unit-1

security concepts:

1.1 Introduction:

cryptography:

The many schemes used for encryption consitute the area of cryptography such a scheme is known as cryptographic system.

In cryptography and network security, we study the cryptographic algorithms and protocols

Cryptography is the study of secure communication techniques that allow only the sender and intended recipient of a message to view its contents. The term is derived from the Greek word kryptos, which means hidden.

Computer Security:

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources [includes hardware, software, firmware, information / data]

Network and Internet Security:

This consists of measures to detect, prevent and correct security violations during transmission of information over a network.

1.4 Principles of Security:

Key objective of Computer Security:

① Confidentiality:

ⓐ Data Confidentiality → Assures that private or confidential information is not made available or disclosed to unauthorized individuals.

ⓑ Privacy: The individual info. that is collected and stored is disclosed to authorized individuals/entities

② Integrity:

ⓐ Data Integrity → Assures that info and programs are changed only in a specific & authorized manner.

ⓑ System Integrity → Assures that a system performs its intended function in an unimpaired manner free from deliberate unauthorized manipulation of system

③ Availability:

Assures that system work promptly and service is not denied to authorized users.

we can the above objectives are (CIA)

④ Authenticity:

Being able to verify and trust the source of information.

⑤ Accountability:

Being able to trace the actions of an entity to that entity only.

It supports.

- Non-repudiation
- deterrence
- fault Isolation
- intrusion dection
- prevention
- after-action recovery
- legal action

we should be able to trace a security breach to the responsible party.

(1.2) The Need for Security:

When computer application were developed to handle financial and personal data, the real need for security was felt like never before.

Two typical examples of such security mechanism were as follows:

i) Provide a user identification and password to every user, and use that information to authentic a user.

ii) Encode information stored in the database in some fashion. So that it is not visible to users who do not have the right permission.

Modern nature of Attacks:

changes in computer-based systems are mainly due to the speed at which things happen and the accuracy that we get, as compared to the traditional world.

some modern nature of attacks.

① Automating Attacks:

The speed of computers make several attacks worthwhile for miscreants traditional attack: Produce coins using some machinery and bring them into circulation.
Modern attack: steal half a dollar digitally from a million accounts in a few minutes.

changing nature of attacks due to automation.

"Human dislike mundane and repetitive tasks automating them can cause financial destruction or security nuisance quite rapidly.

2. Privacy Concern:

Collecting information about people and later (mis)using it is turning out to be a huge problems in these days.

Every company (e.g. shopkeepers, banks, airlines, insurance) are collecting and processing a mind-boggling amount of information about us, without us realizing when and how it is going to be used.

3. Distance does not Matter:

Thieves are not come to bank directly with mask sit in home hack bank system.

In 1995, a Russian hacker broke into Citibank computers remotely, stealing $12 million. Although the attacker was traced, it was very difficult to get him extradited for the court case.

1.3 Security Approaches:

Trusted System: It is a computer system that can be trusted to a specific extent to enforce a specified security policy.

T.S is initially of military. nowadays in various areas, in banking and financial community, but the concept never changed.

T.S use term reference monitor. This is a logical heart of the computer system.

Security Models:

An organization can take several approaches to implement its

its security model.

① No security: It is a simplest case, the approach could be a decision to implement no security at all.

② Security through obscurity: In this model, a secure simply because nobody known about its existence and contents. This approach work for too long, as there are many ways an attacker can come to know about it.

③ Host security: In this scheme: the security for each host enforced individually it is very safe approach.

④ Network security:

Host security is tough to achieve as organizations grow and become more diverse. In this technique, the focus is to control network access to various hosts and their services, rather than individual host security.

Security-Management practices

Good security-management practices always talk of a security policy being in place. A good security policy and its proper implementation go a long way in ensuring adequate security-management practices. Four key aspects as follows.

i) Affordability: How much money and effort does this security implementation costs

ii) Functionality: what is the mechanism of providing security.

iii) Legality: Does the policy meet the legal requirement.

Cultural Issue: Does the policy complement the people's expectations, working style and beliefs?

once a security policy is place, the following points should be ensured.

a) Explanation of the policy to all concerned

b) outline everybody's responsibilities

c) use single language in all communications.

d) Accountability should be established.

e) provide for exceptions and periodic reviews.

② Types of Security Attack:

Security Attack: Any action that compromises the security of information owned by an organization.

Attack: An assault on system security that derives from an intelligent threat. that is, an intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system

Types:

Two types.

① Passive attack

② Active attack

Passive Attack:

Attempts to learn or make use of information from the system but does not affect system resources.

P.A are in the nature of eavesdropping on, or monitoring of transmission. The goal of the opponent is to obtain info. that is being transmitted.

Two types of P.A are the release of message contents and traffic analysis.

→ The release of message contents is easily understood. (ex: telephone conversation, e-mail) and a transferred file may contain confidential information

→ Traffic Analysis is subtler, Suppose we had a way of masking the contents of message or other information traffic so that opponents, even if they captured the message, could not extract the information from the message.

Passive attack are very difficult to detect, because they do not involve any alteration of the data.

Active Attacks:

Active attacks involves some modification of the data stream or the creation of a false stream.

A.A divided into four categories

Masquerade: Takes place when one entity pretends to be a different entity. It is attack usually includes one of the other forms of active attack.

Replay:

Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

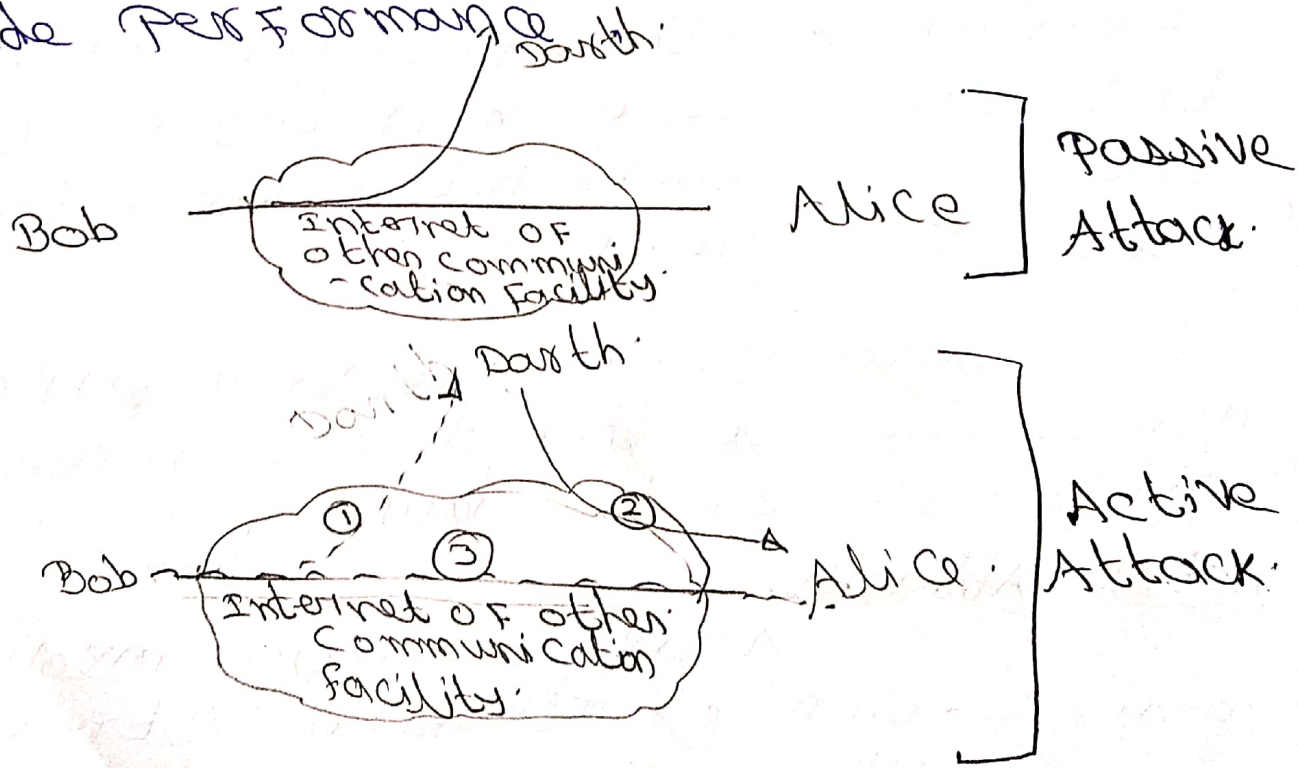
Modification of messages:

Simply means that some portion of a legitimate message is altered, or the messages are delayed or reordered, to produce an unauthorized effect.

Denial of Service:

prevents or inhibits the normal use of management of communication facilities

Ex: Disruption of an entire network either by disabling the network or by overloading it with message so as to degrade performance.



OSI security Architecture:

security Architecture of OSI, defines a systematic approach. OSI security Arch. provides a useful, architecture focuses on security attacks, mechanisms and services.

① **Security Attack:**
Any action that compromises the security of information owned by an organization.

② **Security Mechanism:**
A process that is designed to detect, prevent, or recover from a security attack.

③ **Security Service:**
A processing or communication service that enhances the security of the data processing systems and information transfers of an organization.

③ Security Services:

X.800 defines a security service that is provided by a protocol layer of communicating open systems. SS is processing or communication services that is provided by a system to give a specific kind of protection to system resources.

a) **Authentication:**
The assurance that the communicating entity is that one that it claims to be.

a) Peer Entity Authentication - used in association with a logical connection to provide confidence in the identity of the entities connected.

b) Data-origin Authentication - In a connectionless transfer, provides assurance that the source of received data is as claimed.

2) Access control:
The prevention of unauthorized use of a resource.

3) Data confidentiality:
The protection of data from unauthorized disclosure.

(a) connection confidentiality:
The protection of all user data on a connection.

(b) connectionless confidentiality:
The protection of all user data in a single data block.

(c) selective-field confidentiality:
The confi. of selected fields within the user data on a connection or in a single data block.

(d) traffic-flow confidentiality:
The protection of the information that might be derived from observation of traffic flow.

4) Data Integrity
The assurance that data received are exactly as sent by an authorized entity (no modification, insertion, deletion)

a) Connection Integrity with Recovery:
Provide for the integrity of all user data on a connection and detects any modification, insertion, deletion or replay of any data within an entire data sequence, with recovery attempted.

b) Connection Integrity without Recovery.
As above, but provides only detection without recovery.

c) Selective - Field connection Integrity:
of selected fileds within user data of data block transfer over connection.

d) connectionless Integrity:
Provide integrity of a single connectionless data block and may take the form of detection of data modi - Fication.

e) Selective Field Connectionless Integrity:
Provides for the integrity of selected fields within a single connection - less data block.

(5) Non Repudiation:
Provide protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

(a) non repudiation, origin:
Proof that the message was sent by the specified party.

(b) non repudiation, Destination:
Proof that the message was received by

the specified party.

(4) Security Mechanisms:
The mechanism are divided into TCP (or) an application layer protocol.

(1) Specific security mechanisms:
May be incorporated into the appropriate protocol layer in order to provide some of the OSI security service.

① Encipherment → use of mathematical algorithms to transform data into a form that is not readily intelligible.

② Digital signature → Data appended to or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source & integrity of the data unit & protect against forgery.

③ Access control:
A variety of mechanisms that enforce access rights to resources.

④ Data Integrity:
A variety of mechnisms used to assure the integrity of a data unit.

⑤ Authentication Exchange:
A mechanism intended to ensure the identity of an entity by means of information exchange.

⑥ Notarization: The use of a trusted third party to assure certain properties of a data.

⑦ Traffic padding: The insertion of bits into gaps in a data stream to frustrate traffic attempt.

(2) Pervasive security mechanisms.
Mech. that are not specific to any particular OSI security service or protocol layer.

① Trusted Functionality:
That which is perceived to be correct with respect to some criteria

② Event Detection:
Detection of security-relavant events.

③ Security Audit Trail:
Data collected & potentially used to facilitate a security audit, which is an independent review & examination of system records and activities.

⑤ A Model for Network Security:

A message is to be transferred from one party to another across some sort of internet service.

Two parties, who are the principal (Mutual) in this transaction must cooperate for the exchange to take place.

logical channel:

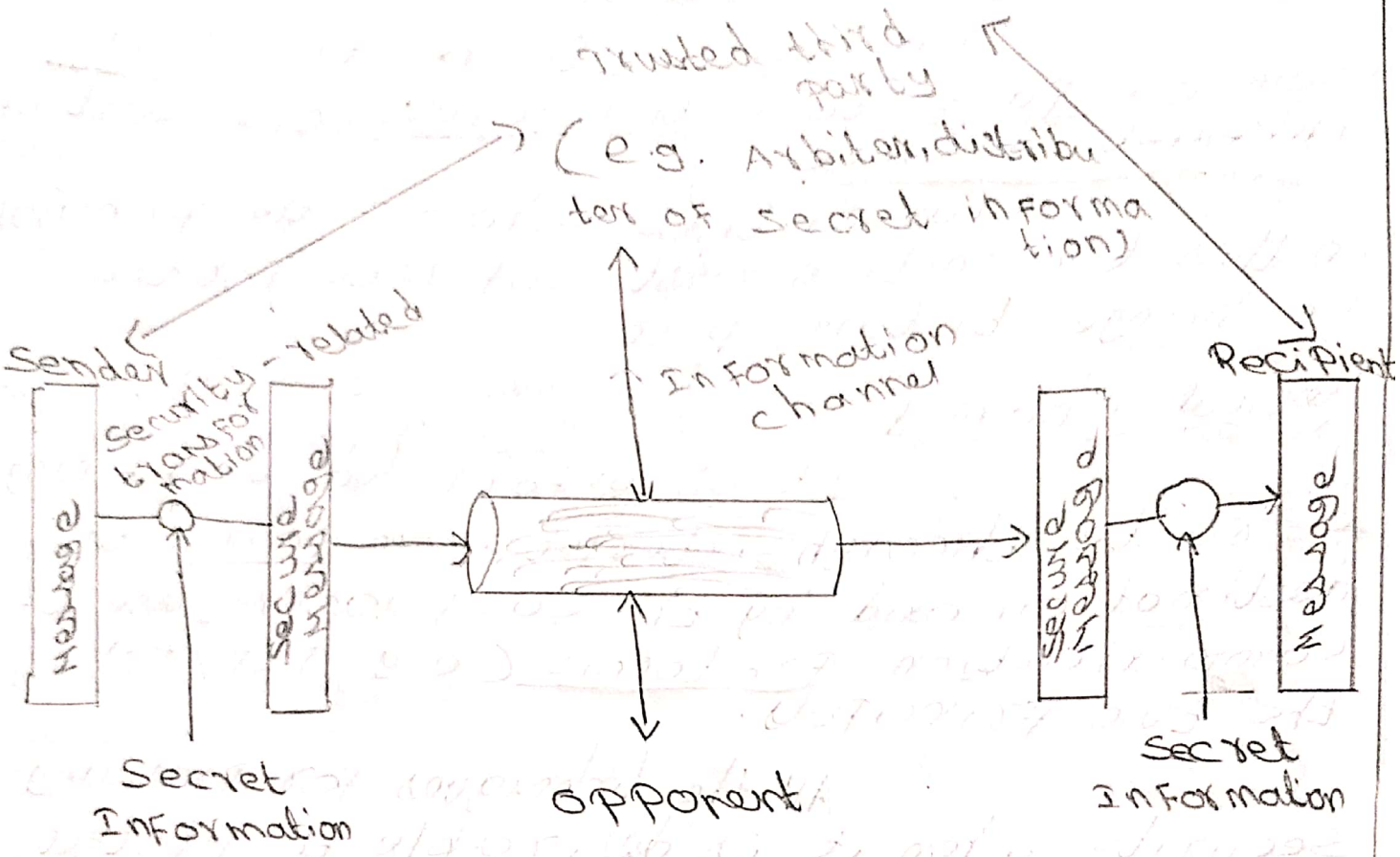
It is established by defining a route through internet from source to destination and by the cooperative use of communication protocols (e.g. TCP/IP) by the two principals.

All the techniques for providing security when it is desirable to protect the information transmission from an opponent who may present a threat to confidentiality.

① A security-related transformation on the information to be sent.

② some secret information shared by the two principals and it is unknown to the opponent.

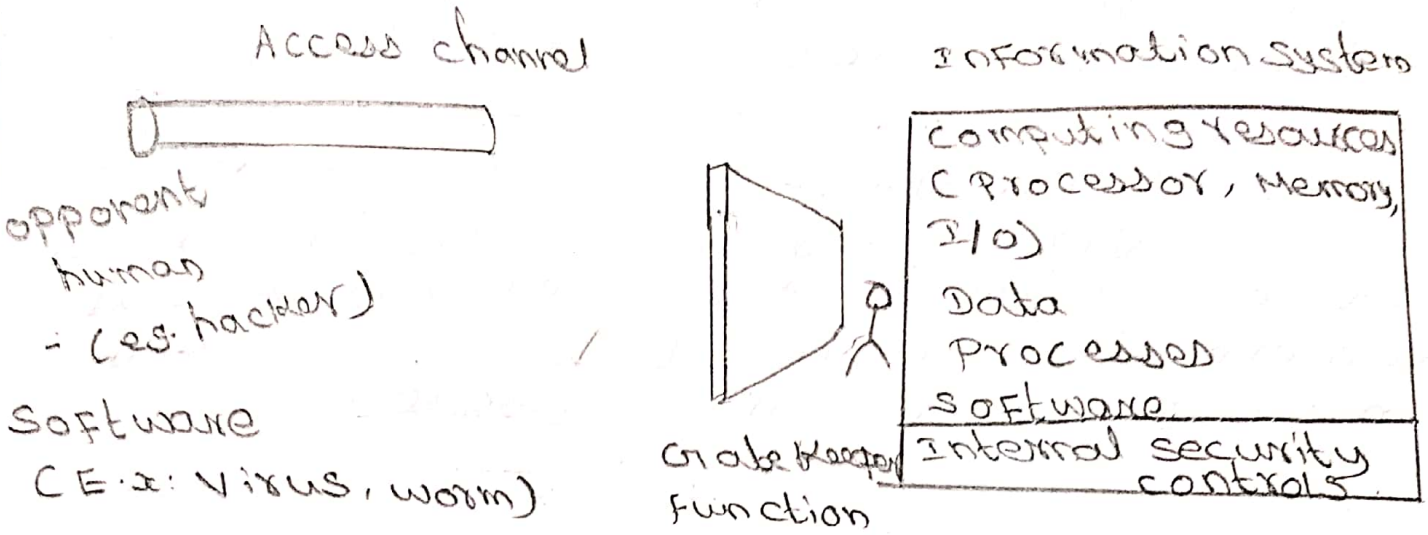
A trust third party may be needed to achieve secure transmission. Third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent. or a third party may be needed to arbitrate disputes between the two principals concerning the authenticity of message transmission.



Model of Network Security

There are four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation.
2. Generate the secret information to be used with the algorithm.
3. Develop methods for the distribution and sharing of the secret information
4. Specify a protocol to be used by the two principals that makes use of security algorithm.



Gate keeper Function protects the data from opponents.

opponent:

① Hacker: The hacker can be someone who, with no malign intent, simply gets satisfaction from breaking & entering a computer system.

② Intruder: The intruder can be a disgruntled employee who wishes to do damage or a criminal who seeks to exploit computer assets for financial gain
eg: obtaining credit card numbers.

③ Threats:- Another type of unwanted access is the placement in a computer system of logic that exploit vulnerabilities in the system that can affect application programs as well as utility programs, such as editors & compiler.

Two types of threats:

① Information access threats: Intercept or modify data on behalf of users who should not have access to that data.

of users who should not have access to.

② service threats: Exploit service flows in computers to inhibit use of legitimate users.

Software attacks:

Virus and worms are introduced into a system by means of a disk that contain the unwanted logic concealed in otherwise useful software.

---

second part of 1st unit

Cryptography concepts and Techniques:

① Introduction:

Symmetric encryption also referred to as conventional encryption or) single key encryption

Definitions:

Plaintext:

This is an original message is known as plaintext

ciphertext:

The coded message is called the ciphertext.

Encryption: The process of converting from plaintext to ciphertext is known as encryption.

Decryption: The process of restoring the plaintext from the ciphertext is decryption.

Cryptography: The area of study which constitute the schemes used for encryption is known as cryptography such a scheme is known as cryptographic system or a cipher.

Cryptanalysis: Techniques used for deciphering a message without any knowledge of the enciphering details of an into the area of cryptoanalysis.

Cryptology: The area of cryptography and cryptanalysis together are called cryptology.

② Symmetric cipher model:

A symmetric encryption scheme has five ingredients:

① Plaintext: It is the original intelligible message (or) data that is fed into the algorithm as input.

② Encryption algorithm: The encryption algorithm performs various substitutions & transformation on the plain text.

③ Secret key: - It is also input to the encryption algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exctract substitution and transformations performed by the algorithm depend of the key.

④ Cipher text: This is the scrambled message produced as output. It depends on the plaintext & the secret key.

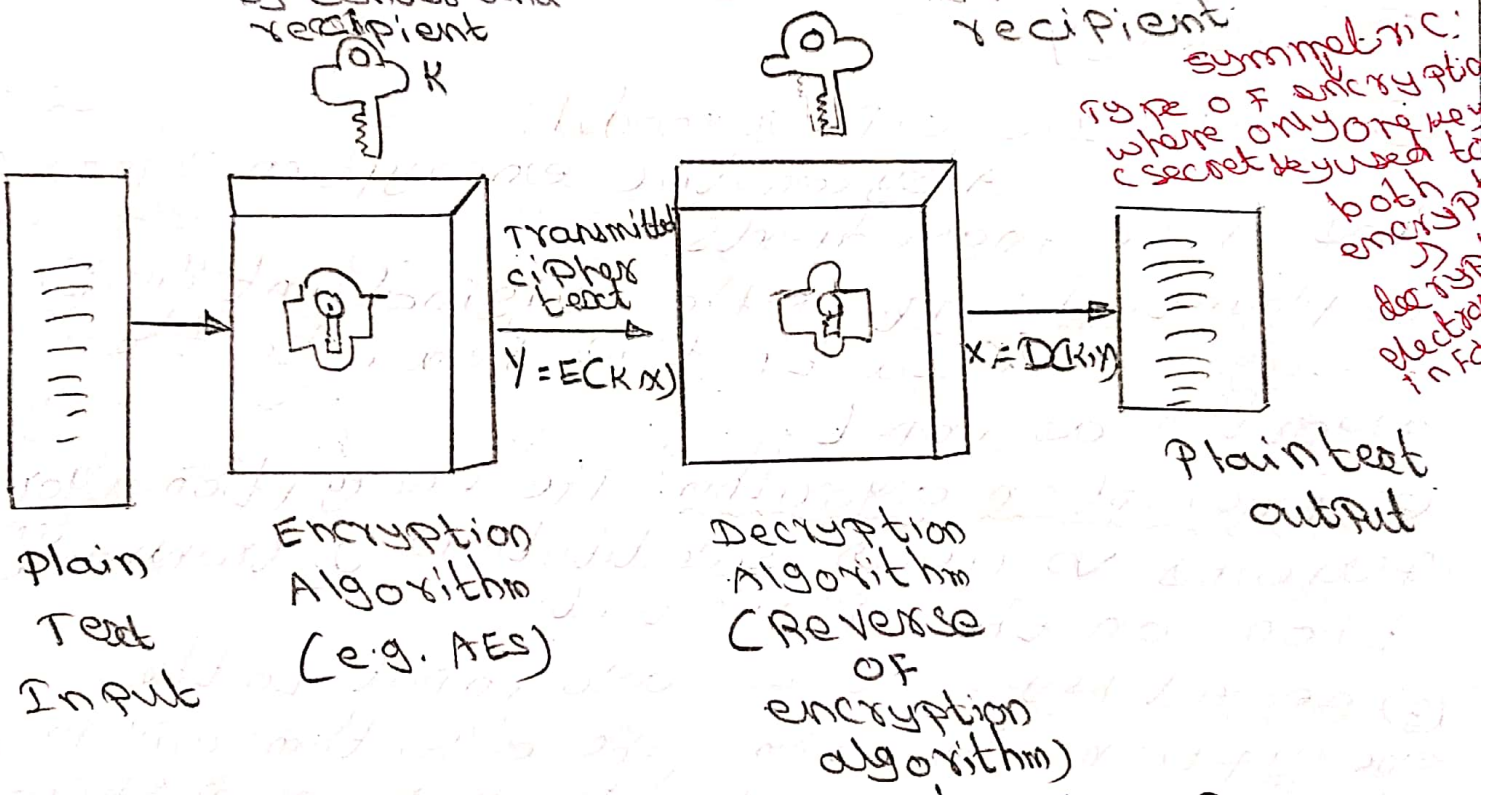
For a given message, two different keys will produce two different ciphertexts.

It is random stream of data, it stands, unintelligible.

⑤ Decryption algorithm: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

Two requirements for Secure use of conventional encryption.

simplified model of symmetric encryption.



symmetric: type of encryption where only one key (secret key) used to both encryption & decryption electronic

Two requirements for secure use of conventional encryption.

1. A strong encryption algorithm:
The opponent even if he knows the algorithm and has access to one or more ciphertexts would be unable to decipher the ciphertext (or) figure out the key.

2. A secret key known only to sender/receiver

Advantage or importance of symmetric key.

It is impractical to decrypt a message on the basis of the ciphertext + knowledge of the encryption/decryption algorithm.

we must kept the key secret.

(3) cryptography:

① The type of operations used for transforming plaintext to ciphertext:

All encryption algorithms are based on two general principles;

(i) Substitution and transposition

(a) Substitution:- In which each element in the plaintext is mapped into another element.

(b) Transposition: In which elements in the plaintext are rearranged.

② The number of keys used:

If both sender and receiver use the same key, the system referred to as symmetric, single key, secret key, or conventional encryption.

If the sender and receiver use different keys, the system is referred to as asymmetric, two key, or public key encryption.

③ The way in which plaintext is processed:

(a) Block cipher: A block cipher processes the input one block of elements at a time, producing an output block for each input block.

⑤ Stream cipher: The processes the input elements continuously, producing output one element at a time, as it goes along.

Cryptanalysis and Brute-Force Attack:

The objective of attacking an encryption system is to recover the key in use rather than simply to recover the plaintext of a single ciphertext.

Two general approaches to attacking a conventional encryption scheme

① Cryptanalysis: cryptography attack rely on the nature of the algorithm plus know-ledge of the general characteristics of the plaintext.

The attack attempt to deduce a specific plaintext or to deduce the key being used.

② Brute-Force Attack: The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

→ A source produces a message in plaintext $X = [X_1, X_2, \ldots X_M]$ for encryption, a key of the form $K = [K_1, K_2, \ldots K_J]$ is generated. If key is generated at source then it must also be provided to the destination by secure channel.

The third party generate the key & securely deliver it to both source & destination.

Also known as Public key & Asymmetric
↳ Encrypts & decrypts the data using 2 separate yet mathematically connected keys

Mathematical notations.

$Y = E(K, X)$

Y - ciphertext
K - encryption key
X - message
D - Decryption

$X = D(K, Y)$

④ Steganography:

The plaintext message may be hidden in one of two ways. The method of Steganography conceal the existence of the message, whereas the methods of cryptography render the message unintelligible to outsiders by various transformation of text.

Various techniques used in steganography are

① character marking: selected letters of printed or type written text are overwritten in pencil. The marks are ordinarily not visible unless the paper is held at an angle to bright light.

② Invisible ink: A number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper.

③ Pin Punctures: Small pin punctures on selected letters are ordinarily not visible unless the paper is held up in front of a light. a light.

④ Type writer correction ribbon: used between lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light.

Advantage: It can be employed by parties who have something to loss should the fact of their communication.

⑤ Substitution techniques:

A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.

If plaintext is viewed as a sequence of bits, then substitution involves replacing ~~each~~ plaintext bit patterns with ciphertext bit patterns.

① ceaser cipher:

It is the simplest, use of Substitution cipher was by Julius ceaser. The cc involves replacing each letter of the alphabet with the letter standing three places further down the alphabet.

eg:

Plain : a b c d e f g h i j k l m n o p q r s t
D E F G H I J K L M N O P Q R S T U V W

u v w x y z
X Y Z A B C

Eg:

Plain: Meet me after the toga party

PHHW PH DIWHU WKH WRJD SDUWB

Thee can assign a numerical equivalent to each letter:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

u	v	w	x	y	z
20	21	22	23	24	25

Then the algorithm can be expressed as follows: For each plaintext letter p, substitute the cipher text letter C:

$$C = E(3, p) = (p + 3) \bmod 26.$$

A shift may be of any amount, so that the general ceaser algorithm is

$$C = E(k, p) = (p + k) \bmod 26.$$

weakness: predictability.

② Monoalphabetic Ciphers:

with only 25 possible key, tk Caesar cipher is far from secure.

