Date __/__/____

Saathi

INFORMATION SECURITY

PART-1

Chapter-1

Information Technology :- Information Technology is the vechicle that stores and transports information. a companies most valuable resource from one business unit to another...

Information Security :- Information security is a process of protecting information availability, data integrity and privacy.

* No collection of products or technology alone can solve every information security problem faced by an organization.

* Effective information security requires successful integration.

* Information security is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.

Saathi

Date __/__/____

Primary Goals / components / objectives :-

C I A

Confidentiality — Integrity — Availability

CIA triad

Confidentiality :- Information is not disclosed to unauthorized individuals, entities & process. That is whenever a sender sends a data / information to reciever, so in case of confidentiality it means that message is only accessable to reciever. Any third person cannot access that information.

Integrity :- maintaining accuracy and completeness of data. This means data cannot be edited in any an unauthorized way.
Integrity is mainly trustfulness of data. It means some data is recieved by the reciever that has been sent by the sender without modification. Data should not be changed or modified at bit or byte level. Any changes can be made by reciever but any unauthorized person cannot make changes in data.

Availability :- Means information must be available when need.
Availability of resources must be 24x7 to the authorized user. It ensures the data to be recieved at the time of need or not.

Page No.

Saathi

Date __/__/____

The main problem of availability is DOS (Denial of Service) attack problem.

Data types :-

- Public (Data is shown to all end users)
- Private / Internal (A group of company people only know about the data)
- Secret (A data is shown to very high authority user. Loss of this data may cause critical damage to company)
- Confidential (Data is accessed by limited no. of private & authorized user.)

Elements of IS :-

- Physical Elements
- System Elements
- Process Elements.

Physical Elements :-

(i) Guard :- Manual checking as a security measure.
(ii) Camera :- CCTV, (theft in Society)
(iii) Zone :- Restricted zone, An area of important & confidential information storage. Only authorized person can enter that area (High level person)
(iv) Downloading :- Downloading stuff of mp3 & mp4 at the time of work is prohibited.
(v) Access rights :- A person working in an institution leaves, so all the rights given to person must be cancelled after his left.

System Elements :-

(i) Antiviruses :- Protect systems from any kind of viruses.
(ii) Malicious software detection Col^{n}. :- Sometimes when we

Page No.

Saathi

Date __/__/____

install a new software in user system, some of the malicious content is also downloaded along with the software. And if it is downloaded, then it should be detected. And after detection we need to find out soln.

And soln. is to remove the data from the system which is effected by the software.

(iii) USB ports :- Disable USB ports, we can disable CD drives.

Process Elements :-

(i) Access control :- An unauthorized user cannot access that data.

(ii) Software details :- Details about software used & duration of time of person using s/w.

(iii) Log Entry :- When a user starts working on a process, a particular log entry about the user is created & only authorized person can access that log entry.

Security Types :-

→ Physical Security → communication security
→ Personal security → Network security
→ Operators security → information security

Date ___ / ___ / _____

Saathi

Ans:- The OSI Security Architecture :-

IOSA - To access effectively the security needs of an organization and to evaluate and choose various security products and policies, the manager responsible for computer and network security needs some systematic way of defining the requirements for security and characterizing the approaches to satisfying those requirements.

ITU-T :- It stands for International telecommunication union- telecommunication standardization sector. recommends X.800 security architecture for OSI that defines a systematic way of defining and providing security requirements. Furthermore, because this architecture was developed as an international standard, computer and communications vender have developed security features for their products and services :-

X.800 consists of
- Attacks.
- Services
- Mechanisms.

(i) Security Attacks :- Any action that compromises the security of information owned by an organization.

(ii) Security Services :- A processing and communication service that enhances the security of data processing system & information transfers of an organization.

(iii) Security Mechanisms :- A process that defines the to detect, prevent & recover from a security attack.

Page No.

Saathi

Date ___/___/_____

Types of Network security Attacks

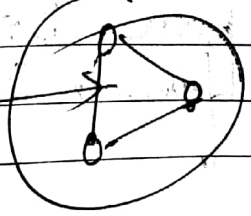
Active attack

Passive attack

Passive attack	Active attack
→ A passive attack attempts to ~~alter~~ system resources or ~~effect~~ their → Attention on prevention	→ Attention is on detection
→ A passive attack attempts to make learn from use of information from the system but does not effect system resources	→ An active attack attempts to alter system resources or effect their operations
→ No modification of packets	→ Packet modification is ~~there~~ present
→ Information collected is about path, source node & destination node	→ Sometimes intruder can give an attractive route to destination node so that it can read those packets.
Keys → System resources cannot be changed	System resources can be changed
Kinds of Active attacks	External attack Internal attack

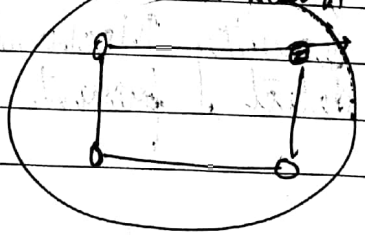
External

→ Attacker does not belong to same domain



Internal

→ Attacker belong to same domain

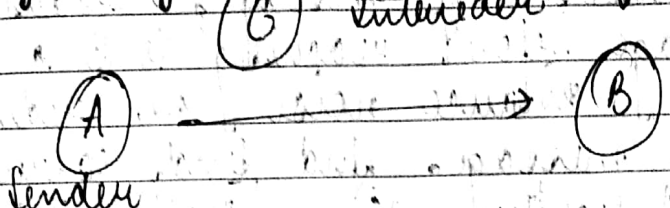


Page No.

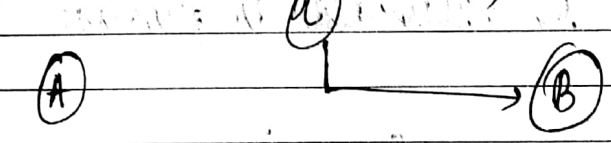
Date ___/___/___

Classification of Active attacks :- Masquerade, Modification of Messages, Repudiation, DOS, Replay

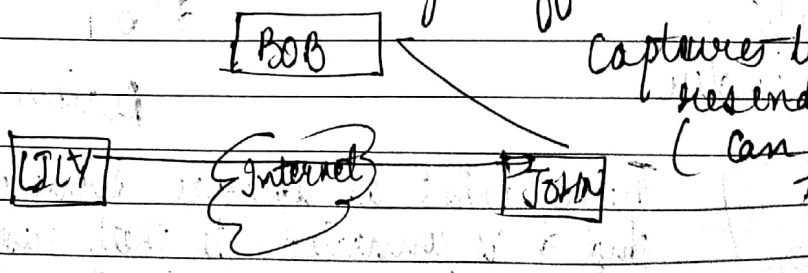
↳ Masquerade :- Masquerade attack takes place when one security entity pretends to be different entity.



Eg : A sends a data to B. It means A has login in his account and By using that account it is sending information to B which means it has username & password as well. A is authentic user but third person / attacker / intruder C hacks the login information of A and C is sending information to B and according to B message is sent by A (authorized user).

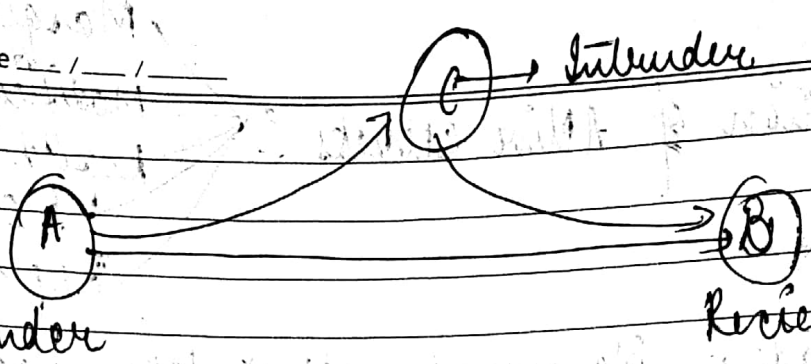


→ Delay :- It is also known as modification of messages. It involves the passive capture of a message and it subsequent the transmission to produce an unauthorized effect.



Page No. ___

Date __/__/____



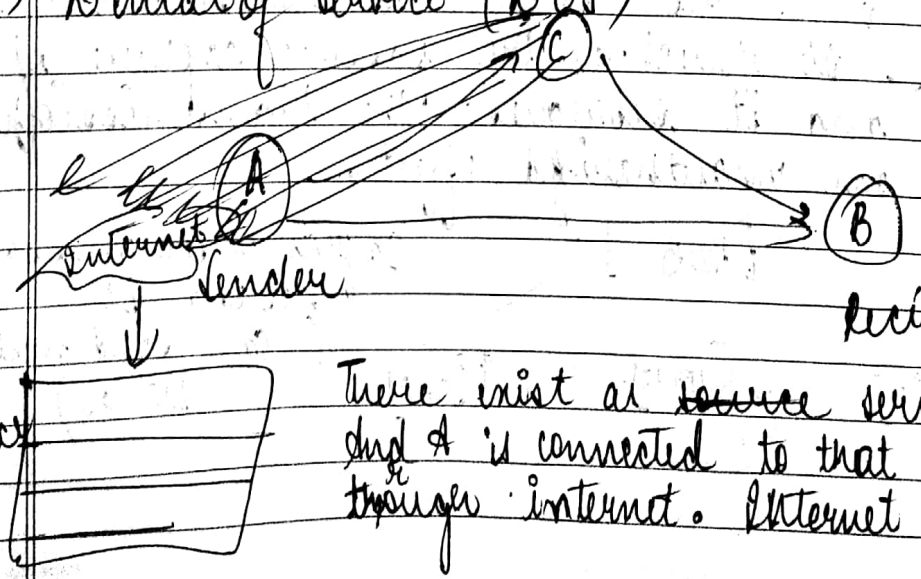
A is sending any message to B. But in the way of transmission of message, C reads and modifies message before reaching to B. C can modify, alter, reduce noise or reduce bits of error from message. And sends corrupted data to B.

[Integrity ✗ Confidentiality ✗] [Availability ✗]

→ Repudiation :- This attack is done by either sender or reciever. The sender or reciever can deny later that he/she has send or reciever message

→ Modification of Messages :- It means that some portion of message is altered or that message is delayed or recorded to produce an authorized effect.

→ Denial of Service (DOS)



There exist a source server/ Resource. And A is connected to that resource through internet. Internet also has

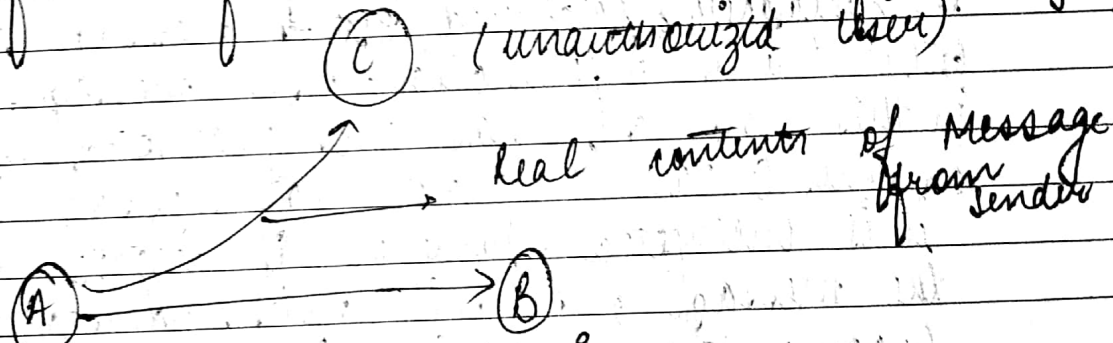
Saathi

Date ___/___/_____

its own capacity & if number of requests or messages increases that capacity limit, then there will be a case of congestion.
C (unauthorized user) sends the continuous messages on the server B and thus because of these unwanted and irrelevant packets getting loaded up and bursted up into the network, the internet will get slow down. And thus resources are not available to A

DDOS :- Distributive Denial of Service attacks
[Multiple hackers at present]
It prevents normal use of communication facilities. This attack may have a specific target.

Classification of passive attacks :- Release of message content, Traffic analysis



A sends message to B, C reads that message, it only reads and does not modify the message without acknowledgement of both A and B.

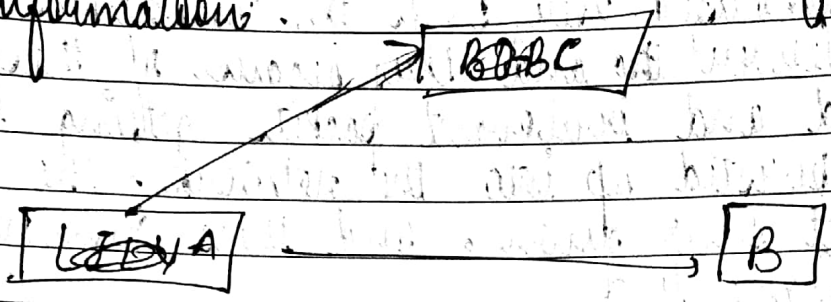
Page No.

Saathi

Date ___/___/_____

→ Release the contents of Message :- Telephonic conversation, an electronic mail message or a transferred file may contain sensitive or confidential information.

b



In this case C only observes the information shared between A and B .. ie. sender & reciever. The unauthorized person reads the information and thus confidentiality does not exists.

→ Traffic analysis :- Suppose that we had a way of masking (encryption) of information, so that the attacker captured message could not extract any information from message. In this case A sends an encrypted message to B. Thus C cannot read that message because it is encrypted. However if attacker observes the message, it will not understands anything because the encryption keys of that message are only with A and B. So when that encrypted message will reach from A to B, then B decrypts that message & reads it. In traffic analysis attacker can get the information about what is the origin of the message, what is the destination of message, time duration, size of packets delivered, ends of communication

Page No.

Date __/__/____

Saathi

Ans:- Types of Security Services :-

- X800 . RFC 2828.

X-800

X-800 defines it in 5 categories :-

(i) Authentication :- Assurance that the communicating entity is the one claimed

(ii) Access control :- Prevention of unauthorized use of resource.

(iii) Data Confidentiality :- Protection of data from unauthorized user.

(iv) Data Integrity :- Assurance that data received is as sent by authorized entity.

(v) Non-Repudiation :- Protection against denial by one of the parties in a communication.

Authentication :-

→ Assurance that the communicating entity is one claimed

→ It helps to establish trust by identifying the particular user / system.

Authentication Services

Peer entity authentication

Data Origin authentication

Page No.

Saathi

Date __/__/____

Peer entity authentication :-

→ Provide confidence in the identity of the entities connected

→ Attempts to provide confidence that an entity is not performing either a masquerade or an unauthorized replay of a previous connection.

Data Origin authentication :-

→ Provides confirmation of the source of a data.

→ Does not provide protection against the duplication or modification of data units.

→ This type of service supports applications where there are no prior interactions between the communicating entities.

Access control :-

→ Ability to limit and control the access to host systems and applications via communications links.

Admin → Read, Write, Execute

User → Read only

To achieve this :- Each entity trying to gain access must first be authenticated

Data confidentiality :-

→ Protection of data from unauthorized disclosure

Services — Connection confidentiality
— Traffic flow confidentiality
— Selective-field confidentiality
— Connectionless confidentiality

Page No.

Date __/__/____

Saathi

(i) Connection :- The security is provided to the connection and information shared in the connection is confidential and only authorized person can access it.

(ii) Connectionless confidentiality :- The protection of all user data in a single data block. Not on whole data but on single data only.

(iii) Selective field Confidentiality :- Only some of the selected field in a block are confidential rest all are not confidential. The confidentiality of selected field within the user data in a connection or in a single data block.

(iv) Traffic flow :- The protection of the information that might be derived from observation of traffic flows.

Data Integrity :-
The assurance that data received are exactly as sent by an authorized entity.
→ Contains no modification, insertion, deletion, or replay.

Integrity Services → Connection Integrity with recovery
→ Connection Integrity without recovery
→ Selective field connection Integrity
→ connectionless Integrity

(i) Connection integrity with recovery :- Provides 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.

Page No.

Saathi

Date __/__/____

(ii) Connection Integrity without recovery :-
→ Provides integrity of all user data on a connection, but provides only detection without recovery).

(iii) Selective Field connection Integrity :-
→ Provides for the integrity of selected fields.
→ Within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

(iv) Connectionless Integrity :-
→ Provides for the integrity of a single connectionless data block.
Only a single data block can apply integrity on it.
→ Replay detection may be provided.

(v) Selective - Field connectionless Integrity :-
→ Provides for the integrity of selected fields within a single connectionless data block.

Non - Repudiation :- Protection against denial by one of the parties in a communication.
→ If a user has sent any message or data to anywhere but that user refused to accept that the data is sent by him. So to assure that he won't refuse if he has sent data, this is called Non - Repudiation
→ Provides protection against denial ~~of by~~ one of the entities involved in a communication of having participated in all or part of the communication

Page No.

