* Introduction to Security Attack :-

→ Attacks are defined as passive and Active.

*** Passive Attack :-**

* Doesn't attempt to perform any modification of the data.

* passive Attack classifications -

(code Lang) 1. Release of Message content
(clues) 2. Traffic Analysis

*** Active Attack :-**

→ Attempt to Modify the data

→ Active Attack classifications -

Attacks in the Form of
1. Masquerade (unauthorized Entity)
2. Modification (Sequence of data)
3. Fabrication (Many login request)

* Threads :- potential for violation of security.

* Risk :- potential for loss or destruction of assets of data.

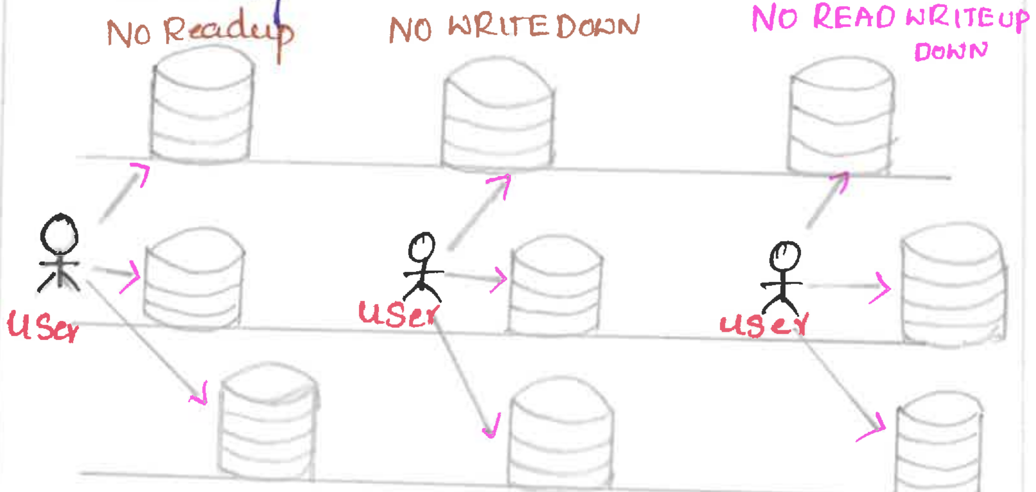
* Security goals :-
1. confidentiality
2. Integrity
3. Availability

Three pillars of Network Security

* Bella - padula Model :-

→ Model was invented by scientists David Elliot Bell and Leonard . J . La padula.

→ used to Maintain the confidentiality of security.



Simple Confidentiality Rule (READ ONLY)

(WRITE ONLY) S TAR confidentiality rule

(READ AND WRITE) Strong star confidentiality rule

* Classical Encryption Techniques :-

→ Substitution Technique :-

1. caesar cipher
2. Monoalphabetic
3. polyalphabetic
4. Hill cipher
5. play Fair

1. Caesar cipher - used for very short communication.

[Substitution table]

A	B	C	D	E	F	G	H	I	J	K	L	M	N	....	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	....	25	26

Key - $1 \le K \le 26$, 'K' value must be between 1 to 26.

* Formula for Encryption - $C = (P+K) \bmod 26$

Formula for Decryption - $P = (C-K) \bmod 26$

Example : P.T = HELLO , K = 4

C.T = (8+4) mod 26
= 12 mod 26

$\boxed{C.T = 12}$ $\boxed{C.T = L}$

P.T = (12-4) mod 26
= 8 mod 26

$\boxed{P.T = 8}$ $\boxed{P.T = H}$

2. Monoalphabetic cipher :- In order to Enhance the security than caesar cipher.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	....	Y	Z
E	I	F	J	B	K	P	M	G	N	Q	A	L	H	D	C		T	V

[Substitution Table]

Example : P.T = HELLO
C.T = MBAAD

3. polyalphabetic cipher / (vigenere cipher)

→ Vigenere tabular method also called vigenere table

→ It is good Encryption technique

For Encryption : $C_i = P_i + K \bmod 26$ (To get cipher Text)

For Decryption : $P_i = C_i - K \bmod 26$ (To get plain Text)

Example : P.T = HELLO , key = APPLE

$C_i = (4+15) \bmod 26$
$= 19 \bmod 26$

$\boxed{C_i = 19}$ / T

$P_i = (19-15) \bmod 26$
$= 4 \bmod 26$

$\boxed{P_i = 4}$ / E

4. HILL cipher :- First polygraphic cipher

→ Here, we are using 2x2 matrix for the key.

For Encryption - $C.T = KP \bmod 26$

For Decryption - $P.T = K^{-1}C \bmod 26$

K^{-1} Formula => $K = \frac{1}{|K|} adj K$

5. play Fair cipher :- We want to consider key in 5x5 matrix.

Rule 1 : Divide a plain text into pair of letters.

Rule 2 : use dummy letters for repeated letters.

Rule 3 : Replace with right most letter if pair of letters in same row.

Example :-

P.T = HELLO

key = NETWORK

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

Transposition Technique :-

→ No replacement and substitution.
→ Rearranging the order of bits
→ Involves two techniques
* Rail fence technique
* columnar Transposition Technique

*** Railfence Technique :-** plaintext is written as a sequence of diagonal.

Example : P.T : WELCOME TO MY SESSION

W L O E O Y E S O
E C M T M S S I N

C.T = WLOEOYESO|ECMTMSSIN

→ In order to convert cipher Text to plain text.

W L O E O Y E S O
E C M T M S S I N

P.T = WELCOME TO MY SESSION

*** columnar Transposition Technique :-**

→ The message is written out in rows of fixed length.
→ Read out again by column by column.

Example : P.T = WE ARE DISCOVERED FILE AT ONCE

KEY : ZEBRAS
6 3 2 4 1 5

→ Here key size is 6.
→ 6x6 column & row.

6	3	2	4	1	5
W	E	A	R	E	D
I	S	C	O	V	E
R	E	D	F	I	L
E	A	T	O	N	C
E	Q	K	J	Z	U

Dummy letters

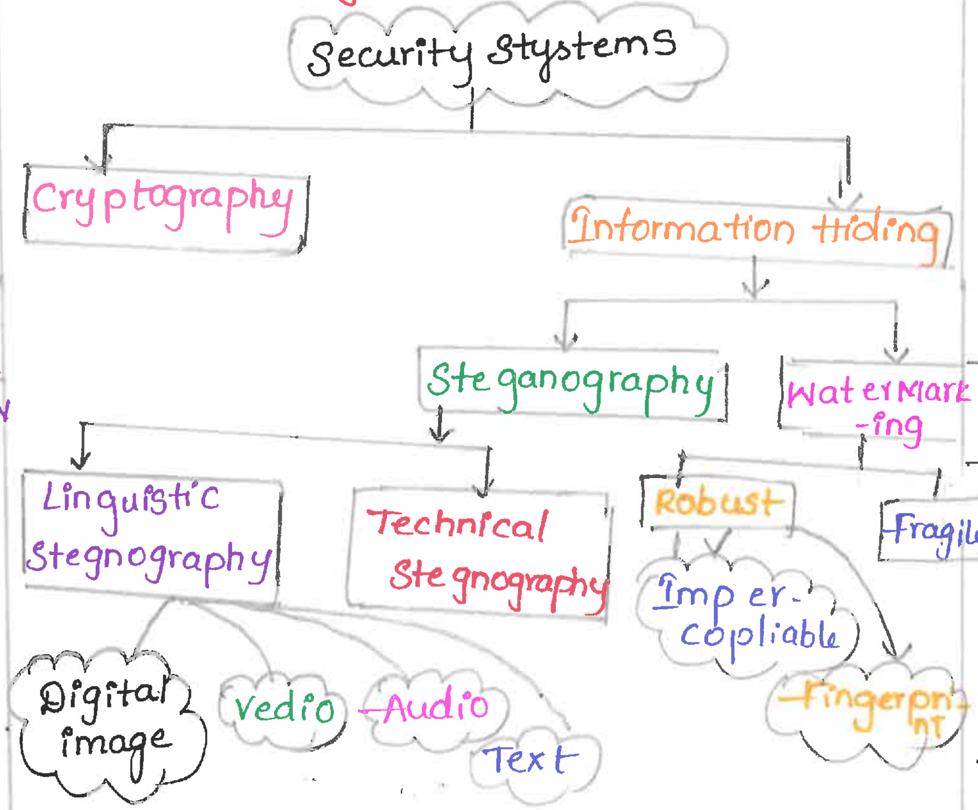
CT = EVINZ ACDTK ESEAQ ROFOJ DELCU WIREE
(1) (2) (3) (4) (5) (6)

Decryption :

6	3	2	4	1	5
W	E	A	R	E	D
I	S	C	O	V	E
R	E	D	F	I	L
E	A	T	O	N	C
E	Q	K	J	Z	U

→ Fill the cipher Text in ascending order in column.
→ Now read the content row by row
→ P.T = WE ARE DISCOVERED FILE AT ONCE

*Steganography :-



Difference btwn steganography & cryptography.

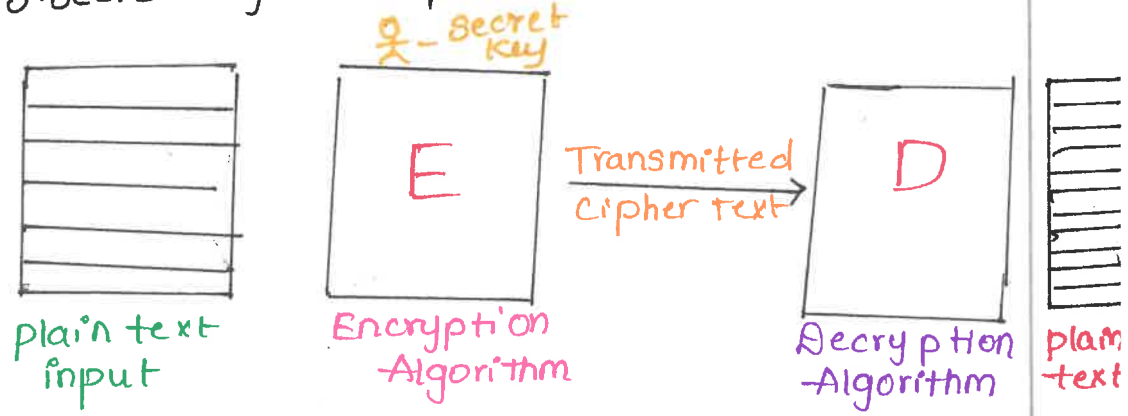
Criteria	Steganography	cryptography
Hiding info	Yes	NO
Carrier	All digital media	Plaintext / image
Additional carrier	Required	Not required
Hidden message	Imperceptible	Detection of message is possible

* Conventional cryptosystem :-

→ Symmetric key Cryptogsystem —also called as→ Secret key
→ Assymmetric key cryptosystem —also called as→ pubic & private key

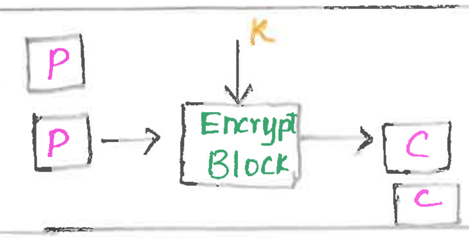
*** conventional Encryption Ingredients :-**

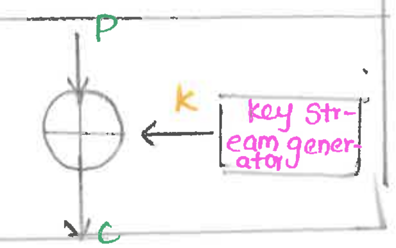
1. plaintext 2. Encryption algorithm
3. Secret key 4. Cipher text 5. Decryption Algo



*** Based on Type of processing Data :-**

Block cipher	Stream cipher
→ Convert plain text into cipher by taking plain text as block at a time	— converts the plain text into cipher text key taking byte of plain text as a time.
→ Reverse Encrypted text is hard.	→ Reverse Encrypted text is Easy.
→ Slow	→ Fast
→ Works on transposition technique	→ works on Substitution Technique.





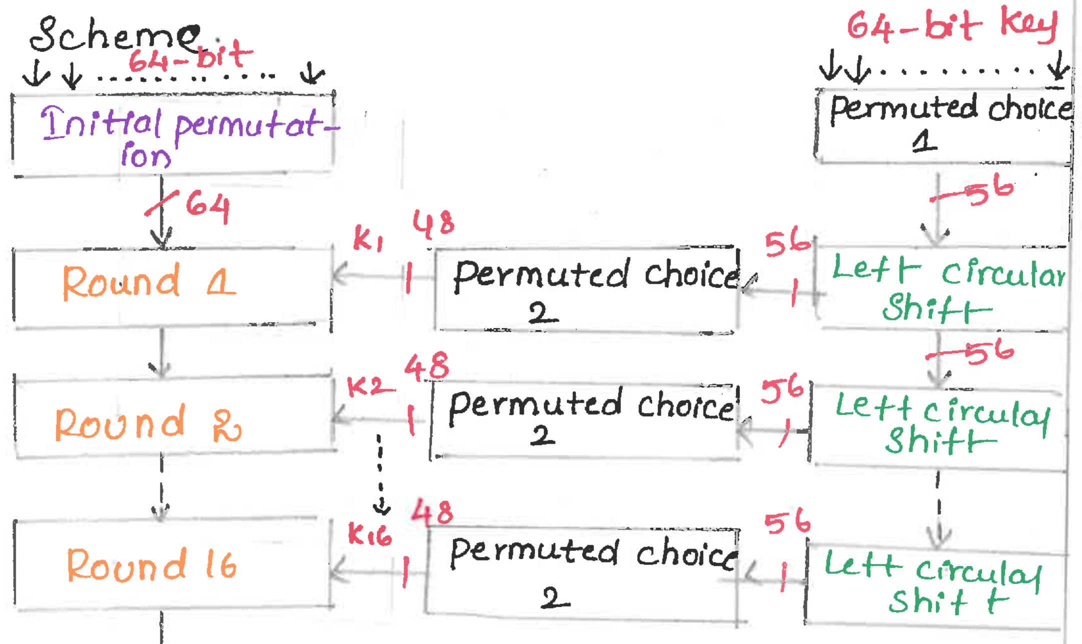
* Symmetric key cryptosystem :-

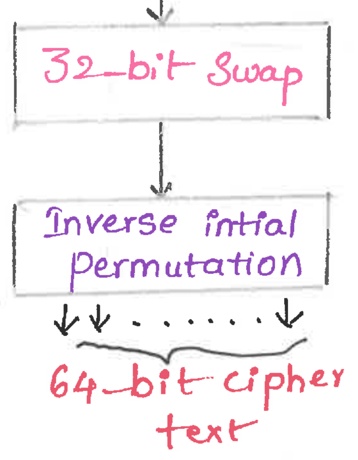
1. DES (Data Encryption Standard)   2. 3-DES
3. Blow Fish   4. RC5 (Rivert cipher)

1. DES (Data Encryption Standard) :-

→ It Follows Feistel Structure.
→ Block size 64-bit & produce 64 bit C.T
→ Block cipher and symmetric key encryption

Scheme



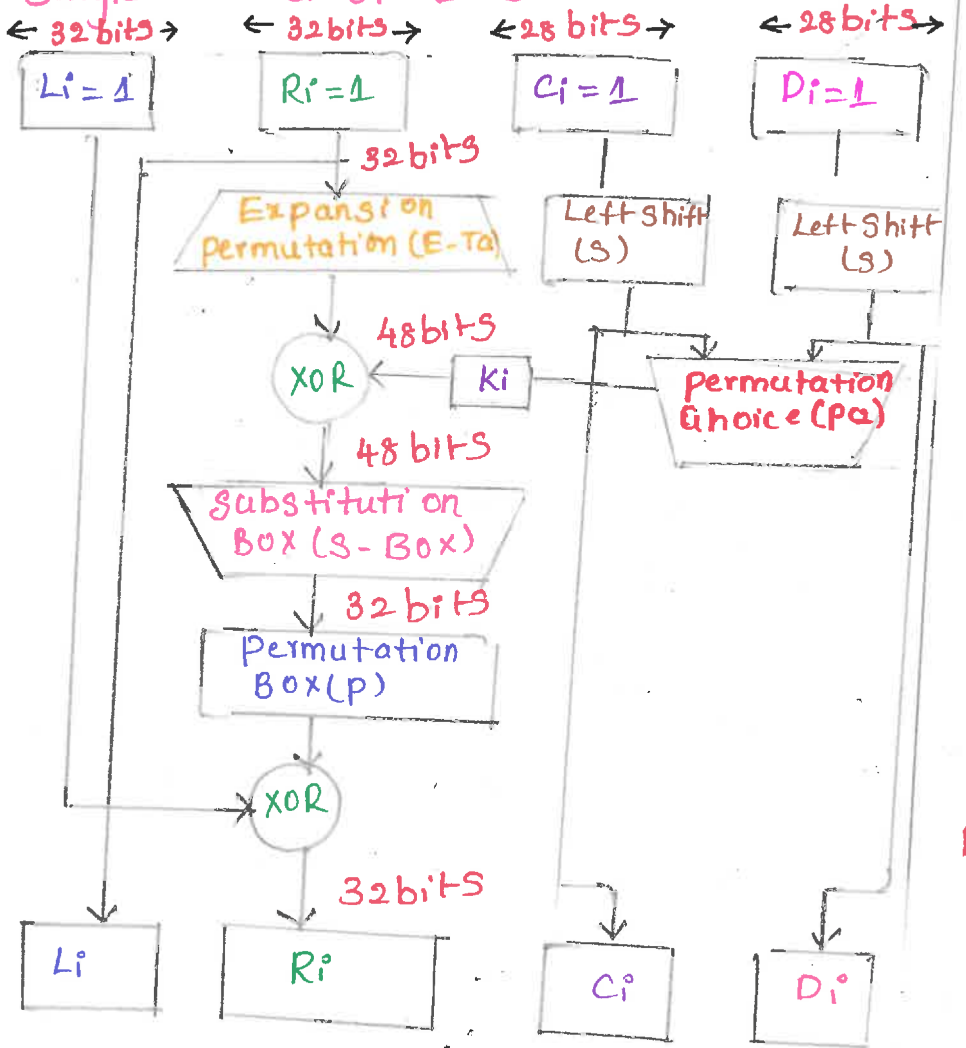


→ same Algorithm and keys are used for Encryption & decryption.
→ 8 bits are used solley for parity check (Error).
→ After discard 8 bits Effective key size is 56-bit