A dramatic increase in the key space can be achieved by allowing an arbitary substitution.

permutation: A permutation of a finite set of elements 'S' is an ordered sequence of all the elements of S, with each element appeared once.

ex: $S = \{a, b, c\}$

six permutations ~~are~~ $S = \{abc, acb, bac, bca, cab, cba\}$.

each plain text letter maps to different random cipher text.

possible key size is very large.

i.e 26! (or) 4×10^{26} possibilities.

ex: →

26 alphabet - $(26 \times 25 \times 24 \times 23 \times \cdots 2)$

Ex:

A	B	C	D
C	Z	S	G

For A → all possible 26 letters = 26!

A → A, B, C, D, E ··· Z

$P = CAB$

$= SCZ$

For single alphabet, writing all the possible combination of letters.

Drawback: Monoalphabetic ciphers are easy to break because they reflect the frequency data of original alphabet.

③ Playfair cipher:

The best known multiple-letter encryption cipher is the playfair. The playfair algorithm is based use of 5x5 of letters constructed using a keyword.

consider a table with 5x5 rows & columns.

Plaintext → HELLO

Key → NETWORK

Cipher Text - ?

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

To Fill the table:-

It repeated letters are there then igore write unique letters.

① Fill with the Key

② write the alphabets

E is there, so write F

③ It is 5×5 Matrix so only 25 letters will come, so, in general I, J are merged I/J

Rules for converting plaintext to cipher text.

① Divide plaintext to Pair of letters

② Differentiate repeated letters in the Pair with dummy letter.

③ IF Two plain text letters are in same row, of the matrix, replace them with right most letters.

④ IF two plain text letters are in same column, then replace with beneath letters.

⑤ IF plaintext letters are in different rows & column, replace with diagnol position.

step1: Divide plain text into pair of letters

HE/LL/O

step2: Find whether each pair have repeated letters.

HE/LL/O

Repeated letters, differentiate with 'x' ← dummy character

EW|OM|KC
WORLDX

HELXLO
T
U
HE|LX|LO

Step3:- consider

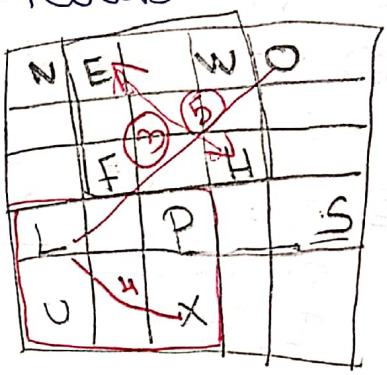
HE → are in the different row, column
H → 4th column
E → 2nd column

HE → replaced with diagonal letters.

HE → FW

for LX. LX → PU

LO → SN



ciphor text for
HELLO → WFUPNS

Example: 2

Plaintext → BALLON
key → NETWORT

ciphortext :-

BA|LL|ON
↑
BA|LX|LO|ON

BA → CB
LX → UP
LO → NS
ON → NE

ciphortext: CBUPNSNE

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

Play Fair cipher

The best known multiple-letter encryption cipher is the play fair, The play fair algorithm is based on the use of 5×5 matrix of letters constructed using a keyword.

Example:

Plaintext: WORLD
Key : SECURE
ciphertext: ?

→ Fill the key in the 5×5 matrix, while filling ignore the repeated letters. I/J is considered as single element.

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

I/J is considered as single Element

Plain text is encrypted two letters at a time, according to the following rules:

1. Divide plaintext into pair of letters
2. Repeating plaintext letter that are in the same pair are seperated with a Filler letter, Such as x.
3. IF two plaintext letters that Fall in the same row, then replace the letter with the letter right to it.
4. IF two plaintext letters that Fall in the same column, then replace them wit the letter benath, IF top of the column circularly Following the last.
5. Two plain text letters are in different row/ in different column then marked

rectangle, and write the letters opposite to the plaintext.

PT: WORLD

WO | RL | DX

① WO - Same column in matrix, so write the element beneath it.

W → E

O → W

② RL - are in different column, row

∴ make a rectangle & write the letter opposite to it.

R - U

L - M

iii) DX - Same column ∴ write the letters below it

D - K

X - C

∴ WORLD

↓ ↓ ↓ ↓ ↓

EWUKC

cipher text:

Decryption: same procedure but 2 rules to be followed:

① two plaintext letters on same row, replace them with left side letters

② two plaintext letters on same column replace them with the above letter

. ciphertext: EW/UM/RC

EW - same column, write letter above it.

W
O

UM → different rows/column, so make rectangle & write the letters opposite to it.

RC → same column, write letter above it.

D X

∴ plaintext for E W U M R C is
W O R L D X

① Try some examples:

plaintext: HELLO

KEY: NETWORK

② plaintext: BALLOON

key: NETWORK.

⑥ Transposition techniques:

The simplest transposition technique is railfence. In Railfence in which the plain text is written down as a sequence of diagonals and then read off as a sequence of rows.

Ex: depth 3

CNS class is important.

	C			C			S			S		P		E	
		N			I			S			I		O		G
			S			G			I		M			R		N

To encrypt start with the column 1, because write down all the letters in treat column.

encryption. First we start with 1st row then 2nd row → 3rd row.

ccssptENISioasaimrn

decryption- Read the letters in zig-zag

Rail Force order

Continue (missed) in substitution technique:

Hill Cipher:

1) Encrypts a group of letters called Polygraph
2) It can used for diagraph & trigraph.
3) use of mathematical knowledge.
4) key → plaintext should be in the form of square matrix.
5) To encrypt the message, the form -ula is.

$$C = KP \bmod 26$$

Formulae

$$C = E(K, P) = PK \bmod 26$$
$$P = D(K, C) = CK^{-1} \bmod 26$$
$$= PKK^{-1} = P$$

C, P → plaintext is a row vector of length 3

K → key is a 3×3 matrix representing the encryption key.

Encryption:

choose a key and key matrix is a square matrix.

0 1 2 3 4 5 6
A B C D E F G

ex: key = $\begin{bmatrix} 2 & 3 \\ 3 & 0 \end{bmatrix}$ key $\begin{bmatrix} C & D \\ D & G \end{bmatrix}$ Plain text: ATTACK.

2×2 matrix = $\begin{bmatrix} A \\ T \end{bmatrix} \begin{bmatrix} T \\ A \end{bmatrix} \begin{bmatrix} C \\ K \end{bmatrix}$ ...

① $\begin{bmatrix} A \\ T \end{bmatrix} = \begin{bmatrix} 0 \\ 19 \end{bmatrix}$

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

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

$C = KP \bmod 26$ [Ciphertext for $\begin{bmatrix} A \\ T \end{bmatrix}$]

$= \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 0 \\ 19 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 2\times0 + 3\times19 \\ 3\times0 + 6\times19 \end{bmatrix} = \begin{bmatrix} 57 \\ 114 \end{bmatrix} \bmod 26 = \begin{bmatrix} 57 \,\%\, 26 \\ 114 \,\%\, 26 \end{bmatrix} = \begin{bmatrix} 5 \\ 10 \end{bmatrix} = \begin{bmatrix} F \\ K \end{bmatrix}$

② $C = KP \bmod 26$ [Plain text $\begin{bmatrix} T \\ A \end{bmatrix} = \begin{bmatrix} 19 \\ 0 \end{bmatrix}$

$= \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 19 \\ 0 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 2\times19 + 3\times0 \\ 3\times19 + 6\times0 \end{bmatrix} \bmod 26 = \begin{bmatrix} 38 \\ 57 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 38 \,\%\, 26 \\ 57 \,\%\, 26 \end{bmatrix} = \begin{bmatrix} 12 \\ 5 \end{bmatrix} = \begin{bmatrix} M \\ F \end{bmatrix}$

③ Ciphertext for $\begin{bmatrix} C \\ K \end{bmatrix} = \begin{bmatrix} 2 \\ 10 \end{bmatrix}$

$C = KP \bmod 26$

$C = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 2 \\ 10 \end{bmatrix} = \begin{bmatrix} 2\times2 + 3\times10 \\ 3\times2 + 6\times10 \end{bmatrix} = \begin{bmatrix} 34 \\ 66 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 8 \\ 14 \end{bmatrix} = \begin{bmatrix} I \\ 14 \end{bmatrix}$

Ciphertext for Attack $= \begin{bmatrix} F \\ K \end{bmatrix} \begin{bmatrix} M \\ F \end{bmatrix} \begin{bmatrix} T \\ A \end{bmatrix} = FKMFIO$

Decryption [Hill cipher)

To encrypt $C = KP \bmod 26$

To decrypt → Find inverse of key matrix^{-1}

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

eg plain → ATTACK , key $K = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$

cipher → FKNFIO

$C = FK \quad MF \quad IO$

$K^{-1} \quad \frac{1}{|K|} \text{adj}(K)$ → determinant value.

determinant of matrix $d = \begin{vmatrix} a & b \\ c & d \end{vmatrix}$

$$d = |ad - bc|$$

e.g $d = \begin{vmatrix} 2 & 3 \\ 3 & 6 \end{vmatrix} = |12 - 9| = 3$ ∴ determinant value = 3

Now Find Multiplicative inverse of the determinant.

i.e. $dd^{-1} \equiv 1 \bmod 26$ (Identity matrix)

So $3 * d^{-1} \equiv 1 \bmod 26$ [26 means $(3 * d^{-1}) \bmod 26 = 1$

So $d^{-1} = 9$

use hit → trial method

$3 * d^{-1} \bmod 26 = 1$

$3 * 9 \bmod 26 = 1$

$27 \bmod 26 = 1$

Now we will Find adjacent of the matrix

Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ then $\text{adj}(A) =$

$$\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Here $K = \begin{bmatrix} 23 \\ 36 \end{bmatrix}$, adj(K) = $\begin{bmatrix} 6 & -3 \\ -3 & 2 \end{bmatrix}$

Before decryption, we have to remove -ve no.

$$adj(K) = \begin{bmatrix} 6 & -3+26 \\ -3+26 & 2 \end{bmatrix} = \begin{bmatrix} 6 & 23 \\ 23 & 2 \end{bmatrix}$$

$$adj(K) = \begin{bmatrix} 6 & 23 \\ 23 & 2 \end{bmatrix} \text{ and } d^{-1} = 9$$

Now $K^{-1} = \frac{1}{|K|} adj(K)$

$= |K^{-1}| \, adj(K) = d^{-1} \, adj(A)$

↑ determinant value.

$$K^{-1} = 9 \begin{bmatrix} 6 & 23 \\ 23 & 2 \end{bmatrix} = \begin{bmatrix} 54 & 207 \\ 207 & 18 \end{bmatrix}$$

Now find its modulo 26

$$K^{-1} = \begin{bmatrix} 54 & 207 \\ 207 & 18 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix}$$

$$\therefore K^{-1} = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix}$$

Hill cipher decryption. Now we can start decryption.

Cipher : EKNFIO

$C = \begin{bmatrix} I \\ K \end{bmatrix} = \begin{bmatrix} 5 \\ 10 \end{bmatrix}$

plaintext. $P = K^{-1} C \bmod 26 \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \begin{bmatrix} 5 \\ 10 \end{bmatrix} \bmod 26$

$P = \begin{bmatrix} 260 \\ 305 \end{bmatrix} \bmod 26 = \begin{bmatrix} 0 \\ 19 \end{bmatrix} = \begin{bmatrix} A \\ T \end{bmatrix}$

$C = \begin{bmatrix} N \\ F \end{bmatrix} = \begin{bmatrix} 12 \\ 5 \end{bmatrix}$

so corresponding plaintext is

$P = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \begin{bmatrix} 12 \\ 5 \end{bmatrix} \bmod 26 \quad \begin{bmatrix} 149 \\ 390 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 19 \\ 0 \end{bmatrix} = \begin{bmatrix} T \\ A \end{bmatrix}$

$C = \begin{bmatrix} I \\ O \end{bmatrix} = \begin{bmatrix} 8 \\ 14 \end{bmatrix}$

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

$P = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \begin{bmatrix} 8 \\ 14 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 16 + 25(14) \\ 25(8) + 18(14) \end{bmatrix} \bmod 26$

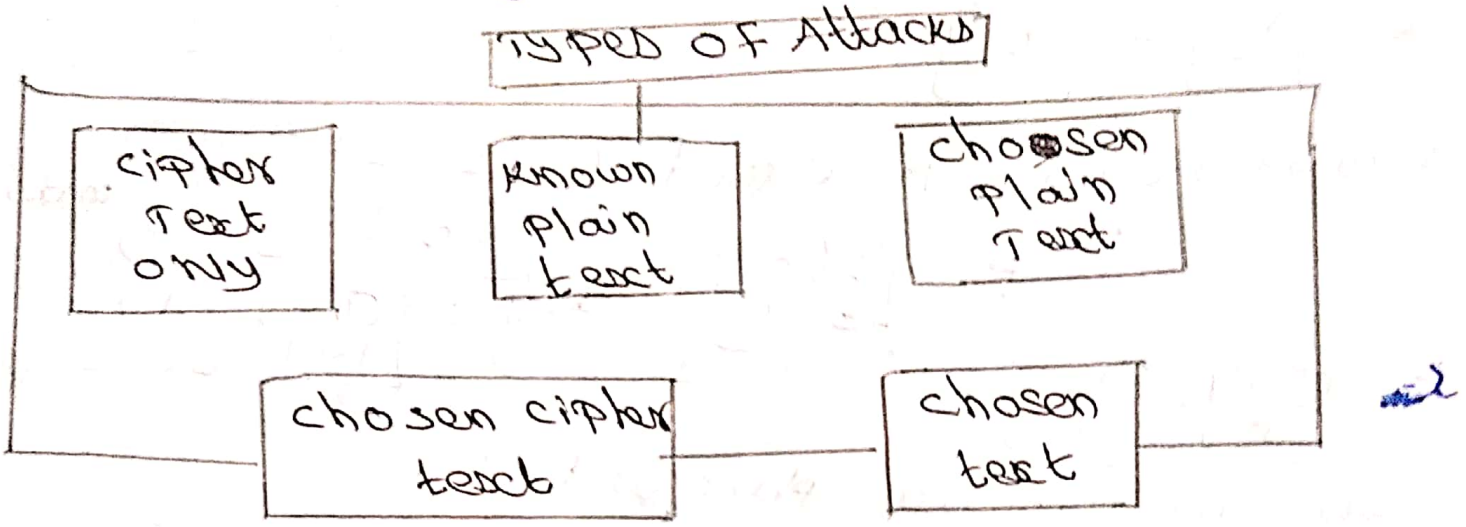
$P = \begin{bmatrix} 366 \\ 452 \end{bmatrix} \bmod 26$

$P = \begin{bmatrix} 2 \\ 10 \end{bmatrix} = \begin{bmatrix} C \\ K \end{bmatrix}$

plain text : ATTACK.

① Possible Types of Attacks

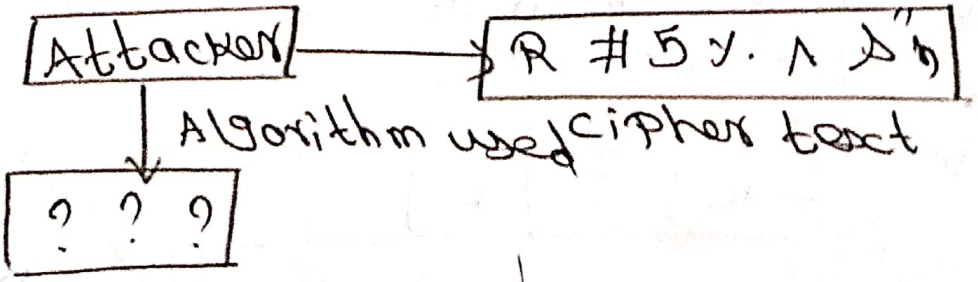
Five possibilities for an attack on this message



① Cipher-text only Attack:

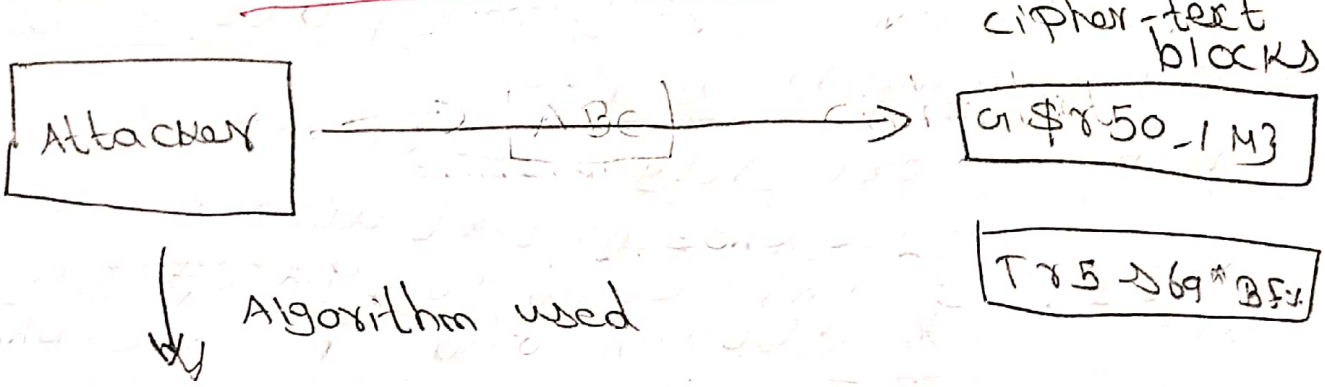
In this type of attacker does not have any clue about the plaintext. She has some or all of the cipher text. The attacker analyzes the cipher text at leisure to try and figure out the original plaintext.

Based on the frequency of letters (e.g. The alphabets very common english) the attacker makes an attempt to guess the plain text. Obviously, the more cipher text, text available to the attacker. More are the chances of successful attack.



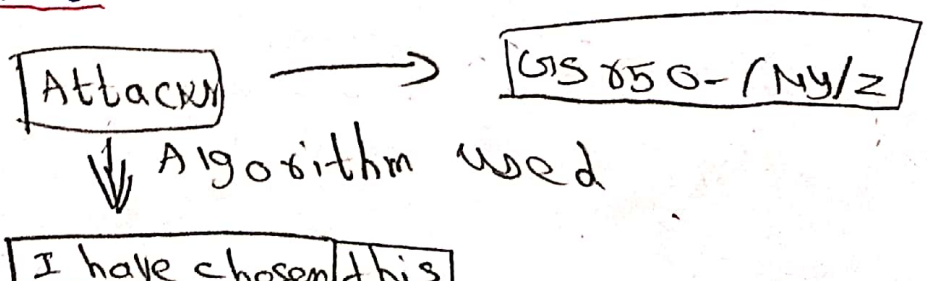
② Known Plain text Attack:

In this case, the attacker known about some pairs of plain text and corresponding cipher text for these pairs. Using this information, the attacker tries to find other pairs and therefore know more and more of the plain text.



③ Choosen Plain text Attack:

The attacker selects a Plaintext block, and tries to look for the encryption of the same in the cipher text. Here, the attacker is able to choose the message to encrypt. Based on this, the attacker intentionally picks patterns of cipher text that result in obtaining more information about the key.

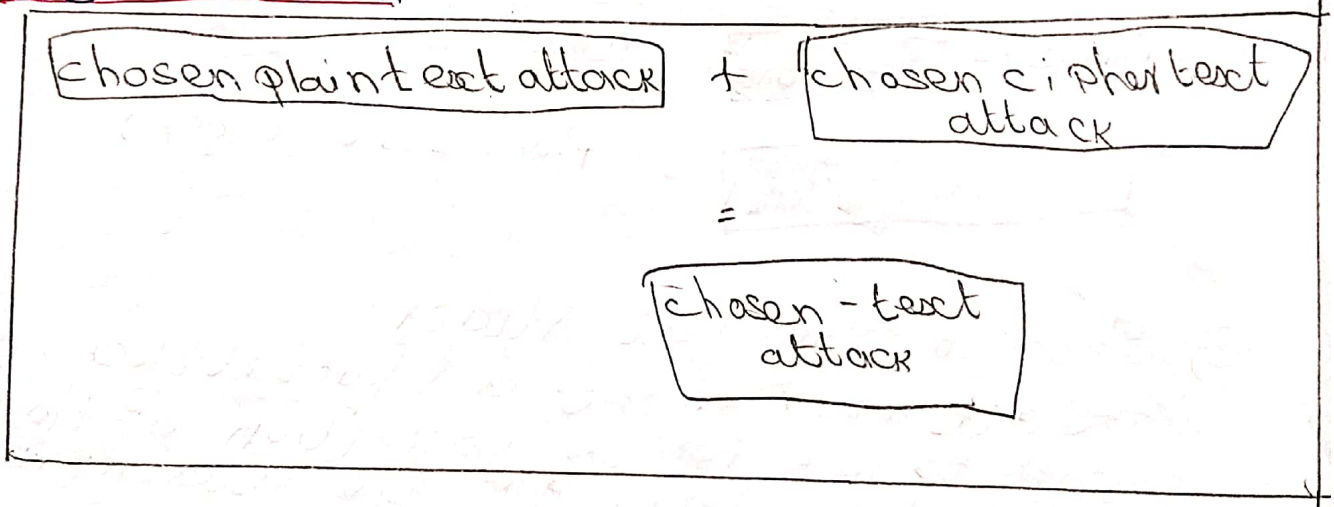


4. Chosen cipher-Text Attack.

In the chosen cipher-text attack, the attacker knowns the ciphertext to be decrypted, the encryption algorithm that was used to produce this ciphertext, and the corresponding plain-text block. The attacker's job is to discover the key used for encryption. However, this type of attack is not very commonly used.

5. Chosen-Text Attack

The chosen-text attack is essentially and combination of chosen plain-text attack and chosen cipher-text attack.



⑧ Key range and Key size:

The concept of key range and key size are related to each other.

Key range: key range is total no. of keys from smallest to largest available key.

An attacker usually is armed with the knowledge of the cryptographic algorithm and the encrypted message, so only the actual key value remains the challenge for the attacker.

Attacker write a code. Thus, only the actual value of the key remains a challenge for the attacker.

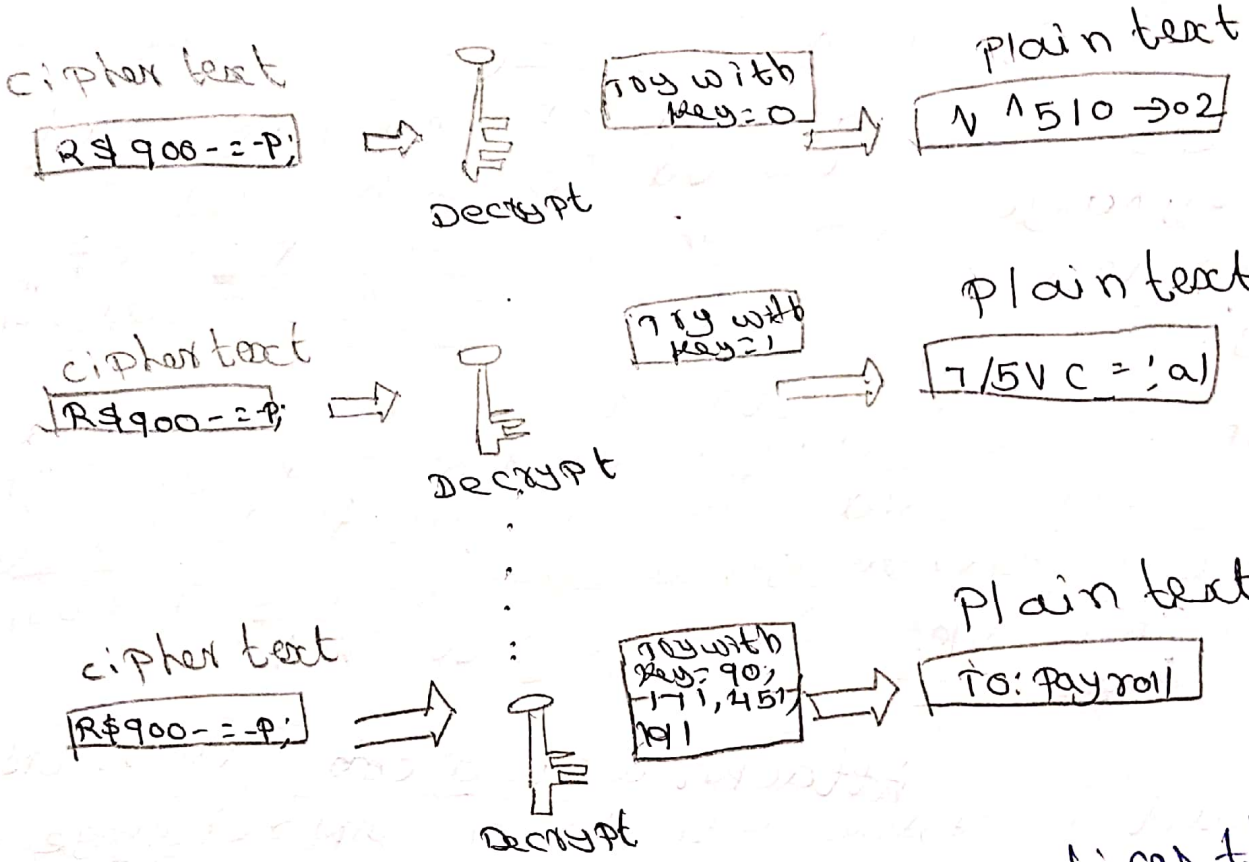
IF key is found, the attacker can resolve the mystery by working backwards to the original plain-text message.

we can consider brute-force attack here, which works on the principle of trying every possible key in the key range, until you get the right key.

How does the attacker determine if plain text and therefore the key, are the right ones? This can be determined depending on the value of the plain text

IF the plain text seems reasonable (very close to actual english word / sentence / number) it is highly probable that the plain text.

what corresponds to the cipher text.



If the attacker Notices that the decryption has yielded unintelligent plaintext, ~~but~~ ~~decryption~~ she continue the process with the next key in the sequence. Finally, she is able to find the right key with a value 90, 171, 451, 191. which yields the plain text :

Payroll

KeySize:

In computer ~~systems~~, the concept Key range leds us to the principles of key size.

How money in dollar, pound or rupees same like we measure the strength of cryptographic key with key size.

→ We measure key size ; b bits and represent it using the binary number system.

→ our key might be of 40 bits, 56 bits, 128, bits

→ The simplest level, the key size can just 1 bit. This means that the key can be either 0 or 1.

→ IF key size is 2:

00
01
10
11

→ IF key size is 3

4 2 1
000
001
010
011
101
110
111

In general, if an n-bit binary number has k possible states, an n+1 bit binary number will have 2k possible states.

key size on bits	time required 1% of keyspace	time required 50% of keyspace
56	1 second	1 minute
57	2 "	2 "
58	4 "	4 "
64	4.2 minute.	4.2 hours.
72	17.9 hours	44.8 hours
80	190.9 days	31.4 years.
90	535 years	321 centuries
128	146 billion	8 trillion

We can represent the possible key range using hexadecimal notation, and see visually how an increase in the key size increses the key range, and therefore, the comple -xity for an. TNS

Key size = 40 bits

00	00	00	00	00
00	00	00	00	01
...				
FF	FF	FF	FF	FF

Key size = 64 bits

00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	01
...							
FF	FF	FF	FF	FF	FF	FF	FF

Key size = 128 bits

00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	01
...															
FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF

clearly we can assume with reasonable confidence that a 128-bit key is quite safe. (because 2^{128} means about 340,000,000,000,000,000,000,000,000,000,000 Possible key!). to day computer capabilities. obviously, as computing power and technique improve, these number change. May be in a few years time, a 128 bit key will be cracked. Then we would need to rely on key of size at least 256 bits, or 512 bits.

One time Pad cipher: [Mixed substitution cipher]

Ex:

PT	C	O	M	E	T	O	D	A	Y
	2	14	12	4	19	14	3	0	24
key	N	C	B	T	Z	Q	A	R	X
	13	2	1	19	25	16	0	17	23
Total	15	16	13	23	44	30	3	17	47
subtract 26 if > 25	15	16	13	23	18	04	3	17	21
cipher Text	P	Q	N	X	S	E	D	R	W

Poly alphabetic ciphers:

1. set of related monoalphabetic substitution rules is used.
2. A key determines which particular rules is chosen for a given transformation.

key: deceptivedecept

P.T: wearediscovered

C.T: ZICVTWQNGRZGVTW

Express in numerically.

Key	3	4	2	4	15	19	8	21	4	3	4	2	4	15	19
PT	22	4	0	17	4	3	8	18	2	14	21	4	17	4	3
CT	25	8	2	21	19	22	16	13	6	17	25	6	21	19	22

Unit - II

Symmetric Key ciphers:

1. Block cipher principles
2. DES,
3. AES
4. Blowfish
5. RC5
6. IDEA
7. Block cipher operation
8. stream cipher
9. RC4

Asymmetric key ciphers:

1. Block cipher principles
2. cryptosystem
3. RSA algorithm
4. Elgamal cryptography
5. Diffie - Hellman key Exchang
6. Knapsack Algorithm

(1) Block cipher principles:

Block cipher:

Block cipher is an encryption/Decryption scheme in which a block of plaintext is treated as a whole and used to produce a cipher text block of equal length.