Date __/__/____ Saathi

Solution :-
Proof that message was sent by specified person.

Non Repudiation Services

Non Repudiation Origin (Sender)

Non Repudiation Destination (Reciever)

Origin :- In this origin we make sure that proof that the message was sent by the specified party.

Destination :- Proof that the message was recieved by specified party.

Availability :-
→ Property of a system or a system resource being accessible by an authorized system entity.
→ A variety of attacks can result in the loss of or reduction in availability.

Security Mechanisms (X.800) :-

Specific Security Mechanisms

Pervasive Security Mechanism.

Page No.

Date / /

Saathi

Ans:- Specific Security Mechanism:-

→ Encipherment:- Hiding data. Original data before sending is hided such that if that data is hacked by the unauthorized person the person will not able to understand that data because real data is not shown to the person using algorithms.
So that confidentiality is maintained

→ Digital Signature:- Used for guaranteed authentication and integrity as well.
Suppose there be two users A and B.

A (Sender) ——→ B (Reciever)

A want to send data is B. So when A sends data to B it applies a private key on that data. A key is a unique number and that only A knows. In that case reciever after recieving the message applies a public key on that message to decrypt the message authenticity and integrity is maintained in digital signature.

→ Access Control:- Suppose there be two levels in an organization one is employee level and other is administrative level. So there will be difference between the services which are accessible to an admin. Employee can only access that data which is not highly confidential.

→ Data Integrity:- Same as previous.

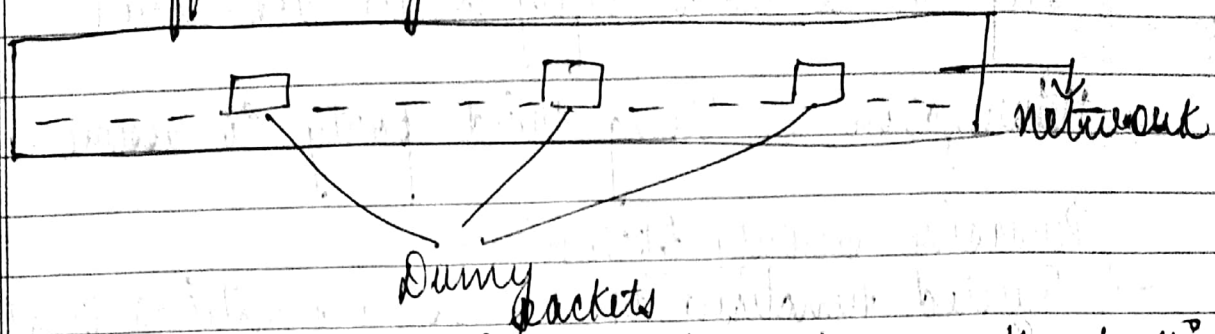
→ Authentication Exchange:- We exchange messages so

Page No.

Saathi

that in order to authenticate users. So that normal communications and transmission can take place.

→ Traffic padding :- A technique to get prevented from Traffic Analysis. ⊖ → Intruder



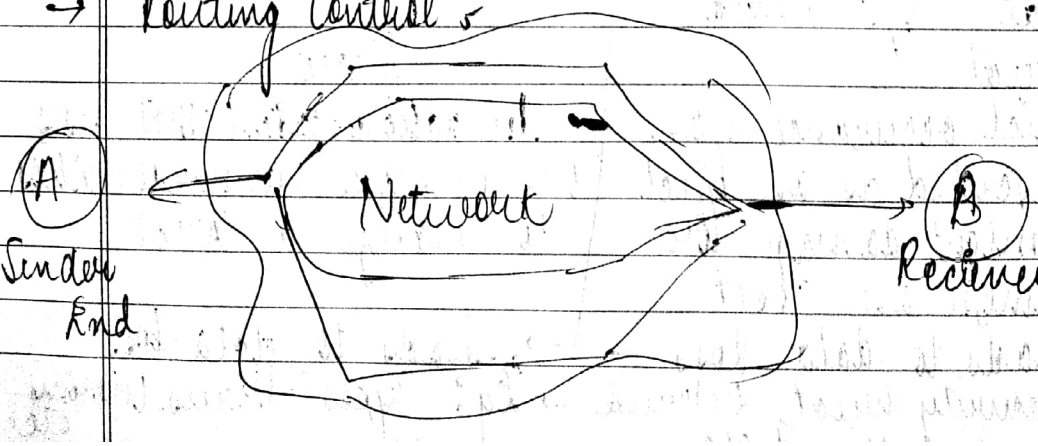
In traffic analysis in intruder observes the traffic pattern.

→ Traffic padding : means dumping the packets in between the message without any reason.

→ So dump a packet in between the message.

→ The actual packets will have a pattern of travelling but the dummy packets will break that pattern. So when we induce those dummy packets along with the actual packets, the intruder will get confused will not be able to trace the root, origin and destination of the message. If network will be congested he will not be able to identify the route of packet as well.

→ Routing Control :-



Saathi

Date ___ / ___ / ____

There are several paths for message to travel from A to B. firstly we prefer path 1 suddenly we switch to another path and so on. which means the path is changing continuously so that the intruder cannot track the route. So it will help us to reach safely to its destination.

→ Notarization :- Using third party to assure security.

Pervasive Security Mechanisms :-

→ Trusted functionality :- Using functions trusted by security policy.

→ Security labels :- Marking of data by its security attributes.

→ Event Detection :- Detection of security related events like violations.

→ Security audit trail :- Recording security audit is possible.

→ Security Recovery :- Recovery in response to event handling and management functions.

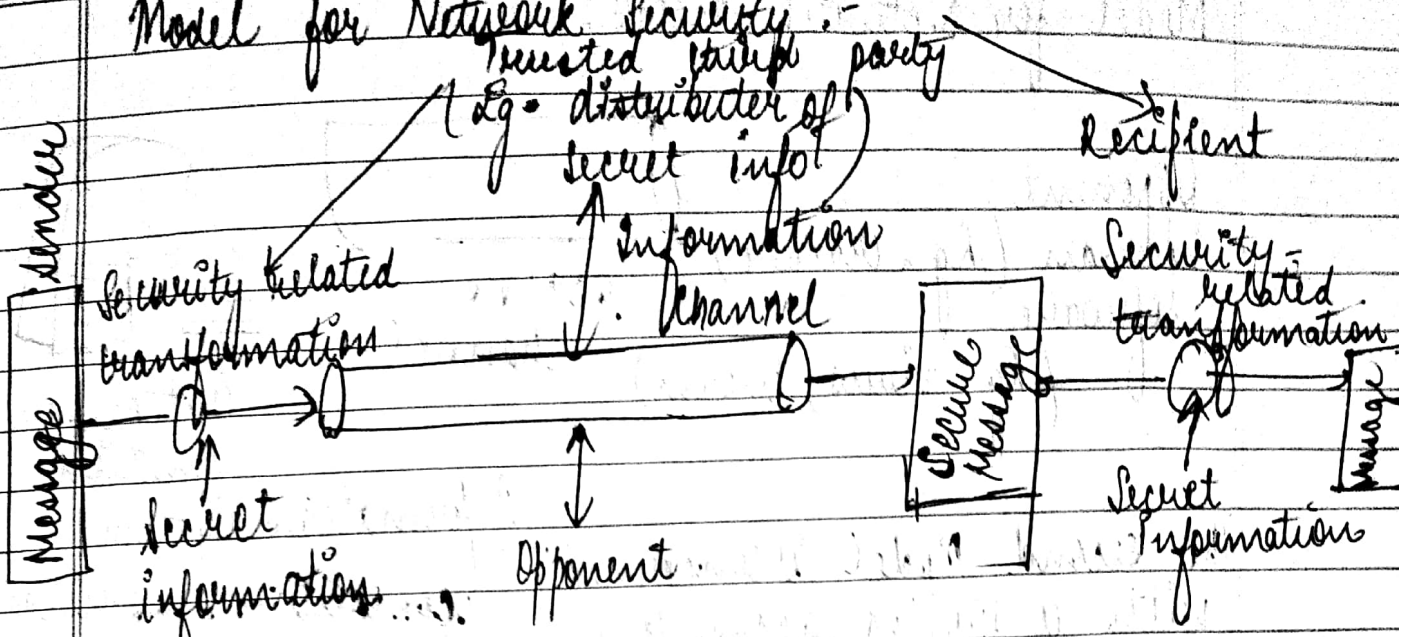
B. Threat V/s Attack

Threat	Attack
→ A potential occurance often best described as an effect that might damage or compromise an asset	→ An action taken that uses one or more vulnerabilities to realize a threat.
→ It leads to data loss	→ Leads to data loss
→ Eg :- Security threat, External threat etc.	→ Eg :- Types :- Viruses, Worms etc.

Saathi

Date __/__/____

Model for Network Security :-



→ Using this model requires to :

(i) Design a suitable algorithm for the security transformation

(ii) Generate the secret information (keys) used by the algorithm.

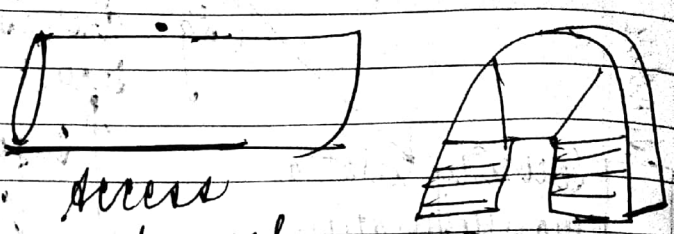
(iii) Develop methods to distribute and share the secret information.

(iv) Specify a protocol enabling the principals to use the transformation and secret information for a security service

Date ___/___/_____

Saathi

Model for Network Access:



The second Model is concerned with controlled access to information or resources on a computer system, in the presence of possible opponents. Hence appropriate controls are needed on the access and within the system, to provide suitable security. Some cryptographic techniques are useful here also.

Using this model requires us to:

(i) Select appropriate gatekeeper functions to identify users.

(ii) Implement security controls to ensure only authorized users access designated information or resources.

(iii) Trusted computer systems can be used to implement this model.

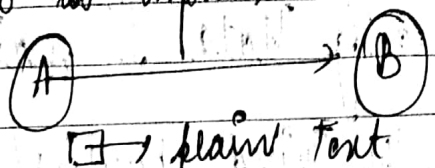
Date __/__/____

Saathi

Chapter - 2

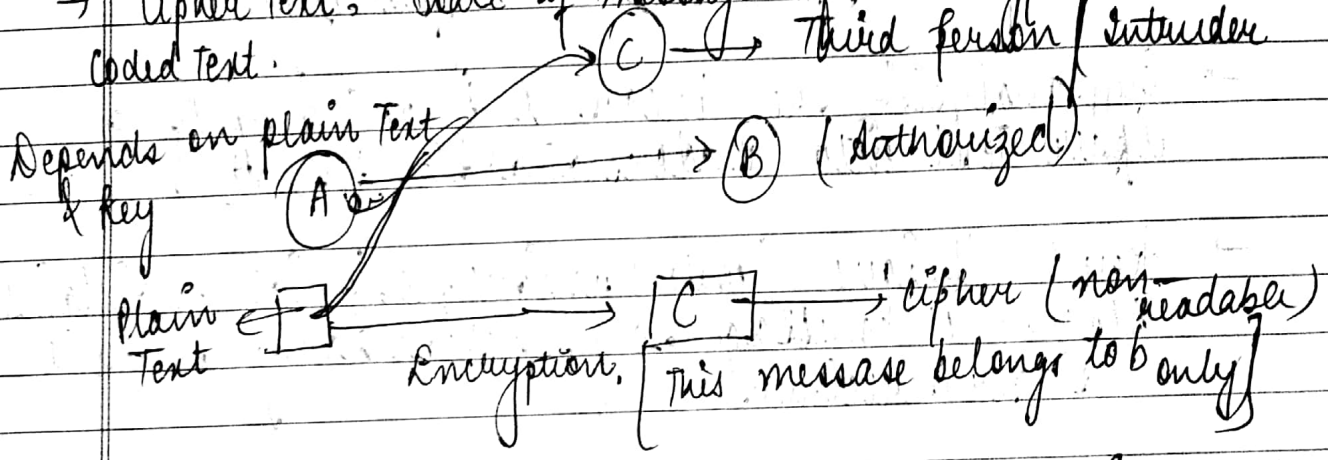
Basics of Network Security

→ Plain text :- Original message / Data / Text that is fed into algo as input.



Text in understandable & Readable format.

→ Cipher Text :- State of message after encryption. Coded Text.



→ Cipher :- Algo transforming plain Text into Cipher text

→ Encryption algo :- Performs various substitutions and transformation on plain Text. It converts plain Text into cipher Text.

→ Secret key :- An input to the encryption algo. It is value independent of plain text and algo. The algo will produce different output depending on key.

→ Decryption algo :- Encryption algo reverse. Depends upon cipher text & secret key to produce plain text.

Page No.

Saathi

Date ___ / ___ / _____

→ Encipher (Encrypt) :- Converting PT into CT.

→ Decipher (Decrypt) :- Converting CT into PT.

→ Cryptography :- Study of Encryption principles / method which helps in hiding data & maintaining secrecy.

→ Cryptanalysts :- The third parties / intruders sometimes try to convert cipher text into plain text by applying various algorithms on it. That person is called cryptanalysts.

→ Cryptanalysis :- The process of breaking up PT or cipher text into understandable format.

→ Key :- Unique (code) unique no. which maintains secrecy of message. Info which is only known to sender & reciever.

Classification of cryptographic Systems :-

(i) Operations used for transforming plain Text to cipher Text :-

- Substitution
- Transposition
- Product

(ii) The no. of keys used :-

- Hash functions (no key)
- Symmetric (1 key)
- Asymmetric (two keys)

Date __/__/____

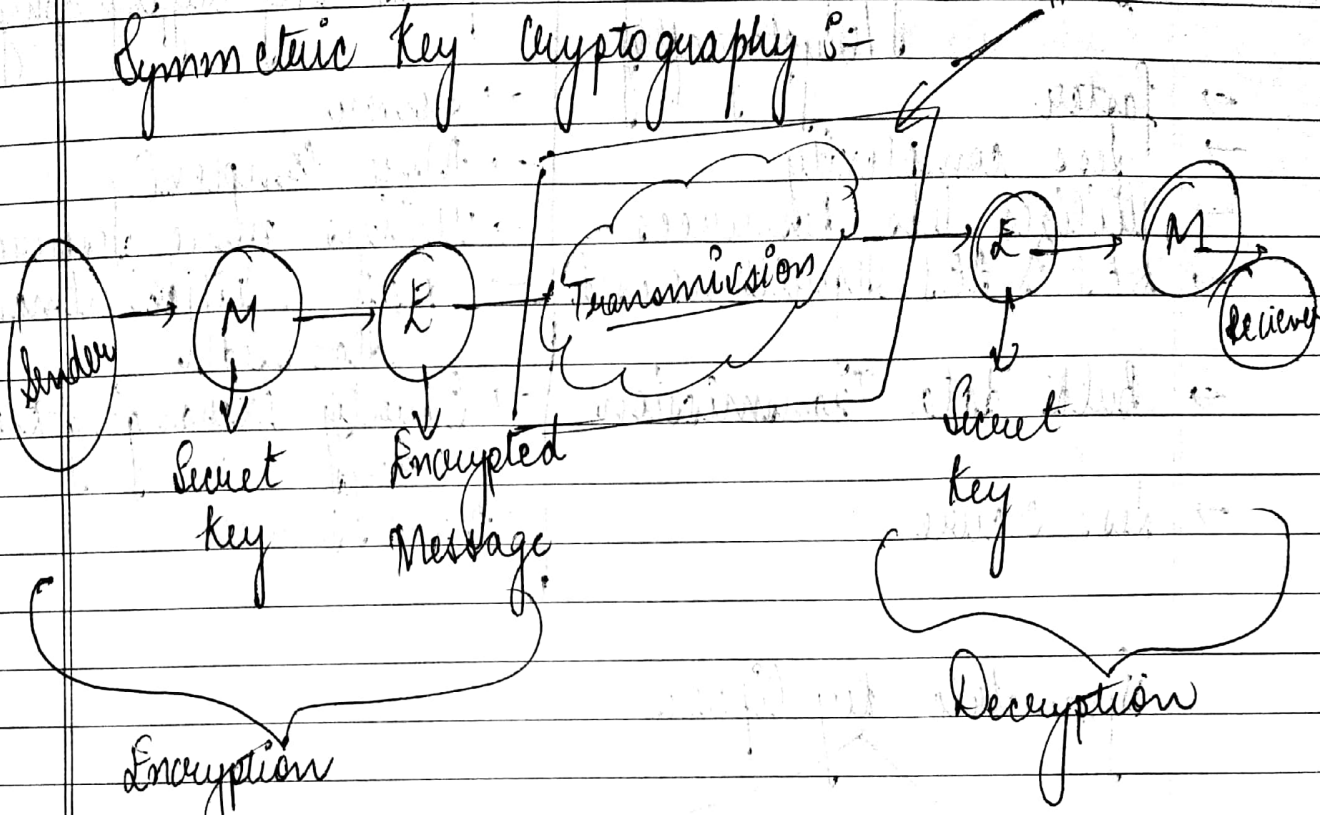
Saathi

(iii) The way in which plain text is processed.

