker can come to know about it.

III) Host-Security

In this scheme, the security for each host is enforced individually.

IV) Network Security

In this scheme, the focus is to control network access to various hosts and their services, rather than individual host security.

Security Management Pratices

- Good security management pratices always talk of security policy being in place.
- putting a security policy in place is actually quite & tough.
- A good security policy generally takes care of four key aspects.

(I) **Affordability**

Cost & Effort in security implementation.

(II) **Functionability**

Mechanism of providing security.

(III) **Cultural Issues**

Weather the policy gets well with peoples expectations, working style and believes.

(IV) **Legality**

Weather the policy meets the legal requirement.

1.3 Principles Of Security

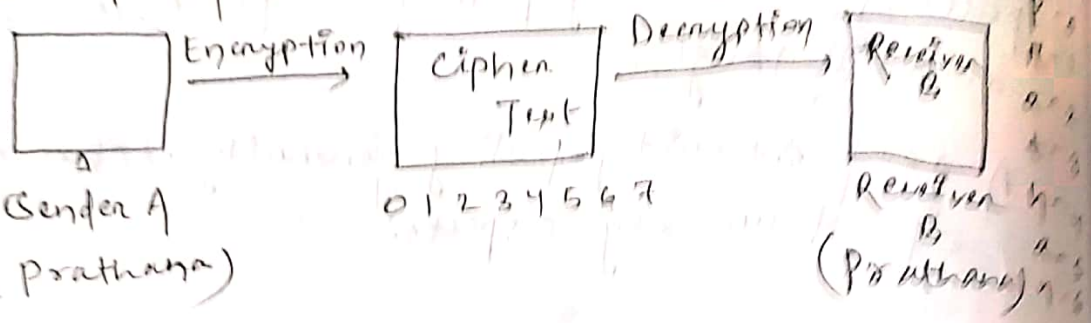
(1) **Confidentiality**

Only sender, intended receiver should understand message contents.

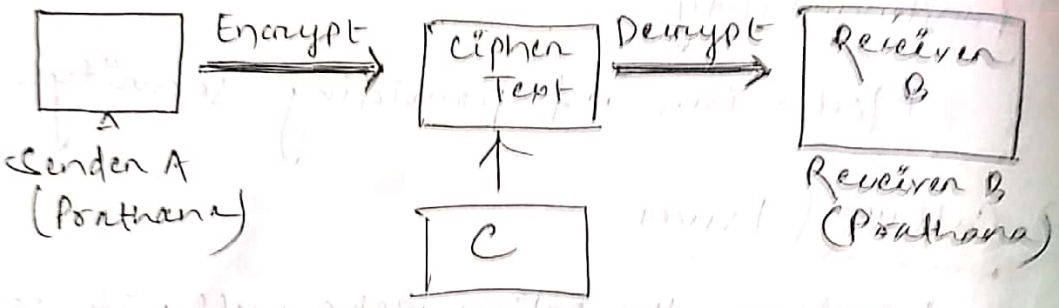
(a) Sender Encrypts the message

(b) Receiver Decrypts the message

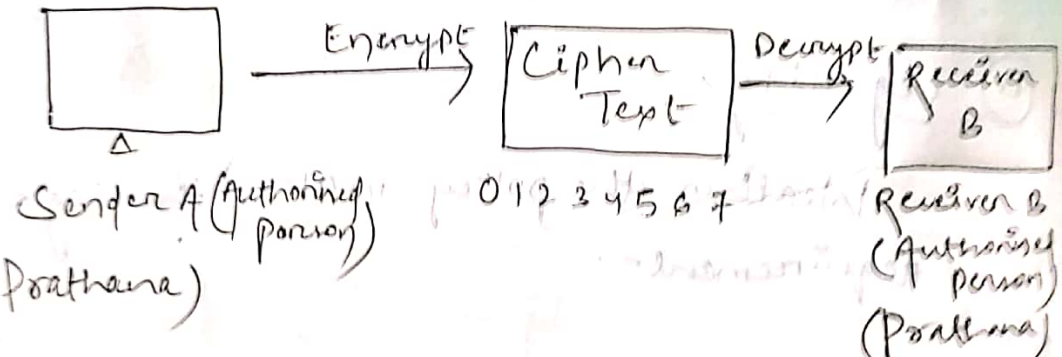
- 3rd Person cannot access to the hide message



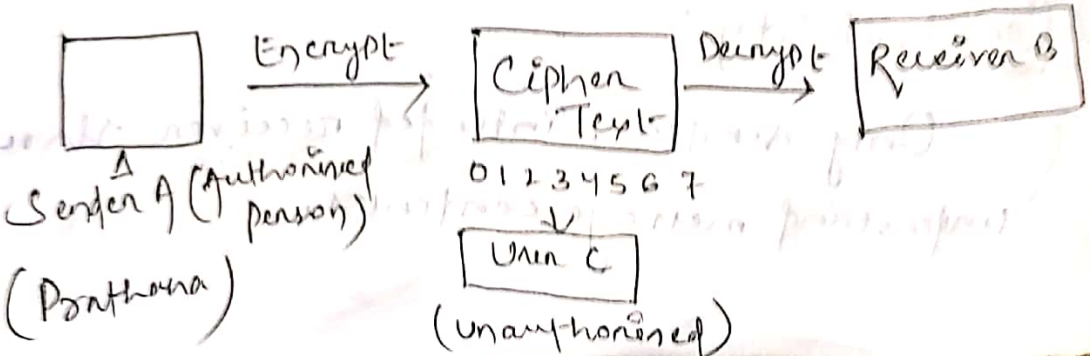
Loss Of Confidentiality



(II) Authentication

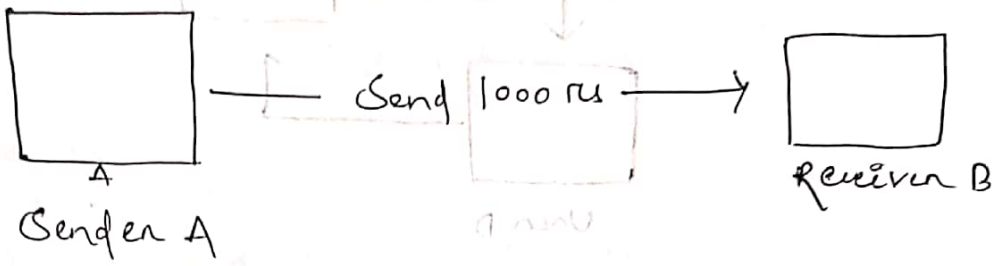


Loss Of Authentication



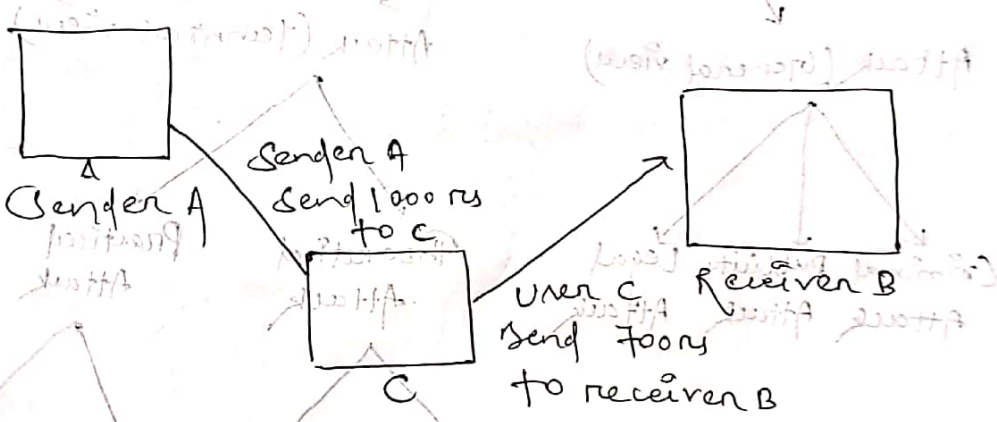
- Sender, Receiver want to confirm identity.
- Both sender and Receiver should be authorised to communicate the system.

(III) Message Integrity

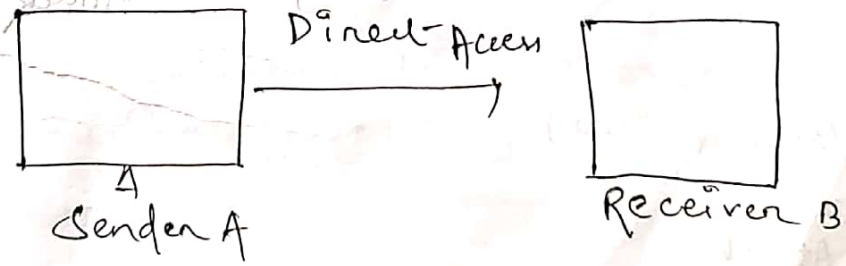


- Sender and Receiver want to ensure message content not altered without detection.

Loss of Message Integrity

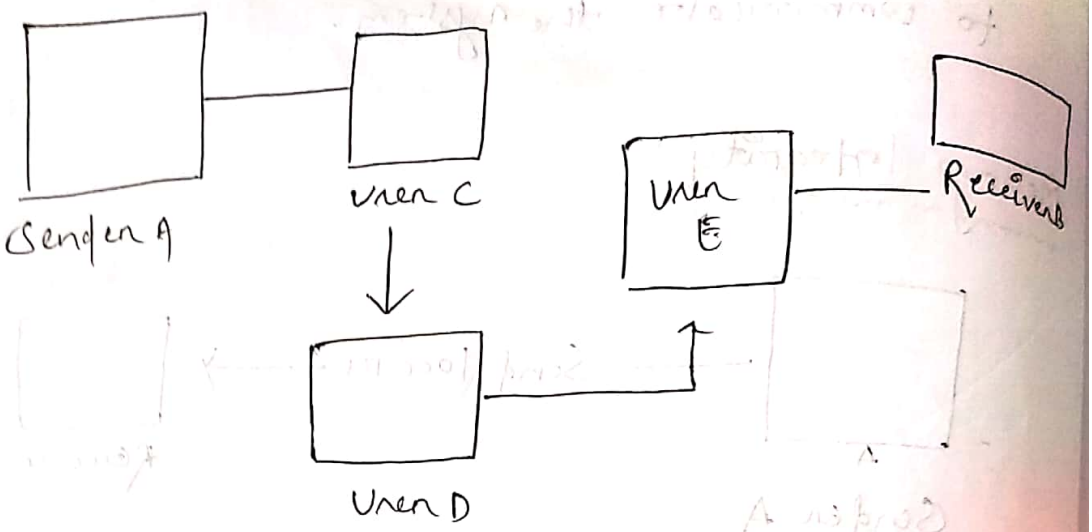


(IV) Access & Availability



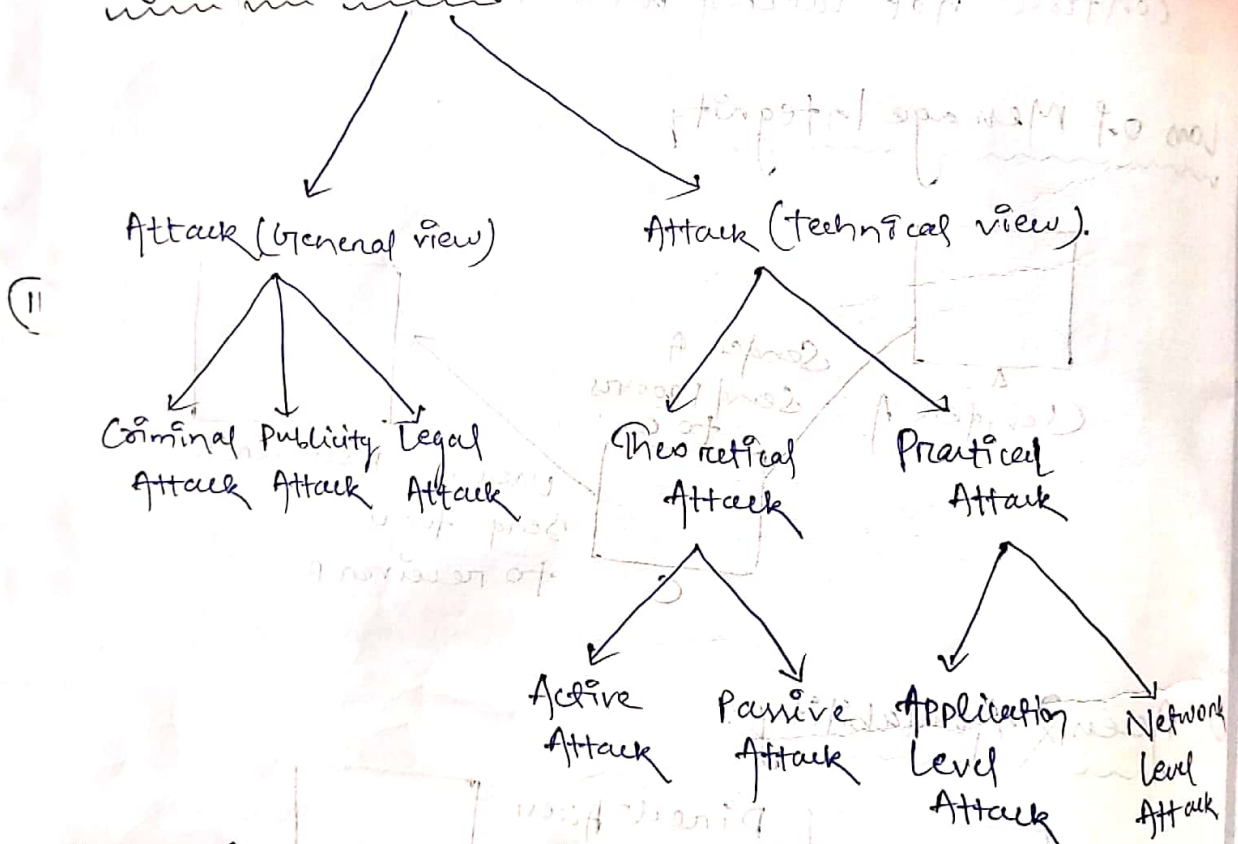
- Services must be accessable and available to the user.

Loss of Access and Availability



1.4 Types of Attack

DT-15.01.19



Attack (General view)

- Criminal Attack

- Criminal Attacks are the simplest to understand their, the sole aim of the attackers is to

maximize financial gain by attacking computer system.