→ DES consists of 16 rounds.
→ Each round performs Substitution and Transposition → A B C → B C A

Substitution: A → x, B → y, C → z

Single Round of DES :-



$L_i = R_{i-1}$

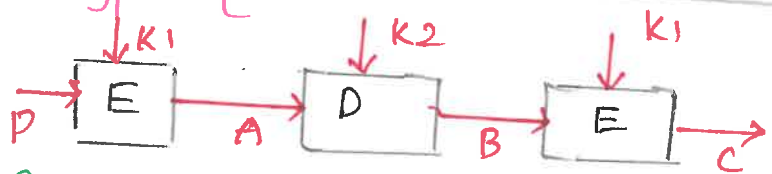
$R_i = L_{i-1} + f(R_{i-1}, K_i)$

Triple DES (3-DES) :-

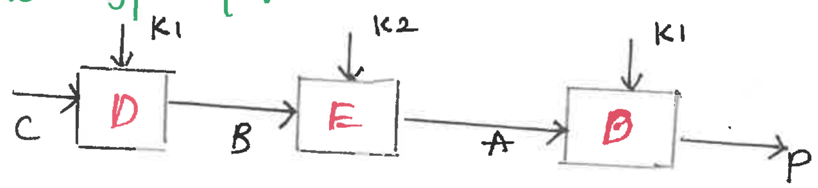
$C = E(K_1, D(K_2, E(K_1 P)))$

Triple DES as an Encrypt – Decrypt – Encrypt process

Encryption –

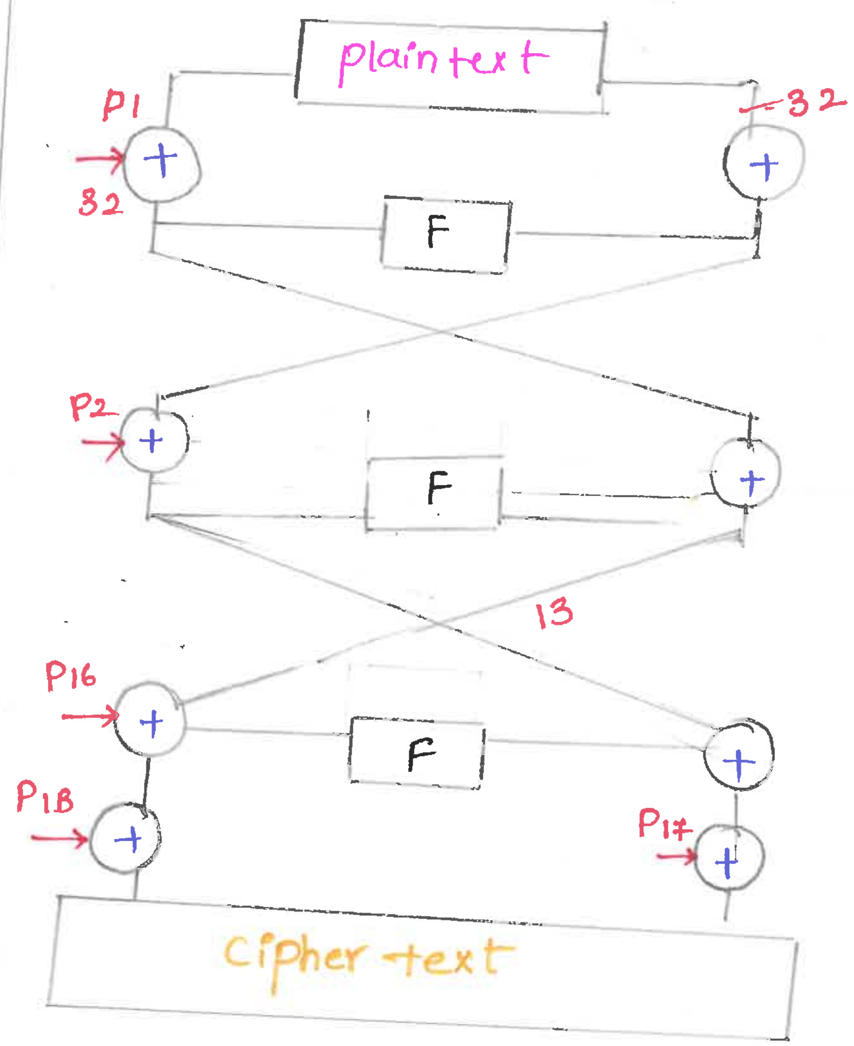


Decryption :-

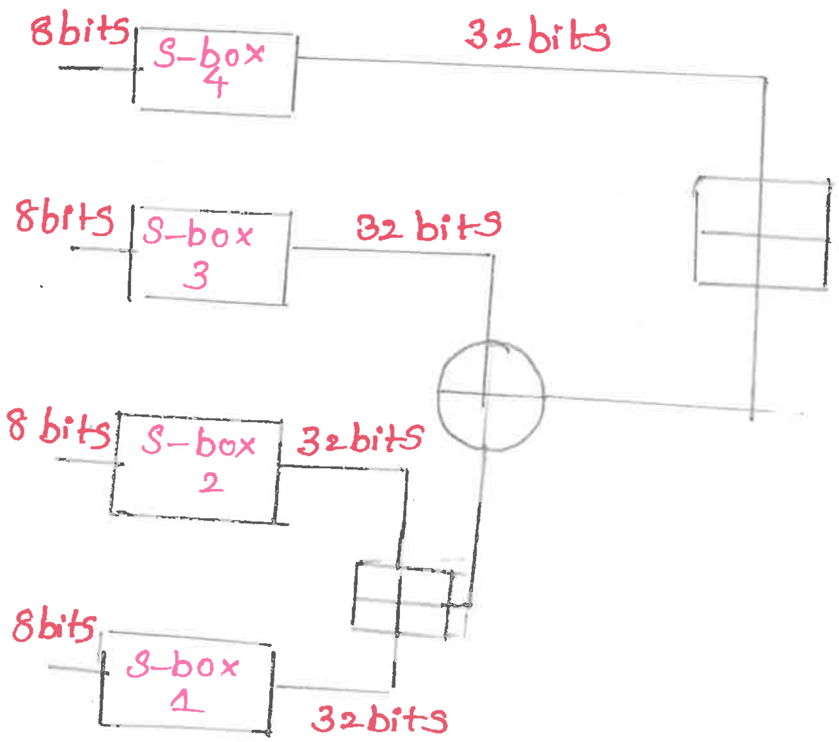


→ key length : 56×3 = 168 bits

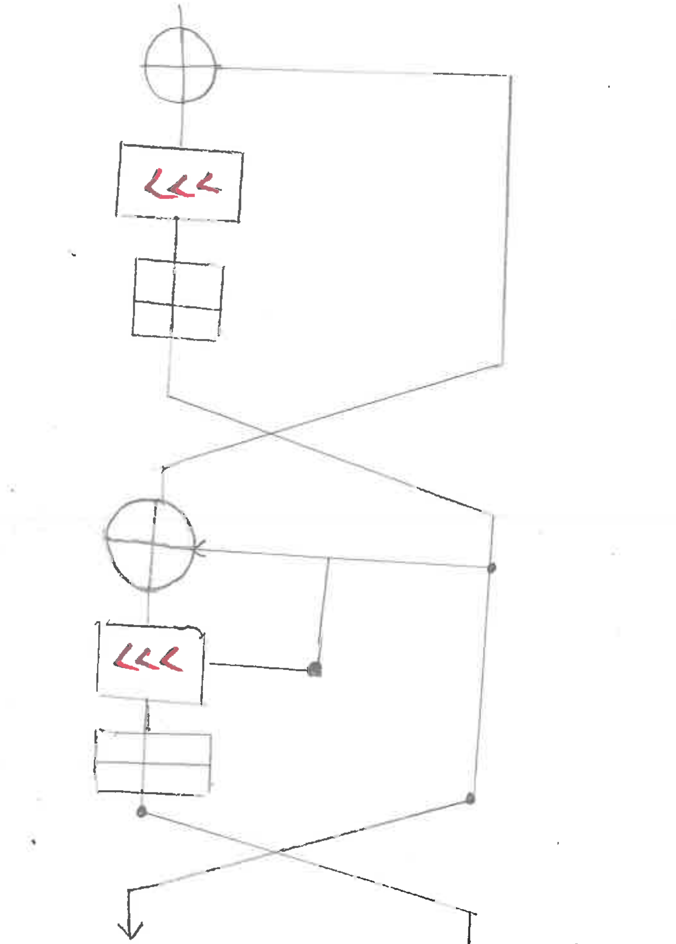
Blow Fish :-



Function F :-



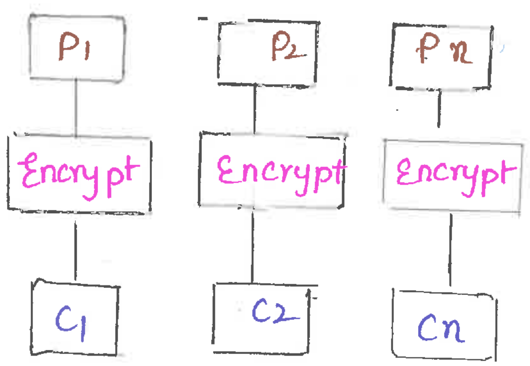
RC5 Single Round of RC5:-



→ Black cipher with variable block size.
→ i/p random key is expanded to 2r+2 word size 32 bit

* Block cipher Mode of operation

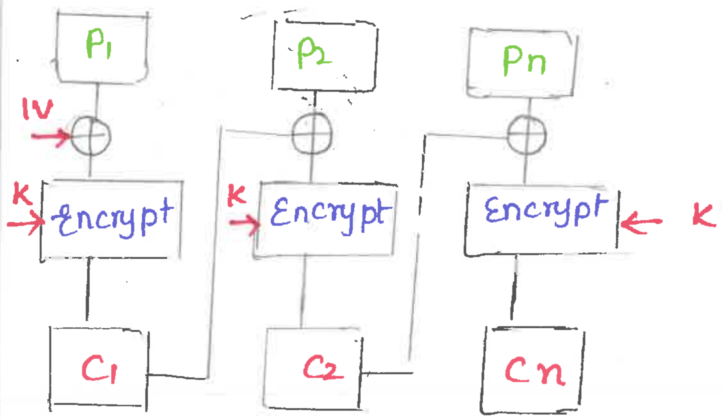
→ Electronic code Book (ECB)-



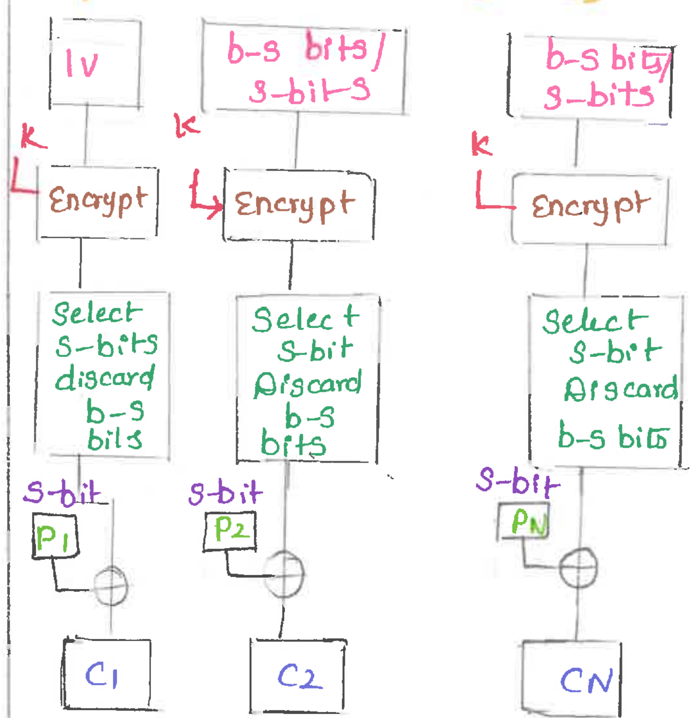
Cipher Block chaining (CBC):-

$C_i = E(K, [P_i, (i-1)])$

$P_i = D(K, C_i) \oplus C_{i-1}$



Cipher Feedback (CFB)



Encryption:-

$O_i = E(K, x_i)$

$C_i = P_i \oplus MSBs(O_i)$

$x_{i-1} = LSB_{b-s}(x_i) \| C_i$

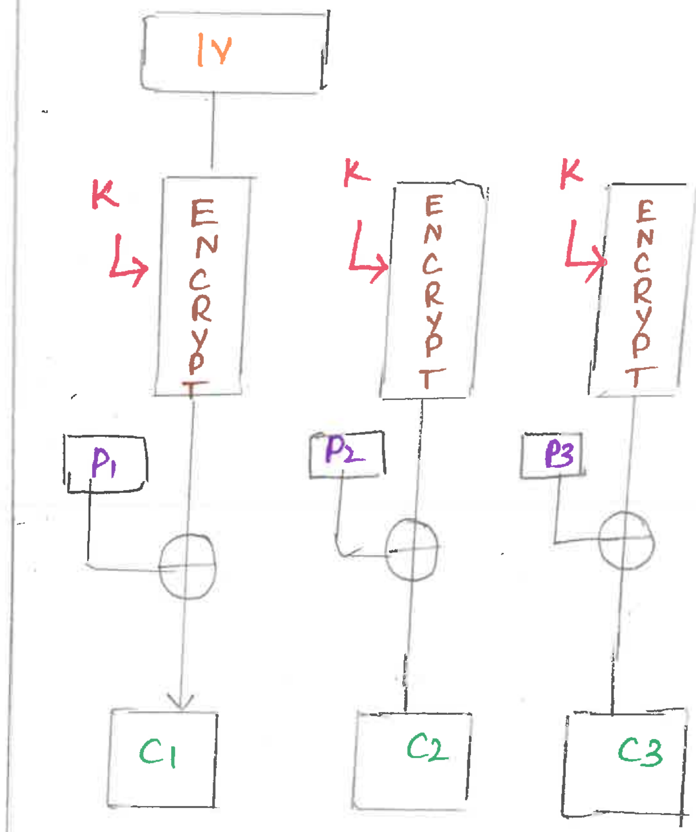
Decryption:-

$O_i = E(K, x_i)$

$P_i = C_i \oplus MSBs(O_i)$

$x_{i+1} = LSB_{b-s}(x_i) \| C_i$

Output Feedback (OFB)



→ $O_i = E(K, x_i)$

→ $C_i = P_i \oplus O_i$

→ $x_{i+1} = O_i$

→ $C_N = P_N \oplus MSBs(O_N)$

Counter Mode :-

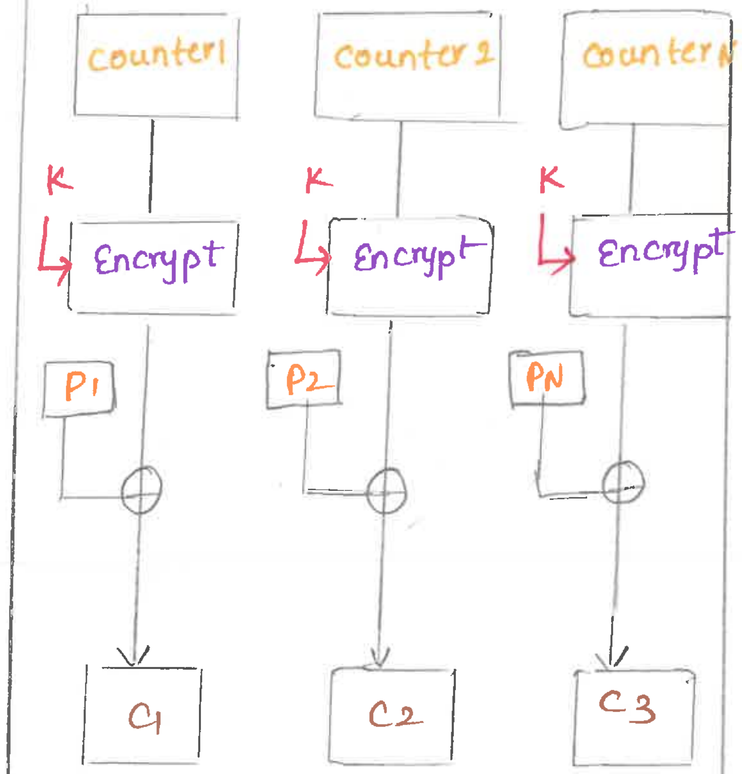
→ $O_i = E(K, x_i)$

→ $C_i = P_i \oplus O_i$

→ $x_{i+1} = x_i + 1$

→ $C_N = P_N \oplus MSBs(O_N)$

CTR Mode is independent of feedback use so parallel implementation is possible.



→ consider counter value which is the length = P.T

→ XOR counter value and plain Text.

→ Increment counter value in second round.

→ Here No decryption process.

→ only Encryption Algorithm

Counter Value 1

↓

Encrypt + key

↓

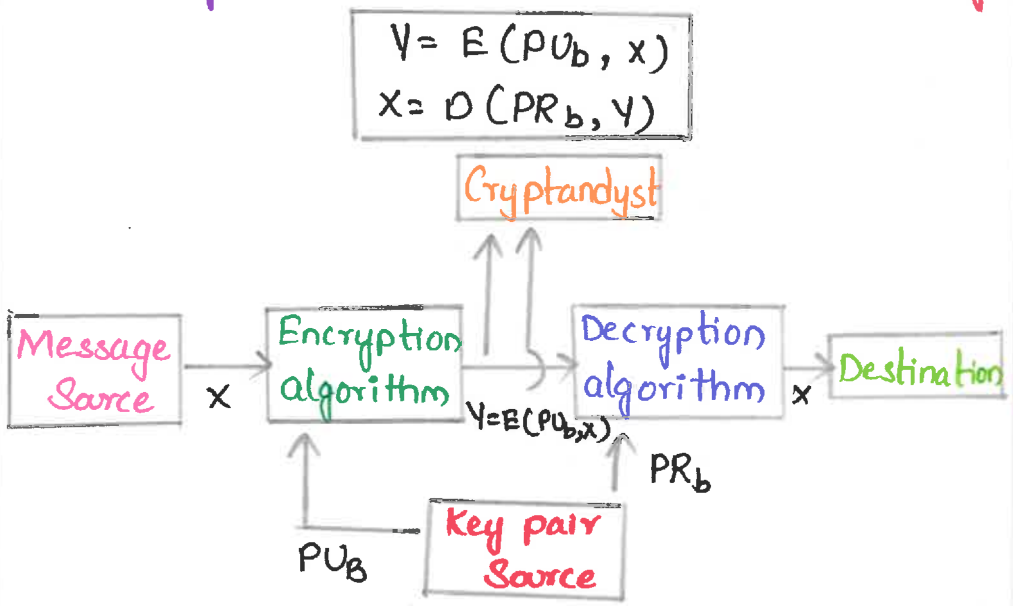
XOR (Pi)

↓

C2

Public Key Cryptosystems

* Two different keys are there
* One key for encryption → PU [Public key]
* One key for decryption → PR [Private key]



Classification :-

⇒ Encryption / Decryption

plain text can be encrypted using PU_B

Cipher text can be decrypted using PR_b

⇒ Digital Signature

- It is cryptographic value from data.
- Secret key known only by the signer.