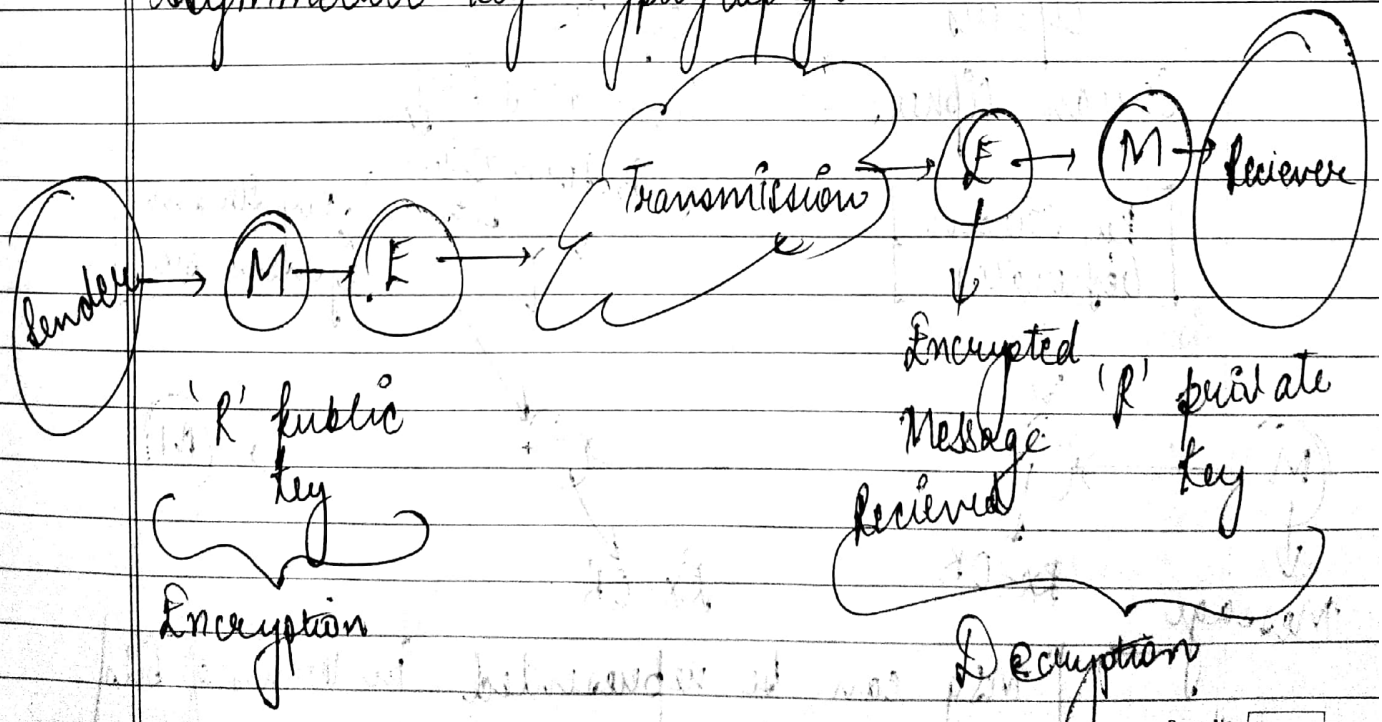
Block cipher

Stream cipher

Symmetric Key Cryptography :-



Asymmetric Key Cryptography :-



Page No.

Saathi

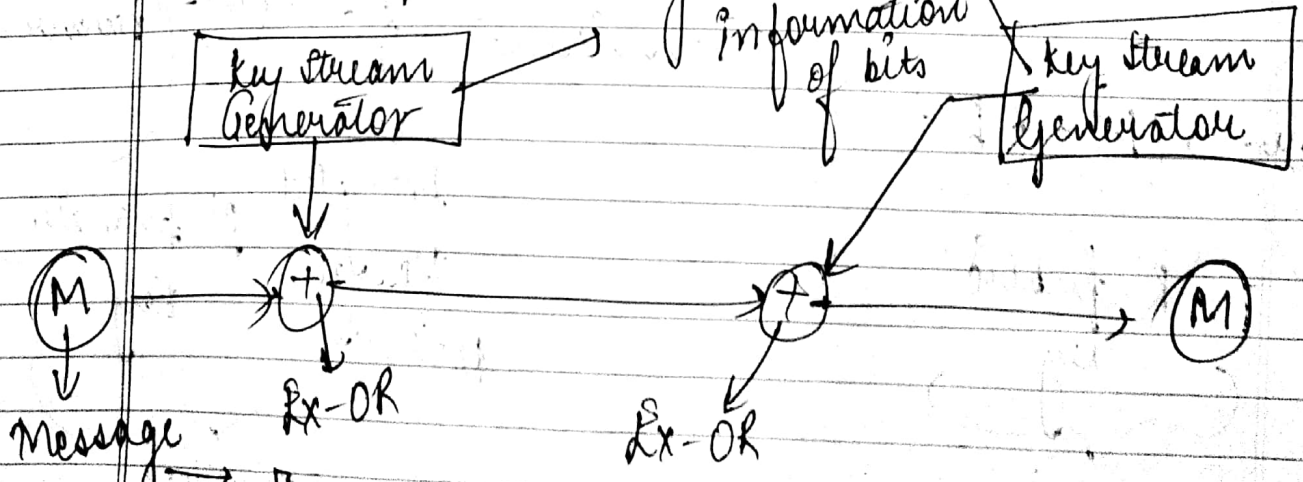
Date ___ / ___ / ___

Symmetric key Cryptography	Asymmetric key cryptography
→ Single key is used	→ 2 keys used
→ Secret key / private key cryptography	→ public key cryptography
→ faster	→ Slower
→ less complexity	→ More complexity
→ Utilizes less resources	→ Utilizes more resources
→ DES & AES algorithms used	→ RSA & Diffiehellman Algo used
→ Bulk data Transmission	→ Securely exchanging the keys.
→ less secure	→ More secure

Symmetric key Ciphers

Stream Ciphers | Block Ciphers

Stream Ciphers :-



[Msg can be represented in terms of bits]

Page No.

Ex-OR

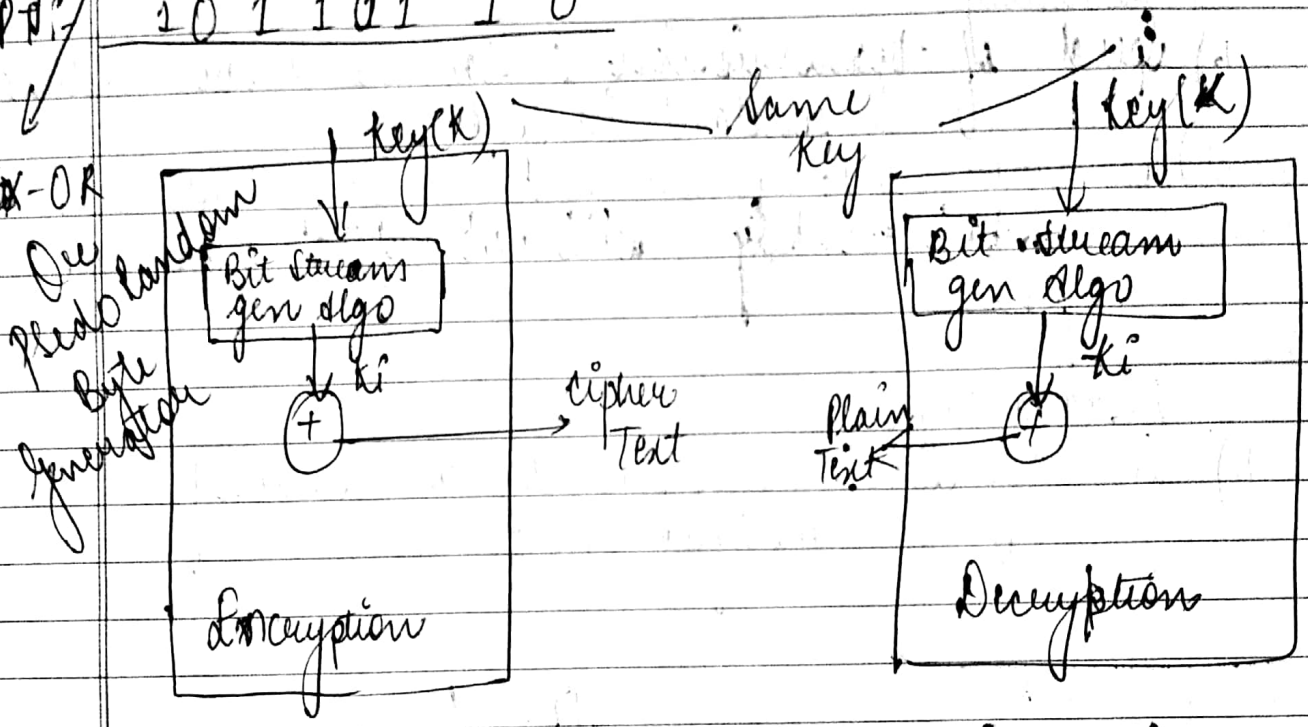
Saathi

Date __/__/____

PT: 1 0 1 1 0 1 1 0 → Sender side [8 bit]
key ⊕ 0 1 0 1 0 1 0 1 → key
CT 1 1 1 0 0 0 1 1 → (Encrypted Message)

Same Value - 0
Opposite value - 1

CT:- 1 1 1 0 0 0 1 1
key ⊕ 0 1 0 1 0 1 0 1
PT: 1 0 1 1 0 1 1 0



→ Generation of 1 time pad
→ Stream cipher is initialized with short key
→ Key is stretched into long key stream
→ Make a pseudo random property
→ Key stream is used like 1 time pad
→ Ex-OR operation is performed before encryption/Decryption

Definition :- A symmetric key cipher where plain text digits are combined with a pseudo random cipher digit stream.

Page No.

Saathi

Date ___ / ___ / _____

Let E be an encipherment algorithm. Let $E_k(b)$ be the encryption of message (b) with key k. Let the message $m = b_1, b_2 \ldots$ where each b_i is of fixed length and $k = k_1, k_2 \ldots$.

A stream cipher is a cipher for which

$$E_k(m) = E_k(b_1)\, E_{k_2}(b_2)$$

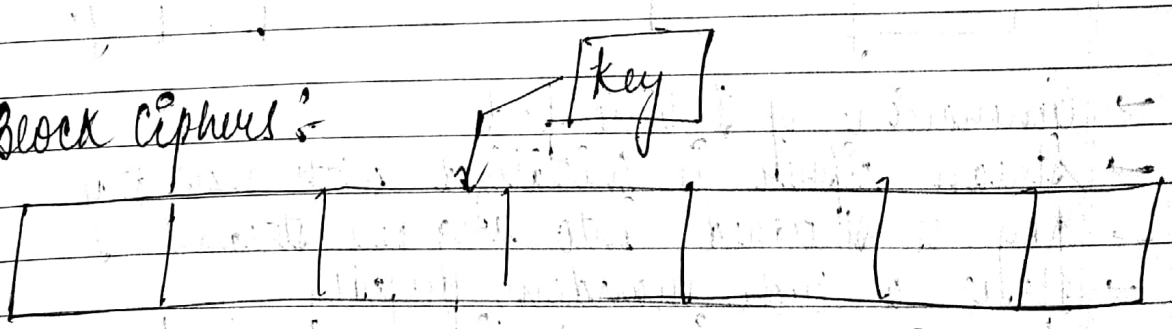
Advantages :-

1) Speed of transmission :- Algo are linear in time & constant in space.
2) Low error propagation :- Error in encryption of symbol likely will not effect subsequent symbol.

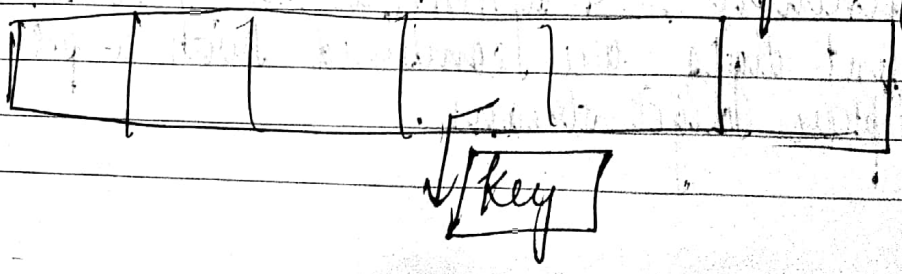
Disadvantages :-

1) Low diffusion :- Susceptability to insertion / Modifications

Block ciphers :-



→ Plain Text divided into blocks
→ Key is applied on each block of plain Text.
→ Generated Text will cipher text in form of blocks



Page No.

Saathi

Date ___/___/___

(40, 56, 64, 128, 256 bits)
↳ usual size of key.

Eg:- Data Encryption standard (DES)
↳ Block size = 64 bits (fixed)
↳ CT = 64 bits
↳ Key size = 56 bits

Substitution Ciphers Techniques :-
Converting PT to CT.

Advantages :- (i) Highly diffusion :- Information from one plain text symbol is diffused into several cipher text symbols.
(ii) Immunity to tempering :- Difficult to insert symbols without detection

(iii)

Disadvantages :-
(i) Slowness of Encryption
(ii) Error propagation :- Error in 1 symbol may corrupt entire block

Let E be an encipherement algo. & let $E_k(b)$ be the encipherement of the message b with key k
Let a msg $m = b_1, b_2 \ldots$ where b_i is of all fixed length (block cipher is a cipher for which

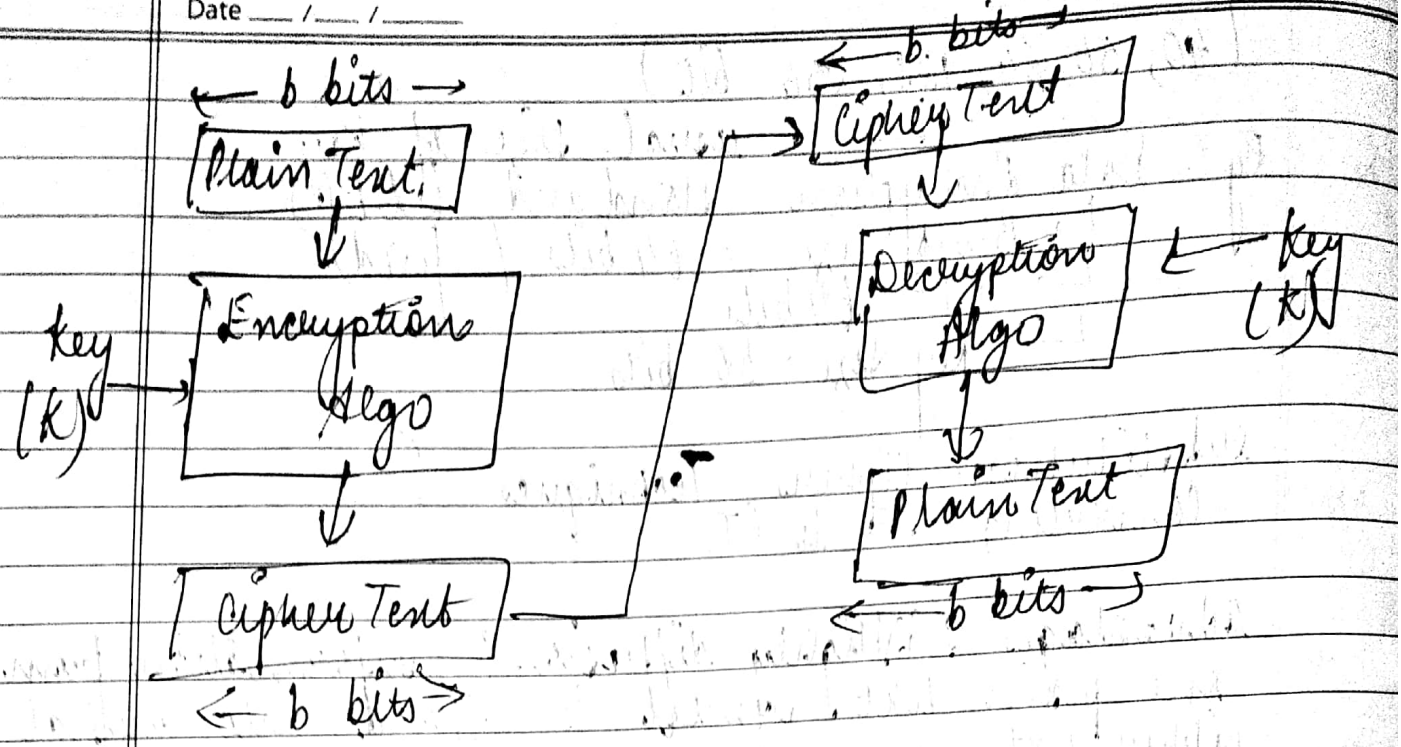
$$E_k(m) = E_k(b_1)\, E_k(b_2) \ldots$$

$E_k(b_1)$ → key stream
$E_k(b_2)$ → key stream
→ Block

Page No.