- These attacks are i) fraud
  ii) Scam
  iii) Destruction
  iv) Identity theft
  v) Intellectual identity theft
  vi) Brand theft

- Publicity Attack
  - It occurs because the attackers wants to see their names appear on television, News channel and News paper.
  - History suggest that these type of attackers are usually not hardcore criminal there people such as students in the Universities or employees in large organization who seek publicity by adopting a novel approach of attacking computer system.

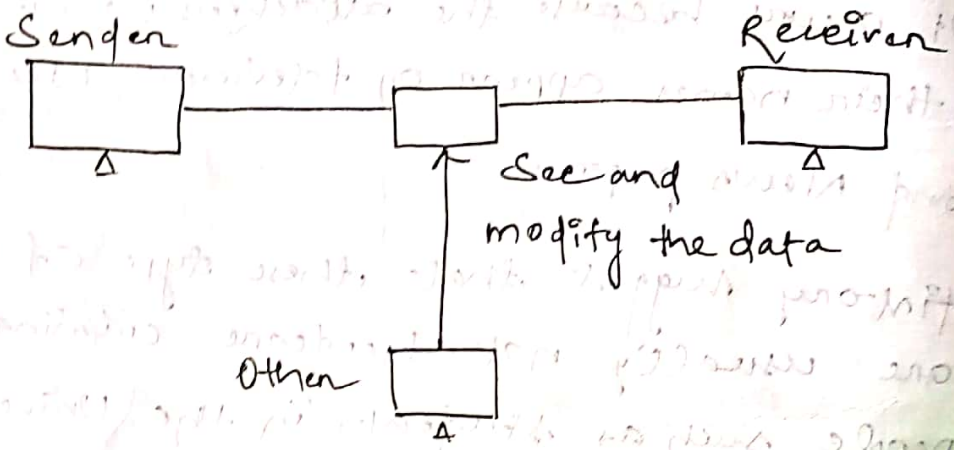
- Legal Attack
  - This form of attack is quite novel and unique.
  - Here the attackers tries to make the Judge or the Jury doubtful about the security of the computer system.
  - These attackers attack the computer system and attack the party they manages to take the attacker to the court while the case is being fought.

Attack (Technical View)

Theoretical Attack

1) Active Attack

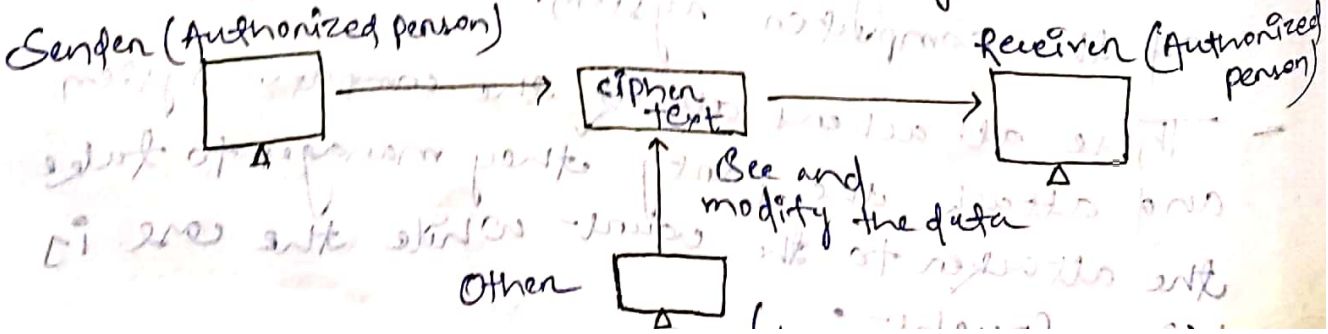
- In Active attack the main aim of attacker is just to obtain information.
- The Attacker modify the data or harm the syste
-



- Active Attack are 3 types :-
  - (I) Interruption
  - (II) Modification
  - (III) Fabrication

(I) Interruption

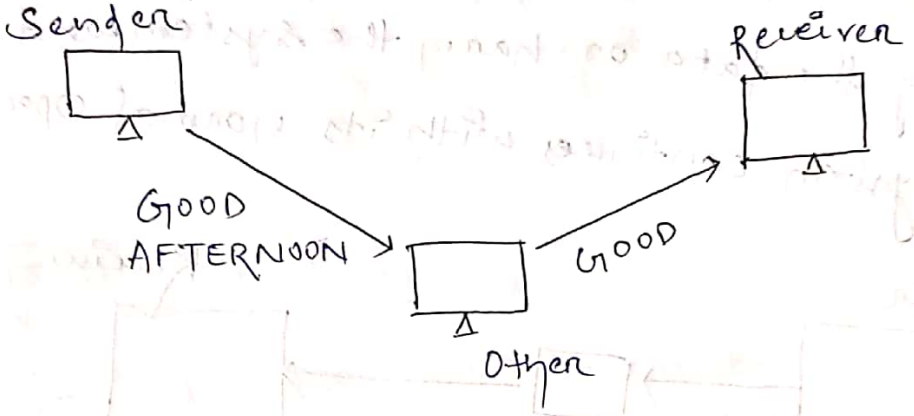
- It means that an unauthorize party has gain access to resource the party can be person or program on computer based system.



DT-16-01-19

(II) Modification

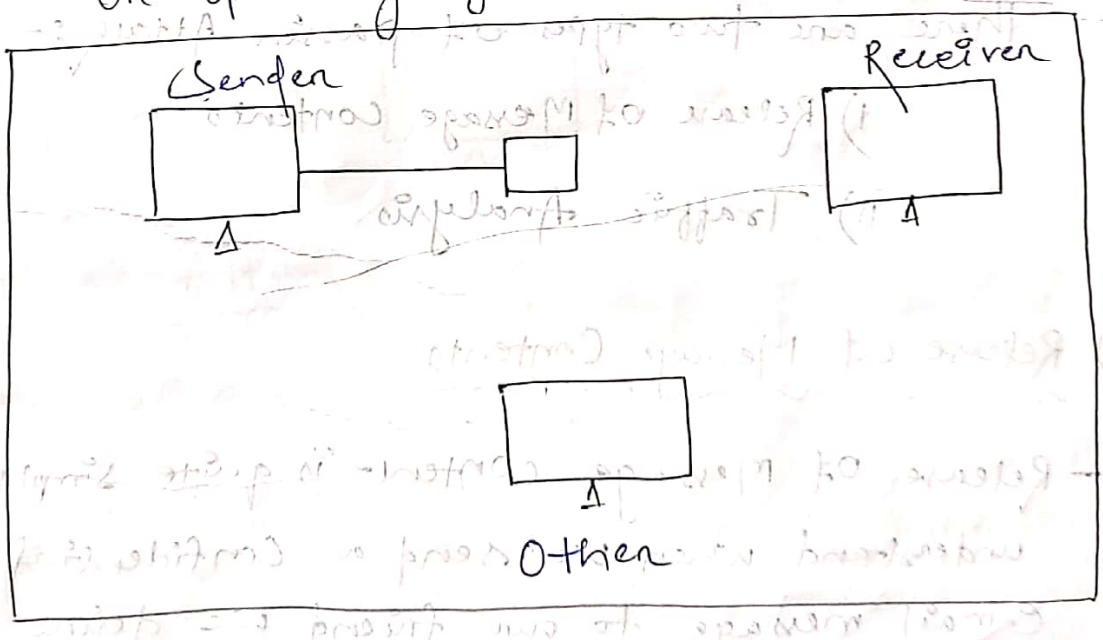
- Sender, Receiver want to ensure message content change without detection.



(II) Fabrication

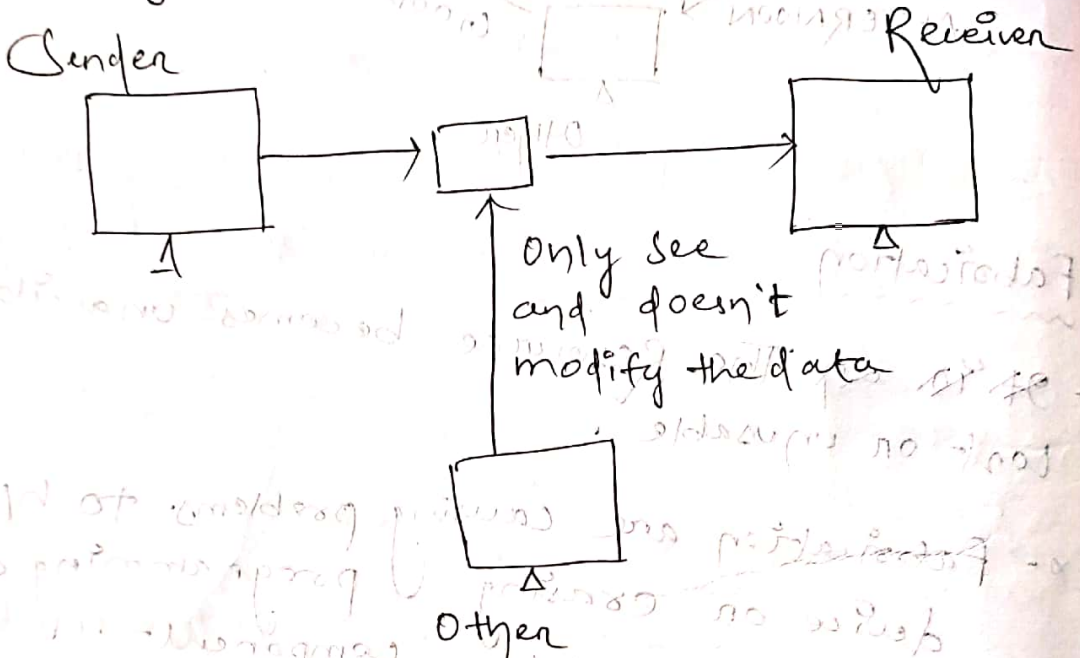
- The Resource becomes unavailable, Lost or unusable.

Ex- Fabrication are causing problems to h/w device or erasing programming data or operating system component-.



11) Passive Attack

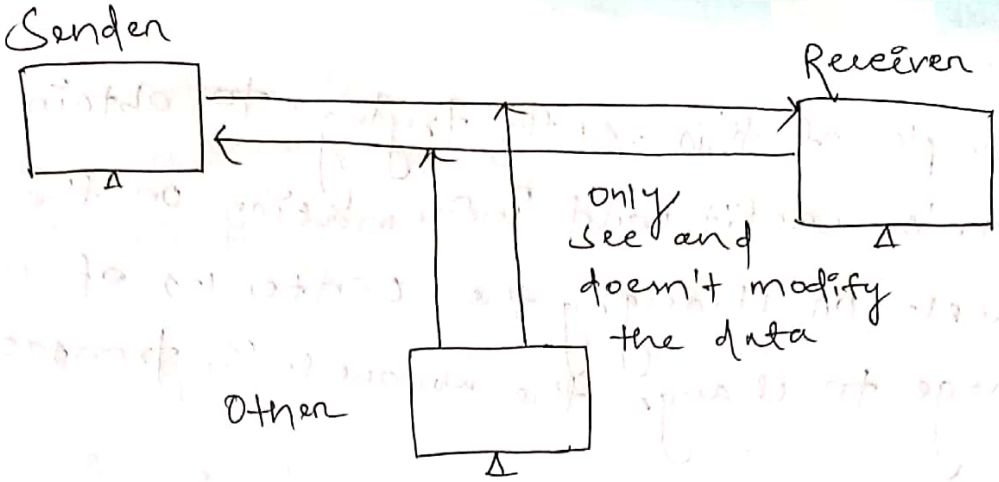
- In Passive Attack the attackers goal is just to obtain Information. This Attack doesn't modify the data or harm the system and the system continues with its normal operation.



- There are two types of passive Attack :-
  1) Release of Message contents
  11) Traffic Analysis

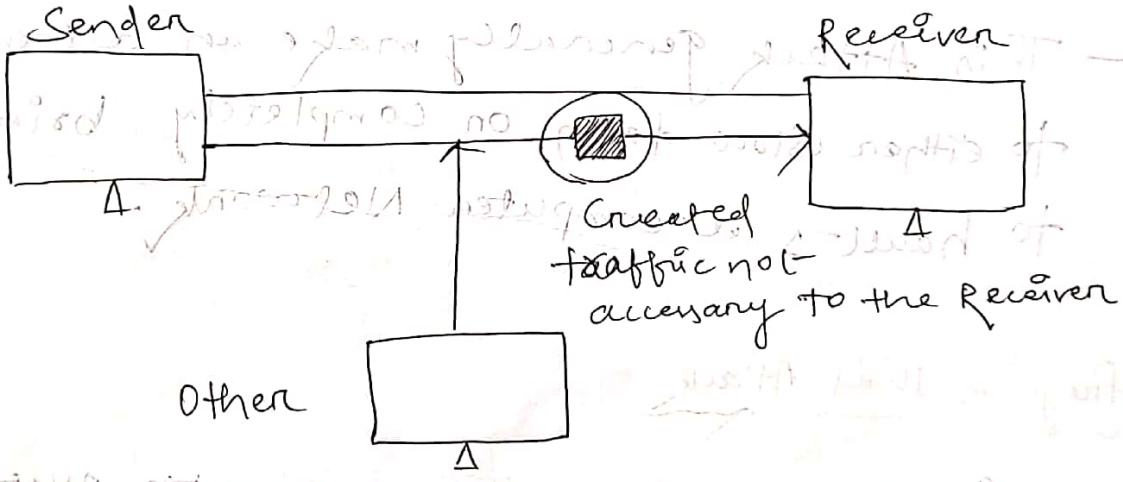
1) Release of Message Contents

- Release of message content is quite simple to understand when we send a confidential e-mail message to our friend we desire that only third person able to access it.



11) Traffic Analysis

- It is the process of intersecting and examining message in order to deduce information from patterns in communication.



Practical Attack

1) Application Level Attack

- These Attacks happen at an application level in the sense that the attacker attempts to access, modify or prevent access to information of a particular application or to the application itself.

Example -

Example of this earth trying to obtain someone's credit card information on the internet or changing the contents of a message to change the amount in transaction.

II) Network level Attack

- These Attacks generally aim at reducing the capabilities of network by a number of possible means.

- This Attack generally make an attempt to either slow down or completely bring to halt a computer Network.

Program that Attack

- A few programs that attack computer system to cause some damage or to create some confusion.

- program that attack under —

(i) Virus

- A virus is a computer programs that attaches itself to another legimate program and cause damage to the computer system or to the network.