⇒ Key exchange

Alice Calculates a public key $Y_A = \alpha^{X_A} \bmod q$

Bob calculates a public key $Y_B = \alpha^{X_B} \bmod q$

Y_A Y_B

Alice receives Bob's public key Y_B in plaintext

Bob receives Alice's public key Y_A in P.T

RSA (Rivest, Shamir, Adleman)

- Block cipher, plaintext and cipher text
- These 3 are integers between 0 and n
- Size for n ⟶ 1024 bits (or) 309 decimal digits

Requirements :-

- Relatively easy to calculate $M^e \bmod n$ and $c^d \bmod n$ for all values of $M < n$
- Infeasible to determine d from e & n.
- Infeasible to find prime factors of n.

Steps :-

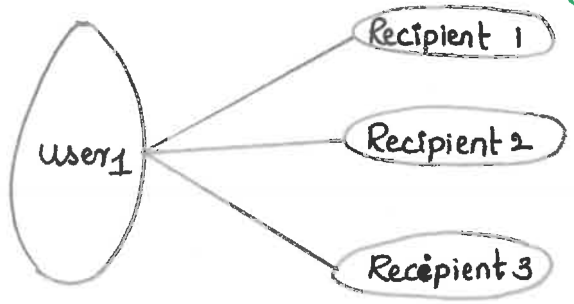
* Select secret primers p and q.
* Calculate $\boxed{n = pq}$
* Calculate $\boxed{\psi(n) = (p-1)(q-1)}$
* Choose encryption exponential e with $\boxed{\gcd(e, \psi(n)) = 1}$ & $(1 < e < \phi(n))$.
* Compute decryption exponent d with $\boxed{de = (1 \bmod (\psi(n))}$
* Make n and e public, d, p, q secret
* Message M is encrypted using $\boxed{C = M^e \bmod n}$
* Decrypts by computing $\boxed{M = c^d (\bmod n)}$

Distribution of Public key :-

- The public key can be distributed in four ways:

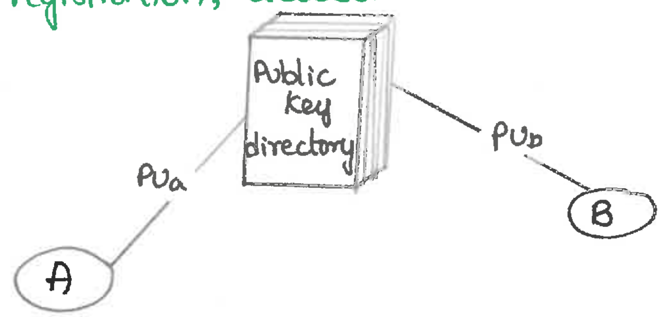
⇒ Public Announcement:

- Public-key is boardcasted to every one.
- Weakness of this method is forgery.



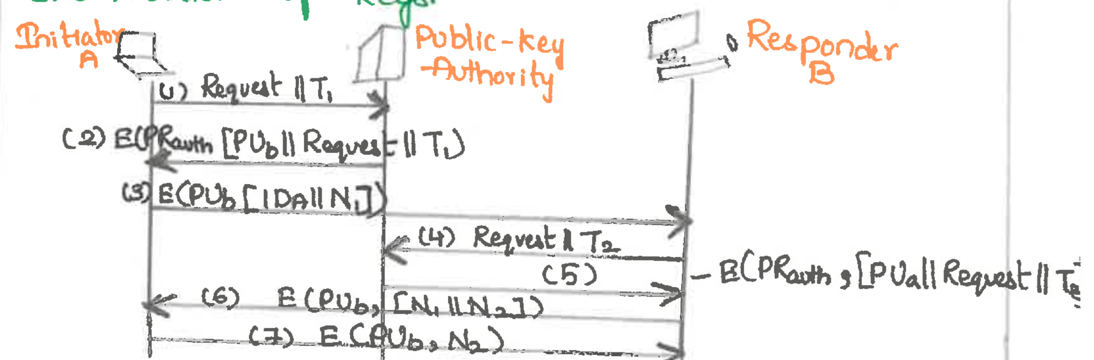
⇒ Publicly Available Directory:

- Public key stored in public directory.
- Directories are trusted here, like participants registration, access.



⇒ Public key Authority :-

- It is similar to directory
- improves security by tightening control for distribution of keys.



⇒ Public Certification :-

- This time authority provides certificate.
- Certificate - Period of validity, rights of use.

Diffie Hellman key exchange.

→ Enables 2 users to securely exchang a key that can be used for subsequent encryption of Messages

→ Fix a prime p, Let α & β → Non zero integers

$$\beta = \alpha_x \pmod{p}$$

Primitive root: It is a primitive root of q, where q → prime. $a^n \bmod q$, where n=1 to q-1,

→ It produce each integer from 1 to q-1 exactly once.

STEPS:

1. Either A (or) B select a large secure Prime Number p and a primitive root α. Both p and α can be Made Public
2. User A chooses a private key X_A with $X_A < P$, Computes public key and sends to user B. $Y_A = \alpha^{x}A \pmod{P}$
3. User B selects a private key X_B with $X_B < P$, Compute public key and sends To user A $Y_B = \alpha^{x}B \pmod{P}$
4. User A receives Public key Y_B and calculate shared secured key K by $K = (Y_B)^{x}A \pmod{P}$
5. User B receives public key Y_A and calculate shared key K by $K = (Y_A)^{x}_{B} \pmod{P}$

Elliptic Curve crytography

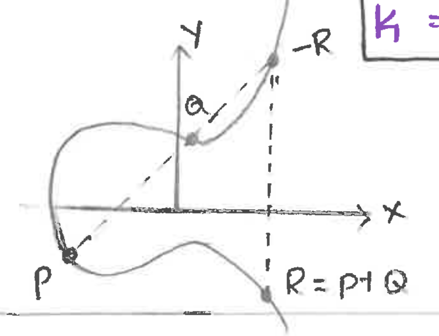
→ Approach to public key cryptography based on algebraic structure of elliptic curves over finite fields.

Equation of elliptic curve :

$$y^2 = x^3 + ax + b$$

ECC Diffie Hellman key exchange:

1. Let $E_q(a,b)$ → elliptic curve with parameters a, b and q, where q is a prime and a be a point on elliptic curve whose order is large value n.
2. User A selects private key (n_A) less than n. A then calculates public key $\boxed{P_A = n_a * G}$
3. User B selects private key (n_B) less than n. B then calculates public key $\boxed{P_B = n_b * G}$
4. User A generates secreat key $\boxed{K = n_A * P_B}$
5. User B generates secret key $\boxed{K = n_B * P_A}$



⟹ $y^2 = x^3 - 3x + 5$

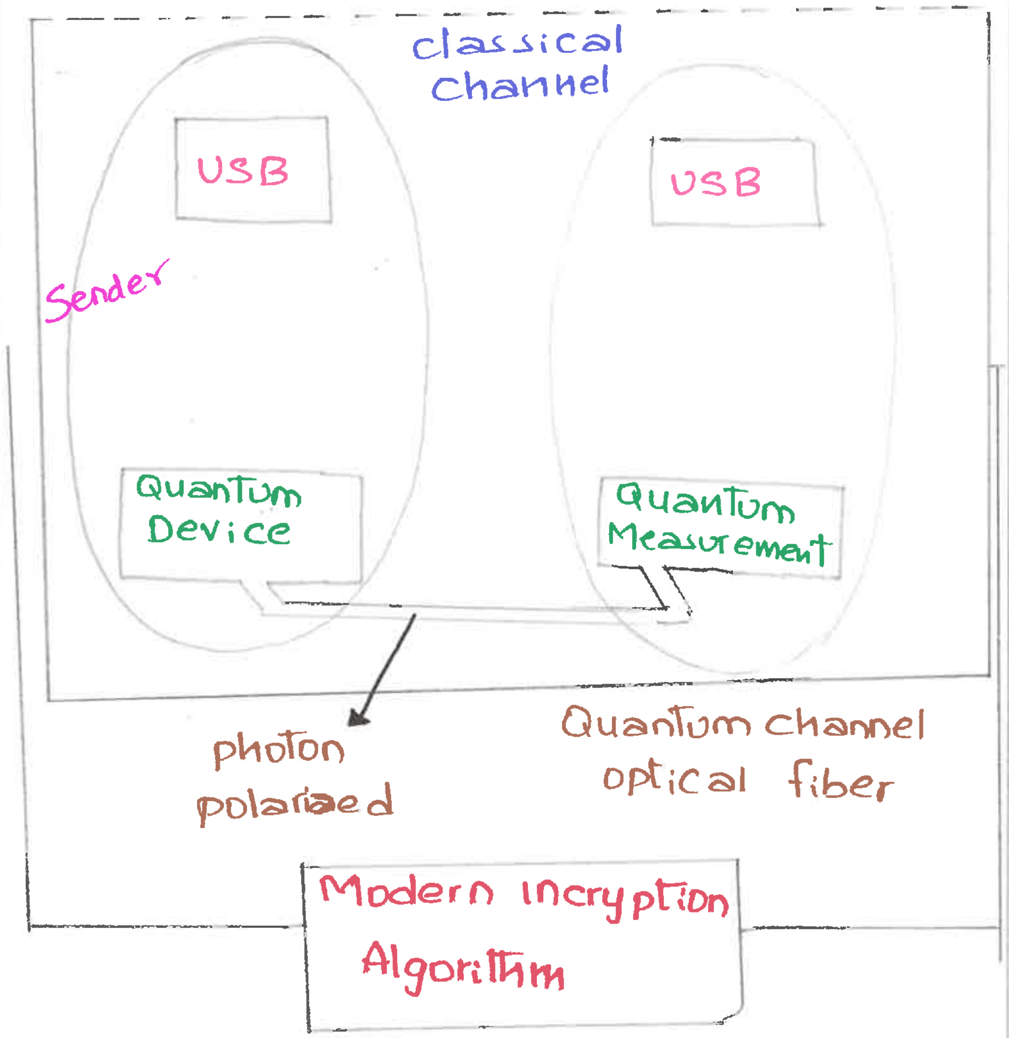
Elliptic Curve Encryption | Decryption

$$C_m = [KG, P_m + K P_B]$$

$$P_m + K P_B - n_B(KG) = P_m + K(n_B G) - n_B(KG) = P_m$$

Quantum Cryptography.

→ uses the principles of Quantum Mechanics to encrypt data and Transmit it in a way that cannot be hacked.



HASH ALGORITHMS AND AUTHENTICATION SCHEMA

Hash Function :-

$h = H(M)$ ∴ $M \rightarrow$ preimage of h

H (cryptographic hash function) → Takes an input message of arbitary Length of produces output of fixed length.

=> output of hash function → Message digest (MD)

=> cryptographic hash function → Needed for security applications.

uses of hash function :-

=> useful in digital signature

=> To check data integrity (message authentication)

=> useful to construct pseudorandom function (PRF) or pseudorandom number generator (PRNG)

Collision :- occurs $m_1 \neq m_2$

$H(m_1) = H(m_2)$

Requirements of hash function (or) properties :-

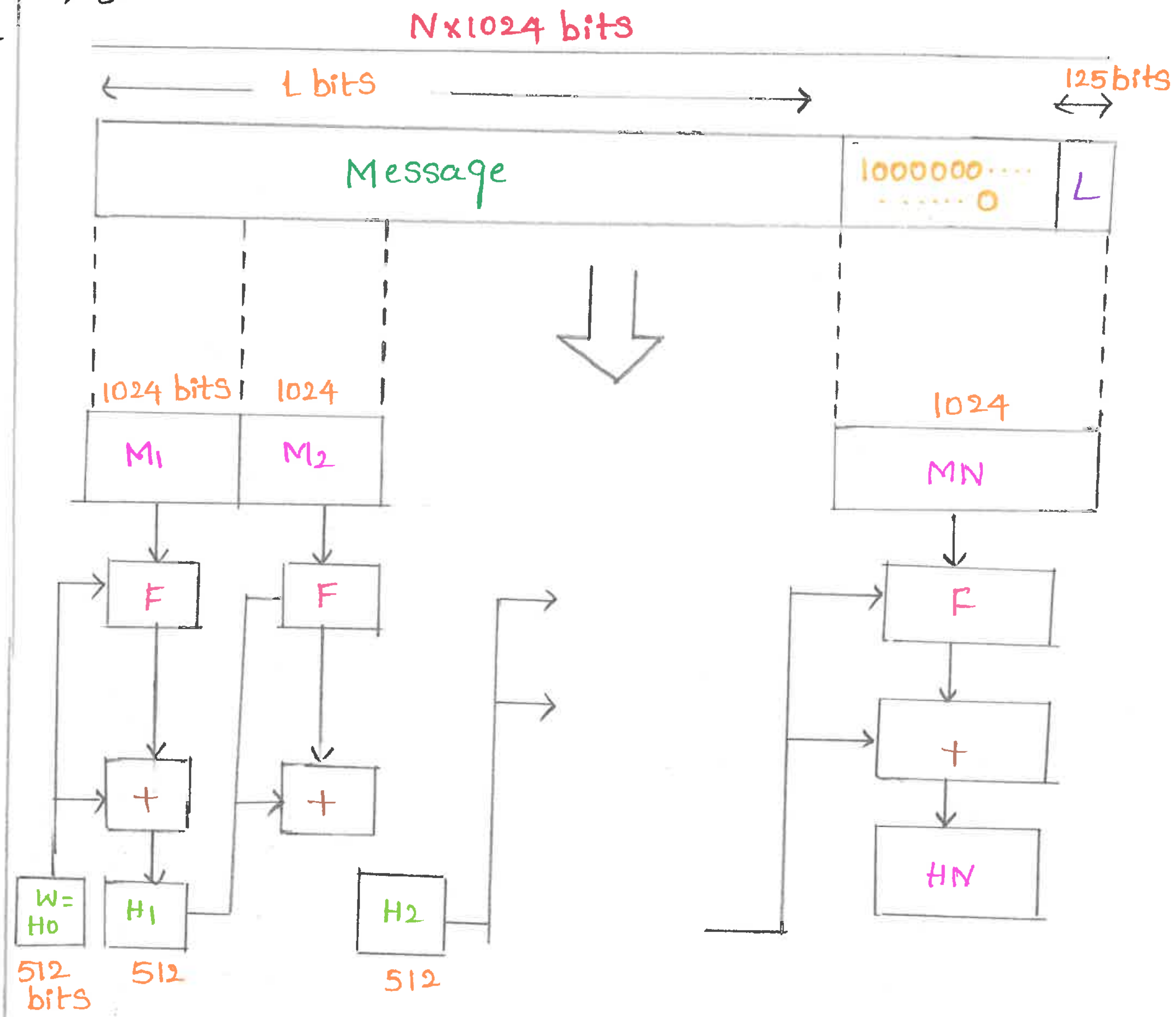
* preimage resistant
* collision resisdant
* Second preimage resistant

Birthday attack :- cryptanalysis techniques that is based on birthday pardox can be used to tint collision for hash function.

SHA (Secure Hash Algorithm) :-

=> produces 160-bit hash

=> SHA-0, SHA-1, SHA-256, SHA-354, SHA-512



=> Algorithm takes an input a message Hash code maximum length of less than 2_{128} bits and produce as output a 512-bit messages.

=> Input is proiened in 1024 bit blocks.

DIGITAL SIGNATURE

Digital signature : Authentication

Mechanism that enables the creator of the message to attach a code that acts as signature.

2 distinct steps : Signing process / Verification process

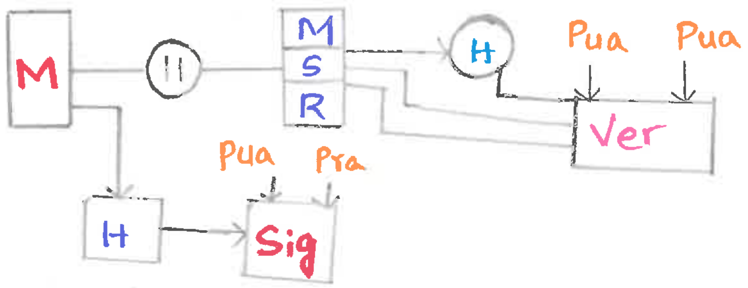
Properties :

→ Must verify Author & date, time of signature

→ Must authentiate the contents at the time of sign

→ Must be verifiable by the 3rd parties to resolve disputes.

DSS [Digital signature standard]



Initialization phase :

1) select a prime q (160 bits), choose prime p that satisfies
2) g be a primitive root mod p and Let $\alpha = g(p-1)/q \pmod p$
3) secret integer a with $a < q-1$ & $B = \alpha a \pmod p$
4) Values (p, q, α, B) Public is a secret

Signing phase

1) choose a secret random integer k with $k < q-1$
2) $r = (\alpha_k \pmod p) \bmod q$
$S = k-1(m+ar) \bmod q$
3) signature (r, S)

Verification phase.

1) $U_1 = S^{-1} m \pmod q$
$U_2 = S^{-1} r \pmod q$
2) $V = \alpha U_1, BU_2 \pmod p$
3) signature is valid if $v = r$

ELGAMAL DIGITAL SIGNATURE

→ Elgamal cryto system is a public key used for encryption & digital signature

→ use of private key for encryption

→ public key for decryption

→ relies on difficulty of computing discrete logrithms.

Initialization phase :

global element are prime number q & α, which is a primitive root of q user a generates Private / public key pair as follows :

1) choose a random integer X_A such that $1 < X_A < q-1$
2) Compute $Y_A \equiv \alpha^{X_A} \bmod q$
3) A's private key is X_A, A's public key is $\{q, \alpha, Y_A\}$

Signing phase.