Saathi

Date ___ / ___ / ____



Stream Ciphers V/s Block Ciphers

Stream Ciphers	Block Ciphers
→ Stream ciphers combines i/p text bits with a pseudo-random cipher bits stream using XOR	→ Block ciphers encrypt fixed length block of bits
→ Stream ciphers use varying transformation based on the state of engine	→ Use the same transformation
→ Executed faster	→ Execute slowly
→ less complex	→ More complex
→ Used when PT is available is varying quantities. ∴ Block ciphers cannot operate directly on blocks ~~without~~ shorter than block size	→ Using certain modes of op'n, a block cipher can be used to act as a stream cipher by allowing it to encrypt the smallest unit of data available

Page No.

Saathi

Date

Substitution ciphers

- Monoalphabetic
  - Caesar cipher
- Polyalphabetic
  - Playfair cipher
  - Vigenere cipher
  - Vernam cipher

Caesar cipher :- It is a monoalphabetic cipher in which for a given e, the cipher alphabet for each plain alphabet is fixed through out the encryption process.

Monoalphabetic ciphers :- It is a substitution

Eg :- If A is encrypted as D, for any number of occurance in that plain text it will gets encrypted to D all the time.

These ciphers are highly susceptible to encrypt analysis. The key set consist of 25 keys, as a result proof ↑ attacks are quite common.

In order to enhance the security of encryption, simple substitution cipher invented.

Caesar cipher :- Encryption → Plain Text

$$C = E(key, P) = (P + key) \bmod 26$$

$$P = D(key, C) = (C - 3) \bmod 26$$

Decryption ← Cipher Text

Page No.

Saathi

Date

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19
A B C D E F G H I J K L M N O P Q R S T
a b c 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
20 21 22 23 24 25
x y z a b c

Q:=

Sender Encryption: Plain Text : FIVE MINUTES ENGINEERING
Cipher Text : ilyh plqxwhv hqjlqhhulqj

Receiver Decryption: CipherText : ilyh plqxwhv hqjlqhhulqj
Plain Text : FIVE MINUTES ENGINEERING

It is a monoalphabetic cipher in which each letter of plain text is substituted with another letter to form a cipher text.

It is a simplest form of substitution cipher scheme.

This crypto system is generally refered to as shift cipher.

The concept is to replace each alphabet by another alphabet which is shifted by some fix number of position between 0-25.

For this type of schima both sender and receiver agree on a secret shift number of shift alphabets

Saathi

Date ___ / ___ / _____

1. Consider the above formula.
2. Now consider any alphabet suppose A and write the no. assigned to A i.e 0 equals to B. Now after applying formula mentioned above E(3, 0) = 3.
3. Now find alphabet assigned 3 is D. Write 'd' instead of D below 'A'.
4. If you get 'A' anywhere in the PT substitutes it with 'd'.
5. Similarly solve it for other nos. as well.
6. Hence the plain text will be encrypted
7. For decryption, apply the second formula.
8. ~~Now the alphabet assigned 3 is d.~~ Move backwards and then write the alphabet which comes on its turn.
9. Hence the message is decrypted.

Advantage :-

→ Simple to implement

Disadvantage :-

→ Not so difficult for intruder to decode

→ Not secured crypto system.

Saathi

Date ___ / ___ / _____

Polyalphabetic ciphers:

→ Playfair

→ Vigenere

↔ Vernam

Playfair cipher

Plain Text

Message (PT):- JAZZ , Message: OFF

Keyword:- MONARCHY

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

PT: JA ZZ

J ↓ ↓ ↓

↓ ZX ZX

SB UZ UZ

CT: SB UZ UZ

PT: OF F

↓ → FX

OF ↓ ↓

↓ HP IV

CT: HP IV

PT: GREET

↓ ↓

GR EX ET

↓ ↓ ↓

KN IU KL

CT: KN IU KL

Date __/__/____

Saathi

1. Construct a base structure of 5x5 matrix
2. In a playfair cipher initially a key table is created. A key table is 5x5 grid of alphabets that acts as key for encrypting the PT.
3. Each of 25 alphabets must be unique and one letter of the alphabet usually j is omitted from table as we need only 25 characters instead of 26. e
4. If PT contains j then it is replaced by i.

A sender and reciever will decide key

Let Key = monarchy

1. The PT is split into pair of 2 letters.
2. If there is an odd no. you will add z at the end.
3. Rules (i) If both letters are in same column, take the letter below each one going back to the top if at the bottom.

(ii) If both the letters are in same row, take letter to the right of each one going back to the left if at the farthest right

(iii) ~~Neighbor~~ Neither of preceeding two rules are true, form a rectangle with 2 letters & take the letters from the horizontal opposite corner of the rectangle.

→ In case (ii) consider the opposite corners of given corners

→ Now in the row of given alphabet consider the alphabet present in that same row.

Page No.

Date __/__/____

Saathi

Polyalphabetic Ciphers:-
It is the substitution cipher in which the cipher alphabet for plain alphabet is different at different places during encryption process.
One character is replaced by multiple characters.

Vigenere Ciphers.

Encryption: FORWARD
Decryption: BACKWARD

Key = POINT
MSG = ATTACK FROM SOUTH EAST.

P O I N T
16 15 9 14 20

a b c d e f g h i j k l m n o p q r
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18
s t u v w x y z
19 20 21 22 23 24 25 26

PT	a	t	t	a	c	k	f	r	o	m	s	o	u	t	h
key	16	15	9	14	20	16	15	9	14	20	16	15	9	14	20
CT	q	i	c	o	w	a	u	a	c	g	i	d	d	h	b

PT	E	A	S	T
key	16	15	9	14
CT	u	p	b	h

CT:- qicowaciacgiddhsupph

Saathi

Date __/__/____

Decryption :-

PT	g	i	c	o	w	a	u	a	c	g	i	d	d	h	b	u	p	b
key	16	15	9	14	20	16	15	09	14	20	16	15	9	14	20	16	15	9
CT	a	t	t	a	c	k	f	R	O	M	S	D	u	T	h	e	A	S

PT	h
key	14
CT	T

→ The sender and the reciever reside on a key say point. Numeric representation of this key is 16, 15, 9, 14, 20.

→ The sender wants to encrypt the message say "attack from southeast". He will arrange the plain text & numeric key as follows.

→ Now he shifts each plaintext alphabet by number written below it to create cipher text as shown

→ Here each plain character has been shifted by a different amount is that amount determined by key.

→ The Key <= message

→ For decryption, the reciever uses the same key & shifts recieved cipher text in reverse order to obtain the plain text.

Date ___/___/_____

Saathi

Vernam Ciphers (One time pad)

(1.) Plain Text H E L L O [key can be random]
7 4 11 11 14
Key b a x y c [length of key = length of PT]
1 0 23 24 2

A B C D E F G H I J K L M N O P Q R S T U
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
V W X Y Z
21 22 23 24 25

PT 7 4 11 11 14
Key no 1 0 23 24 2
Add 8 4 34 35 16

In case of value more than 26 sub 26 from no.

Subtract :- 8 4 34 35 16
- 26 26
CT :- 8 4 8 9 16
i e i j Q (Encrypted at Sender side)

Saathi

Date __/__/____

(2.) PT :- HELLO
Key :- XMCKL

PT :- H E L L O
8 5 12 12 15
Key :- X M C K L
24 13 3 11 12
Sum 32 18 15 23 27

After modulus
Subtract 6 16 13 21 2 → CT :- FROWA
(Encrypted at sender side)

FROWA — CT
6 18 15 23 1
X M C K L — Key
24 13 3 11 12
(subtract)
-18 5 12 12 -11
+26 +26
8 5 12 12 15
H E L L O

{Add 26 if no. is -ve}

This cipher is more secured as compared to other ciphers.

1. It was developed by Gilbert Vernam in 1917 in AT&T
2. Implimented by using one time pack (key)
3. Key is discarded after one use.
4. Length of input cipher text is equal to of original plain text.

Date __/__/____

Saathi

Algo

1. Write each plain text alphabet as number either (A=1, B=2 upto Z=26) or (A=0, B=1 upto Z=25)
2. Same process will continue for key (key)
3. Add PT alphabet no to the key no.
4. If sum >= 26, subtract 26 from it
5. Convert each no. of sum of alphabet.

Modulo :- Process of keeping a computed no. written a specified range.

Range :- 26 modulo

Transposition Ciphers → Rearrange the order of PT bits
→ No Replacement / Substitution

Railfence — Row transformation (columnar)

(i) Rail Fence

Plain Text :- FIVE MINUTES ENGINEERING

key :- 43512 (No ~~replacement~~ repeat no.) [next column size]

1	2	3	4	5
F	I	V	E	M
I	N	U	T	E
S	E	N	G	I
N	E	E	R	I
N	G			

column size = 5

Saathi

Date __/__/____

(top to down) CT:- ETGR VUNE MEII FISNN INEEG

[column wise]

6. PT:- WELCOME TO MY SESSION
key:- 3:451

(Zebra
26 5 2 1
according to position of alphabet)

3 2 4 5 1
W E L C O
M E T O M
V S E S S
I O N X V → Dummy characters

CT:- OMSY EESO WMYI LTEN COSX
[read row wise]

Rail fence cipher
PT:- TEXT BOOK PAGE THREE
key:- 3 [3 Rows]

T	-	-	-	B	-	-	-	P	-	-	-	T	-	-	-	E
-	E	-	T	-	O	-	K	-	A	-	E	-	H	-	E	-
-	-	X	-	-	-	O	-	-	-	G	-	-	-	R	-	-

CT:- TBPTEETOKAEHEXOGR

Jumbling of characters is done in rail fence cipher to get the cipher text. It is used for short length msgs. and easily crackable. Firstly we will decided the value of key. Suppose the value is 3 then we will make 3 rows & then count the no. of ~~house~~ alphabets present in the original

Page No.

Saathi

Date ___ / ___ / _____

message make that much amount of columns :-
Eg :- Welcome to ALET
for this case there will be 4 rows & 11 columns.

Key less ~~Transfold~~ Transposition :-

Plain Text :- FIVE MINUTES

Row 1 :- I E I U E

Row 2 :- f V M N T S

Cipher Text :- IEIUEfVMNTS

1. Write Plain Text in zig zac manner
2. Now write the cipher text from left to right row wise

Without key this a method is used.

Date ___/___/_____

Saathi

Chapter-3

Basics of Steganography:-

Steganography:- It is the technique of hiding of image in the other message. The hidden message will only be known to either reciever or sender.

Various Techniques used:-

(i) Character Marking:- Selected letter of printed or written text are overwritten in pencil. The marks are ordinarily not visible unless the paper is held at an angle to brightlight

(ii) Invisible Ink:- A no. of substances are used for writting but leave no trace until some heat or chemical is applied to the paper.

(iii) Pin Punchers:- Small pin punches on selected letters are ordinarily not visible unless the paper is held up in front of the light.

(iv) Type writter correction ribbon:- Used b/w lines typed with black ribbon. The results of typing with correction tape are visible under a strong light.

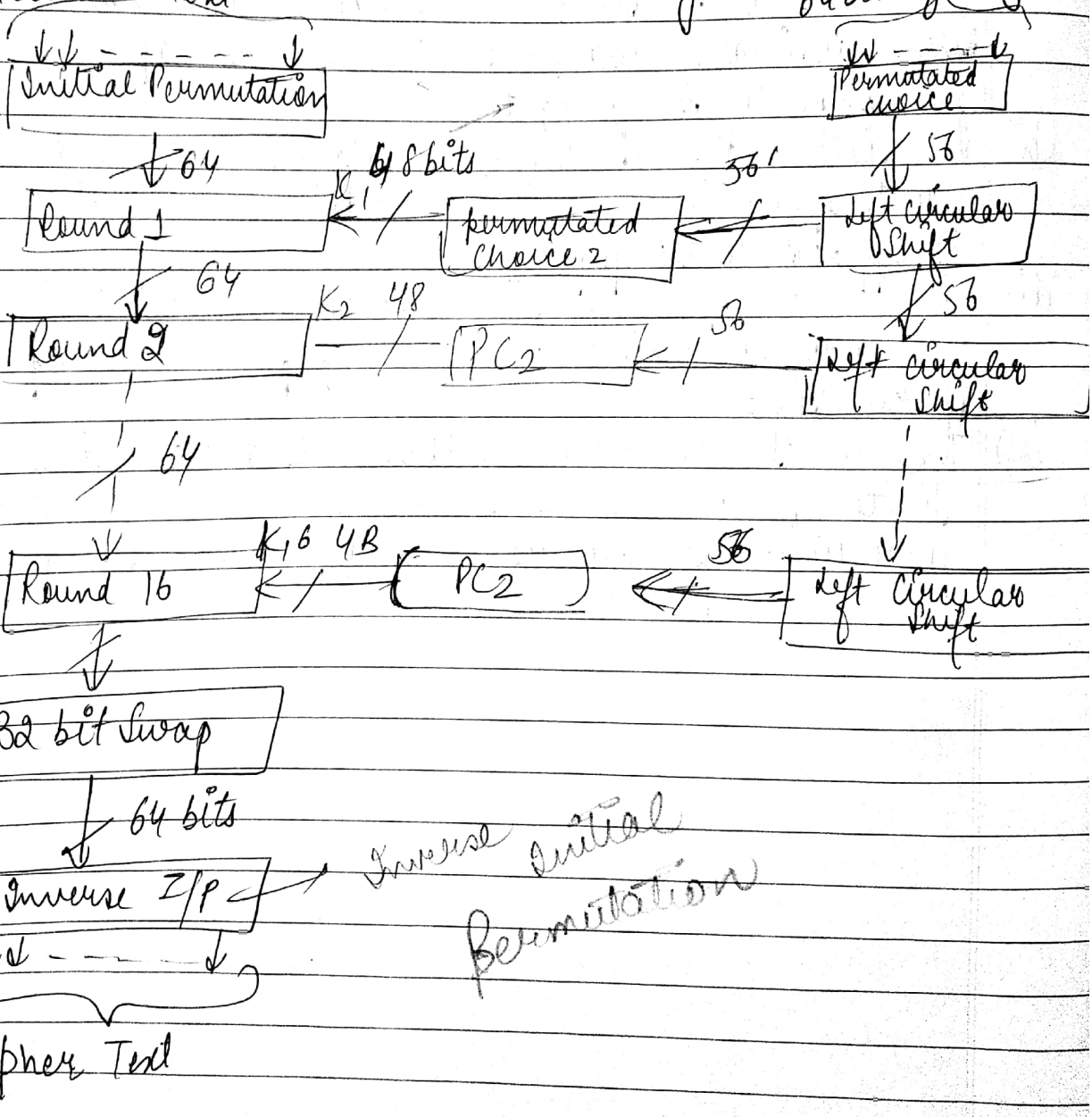
Date ___/___/_____

Saathi

Sub :- DES

DES stands for data Encryption Standard.