Most of the block cipher techniques are follow a common structure feistel structure.

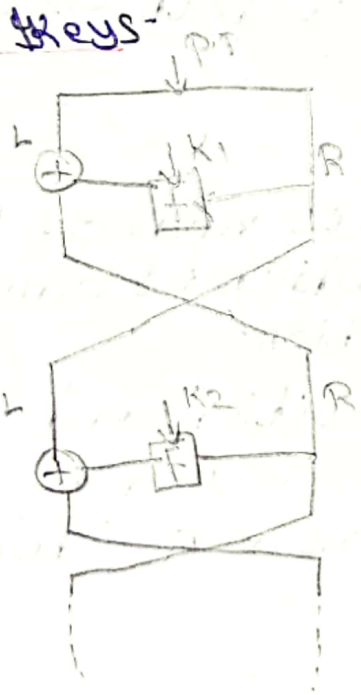
Feistel structure:

comparison of stream ciphers and block ciphers: i) Divide the plaintext into two equal halves.

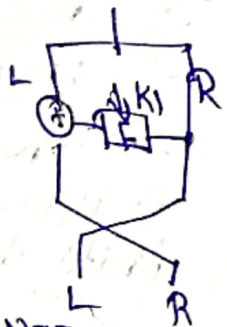
ii) For Right half apply any logical Function.

iii) In Function, we will use a separate key output for this function is X-ORed with left half.

iv) The process of converting plain text to ciphertext depends on number of rounds, processing is done in 10 rounds with 10 keys.



→ plain text → two equal halves.
→ No. of Rounds
→ No. of subkeys
→ swapping
→ Apply function to Right half
→ Result is X-ORed with left half & swapping is done.
→ This process repeats on no. of rounds.



Ex: DES Algorithm follows Feistel structure.

Fiestel proposed the use of a cipher that alternates Substitutions and permutations.

Substitution:

Each P.T element or group of elements is uniquely replaced by a corresponding C.T element or group of elements.

Permutation:

A sequence of P.T elements is replaced by a permutation of that sequence. That is no elements are added or replaced or deleted in the sequence, rather the order in which the elements appear in the sequence is changed.

2. THE DATA ENCRYPTION STANDARD:

It means Data encryption standard algorithm
symmetric key

→ it is a block cipher algorithm

→ published by NIST (National institute of standards and Technology)

→ It encrypt 64-bit block.

→ DES symmetric key algorithm: The same algorithm & key is used for both encryption & decryption.

→ key size is 56-bit

→ The encryption process is made of two permutations (P-boxes), which is called initial and final permutation.

→ DES uses both transposition and substitution and for the reason is sometimes referred to as a product cipher.

→ The input, output and key are each 64-bit long. The sets of 64-bits are referred to as blocks

→ The cipher consists of 16 rounds or iterations. Each round uses a seperate key of 48 bits [block]

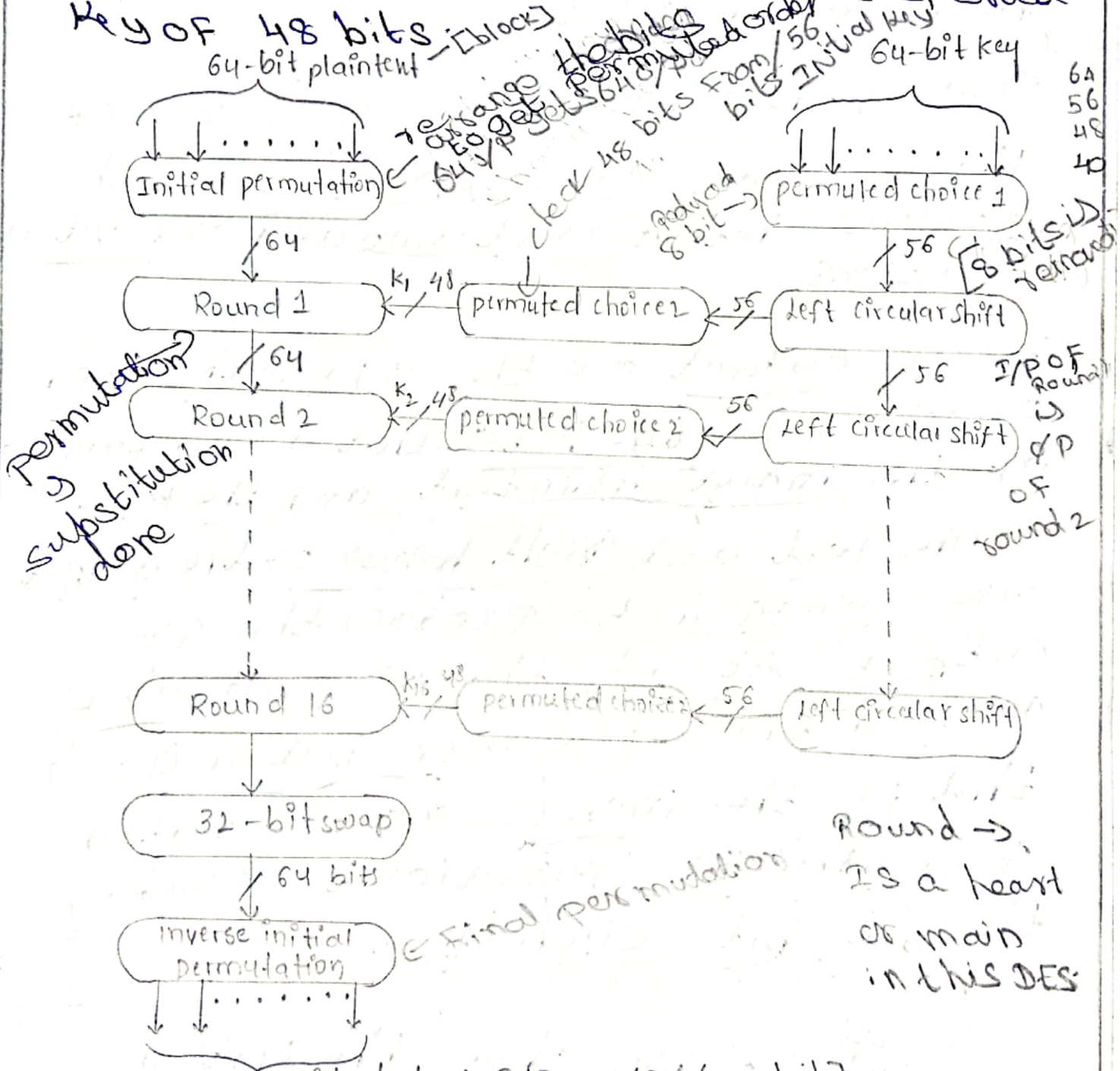


Figure 4.5 General Depiction of DES Encryption Algorithm

The figure shows DES encryption algorithm.

→ First the 64-bit plaintext passes through an initial permutation (IP) that rearranges the bits to produce the permuted input.

→ Then there is a phase consisting of 16 rounds of same function, which involves both permutation and substitution functions.

→ The output of the sixteenth round consits of 64-bits that are a function of the input plaintext and the key.

→ The left and right halves of the output are swapped to produce the pre-output. At last, the pre-output is passed through a permutation (IP^{-1}), that is the inverse of the Initial permutation function to produce the 64-bit ciphertext.

Initial permutation:

The table shows the initial permutation and its inverse. The input to a table consist of 64bits numbered from 1 to 64

The 64 entries in the permutation table contain a permutation of the numbers from 1 to 64. Each entry in the permutation table indicates the position of a numbered input bit in the output, which also consists of 64-bits.

Initial permutation (IP) table

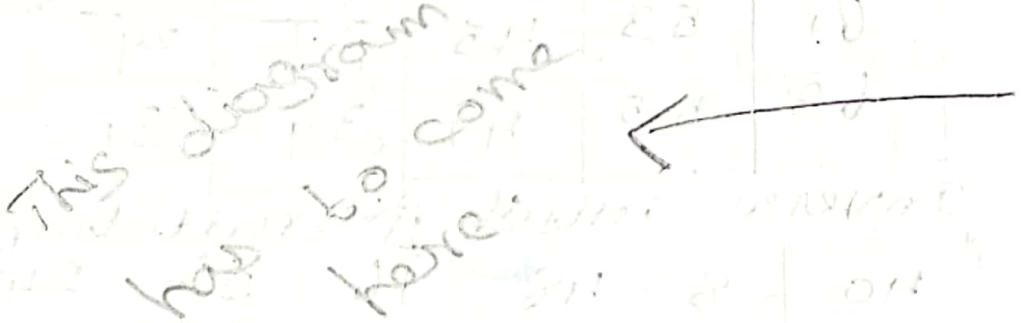
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Inverse initial permutation (IP^{-1})

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

Purpose of S-box in DES:

The below figure shows single round of DES algorithm. The left and right halves of each 64-bit intermediate value are treated as separate 32-bit quantities, labeled L and R.



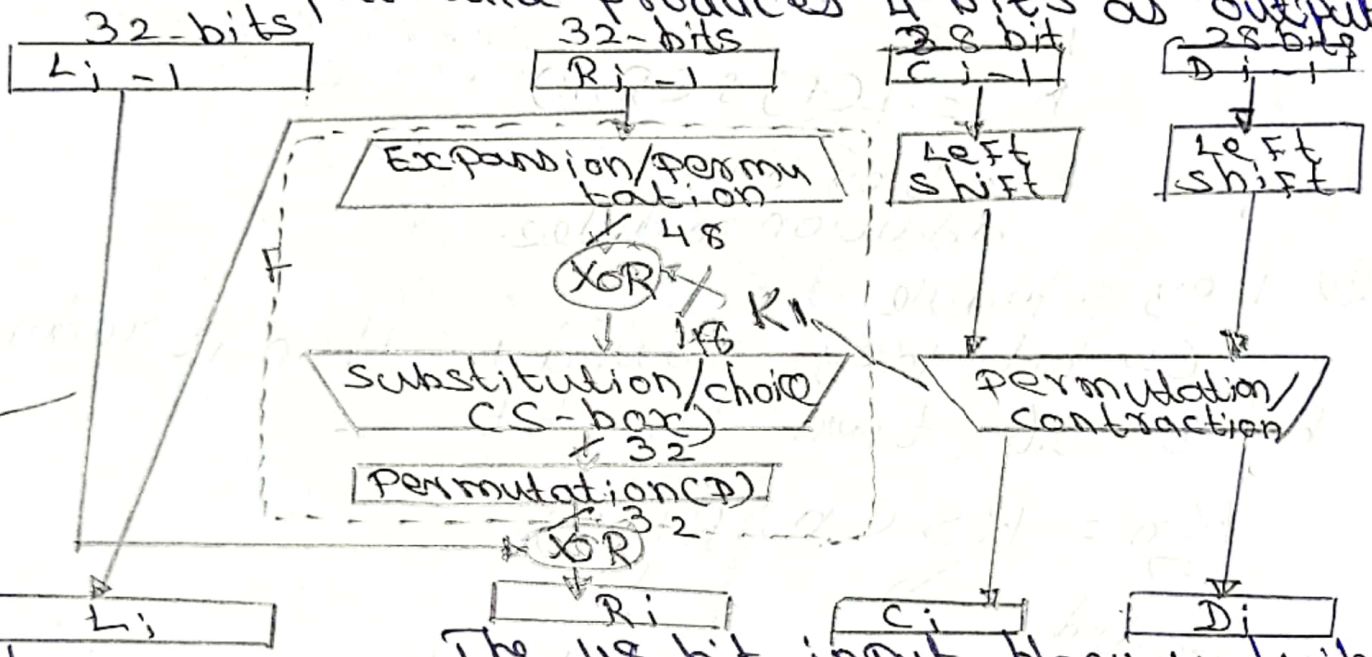
The overall processing at each round can be summarised in the formulae:

$$L_i = R_{i-1}$$

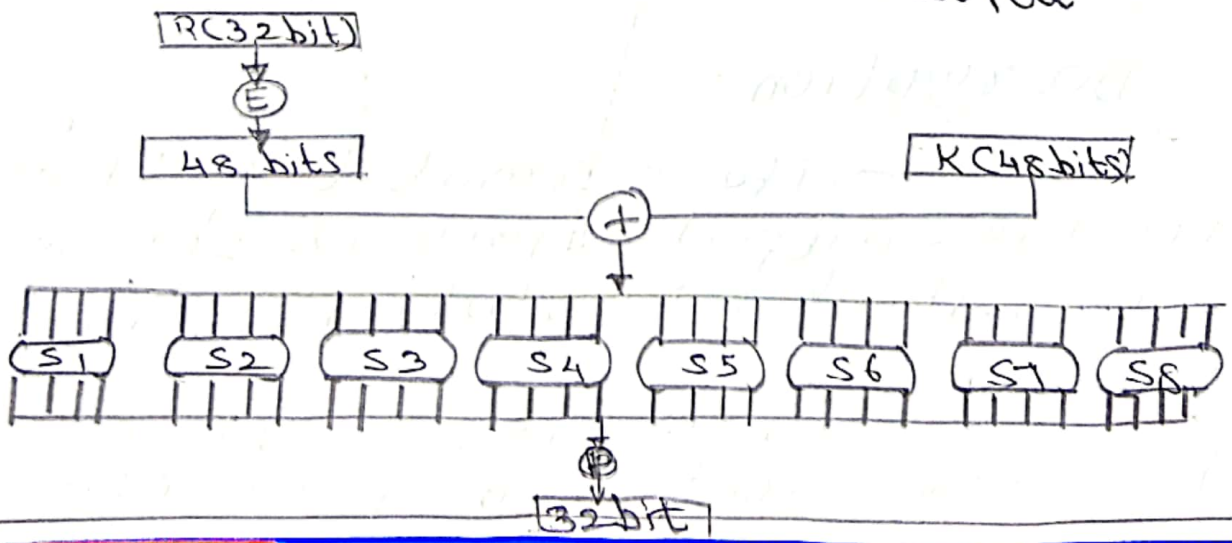
$$R_i = L_{i-1} \times F(R_{i-1}, K_i)$$

· The left output (Li) is simply copy of the right input (Ri-1). The right output (Ri) is the XOR of left input (Li-1) and right input (Ri-1) and key for this stage is Ki. In this stage, the substitution and permutation both functions are used.

The below figure shows role of S-boxes in the function F. It consists of set of eight S-boxes, each of which accepts 6 bits as input and produces 4 bits as output.



The 48 bit input block is divided into 8 sub blocks and each subblocks is given to a S-box. The S-box transforms the 6 bit input into a 4 bit output



DES Encryption and Decryption Method:

DES Encryption:

① Initial permutation: 64-bit i/p block → enciphered → permutation → Initial permutation

② Key dependent computation:
permuted input block → produce → pre-output block.
Input
The output L' R'
LR defined by
$L' = R$
$R' = L(+)\ f(R, K)$
(+) → bit by bit addition modulo2.

③ Key schedule:
64 bit key round, then it reduce by 8 56 then 48-bit

$K_n = KS(n, KEY)$
↗ permuted selection of bits from KEY
↘ Key schedule.
↖ Input and yield o/p as 48-bit block.

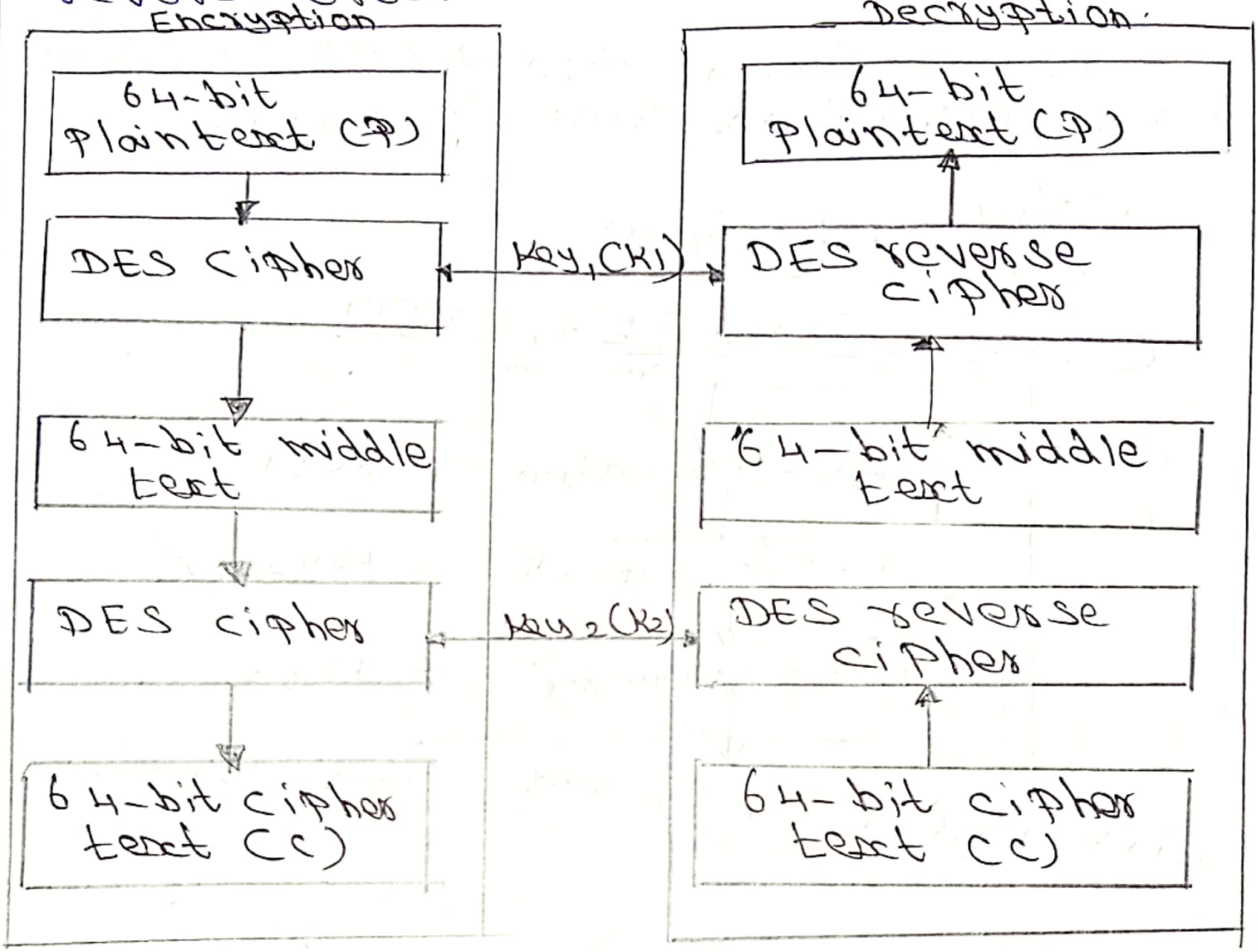
64 / 8 / 56 / 8 / 48

DES Decryption:

→ The permutation IP^{-1} applied to the pre-output block is the inverse of the initial permutation → apply → input.

→ key size or block key to be same what used in enciphered

must used for decipherment. → block in reverse order.



Triple DES:

→ Triple DES is simply another mode of DES operation.

→ It takes three 64-bit keys, for an overall key length of 192 bits.

→ procedure → encryption → same → repeate 3 times. [so it is Triple DES]

→ Triple DES used 2 or 3 keys.

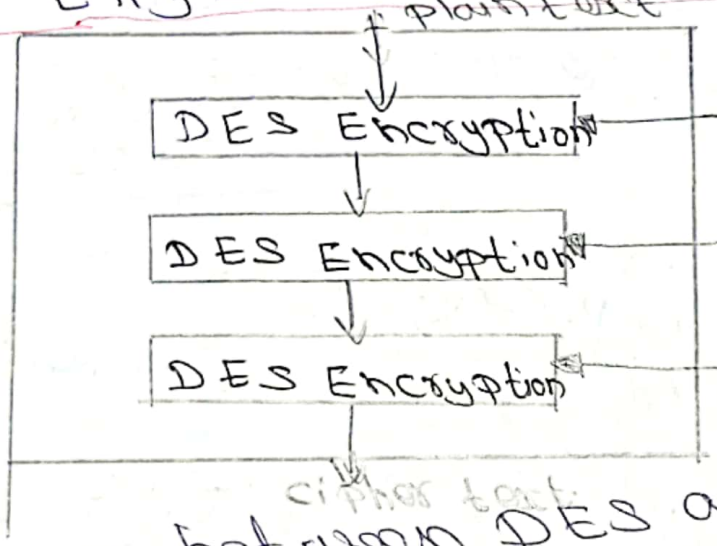
→ The data is encrypted first key K1 → decrypt with second key → K2 and Finally encrypted again → Third key (K3)

→ Brute-force attack is impossible in Triple DES.

→ Meet-in-middle attacks need 256 plain text - ciphertext pairs per key.

→ Cipher text produced as

$$C = E_{K3}[D_{K2}[E_{K1}[P]]]$$



Difference between DES and 3DES

Factor	DES	3DES
1) Key Length	56 bits	168 bits (3-key) 112 bits (2-key)
2) cipher type	symmetric block	symmetric block.
3) Block size	64 bits	64 bits.
4) Developed	1977	1978
4) Security	Better	Inadequate.
5) possible key	2^{56}	2^{112}
5) Rounds run algorithm	16	48

Advantages of DES Algorithm:

① 56 keys used 70 quadrillion possible key specific key cannot be identified easily.

② length of key increased → security also increase.

Limitation:

Symmetric → both sender & receiver must use same algorithm. key should not intercepted.

Techniques to Improve:

i) Multiple enciphering with DES.
ii) Extending the key expansion calculation

② Blowfish: [Replacement of DES or IDEA]

Blowfish was developed by Bruce schneier and has the reputation of being a very strong symmetric key cryptographic algorithm. According to schenier, Blowfish was designed with the following objectives in mind:

a) Fast: Blowfish encryption rate on 32-bit microprocessors in 26 clock cycle per byte.
b) Compact: Blowfish can execute in less than 5KB Memory.
c) Simple: Blowfish uses only primitive operations, such as addition, XOR and table look-up, making its

design and implementation simple.

d) Secure: Blowfish has a variable key length up to a maximum of 448 bits long, making its both flexible & secure.

Blowfish suits application where the key remains constant for a long time.

Operations:

a) Subkey Generation:

This process converts the key up to 448 bits long to subkeys totaling 4168 bits.

b) Data Encryption:

This process involves the iteration of a simple function 16 times, Each round contains a key-dependent permutation & key and data dependent substitution.

① Subkey generation:

Steps:

i) key is represented in array

$K_1, K_2 \ldots K_n \; [1 \leq n \leq 14]$

each key length is 32-bits.

ii) Initialize P-array

$P_1, P_2 \ldots P_{18}$ [32bit]

↓

32-bit

iii) Initialize 4 S-boxes.

S1 → S0,0, S1,1 ..... S1, 255

S2,0, S2,1 ..... S2, 255

S3,0, S3,1 ..... S3, 255

S4,0, S3,1 ..... S4, 255

[each contain 256 32-bit entries in each S-box]

iv) P-array, S-boxes. [Hexadecimal values from for Pi]

P1 = 243F6A88

P2 = 85A308D3

...

S4,254 = 578FDFE3

S4,255 = 3AC372E6

v) Bitwise operation (XOR of P1 with K1

P1 = P1 XOR K1

P2 = P2 XOR K2

P14 P14 XOR K14

P15 = P15 XOR K1

P16 = P16 XOR K2

P17 = P17 XOR K3

P18 = P18 XOR K4.

vi) 64-bit plain text

10 01

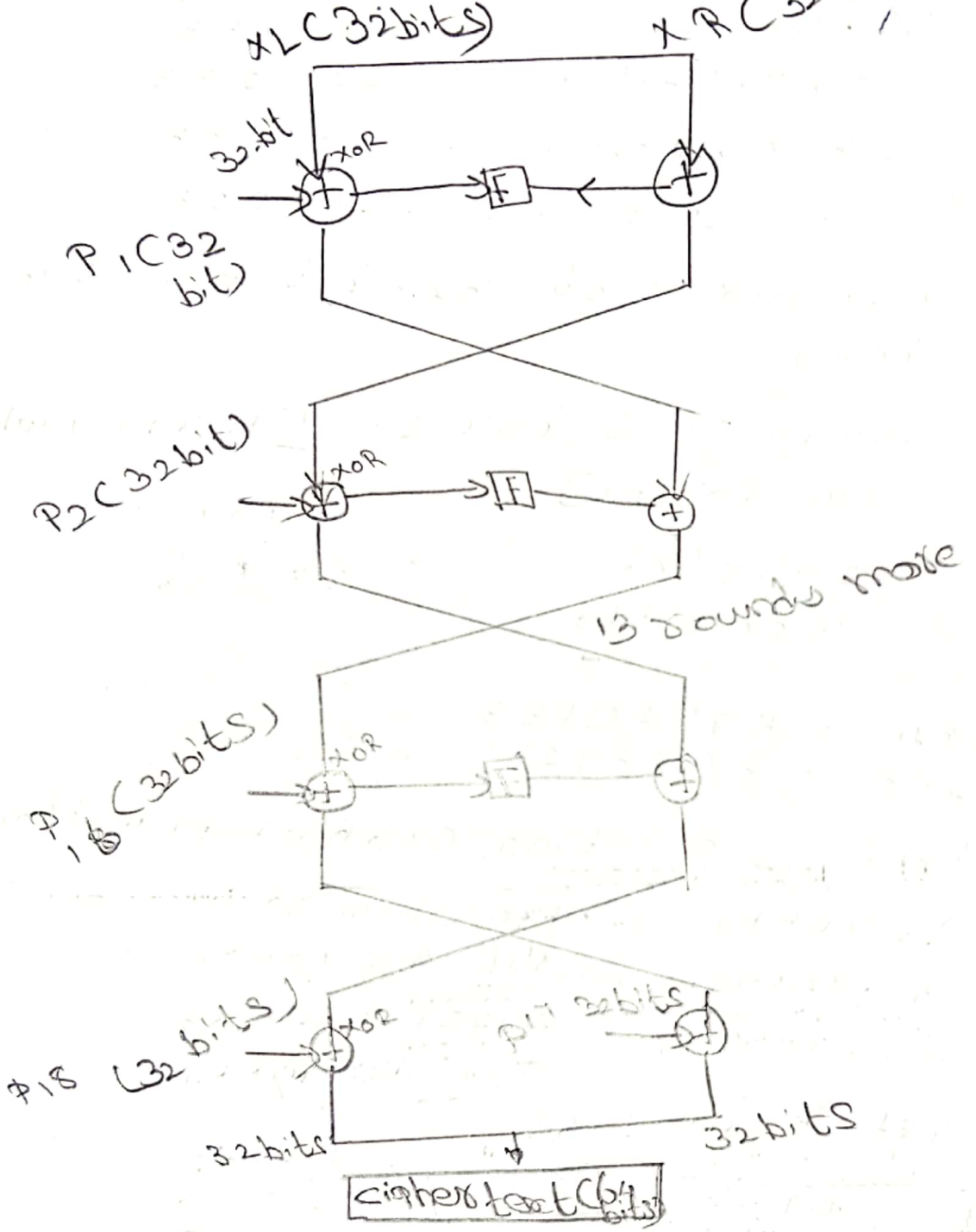
↓

Blowfish Encryption → subkey generates [when all P and S-box values are replaced]

② Data Encryption and Decryption:

Encryption of 64-bit block plain-text input X we use the P-array and S-boxes during the encryption and decryption process.

Working of blow Fish



1. Divide x into 2 blocks.
   XL and XR of equal size. Thus, both XL and XR will consist of 32-bits each.
2. For i = 1 to 16
   XL = XL XOR Pi;
   XR = F(XL) XOR XR
   Next ;

~~swap xL, xR~~

3. swap xL, xR (i.e. undo last swap)

4. xL = xL XOR P18.

5. combine xL and xR back into x.

The function of F as follows;

a) Divide the 32-bit xL block into four 8-bit sub-blocks, named a, b, c and d.