→ First compute hash $m = H(M)$

1) choose random integer K such that $1 \le K \le q-1$ & $\gcd(K, q-1) = 1$
2) $S_1 \equiv \alpha^K \bmod q$
3) $K-1 \bmod (q-1)$
4) $S_2 \equiv K^{-1}(m - X_A S_1) \bmod q-1$

Signature (S_1, S_2)

Verification process.

$V_1 \equiv \alpha^m \bmod q$

$V_2 = (Y_A)^{S_1} (S_1)^{S_2} \bmod q$

Signature is valid of $V_1 = V_2$

Schnorr Digital signature.

→ based on discrete logarithms

→ Minimizes message dependent amount of computation required to generate a signature.

Initialization phase :

1) choose prime p & q, q is a prime factor of $p-1$
2) choose integer a, $a^q \equiv 1 \bmod p$
3) $0 < s < q$ (user's private key)

Signing process :

1) Choose $0 < r < q$, and calculate $x = a^r \bmod p$
2) $e = 1 + (M/x)$
3) $y = (r + se) \bmod q$
4) signature $= (e, y)$

Verification process :

1) $x' \equiv a^y v^e \bmod p$
2) Verify that $e = 1 + (M/x')$

$x' \equiv a^y v^e$

$x' \equiv a^y a^{-se}$

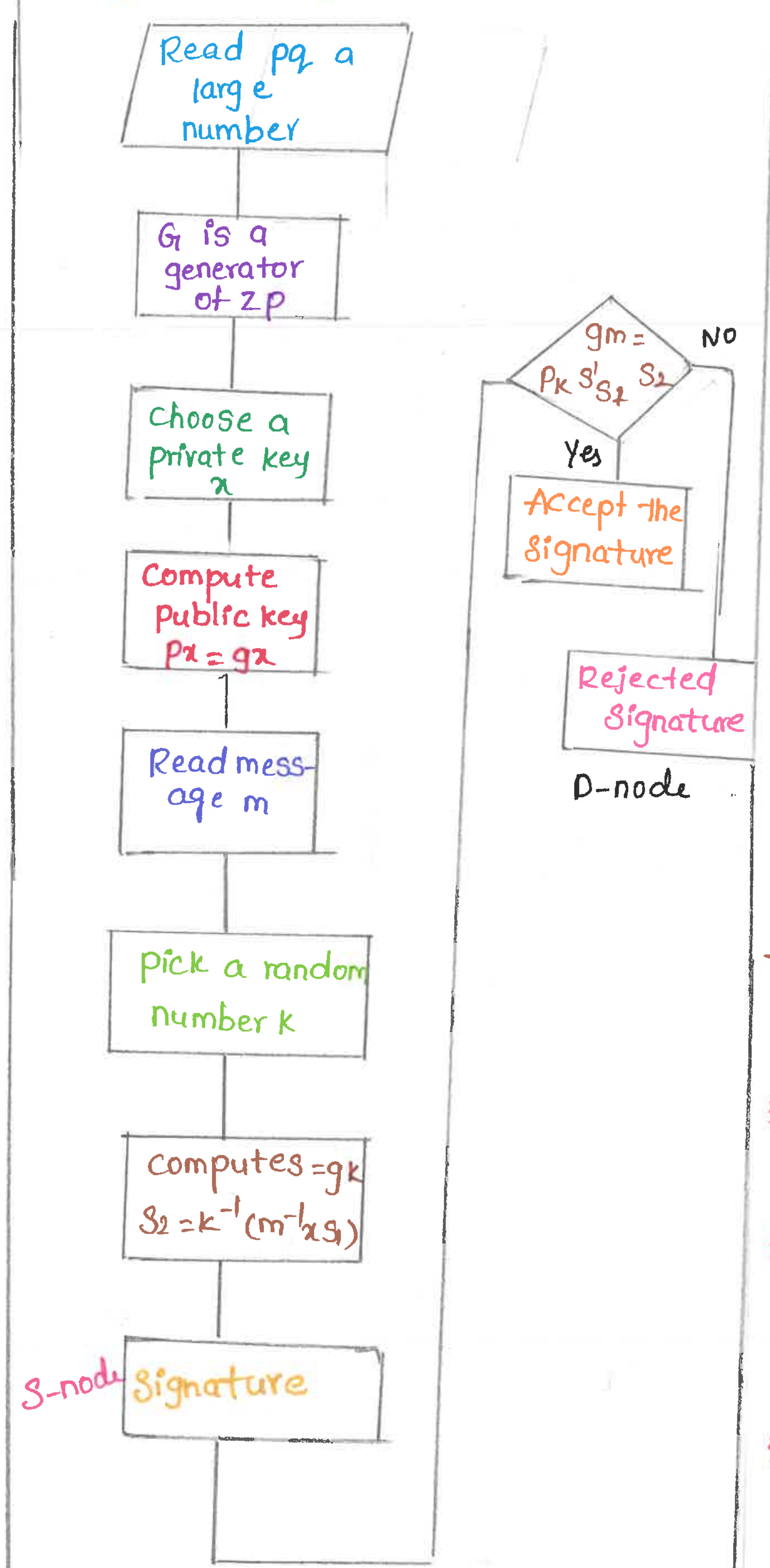
$x' \equiv a^{y-se}$

$x' \equiv a^r$

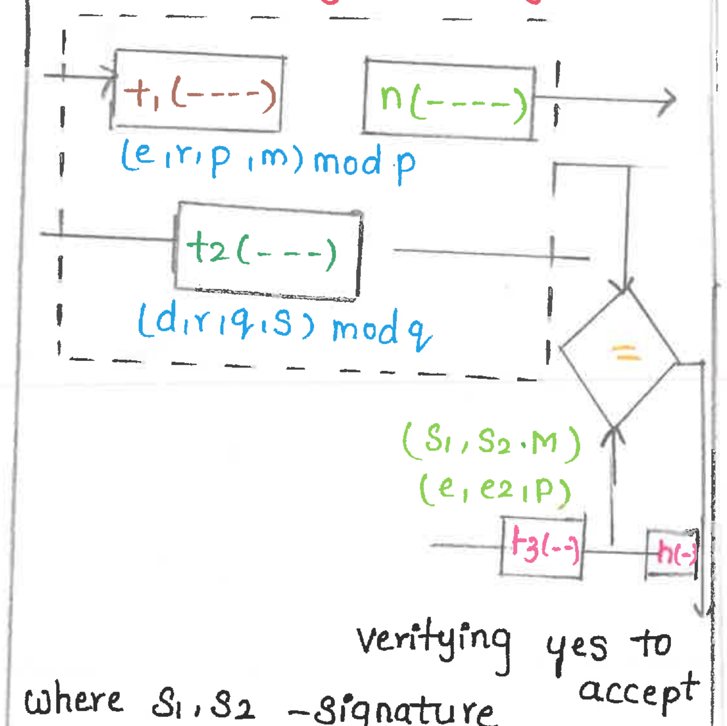
$x' \equiv x$

$\therefore 1 + (M/x) = (M/x')$

Elgamal digital signature :-



Schnorr digital signature :-



where S_1, S_2 - signature

d → Alice's private key

r → Random secret

M → Message

(e_1, e_2, p, q) → Alice's public key

Authentication Service :-

KERBEROS -

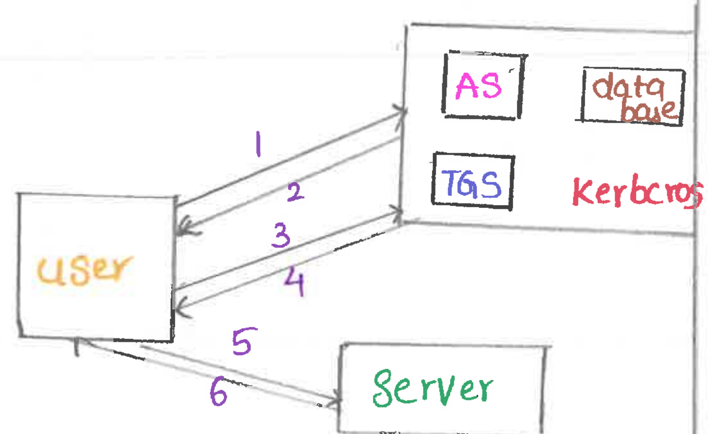
* provides a centralized authentication server.
* whose function into authenticate users to serves and servers to users
* used for client authentication
* RUNS as a third party used server known as key distribution center (KDC)

Main components :-

=> Authentication Server

=> Database

=> Ticket granty server



Kerberos ticket structure :-

Kerberos Version
Server Realm
Server name
Flags
Session key
client Realm
client name
Validity start time
validity end time

X.509

* Defines frame work for authentication services
* Defines authentication protocol.

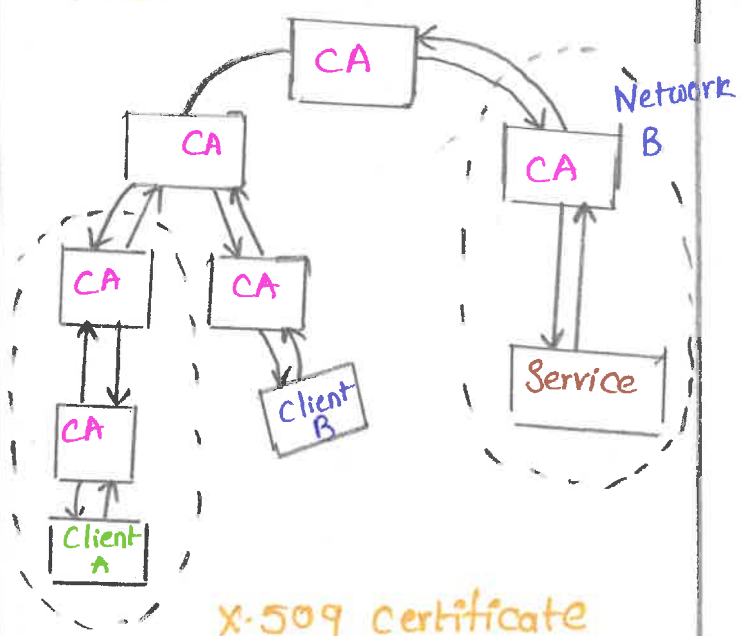
* user public key cryptography & digital signature.

* part of CC & TTX-500 directory services & standards.

* 3 alternate authentication procedures.
  * 1-way
  * 2-way
  * 3-way

  } all uses public key signature

* X.509 Hierarchy of Trust.



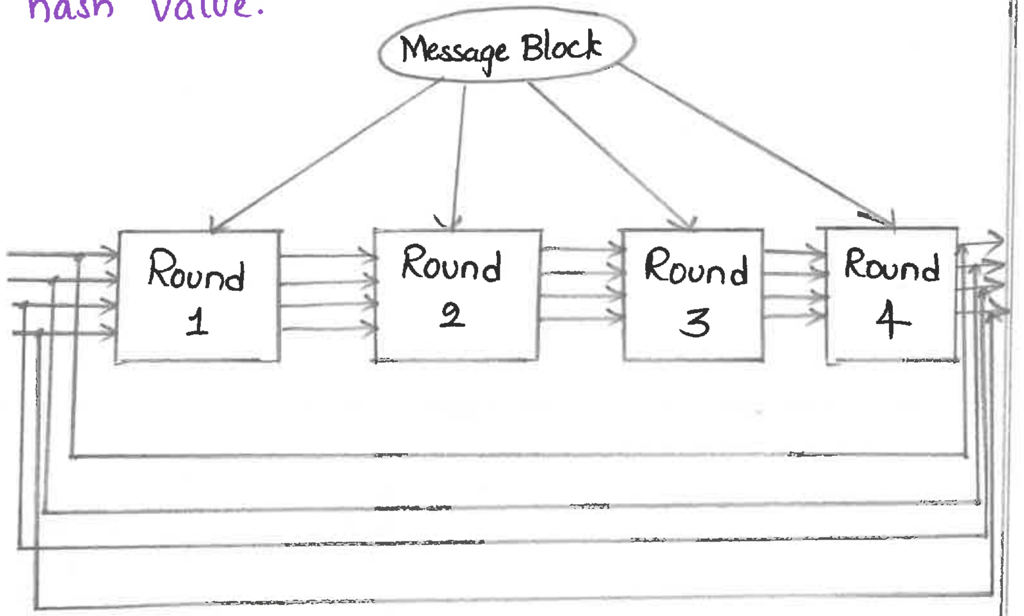
X.509 certificate

Version Number
Signature algorithm
Issue name
Subject name
Subject unique ID
Extensions

MD5 (Message digest)

⇒ Process the input text in 512 bit blocks divided into 16, 32 bit sub blocks.

⇒ The algorithm is set of 4 32 bit blocks which combine to form a single 128-bit hash value.



MD5 Main loop

⇒ Four 32 bit variables called chaining variables are intialised.

A = 01234567

B = 89ABCDEF

C = FEDCBA98

D = 76543210.

⇒ 4 Non linear functions different one is used for each round.

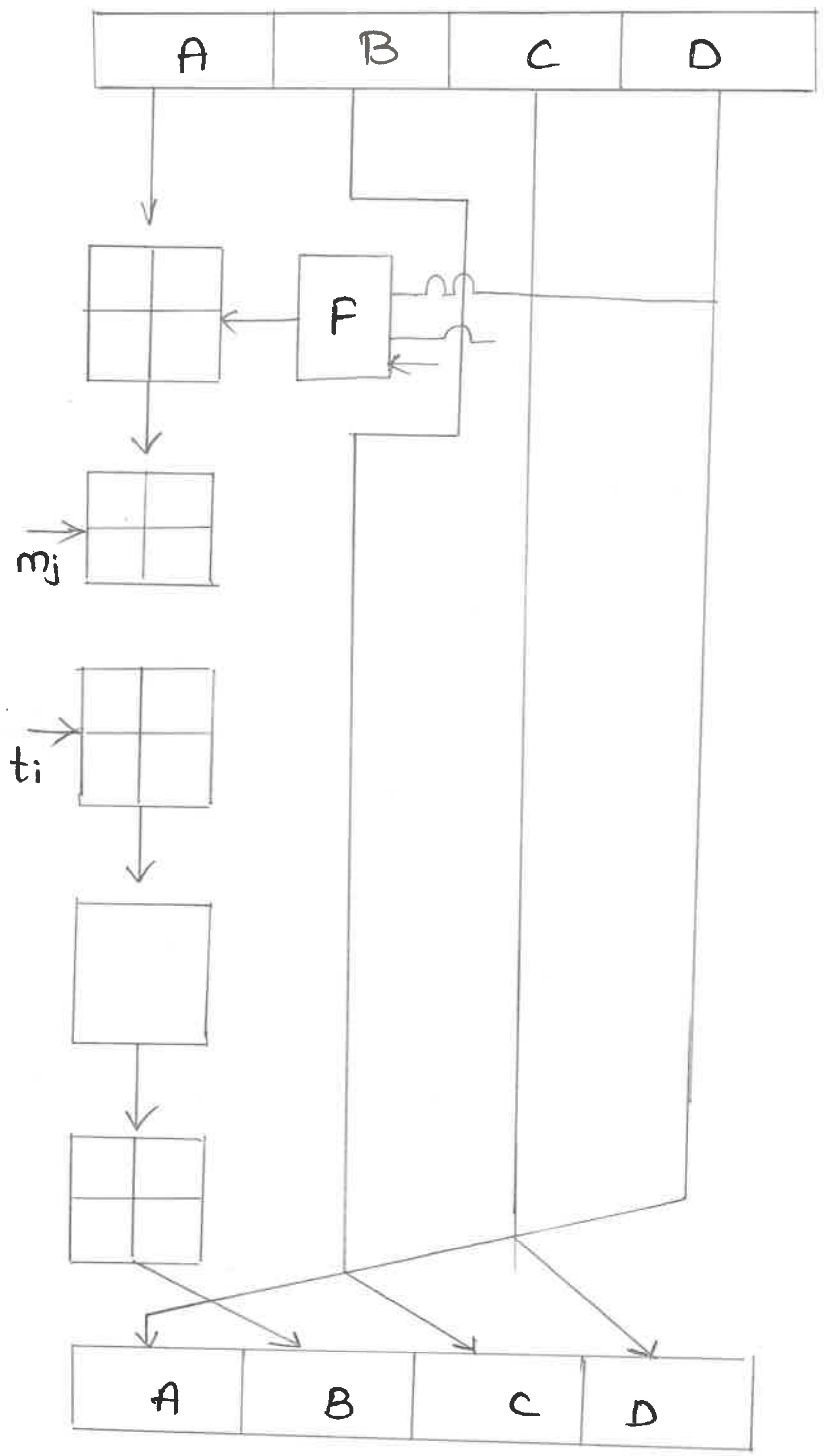
F(B,C,D) = (B∩C) v (¬B∩D)

G(B,C,D) = (B∩D) v (C∩¬D)

H(B,C,D) = B⊕C⊕D

I(B,C,D) = C⊕ (BV¬D)

One MD5 Operation



⇒ SHA-1 ⇒ i/p bits are used more often during the curse of hash function then MD5.

⇒ SHA-1 more secure, Little slower.

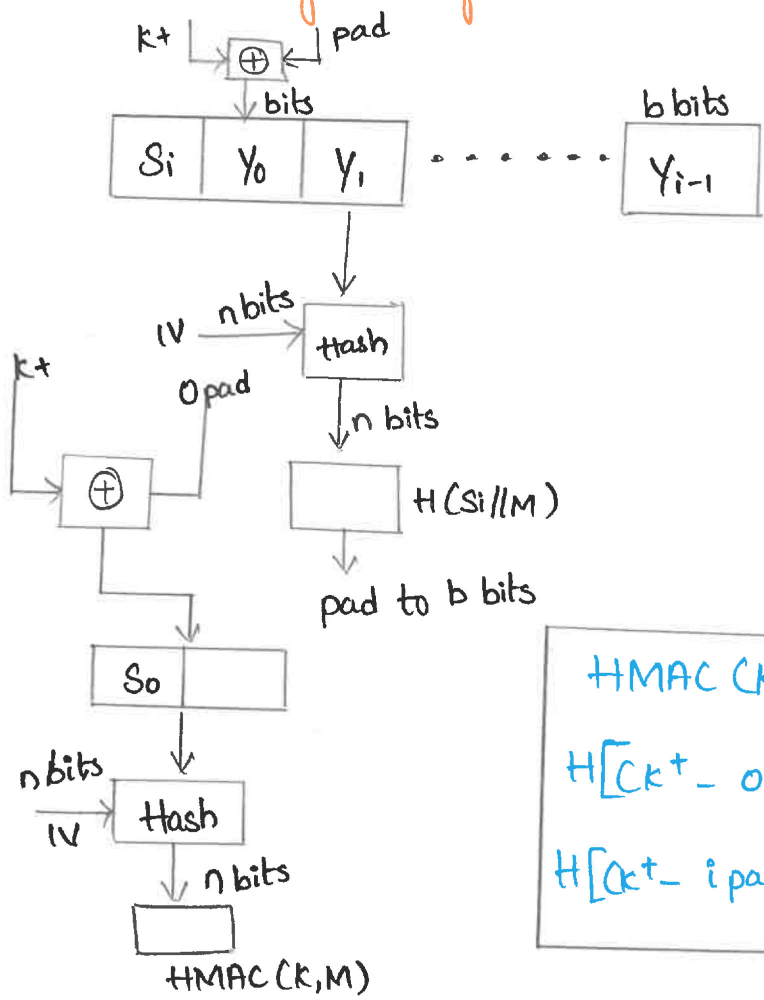
MAC :-

⇒ Message authentication code is a function of the message and a secret key produces fixed - Length value - that serves as authentication Cafor

$\boxed{T = MAC(K,M)}$

HMAC :-

⇒ MAC algorithm generates authenticator or tag using hash function.