(i) Most widely used block cipher in world
(ii) Adopted ind 1977 by NBS
(iii) Encrypts 64-bit data using 56-bit key
(iv) Has widespread use
(v) Has been considerable controversy over its security



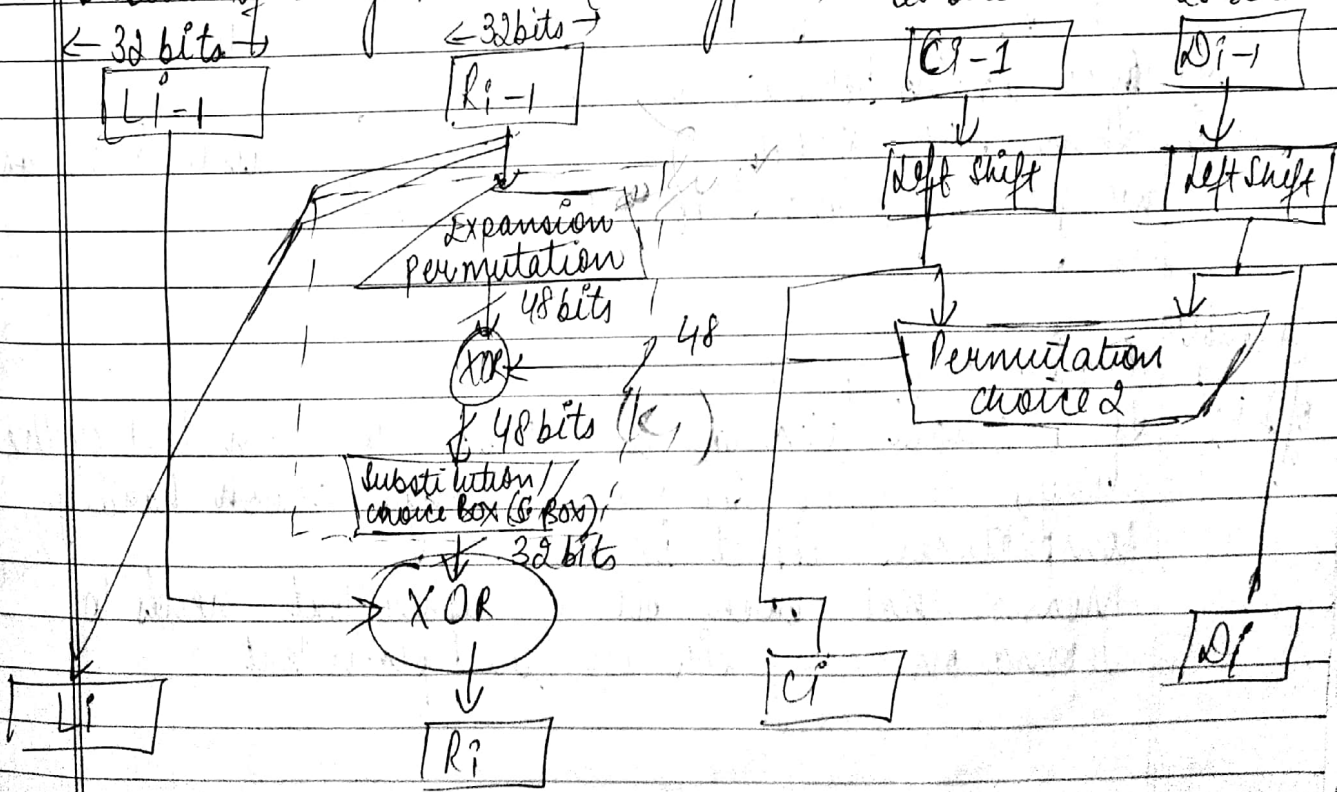
Date __/__/____

Different keys for every round (Ki)

Permutated choice means a table which has random values and after permutation a new value is generated ie: 64 bit key is converted to 56 bit key.

There are 16 Rounds from the encryption of Plain Text to cipher text.
The 8 bits (i.e. 64-56) are used for parity or error checks.
Left Circular shift shifts the key to the round.
Again a permutated choice will be applied on the key we get 48 bits of key which we will apply on the rounds.
After all the rounds are done a 32 bit swap will be done and finally inverse. Initial permutation will be applied & will generate the cipher text.

Inside of every Round (Encryption)



Page No.

Saathi

Date ___ / ___ / ___

(i) Plain text gets divided into 32-32 bits
(ii) In Round;-, ϕ expansion permutation is applied which converts 32 bits to 48 bits.
(iii) In key generation the 48 bit key is left circular shifted bounded the round;-, in which 48 bits plain text is XOR with the 48 bits key.
(iv) After doing XOR what is produced will be shifted towards substitution box i.e. S Box.

In S. BOX

48 bits

6 bits 6 bits 6 bits 6 bits 6 bits 6 bits 6 bits 6 bits

4 bits 4 bits 4 bits 4 bits 4 bits 4 bits 4 bits 4 bits

32 bits.

(v) After SBox we get the original 32 bits of plain text back.
(vi) Once again permutation done
(vii) Then the XOR of L_{i-1} & R_{i-1} is done & at cost we get the right hand side ie R_i.

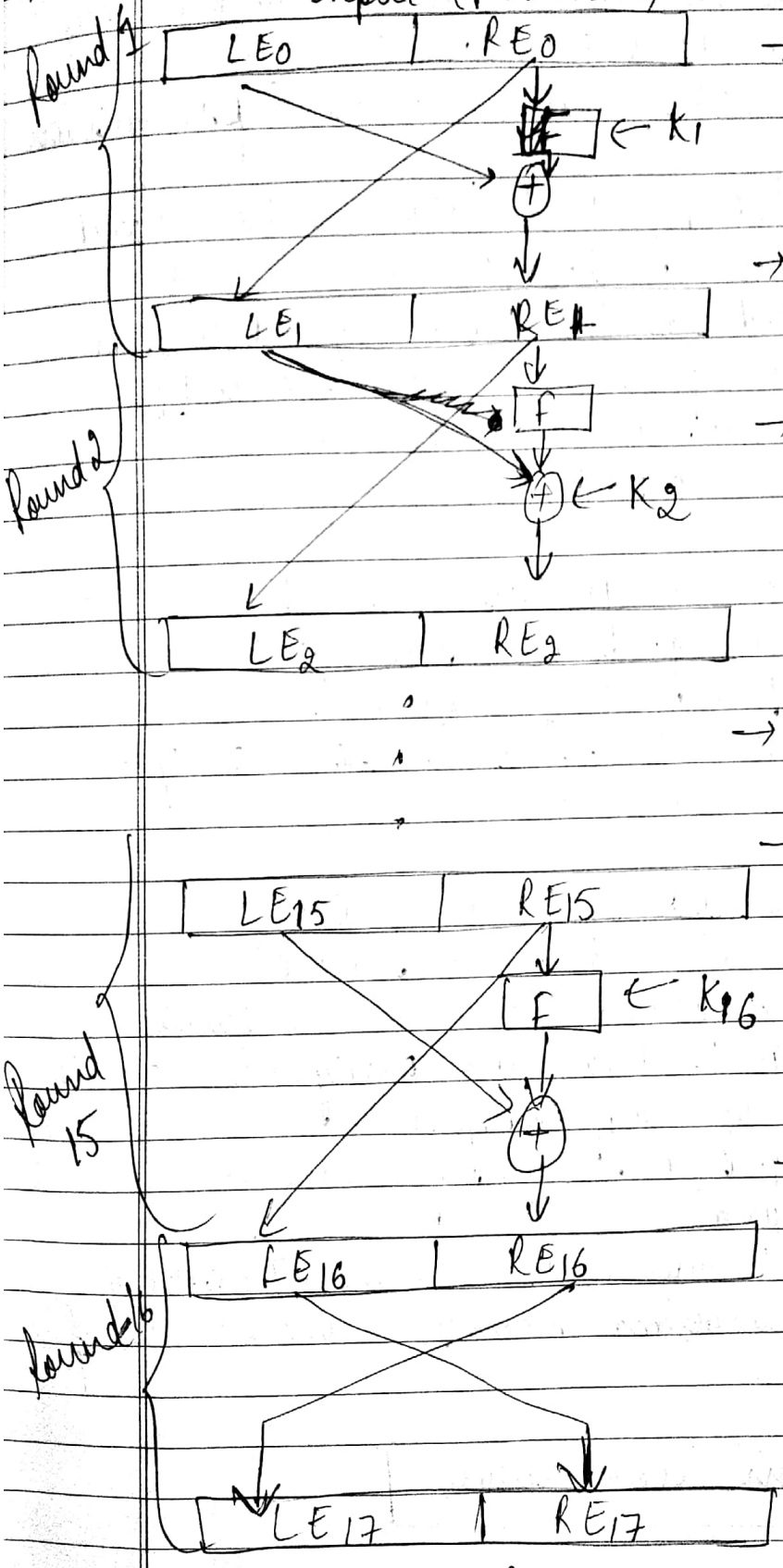
Strength of DES

Avalanche effect in DES:-
If a small change in either the plain text or the key, the cipher text should change ~~mouth~~ handley.
completeness effect in DES:-
Means that each bit of cipher text needs to depend on many bits on the plain text

Saathi

Date ___ / ___ / _____

Ans:- Feistel Cipher Structure :-



Explaination

→ plain text is divided into 2 parts

Left Right

→ Left part is denoted by L and Right part is denoted by R

→ The processing / encryption is carried out in rounds ie processing of conversion of plain text into cipher text is carried out in rounds

→ Actions of rounds are pre defined

→ Combination & permutation takes place in each round.

→ Left half will carry X-OR operation & nothing to be performed on right half

→ F is a round function / encryption fun^n which takes 2 input from R (Right half) & K (key)

→ For each round there are specific keys like K_1, K_2, etc

→ This key is derived from original function key

Page No.

Saathi

Date ___/___/_____

→ These keys are round keys / sub keys.
→ These keys are derived from original encryption key
→ The value of key will be put into function in place of key's value. The function will generate input function for each key.
→ The output generated by the function & the left part of PT will perform X-OR operation.
→ The output generated in the above round will be the new right part of the next round & (old) right part of previous round will be directly converted into new left part
→ Similarly it will generate in every round.
→ During the final step of generating the cipher text, the final actions are going to be reverse of the initial actions (opposite) ie. Both the parts left & right are now combined in the last step & it will be sent to reciever.

Block size :- Larger block sizes means greater security
key size :- Larger key size means greater security.
No. of rounds :- Multiple rounds offer increasing security
Subkey generation algo :- Greater complexity will lead to greater difficulty of cryptanalysis
Round function :- Greater complexity means greater resistence of cryptanalysis
Fast ~~flow~~ software encryption / Decryption :- The speed of execution of the algorithms becomes a concern case of analysis.

* DES algo is based on Feistel Ciphers

Date ___/___/_____

Saathi

Sub: Symmetric Block Ciphers

Triple DES :-

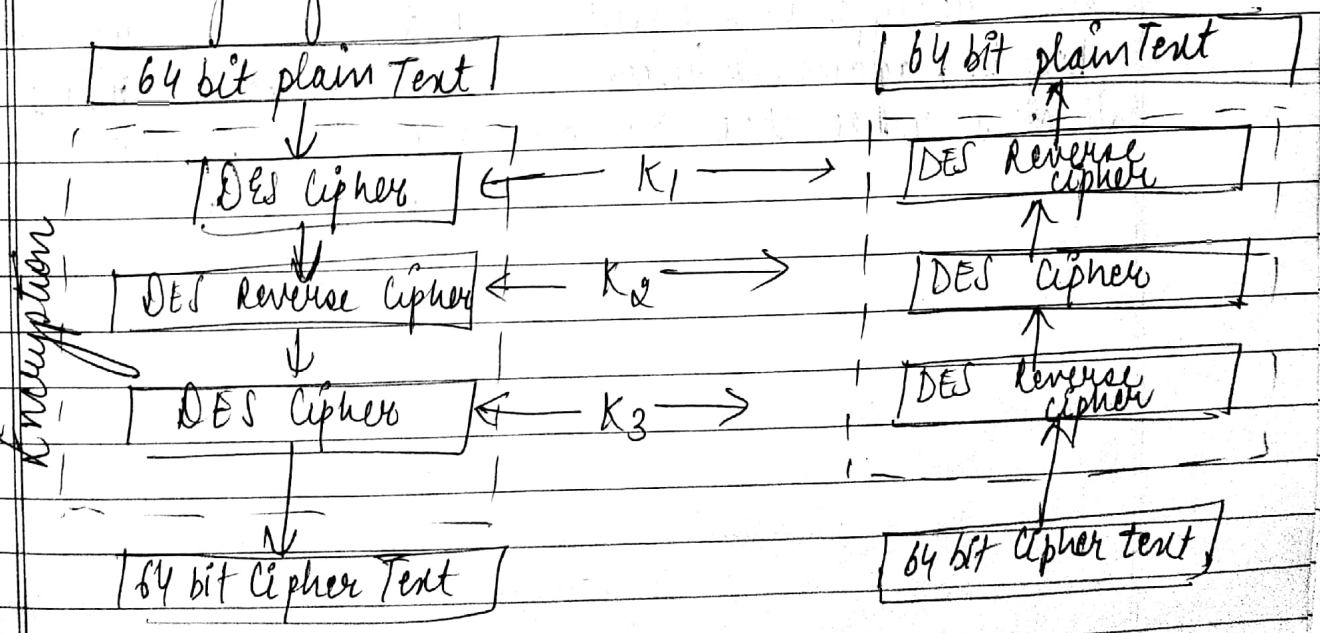
Short coming of DES is that it uses 56 bit key which means key space is relatively small. To overcome this, we run DES multiple times each using different key.

There are two variants of Triple DES :-

3 Key triple DES | 2 key triple DES.

(1) 3 key triple DES.

Before using 3TDES, user first generate and distribute a 3TDES key K_1 which consists of three different DES keys K_1, K_2, K_3. This means that the actual 3TDES key has length of $3 \times 56 = 168$ bits.



Page No.

Saathi

Date ___ / ___ / _____

The encryption - decryption process is as follows:-

(i) Encrypt the plain text blocks using single DES with key K_1

(ii) Now decrypt the output of step 1 using single DES with Key K_2.

(iii) Finally encrypt the o/p output of step using single DES with key K_3.

(iv) The output of step 3 is the cipher text.

(v) Decryption of a cipher text is a reverse process. User first decrypt using K_3, then encryption with K_2 & finally decrypt with K_1

(2) 2 key Triple DES

Second Variant of Triple DES ie 2TDES is identical to 3TDES except that K_3 is replaced by K_1 in another words, user encrypt plain text blocks with key K_1, then decrypt with key K_2 and finally encrypt with key K_1, again. Therefore 2TDES has key lengths of 112 bits. It does twice that DES normally does only once.

Date __/__/____

Saathi

Ans:- Blowfish :-

Blowfish is an encryption method that is very strong weapon against hackers and cyber-criminals. Used in a wide varray of products including

→ Some secure e-mail encryption tools.
→ Backup software
→ password management tools.

Blow fish is an encryption algorithm that can be used as a replacement for the DES or IDEA algorithms.

It is a symmetric block cipher that uses a variable-length key from 32 bits to 448 bits.

Blow fish uses a ~~[illegible]~~ unique form of key generation. The second part of the blowfish routine is a key expansion that converts a single key of up to 448 bits into a table of subkeys further increases security, because a hacker would have to crack more than just the original key.

Strength of Blow fish:-

→ Blow fish is an incredibly fast cipher that has a relatively simple structure & is very effective
→ Blowfish generates a really large key and this alone is a huge benefit to security.

Page No.

Saathi

Date __/__/____

Ans:- IDEA :-

Full form of IDEA is "International Data encryption algorithm".

Elements of IDEA:-

- → Key size = 128 bits.
- → Block size = 64 bits
- → Round = 8.
- → complex functions replace S boxes.
- → Highly resistant to cryptanalysis

RC5 :-

RC stands for "Rivest Cipher".

- → RC5 has a variable block size (32, 64, 128 bits)
- → Key size (0 to 2040 bits)
- → No. of rounds (0 to 255)

Confidentiality using Symmetric Encryption

Placement of encryption function has two approaches:-

(i) Link Encryption

(ii) End to End Encryption.

Link to link Encryption:-

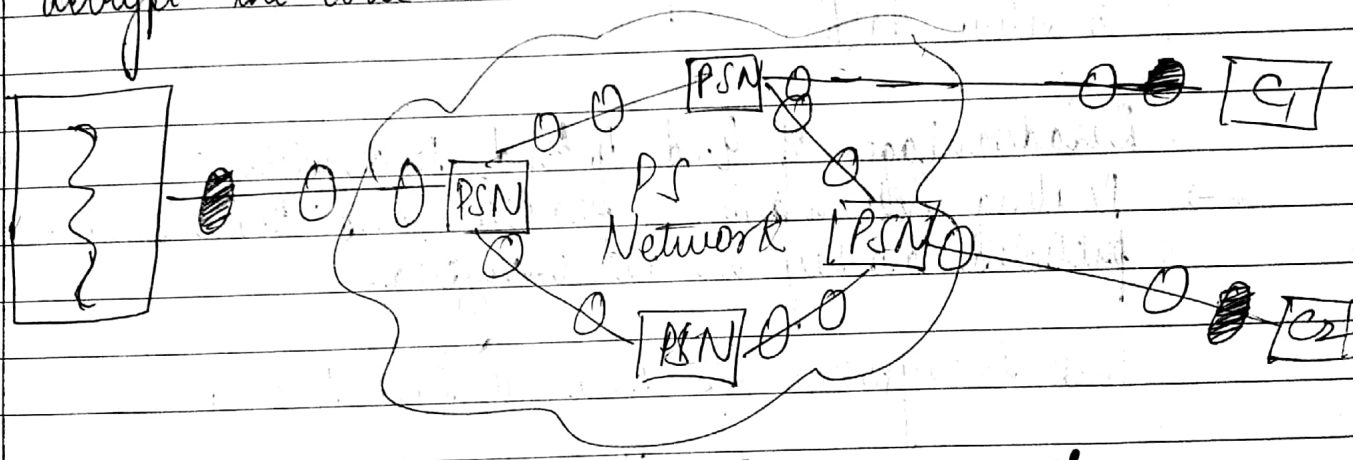
With link encryption, each vulnerable communication link is equipped on both ends with an encryption device. Thus, all traffic over all communication links are secured

Saathi

Date ___ / ___ / _____

Link encryption is an approach to communications security that encrypts and decrypts all traffic at each network routing point.