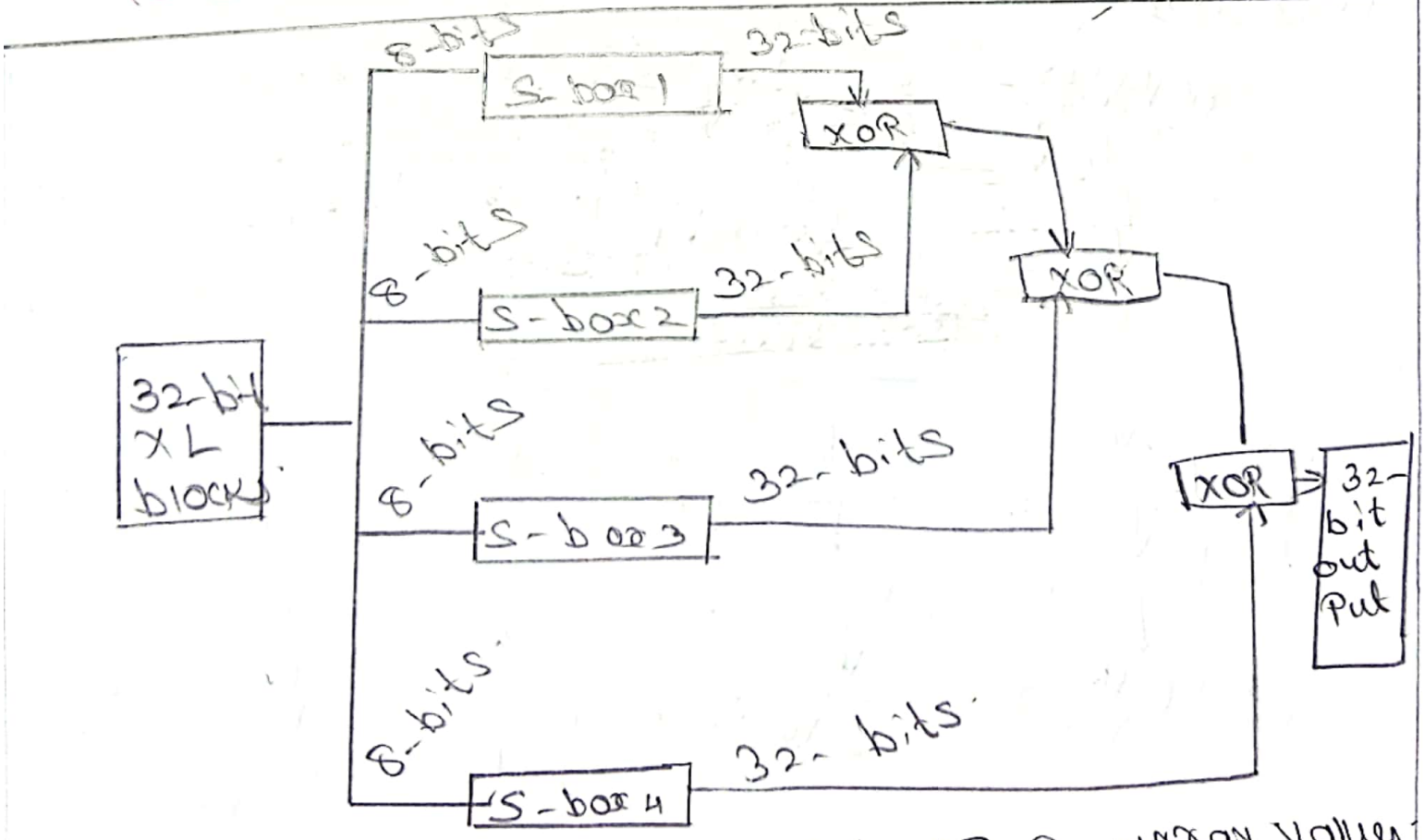
b) compute F[a, b, c, d] = ((S1, a + S2, b) XOR S3, c) + S4, d

for example

if a = 10 b = 95 c = 37 and d = 191, then computation of F would be:

F[a, b, c, d] = ((S1, 10 + S2, 95) XOR S3, 37) + S4, 191.

diagrammatic view of the function F:



Decryption is reverse of P-array values

③ IDEA : Basic principles.

→ IDEA - International Data Encryption Algorithm.

→ It is a symmetric block cipher developed by Xuejia Lai and James Massey of ETH Zurich.

→ IDEA uses a 128-bit key.

→ IDEA & DES both uses round function and subkey generation function.

→ IDEA does not use S-boxes.

→ IDEA relies on 3 different mathematical operations:

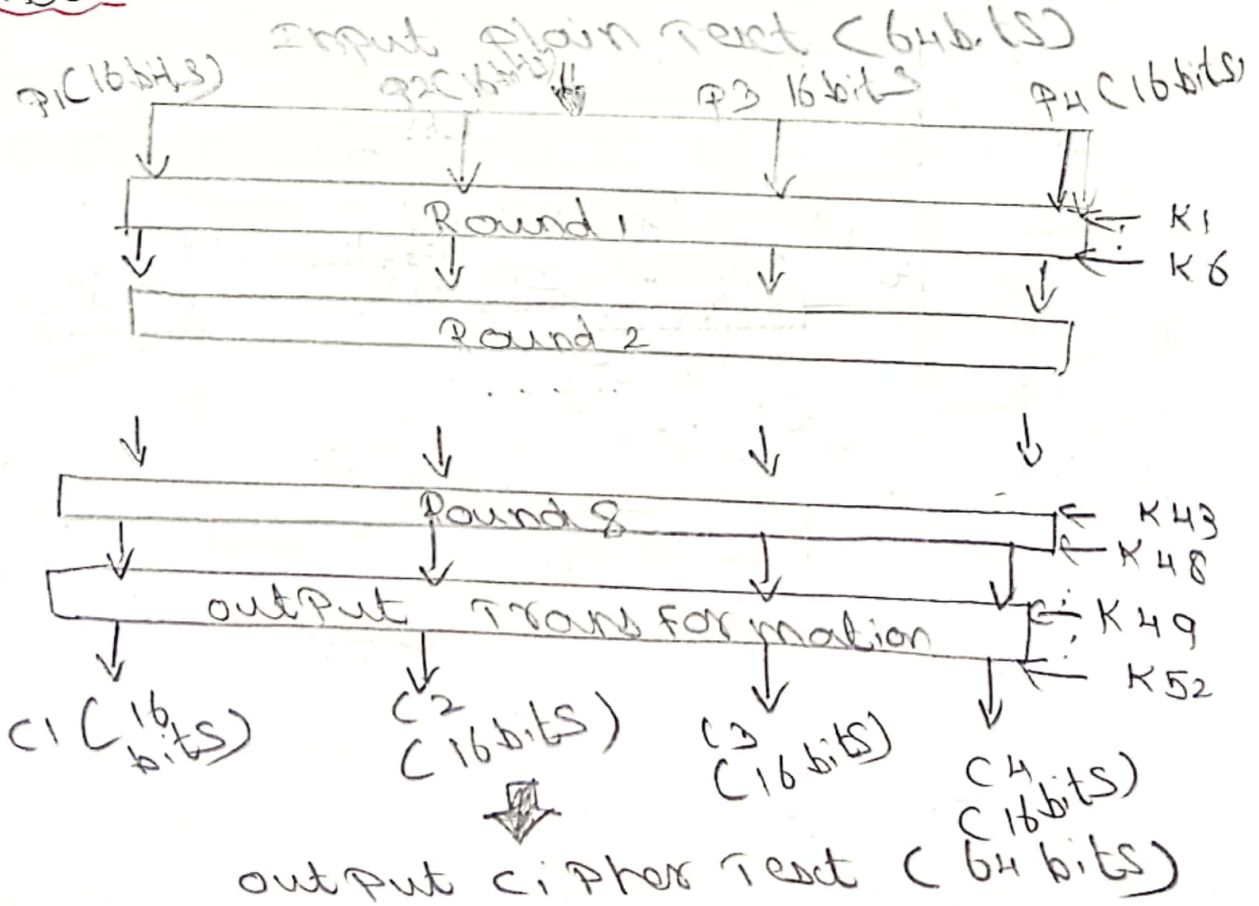
a) XOR

b) binary addition of 16-bit integer

c) binary multiplication of 16-bit integer.

Combine these two produce complex transformation. It is very difficult to analyze and hence very difficult to cryptanalyze.

Rounds:



One round in IDEA

step1: multiply * P1 and K1

step2: Add * P2 and K2

step3: Add * P3 and K3.

step4: Multiply P4 and K4

step5: XOR the results of step1 and step3

step6: XOR the results of step2 and step4.

step7: Multiply * the results of step5 with K5.

step8: Add * the results of step6 & step7.

step9: Multiply * the results of step8 with K6.

step10: Add * the results of step7 and step9

step11: XOR the results of step1 and step9

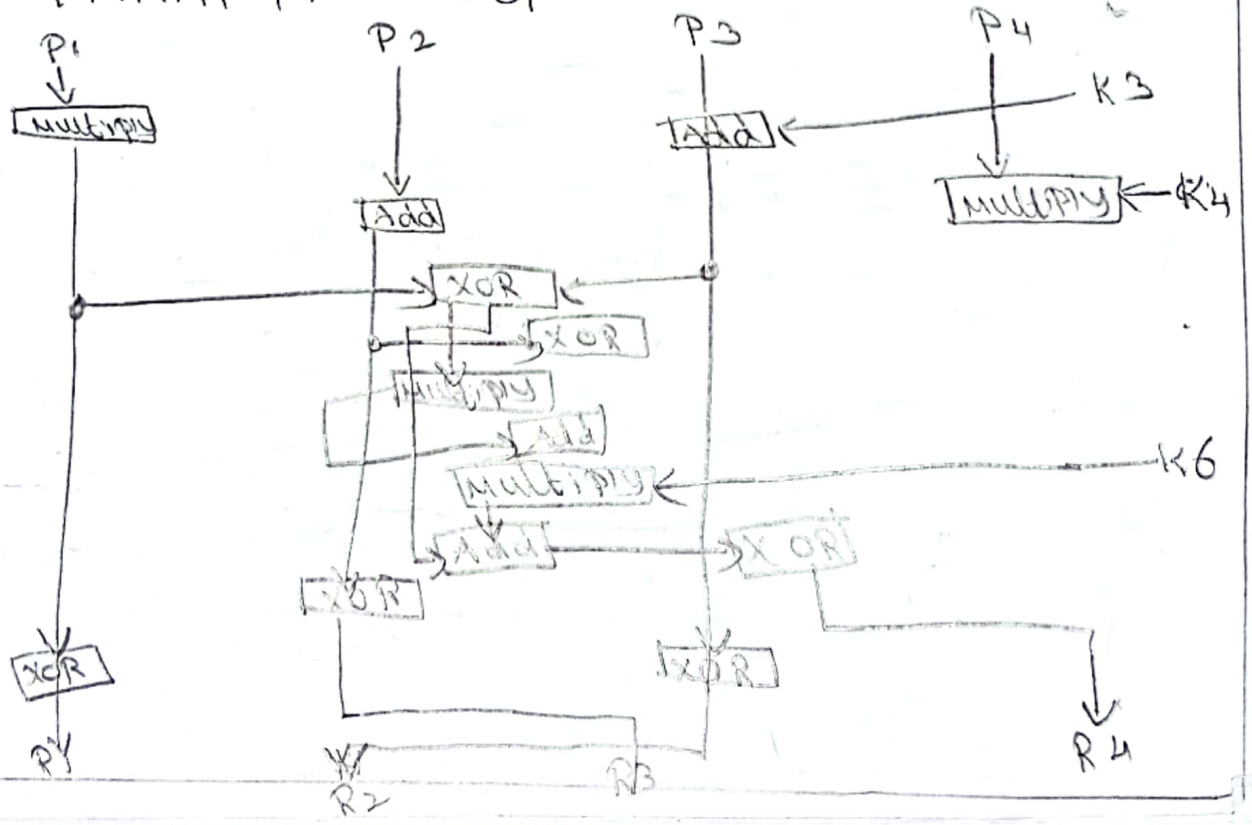
step12: XOR the results of step3 and step9

step13: XOR the results of step2 and step10

step14: XOR the result of step4 and step10.

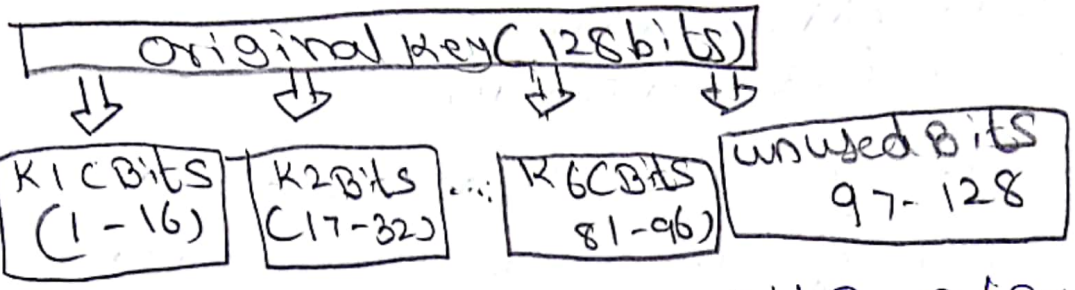
Binary addition of two 16-bit Number.

```
  11111111  00000000
+ 11111111  11000001
-----------------------
  11111111  11000001
```



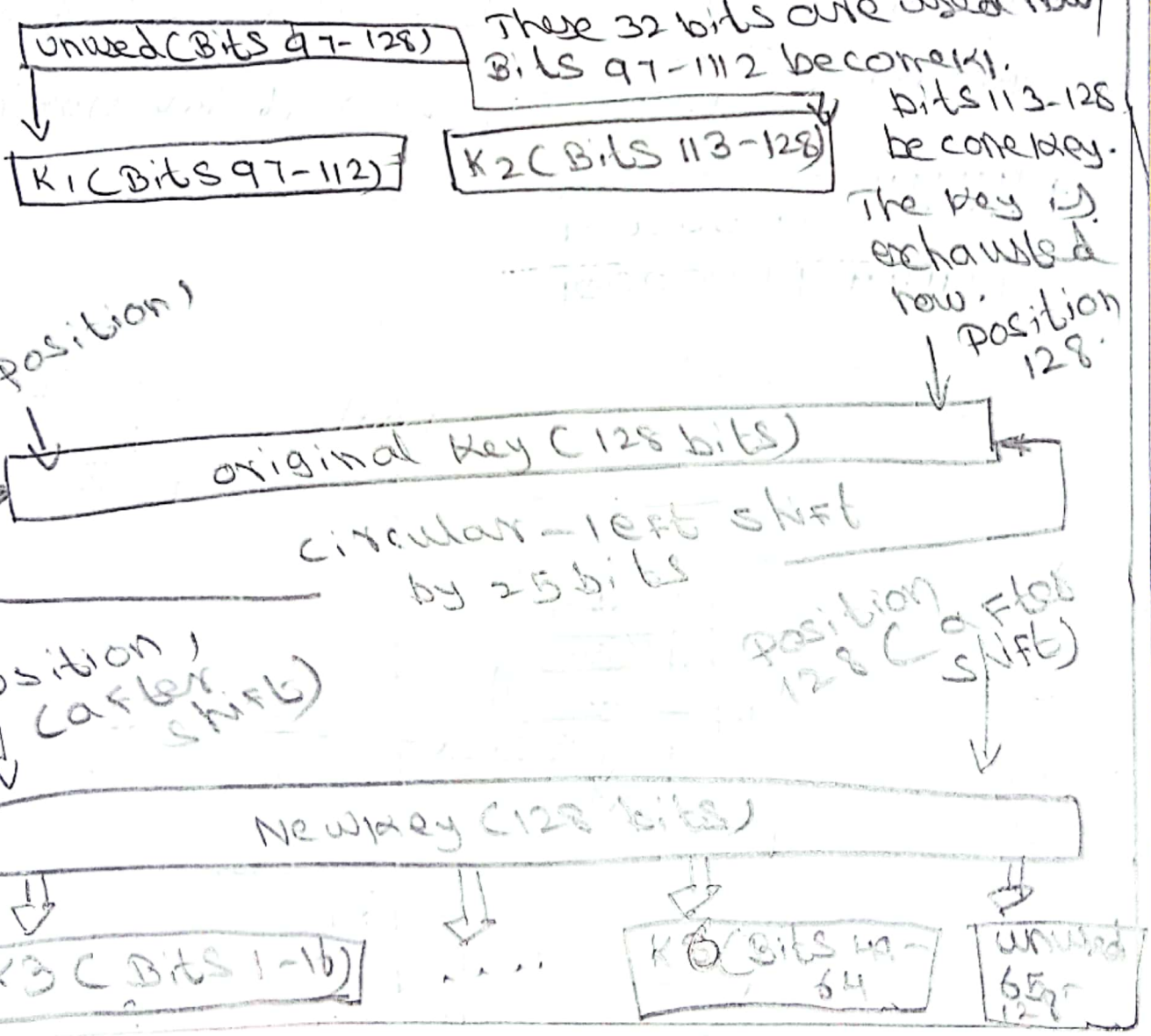
3. Sub Key generation for a Round:

First Round:



→ Initial key consists of 128 bits → 6 sub keys → K1 to K6 → first round.
→ First 96 bits used for first round
→ End of the first rounds bits 97-128 original key are unused.

Second Round:



④ output transformation

output transformation is a one-time operation. It takes at the end of 8th round. Input & output transformation is, of course, the output of 8th round.

⑤ Subkey generation for the output transformation:

It is exactly similar to the subkey generation process for the eight rounds. Recall that at the end of eighth and final round, the key is exhausted and shifted. This round, the first 64 bits make up subkeys K1 to K4, which are used as the four subkeys for this round.

AES: Advanced Encryption standard. It is a symmetric key block cipher.

→ It is a Non-Feistel cipher.

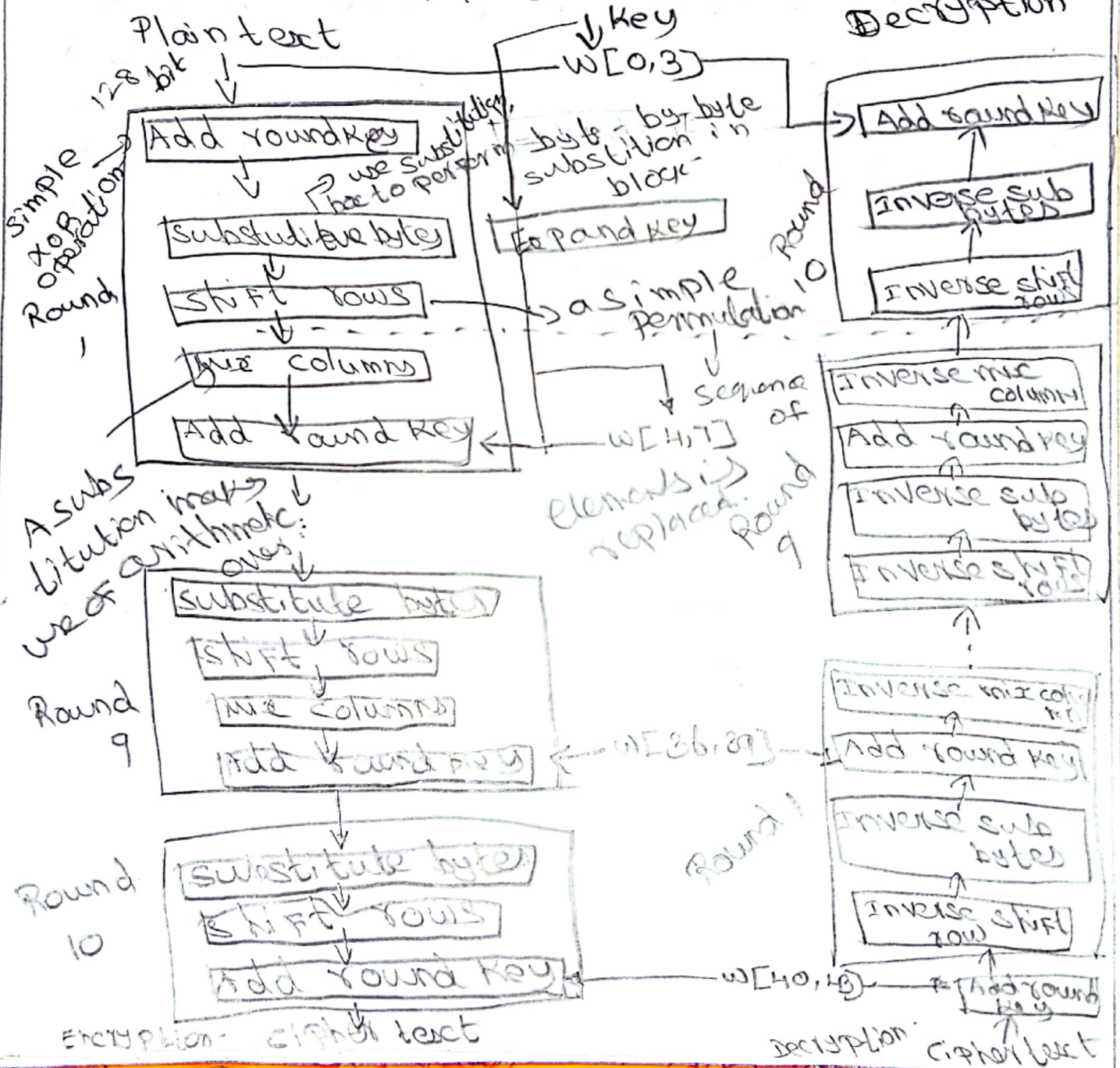
→ 128 data block size [encrypt decrypt

→ key size 128, 192 or 256 bits.

→ No. of rounds for key.
rounds bits.
10 → 128 bits
12 → 192 bits
14 → 256 bits.

1 word - 32 bits
4 bytes.

AES Encryption & Decryption.



128-bit AES each round contains 4 stages:

i) Byte substitution:

ii) Row shift

iii) column mixing

iv) Round key addition.

→ AES several round → each round is made of serval stage.

→ Data block is transformed from one stage to another.

→ Data block referred as state.

→ Block is copied into state array which is modified at each stage of encryption & decryption. After the final stage, state is copied to an output matrix.

working procedure:

i) not Fiestel structure

ii) The key that provides as input is expanded into an array of forty-four 32-bit words, w[i]

iii) four different stages are used, one of permutation and three of substitution.

iv) For both encryption & decryption, the cipher begins with an Add Round key stage, followed by nine rounds that each includes all 4 stages, followed by a tenth round of 3 stages.

5. Only the Add Round key stage make use of the key.
6. The Add round key stage make use of the key.
6. The Add round key stage is, in effect, a form of Verman cipher and by itself would not be formidable.
7. easily reversable.
8. The decryption algorithm makes use of the expanded key in reverse order.
9. once it is established that all 4 stages are reversable, it is easy to verify that decryption does recover the plain text.
10. The Final round of both encryption & decryption consists of only three stages

NIST evaluation criteria for AES are.

1. Security :→ Actual security compared to another algorithm, soundness (mathematical basis) Randomness (random permutation on the input block.

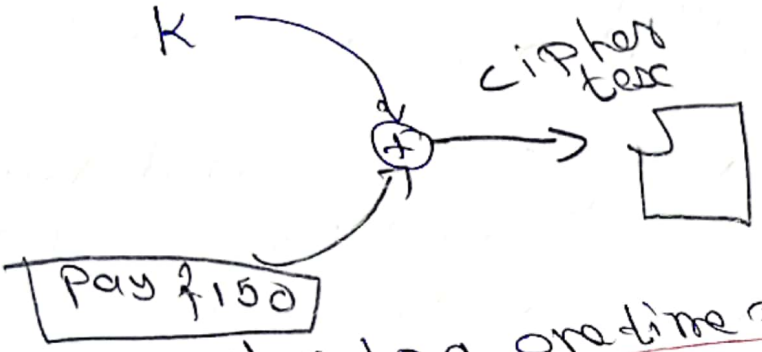
2. cost : Licensing requirements (world wise using) computational efficiency (applicable to both h/w & s/w implementations. memory requirements (Algorithm in h/w & s/w will be considered)

3. Restricted space Environment.
4. Hardware Implementation.
5. Attacks on implementation
6. Encryption versus decryption
7. key agility.

stream ciphers:

stream cipher is one that encrypts a digital data stream one bit or one byte at a time. s.c encrypt plaintext message by applying an encryption algorithm with a pseudorandom cipher digit stream (key stream)

s.c algorithm are designed to accept a crypto key and a stream of plain text to produce a stream of ciphertext.



s.c is similar to a one time pad
s.c encrypts smaller block of data, typically bits or bytes.

- A key stream generator outputs a stream of bits $k_1, k_2, k_3 \ldots k_n$
- A key stream is xored with a stream of plaintext bits $p_1, p_2 \ldots p_i$ to produce the stream of cipher text bits

$$c_i = p_i \oplus k_i$$

At the description end, the cipher text to recover the plaintext bits.

$$p_i = c_i \oplus k_i$$

The system security depends entirely on the insides of the keystream generator.

Adv:
Speed of transformation
Low error propagation

Dis:
Low diffusion
susceptibility to malicious insertation and modification.

RC4:
→ RC4 → Ron Rivest in 1987 → RSA security
→ Algorithm → based → random permutation.

→ RC4 used SSL/TLS standards for comm. between web browsers & servers.
→ Variable length of key is from 1 to 256 bytes.
S[0], S[1], ... S[255]
↗ permutation of 8-bit numbers from 0 to 255.

for encryption & decryption, a byte k is generated from S by selecting one of the 256 entries in a systematic fashion.

As each value of k is generated, the entries in S are again permuted.

Initialization of S

To begin entries of S are equal to the value from 0 to 255 in ascending order @ S[i] = i, i = 0 ..... 255.

A temoporary vector T is also created. If the length of key K is 256 bytes, then K is transfered to T. otherwise key of length keylen bytes, keylen element of T are copied from K and then it repeated as many times as necessary to fill out:

preliminary operation.

```
/* initialization */
for i = 0 to 255
{
S[i] = i;
T[i] = K[i mod keylen];
```

Next use T to produce initial permutation S. This involves starting S[0] through S[255].

Temporary vector

```
/* initial permutation of S */
j = 0
for i = 0, 255
{
  j = (j + S[i] + T[i]) mod 256;
swap(S[i], S[j])

}
```

Because the only operation on S is a swap, only effect is a permutation.

S still contains the number from 0 to 255.

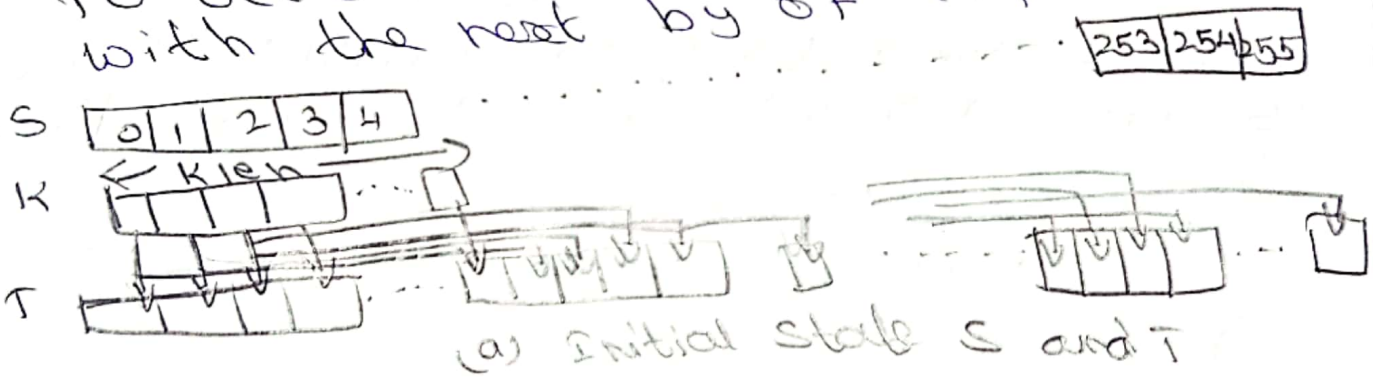
Stream Generation:

S.g involves starting with S[0] going through to S[255] each swapping S[i] after reached S[255] process continues starting over again at S[0].

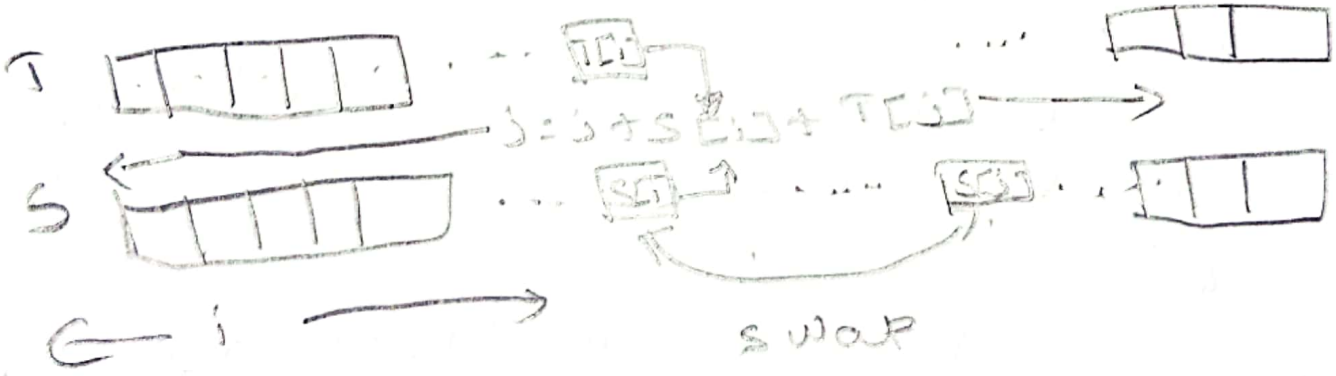
```
/* stream generation */
    i = j = 0
    while (true)
    {
    i = (i+1) mod 256
    j = (j + S[i]) mod 256
    swap( S[i], S[j] mod 256.

     k = S[t];
```

To encrypt, XOR the value of k with the next byte of plaintext.