HMAC(K,M) =

H[(K+ - opad) ||

H[(K+ - ipad) || M]]

⇒ This structural implementation holds efficiency for Shorter MAC values.

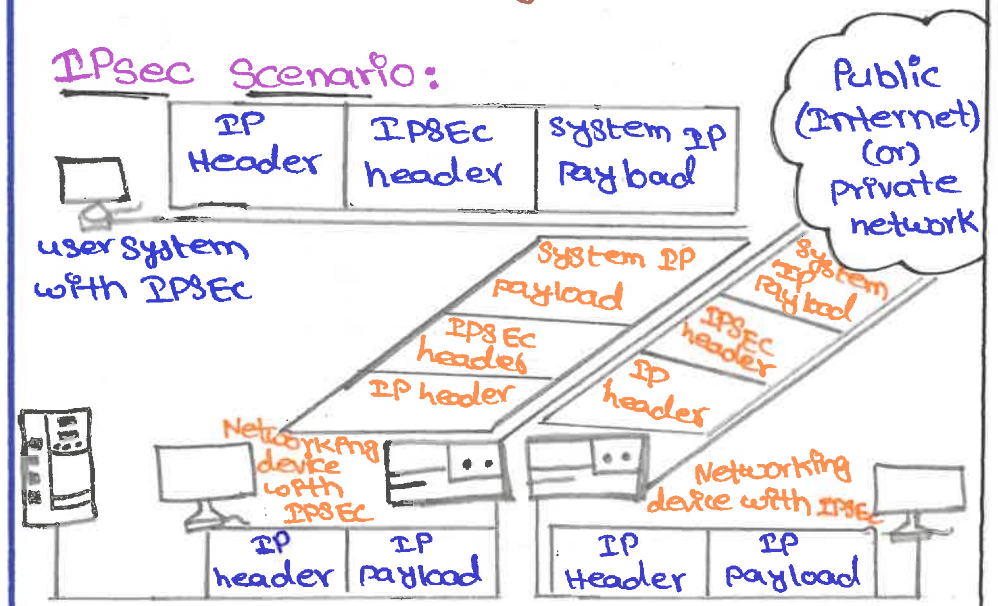
IP Security:

Capability that can be added to IP protocol by means of additional headers.

IPSec Functional areas:

⇒ Authentication
⇒ Confidentiality
⇒ Key management

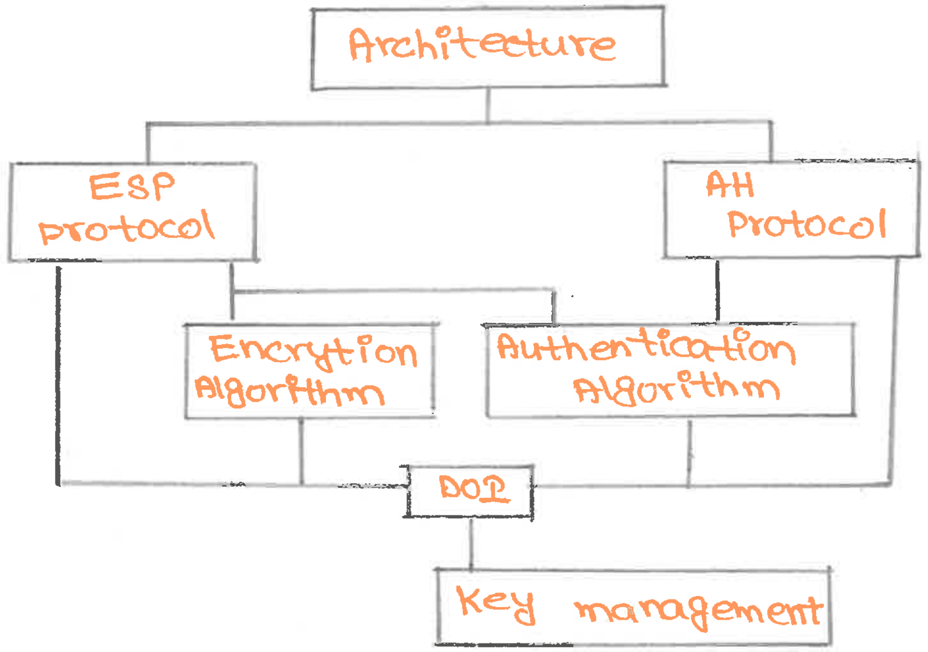
IPSec Scenario:



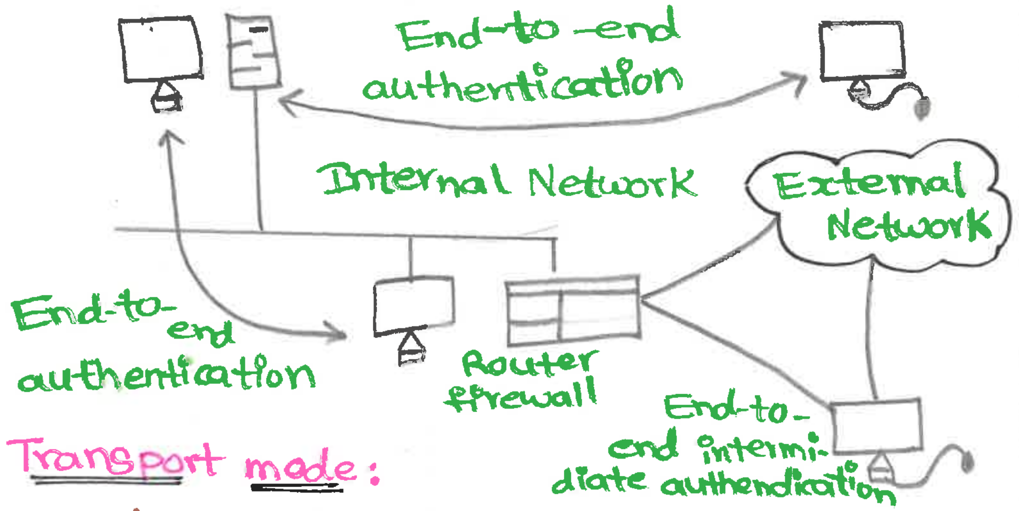
IPSEC SERVICES:

⇒ Access control
⇒ Connectionless Integrity
⇒ Data origin authentication
⇒ Rejection of replayed packets
⇒ Confidentiality
⇒ Limited traffic flow confidentiality.

IPsec overview in document:



Transport and Tunnel Modes:



Transport mode:

⇒ In transport mode AH authentication IP payload & selected portions of IP header & IPv_6 extension headers.

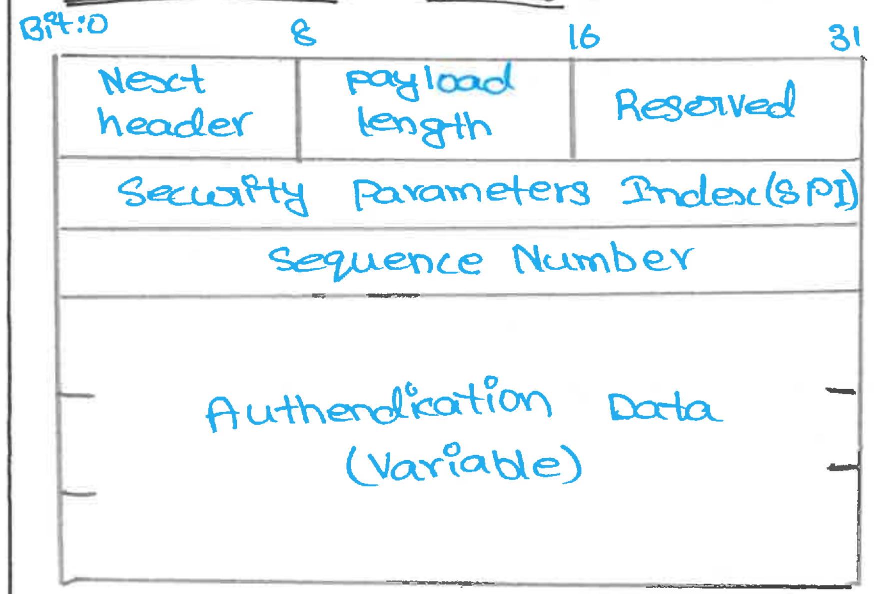
⇒ ESP encrypts IP Payload & and IPv_6 extension headers following the ESP header.

⇒ Good for ESP End to End traffic.

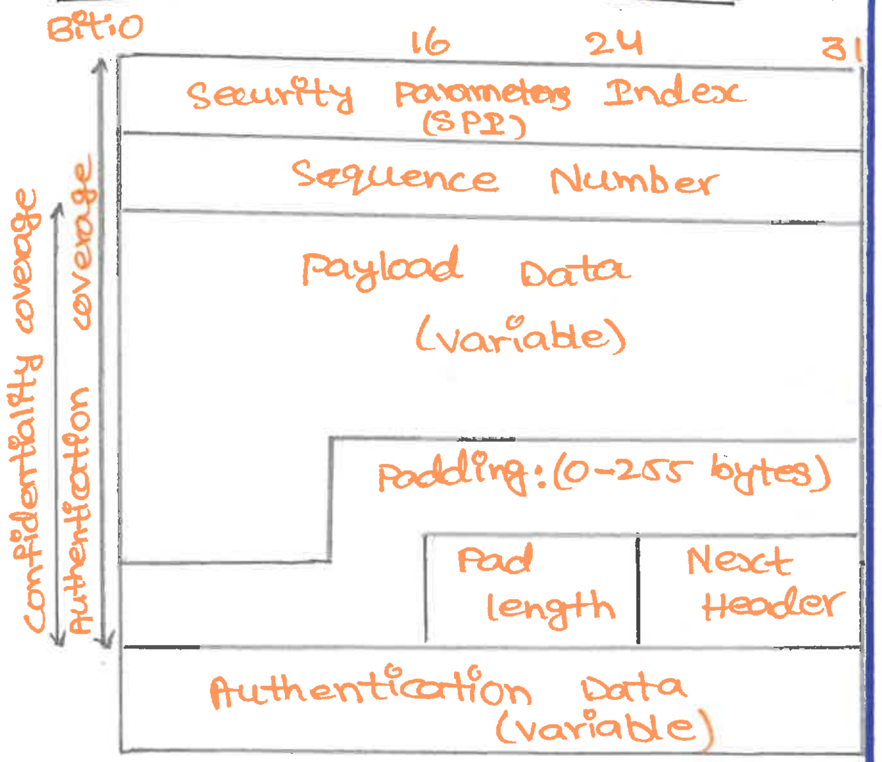
Tunnel mode:

In Tunnel mode AH authenticates entire inner IP packet plus selected portions of outer IP header.

Authentication header (AH):



Encapsulating security payload (ESP):



IP Security

What is IP Security?

* have a range of application speci-fic security mechaniesms.

 eg. S/MIME, PGP

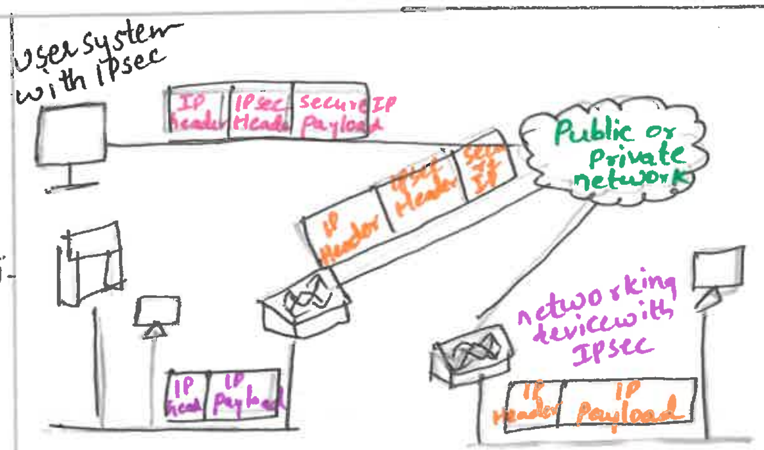
* however security concerns that cut accross protocol layers
* Provides
    * authentication
    * confidentiality
    * key management
* Applicable to use over LANS, across Public & Private WANS.

IP Security Architecture

* Specification is quite complex.
* defined in numerous RFC's.
    * incl. RFC 2401/2402/2406/2408
* mandatory in IPV6, optional in IPv4.
* have two security header extensions
    * Authentication Header (AH)
    * Encapsulating Security Payload (ESP)

IP Services

* Access Control
* Connectionless integrity
* Data Origin authentication
* Confidentiality (encryption)



Benifits:-

* in firewall provides strong security to all traffic
* can be transperent to end users
* secures routing architectures

Combining Security Associations

* SA's can implement either AH or ESP
* to implement both need to combine SA's
    * form a security association bundle
    * combined by
        * transport adjecancy
        * iterated tunneling

Key Management

* Handles key generation & distribution
* typically needs 2 pairs of keys
    * 2 per direction for AH & ESP
* manual key management
    * sysadmin manually configures every system.

Oakley

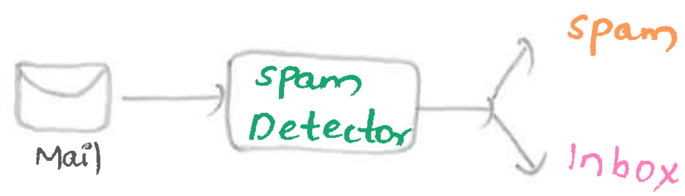
* a key exchange protocol
* based on Diffie-Hellman key exchange
* adds features to address weakness
* can use arithmetic in prime fields or elliptic cure fields.

Email Spam Detection

* Detects unsolicited, unwanted, and virus-infested email.
* stops it from getting into email inboxes.
* These spam detection tasks are done by Natural Language Processing (NLP).
* which processes text into useful insights that can be applied to future data.
* there are many types of NLP problems, one of most common types is classification of strings.

Problem Description

* Understand problem in crucial first step in solving any machine learning problem.



* Can prevent spam messages from creeping into user's inbox.
* Improves user expeience

To classify Email into spam or not spam

i) Text Processing

* Processing the text data is first step
* transform raw data is essential.
* Fundamental steps
    * cleaning raw data
        * removal of numbers
        * Lowering case
        * remove whitespaced
    * Tokenizing cleaned data

ii) Text sequencing

a) Padding – making tokens for all emails an equal size

b) Label the encoding target variable.

iii) Model selection

A machine learning model has to understand text by utilizing already learned text.

iv) Implementation

Embedding is process of converting formatted data into numerical values which a machine can interpret.

EMAIL IP & WEB SECURITY

Email security:

Describing different procedures and techniques for protecting emal Accounts, Content and Communication against unauthorized access loss or Compromise.

Pretty Good privacy (PGP)

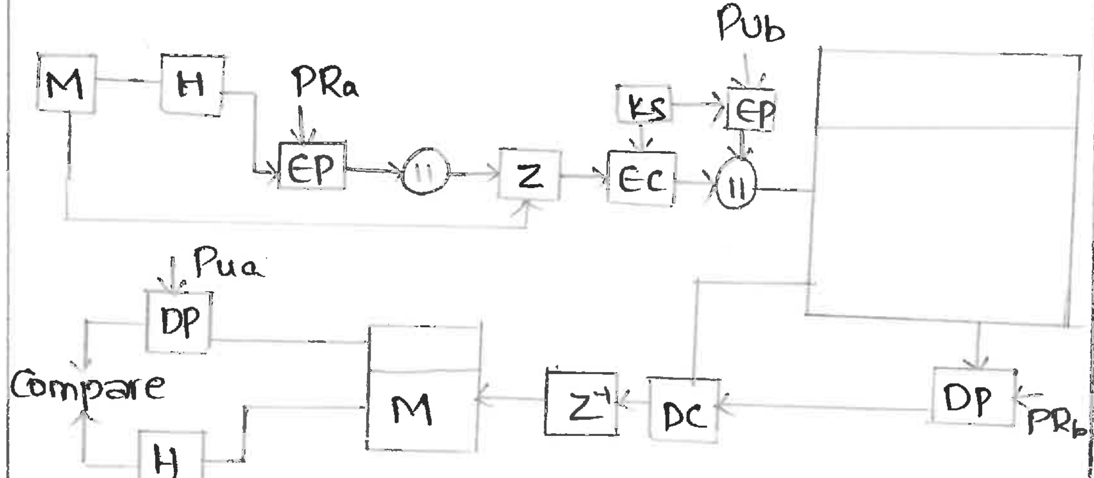
→ open source Freely available Software package for email security

PGP operations & Algorithms

Function	Algorithms
Digital signature	RSA/SHA (or) DSA/SHA
Encryption	CAST or IDEA or 3DES with RSA or Diffie-Hellman
Compression	ZIP
Compatibility	radix 64 Conversion
segmentation	–

* sender forms 128-bits random session key.
* encrypts Message with session key
* Attaches session key encrypted with RSA.

Confidentiality and Authentication



PGP Message:

Content | operation

- session key Component
  - Recipient's Public key (Pub)
  - session key (KS) — E(Pub,¥)
- signature
  - Time stamp
  - sender's Public key (Pua)
  - Leading Two octets of Message digest
  - Message digest — E (PRa, ¥)
- Message
  - filename
  - Time stamp
  - Data

ZIP(KS,¥) — E

S/MIME:

secure / Multipurpose internet Mail extension (S/MIME) security enhancement to the MIME

RFC 5322 (RFC 822)

→ Traditional email Format standard

→ Format for text Messages that are sent using electronic Mail.