(ii) Worm

- A Worm doesn't perform any destructive actions and instead, only consume system resources to bring it down.

(iii) Trojan Horse

- A Trojan Horse allows an attacker to obtain some confidential information about a computer or a network.

2. Cryptography Concepts

2.1 Plain Text & Cipher Text

* **Plain Text** (Readable Text)

- Any communication in the language that we speak i.e. the human language takes the form of plain Text or Clear Text.
- A Clear Text or plain Text signifies a message that can be understood by sender and the receiver and also by anyone else who gets an access to the message.

* **Cipher Text** (Non-Readable Text)

- When a plain Text message is codified using any suitable scheme, the resulting message is called Cipher Text.

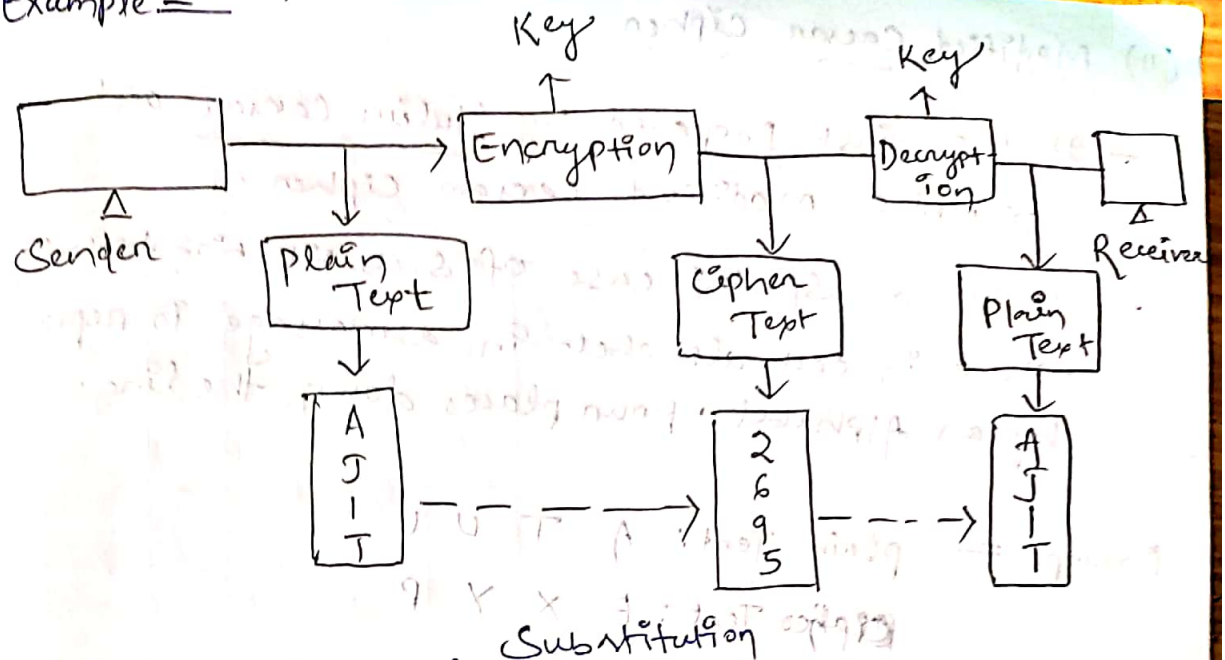
Transformation of plain Text to Cipher Text using two techniques:-

i- Substitution Technique
ii- Transposition Technique.

2.2 Substitution Technique

- In the Substitution techniques the characters of plain text are replaced by other characters or number or symbols.

Example —



- Different types of Substitution techniques are —

(1) Caesar Cipher
(2) Modified Caesar Cipher
(3) Mono-alphabetic cipher
(4) Poly-alphabetic cipher
(5) playfair cipher

(1) Caesar Cipher

- It was first proposed by Julius caesar and termed as Caesar Cipher.
- It is a special case of substitution techniques where in each alphabet in a message is replaced by an alphabet, three places down the line.

Example —

(i) plain Text : A T U L
Cipher Text : D W X O

(ii) plain Text : CRICKET
Cipher Text : FULFNHW

(II) Modified Caesar Cipher

- It was first proposed by Julius Caesar and termed as modified caesar cipher.
- It is a special case of substitution technique where in each alphabet in a message is replaced by an alphabet, four places down the line.

Example = plain Text: A T U L

Cipher Text: E X Y P

(III) Mono-Alphabetic Cipher

- It uses fixed substitution over the entire message. It is also "one to one" substitution cipher method.

Example =

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

Plain Text: C R I C K E T
↓ ↓ ↓ ↓ ↓ ↓ ↓
Cipher Text: D M J D H B U

(IV) Poly-Alphabetic Cipher

DL-19.01.19

- A poly-alphabetic cipher uses a number of substitution at different positions in the menage.
- It is also one-to-many substitution cipher method.

Example —

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

HELLO - plain Text-
↓ ↓ ↓ ↓ ↓
URYAB - Cipher Text-

CRICKET - plain Text-
↓ ↓ ↓ ↓ ↓ ↓ ↓
PCVRXRE - Cipher Text-

ELECTRICAL - plain Text-
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
RYTPECVRNA - Cipher Text-

(VI)

(v) Playfair cipher (5×5 matrix is used)

- The playfair cipher, also called as playfair square, is a cryptographic technique i.e. used for manual encryption of data. This scheme was invented by charles wheatstone in 1854.

Algorithm —

Step-1 - Choose Keyword (PLAY FAIRENCRYPTION)

Step-2 - Enter characters of keyword in 5×5 matrix row wise from left to right.

Step-3 - Fill remaining spaces in matrix with rest of English alphabet.

Step-4 - Combine I and J in same cell.

Example—

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

PLAYFAIR ENCRYPTION

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

→ Encryption Process ——

1- Broke the plain Text in group of two alphabets.

2- If both alphabets are same (or only one in left) add an X after first Alphabet.

3- If both the alphabet in the pair appear in the same row of matrix, replace them with alphabets to their immidiate right respective.

4- If both alphabets in the pair appear in the same Colum replace with alphabets immidiately below then respective.

5- If the alphabets are not in same row or column, replace them with alphabets in the same row respective but at other pair of corners.

Step-1

N A M E

N A
↓ ↓
M E

Step-2 A L I C E

A L
I C
E (X)

Step-3

F P
↓ ↓
P L

Step-4

E M
↓ ↓
B W

Step-5

K W
↓ ↓
U/W K/Q

2.4 Encryption & Decryption

Encryption	Decryption
- It is the process of converting from plain text to cipher text using a key.	- It is the process of converting from cipher text to plain text using a key.

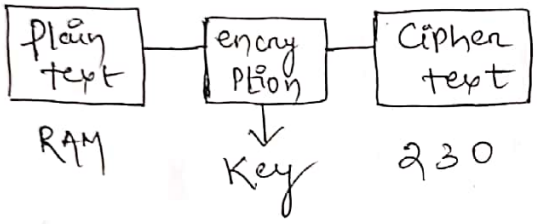
- It has automatic in nature because whenever the data is transfered or send between two machines, it is automatically encrypted.

- In that process text will be considered as coded form (Non-readable form).

- It has automatic and manual in nature because the receiver of the data automatically converts the data from the codes to original code. In some case it is done manually as well.

- In that process that will be considered as non-coded form (Readable form).

-



-

2.3 Transposition Techniques — DL- 21.1.19

- A Transposition Cipher is a method of encryption by which the positions held by unit of plaintext (which are commonly characters or group of characters) are shifted according to a regular system, so that ciphertext constitutes a permutation of plain text.

- Position of Plain text will be changed to convert the cipher text.

Example —

T	H	I	N	K
0	1	2	3	4

- Plain Text

3 1 0 2 4

N	H	T	I	K

- Cipher Text

- The different types of Transposition techniques are =

① Rail Fence Technique

② Simple Columnar Technique

① Rail Fence Technique =

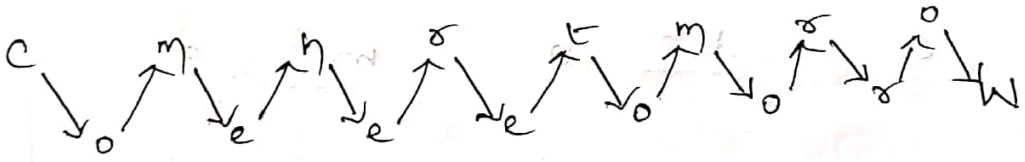
Step-1 = Write down the plain text message as sequence of diagonals.

Step-2 = Read the text Row by Row.

(Step-1)

Ex =

Come here tomorrow — plain Text



(Step-2)

Ex =

Cmrtmroeeeoorw — Cipher Text

② Simple Columnar Technique =

Step-1 = Write the plain text message Row by Row in a Rectangle of a pre-defined size.

Step-2 = Read the message column by column, however it need not be in the order of columns 1, 2, 3 etc.

It can be any random order such as - Column 2, 3, 1 etc.

(Step3 =) The message thus obtained is the ciphertext message.

(Step-1)

Ex =

Come home tomorrow

- plain text

Let us consider a rectangle with the 6 columns

Col1	Col2	Col3	Col4	Col5	Col6
C	o	m	e	h	o
m	e	t	o	m	o
r	r	o	w		

(Step-2)

Ex =

Let us decide the order of column as some random order say that -

4 2 1 6 3 5

eow oer cmr oo mto hm

- Cipher text

2.5 Symmetric & Asymmetric Key Cryptography

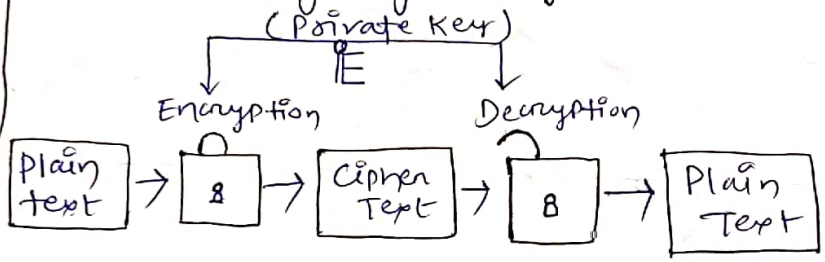
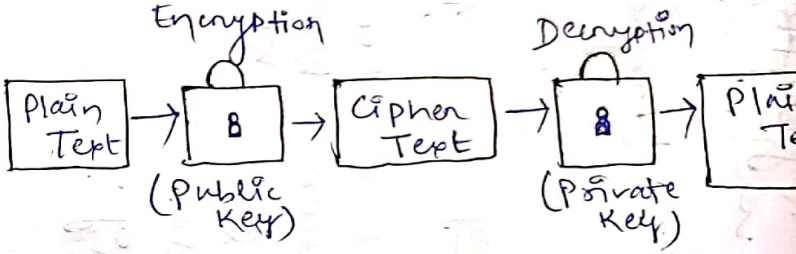
Difference Between Symmetric & Asymmetric Key

Attribute	Symmetric Key	Asymmetric Key
(1) Keys	1 Key is shared betw two or more entities both encryption & decryption are done with private key.	1 entity has public-key & other entity has a private key.

gmp

Difference Between Symmetric & Asymmetric Key

Dt- 24-01-

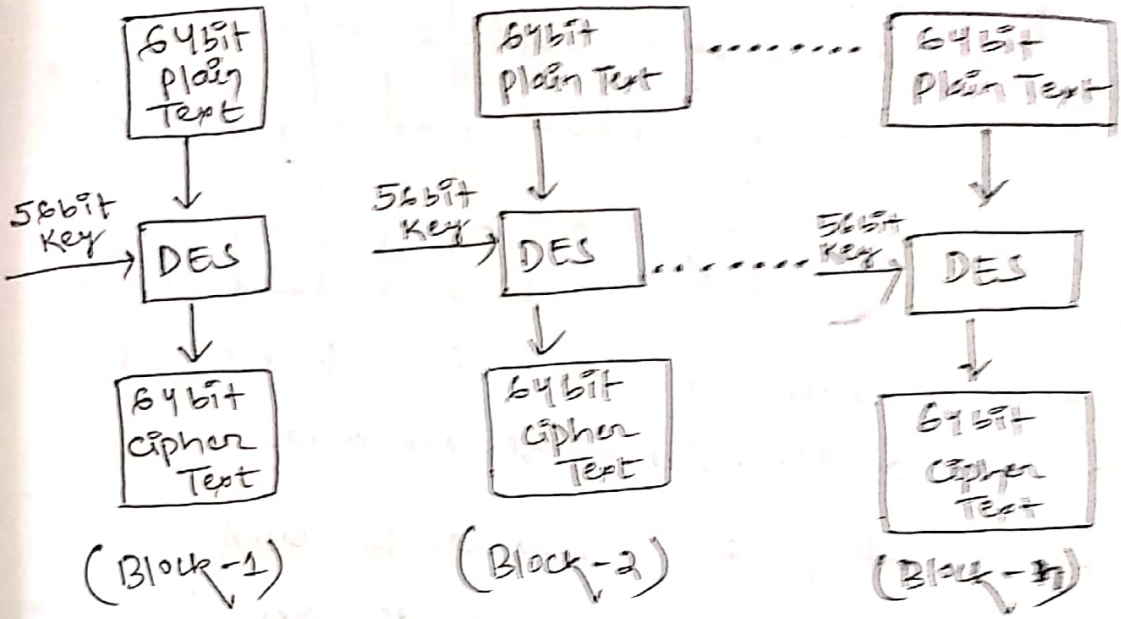
Attribute	Symmetric Key	Asymmetric Key
① Keys	One key is shared between two or more ~~empty Key~~ entity. 	One entity has a public key other entities has a private key. 
② Key Exchange	Out- of band (Problem of Key exchange)	Limit of band (No problem of Key Exchange)
③ Speed	Algorithm is less complex and Faster.	Algorithm is more complex and slow
④ No. of Key	grows exponentially as users grow.	grows linearly as user grow.
⑤ Security Services provided	Confidentiality	Confidentiality, Authentication, Access & Availability

3.1 Symmetric Key Algorithms =

- It has two types :-
  (I) Stream Cipher (mono alphabetic cipher)
  (II) Block Cipher (polyalphabetic cipher)

* Stream Cipher	Block cipher
- Stream cipher is equivalent to mono alphabetic cipher.	- Block cipher is equivalent to poly alphabetic cipher.
- Stream cipher operates on smaller unit of plain Text.	- Block cipher operates on larger block of data.
- Faster than Block Cipher.	- Slower than Stream Cipher.
- Required less code.	- Required more code.
- One to One Key is used.	- One to many key is used.
- Stream cipher is also used as Hardware implementation.	- Block cipher is also used as Software implementation.
- Example = Monoalphabetic Cipher, OTP (One time password)	- Example = polyalphabetic Cipher, Data Encryption Standard (DES)
- Application = Secure communication on the web.	- Application = Database, file encryption

3.3. Data Encryption Standard (DES)



- Data Encryption Standard is also called as Data Encryption Algorithm by ANSI (American National Standard Institute) and also it is organised by ISO (International Standard organization).