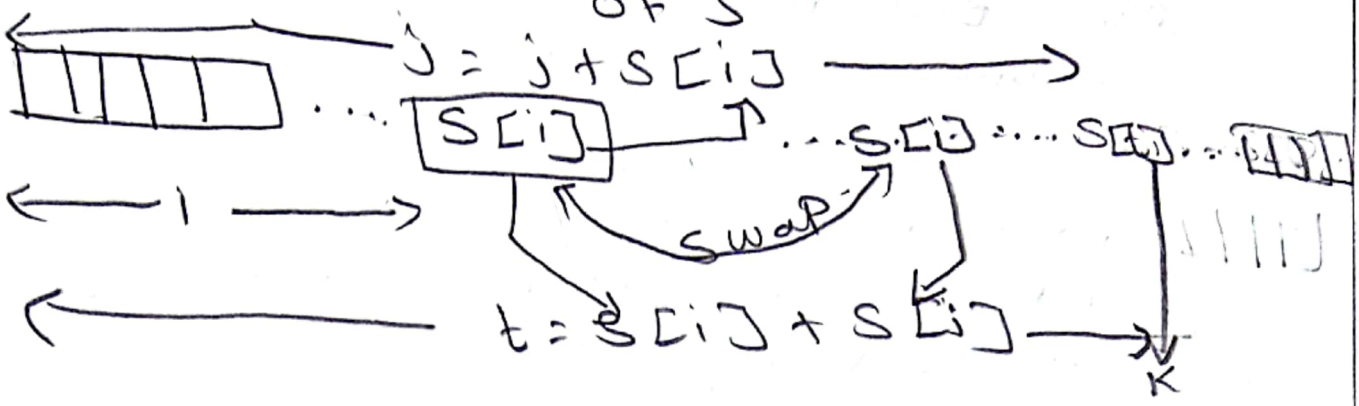
To decrypt, XOR the value of k with with the next by of ciphertext.



(a) Initial state S and T



b) Initial permutation of S



RC5 a. Basic principles:

RC5 Encryption algorithm is fast, symmetric block cipher suitable for hardware and software implementation.

block of plain text = length 32, 64 or 128 bits.
cipher text also same length.
key range → 0 to 2040 bits.

RC5 need 3 parameters.

w →	word size of in bits	16, 32, 64
R →	No. of rounds	0, 1 - - - 255
B →	Number of 8-bits	0, 1 - - - 255

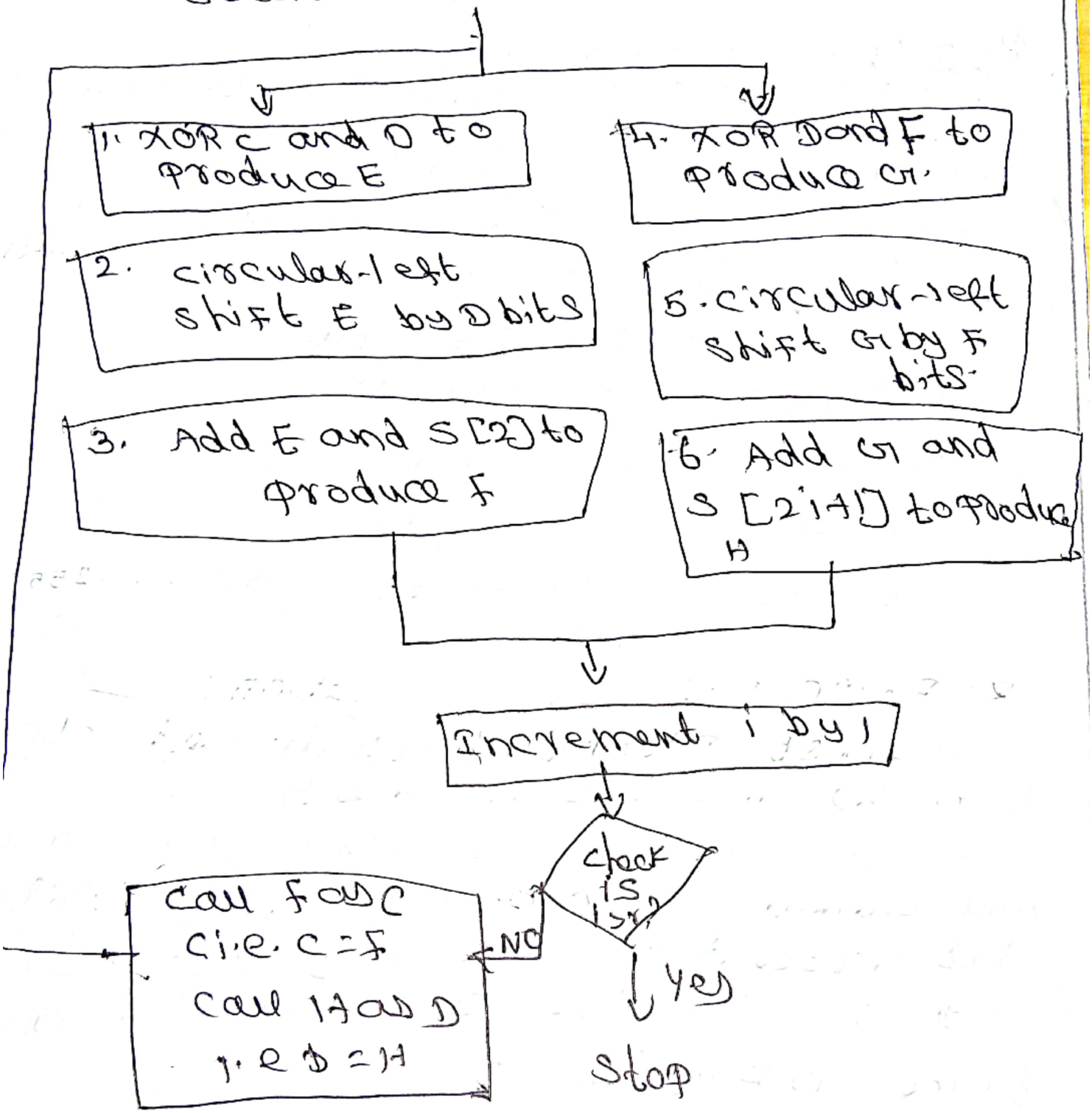
b. principles of operation:

→ first plaintext is divided into two 32-bit blocks A & B.

→ The first two subkey S[0] and S[1] are added to A and B, respectively. This procedures C and D respectively, and marks the end of the one-time operation.

First, divide the original plaintext into two blocks of equal sizes. Call them as A and B.

Add A and S[0] to produce C
Add B and S[1] to produce D
start with a counter i = 1

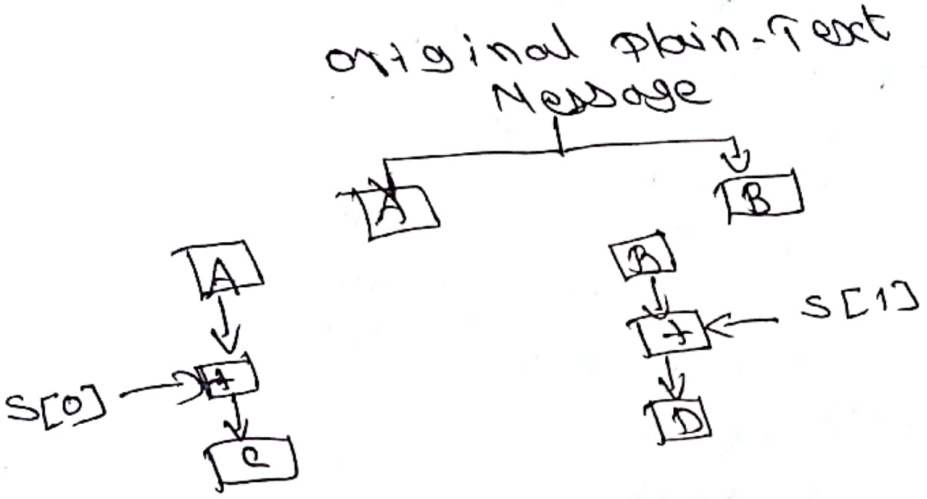


Then the rounds begin. In each round, there are following operations:

* Bitwise XOR & Left circular-SNft
* Addition with next subkey for both C & D.

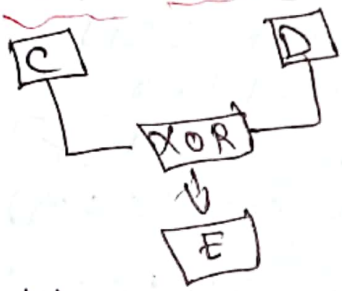
• This is the addition operation first, and then the result of addition mod 2^{32} (since w = 32 here, we have 2^{32}) is performed.

3. one-time initial operation



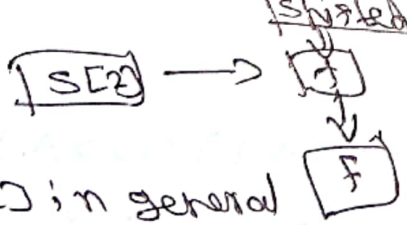
4. Details of one Round

step1: XOR C and D



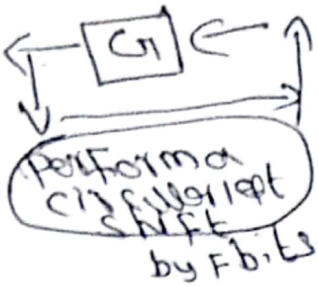
step2: circular-left shift E

step3: Add E and next subkey.

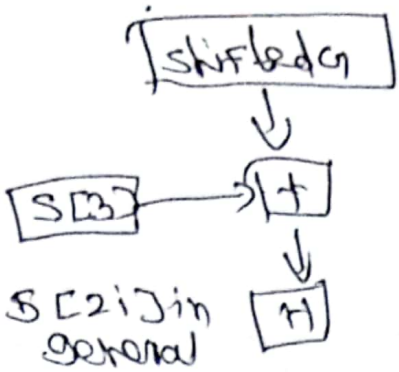


step4: XOR D and F

Step 5
Circular left shift G



Step 6: Add G and Next Subkey



Step 7: Miscellaneous Tasks:

1. Increment i by 1
2. Check to see if i<r
   i = i+1
   if i<r
   call F as C again
   call H as D again
   Go back to step 1

ELSE
   stop
End-if

5. Mathematical Representation:

A = A + S[0]
B = B + S[1]
FOR i = 1 to r
FOR i = 1 to r → left shift.

A = ((A XOR B) <<< B) + S[2i]
B = ((B XOR A) <<< A) + S[2i+1]

Next i;

FOR i = r to 1 step -1
A = ((B - S[2i+1]) >>> A) XOR A
B = ((A - S[2i]) >>> B) XOR B
Next i;
B = B - S[1] A = A - S[0]

6. subkey creation

Subkey generation ⇓ Subkey Mixing

Generate S[0], S[1] ....

Mix with L[0], L[1], ...

RC5 Modes:

a) RCB block cipher: same length as input (2w bits)

b) RC5-CBC: cipher block chaining similar to DES.

c) RC5-CBC-Pad: similar to RC5-CBC.

d) RC5-CTS - ciphertext stealing mode.

Asymmetric key ciphers.

① Block cipher principle.

i) It must be computationally easy to encipher or decipher a message given the appropriate key.

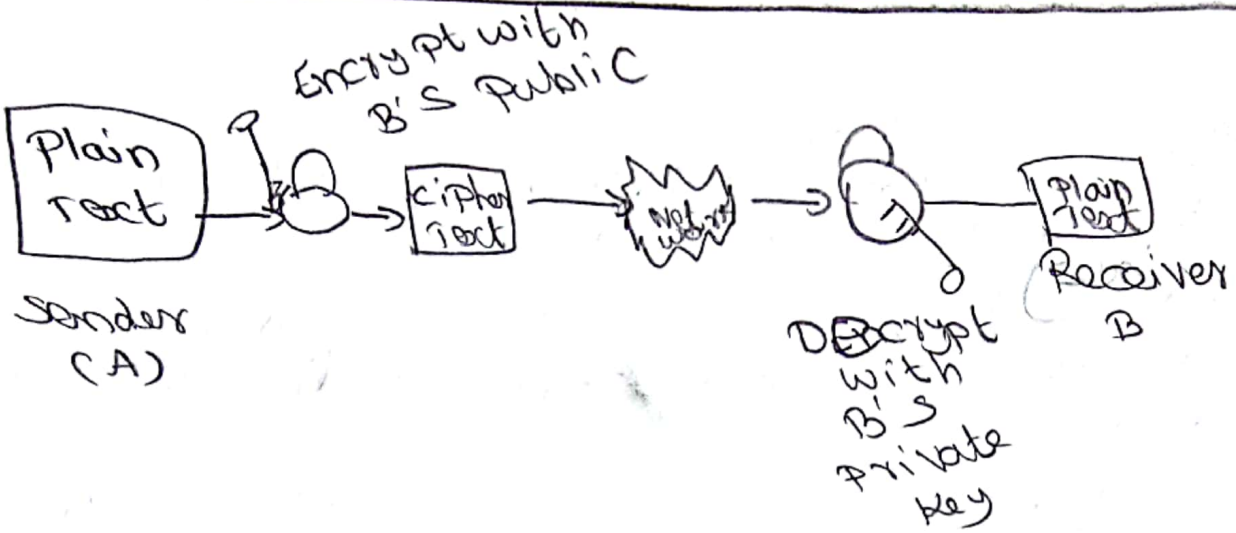
ii) It must be computationally infeasible to derive the private key from the public key.

iii) It must be computationally infeasible to determine the private key from a chosen plain text attack.

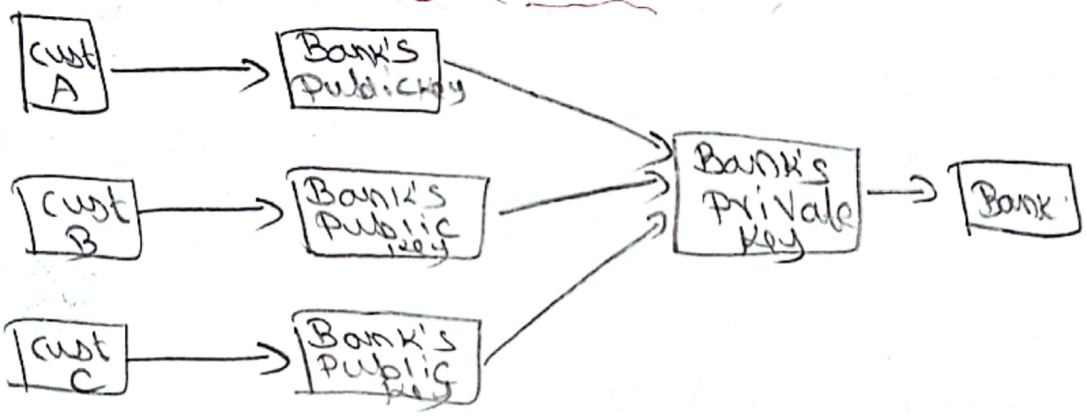
key details	A should know	B should know
A's private key	yes	NO
A's public key	yes	yes
B's private key	No	yes
B's public key.	yes	yes.

(2)

A - should keep his private key secret.
B - should keep his private key secret.
A - should inform B about his public key
B - B should inform A about his public key.



Use of a Public key - private key pair by bank



A symmetric key cryptography work as Follow:

1. when A want to send a message to B, A encrypt the message using B's Public key. This is possible because A knows B' Public key.
2. A send this message (which was encrypt-ed with B's Public key) to B.
3. B decrypt A's message using B's Private key. Note that only B knows about her Private key. Also note that the message can be decrypted only by B's Private key nothing else.

② Crypto system:

Use of public key cryptosystems into three categories.

① Encryption/Decryption: The sender encrypts a message with the recipient's public key.

② Digital signature: The sender "Sign" a message with its private key. Singing is achieved by a cryptographic algorithm applied to the message or to a small block of data that is a function of the message.

③ Key Exchange: Two sides cooperate to exchange a session key, several different approaches are possible, involving the private key(s) of one or both parties.

③ RSA Algorithm:

RSA Algorithm developed in 1977 by Rivest, Shamir, Adleman (RSA) at MIT. It is public key encryption algorithm.

In this algorithm, one user uses a public key and other user uses a ~~public~~ private key (secret) key.

Algorithm:

① choose two large prime number P and Q

2. Calculate $N = P \times Q$.
3. Select the public key (i.e. the encryption key) E such that it is not a factor of $(P-1)$ and $(Q-1)$
4. Select the private key (i.e the decryption key) D such that the following equation is true:
   $(D \times E) \bmod (P-1) \times (Q-1) = 1$
5. For encryption, calculate the cipher text CT from the plain text PT as follows:
   $CT = PT^E \bmod N$
6. Send CT as the cipher text to the receiver.
7. For decryption, calculate the plain text PT from the cipher text CT as follows:
   $PT = CT^D \bmod N$.

Ex:

1. Choose two large prime numbers P & Q
   Let $P = 7$, $Q = 17$
2. Calculate $N = P \times Q$
   we have, $N = 7 \times 17 = 119$
3. Select the public key
   $(P-1) \times (Q-1)$
   $(7-1) \times (17-1) = 6 \times 16 = 96$

Factor of 96 are -> 2, 2, 2, 2 and 3 (because 7 is not its factor)
Thus, we have to choose E not its factor 2 and 3.
Let we choose E as 5. (It could have been other number that does not its factors as 2 and 3)

2	96
2	48 - 0
2	24 - 0
2	12 - 0
2	6 - 0
3	3 - 0
	1 - 1

4. (D x E) mod (P-1) x (Q-1) = 1
Let us substitute the values of E, P and Q in the equation.
we have (D x 5) mod (7-1) x (17-1) = 1
Thus (D x 5) mod (6) x (16) = 1
That is (D x 5) mod (96) = 1
After some calculations Let us take D = 77. Then the following is true.
(77 x 5) mod (96)
= 385 mod 96 = 1, which is what we wanted.

5. $CT = PE^{E} \bmod N$
Let assume we want to encrypt plain text 10. Then we have.
$CT = 10^{5} \bmod 119$
$= 100000 \bmod 119 = 40$

6. send CT as the cipher text to the receiver
Send 40 as the cipher text to the receiver.

7. Decryption. $PT = CT^{D} \bmod N$
$PT = CT^{77} \bmod N$
$PT = 40^{77} \bmod 119 = 10$ [what we get in step 5]

Q. ElGamal cryptography:

Taher ElGamal created ElGamal crypto-graphy more popularly known as ElGamal cryptosystem. 3 aspects to be discussed.

1. ElGamal key generation
2. ElGamal encryption
3. ElGamal decryption.

① ElGamal key generation:

This involves the following steps:

a) select a large prime number called p. This is the first part of the encryption key or public key.

b) select the decryption key or private key D. There are some mathematical rules that need to be followed we are omitting for keeping things simple.

c) select the second part of the encryption key or public key E1.

d) The third part of the encryption key or public key E2 is computed as

$$E2 = E1^{D} \bmod p$$

(second part → public key, third part → private key)

e) The public key is (E1, E2, p) and the private key is D → private key

For ex: $p = 11$, $E1 = 2$, $D = 3$, Then $E2 = E1^{D} \bmod p = 2^{3} \bmod 11 = 8$

Hence, the public key is (2, 8, 11) and the private key is 3.

Elgamal key Encryption:

Involve the following steps:

1. select a random integer R that fulfills some mathematical properties, which are ignored here.
2. compute the first part of the cipher text $C1 = E_1^R \bmod p$.
3. compute the second part of the cipher text $C2 = (PT \times E2^R) \bmod p$. where PT is the plain text.
4. The final cipher text is (C1, C2)

ex: R = 4, plain text PT = 7:

$C1 = E1^R \bmod p = 2^4 \bmod 11$

$16 \bmod m = 5$

$C2 = (PT \times E2^R) \bmod p = (7 \times 2^8) \bmod 11$

$= (7 \times 4096) \bmod 11 = 6$

Hence cipher text is (5, 6)

Elgamal key decryption:

Involves the following step:

compute the plain text PT using the formula

$$PT\ [C2 \times (C1^D)^{-1}] \bmod p$$

ex:

$$PT\ [C2 \times (C1^D)^{-1}] \bmod p$$

$$PT = [6 \times (5^3)^{-1}] \bmod 11$$

$$= [6 \times 3] \bmod 11$$

$= 7$ This our original plain text.

Knapsack Algorithm:

Ralph Merkle and Martin Hellman developed the first algorithm for public-key encryption, called the knapsack algorithm.

It is based on knapsack problem. This is actually a simple problem: Given a pile of items. each with different weights, is it possible to put some of them in a bag (i.e. knapsack) in such a way that the knapsack has a certain weight?

That is if $N1, N2 \ldots Nn$ are the given values and S is the sum, find out b_i so that.

$$S = b_1N_1 + b_2N_2 + \ldots + b_nN_n$$

Each b_i can be 0 or 1, 1 indicates the item is knapsack and 0 indicates that it is not.

A block of plain text equal in length to the number of items in the pile would select the items in the knapsack The cipher text is the resulting sum.

For esc:

Knapsack 1, 7, 8 || 2, 14, 20 then the plain text and the resulting ciphertext

plain text	0	1 1 0 1 1	1 1 1 0 0 0	0 1 0 1 1 0
Knapsack	1	7 8 12 14 20	1 7 8 12 14 20	1 7 8 12 14 20
cipher text	7	8 14 20 = 49	1+7+8 = 15	7+12+14 = 33

Diffie-Hellman Key Exchge

This algorithm is to enable two users to exchange a key securely that can then be used for subsequent encryption of message.

How key exchange has done:

Diffie Hellman key agreement protocol was developed by Diffie and Hellman in 1976. This protocol allows two users to exchange a secret key over an insecure medium without any prior secrets.

Suppose Alice & Bob want to agree on a share secret key using the Diffie-Hellman key agreement protocol. They proceed as follows;

① First, Alice generates a random private value 'a' and Bob generates a random private value 'b'.

② Both a and b are drawn from the set of integers. They derive their public values using parameters p and g and their private values.

③ Alice public value is $g^a \bmod p$ and Bob public value is $g^b \bmod p$

④ They then exchange their public values.

5. Finally, Alice computes

$$g^{ab} = (g^b)^a \bmod p$$

6. Bob computes $g^{ba} = (g^a)^b \bmod p$

7. since $g^{ab} = g^{ba} = K$, Alice & Bob now have shared secret key K.

Algorithm:

Select two numbers

1. prime number q
2. α an integer that is a primiti -ve root of q.

Suppose the users A & B wish to exchage a key.

① user A select a random integer $X_A < q$ and computes $Y_A = \alpha^{X_A} \bmod q$

② user B select a random integer $X_B < q$ and computes $Y_B = \alpha^{X_B} \bmod q$.

③ Both side keeps the X value privately & makes the Y value available publicly to the other side.

④ user A computes the key as

$$K = (Y_B)^{X_B} \bmod q$$

5. User B computes the key as
$k = (Y_A)^{X_B} \bmod q$.

- Both side gets same results:

$$k = (Y_B)^{X_A} \bmod q$$
$$= (\alpha^{X_B} \bmod q)^{X_A} \bmod q$$
$$= (\alpha^{X_B})^{X_A} \bmod q$$
$$= \alpha^{X_B X_A} \bmod q$$
$$= (\alpha^{X_A} \bmod q)^{X_B} \bmod q$$
$$= (Y_A)^{X_B} \bmod q.$$

Consider a Diffie Hellman scheme with a common prime $q = 11$ and a primitive root $\alpha = 2$.

a) If user A has public key $Y_A = 9$, what is A's private key X_A.
b) If user 'B' has public key $Y_B = 3$, what is shared secret key k.

Ans:

$2 \bmod 11 = 2$, $2^2 \bmod 11 = 4$, $2^3 \bmod 11 = 8$
$2^4 \bmod 11 = 5$, $2^5 \bmod 11 = 10$, $2^6 \bmod 11 = 9$
$2^7 \bmod 11 = 7$, $2^8 \bmod 11 = 3$, $2^9 \bmod 11 = 6$
$2^{10} \bmod 11 = 1$

Since $2^i \bmod 11$ for $0 < i < 11$ contain all numbers from 1 to 11-1, the size of this set is equal to $\phi(q)$. The order is 9. Hence 2 is a primitive root of 11.

Cryptographic Hash Function:

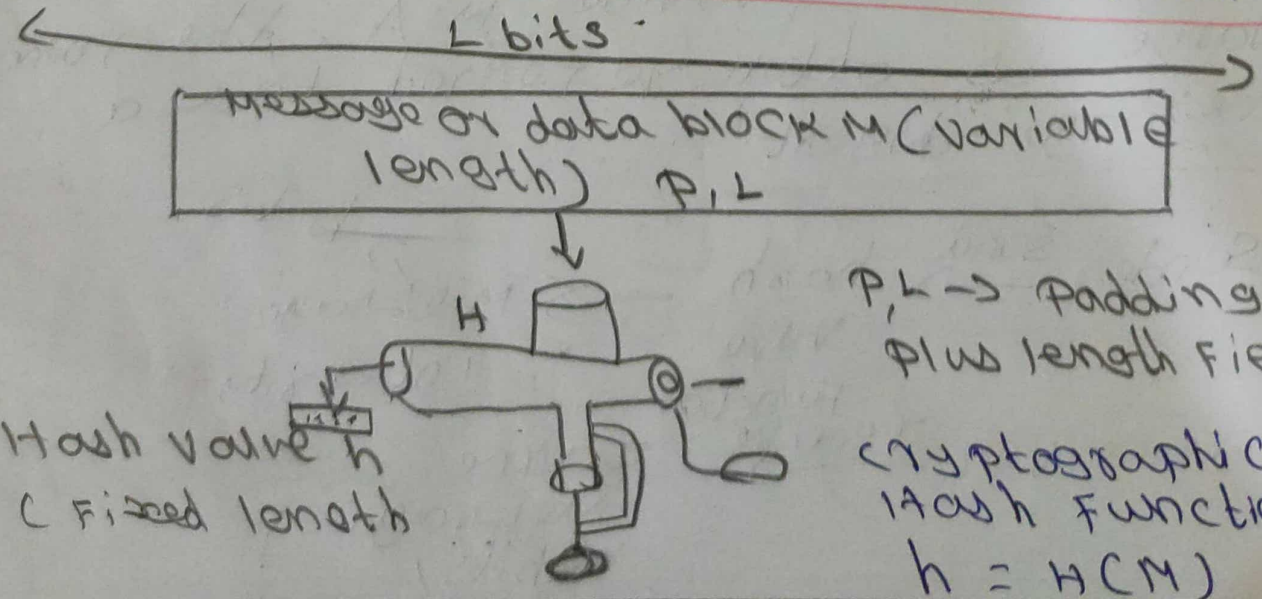
Hash Function:

A hash function H accepts a variable-length block of data M as input and produces a fixed-hash function value $h = H(M)$.

A good hash function has the property that the result of applying the function to a large set of input will produce outputs that are evenly distributed & apparently random.

H.F principal object is data integrity. A change to any bit or bits in M results, with high probability, in a change to the hash value.

The kind of hash function needed for security application is referred to as a cryptographic hash function.



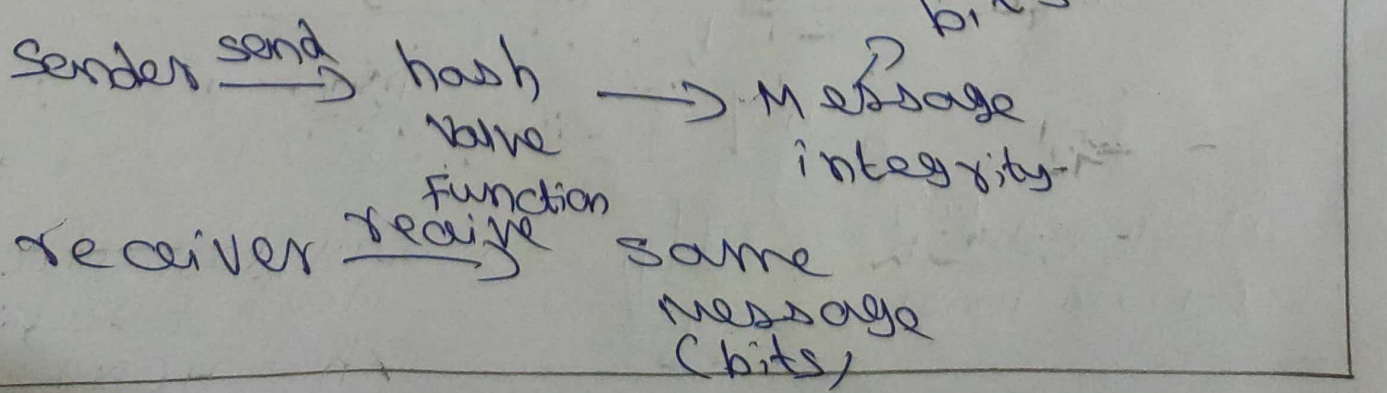
The above diagram depicts the general operation of a cryptographic hash function. Typically, the input is padded out to an integer multiple of some fixed length (e.g. 1024 bits) and the padding includes the value of length of the original message in bits. The length field is a security measure to increase the difficulty for an attacker to produce an alternative message with the same hash value, as explained subsequently.