End to End Encryption :-
With end to end encryption, the encryption process is carried out at the two end systems. The source host or terminal encrypts the data. The data in encrypted form are then transmitted unattacked across the network to the destination terminal or host. The source shared a key with the destination & so is able to decrypt the code.



● = End to End encryption device
O = Link encryption device
PSN = Packet Switching node.

Advantages of Link Encryption :-
→ All data are encrypted including headers, addresses, and routing information
→ Users do not need to do anything to initiate it.
→ Encryption is automatic so there is less opportunity of human error

Page No.

Saathi

Date ___ / ___ / _____

Disadvantages of link Encryption:-

→ Key distribution and management are more complex because of each hop device must receive key, and when keys ~~are~~ change, each must be updated.

→ Packets are decrypted with each hop.

Advantages of end to end Encryption:-

→ A separate key is not req. for decryption of packet data.

→ Greater flexibility to user in ~~designing~~ deciding which data to encrypt.

→ Selective encryption provides great help in the case of sensitive data.

Disadvantages of End to End Encryption:-

→ Routing information, headers and trailers are not protected as they are not encrypted.

Link Encryption V/s End to End Encryption

Link Encryption	End to End Encryption
→ Encryption over individual links in network	→ Encrypt data at network end-points
→ Each link end point shares secret key.	→ Each pair of hosts/ applications share a secret key.
→ Requires all links/ devices to support encryption	→ Does not rely on intermediate network devices
→ Encrypts all the data along with specific communication path. Not only the information is encrypted, but the header, address etc that are part of the packets are encrypted	→ The headers, trailers, routing & addresses are not encrypted enabling attackers to learn more about captured packet & where it is headed

Page No.

Date ___/___/_____ Saathi

→ Works at physical & data link layers in OSI model | → Works at network layer & above.

Ans: Traffic analysis of traffic Confidentiality :-

1) In packet-switching Network, the packet header cannot be encrypted.
2) Monitoring of communications flows b/w parties
3) Link Encryption observes header details.
4) Traffic padding can further obscurer flows.
5) Traffic analysis reveals :-
   (i) Identities of partners
   (ii) How frequently the partners are communicating
   (iii) Message pattern, message length, quantity of message etc.

Key Distribution :-

(i) Symmetric schemes require both parties to share a common secret key.
(ii) But the issue is now to securely distribute this key. Hence are some alternatives of key distribution between the given parties A & B

(a) A can select key & physically deliver to B
(b) Third party can select & deliver key to A & B
(c) If A & B have communicated previously can use previous key to encrypt a new key.
(d) If A & B have secure communications with a third party C, C can relay b/w A & B

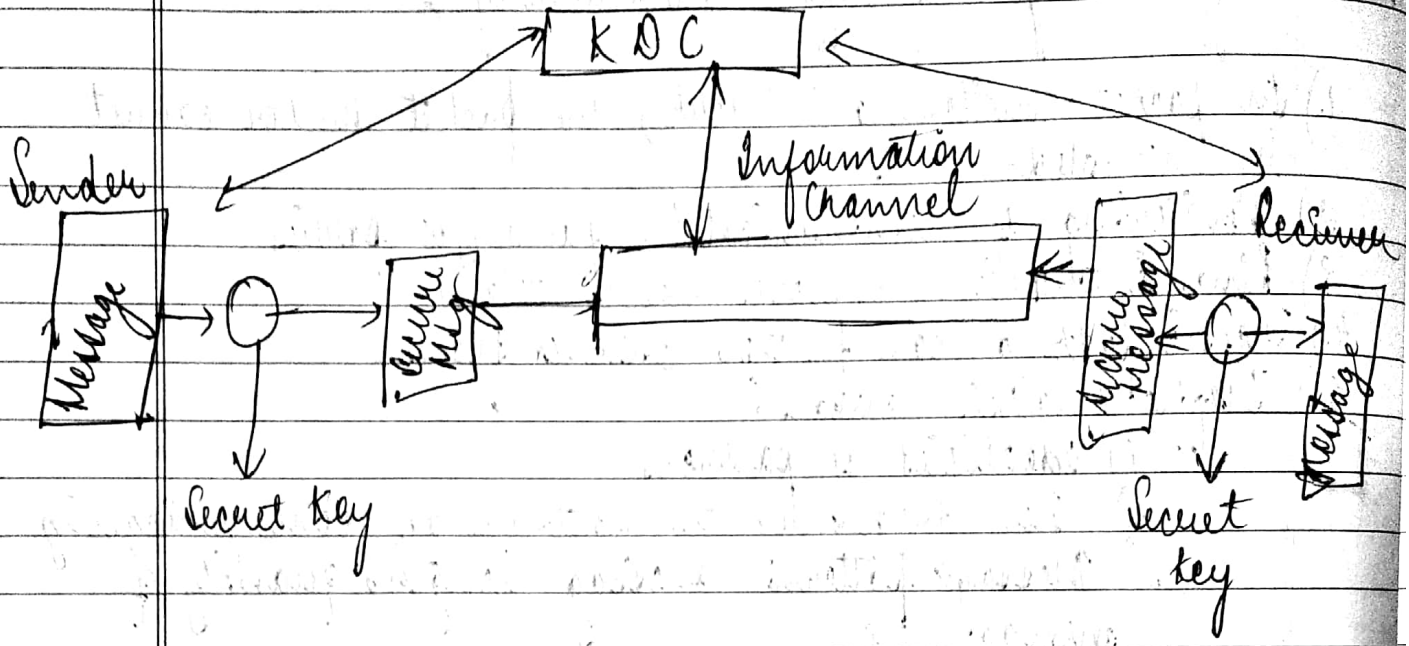
Page No. ____

Saathi

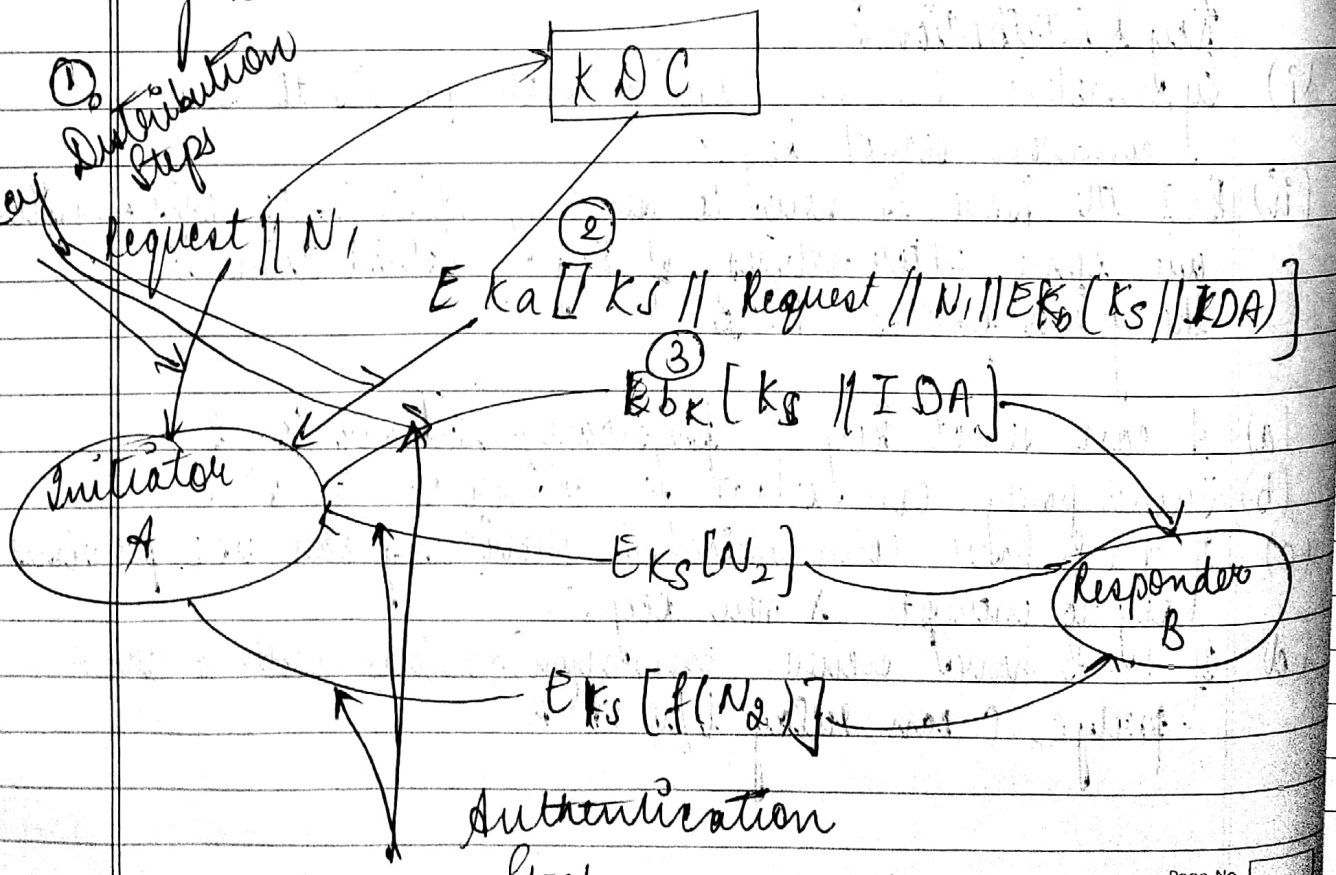
Date ___ / ___ / _____

Key distribution Centre :- (KDC)

KDC share a unique key ie Master key with each user to distribute secret key (session key) b/w a pair of users.



Key Distribution Scenario :-



Page No.

Saathi

Date __/__/____

1) A issues a request to the KDC for a session key
   (i) Nonce is also sent
   (ii) Nonce includes identities of communicating parties and a unique value

2) KDC sends a response encrypted with A's secret key K_A.
   (i) It includes one time session key K_s
   (ii) Original request message, include the nonce
   (iii) Message also included K_s & ID of A encrypted with K_B intended for B.

3.) A stores K_s and forwards information for B
   ie $E_{K_B}[K_s || ID_A]$

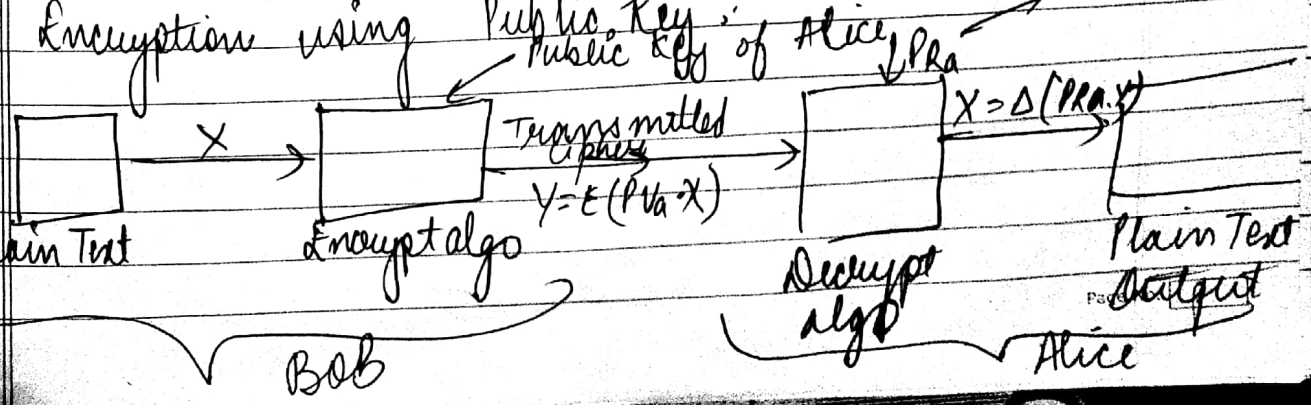
4) B sends a nonce to A encrypted with K_s.

5.) A responds by performing some function on nonce.

Assymetric Encryption or Public Key Cryptography

→ Plain Text
→ Encrypt algo
→ Public Private key
→ Cipher Text
→ Decrypt algo

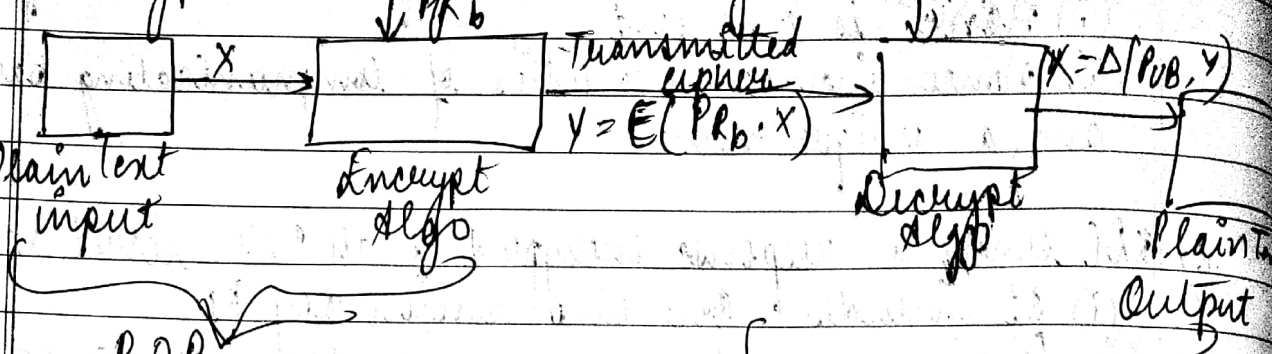
Encryption using Public key of Alice



Saathi

Date ___ / ___ / _____

Encryption using Private Key :-



Requirements of key management

- Secrecy of private keys
- Assurance of public key

Cryptography
- Symmetric (1 keys)
- Asymmetric (2 keys)

(PKI) Public key infrastructure :- (Standard for digital Certificates)
It provides the identification of public keys & their distribution.

- Public key certificate (Digital Certificate)
- Certificate Management System
- Private key tokens
- Certification Management Authority
- Registration authority

Saathi

Date ___ / ___ / _____

INFORMATION SECURITY

Part-2

Random Numbers :-

→ Many uses of Random Numbers in cryptography
(i) Nonces in authentication protocols to prevent replay
(ii) session keys.
(iii) public key generation
(iv) key stream for a one-time pad.

→ in all cases its critical that these values be
(i) statistically random, uniform distribution, independent
(ii) Unpredictability of future values from previous values.

Types of Random Numbers

- PRNG
  - Using ciphers as PRNGs
  - Pseudorandom function (PRF)
- Natural Random noise (TRNG)

Date __/__/____

Saathi

Pseudorandom Number Generators (PRNGs)

- Often use deterministic algo techniques to create "random numbers".
  - (i) Although are not truly random
  - (ii) can pass many tests of "randomness"

Seed → Deterministic algo → Pseudo random bit stream

- Generates a long-length random Number using algo based on a short "initial value"
- Known as "pseudorandom numbers."
- Created by "Pseudorandom Number Generators (PRNGs)"

PRNG's Requirements:-

- Randomness
- Uniformity
- Scalability
- Consistency
- Unpredictability
  - forward unpredictability
  - Backward unpredictability

Using block ciphers as PRNG's

- for cryptographic application
- for creating session keys from master key.
- Counter Mode $X_i = E_{Km}[i]$
- Output feedback Mode $X_i = E_{Km}[X_{i-1}]$

Pseudorandom Function

- It is used to produce pseudorandom string of bits of some fixed length
- Eg:-
  - (i) Symmetric Encryption keys
  - (ii) Nonces.

Seed, Context Specific Values → Deterministic algo → Pseudo Random Bit Stream

Page No.

Saathi

Date ___ / ___ / _____

Natural Random Noise (TRNG)

- Best source is natural randomness in real world
- find a regular but random event & monitor
- do generally need special h/w to do this
- Starting to see such h/w in new CPUs
- problems of bias or uneven distribution in signal

Source of True Randomness (Entropy Source)

↓

Conversion to Binary

↓

Random bit Stream

PRNG V/s TRNG

PRNG	TRNG
→ Deterministic system	→ Non Deterministic System
→ intentially generates a random no. not a complete random no.	→ generates a true random no.
→ The no. is usually generated by a s/w way	→ The no. is generated primarily by h/w way

~~Modular Arithmetic~~ :

Security policies :

Security Policies :- A general statement of security of particular organization or a set of rules & regulations of security of that organization or a documentation of that organization w.r.t security

Date __/__/____

Saathi

Need of security policies :-

→ Control security risk :- It is used to control certain security risk in an organization. The major primary resource of an organization is data. Any error in data, the data gets corrupted or any bits missing from data all these cases are case of security risk. There can exists other risks also, risks related to system, hardware, software, memory etc are controlled by security policies.

→ Identify theft :- Data theft, time of theft, place etc are measured / find by measures defined in security policies

→ System fraud :- Misusing organizations information & system for other purposes.