Working principal of DES

- It is Block Cipher
- It encrypts the data block of size is 64bit each
- 64 bits of plaintext is input to DES, which produces 64 bit of cipher text.
- The same algorithm & same key is used for Encryption & Decryption.
- The key length is 56 bits.
- Initially key consist of 64 bit.
- Before, the DES process even starts, every 8th bit of the key is discarded to produce a 56-bit key & bit positions are 8, 16, 24, 32, 40, 48, 56, 64.

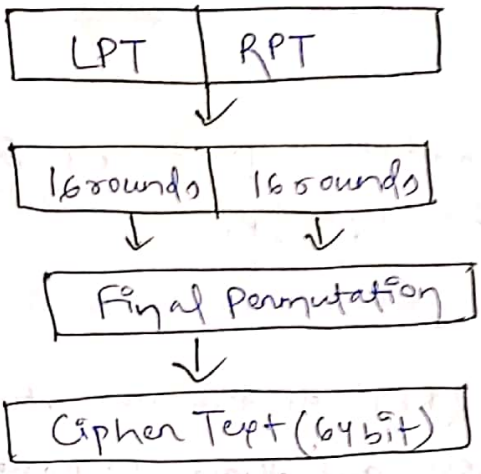
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64

- From this diagram we concluded that every 8th positions as discarded to shaded area.
- Before discarding these bits can be used for block checking to ensure that the key doesn't contain any error.
- Thus, discarding of every 8 bit of the key produces a 56 bit key from the original 64 bit key.
- DES based on the two fundamental attributes of cryptography:-
  (I) Substitution (confusion)
  (II) Transposition (Diffusion)
- DES consist of 16 steps & each step is called Round
- Each round performs the step of Substitution or Transposition.

- Board Level Steps of DES ——

- Step-1 → Plain Text (64 bit)
- Step-2 → Initial Permutation

- Step-3
- Step-4
- Step-5
- Step-6



Step-1

In the first step the 64 bit plain text block is handed over to an initial permutation.

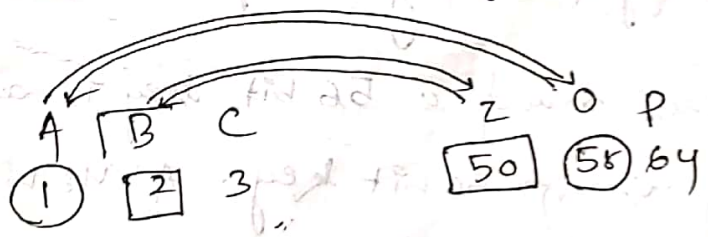
Step-2

Initial permutation is the perform to the plain Text.

* Initial permutation —

- It happens only once and it happen before the first round.
- It also suggest how the transposition in IP should process.
- IP replaces the first bit of the original plain text block with 58th bit of the original plain text block, the second bit replace with the 50th bit of the original plain text block.

Example —



- After IP is done the resulting 64 bit permuted text block divided into two half block & each block consist of 16 bit.
- We have called LPT (Left plain text) & RPT (Right plain text).

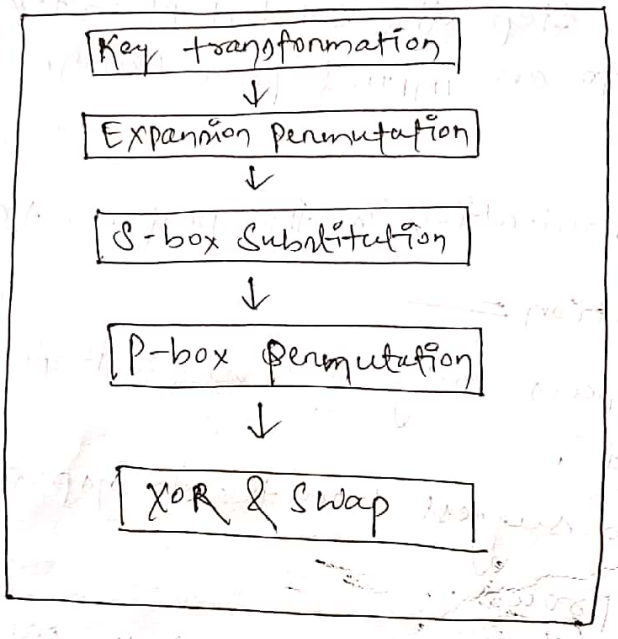
DE - 28.01.19

Step-3

The initial permutation produces 2 halves of permuted block i.e. LPT & RPT.

Step-4

Each of the LPT & RPT go through the 16 round of encryption process and these 16 round are perform on these DES block.



* Key Transformation

- Here the initial 64 bit key is transfered into 56 bit by discarding every 8 bit of initial key.
- For each round a 56 bit key is available of from which 56 bit key. A 48 bit Soft key is generated during an round using a process is called as Key Transformation.

* Expansion Permutation

- We had two 32 bit plain text areas called as LPT & RPT.
- During expansion permutation the RPT & LPT is expanded from 32bit to 48bit.

* S-box Substitution

- It is the process that accept the 48bit input from the XOR operation involving the compressed key and expanded RPT & produces an 32bit output using the substitution technique.
- This technique is performed by 8 substitution boxes is called as S-box substitution.

* P-box permutation

- The output of S-box consist of 32bits & these 32bits are permuted using a P-box.
- The straight-forward permutation mechanism involves simple permutation i.e. replacement of each bit with another bit, as specified in the p-box table without any expansion & compression this is called P-box permutation.

* XOR & Swap

- Performing all the operation only on the 32bit right half portion of the 64bit original plaintext, left half portion was also touched.

- So the left half portion of the initial 64 bit plain text block is appended with the output produced by P-box permutation.

Step-5

At the end of the 16 rounds the final permutation is performed only once which is called as simple transposition.

Step-6

Finally we get the ciphertext.

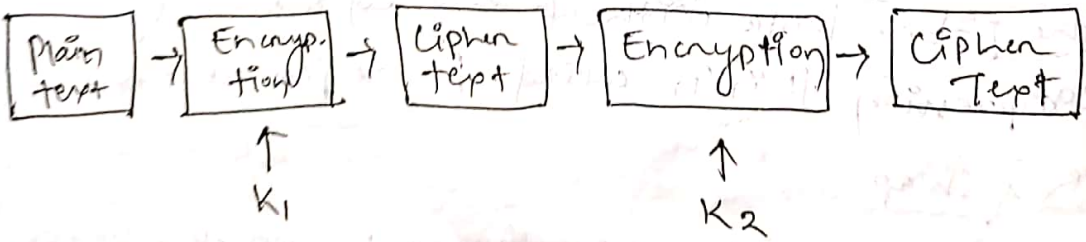
Dt - 31.01.19

Variation of DES :-

DES has 2 types :- i) Double DES
ii) Triple DES

i) Double DES —

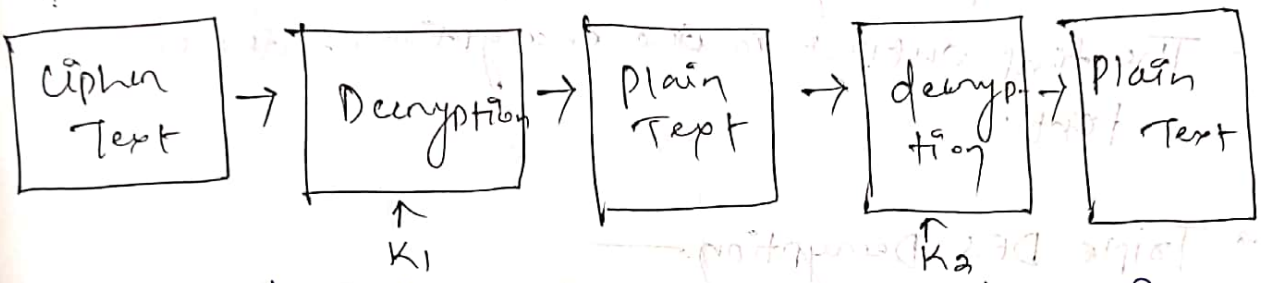
* Double DES Encryption —



- Double DES encryption uses 2 keys i.e. K_1 & K_2.
- The first performs on DES on the original plain text using K_1 to get the encrypted text.

- It again performs DES on the encrypted text but this time will the other key i.e. K_2.
- The final output is the encryption of the encrypted text.

* Double DES Decryption ——



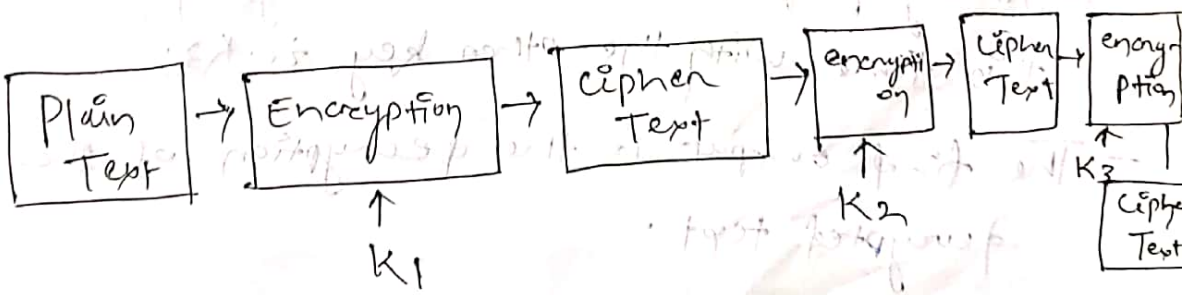
- Double DES Decryption uses 2 key i.e. K_1 & K_2.
- It first performs DES on the original ciphen text using K_1 to get decrypted text.

DE - 04.02.19

- It again performs DES on the decryption text but this time with the other key i.e. K_2.
- The final output is the decryption of decrypted text.

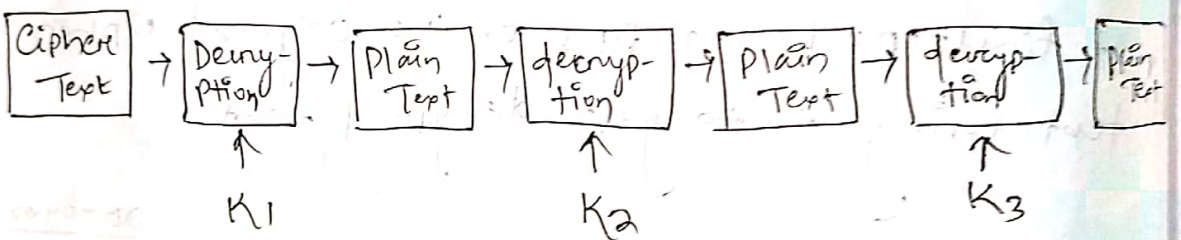
(ii) Triple DES —

* Tripple DES Encryption —



- Triple DES Encryption uses 3 keys i.e. K_1, K_2, K_3.
- It first perform DES on the original plain text using K_1 to get encrypted text.
- It again perform DES on the encrypted text but this time with the other key i.e. K_2.
- It finally perform DES on the encrypted text but this time with the other key i.e. K_3.
- The final output is the encryption of the encrypted text.

* Triple DES Decryption —



- Triple DES Decryption uses 3 keys i.e. K_1, K_2, K_3.
- It first perform DES on the original cipher text using K_1 to get decrypted text.
- It again perform DES on the decrypted text but this time with the other key i.e. K_2.
- It finally perform DES on the decrypted text but this time with the other key i.e. K_3.
- The final output is the decryption of the decrypted text.

The RSA Algorithm

- It was purposed by Ron Revest-Adi Slamir and Leonard Adleman at MIT, USA.
- It is an Asymmetric key cryptography algorithm.
- RSA is most widely accepted publically solution as it schemes the problem of agreement and distribution.
- It used prime number and form basic of the RSA Algorithm.
- Prime number is that number i.e. divisible by itself or divisible by one.

  ex- 2, 3, 5, 11, etc.

- The RSA Algorithm is based on the mathematical fact i.e. easy to find & multiply large prime number but it is difficult to factor their product.
- The private key and public key RSA based on the very large prime number.
- Main aim of the RSA Algorithm is to convert plain text to cipher text and also cipher-text to plain text.

Algorithm —

Step-1 Choose large prime number P and Q

Step-2 Calculate $N = P \times Q$

Step-3 Select the public key (for encryption) E, such that it is not factor of $(P-1)$ and $(Q-1)$

Step-4 Select the private key (for decryption) D, such that the given equation is true

$$D \times E \bmod (P-1) \times (Q-1) = 1$$

Step-5 For Encryption calculate the cipher text (CT) from the plain text (PT) as follows

$$CT = PT^E \bmod N$$

Step-6 Send cipher text as the CT to the receiver

Step-7 For decryption calculate the plain text (PT) from the cipher text (CT) as follows

$$PT = CT^D \bmod N$$

Examples :— DT-06.02.19

Step-1

Let $P = 7$, $Q = 11$

Step-2

$N = P \times Q = 7 \times 11 = 77$

Step-3

$(7-1) = 6 = 2 \times 3$

$(11-1) = 10 = 2 \times 5$

$E = 13$

Step-4

$(D \times E) \bmod (P-1)(Q-1) = 1$

$\Rightarrow D \times 13 \bmod (7-1)(11-1) = 1$

$\Rightarrow D \times 13 \bmod 6 \times 10 = 1$

$\Rightarrow D \times 13 \bmod 60 = 1$

$\Rightarrow 37 \times 13 \bmod 60 = 1$

$\Rightarrow 481 \bmod 60 = 1$

So, $D = 37$

$60 = 13 \times 4 + 8$ (quotient 4, remainder 8)

$60 = 13 \times 9 + 3$ (quotient 9, remainder 3)

$60 = 13 \times 13 + 1$ (quotient 13, remainder 1)

$60 = 13 \times 3 + 21$ (quotient 3, remainder 21)

$60 = 13 \times 2 + 34$ (quotient 2, remainder 34)

$60 = 13 \times 1 + 47$ (quotient 1, remainder 47)

$60 = 13 \times 8 + (-1)$ (quotient 8, remainder -1) ✓

So $D = 37$

Step-5

$CT = PT^E \bmod N$

Let $PT = 2$

$= 2^E \bmod 77$

$= 2^{13} \bmod 77$

$= 8192 \bmod 77$

$= 30$

77 | 8192 | 16
77

115

Step-6

$CT = 30$ Send to the receiver.