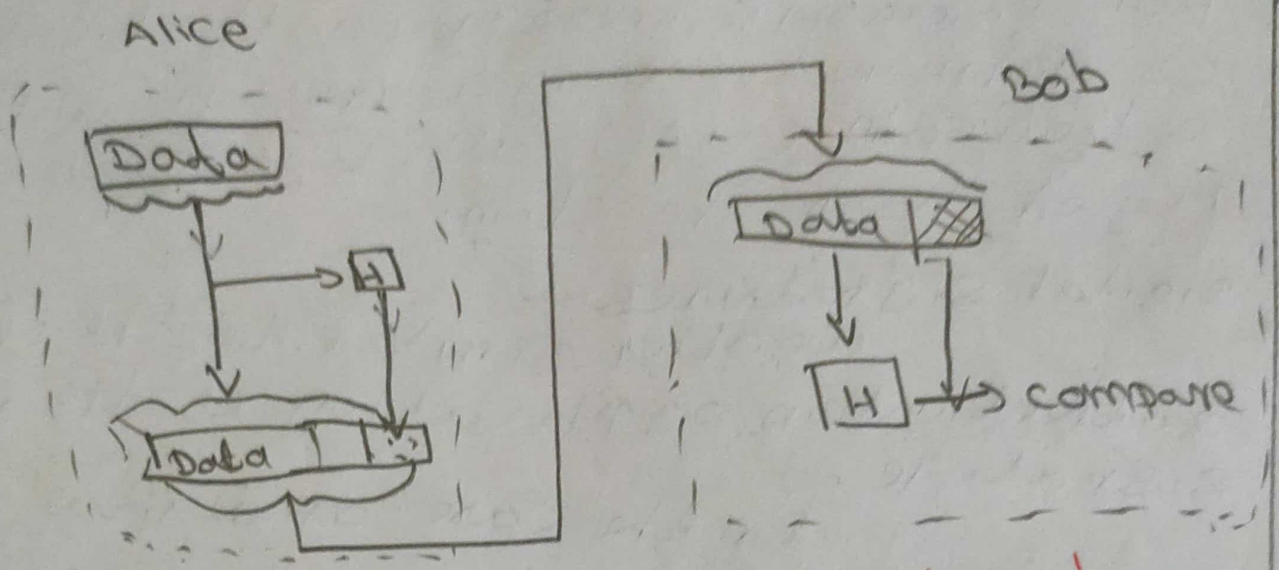
Applications of Cryptographic Hash Functions:

① Message Authentication:

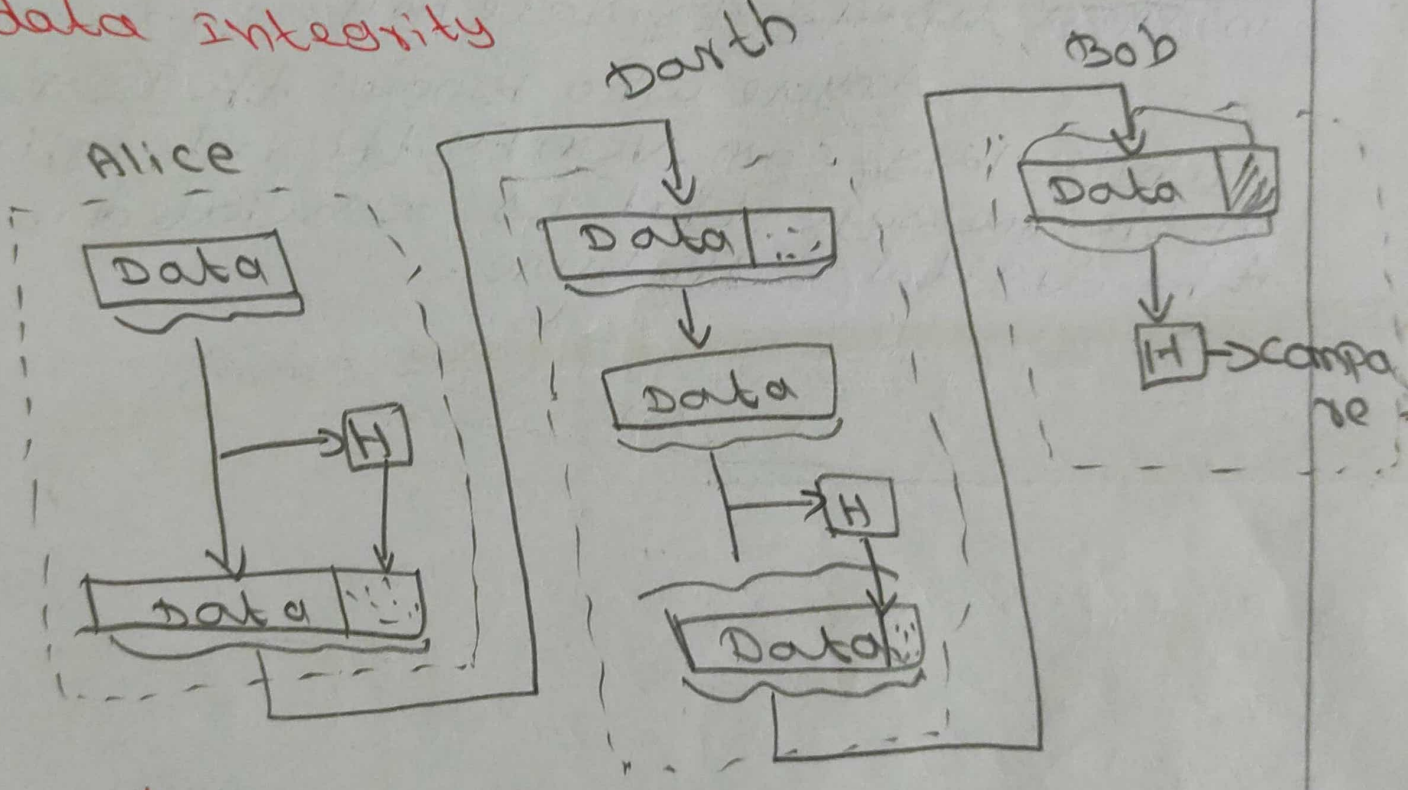
M.A is a mechanism used to verify the integrity of a message. M.A assures the data received are exactly as sent (No modification, insertion, deletion, or replay).

In many cases, authentication mechanism assures the purpose identity of sender is valid. when hash function is used to provide M.A, the function value is often referred to as a message digest.

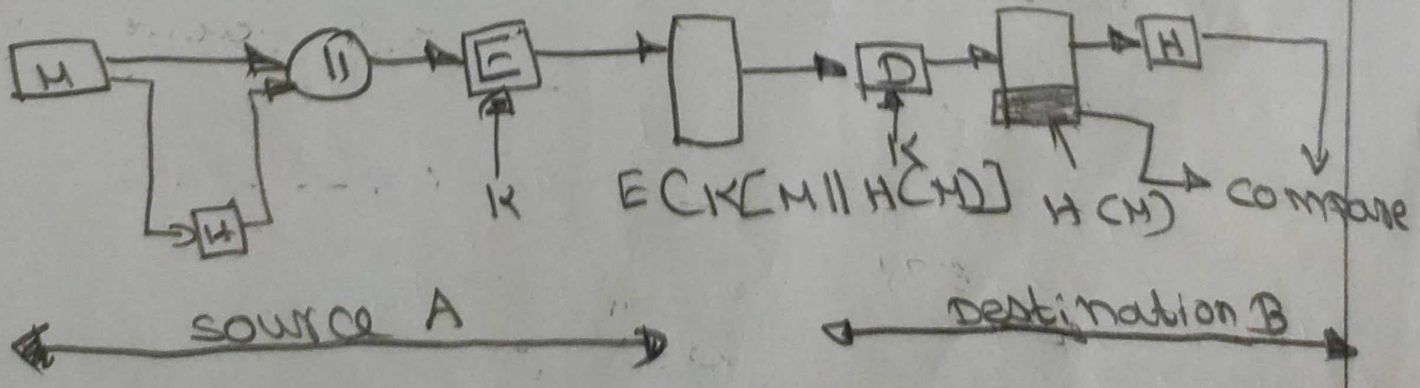




a) Use of hash function to check data integrity



b) man-in-the middle attack.



More commonly, message authentication is achieved using a message authentication code (MAC) also known as keyed hash function.

Digital signatures:

another similar to the message authentication application is the digital signature.

In the case of digital signature the hash value of the message is encrypted with a user's private key.

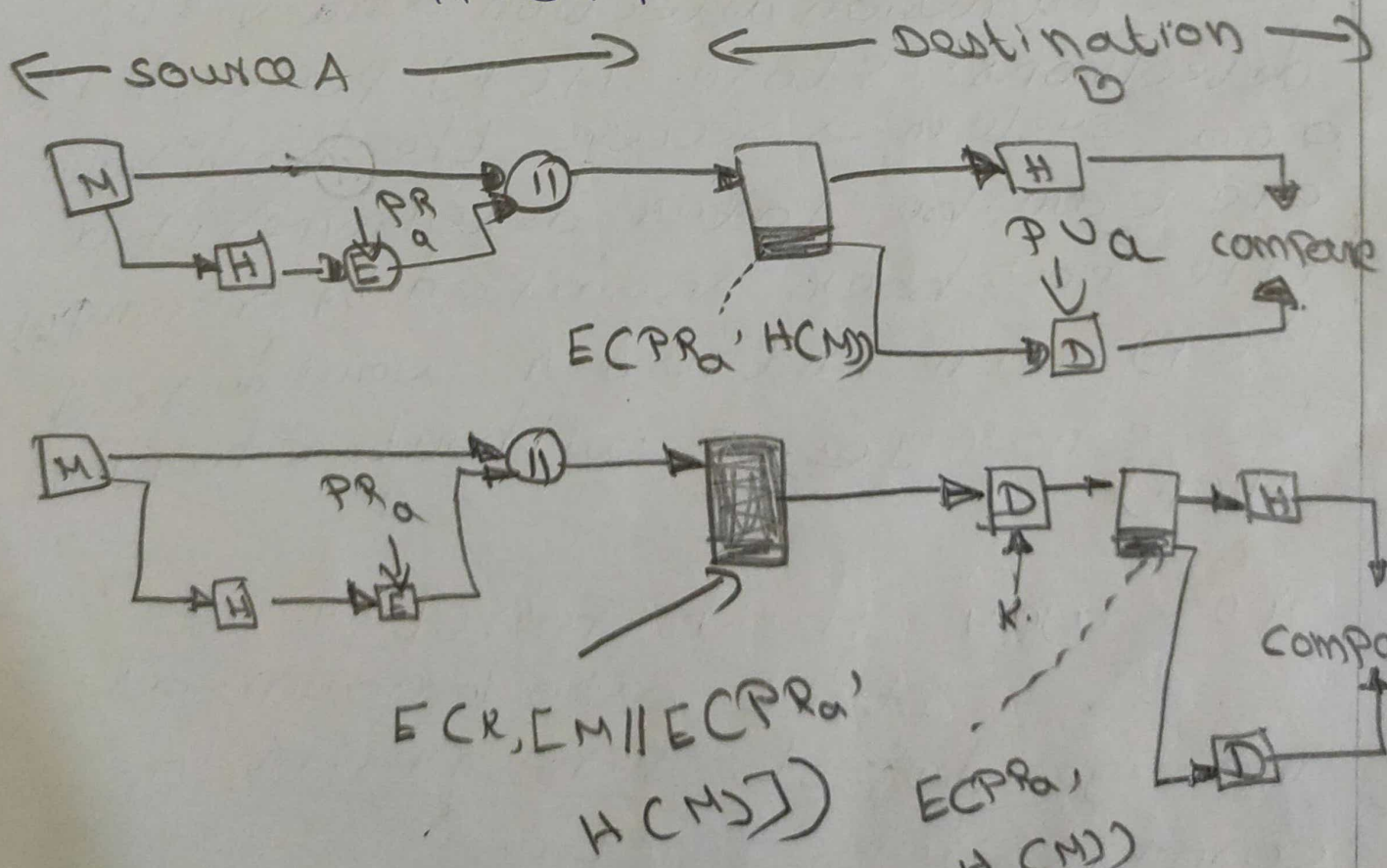
Anyone who knows the user's public key can verify the intergity of the message that is associated with the digital signature.

a. The hash code is encrypted, using public-key encryption with the sender's private key. This authentication. It also provides a digital signature, because only the sender could have produced the encrypted hash code. In fact, this the essence of the digital signature technique.

b. If confidentiality as well as a digital signature is desired, than the message plus the private-key-encrypted hashcode can be encrypted using a symmetric secret key. This is a common technique.

~~Password verification:~~

1 ~~test~~ F.



other application:

Hash function are commonly used to create a one-way password file.

Password protection:

The actual password is not retrievable by a hacker who gains access to the password file. In simple term when a user enters a password, the hash of that password is compared to the stored hash value for verification. This approach to password protection is used by most operating systems.

Hash functions can be used for Intrusion detection and virus detections. Store H(F) for each file on a system & secure the hash value. one can be later determine if a file has been modified by recomputing H(F). An intruder would need to change F without changing H(F).

one-way Hash Function:

It is also known as message digest, fingerprint or compression function.

⇒ It is a mathematical function s takes a variable-length input string s converts it into a fixed-length binary sequence.

⇒ one-way hash function is designed in such a way that is hard to reverse the process.

⇒ All modern hash algorithm produce hash value of 128 bits s higher.

⇒ Even a slight change in an input string should cause the hash value to change drastically. Even if 1 bit is flipped in the input string, at least half of the bits in the hash value will flip as a result this is called an avalanche effect.

⇒ A common way for one-way has functions is to deal with the variable length input problem is called as compression function.

⇒ compression function work by viewing the data being hased as a sequence of n fixed length blocks.

⇒ To compute the hash value of a given block, the algorithm need two things:

a) The data in the block

b) An input seed.

In Input seed is a set to some constant value (0), and the algorithm compules the hash value h_1 of the first. Next the hash value of the first block h_1 is used as the seed for the second block.

- The function proceeds to compute the hash value of the second block based on the data in the second block and the hash value of the first block, h_1. So, the hash value for block n is related to the data in block n and the hash value h_{n-1} (for $n > 1$) The hash value of the entire input stream is the hash value of the last block.

Birthday attack:

Birthday attack refers to a class of brute-force attacks.

- The attack is named after the statistical property of birthday duplication- you need only 23 people to have a larger than 50% chance that they are born on the same day of the year.
- This is due to the fact that each time you adding one person to the set of people you are looking for duplicates in, you are looking for duplicates against

all the people already in the set, not just one of them.

- Some technique can be used to look for conflicts in one-way function.
- Instead of taking one output of the one-way function you create or acquire a set of values that have a some property s then create another set of other values that have different properties (b) and try to find any value that is in both a and b. This is a much smaller problem that finding a value that ~~is in~~ b match a particular value in a.

The properties in a & b might for instance be.

1. 'a' contains secure hashes of an innocent message & b contains one of less innocent message, so the attacker can substitute the message at a later date.

2. a is the password hashes of a system the attacker wants to get an account on, and b is the set of password hashes that the attacker knows the password for.

3. a is the set of Public key from the discrete algorithms based cryptosystem where g, y, p are static while b is the set of $g^{1c} \bmod p$ functions that the attacker knows e' for.

- Birthday attacks are often used to find collisions of hash functions to avoid this attack, the output length of the hash function used for a signature scheme can be chosen large enough so that the birthday attack becomes computa-tionally infeasible.

SHA-1

It means secure Hash algorithm. It is a cryptographic hash Function which takes an input & produce a 160-bit (20 byte) has value known as a message digest.

SHA is based on the hash Function MD4, SHA-1 produces a hash value value of 160 bits.

SHA developed by the national institute of standard and techno-logy. (NIST).

Comparision of SHA Parameters

Algorithm	Message size	Block size	word size	Mess. Digest Form	No. of Steps
SHA-1	$< 2^{64}$	512	32	160	80
SHA-224	$< 2^{64}$	512	32	224	80
SHA-256	$< 2^{64}$	512	32	256	64
SHA 384	$< 2^{128}$	1024	64	384	80
SHA-512	$< 2^{128}$	1024	64	512	80
SHA 512/224	$< 2^{128}$	1024	64	224	64
SHA-512/256	$< 2^{128}$	1024	64	256	80

both SHA-1 & SHA-256 are begins by converting the message to a unique representation of the message that is multiple of 512 bits in length without loss of information about its exact original length in bits as follows:

Append 1 to the message. Then add as many zeros as necessary to reach the target length, which is the next possible length that is 64-bit less than a whole multiple of 512 bits. Finally, as a 64-bit binary number, append the original length of the message in bits

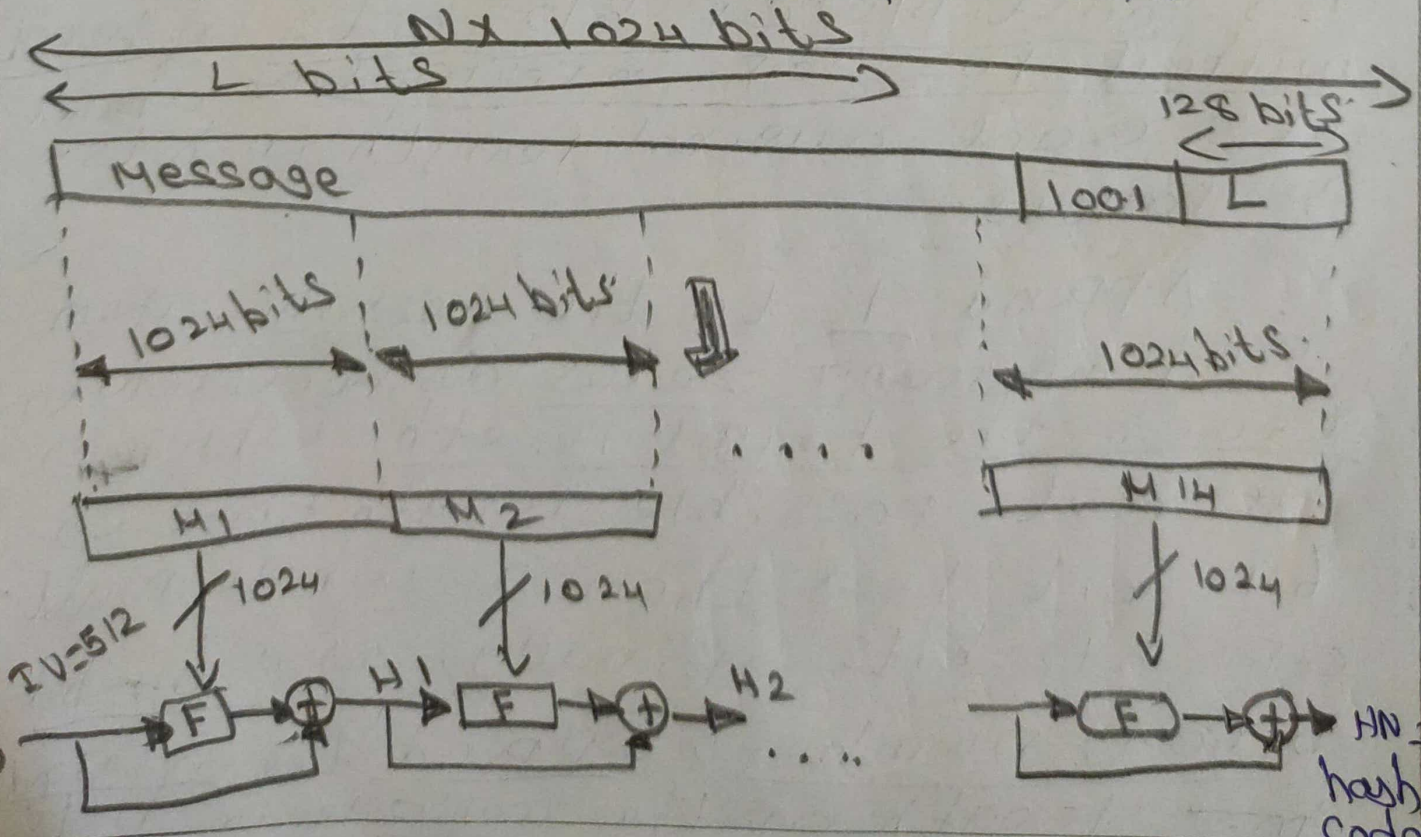
Description of SHA-1 1993

Expand each block of 512, when it is time to use it into a source of 80 32-bit subkeys as follows: The first 16 subkeys are the block itself.

SHA-1 produces a hash value of 160 bits. In 2002, NIST produced a revised version of standard 180-2 three new version of SHA, with hash value length 256, 384, & 512 bits. collectively all this hash algorithm known as SHA-2

SHA-12 Logic:

The algorithm takes as input a message with a maximum length of less than 2^{128} bits & produces as output a 512-bit message digests. The Input is processed in 1024-blocks.



Steps:

1. Append padding bits:
The message is padded so that its length is congruent to 896 modulo 1024 [length ≡ 896 (mod 1024)]. Padding is always added, even if the message is already of the desired length.
Padding consist of single 1 bit followed by the necessary no. of 0 bits.

2. Append length: A block of 128-bits is appended to the message. This block is treated as an unsigned 128-bit integer that contains the length of original message (before the padding)

3. Initialize hash buffer:
A 512 bit buffer is used to hold intermediate & final results of the hash function. The buffer can be represented as eight 64-registers (a, b, c, d, e, f, g, h) these register initialize to the following 64-bit integer (hexadecimal values:

a = 6A09E667F3BCC908
b = BB67AE8584CAA73B
c :
d :
e :
f :
g :
h :

These values are stored in big-endian format. which is the most

significant bytes of word in the low-address (left most) byte position)

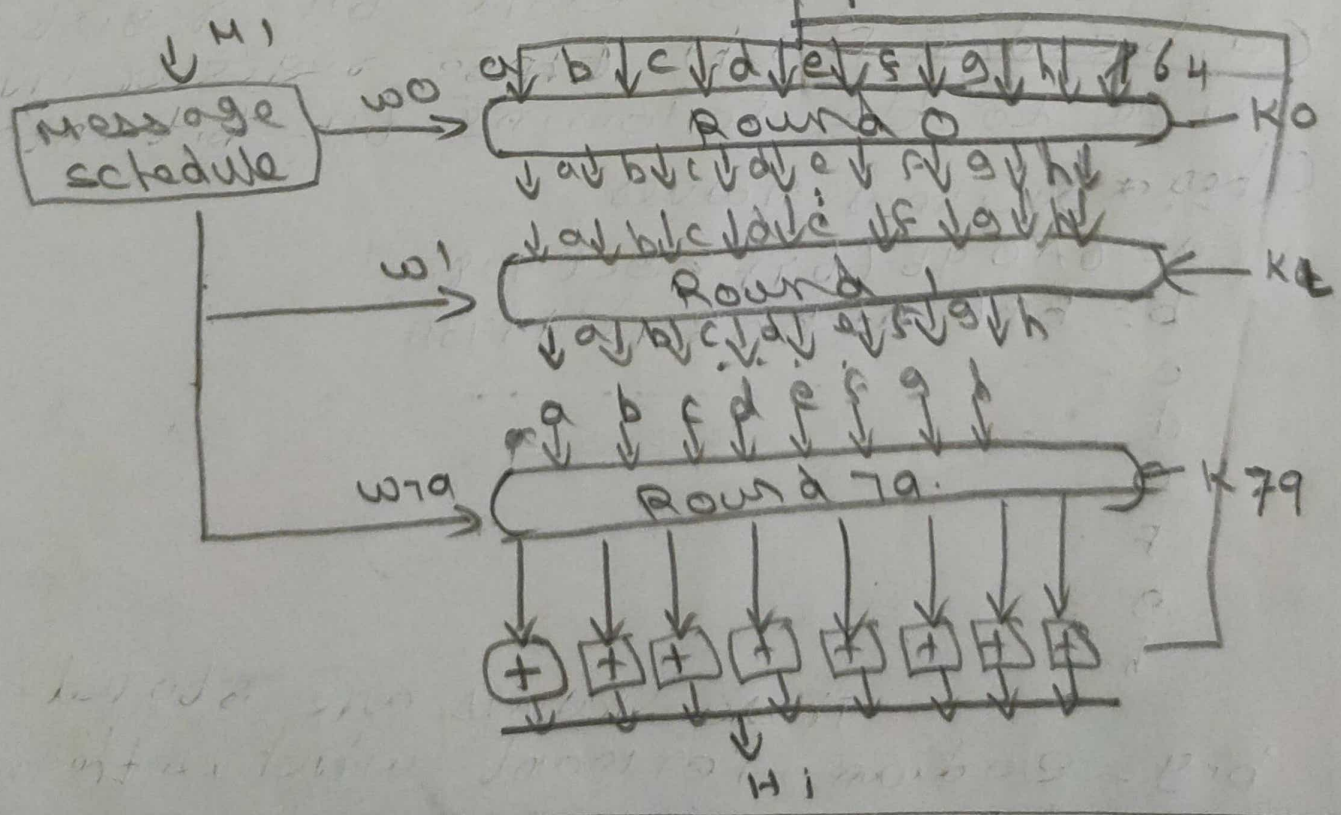
Step 4: process message in 1024-bit (128-bytes) blocks:

The heart of the algorithm is a module that consists of 80 rounds. This module is labeled F.

Each round takes as input the 512 bit buffer value, abcdefgh, & updates the contents of the buffer.

At input to the first round, the buffer has the value of the intermediate hash value H_{i-1}, each round t makes use of 64-bit value W_t, derived from the current 1024-bit block being processed (M_i).

Each round makes use of an additive constant K_t, where $0 \leq t \leq 79$ indicates one of the 80 rounds.



output: The output from the N^{th} stage is the 512-bit message digest.

The behaviour of SHA-512

$H_0 = IV$

$H_i = Sum_{64}(H_{i-1}, abcdefgh)$

$MD = H_N$

where IV = Initial Value of the abcdefgh buffer

abcdefgh = The output of the last round of processing of the i^{th} message block.

N = The no. of blocks in the message.

SUM64 = Addition modulo 2^{64} performed separately on each word of the pair of input.

MD = Final message digest value.

SHA-512 round Function:

Each round is defined by the following set of equation.

$T_1 = h + ch(e,f,g) + \left(\sum_1^{512} e\right) + W_t + K_t$

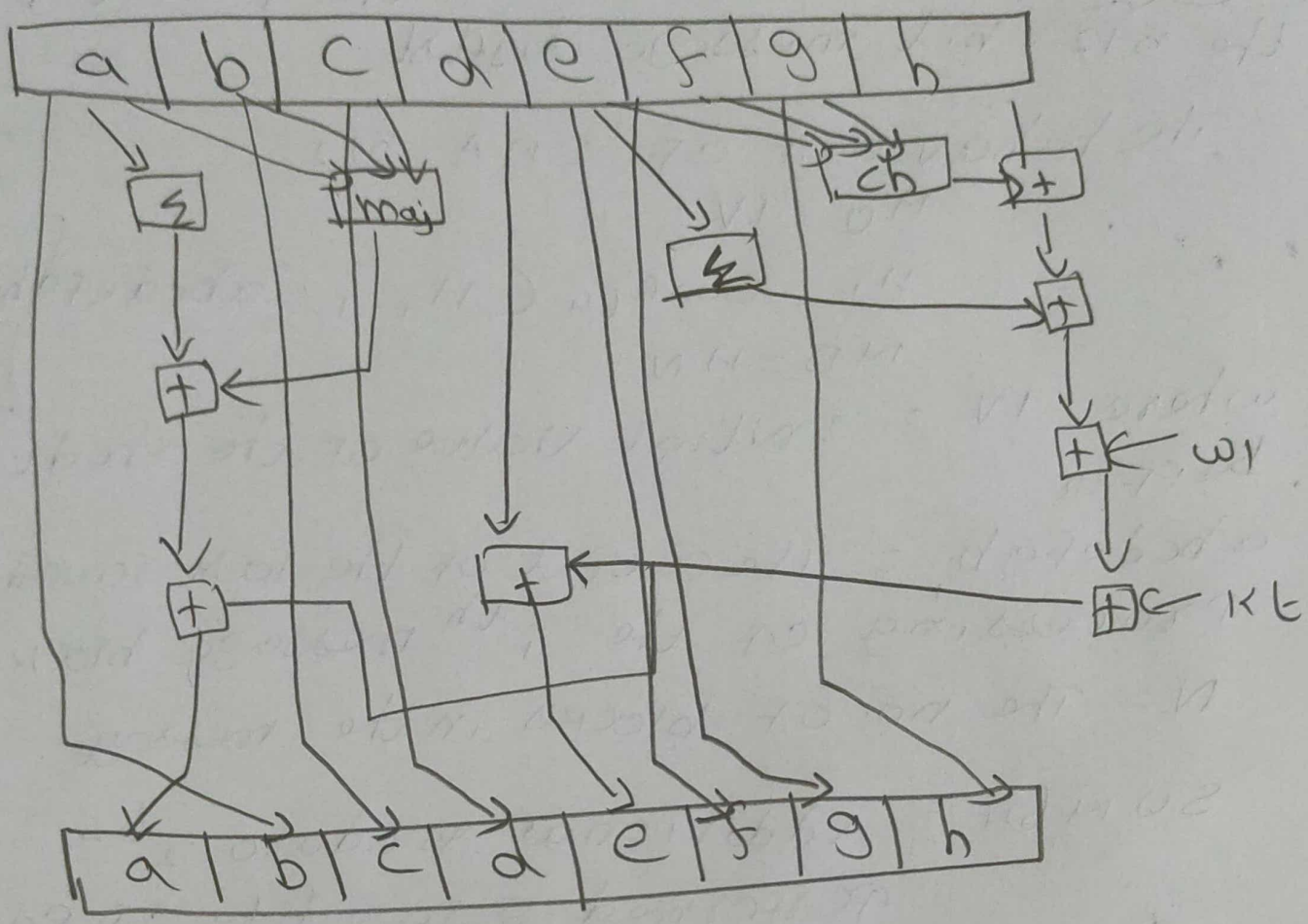
$T_2 = \left(\sum_0^{512} a\right) + Ma j(a,b,c)$

$a = T_1 + T_2$

$b = a$

$c = b$

$d = c$



$e = d + T_1$

$f = e$

$g = f$

$h = g$

List and explain the features of SHA-1

① The SHA-1 is used to compute a message digest for a message or data file that is provided as input.