→ System misuse / fraud detection :- Used to detect system fraud.

Primary Security Policies :-

→ Regulatory :- A set of standard rules which need to be followed in each and every organization

→ Advisory :- Certain set of instructions / measures or a form of advise the employee of organization about dos and don'ts for organization.
Eg :- behaviour of Employee etc.

→ User policies :-
Eg :- User must change password periodically to be more secured or If a user is given a system from an organization the system must be used for that organization only not for any other work.

Page No.

Saathi

Date __/__/____

Active attack	Vs	Passive attack
Active		Passive
→ Modifies the data		→ Monitors the data
→ Effect the system		→ Does not effect the system
→ can be easily detected		→ cannot be easily detected
→ Threat to integrity & availability		→ Threat to confidentiality
→ Capture physical control over link.		→ Just observe the transmission
→ Detection		→ Prevention.

Modular Arithmetic:-

→ $x \equiv y \bmod n$:- If both x and y leave same remainder when divided by 'n'.
Eg:- $3 \equiv 24 \bmod 12$

→ $x \equiv y \bmod n$:- If n divides $(x-y)$
Eg:- $20 \equiv 3 \bmod 7$ (17 divides $(20-3=17)$)

→ If $x \equiv y \bmod n$ & $a \equiv b \bmod n$ then
$(x+a) \equiv (y+b) \bmod n$
Eg:- $17 \equiv 4 \bmod 13$ & $42 \equiv 3 \bmod 13$
$\Rightarrow 59 \equiv 7 \bmod 13$

→ If $x \equiv y \bmod n$ & $a \equiv b \bmod n$ then $(x-a) \equiv (y-b) \bmod n$
Eg:- $42 \equiv 3 \bmod 13$, $14 \equiv 1 \bmod 13$ ⇒ $28 \equiv 2 \bmod 13$

→ If $x \equiv y \bmod n$ and $a \equiv b \bmod n$ then
$(x * a) \equiv (y * b) \bmod n$.
Eg:- $6 \equiv 1 \bmod 5$, $7 \equiv 2 \bmod 5$ ⇒ $42 \equiv 2 \bmod 5$

Page No.

Date ___ / ___ / _____ Saathi

Number Theory :- No. of concepts from number theory does are essential in the design of public key crypto algo.

→ No. theory deals with the theory of numbers & is probably one of the oldest branches of mathematics

Divided into several areas including
→ Elementary
→ Analytic
→ Algebraic no. theory.

→ Prime Numbers:- A prime no. p is an integer greater than 1 with only two five divisors, 1 & itself
∴ its factors consists of four integers.
+1 & ±1

→ Prime nos. are of atmost importance to certain cryptographic algos & most of the techniques used will not work without them.

→ Any integer $a > 1$ can be factored in unique way as.

$$a = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_t^{a_t}$$

where $p_1 < p_2 < \cdots p_t$ are prime nos & where each a_i is a +ve integer.

Eg:- 5 is a prime no.
∴ its factors are 1 & 5
ie $5 = 1 \times 5$.

Eg:- 3, 7 is a prime no.
21 is not.
But $21 = 3 \times 7$ (ie. product of primes)
$63 = 3^2 \times 7$ ~~$= 9 \times 7$~~

Similarly $9975 = 3 \times 5^2 \times 7 \times 19$

If an integer is not prime, it is composite no.

Page No.

Saathi

Date ___ / ___ / ___

Relatively Prime Nos :- No common divisor apart from 1

(i) Eg :- 8 & 15 are 2 nos.

$8 \Rightarrow 1, 2, 4, 8$

$15 \Rightarrow 1, 3, 5, 15$ → & common factor is only 1

$GCD(8, 15) = 1$

General formula :- $a = \pi_{p \in P} p^{ap}$ where $ap \geq b$

(ii) $GCD(a, b) = C$

gcd (24, 32)

$24 = 1, 2, 3, 4, 6, 8, 12, 24$

$32 = 1, 2, 4, 8, 16, 32$

Common divisors $= \pm 1, \pm 2, \pm 4, (\pm 8)$ → GCD

$GCD(24, 32) = 8$

Def :- Fermat's Theorem :-

Useful in public key & primality testing. if

→ p is prime

→ 'a' is positive integer not divisible by p

ie $(\gcd(a, p) = 1)$

then

$a^{p-1} \equiv 1 \pmod p$ or $\frac{a^p}{a} \equiv 1 \pmod p$

$a^{p-1} \pmod p \equiv 1$

or $a^p = a \pmod p = a$

~~$x^{n-1} = 1 \bmod$~~

Saathi

Date __/__/__

Eg :- $13^6 \mod 17$

$a = 13$

$p = 17$

Satisfies all the conditions.

$\therefore 13^6 \mod 17 = 1$

So, $13^{17-1} \equiv 1 \pmod{17}$

$\frac{13^{17}}{13} \equiv 1 \pmod{17}$

$13^{16} \equiv 1 \pmod{17}$

2.) $5^{18} \mod 19$.

$a = 5$

$p = 19$ $\quad p - 1 = 18$

$15^{18} \mod 19 = 1$

3.) $5^{90} \mod 19$

$5^{19 \times 17 + 1} \mod 19$

$\Rightarrow 5^{19} \cdot 5^1 \mod 19$

$\Rightarrow 5^{18} \mod 19 \cdot 5 \mod 19$

$\Rightarrow 5 \cdot 5$

$= 25$

Left hand side is smaller than right hand side then the LHS is answer

3.) $13^{15} \mod 15$

$\Rightarrow 13$

$\Rightarrow 13^{16} \mod 17$

$p = 17$

$a = 13$

but $17 - 1 \nmid 15$

Fermat's theorem will not be applied

Saathi

Date ___ / ___ / _____

def:- Euler's totient function :-
Very useful in RSA Algo.

→ $\phi(n)$ for $(n \geq 1)$ is defined as the no. of +ve integers less than 'n' that are co-prime to 'n'.

co-prime ⇒ gcd (2 nos) = 1

$\phi(5) = \{1, 2, 3, 4\} = 4$
$\phi(6) = \{1, 2\} = 2$ → No. of elements in set due totient fun^{n}.

[Only those elements are included in this set those who have gcd(a, b) = 1]

When 'n' is a prime no.
$\phi(n) = n - 1$ (no. of elements in set)
Eg:- $\phi(23) = 22$

$\phi(a * b) = \phi(a) * \phi(b)$ [a & b are co prime]

$\phi(35) = \phi(7) * \phi(5)$
$= (7-1) * (5-1)$
$= 6 * 4$
$= 24$

[gcd(7, 5) = 1]

Can be represented by multiplication of two prime nos.

Saathi

Date ___/___/_____

Aut:- Euler's theorem:- (relatively primes)
If x and n are co primes then it can be written in the form of:
$x^{\phi(n)} = 1 \bmod n$
where $\phi(n)$ is Euler totient function
↓
count of nos. which are relatively prime to n and those less than n.
Eg:- $\phi(10) = 4 = \{1, 3, 7, 9\}$

case 1:- If n is prime
$\phi(n) = n-1$
Eg:- $\phi(7) = 6$
nos. relatively prime to 7 are:- 1, 2, 3, 4, 5, 6.
count is 6.

Case 2:- If n is a product of two prime nos. p & q.
$\phi(n) = \phi(p) * \phi(q)$
$= (p-1) * (q-1)$
Eg:- $\phi(21) = \phi(7) * \phi(3)$
$= 6 * 2$
$= 12$ 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20
Relatively prime:- {1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20}

Case 3:- If $n = p^e$ where.
$\phi(n) = p^e - p^{e-1}$
Eg:- $\phi(8) = \phi(2^3) = 2^3 - 2^{3-1}$
$= 2^3 - 2^2$
$= 8 - 4 = 4$
Rel. prime = {1, 3, 5, 7}

Page No.

Saathi

Date ___ / ___ / _____

Ans:- RSA Algorithm:-

→ RSA stands for Rivest, Shamir, Adleman.
→ Named after Rivest, Shamir, Adleman
→ Encrypt & Decrypt based on no. theory
→ Variable key length; short (512 bits)

Algo:- [Key generation process:-]

Symmetric :- same key in both sides
Asymmetric :- Two keys.
public private

→ Consider two larger prime nos, p & q
→ Calculate $\phi(n) = (p-1)*(q-1)$ p & q.
→ Euler's totient fun^n.
$$\phi(n) = (p-1) * (q-1)$$

- Assume 'e' (public key used by sender at encryption sides)
e is such that $\gcd(e, \phi(n)) = 1$

- Assume 'd' (private key used by reciever at decryption side).

d such that → congruent module

$$d \equiv e^{-1} \bmod \phi(n)$$
$$d \times e \equiv 1 \bmod \phi(n) \rightarrow \text{equals}$$
$$d \times e \bmod \phi(n) = 1 \bmod \phi(n)$$
$$d \times e \bmod \phi(n) = 1$$

Page No.

Saathi

Date __/__/____

Public key = { e, n }
Private key = { d, n }

Public key of sender is known to receiver & public key of receiver is known to sender.
And private key of sender is not known to receiver & similarly receiver's private key is not known to sender.

→ 1.) Choose 2 prime nos. p & q
p = 7, q = 3. [p & q can be more largen]

→ 2.) Compute n = p * q = 7 × 3 = 21

→ 3). $\phi(n) = \phi(p * q)$
$= \phi(p) * \phi(q)$
$= (p-1) * (q-1)$
$= 6 \times 2$
$= 12$

value of e should be coprime to $\phi(n)$

4.) Choose 'e' $1 \leq e < \phi(n)$ compute to $\phi(n)$

Co primes :- gcd(3, 7) = 1,

Saathi

Date ___/___/_____

Encryption :-

$M < n$ (M = Original message, cipher text, $C = M^e \bmod n$)

Decryption :-

$M = C^d \bmod n$

Eg :- Consider $p = 7$, $q = 3$.

$n = p * q$

$n = 7 * 3$

$n = 21$

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

$= 6 * 2$

$\phi(n) = 12$.

Now, assume $e = 5$

ie. e, $\gcd(e, \phi(n)) = 1$

$\gcd(5, 12) = 1$.

Now d,

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

$d \times 5 \bmod \phi 2 = 1$

$5 \times 5 \bmod 12 = 1$

$25 \bmod 12 = 1$

public key = {5, 21}

private key = {5, 21}

Saathi

Date __/__/____

Encryption :-

$M = 20$

$C = M^e \bmod n$

$= 20^5 \bmod 21$

$= 3200000 \bmod 21$

$\boxed{C = 20}$

Decryption

$M = C^d \bmod n$

$= 20^5 \bmod 21$

$= 3200000 \bmod 21$

$\boxed{M = 20}$

Cryptanalysis :- Cryptanalysis is the study of cipher text, ciphers & cryptosystem with the aim of understanding how they work & finding & improving techniques for defeating or weakening them.

Linear cryptanalysis :- It is general form of cryptanalysis based on finding affine (approximations) to the action of the ciphers. Attacks have been developed for block ciphers & stream ciphers.

Differential Cryptanalysis :- It is the study of how differences in information input can affect the resultant difference at the output.

Digital Certificates :-

[Standardized by PKI]

→ Small file on computer / Electronic device
→ File extension is generally (.cer)
→ Establish relation b/w user & public key.
→ Certificate must be issued by trusted entity.

CA (Certification Authority) [X.509 defines the standard of DC]

→ A trusted agency issuing digital certificates
→ It takes responsibility for identifying correctly the identity of the client asking for a certificate

Page No.

Date ___ / ___ / _____

Functions of CA :-

→ Generating key pairs :- CA generates key pairs independently or join with client.

→ Issuing digital certificate.

Date __/__/____

Saathi

INFORMATION SECURITY

Part III

Chapter 8 :- Authentication Protocols

Authentication Application :-

Authentication means verifying user identity ie

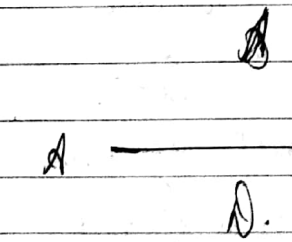
Keys

Public → Private → Not Shareable.

Encryption Decryption

→ Public Access

Suppose if a network consists of four different users. Let it be A, B, C and D.



All users are having permissions to communicate with each other.

If A wants to communicate with C. C should be authenticated by A and A should be authenticated by C. ie. C must know that the received message is coming from the perfect sender.

Page No.

Date ___/___/_____

Saathi

Types of authentication

→ Message authentication / Authentication function / Message Encryption

→ Message Authentication Code

→ Hash function

→ Message Authentication :-

Cipher text → Authenticator

~~In this message author~~ Sender and reciever should be authenticated by each other. This process is done only through cipher text. Thus it called authenticator.

→ Message authentication code.

There are some authentication functions. Apply the authentication functions from plain text along with key which uses a fixed length code is called message authentication code. (MAC)

$C(M, K)$ = Fixed length code (MAC)

C → Authentication function; M → plain Text Message; K → Key

Fixed length code → Authenticator (Msg Authentication code) (Msg digest)

MD or

→ Hash functions :-

← Similar to MAC

Apply hash functions here.

H → Represents hash functions

$H(M)$ = Fixed length code (HASH Code)

Independent of Key

H → hash fun.; M → plain Text Msg

Authenticator

Page No.

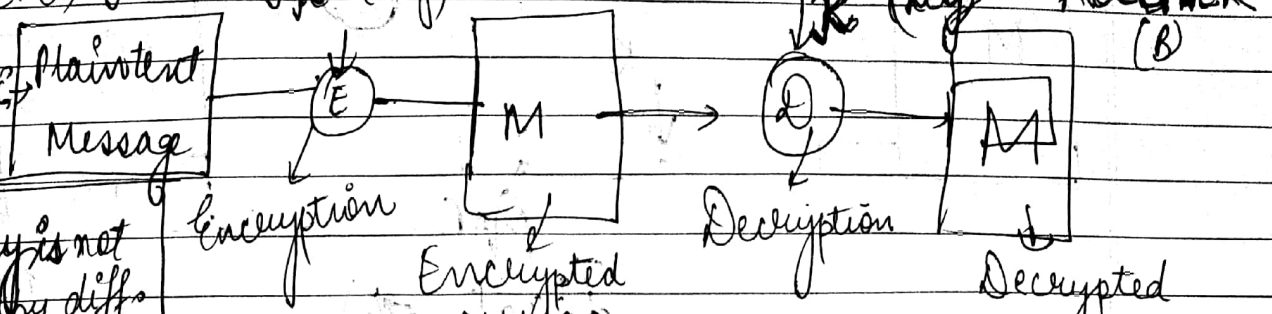
Date __/__/____

Saathi

Message Encryption (Cipher text - Authenticator)

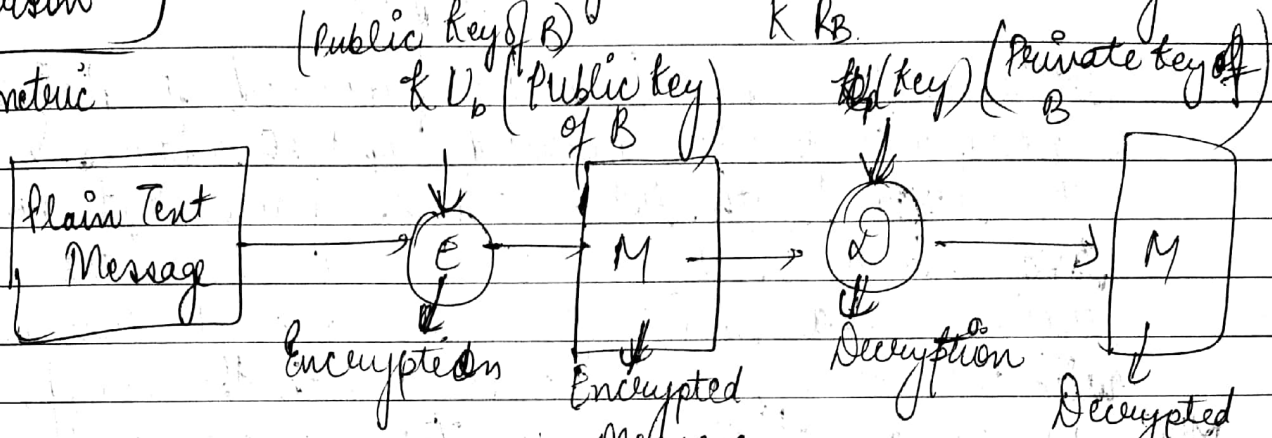
SENDER (A) — RECEIVER (B)

(i) Symmetric



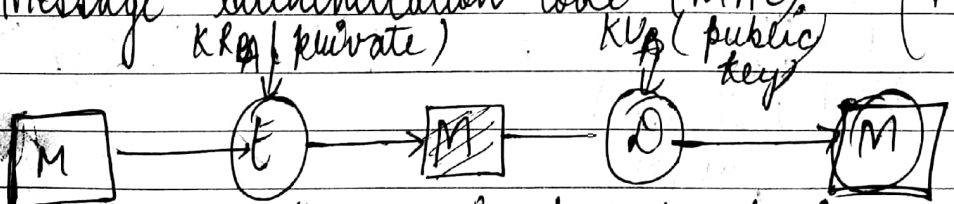
The key is not shared by diff. person

(i) Asymmetric



At encryption side public key of user B is used.
Here A is not authenticated by B.
At sender side anyone can sent the message but at recievers side only B can recieve the message.
Confidentiality is achieved but authentication is not achieved.