Step-7

$PT = CT^D \bmod N$

$= 30^{37} \bmod 77$

$= 2$

DE-07-0219 DIGITAL CERTIFICATE AND PUBLIC KEY INFRASTRUCTURE

Unit-4

Digital Certificate :—

- In cryptography a public key certificate (also known as Digital certificate or Identity certificate) is an electronic document that uses a digital signature to bind a public key with an identity information such as name of person, organization, address, date of birth etc.
- This Certificate can be used to verify that a public key belongs to an individual.
- Digital certificate also ensures confidential communication between two parties using encryption.
- The Digital certificate must be issued by trusted entity.
- Digital certificate establishes the relation between a user & a public key.

Example -

Someone in travelling to another country as passport is used as proof for identifying in same manner digital offers similar types of identification on Internet.

Sample Of Digital Certificate :-

User name : ankit

Public key : {1, 2, @, &, a, b, c}

Serial No : 239021

Email ID : ankit21@gmail.com

Valid from : 15|10|2016

valid to : 15|10|2019

Issuer name : UDAI

Digital Certificate Creation Steps :-

Step-1 :- Key generation

↓

Step-2 :- Registration

↓

Step-3 :- Verification

↓

Step-4 :- Certificate creation

① Key-generation

- Key generations are two types :-
  - (I) private Key
  - (II) public Key
- There are two types of approaches for this purpose :-

(i) The subject can created a private key or public key pair using some s/w which is a part of the web-server.

(ii) The private key generated is kept secret. The subject sends the public key along with the other information about himself or herself to registration authority.

(2) Registration

- This is done after the step 1 i.e. key generation.
- The user now sends the public key & the associated registration information (subject name to be apart of digital certificate).
- And all the evidence about himself or herself to the registration authority like paper page document such as :- a copy of present or business document to the registration authority.

01-08-02-19

(3) Verification

- After the registration process is complete, the registration authority has to verify the users credentials.
- The verification is in to repeats as follows :-

(i) Firstly, the registration authority

needs to verify the users credentials. such as the evidence provided are correct and that they are acceptable.

(ii) Second step is to ensure that the user who is requesting for the certificate does indeed process the private key corresponding to the public key i.e. send as a part of a certificate request to the registration Authority. This check is called as Checking the proof of credentials of the private key.

(4) Certificate Creation

- Here the registration authority (RA) passes all the details of the user to the Certificate authority (CA).
- The CA does its own verification & creates a digital certificate for the user.

Private Key Management -

(1) Protecting private keys

- The private of the user might be require to be transferred from one location to another location
- The certificate & the private key must be protected as they are moved another location

- The public key cryptography standard ensure that they are encrypted using a symmetric key which is derived from the user private key protection password.

(II) Multiple key pairs

- The private key approaches recommanded that in serious business application the user should possess multiple key pair.
- The need for this, is that one certificate should be strictly used for signing & another for encryption. This is ensure that the loss of the private key doesn't affect the complete operation of a user encryption and decryption.

(III) Key update

- The security practices demand that the keypair should be updated periodically because overtime, key become susceptible to cryptography attack.
- The digital certificate expire after a certain data ensure this required an update to the key pair.

(IV) Key Arrival / Achival

- The key must be plan for & maintain the history of certificate and the key of its use or this can cause serious legal problems therefore, the key achieval is very significant respect

Of any private key solution.

PKIX MODEL (Public Key Infrastructure X.509)

- The X.509 standard defines the digital certificate structure format & fields. It also specify the procedure for distributing the public key.
- In order to extend such standard & make them universal the Internet Engineering Task Force (IETF) from the public key in Infrastructure X.509 (PKIX) model working good.
- It mainly specifies how the digital certificate can be deployed in the world of Internet.

PKIX SERVICES

- The PKIX identifies the primary goal of a public key Infrastructure & this services include.
  - Registration
  - Initialization
  - Certification
  - Key pair recovery
  - Key generation
  - Key update
  - Cross Certification
  - Revocation

Registration

- It is a process where an end entity makes itself known to a certificate Authority & this is done through Registration Authority (RA).

Initialization

- It deals with the basic problems such as how the end entity is sure that it is taking to the right certificate Authority (CA).

Certification

- The certificate Authority creates a digital certificate for the end entity & Returns to the end entity. Maintain a copy for its own record & also copies it's to public directory.

Key pair Recovery

- Key used for encryption maybe required to be recover at a later date for decryption some old document.

Key generation

- The PKIX specifies that the end entity should be able to generate public key & private key pairs or the CA & RA should be able to do this fault for the end entity.

Key update

- It always a smooth transation from one expiring key pair to a fresh one by the automatic renewal of digital certificate.
- There is a provision for manual digital certificate renewal request & responds.

Cross Certificate

- It helps in establishing trust model as the end entity that are certified by different certificate Authorities can cross verify others.

Revocation

- PKIX provide support for the checking of the certificate status in two models i.e. online or offline.

Dt - 11.02.19

Public Key Cryptography Standard (PKCS)

- It is the no. of PKIX Standard, that have been define by the RSA composition.
- The main purpose of PKCS is a standardized the public key infrastructure.
- The Standardization is in many respects such as Formatt-ing & Modifying.

Standard	Purpose	Details
• PKCS # 1	• RSA Encryption Standard.	• It defines the basic formatting for RSA public-key function i.e. for digital signature & It defines how digital signature should be calculated.
• PKCS # 2	• RSA Encryption Standard for menage digests	• This standard outlines the menage digest-calculation.
• PKCS # 3	• This standard is define hellman Key agreement-standard.	• It defines the mechanism to implement hellman agreement-protocol.
• PKCS # 4	•	• It merge with the PKCS # 1.

Standard	Purpose	Details
• PKCS # 5	• This stands in password based encryption (PBE)	• It describes a method for encrypting string with asymmetric, the symmetric key is derived from a passw
• PKCS # 6	• This standard is extented - Certificate syntax stand.	• It defines syntax for extending a basic attribute of an X.509 digital certificate.
• PKCS # 7	• This standard is cryptography syntax standard.	• It specifies a syntax for data. That is the result of a cryptogra operation.
• PKCS # 8	• This standard in private key information standard.	• It defines the syntax for private key information.
• PKCS # 9	• This standard is selected attribute types.	• It defines the selected attribute types for use in PKCS # 6 extended certificate.
• PKCS # 10	• This standard is certificate request - syntax standard.	• It defines the syntax for requesting for digital certificate.

• PKCS # 11	• This standard is cryptography token interface standard.	• This standard is specify to token as cryptography.
• PKCS # 12	• This standard is personal information exchange syntax standard.	• It defines the syntax for personal identity information such as private key, Digital certificate.
• PKCS # 13	• This standard is elliptive curve cryptography standard.	• This standard is current under develope. This standard deals with a new cryptography mechanism.
• PKCS #14	• This standard is pseudo Random no generation standard.	• This is also under development. It specify the requirement & Proces of Random no generation.
• PKCS # 15	• This standard is cryptography token information system standard.	• It defines a standard for cryptography standard so that they can inter-operate.

Dt-12.02.19 INTERNET SECURITY PROTOCOLS Unit-5

Internet Security protocol (IPsec)

Protocol:-
Protocol is a set of rules and regulation which governs data communication between two or more users on the internet.

IP

- IP is a protocol or method by which data is ~~send~~ from one place to another place on the internet.
- Each computer on the internet has atleast one IP address that uniquely identifies, it from all other computers on the internet.

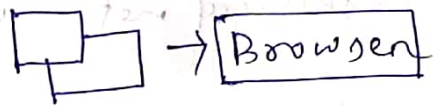
IP Address

- IP address is a numerical level assigned to each device connected to computer that use the internet protocol for communication.

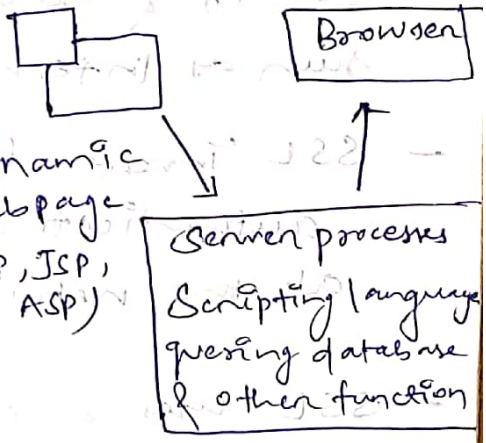
Difference Between Static & Dynamic Webpage

Static Webpage	Dynamic Webpage
- There is a no database connectivity in the webpages.	- There is a database connectivity in the webpg
- Automatic data will not upload (update).	- Automatic data will be upload.

- Content is same each time the page is loaded.	- Content is generated on the fully and changes regularly.
- Content only changes whereas some one updates and publish the site.	- Page contains server side code allows the server to generate unique content when the page is loaded.
- Ex:- HTML code	- Ex:- JSP, PHP; ASP



Passed straight-
Static webpage to browser (HTML)



Internet protocol Security

Internet protocol Security (IP sec) is a suit of protocol that allow secure, encrypted communication between two computer over an unsecured network.

Goals of Ip Security

1. To process IP packet-
2. provide defence against n/w attacks.
3. Ip-sec supports n/w level peer authentication, data origin authentication, data integrity, data confidentiality and replay protection.

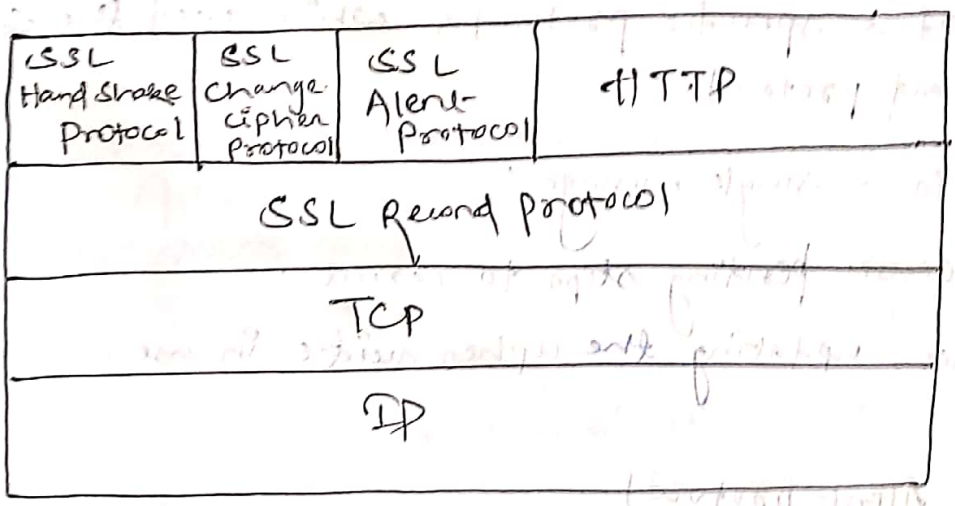
④ Ip Sec is an end to end security operating in the internet layer of the internet protocol suite.

Secure Socket Layer (SSL)

DE-13.02.19

- SSL is a computer networking protocol for securing connections between network applications clients & server over an insecured network such as internet.
- SSL eventually came to be used secure authentication & encryption for communication at the network & the transport layer.
- SSL uses a combination of publickey and symmetric key encryption to secure a connection between two computer system.
- SSL runs above the transport layer i.e. network layer. & SSL has been implementing for application including e-mail, file transfer etc.
- SSL protocol i.e. HTTPS.
- SSL address the need for security in internet communication
  1. Privacy - Convential Encryption
  2. Integrity - Message Authentication code
  3. Authentication - X.509 protocol

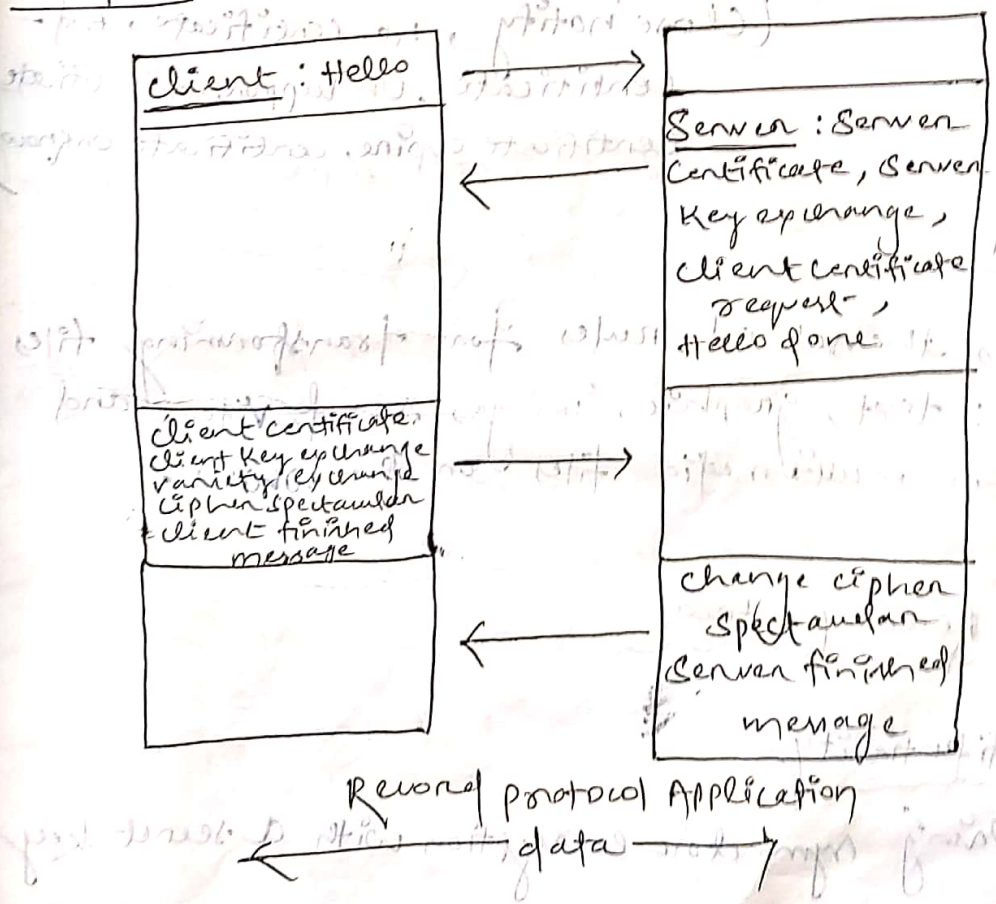
SSL Architecture



SSL Handshake Protocol

- It is used exchange all information by both sides for exchange of actual application's data by the transport layer.