→ Messages Consists of some number of header lines followed by unrestricted text.

MIME:

→ MIME-Version → is extension of SMTP

→ Content type → Type & subtype of data.

→ Content Transfer - Encoding

→ Content - ID

→ Content - Description

7 Major Types of Content Formed

(Rb4) → Text type
→ Multipart type
→ Message
→ Image
→ video
→ Audio
→ Application

S/MIME Functions:

→ Enveloped data

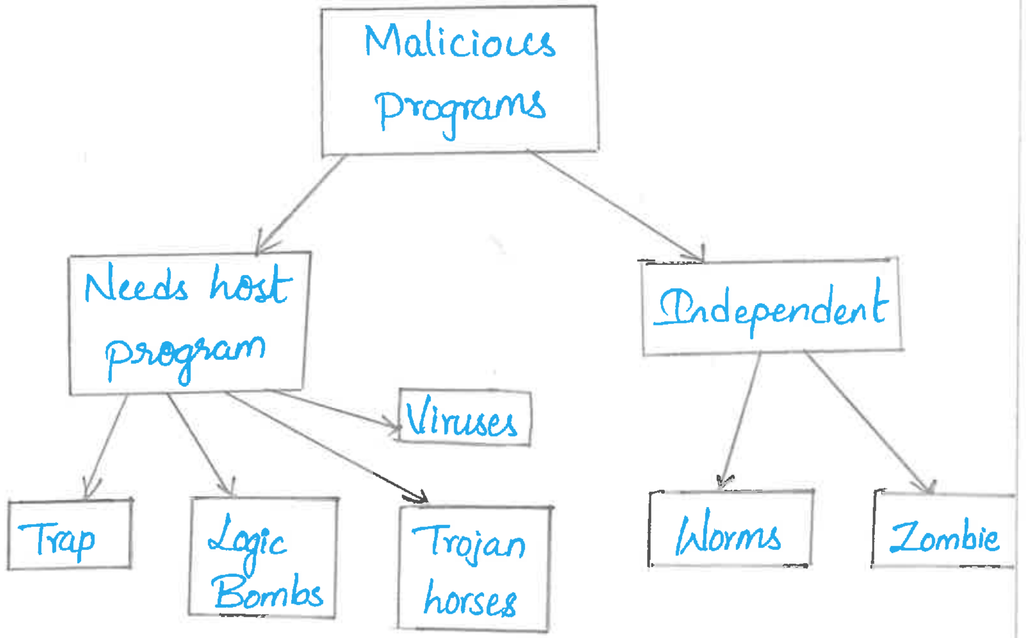
→ signed data

→ clear signed data

→ signed & enveloped data.

Overview of the Web Security measures and Standards

MALICIOUS SOFTWARES:-



Types of Viruses

* Parastic
* Memory Resident
* Boot Sector
* Stealth
* Polymorphic
* Macro
* E-MAIL

Anti Virus Techniques

* Detection
* Identification
* Removal

Advanced Anti-Virus Techniques :-

* Generic decryption – [use CPU simulator]
* Digital Immune System (IBM)
  - general purpose emulation
  - Virus detection
  - Virus was captured, analyzed, removed.

FIREWALLS AND TYPES OF FIREWALLS

- Provides 4 type Control access

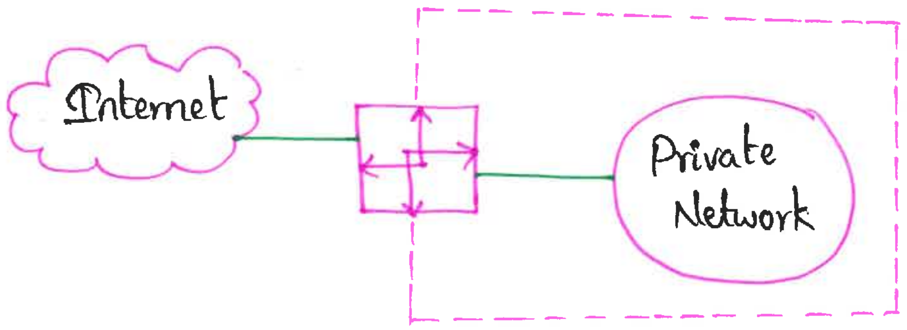
* Service Control – [It may filter traffic on the basis of IP address and TCP port no.]
* Direction Control – [determines the direction]
* User Control – [It may applied to incoming traffic]
* Behaviour Control – [Controls how particular services are used.]

- It accepts, rejects or drops that Specific traffic.

Accept :- allow the traffic
Reject :- block the traffic but reply
Drop :- block the traffic with no reply.

Types of firewalls :-

* Packet - Filtering Router
* Application level Gateway
* Circuit - level Gateway.

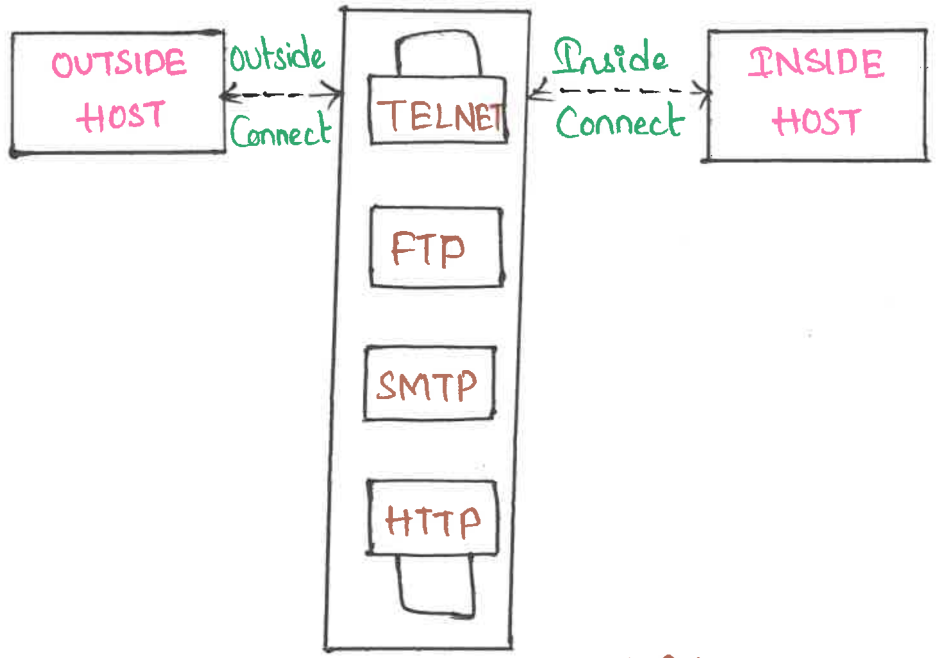


Packet filtering router

PACKET FILTERING ROUTER

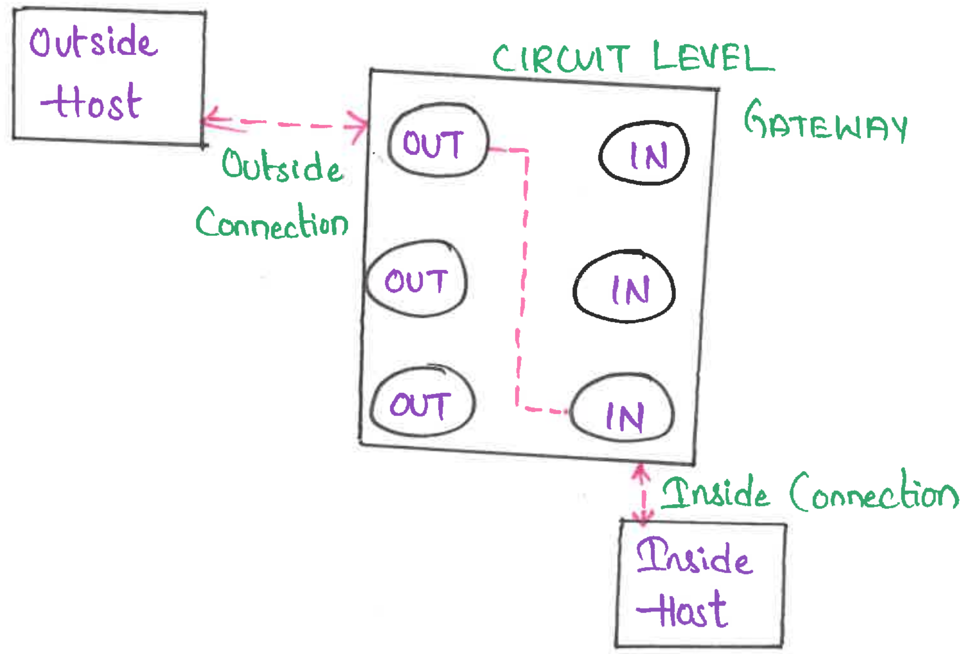
Application level Gateway :-

* Application proxy
* ALG is a security Component that augments a firewall or NAT employed in a computer network.



Application level Gateway.

Circuit Level Gateway :-



Overview of the web security measures & standard

SSL Architecture :-

* Security services between TCP and application that use TCP.
* Internet standard version is called (TLS).
* SSL provides confidentiality using symmetric encryption and message integrity using a message authentication code.

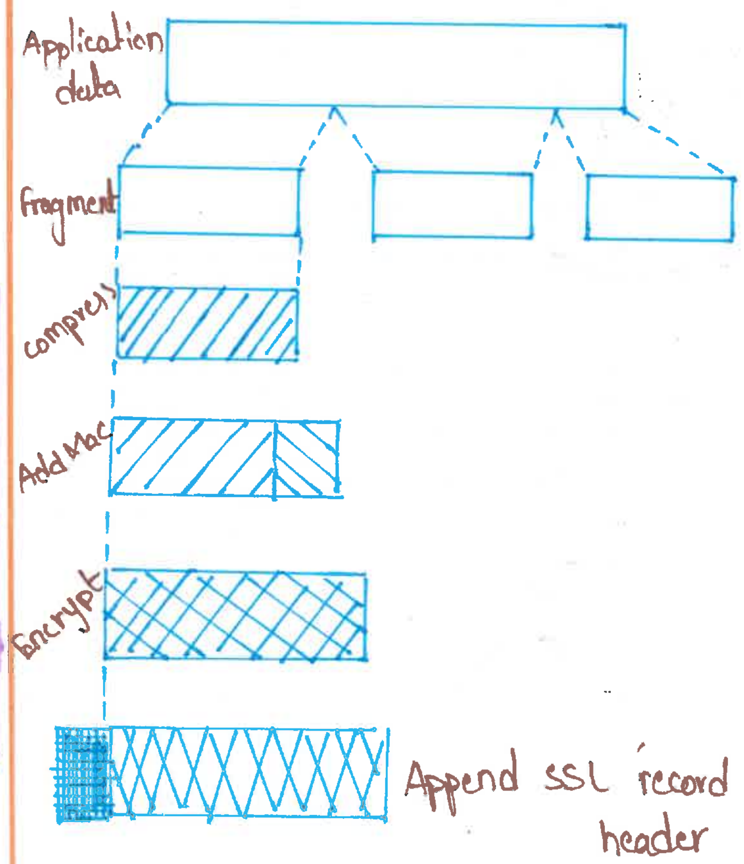
SSL Architecture :-

SSL Handshake protocol	SSL change cipher spec protocol	Alert protocol	HTTP
SSL Record Protocol			
TCP			
IP			

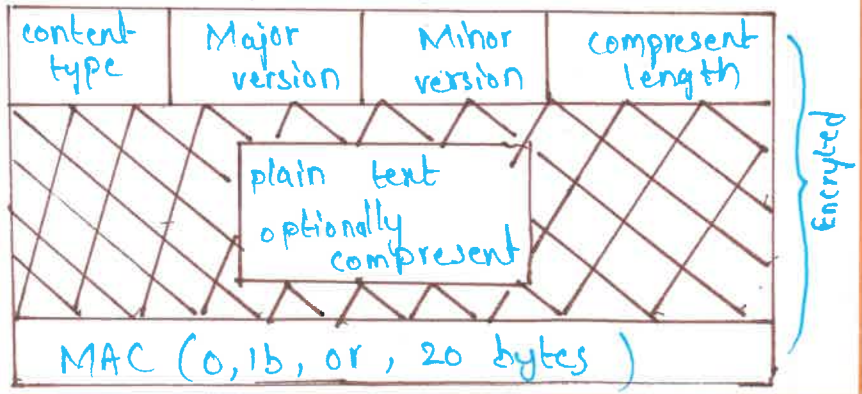
SSL Concepts :-

* SSL session → association between client & server, created by handshake protocol
* SSL connection → transport that provide a suitable type of service
* Every connection is associated with one session.

SSL Record protocol operations :-

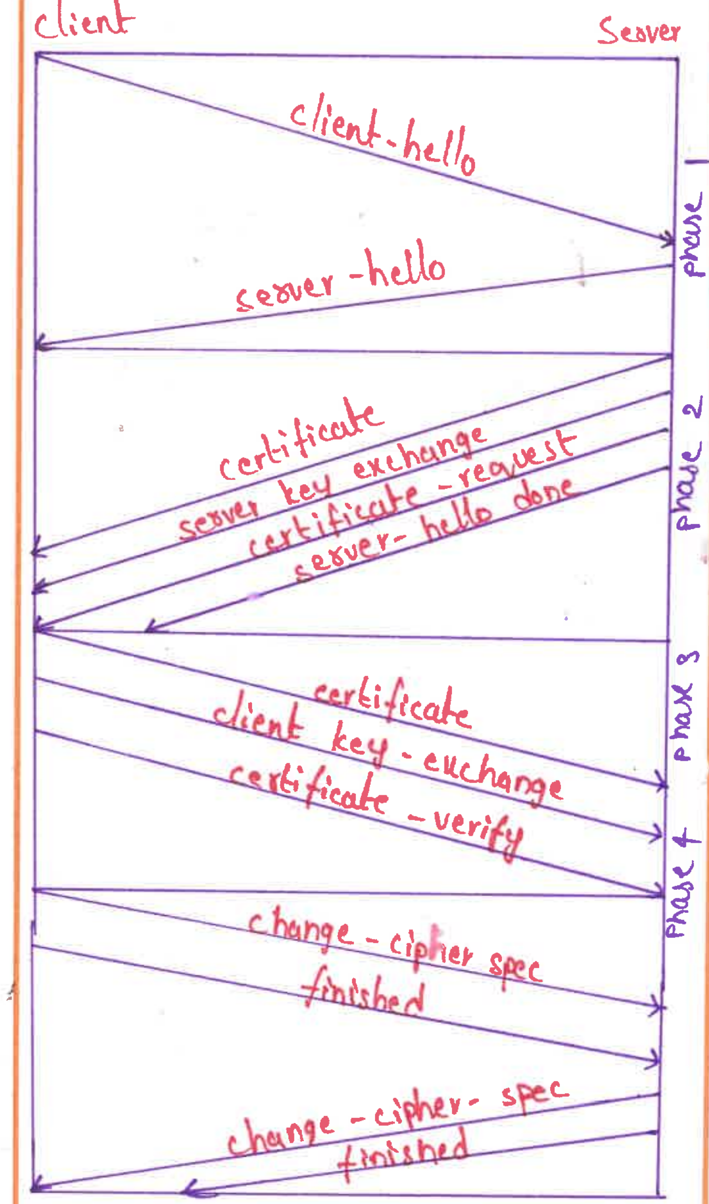


SSL Record protocol Format :-



SSL

Handshake protocol Actions



phase 1 → establish security capabilities

phase 2 → server Authentication & key exchange

phase 3 → client & Authentication key exchange

phase 4 → Finish

SET :- set of security protocols and formats that enables uses to utilize the credit card payment infra on an open network.

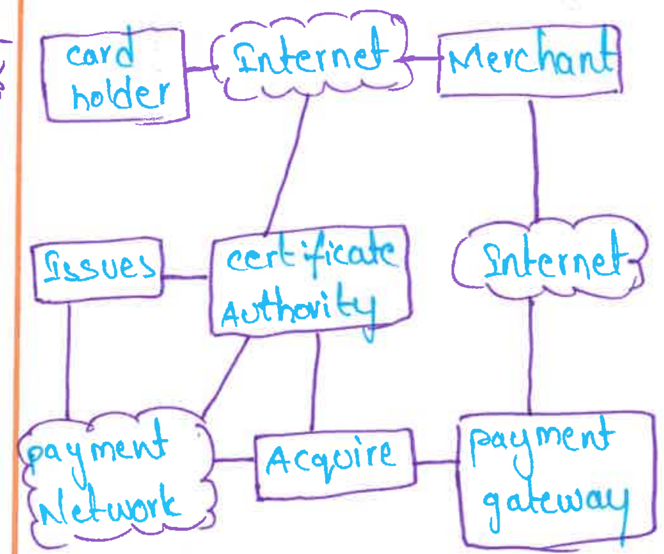
SET Services :-

* Secure communication
* Provide trust (X.509V3)
* Restrict access of information

Key features of SET :-

* Confidentiality of information
* Integrity of data
* card holder account authentication
* Merchant authentication

SET participants :-



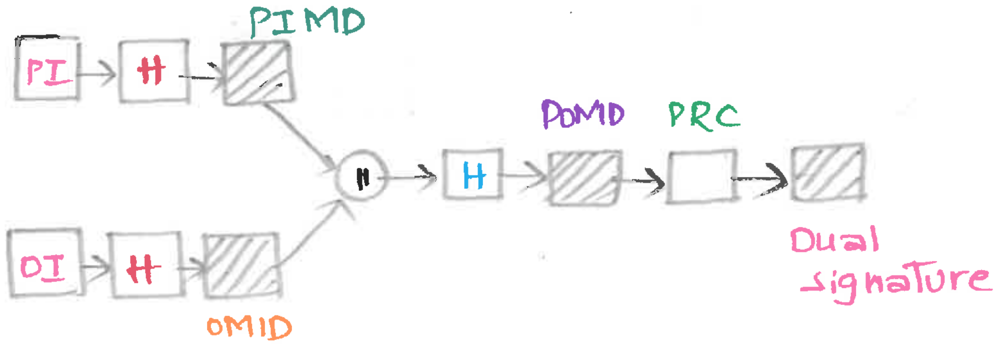
Certification authority :-

An entity that is trusted to issue X.509 V3 public key certificates for cardholders, Merchants and payment gateways.

SET

Secure electronic Transactions.