2. The message or data file should be considered to be a bit string.

3. The length of the message is the number of bits in the message (empty message has length 0)

4. If the no. of bits in the message is multiple of 8, for compactness we can represent the message in hex.

5. The purpose of message padding is to make the total length of a padded message a multiple of 512.

6. The SHA-1 sequentially processes blocks of 512 bits when computing the message digest.

7. The 64-bit integer is l, the length of the original message.

8. The padded message is then processed by the SHA-1 as n 512 bit block.

Unit-IV

① Transport Level Security:

- TLS (Transport layer security) is a protocol that encrypts and delivers mail securely.

- TLS encryptions requires digital certificate → It contains identity info. about the certificate owners as well as a public key, used for encrypting communications.

Different code alert TLS Protocol:

① Record overflow: received with a payload (CT) whose length exceeds 2^{14} + 2048 bytes.

② unknown-ca: certicate not accepted

③ Accessdenied: Valid certificate received but when access control was applied, the sender decided not to proceed with the negotiation.

④ Decode-error: message Incorrect (length of range)

⑤ Protocol-version: The client attempted to negotiate is recognized but not supported.

⑥ insufficient security: Returned instead of handshake failure.

7. unsupported extension: sent by clients that receive an extended server hello containing an extension not in the corresponding client hello.

8. Internal-error: error unrelated to the peer or the correctness of the protocol makes it impossible to contin

9. decrypt-error: A handshake cryptograph operation failed, including being unable to verify a signature, decrypt a key exchange, or validate a Finished message.

(2) web security consideration:

The web is very visible:-
The www is widely used by business, government agencies and many individu
But the internet & the web are extremely vulnerable to compromises of various sorts, with range of threats.

→ complex s/w hides many security flaws.

→ web servers are easy to configure & manage. users are not aware of the risk.

passive attack
→ network traffic b/w browser & server.

Active attacks → impersonating another user, altering message in transmit b/w client and server & altering information on a website.

The web needs added security mechanisms to address these threats.

(24) web traffic security approaches:

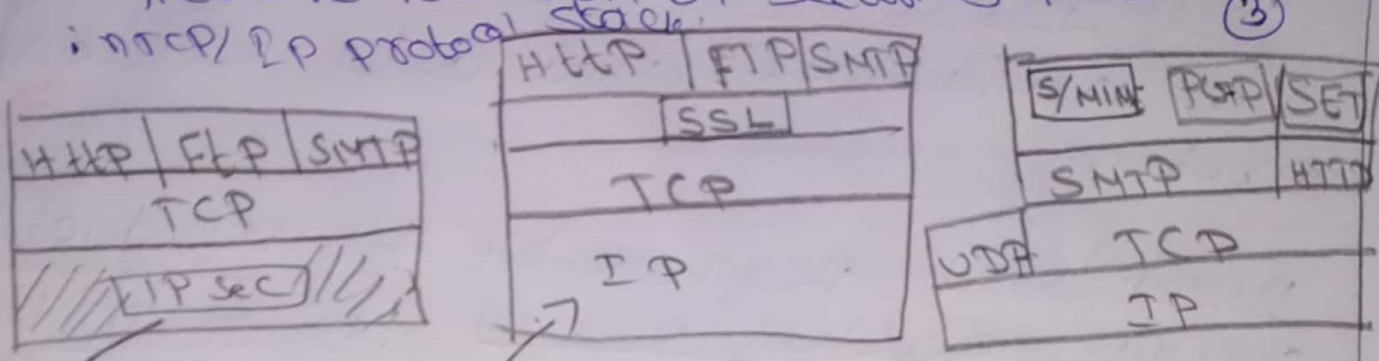
Various approaches are used for providing security to the web. one of the example is IP Security.

following table shows the comparison of threats on the web.

Parameters	Threats	Consequences	Counter Measure
Integrity	1. Modification of user data 2. Trojan horse browser 3. Modification of memory 4. Modification of message traffic in transit.	1. Loss of info. 2. compromise of machine 3. Vulnerability of another threats.	crypto graphic checksum

confidentiality	1. Eavesdropping on the net 2. Theft of info. From server 3. Theft of data from client. 4. Info. about network	1. Loss of Info. 2. Loss of Privacy	Encryption web proxy
Denial of Services	1. Killing of user threads 2. Flooding machine with with bogus request 3. Filling up disk or memory 4. Isolating machine by DNS attacks	1. Disruptive 2. Annoying 3. Prevent user from getting work done.	Difficult to Prevent
Authentication	1. Impersonation of legitimate user 2. Data forgery	1. Misrepresentation of user	Cryptographic techniques.

Relative location of security facility: ③



Network level — Filtering capability

one way — web security

Transport level

Application level

③ TLS Layer security and hand shake protocol:

→ Feature of mail servers designed to secure the transmission of e-mail from one server to another using encryption technology.

→ Reduces the risk of mail forgery communication.

Browser needs while transaction on Internet:

1. Make sure the server belongs to the actual vendor.
2. Contents of message are not modified during transition.
3. Make sure that the imposter does not interpret sensitive information such as credit card number

Two protocols:

a) HandShake and data exchange protocol:

HandShake: responsible for negotiating security, authenticating the server to the browser → defining other communication parameters

It allow authentication b/w the server and client and the negotiation of an encryption algorithm & cryptographic keys before the app. protocol transmits or receive any data

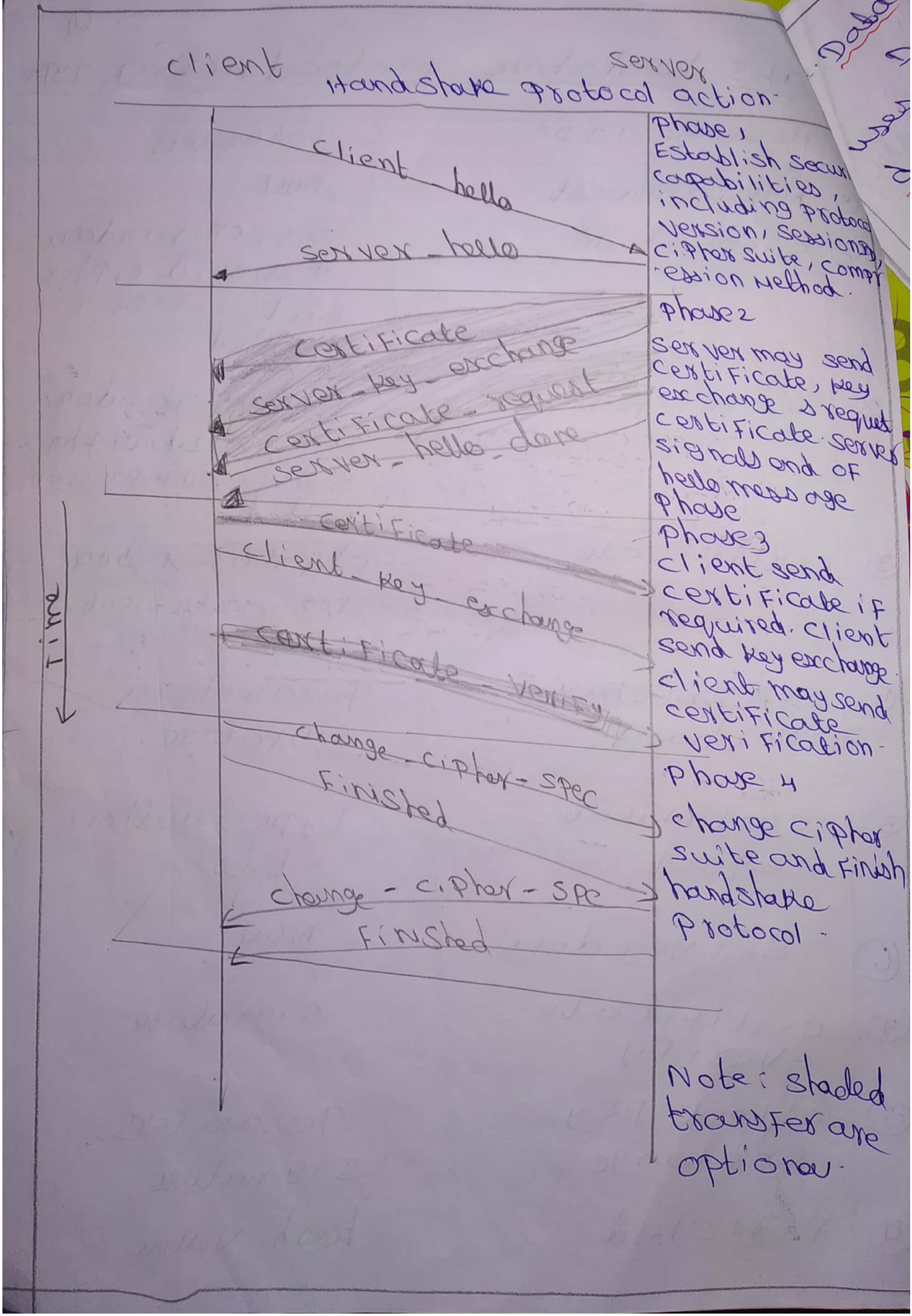
Format of message exchange b/w the client & server: Each message has 3 fields.

1. Type (1 bytes): Indicates one of 10 messages
2. Length (3 bytes) The length of the message in bytes.
3. content ($\geq$ bytes): The parameter associated with this message.

The initial exchange needed to establish a logical connection b/w client & server. It is of 4 phases.

TLS handshake protocol message type

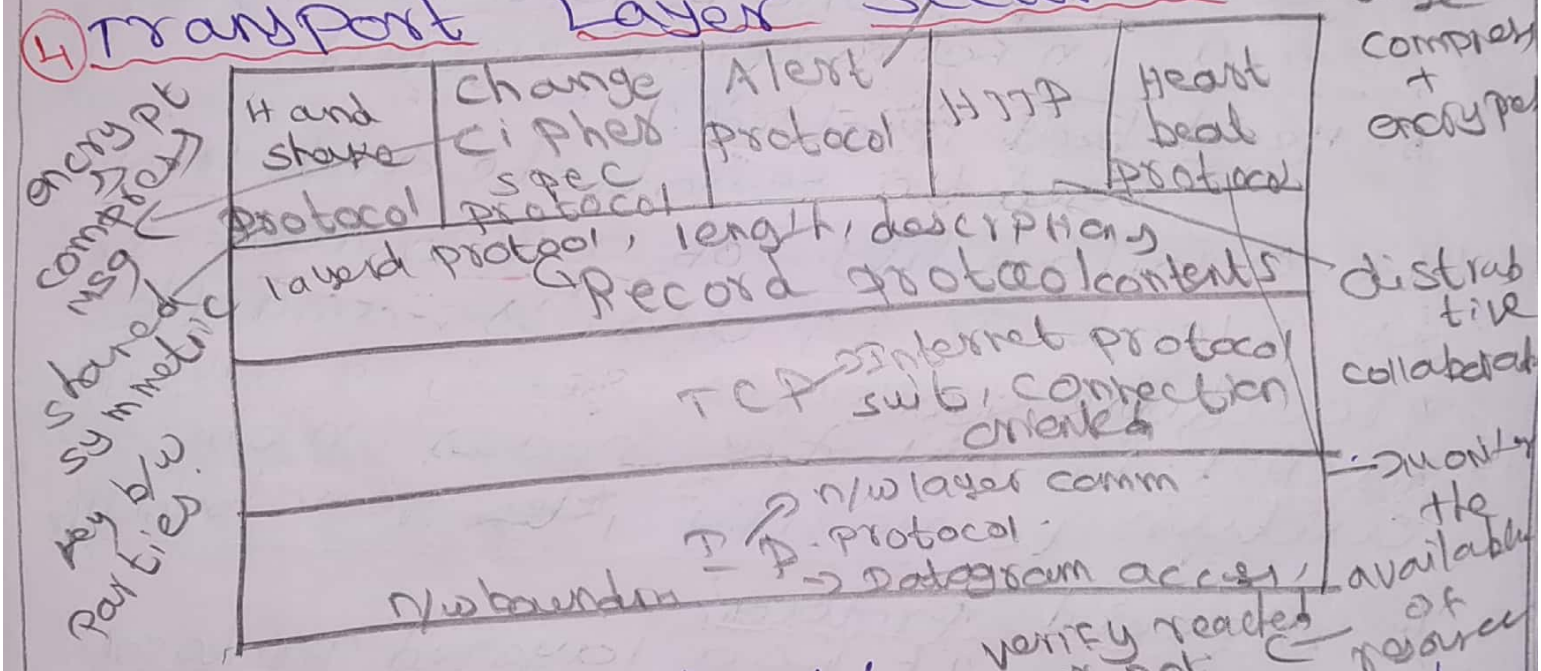
	Message Type	Parameters
①	hello-request	nul
②	client_hello	version, random, sessionid, cipter suit, compression Method.
③	server_hello	version, random, sessionid, cipter suite, compression method.
④	certificate	chain of X.509 V3 certificater
⑤	server-key-exchange	Parameter, signature.
⑤	certificate-request	type, authori-ties.
⑥	Serverdone	Nul
⑦	certificate-verify	signature
⑧	client key exchange	Parameters, signature
⑨	Finished	hash value.



4. Data exchange record protocol:

Data exchange (record) protocol uses the secret key to encrypt the data for secrecy and to encrypt the message digest for integrity. The TLS record protocol to designed to protect confidentiality by by using asymmetric data encryption.

(4) Transport Layer Security:



Hand shake protocol: It uses public key infrastructure PKI to establishes a shared symmetric key b/w the parties to ensure confidentiality, integrity & comm. data.

change cipher spec protocol

signaling strategies. This protocol consists of a single message, which is encrypted & compressed under the current connection state. 1 bytes.

3. Alert Protocol:
used to convey SSL-related alerts to the peer entity. alert messages are compressed and encrypted, as specified by the current state. each message consists of 2 bytes.

4. HttP:
Hyper text transfer protocol is an internet protocol suit model distributed, collaborative, hyper media information system.

5. Heart beat protocol:
used to negotiate and monitor the availability of a resources. such as floating IP address, and the procedure involves sending network packet to all the nodes in the culture to verify its reachability

6 Record protocol:
It is a layered protocol each layer messages may include fields of length, ~~message~~ description contents.

7. ICP
one of the main protocols of the internet protocol suite. It originated in initial n/w implementation. connection oriented

8. IP
It is a network layer comm. protocol in the internet protocol suit for relaying datagram across n/w boundary.

ireless Network Security:

In wireless LAN, Data transmission and receiving medium is an air using radio Frequency.

It minimize the wiring connection. wireless LANS combine data connectivity with user mobility.

wireless Lan used by type of organization and users.

Security issue wireless network is more critical then wired network.

Packet sent on wireless system is quite broadcast so it is possible to otheruser to collect data.

Higher security of risk in wireless network:

① Communication channel:
wireless network typically involves broad cast communication jamming then wired network.

② Mobility: wireless devices are far more portable & mobile, thus resulting in a no. of risk.

③ Accessibility: some wireless device such as sensor & robots may be left unattended in remote and/or hostile location increase vulnerability of physical attack.

Types of wireless attack:

① Interruption of service:
Resource become unavailable because it is destroyed.

② Modification: Modification the database value, alter the program etc.

③ Fabrication: The attacker send Fake message to neighbouring nodes without receiving any related message.

④ Jamming: Dos attack. Jammer trasmit signal along with security threats.

⑤ Attack against encryption:
Encryption method 802.11b wireless Lan.

⑥ Brute force attack:
Variety of password try to crack.

⑦ Mis configuration:
Heavy load on the network admin, most of the access point are not configure properly.
High risk of being accessed by unauthorized or hacker.

⑧ Interception:
communication take place

- wireless medium easily intercepted receiver turned on property Frequency.

Aim is confidential info. that should be kept secret during the communication.

Information like Private key, Public key location or password.

How to secure wireless network:

1. Use encryption:

Built in encryption mech for router-to-router traffic.

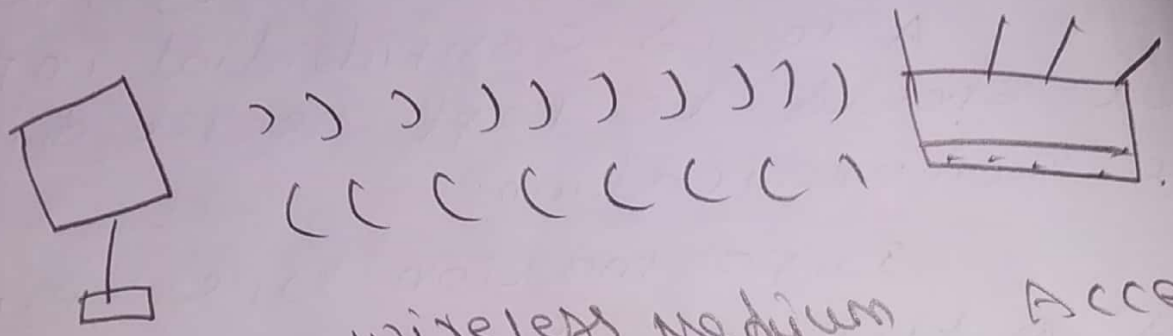
2. Antivirus and antispyware software, firewall.

3. Turn off Identifier broad-casting.

4. choose the identifier on your router from the default.

5. change your router preset password for administration.

6. Allows only specific computer to access your wireless network.



In simple terms, the wireless ~~comm~~ environment consists of 3 components that provide point of attack. The wireless client can be a cell phone, a wi-fi enabled laptop or tablet, a wireless sensor, a bluetooth devices, and so on.

The wireless access point provides a connection to the network or service.

Wireless Network Threats:

1. Accidental association → overlapping transmission
2. Malicious association → operate range to steal password.
3. Identify theft → Identity MAC address of computer
4. man-in middle attack.

Mobile device security

→ security measures designed to protect the sensitive information stored on and transmitted by smart phones, tablets, laptops & other mobile devices.

Elements in mobile device security

① Device security:

A no. of org. will supply mobile devices for employee use and pre-configure those devices to confirm to the enterprise security policy. org. should configure the device with security controls:

① Including the enable auto-lock. 2. Enable PIN or password protection 3. Avoid using auto-complete features that remember user names or passwords 4. Enable remote wipes. Ensure or make sure s/w, OS and appli-cation up to date 5. Install antivirus s/w

② Traffic security:

Based on the usual mechanism for encryption & authentication. All traffic should be encrypted & travel by secure means such as ssl or virtual private network. can be confi-gured so that all traffic between the mobile devices and the organization network is via a VPN → virtual private n/w. ↳ you to create a secure connection to another one over internet

3. Barrier security

The organization should have security mechanism to protect the network from unauthorized access. The security strategy can also include firewall policies specific to mobile device traffic.

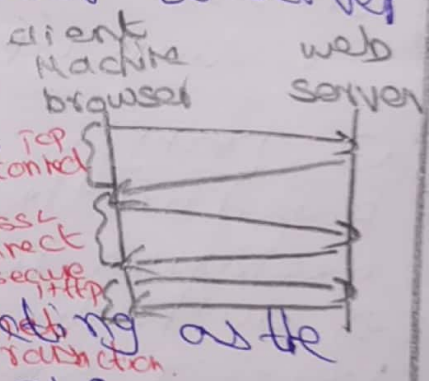
Firewall policies can limit the scope of data & appli-cation access for all mobile devices.

HTTPS:

HTTPS refers to the combination of HTTP and SSL to implement secure communication between a web browser and a web server. The HTTP capability is built into all modern web browsers.

The HTTPS is used, the following elements of the communication are encrypted.

- → URL of the requested document
- → Contents of the document
- → Contents of browser forms (filled by browser user)
- → Cookies sent from browser to server and from server to browser
- → Contents of HTTP header.



Connection Initiation:

→ For HTTPS, the agent acting as the HTTP client also acts as the TLS client. The client initiates a connection to the server on the appropriate port and then send the TLS client Hello to begin the TLS handshake.

When the TLS handshake is Finished, the client may then initiate the first HTTP request. All HTTP data is to be sent as TLS application data.

normal HTTP behavior, including retained connection, should be followed.

3 Levels of awareness of a connection in HTTPS. At the HTTP levels, an HTTP client request connection to an HTTP server by sending a connection request to the next lowest layer.

Typically, the next lower layer is TCP, but it also may be TLS/SSL.

At the level of TLS, a session is established between a TLS client and a TLS server.

The session can support one or more connections with the establishment of a TCP connection between the TCP entity on the client side and the TCP entity on the server side.

Connection Closure:

An Http client or server can indicate the closing of a connection by including the following line in a HTTP record:

Connection: Close.

This indicates that the connection will be closed after this record is delivered.

At the TLS level, the proper way to close a connection is

For each side to use the TLS alert protocol to send a close_notify alert.

A TLS implementation may, after sending a clouse alerts before closing a connection. TLS imp. after sending a clouser alert, generating an "incomplete close".

Http clients also must be able to cope with a situation in which the underlying TCP connection is terminated without a prior close_notify alert and without a connection: close indicator.

(8) SSH:

Secure shell is a protocol for secure network comm. designed be relatively simple & inexpensive to imple ment.

SS for secure remote login → other secure network services over an insecure network.

Why use SSH:

1. Designed to be a secure replace of r/login, telnet.
2. Strong authentication. closes several security

3. Improved Privacy. All communications are automatically & transparently encrypted.

4. Arbitary TCP/IP ports can be redirected through the encrypted channel in both direction.

5. The software can be installed and used even without root privileges.

6. optional compression of all data with gzip, which may result in significant speedup on slow connection.

SSH User Authentication protocol	SSH connection protocol
Authenticates the client-side user to the server	Multiplexes the encrypted tunnel into several logical channel.
SSH Transport Layer protocol	
provides server authentication, confidentiality, and integrity. It may optionally also provide compression.	
TCP	
Transmission control protocol provides reliable, connection oriented end-to-end delivery.	
IP	
Internet protocol provides datagram delivery across multiple networks.	

SSH Protocol Stack.

① SSH User user authentication Protocol

→ The user authentication protocol provides the means by which the client is authenticated to the server.

a) Message type and Formats:

3 types of messages are always used in the user authentication protocol. Authentication requests from the client have the format.

byte	SSH_MSG_USERAUTH_REQUEST(50)
string	user name
string	service name
string	method name
....	method specific fields

where user name is the authorization identity the client is claiming, service name is the facility to which the client is requesting access, and method name is the authenticated method being used in request. The first byte has decimal value 50, which is interpreted as SSH_MSG_USERAUTH_REQUEST.

b) Message exchange steps:

① client send SSH_MSG_USERAUTH_REQUEST

2. server checks → user name valid → if not → server returns SSH_MSG_USERAUTH_FAILURE → Fails.

3. IF user → Valid → proceeds to step 3.

4. Server returns → SSH_MSG_USERAUTH_FAILURE → one or more Authentication method is used.

5. Client → select one of acceptable authentication methods → send SSH_MSG_USERAUTH_REQUEST
   → with method name → exchange to be performed.

6. IF authentication success → step 3 will be repeate.

7. All authentication method succeed → server send SSH_MSG_USERAUTH_SUCESS →

Authentication protocol over

① Authentication Method

The server may require one or more of the following authentic methods.

① Public key: Public key algorithm chose Signature → key is authentic and

② Password: client send → MSG Plainext → Password

which is protected by → encryption by the transport Layer Protocol.

② connection protocol:

The SSH connection protocol runs on top of SSH transport Layer Protocol. -Secure authentication connection protocol to multiplex a number of logical channel.

③ channel mechanism:

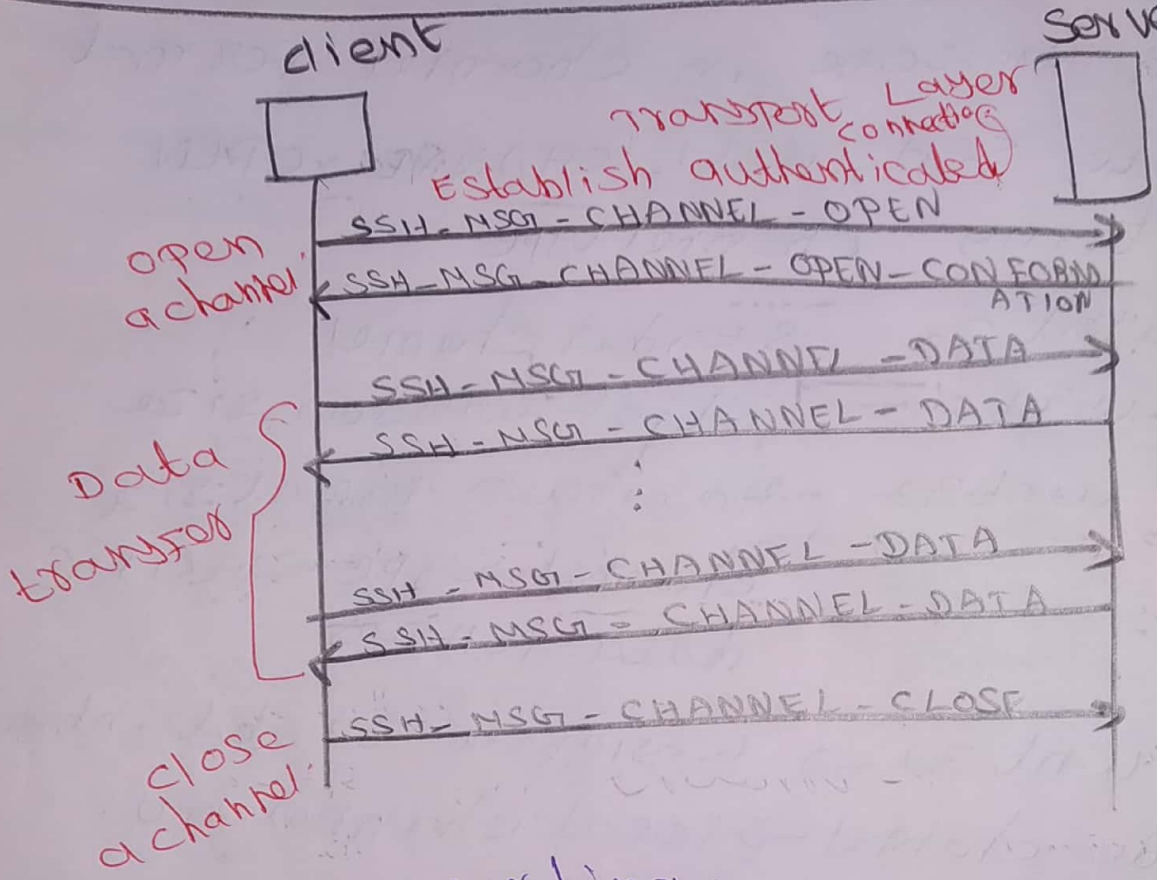
All types comm. using SSH, such as a terminal session, are supported using separate channel. For each channel, each side associates a unique channel number, which need not be the same on both ends. window mechanism will follow. No data may be sent over to a channel until a message is received to indicate that window space is

send Message in channel Format

byte SSH_MSG_CHANNEL_OPEN
string channel type
uint32 sender channel
uint32 initial window size
uint32 Maximum packet size
... channel type specific data follows

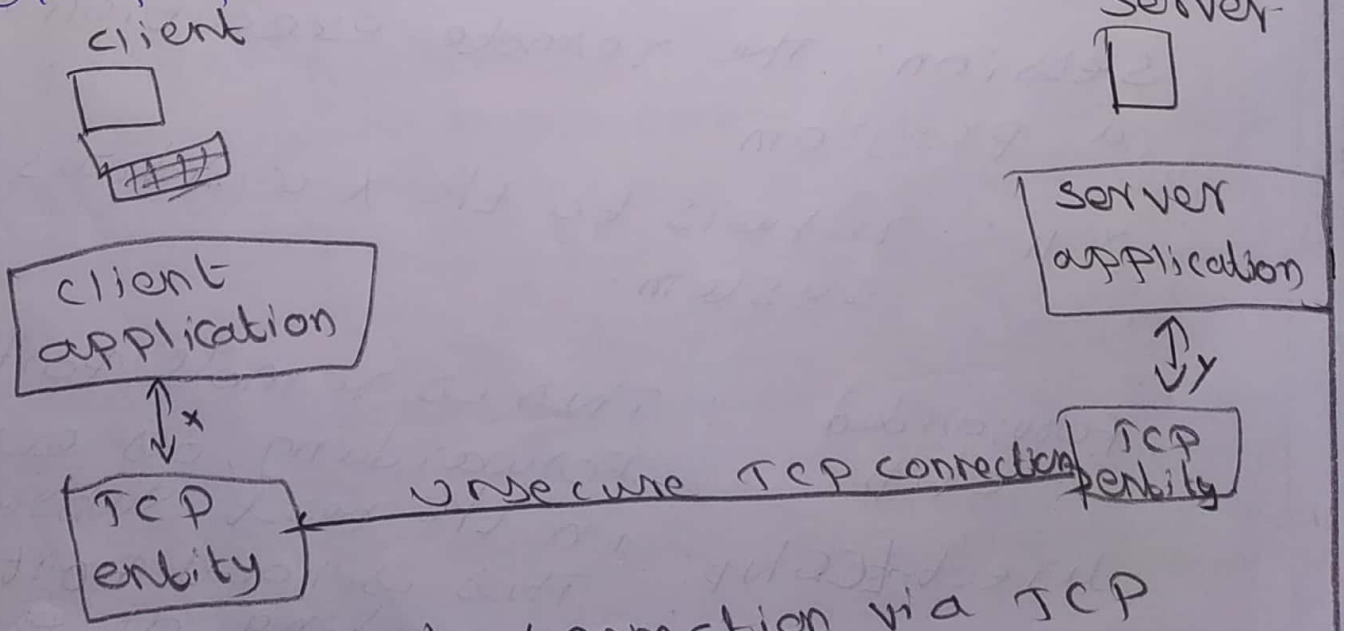
uint32 → unsigned 32-bit integer.
Sender channel → local channel no.
Initial window size → How many bytes of channel data can be sent to the sender of this msg without adjusting window.