Example



ii) SSL Change Cipher protocol

- 1 of 3 specific protocols which used the SSL record protocol.
- It is a single message
- It causes pending steps to correct.
- Hence, updating the cipher suite in use.

iii) SSL Alert protocol

- It conveys SSL related alert to peer entity.
- Severity (Warning)
- Specific Alert (Unexpected message, Bad record mac, de-compression failure, handshake failure, illegal parameter)
  (Close notify, no-certificate, Bad certificate, Unsupported certificate, certificate expire, certificate unknown)

iv) HTTP

- It is the set of rules for transforming files like: text, graphic, image, sound, video and other multimedia files on the WWW.

v) SSL Record protocol

- Confidentiality

  Using symmetric encryption with a secret key

by handshaking protocol.

- Message Encryption
  Using message Authentication code (MAC) with share secret key.

vi) TCP
- It is a Network communication protocol designed to send data packet over the Internet.

vii) IP
- It is a protocol or method by which data is sent from one place to another on the Internet. Each computer on the Internet has atleast one IP address that uniquely identifies it from all other computers on the Internet.

7) Transport Layer Security (TLS)
- TLS is a cryptography protocol that provides end-to-end communications security over networks and is widely used for Internet communications & on-line transactions.
- TLS is a staple security protocol and more efficient than SSL protocol.
- TLS protocol specification defines two layers:-
  (1) TLS Record protocol
  (2) TLS handshake protocol

(1) TLS Record Protocol

- It provides connection security.

(2) TLS Handshake protocol

- It enables the client & server to authenticate each other and to negotiate security keys before any data is transmitted & also TLS Handshake is multi-step process.

- TLS is a succession to the secure socket layer

DL-14.02.11

Secure HyperText Transfer Protocol

- It allows the secure exchange of files on the world wide web (WWW).
- Each SHTTP file is either encrypted, contains a digital certificate for both.
- For a given document SHTTP is an alternative to another well known security protocol, Secure Socket Layer (SSL) a major difference is that SHTTP allows the client to send a certificate to authenticate the user.
- But SSL allows the server to send a certificate to authenticate user.
- SHTTP is more tightly to be used in situation where a server represent a bank &

request- authentication for the user ie. more secured than i'd & password.

Time Stamping protocol (TSP)

- Each Transaction is issued in time stamp when it enters the system.
- If an order (old) transaction T_i & time stamp $T_s(T_i)$, a newer transaction T_j and time stamp $T_s(T_j)$ such that $T_s(T_i) < T_s(T_j)$.
- This protocol manages con-current execution such that in timestamps determine the Serializability order.
- For each data item queue two time stamps are maintain (1) ~~W-W~~ time stamp (Q) is the largest- timestamps of any transmission that executed right-(Queue) successfully.

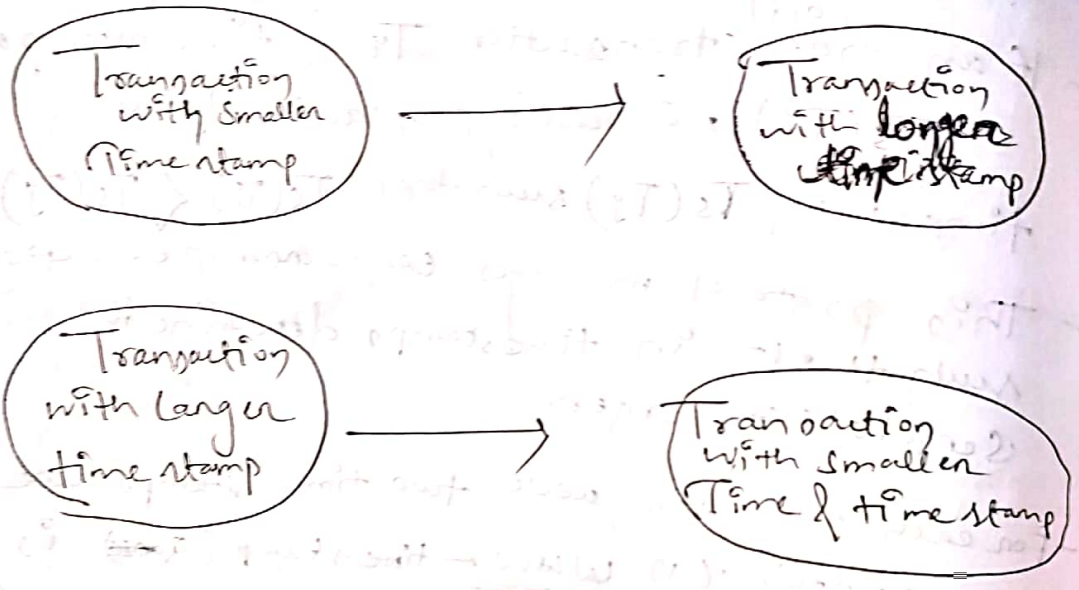
(11) Time-stamp (Q)

~~or Read time~~

- It is the largest- time stamp of any transaction that executed read (Q) successfully.
- The time stamping protocol ensure that any conflicity; read & write operation are executed in time stamp Order.

Correctness of Time Stamping Ordering Protocol

- The time stamping order protocol guarantee that serializability since all the data in the precedence graphs are of the form.



- This time stamp protocol ensures freedom from the deadlock. As no transaction ever waits.

V.V.I

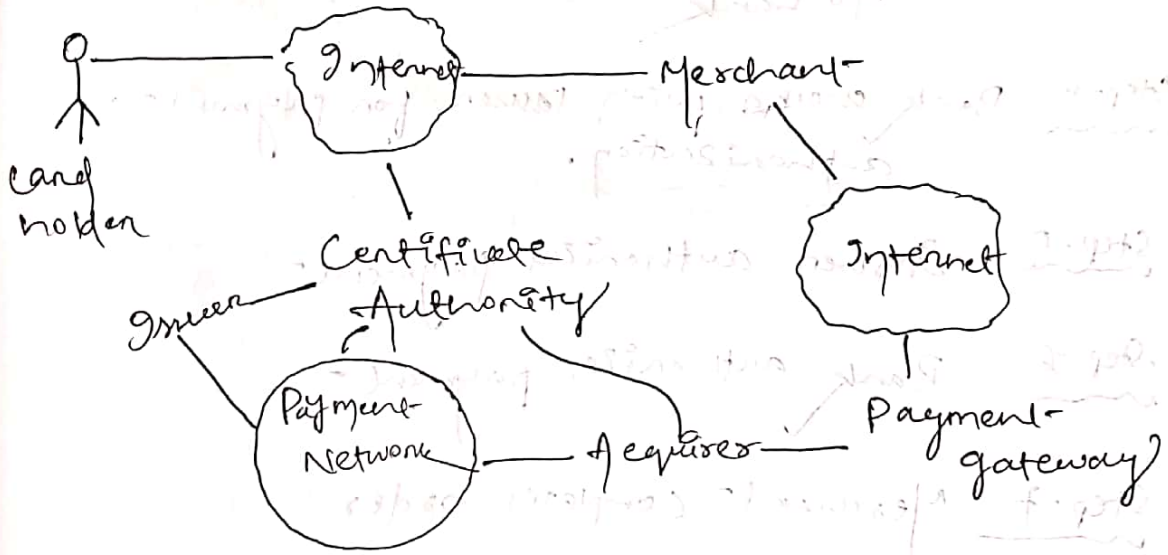
SET (Secure Electronic Transaction)

Dt-16.2.21

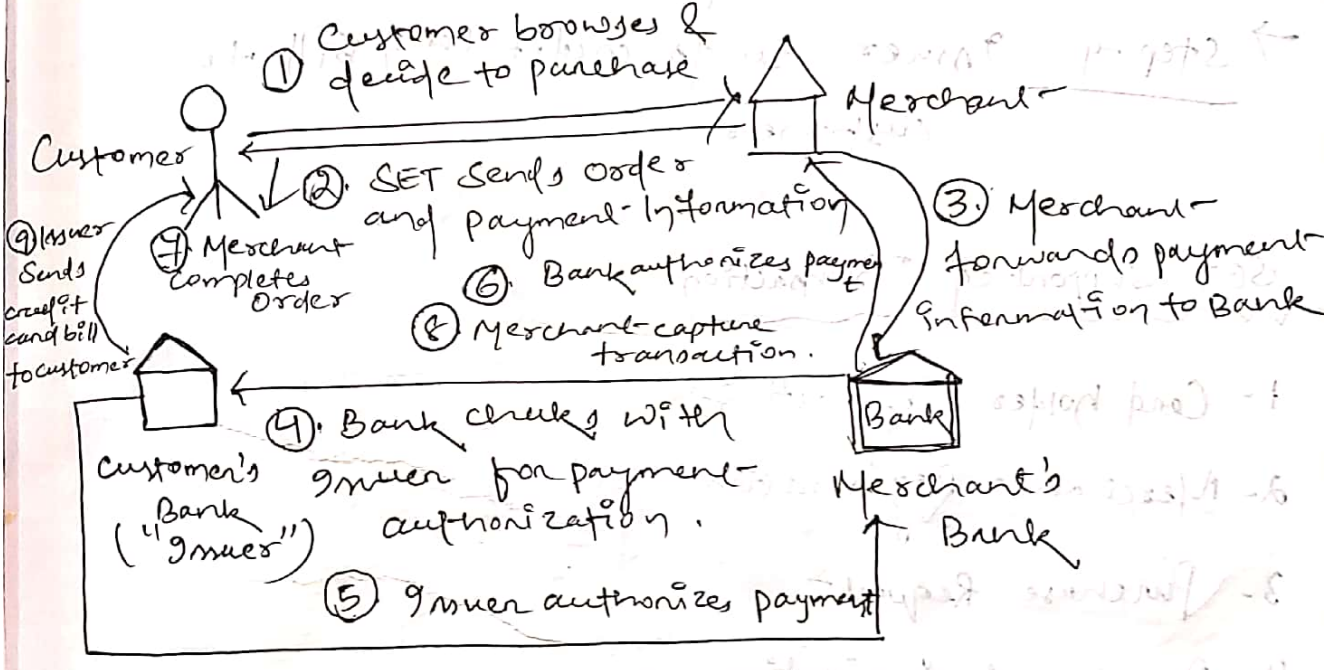
- It is developed by Visa, Mastercard, Rupay etc.
- Designed to protect credit card & Debit card transaction.
- 3 major cases including their
  1) Confidentiality :- All messages encrypted
  2) Trust :- all parties must have digital certificate

3) Privacy :- Information made available only when and where necessary.

Participants in the SET system :-



SET Transaction Principle



→ Step-1 Customer Browses and decide to purchase.

→ Step-2 SET sends order and payment-information

→ Step-3 Merchant forwards payment-information to bank

→ Step-4 Bank checks with issuer for payment-authorization.

→ Step-5 Issuer authorizes payment-

→ Step-6 Bank authorizes payment-

→ Step-7 Merchant completes order

→ Step-8 Merchant-capture transaction

→ Step-9 Issuer sends credit card bill to customer.

SET Supported Transaction

1- Card holder Transaction
2- Merchant-Registration
3- Purchase Request-
4- Payment-Authorization
5- Payment-capture
6- Certificate Query
7- Purchase Inquiry

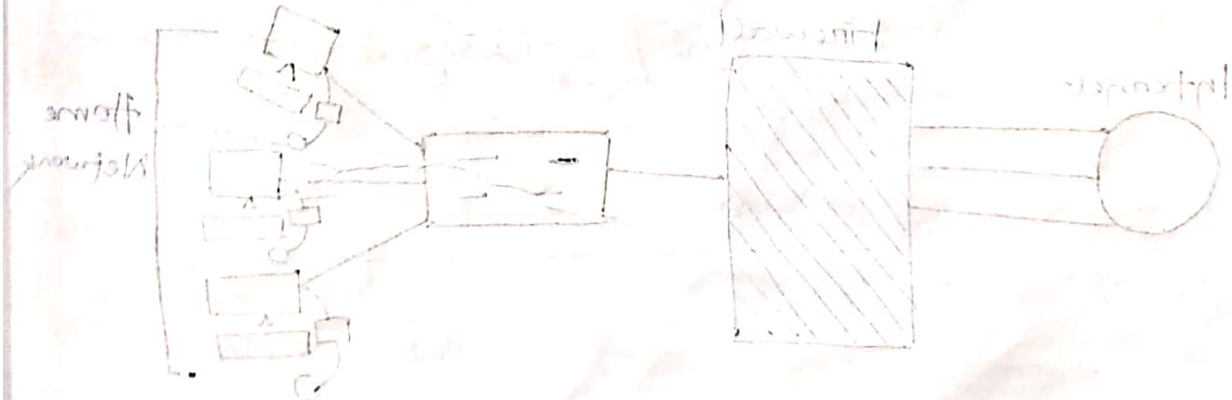
8- purchase Notification

9- Sale Transaction

10- Authorization Reversal

11- Capture Reversal

12- Credit or payment Reversal

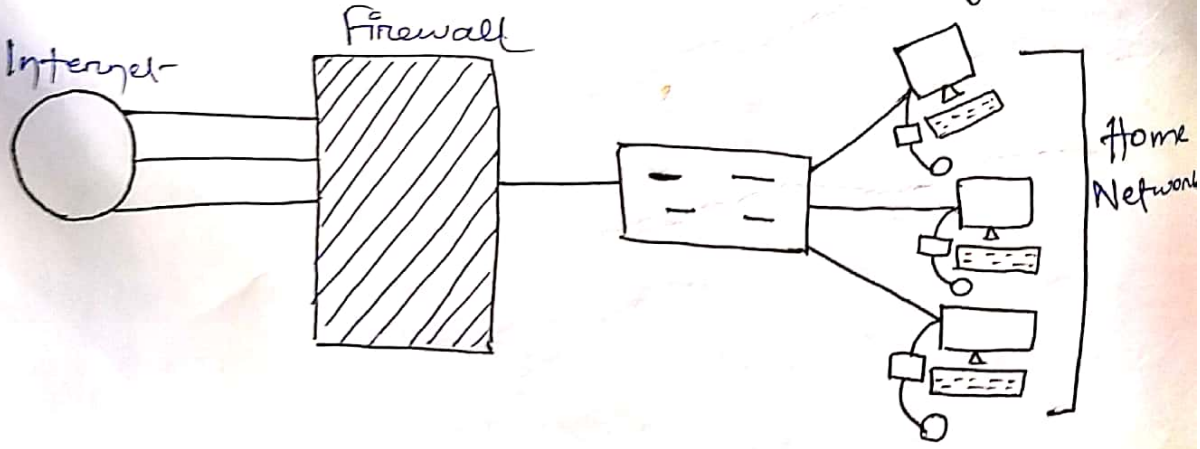


7. NETWORK SECURITY & VPN

Brief Introduction of TCP/IP :-

Firewall : (Network layer)

- Firewall acts like a security. It implemented like a guard to co-operate network by standing between the network and the outside world.
- A firewall is a system design to prevent unauthorised accessed to or from a private network.
- Firewall can be implemented in both hardware & software, the firewall decides if the traffic can be allowed to flow or whether it must be stopped from proceeding further.