Dual signature.



customer encrypts final hash with his private key creating Digital signature.

$$Ds = E\left(PR_c\left[H\left(H(PI)\,\|\,H(OI)\right)\right]\right)$$

Merchant can Compute the Quantities.

$H(PIMS \,\|\, H[OI])$;

$D(PU_c, DS)$

If Three Quantities equal, Merchant bank Compute verified signature

$H(H(OI) \,\|\, OIMD)$;

$D(PU_c, DS)$

If three Quantities equal bank verified signature.

TLS

Transport Layer security

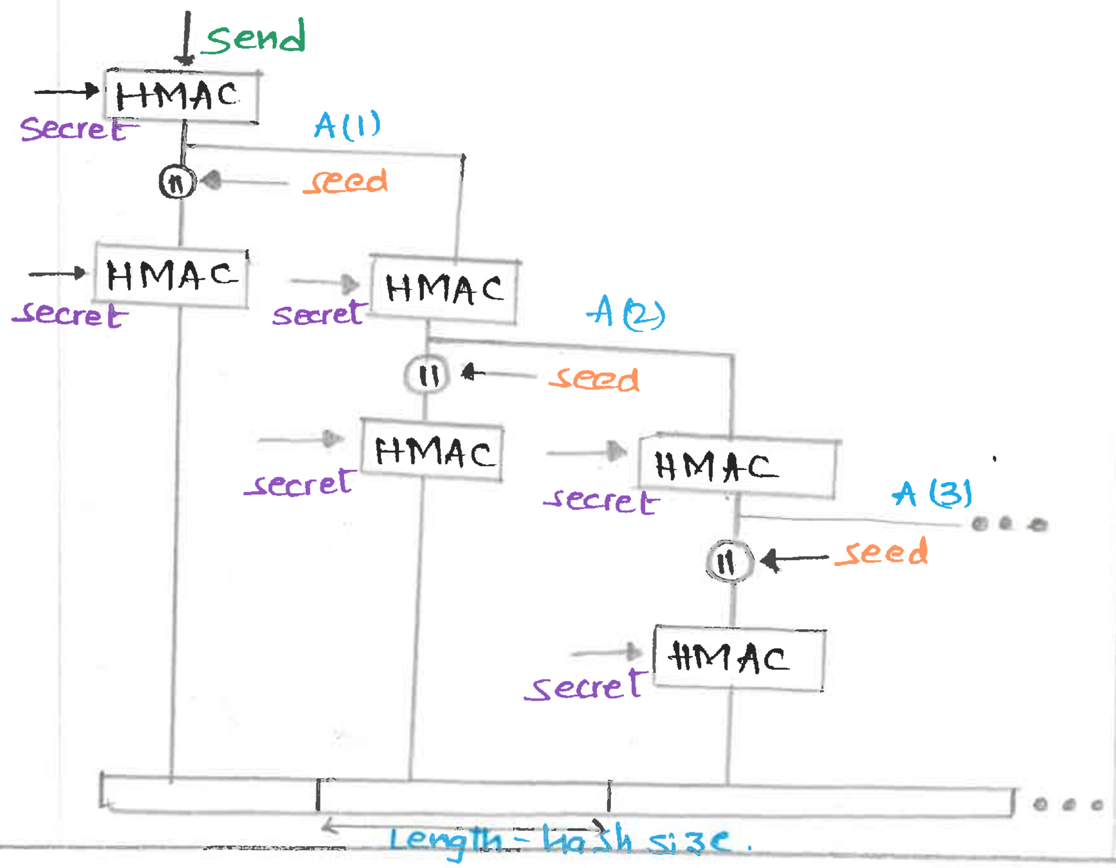
* TLS is an IETF standardization initiative whose Goal is to produce an internet standard version of SSL.
* TLS is defined as a proposed internet standard in RFC 5246.
* RFC 5246 is very similar to $SSLV_3$.

Version Number

→ version Number of Current version of TLS, the Major version is 3 and the Minor version is 3.

$$HMAC_K(M) = H[(K^+ \oplus opad) \,\|\, H[(K^+ \oplus ipad) \,\|\, M]]$$

H = embedded hash function
M = Message input to HMAC
K^+ = secret key
iPad = 00110110
opad = 01011100



ALERT CODES

→ TLS supports all of the alert codes defined in $SSLV_3$ with the exception of no_certificate.

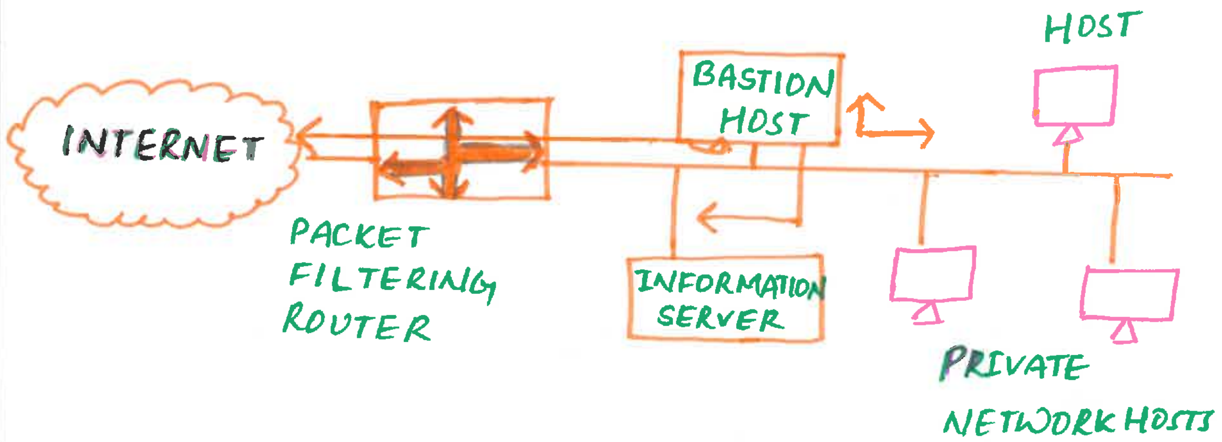
Codes	
record_overflow	A TLS record was received with a payload.
unknown_ca	A valid certificate chain
Access_denied	Valid certificate is received.
decode_error	Message could not be decoded.
Protocol_version	Client Attempt to Negotiate.
insufficient_security.	returned instead of handshake_failure
Unsupported_extension	sent by clients that receive
internal error	unrelated to the peer
decrypt_error	handshake cryptographic operation failed.
user_canceled	handshake is being canceled.
no_renegotiation	sent by a client in response.

Cipher suites.

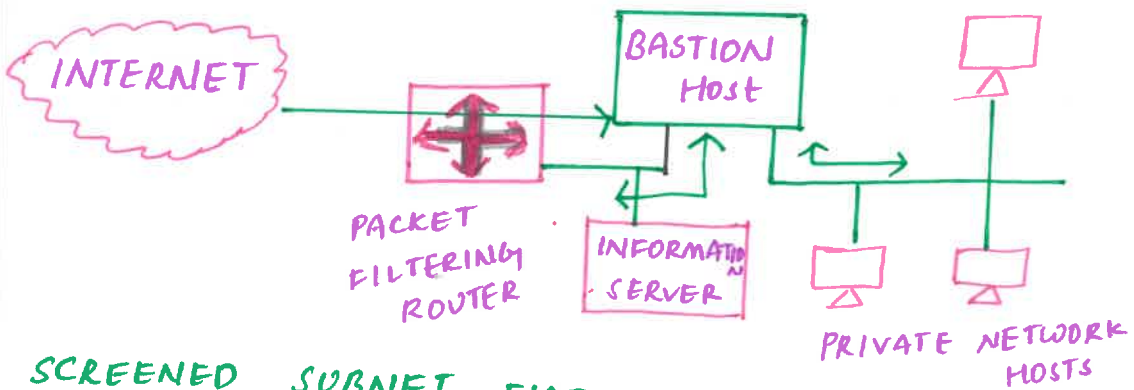
1. key Exchange: TLS supports all of the key exchange techniques of $SSLV_3$
2. Symmetric Encryption Algorithm: [SEA] includes all types of SEA Found in $SSLV_3$

FIREWALL CONFIGURATION

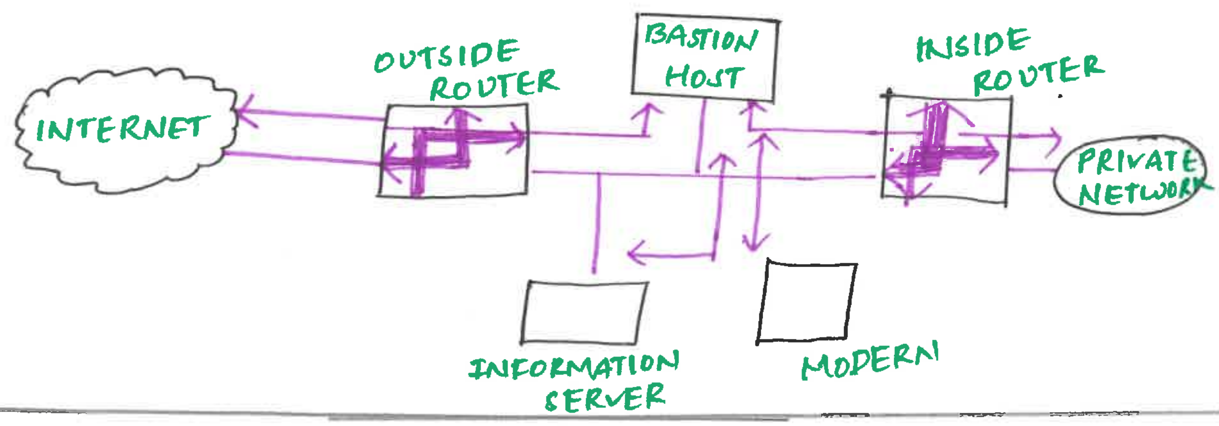
SCREENED HOST FIREWALL, SINGLE-HOMED BASTION



SCREENED HOST FIREWALL, DUAL-HOMED BASTION



SCREENED SUBNET FIREWALL



INTRUSION DETUTION / PREVENTION STEPS

INTRUDER
- MASQUERADER – Attacker pretends to be an unauthorized user in order to get access.
- MISFEASOR – caterogy of individuals that are authorised to use the system.
- CLANDESTIRE USER – Category of individuals those have supervision / administrative control over the system. Access control.

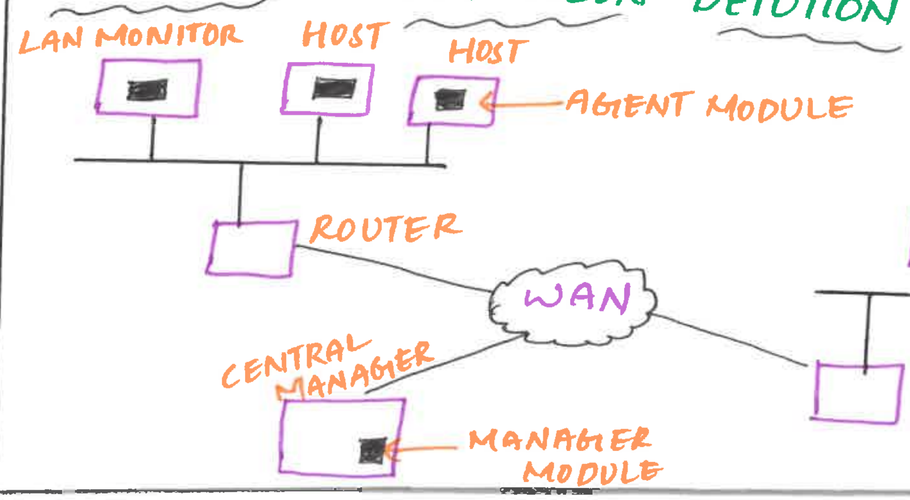
AUDIT RECORDS
- NAIVE AUDIT RECORDS
- DETUTION SPECIFIC AUDIT RECORDS

AUDIT RECORDS
- SUBJECT
- ACTION
- OBJECT
- EXCEPION CONDITION
- RESOURCE USAGE
- TIME STAMP

→ sequence of audit tokens.
→ Each audit token contain event into such as user ID, time & date.

DETECTION
- STATISFIED ANAMOLY DETECTION
  - THRESHOLD DETECTION
  - PROFILE BASED
- RULE BASED DETECTION
  - ANOMLY DETECTION
  - PENETRATION IDENTIFICATION

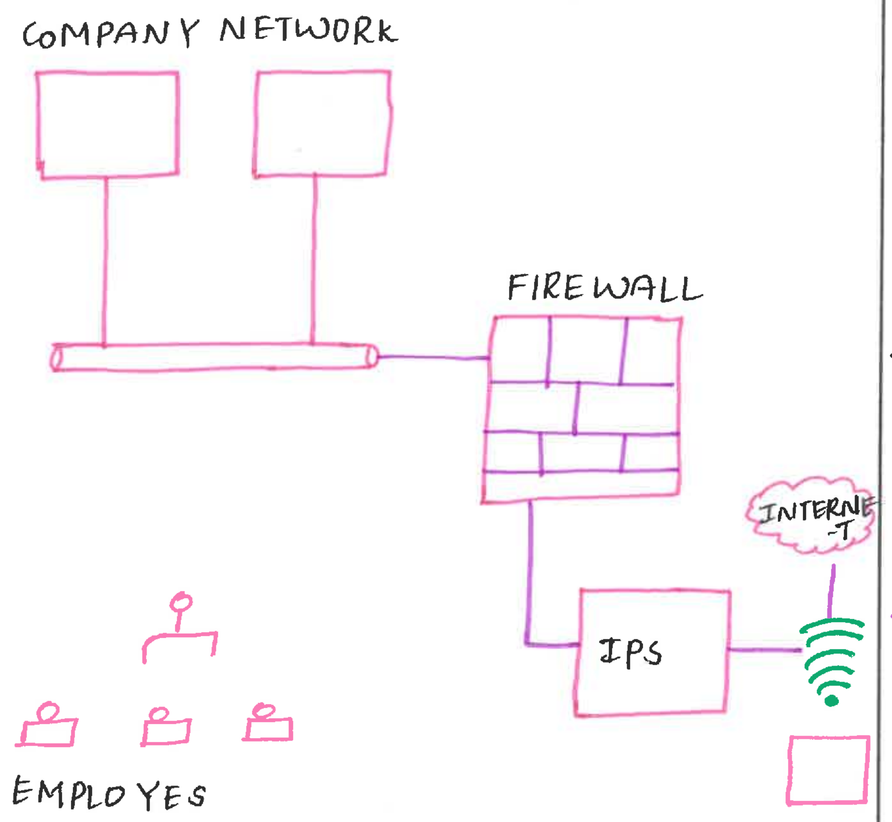
DISTRIBUTED INTRUSION DETUTION



→ All of which communicate with each other, or with a central server that facilities.

→ Advance network monitoring.

INTRUSION PREVENTION SYSTEMS



IPS → Designed to spot attacks based on
* Signature
* Anomalies

CLASSIFICATION :-

* NETWORK-BASED (NIPS)
* WIRELESS (NIPS)
* NETWORK BEHAVIOUR ANALYSIS (NBA)
* HOST-BASED (HIPS)

DETUTION METHOD OF IPS :-

* SIGNATURE BASED DETUTION
* STATISFICAL ANAMOLY BASED DETUTION
* STATEFUL PROTOCOL ANALYSIS DETUTION

IPS DESIGNED PREVENT FOLLOWING ~~STEPS~~ THREATS

* Dos ATTACK – Attacker attempts to disrupt service by host
* DDos ATTACK – overload a targeted resource by consuming.
* VARIOUS TYPE OF EXPLOITS – Local Exploits, Remote Exploits
* WORMS → Encrypt data on
* VIRUSES the victim's system.

TYPES OF PREVENITIONS

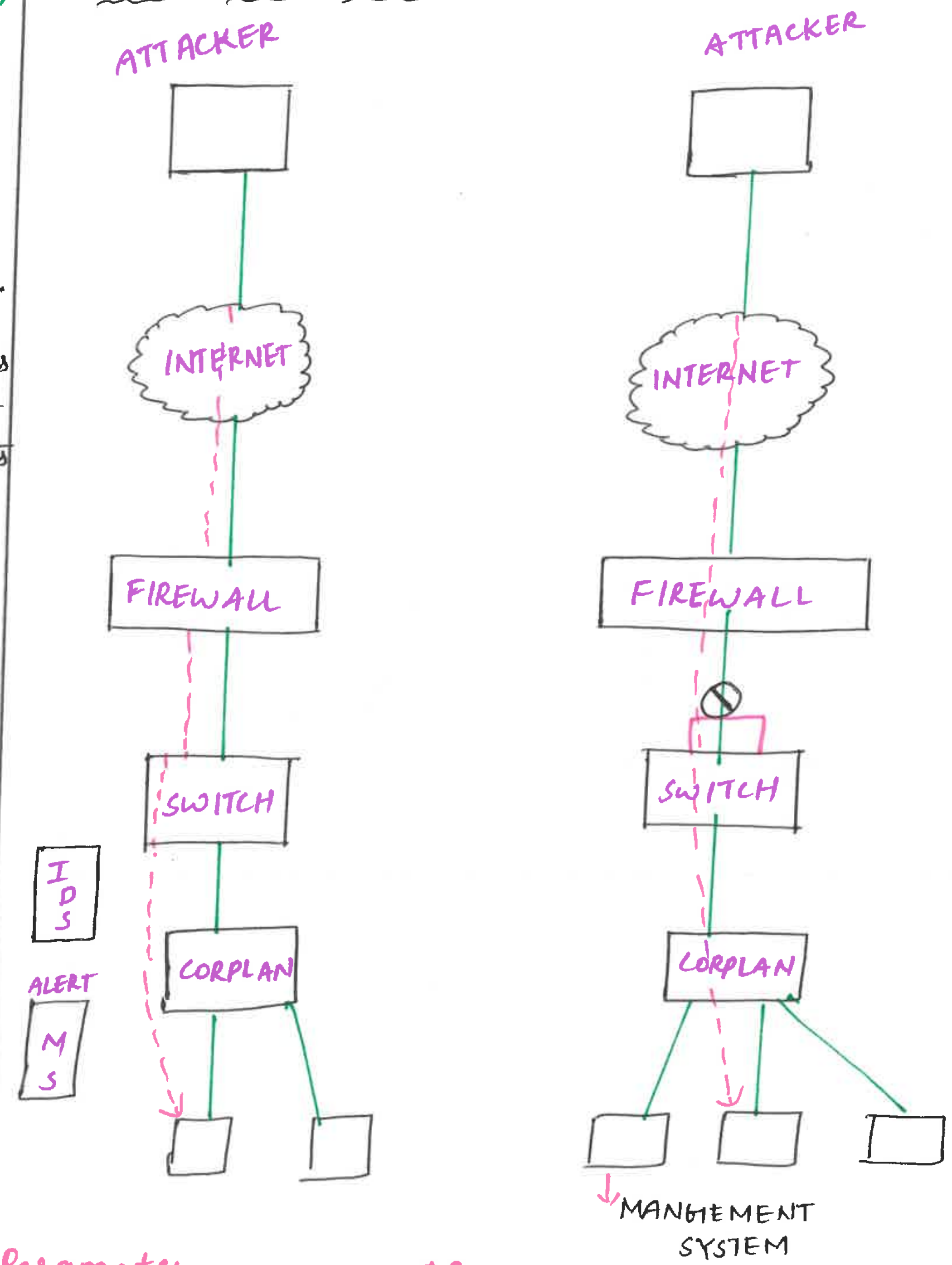
* SIGNATURE BASED
* ANOMALY BASED
* POLICY BASED

The data is appropriately Encrypted falls in wrong hands.