(b) channel Types: Four channel types are recognized in the SSH connection protocol specification.
session: The remote execution of a program.
X11: refers to the X windows system.
Forwarded TCP/IP: This is remote port forwarding, as explained in the next subsection.
direct-TCP/IP: This is local port forwarding, as explained in the next subsection.

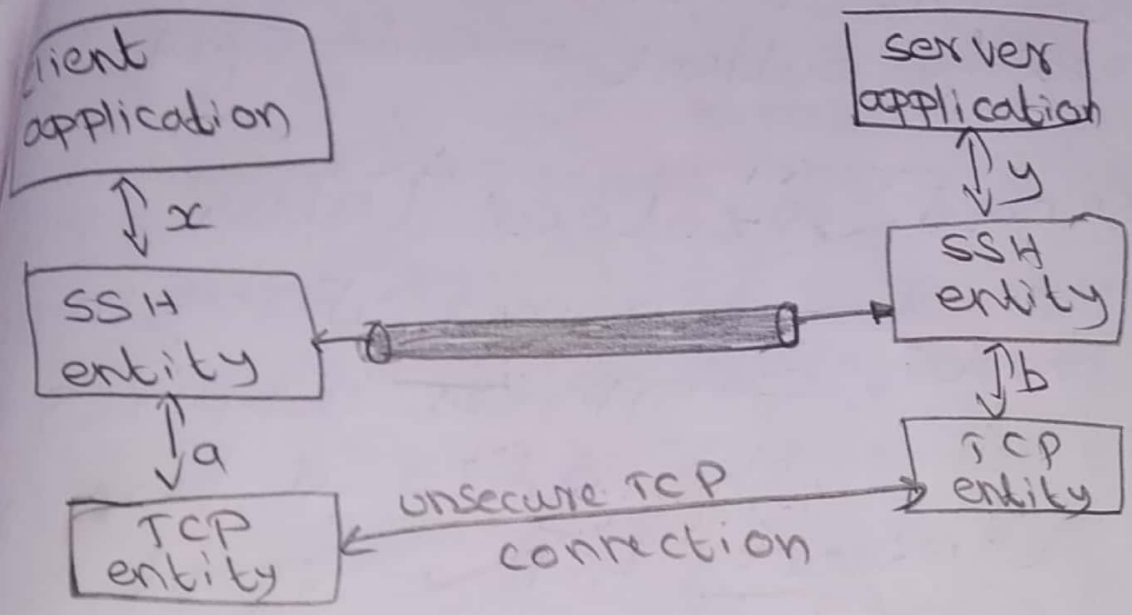


(c) Port Forwarding:

Port forwarding provides the ability to convert any insure TCP connection into a secure SSH connection. This also refered as SSH tunneling. we need to know what a port is in the context of a user of TCP.



(a) connection via TCP



(b) connection via SSH tunnel

(8) SSL and transport Layer Security:

SSL → standard secret layer is a standard security proto-col for establishing encrypted link b/w web server and a browser in an online communication.

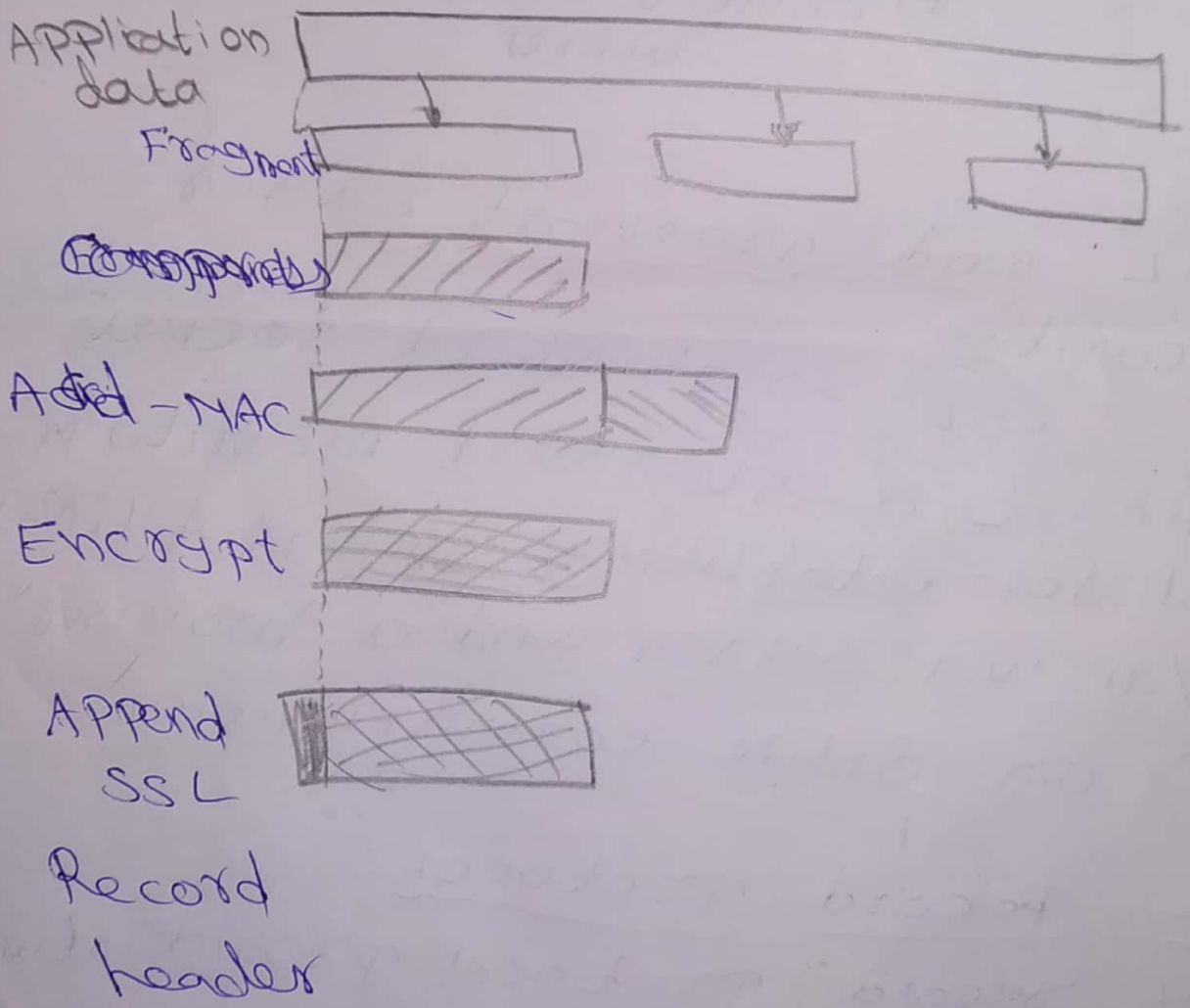
SSL Record protocol:

SSL record protocol provides two services for SSL connection.

1. confidentiality - Handshake protocol for encryption of SSL Payload

2. Message integrity: Handshake Proto
For Message authentication code (MAC)

The Record protocol takes app. message to trasmit, Fragment the data, compress, applies MAC, encrypts, adds a header and trasmit TCP segment.



IEEE 802.11 wireless LAN:

IEEE 802 is a committe that has developed standards for a wide range of local area networks (LANS). In 1990, the IEEE 802 committee formed a new working group IEEE 802.11 with a charter to develop protocol and transmission specifications for wireless Lan (WLan). More demand need for WAN again IEEE intro. 802.11

Broad Industry accepted 802.11 Standard.

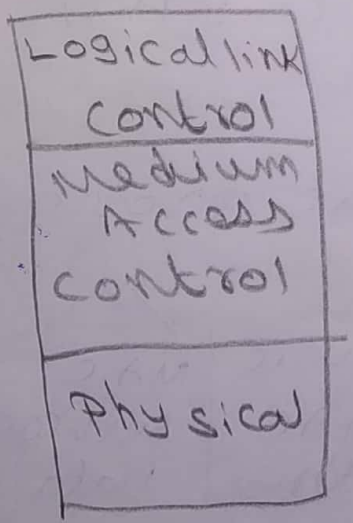
Wi Fi → wireless Fidelity → wi Fi certi Fi cate.

IEEE 802.11 protocol Architecture:

It is a layered set of protocol.

General IEEE 802 Function

Specific IEEE 802.11 Functia.



Flow control
Error control

Assemble data into Frame
Addressing.
Error detection
Medium access.

Encoding / decoding of signals
Bit transmission / reception.
Transmission medium

Reliable data delivery.
wireless access control protocols.

Frequency band definition
wireless signal encoding.

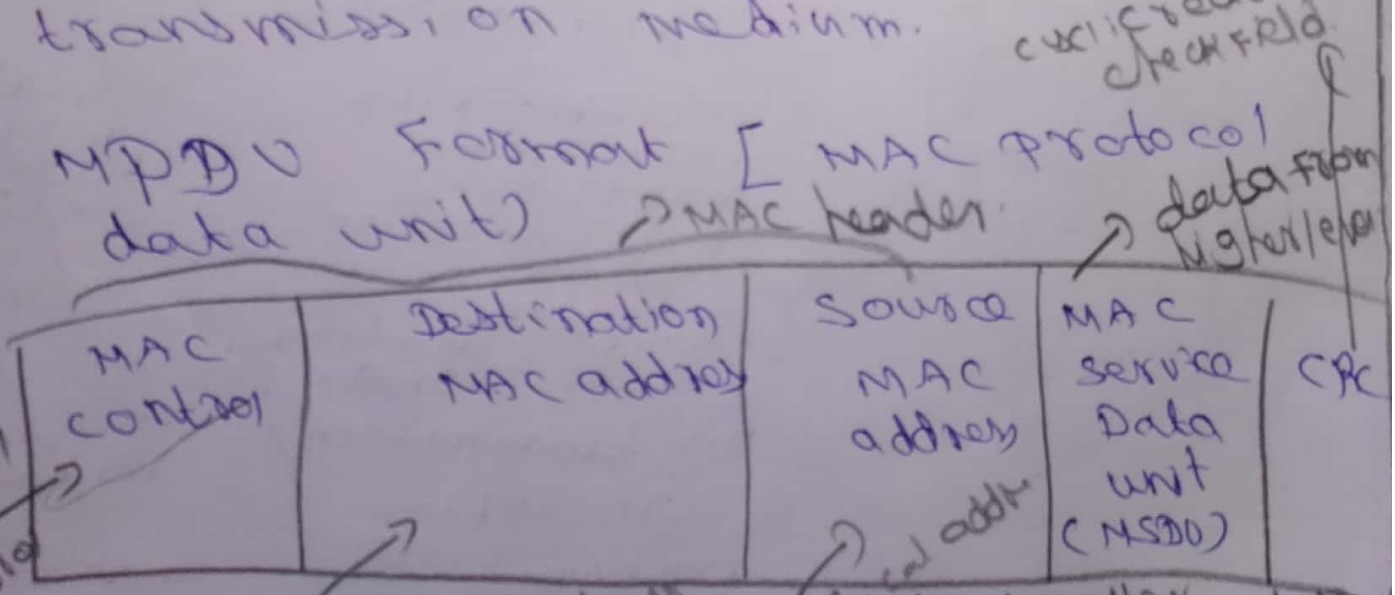
Media access control:

All Lan consist of collections of devices that share the n/w transmission capacity. Some means of controlling access to the transmission medium is needed to provide an orderly and efficient use of that capacity. This function of a media access control (MAC) layer.

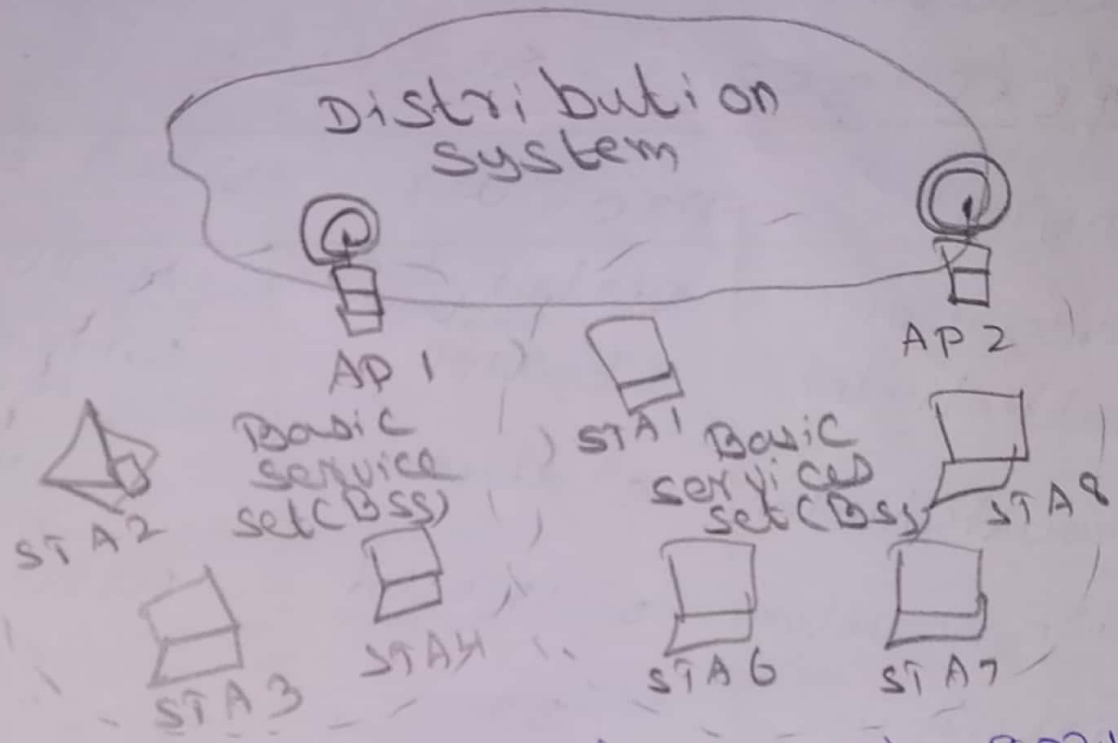
The MAC layer receives data from a higher-layer protocol, typically the Logical Link control (LLC) layer, in the form of a block of data known as the MAC Service data unit (MSDU). In general MAC layer perform following function:

- on transmission, assemble data into frames.
- on reception, disassemble frame, and perform address recognition and error detection.
- Govern access to the LAN transmission medium.

MPDU Format [MAC protocol data unit]



IEEE 802.11 Network components and Architectural model:



The model developed by the 802.11 working group. The smallest building block of a wireless LAN is a basic service set (BSS) which contains some wireless station executing the same MAC protocol & competing for access to a back-bone distribution system DS through the Access point AP → bridge and a relay point.

one station BSS want to comm. with another station BSS → MAC frame will send to the AP (accesspoint) and then. From the AP to the destination station

Extended Service set (ESS):

consists of two or more sets interconnected

by a distribution system. The ext service set appears as a single logical LAN to the logical link Control (LLC) level.

IEEE 802.11 services

service	Provider	Used to support
Association	Distributed system	MSDU delivery
Authentication	station	LAN access & security
Deauthentication	station	"
Disassociation	distributed system	MSDU delivery
Distribution	DS	"
Integration	DS	"
MSDU delivery	Station	"
Privacy	station	LAN access & security
Reassociation	DS	MSDU delivery

Association:

Before station (STA) is allowed to send a data message via an AP. it first becomes associated with AP.

Association:

This service allows the station to with its association from one access point to another.

. Both Association → reassociation are initiated by the station.

Disassociation:

Associated b/w the station and the AP is terminated. This can be initia -ted by either party.

Distribution → Integration:

simply getting the data from the sender to the intended receiver.

The message is sent to the local access point → then distributed through DS to the output AP that the recipient is associated with.

Services:

① Authentication → used to establish the identity of station.
② Deauthentication → services is involved whenever an existing auth. to be terminated.
③ Privacy: → other receipent should not read message

10 IEEE 802.11i wireless LAN Security specification:

① Authentication → exchange b/w a user and an AS that provide mutual authentication and generate temporary keys to be used b/w the client & the AP over the wireless link.

② Access control: This function enforces the use of the authentication function, routes the msg properly, & facilitates key exchange. It can work with a variety of authentication protocols.

③ Privacy with Message Integrity: MAC-level data are encrypted along with a message integrity code that ensure that the data have not been altered.

Wireless application protocol Architecture:

Main objectives:

i) To bring diverse internet content
ii) To provide data services to mobile users & PDA users.
iii) To provide better protocol suit to support worldwide wireless.

, Internet app.
ii) To support wireless like CDPD, GSM etc.

Many solutions derived by WAP forum to meet above requirements they are:

① Scalable: → Customer needs / services
② Interoperable: Allows the terminal s/w for several vendor to comm. with many network s of different providers.
③ Efficient: quality of service suitable to the requirement of wireless and mobile network.
④ Reliable: To provide predictable & consistent platforms for deployment of services.
⑤ Secure: It should have provisions to secure data & preserve data integrity & devices.

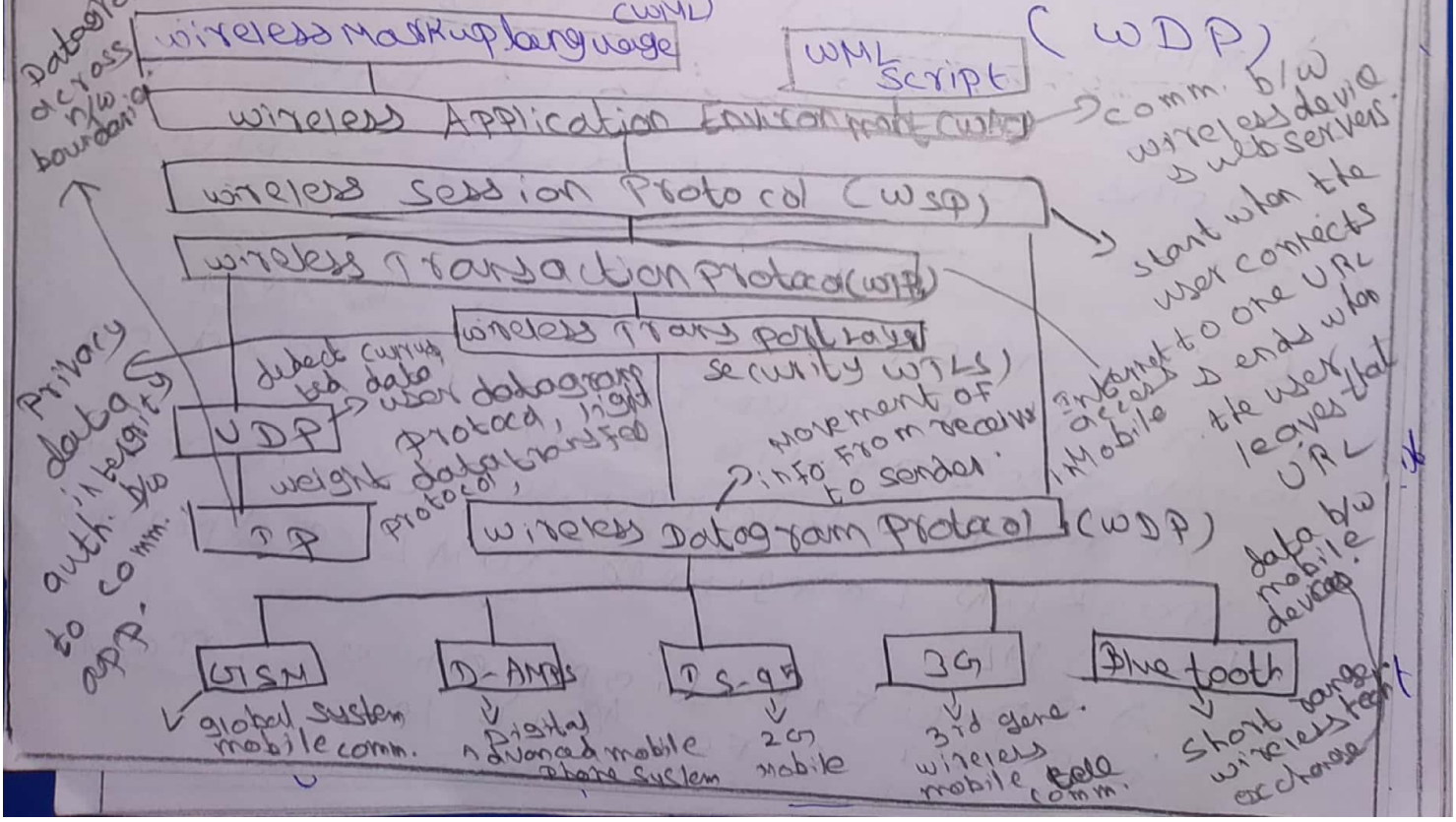
WAP Architecture includes:
1. A programming model based on www programming model.
2. A mark up language, the wireless mark up Language WML adhering to XML.
3. A specification of a small browser (for mobile)

4. A light weight comm. protocol stack.

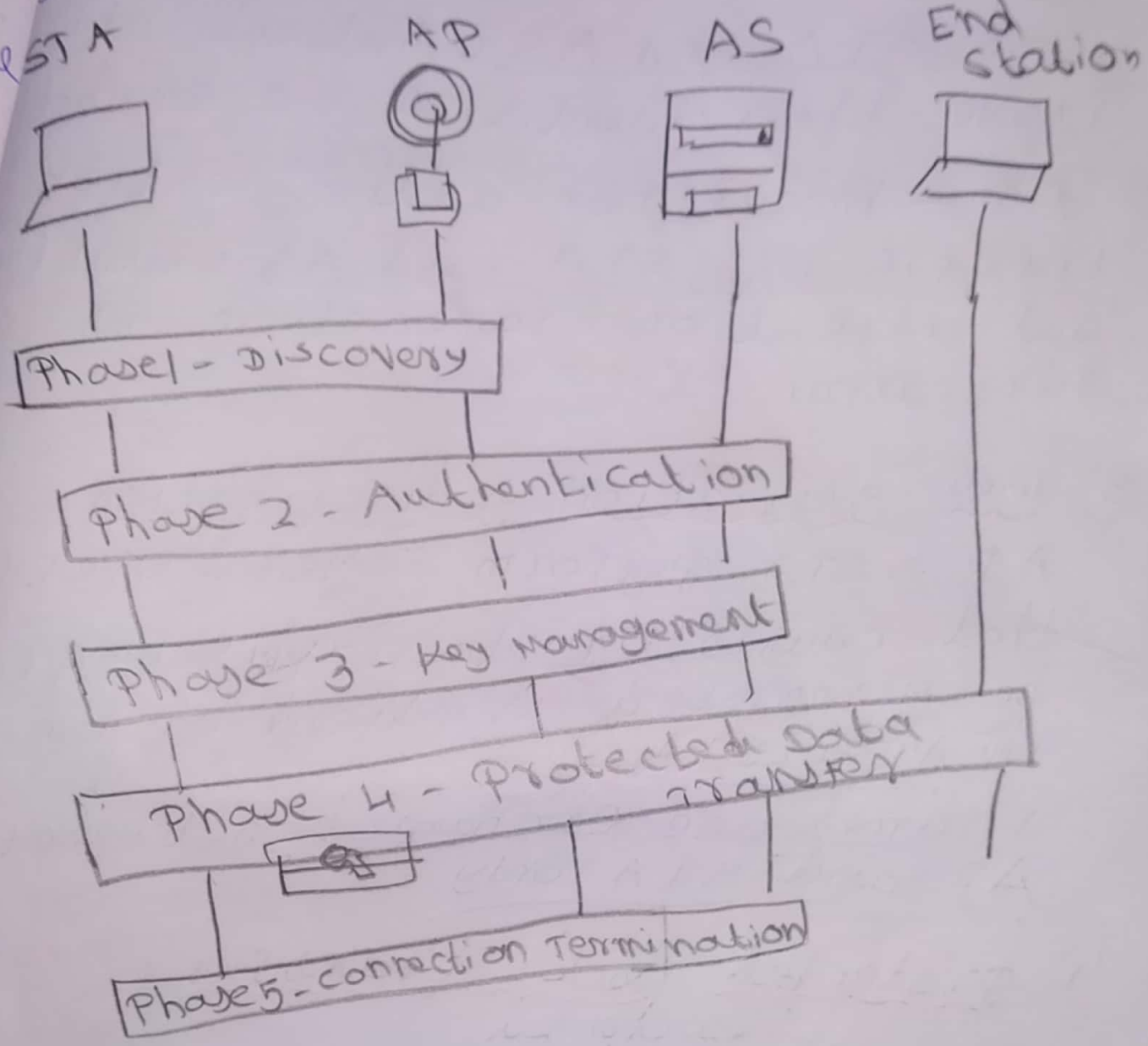
5. A Framework for wireless Tele-phony application (WTAS)

WAP support different protocol and modules.

1. wireless markup language (WML)
2. wireless application environment (WAE)
3. wireless session protocol (WSP)
4. wireless transaction protocol (WTP)
5. wireless transport layer security (WTLS)
6. wireless Datagram protocol (WDP)



802.11i Phases of operation



Discovery:
→ An AP uses message called Beacon and Probe responses to advertise its IEEE 802.11i security Policy.
→ The STA uses these to identify an AP for a WLAN with which is wishes to communication.
→ STA Associates with AP → select → cipher suite & authentication mechanism when Beacons

and probe responses present a choice

2. Authentication:

The STA and AS (Authentication) Prove their identities to eachother.

AP → blocks non-authentication traffic b/w STA and AS until the authentication transaction is successful.

3. Key generation & distribution:

AP & STA perform several operation that causes cryptographic key to be generated & placed on the the AP & STA.

Frames are exchanged between the AP and STA only.

4. Protected data transfer:

Frames exchanged → by the STA and the end station through the AP.

Secure data transfer occurs b/w the STA and the AP only.

security is not provided end-to-end.

5. Connection termination:

The AP & STA exchange frames during this phase, the secure

nection is torn down and connection is restored to the iginal state.

pairwise master key derived from master key:

1. IF a PSK is used, then PSK is used as a PMK.

2. IF a MSK is used, then the PMK is derived from the MSK by function (if necessary)

By the end of the authentication phase, both AP & the STA have a copy of their shared PMK.

The PMK is used to generate the pairwise transient key (PTK) to be used for communication between an STA and AP after they have mutually authenticated.

PTK = HMAC (PMK || the MAC addresses of the STA and AP || nonces)