- It is also hardware or software to protect Computer virus, malware etc

- It can be classified into 5 categories :-

(i) Packet- Filtering Firewalls
(ii) Stateful Inspection Firewalls
(iii) Circuit level gateways firewalls
(iv) Application level gateways Firewalls
(v) Next-gen firewalls

(i) Packet- Filtering Firewalls

- As the most "basic" and oldest-type of firewall architecture.
- The packet- filtering firewalls basically create a check point at a graphic router or switch.
- The firewalls performs a simple check of the data packets coming through the routers inspecting information such as the destination & orgn- IP address, pack type, Port number packet type, Port number etc.

(ii) Stateful Inspection Firewalls

These firewalls combines both packet- inspection technology & TCP handshake verification, to create a level of protection greater than either of the previous firewalls.

(iii) Circuit level gateways firewalls

- As another simplistic firewall type i.e. meant to weakly & easily approve or deny traffic without consuming significant computing resources, circuit level gateways work by verifying the transmission control protocol handshake.

(iv) Application level gateways firewalls

- It is also known as Proxy Firewalls.
- This firewalls operate at the application layer to filter incoming traffic between your network & traffic source hence the name is "application level gateway".

(v) Next-gen firewalls

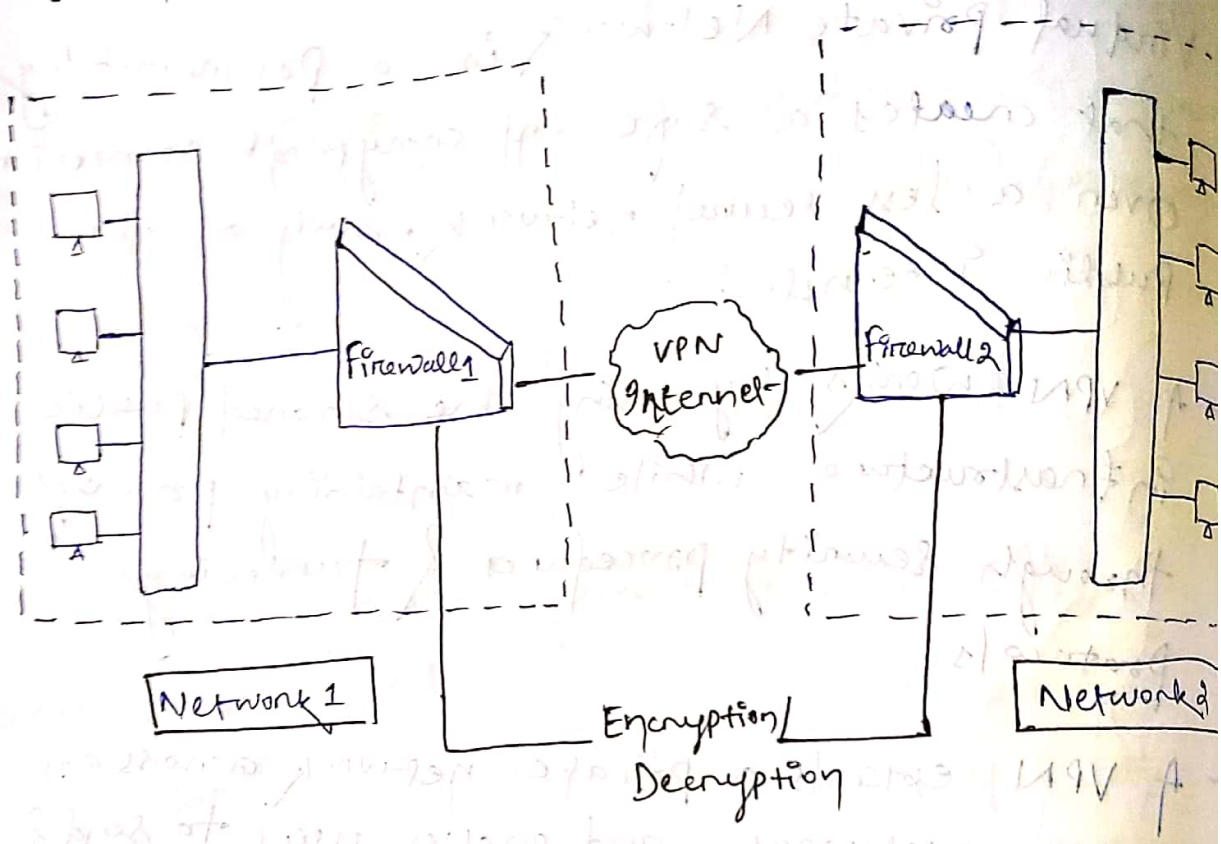
- Some common features of next generation firewall include deep packet-inspection (checking the actual contents of the data packet)
- Next generation firewalls may include other technologies such as Intrusion prevention systems (IPSs) that work to automatically stop attacks against your network.

Virtual Private Network (VPN)

Dt-26.02.19

- Virtual private Net-work is a programming that creates a safe and encrypted connection over a less secured network, such as the Public internet.
- A VPN works by using the shared public infrastructure while maintaining privacy through security procedures & tunneling protocols.
- A VPN extends a private net-work across a public Net-work, and enables users to send & receive data across shared or public networks as if their computing devices were directly connected to the private network.
- A VPN available from the public internet can provide some of the benefits of a wide area network (WAN).
- A VPN can connected distant network of an organization or it can be used to allow traveling user to remotely access a private network securely over the internet.

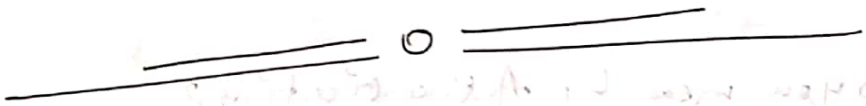
VPN Architecture between Two point



- The Idea of VPN is actually quite simple to understand, suppose an organization has two network which is physically apart from each other and we want to connect them using a VPN approach.
- In such case, we set up two firewalls i.e. Firewall 1 & Firewall 2, the encryption & decryption are performed by Firewall 1 & Firewall 2.
- We have shown two networks i.e. Network 1, Network 2, Network 1 connect to the ~~VPN~~ Internet via Firewall 1.

- Similarly, Network 2 connects to the Internet via Firewall 2.

- However, the key point here is that two firewalls are vertically connected to each other via VPN Tunnel. We have shown this with the help of VPN Tunnel between the two firewalls to protect the traffic passing between any two host on the different network.



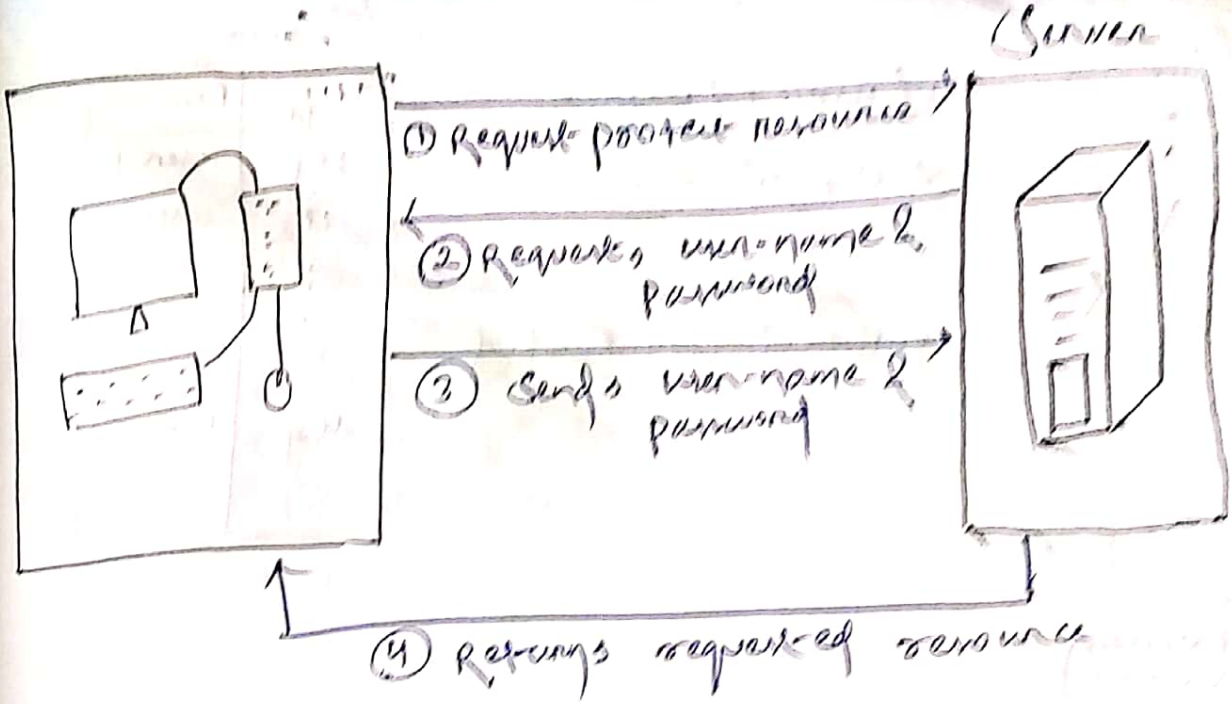
Dt - 7/03/19 User Authentication Ch-6

6.1 Authentication Basic
6.2 Password
6.3 Authentication Tokens
6.4 Certificate based Authentication
6.5 Biometric Authentication

6.1 Authentication Basic

What do you mean by Authentication?
- It helps establish trust - identifying the particular user system depending upon their user id & password.
- Authentication is a process in which the credentials provided are compared to those file in a database of authorized users information on local operating system or within an authentication server. If the credentials match the process is completed & user is granted authorisation access.

HTTP Basic Authentication
- Client sends the user name & password pair in the HTTP header authorization.
- Username & password must be send for every HTTP request for the authorization to be validated.



Types of Authentication Mechanism :-

(a) Password

- (a) Clear Text Password
- (b) Something derived from password
- (c) Message Digest of password

Password

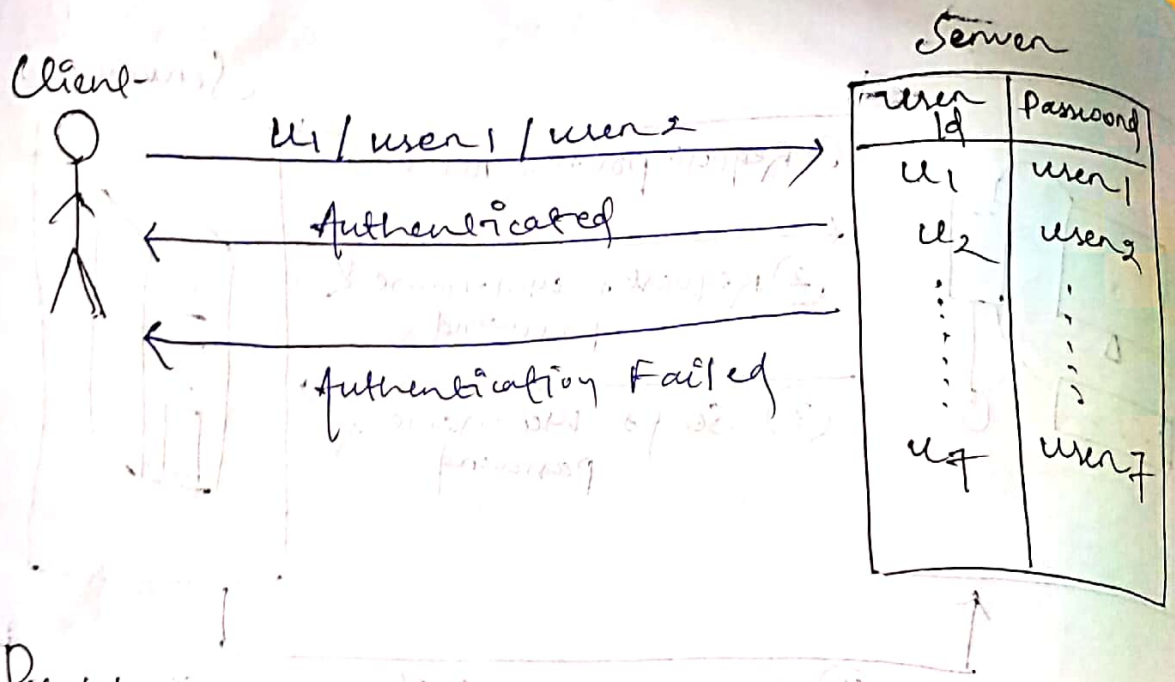
- It is composed of string, alphabet, number - character, special character etc.