HOW IPS WORKS :-

* Sending an alarm to the administrator.
* Dropping the malicious packets.
* Blocking traffic from the source address.
* Resetting the connection.
* Configuring firewalls to prevent future attacks.

IDS VS IPS



Parameter	IPS	IDS
System type	Active Statisficial	Passive
Detection	Anamoly and signature	Signature
Placement	Inline	out of band
Input on n/w performance	data communication slow down	from data communication does not impact

Substitution Techniques

Substitution Techniques:-

1. Caesar cipher:-

*The main drawback of this ST is.
*it is used in very short length communication and it is easy to attack.

A	B	C	D	E	F	G	H	I	J	K	L
1	2	3	4	5	6	7	8	9	10	11	12

M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25	26

*Here the key is the numerical which varies from 1 to 26.

$\boxed{1 \le k \le 26}$

The k value must be b/w 1 to 26.

Encryption:- $\boxed{C = (P+k) \bmod 26}$

Eg:- P.T = zoo , k = 4

Z => C.T = (26+4) mod 26
=> (26+4) mod 26
$\boxed{\text{C.T} \Rightarrow 4}$,,

O => C.T = (15+4) mod 26
C.T = 19 mod 26
$\boxed{\text{CT} = 19}$,,

$\boxed{\therefore \text{CT} = \text{DSS}}$

Decryption:- $\boxed{P = (C-k) \bmod 26}$

Eg:- P = LIPPS , k = 4

L => P.T = (12-4) mod 26
= 8 mod 26
$\boxed{\text{P.T} = 8}$

I = P.T = (9-4) mod 26
$\boxed{\text{P.T} \Rightarrow 5}$

P = P.T => (16-4) mod 26
=> 12 mod 26
$\boxed{\text{P.T} = 12}$

S => P.T => (19-4) mod 26
=> 15 mod 26
$\boxed{\text{P.T} \Rightarrow 15}$

$\boxed{\therefore \text{P.T} \Rightarrow \text{HELLO}}$

2. Mono alphabetic cipher:-

A	B	C	D	E	F	G	H	I	J	K	L	M
L	Q	S	A	K	J	P	D	M	E	T	N	F

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
G	R	U	W	H	V	I	Z	Y	C	O	X	B

Encryption:- Convert plain text to cipher

Eg:- ATTACK

Plain text	A	T	T	A	C	K
cipher text	L	I	I	L	S	T

$\boxed{\therefore \text{C.T} \Rightarrow \text{LIILST}}$

*it is easy to break the C.T. if attackers knows the frequency of letters used.

letters	sequence
e	12.7
t	9.1
a	8.2
o	7.5
i	7.0
n	6.7
s	6.3
h	6.1

3. Play-fair cipher:-

*we want to consider key in 5x5 column
*MY plain text = HELLO.
*MY keyword = Network.
*Now write the alphabetic letters after filling keyword.

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

Rules:- 1:- Divide a plain text to a pair of letters.
Rule-2:- Differentiate repeated letters in the pack with dummy letters.
Rule-3:- if a pair of plain text letters are in same row then replace them with right most.

Eg:- P.T = HELLO → Encryption

HE|LL|O
same letters giving one dummy letter.

HE = WF
LX = VP
LO = ES

$\boxed{\therefore \text{C.T} = \text{WFVPES}}$

4. Poly alphabetic cipher:-

P.T => ACTIVE
Key => PASCAL

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Encryption:- $\boxed{C_i = (P_i+k) \bmod 26}$

A = C_i = (P_i+k) mod 26
=> (0+15) mod 26
=> 15 mod 26
$\boxed{C_i \Rightarrow 15}$,,

C => (2+0) mod 26
$\boxed{C_i \Rightarrow 2}$,,

T => (19+18) mod 26
=> 37 mod 26
$\boxed{C_i \Rightarrow 19}$,,

I => (8+2) mod 26
$\boxed{\text{C.T} \Rightarrow 10}$

V = (21+0) mod 26
$\boxed{\text{C.T} = 21}$,,

E = (4+11) mod 26
C_i = 15 mod 26
$\boxed{C_i = 15}$

$\boxed{\therefore \text{C.T} \Rightarrow \text{PCTKVP}}$

5. Hill cipher:-

C = K×P mod 26 → Encryption
P = K×C mod 26 → Decryption

Eg:- HELP keymatrix = $\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$

HE => $\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 7 \\ 4 \end{bmatrix} \bmod 26$

=> $\begin{bmatrix} 21+12 \\ 14+20 \end{bmatrix} \bmod 26$ => $\begin{bmatrix} 33 \\ 34 \end{bmatrix} \bmod 26$

=> 33 mod 26 => $\begin{bmatrix} H \\ I \end{bmatrix}$ => $\begin{bmatrix} 7 \\ 8 \end{bmatrix}$
=> 34 mod 26

LP => $\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 11 \\ 15 \end{bmatrix} \bmod 26$

=> $\begin{bmatrix} 33+45 \\ 22+75 \end{bmatrix} \bmod 26$

=> $\begin{bmatrix} 78 \\ 97 \end{bmatrix} \bmod 26$

=> 78 mod 26 => $\begin{bmatrix} 0 \\ 19 \end{bmatrix}$ => $\begin{bmatrix} A \\ T \end{bmatrix}$
=> 97 mod 26

∴ "HELP" To cipher text is

$\boxed{\text{C.T} \Rightarrow \text{"HIAT"}}$

These are all the substitution Techniques.

TRANSposition Techniques

Transposition techniques

<No replacement/substitution>

⇒ In this technique the arranging the order OE bits to provide the security.

⇒ In substitution technique we are replacing the plain text with the cipher text character.

⇒ ~~Here~~ we are not going to replace any character

⇒ just re-arranging the order of bits position to provide the security

⇒ In this transposition technique mainly there are '2' technique.

1. Rail fence Technique

This Technique is a type of Transposition technique and does is write the plain text as a sequence of diagonals and changing the order according to each row

It uses a simple algorithm:-

SO, the cipher-text are

* writing down the plain text message into a sequence of diagonals.
* Row-wise writing the plain text written from above step.

example:-

let's say, we take an example of "includeHELP" is AWESOME"

I N U E E P S W S M

N L D H L I A E O W

C.T = (I N U E E P S W S M) → above the line

(N L D H L I A E O W) Below the line

now, as we can see, rail fence technique is very easy to break by any cryptanalyst

2. Columnar transition Technique

It is a slight variation to the rail-fence technique, let's see its algorithm.

* In a rectangle of pre-defined size, write the plain-text message row by row
* read the plain message in random order in a column-wise fashion. It can be any order such as 2,1,3 etc.
* Thus cipher-text is obtained

let's see the example

now we apply the above algorithm and create the rectangle of 4 column (we decide to make a rectangle with four column it can be any number) P.T = INcludeHelp is AWESOME

C-1	C-2	C-3	C-4
I	N	C	L
U	D	E	H
E	L	P	I
S	A	W	E
S	O	M	E

now let's decide on an order of the column as 4,1,3 and 2 now we will read the text in column wise

Cipher text:-

LHIEEIUESSCEPWMNDLAO

It is cipher text include Help is Awesome.

RSA algorithm:-

RSA algorithm

Consider two large prime numbers p, +q

Calculate $n = p * q$

$\phi(A) = p(-1) * q(-1)$

assume e such that $\boxed{gcd(e, \phi(n)) = 1}$

assume d such that $\boxed{d = e^{-1} \bmod \phi(n)}$

public key = {e, n}

private key = {d, n}

$d * e = \phi \bmod \phi(n)$

$d * e \bmod \phi(n) = 1 \bmod \phi(n)$

$d * e \bmod (\phi) n = 1$

Encryption	Decryption
Plain text message <1 m<1 cipher text formula $\boxed{c = m^e \bmod n}$	cipher text message <1 c<1 Plain text formula $\boxed{M = c^d \bmod n}$

if p - prime $\phi(p) = p - 1$

$p = 3 \quad q = 5$

$n = p * q \Rightarrow n = 3 \times 5 \Rightarrow n = 15$

$\phi(n) = p(-1) * q(-1)$

$\phi(15) = (3-1) * (5-1)$

$\phi(15) = 2 \times 4$

$\phi(15) = 8$.

Assume e such that $gcd(e, \phi(n)) = 1$

Prime number of 15

$\Rightarrow 3$

Assume $d = d * e \bmod \phi(n) = 1$

Prime number of 15

$3 \times 3 \bmod \phi(15) = 1$

$9 \bmod \phi(15) = 1$

Public key = {3, 15}

private key = {3, 15}

Encryption	Decryption
$M = 4 < n$ $C = m^e \bmod n$ $= 4^3 \bmod 15$ $= 64 \bmod 15$ $C = 4$ $C = 4$	$C = 4 < n$ $M = c^d \bmod n$ $= 4^3 \bmod n$ $= 64 \bmod 15$ $m = 4$ $m = 4$

Example:-

$p = 11 \quad q = 19$

$n \Rightarrow p * q \Rightarrow n = 11 \times 19 \Rightarrow n = 209$

$\phi(n) = (p-1) * (q-1)$

$\Rightarrow 10 \times 18$

$\phi(n) = 180$

assume 'e' such that $gcd(e, \phi(n)) = 1$

$e = 3$

assume 'd' such that $d = d * e \bmod (n) = 1$

$d = 3$

Encryption	Decryption
$M = 12 < n$ $C = m^e \bmod n$ $= 12^3 \bmod 209$ $= 1728 \bmod 209$ $\Rightarrow 56$	$C = 12 < n$ $M = c^d \bmod n$ $= 156^3 \bmod 209$ $= 175,616 \bmod 209$ $\Rightarrow 56$

advantages:-

* The sender and receiver don't need any prior knowledge of each other.

disadvantages:-

* The algorithm cannot be used for any asymmetric key exchange
* similarly, it cannot be used for signing digital signatures.

Different Hellman key exchange Algorithm

Diffie - Hellman key exchange Algorithm :-

* it is a Asymmetric key Encryption.

Public key   Private key

* it is not a Encryption algorithm.
* Exchange secret / symmetric key.
* Assume " Prime number, q."
* " Here select α, such that $\alpha \rightarrow$ Primitive root of q."
* " Also α is less than q." $\boxed{\therefore \alpha < q}$
* Here A is a primitive root of P.
* if $a \bmod p$, $a^2 \bmod p$, $a^3 \bmod p$, ... $a^{p-1} \bmod p$

$\Downarrow$

1, 2, 3, 4, 5 . . . . . P-1

Assume X_A	(Private key of user A)	$X_A < q$
Calculate Y_A	(Public key of user A)	$Y_A = \alpha^{X_A} \bmod q$
Assume X_B	(Private key of user B)	$X_B < q$
Calculate Y_B	(Public key of user B)	$Y_B = \alpha^{X_B} \bmod q$

Generate a key :- we have to create a key user

user			user	
$\boxed{A}$	$\boxed{k = (Y_B)^{X_A} \bmod q}$	=	$\boxed{B}$	$\boxed{k = (Y_A)^{X_B} \bmod q}$
sender			reciever	

Process To calculation of α :-

Here $q = 11$ means where we take 1 to 10 numbers.

Power ↓

	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	5	10	9	7	3	6	1

↑ Number

* Here we have take the number. which that row 4 Column. There is no repetion Number. we cantake that has α.
* Here $\alpha = 2$. Because there is no repeated number in the colum.

eg :- $q = 11$ $\alpha = 2$ $\boxed{1 \text{ to } q-1}$ (it cannot be repeated)

* Select $\boxed{X_A = 8}$ (Private key)

$Y_A = 2^8 \bmod 11$

$\Rightarrow Y_A = 256 \bmod 11$

$\boxed{Y_A = 3}$ (Public key)

* Select $\boxed{X_B = 4}$ (Private key)

$Y_B = Y_B \Rightarrow \alpha^{X_B} \bmod q$

$Y_B = 2^4 \bmod 11$

$Y_B = 16 \bmod 11$

$\boxed{Y_B = 5}$ (Public key)

user A = $\{ Y_A = 3$ (Public), $X_A = 8$ (Private) $\}$

user B = $\{ Y_B = 5$ (Public), $X_B = 4$ (Private) $\}$

A sender	B reciever
$k = (Y_B)^{X_A} \bmod q$	$k = (Y_A)^{X_B} \bmod q$
$k = (5)^8 \bmod 11$	$k = (3)^4 \bmod 11$
$k = 390{,}625 \bmod 11$	$k = 81 \bmod 11$
$\boxed{k = 4}$	$\boxed{k = 4}$

$\therefore$ Sender and reciever keys are same. $\boxed{\text{Key} = 4}$

* Sender & reciever used key exchange Algorithm.

Elliptic curve cryptography

J

Elliptic curve cryptography :-

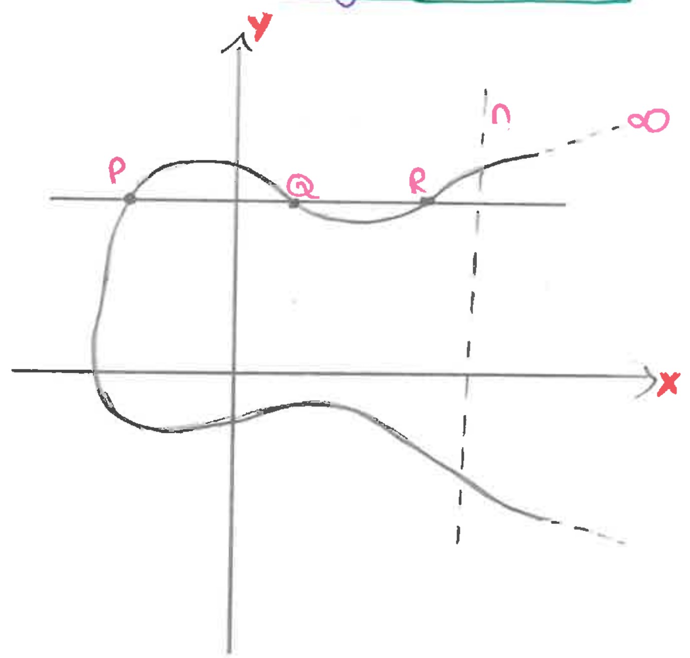
*it is an symmetric/Public key cryptosystem.

*it Provides equal security with smaller key size as compared to RAS/DES algorithms.

*it makes use of elliptic curves.

*elliptic curves are defined by some mathematical functions.

$\boxed{\text{General formula} \Rightarrow y^2 = x^3 + ax + b}$



*Symmetric to the x-axis.

*if we draw a line, it will touch a maximum of 3 points.

ECC Algorithm :- ECC key Generation

(1) $E_q(a,b)$ - Elliptic curve with Parameters a, b + q (Prime number or an integer of the form 2^m).

(2) G- Point on the elliptic curve.

user A key Generation :-

*select private key $n_A \Rightarrow \boxed{n_A < n.}$

*calculate public key P_A $\boxed{P_A = n_A \times G}$

user B key Generation :-

*select private key $n_B \Rightarrow \boxed{n_B < n}$

*calculate public key P_B $\boxed{P_B = n_B \times G}$

calculate of secret key by user A

$\boxed{K = n_A \times P_B}$

*calculate of secret key by user B

$\boxed{K = n_B \times P_A}$

Encryption :-

*first encode this message M into a point on Elliptive curve.

*let m is a message of Pm.

*for Encryption, choose a random positive integer k.

*The cipher point will be.

$$\boxed{C_m = \{\underbrace{kG}_{x\ \text{Points}},\ \underbrace{P_m + kP_B}_{y\ \text{Points}}\}}$$

*This point will be sent to the receiver

Decryption :-

*multiply x-coordinate with receiver's secret key.

$\boxed{kG \times n_B}$

*Then subtract $(kG \times n_B)$ from y-coordinate of cipher point.

$\boxed{P_m + kP_B - (kG \times n_B)}$

* we know that $\boxed{P_B = n_B \times G}$

$\boxed{\therefore P_m + kP_B - kP_B}$

$\boxed{\Rightarrow P_m}$

*so, receive gets the same P_m.

Eg :- find a point in elliptic curve $E_{11}(1,1)$? a=1, b=1. find the points?

Sol :- Ec is represented as $E_p(a,b)$,

So, P=11 a=1, b=1

*Elliptic curve equation is $y^2 = x^3 + ax + b$

=>substitute P, a, b values in the equation

$y^2 = x^3 + ax + b \Rightarrow y^2 = x^3 + 1(x) + 1$

$y^2 = x^3 + x + 1$

$\boxed{x \text{ values} = 0}$ $\boxed{y \text{ values} = +1, -1}$

$\boxed{\text{Points are } (0,1) + (0,-1)}$

since (0,-1) is negative, take mod p

Here we getting the point after mod p is (0,10).

$\boxed{\therefore \text{The Points are } (0,1), (0,10)}$

Difference b/w elliptic curve cryptography + RSA Algorithm :-

ECC	RSA
*ECC offers equivalent security levels with a much smaller key size.	*RSA offers equivalent security levels with a much larger key size.
*The size of the key is 160.	*The size of the key is 1024.
*eg:- online banking, e-business, etc...	*eg:- web browsers, email, VPNs, chat, etc...

Key size		Security level (bits)	Ratio of cost
ECC	RSA/DSA		
160	1024	80	3:1
224	2048	112	6:1
256	3072	128	10:1
384	7680	192	32:1
521	15360	256	64:1

*This is about the ECC Algorithm.