- Password is the most common form of the authentication & it is also 3 types :-

(i) Clear Text password
(ii) Something derived from password
(iii) Message Digest of password

(i) Clear Text password :-

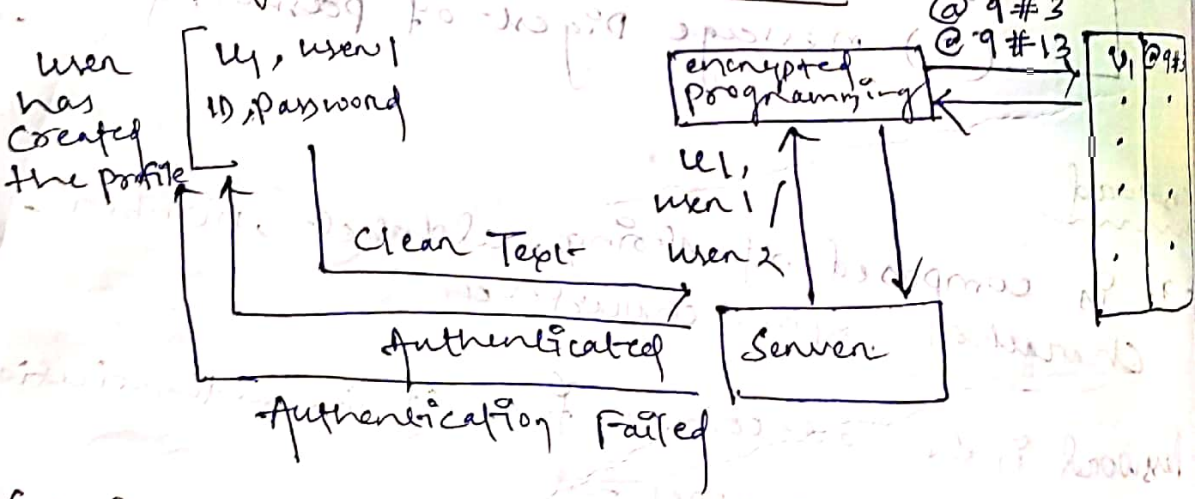
- Store password in the plain text in the - server.



Problem

- Store password in clear text form.
- password travels in clear text from client to server.

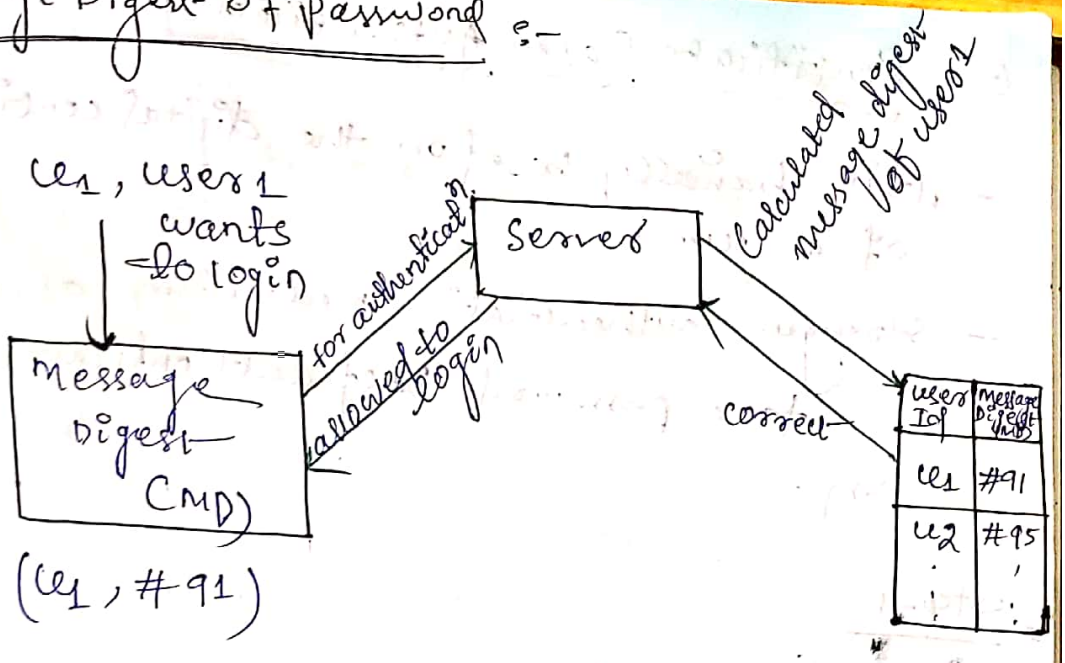
(a) Something derived from password :-



Solution

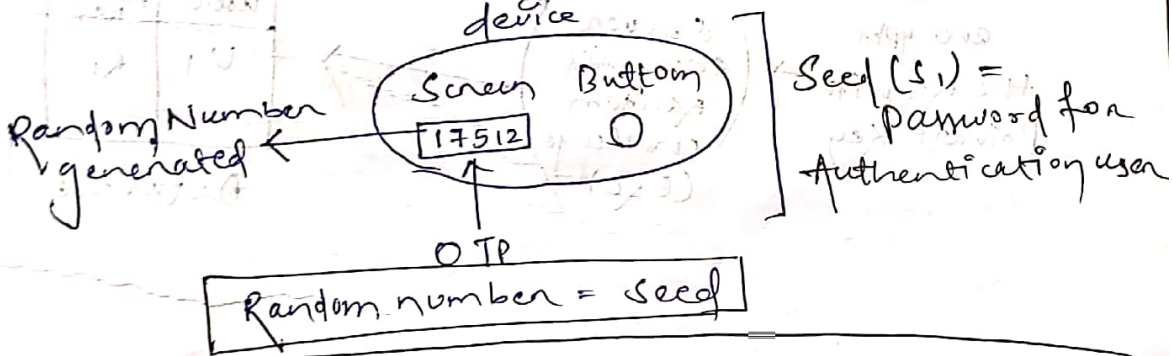
- Store the password in cipher text form.
- Password travels in encrypted format of text from client to server.

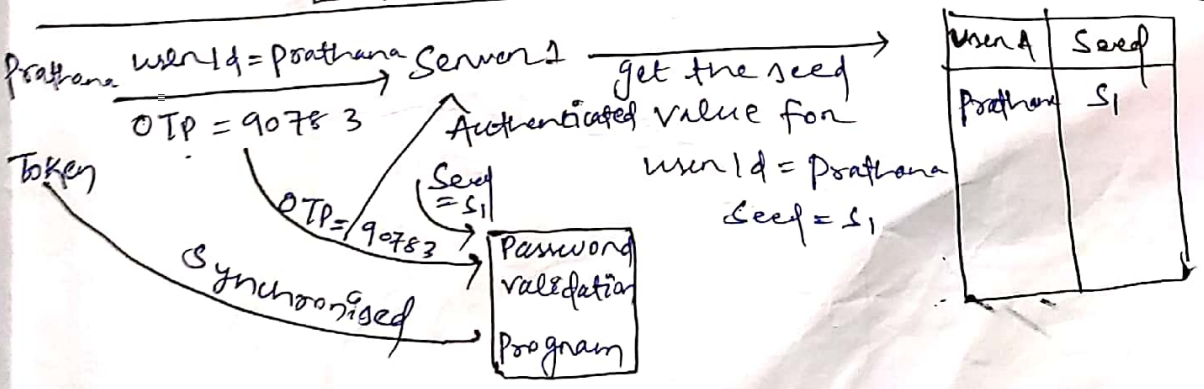
(3) Message Digest of password :-



6.3 Authentication Tokens :

- It is useful to Alternative to password i.e. created by the server.
- It is a small device that generates a new random value everytime it is used.
- Each authentication token is pre-programmed with a unique no called random seed.

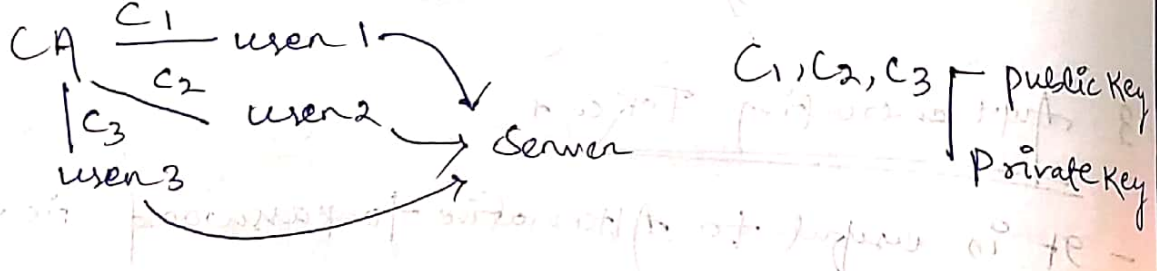




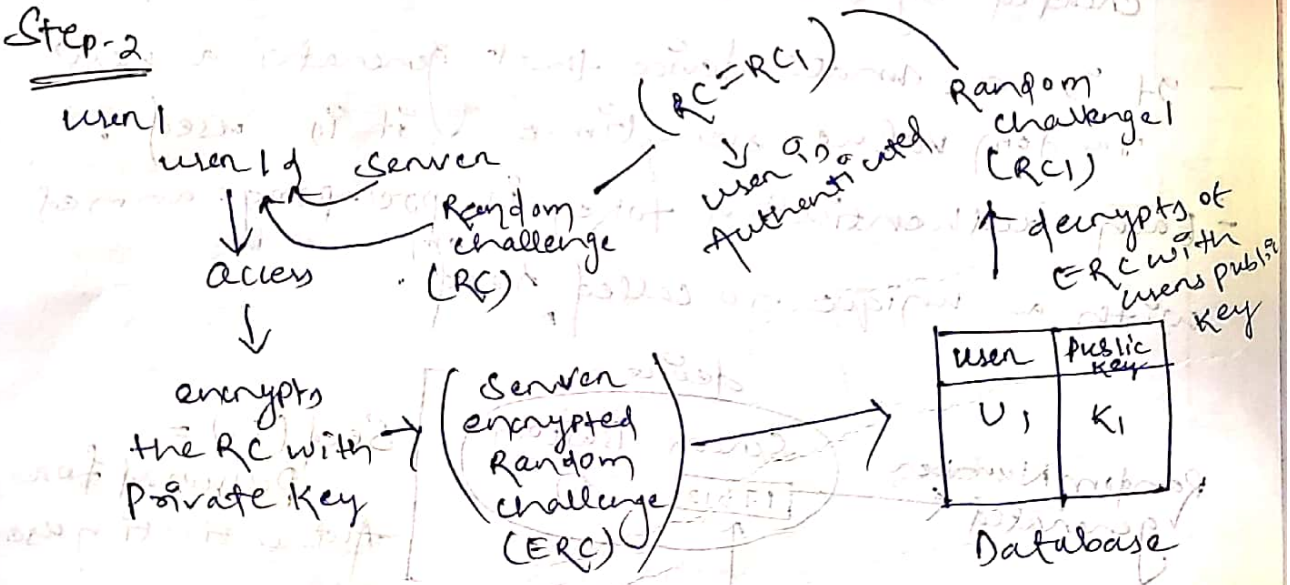
6.4 Certificate Based Authentication

- It is basically based on the digital certificate of a user.
- Stronger authentication mechanism as compared to a password based authentication mechanism.

Step-1



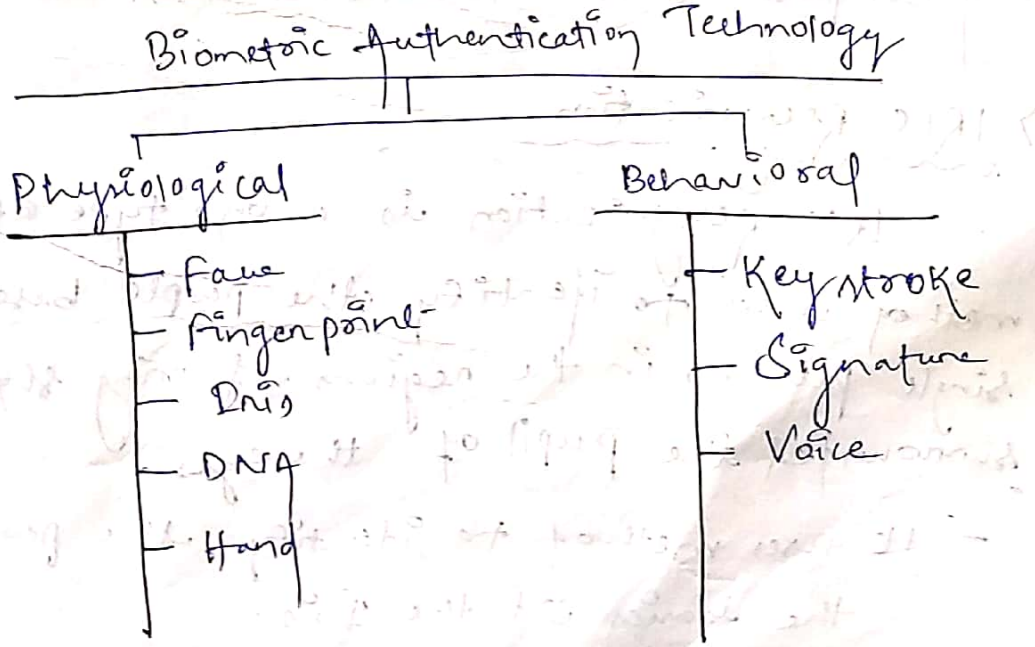
Step-2



6.5 Biometric Authentication

- Biometric authentication is a security process that relies on the unique biological characteristics of an individual to verify that he is, who is say he is?
- Biometric authentication systems compare a biometric data capture to stored confirmed authentic data in a database.
- If both samples of the biometric data match then authentication is confirm.
- Typically biometric authentication is used to manage access to physical & digital resources such as building and computing device.

Types of Biometric Authentication Technology



PHYSIOLOGICAL

> Face Recognization –

Face Recognization system is one type of Biometric computer application which can identify or verify a person from digital image by comparing and analysing patterns.

> Fingerprint Recognization

Fingerprint includes taking a fingerprint image of a person and records its features like Arches, Whorls, Loops along with outlines of edges.

> Hand Recognization

Hand Recognization is a Biometric that identify users by shape of their hands. It measure a user hand along many dimension and compare those measurements store in file.

> IRIS Recognization

- IRIS recognization is a one type of Biometric method used to identify the people based on single patterns in the regions of ring shape surrounded the pupil of the eyes.
- It uses method to identify the people on the basics of the Iris.

> DNA Biometric Recognization

- DNA is the one of the most commonly used Biometric technology around the world.
- DNA is very similar to the fingerprint-biometric because is can be also found anywhere. A fingerprint can be found anywhere is a person has touched something. DNA can be easily found. If you see blood, Urine or any other liquid that has come from a human.
- One more cool thing about DNA is the speed of it this means that the result of a DNA test will be available as little as 90min.

BEHAVIORAL

> Key Stroke