(ii) Message Authentication Code (MAC) (MAC - Authenticator)

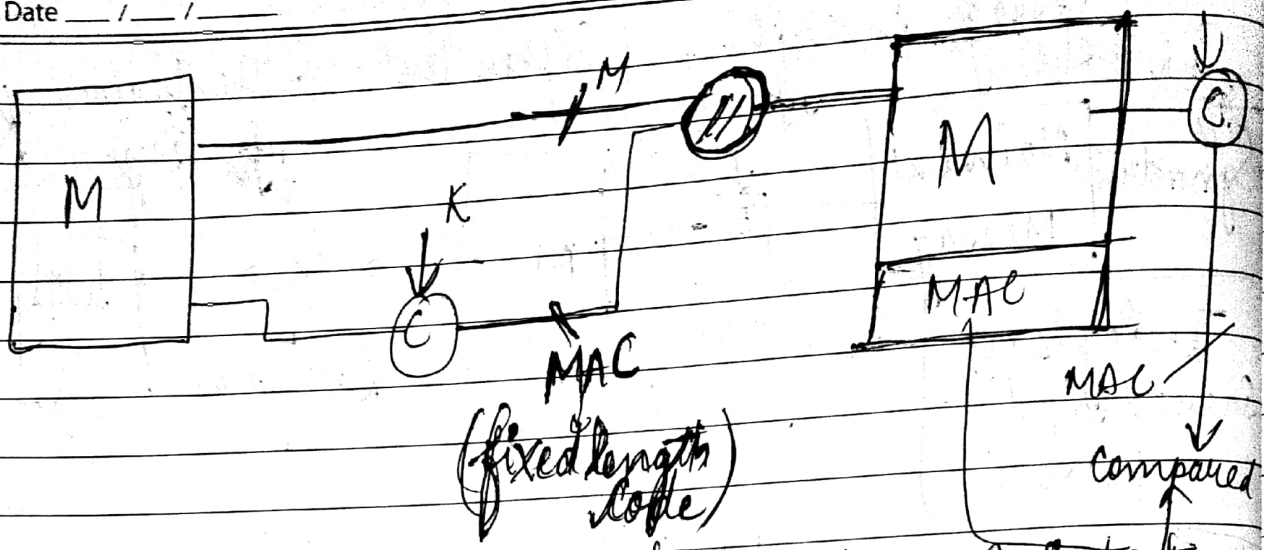


Authentication achieved but not Confidentiality

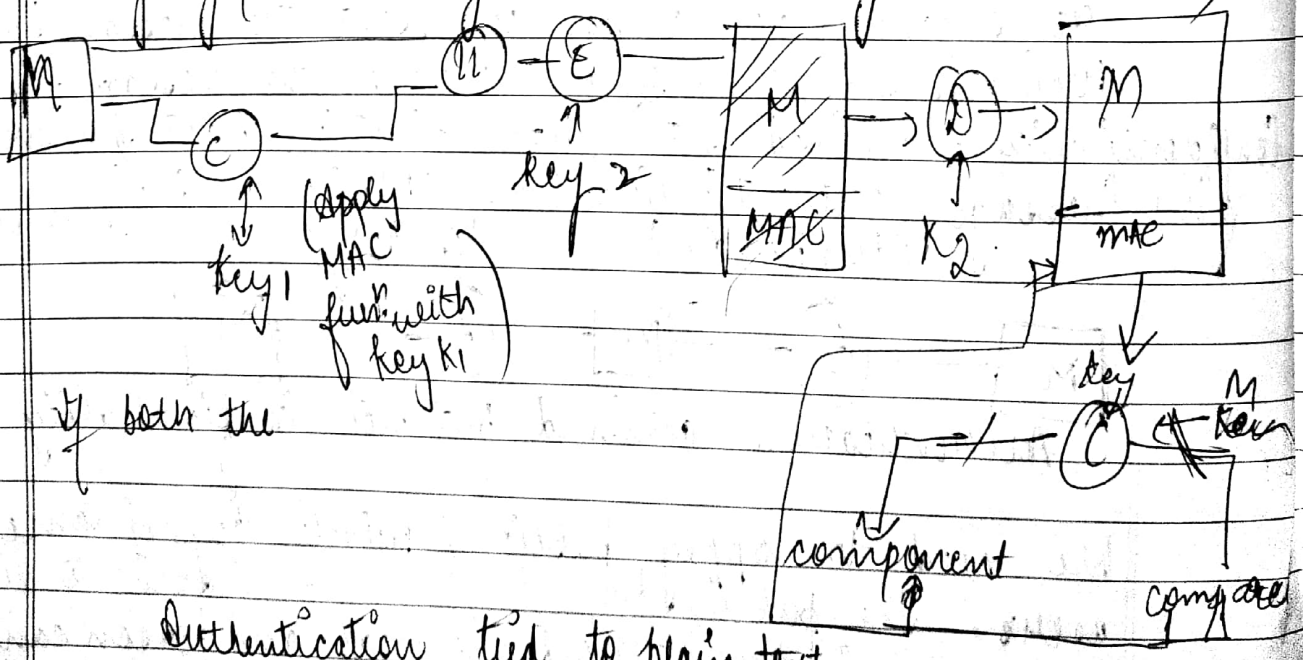
We need to apply public & private keys of same users. The public key of B is available to all the users in the network. So that any person can encrypt the message and sent to the recievers that means, the confiden

Page No.

Date ___ / ___ / _____



Authentication functions are performed on plain text along with the key generated by MAC address & append the fixed length code with plain text message and send it to receiver's end and at the receiver's end again apply same authentication functions with the same key to compare both values. If both MAC are equal that means the message has been successfully reached to its destination and this implies integrity (no change in data during transmission)



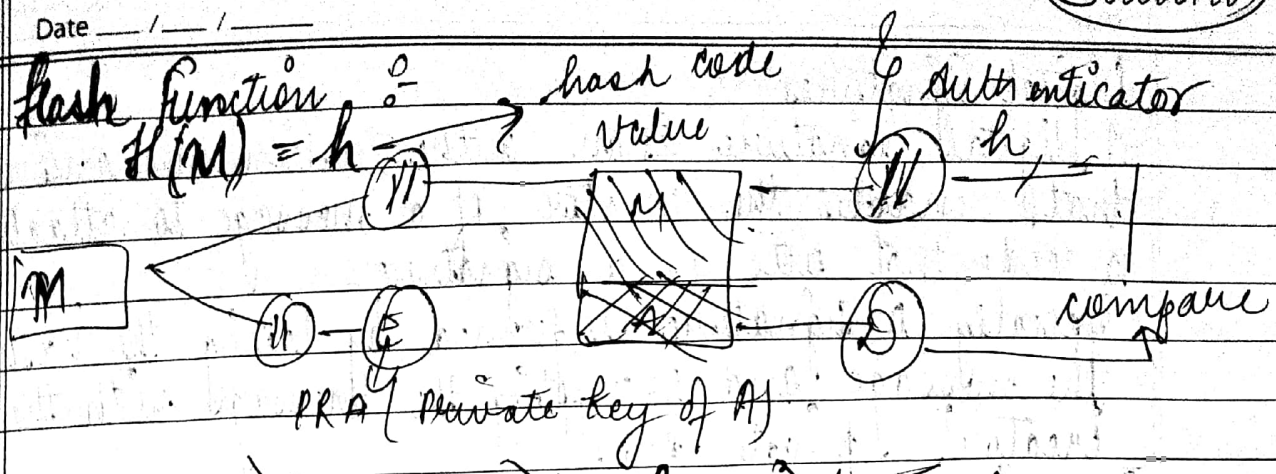
If both the

Authentication tied to plain text.

Saathi

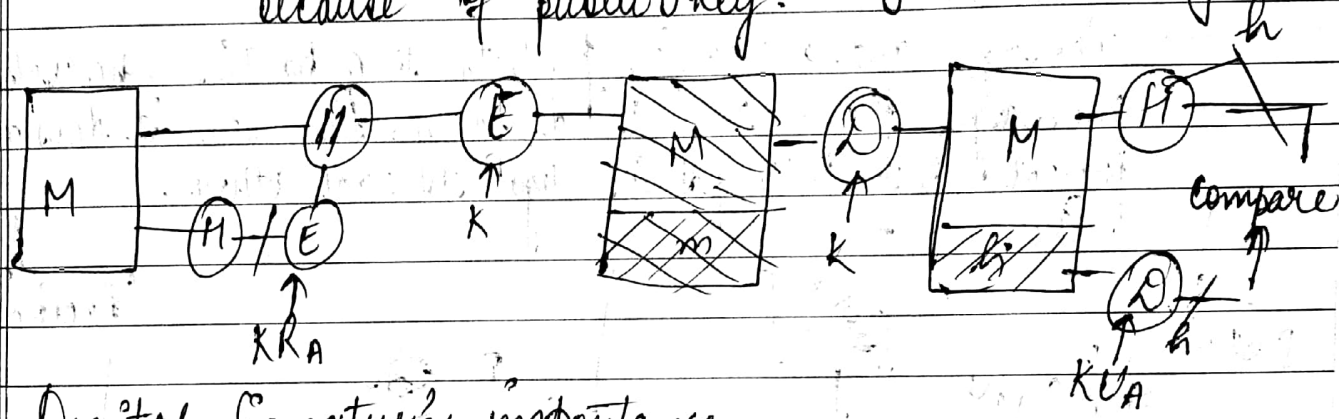
Date __/__/____

(iii) Hash function :- $H(M) = h$ → hash code value



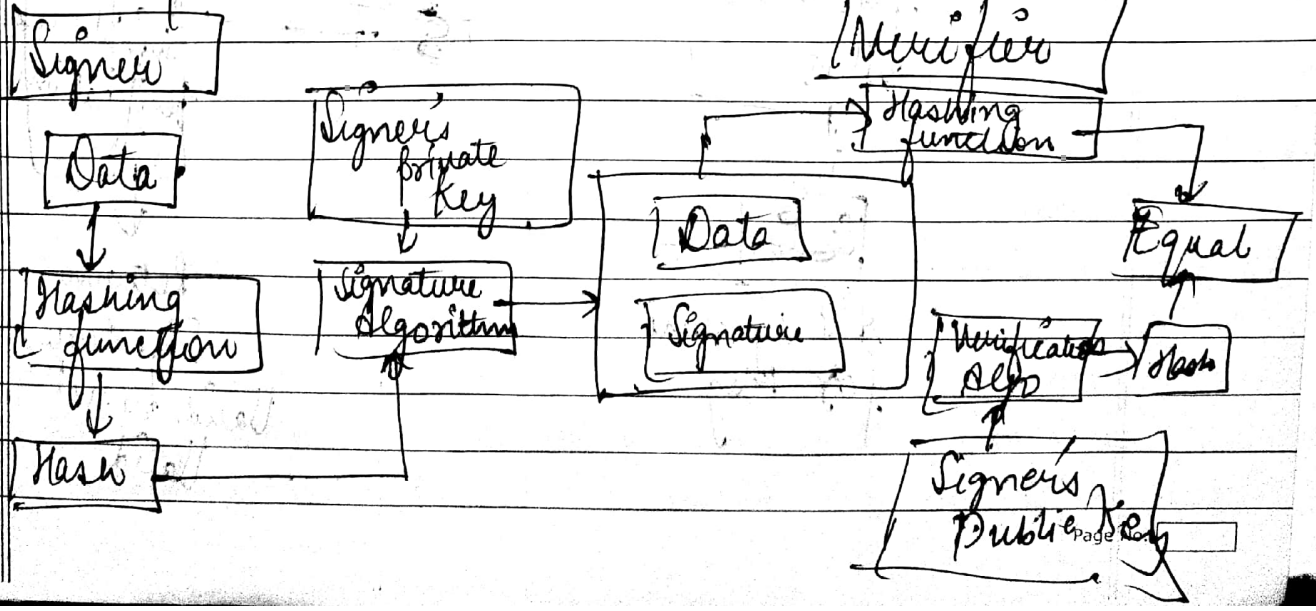
Drawback :- M is not encrypted anyone can decrypt by because decrypted because of public key.

Drawbacks :- M is not encrypted anyone can decrypt because of public key.



Digital Signatures importance

→ Message authentication
→ Data Integrity
→ Non Repudiation



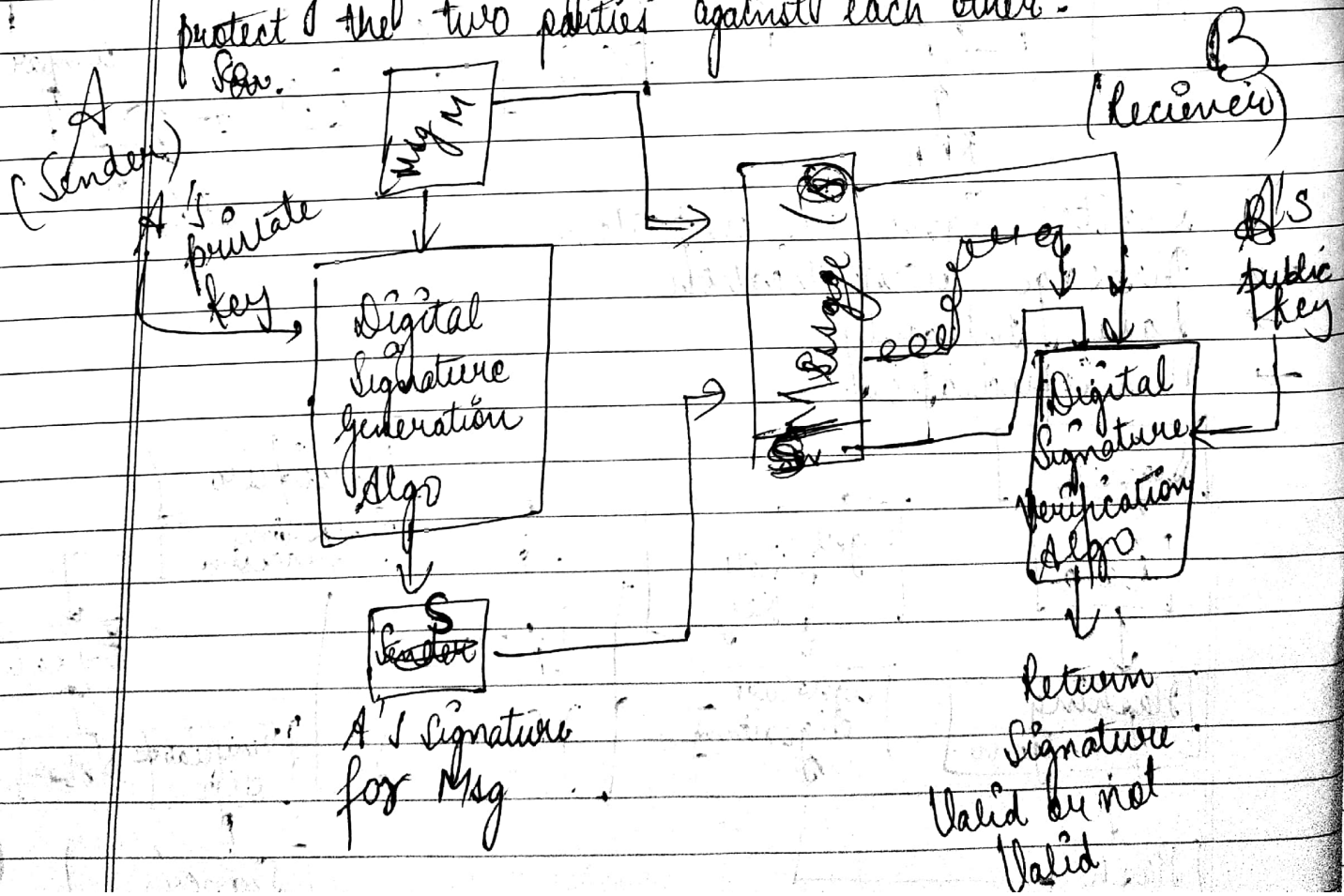
Date ___/___/___

Digital Signatures

A digital signature is an authentication mechanism that enables the creator of a message to attach a code that acts as a signature.
Typically a signature is formed by taking the hash of the message and encrypting the message with the creator's private key.
The signature guarantees the source and integrity of the message.
The digital Signature Standard (DSS) is an NIST standard that uses the secure hash algo (SHA).

Properties :-

→ Message authentication protects two parties who exchange messages from any third party. However it does not protect the two parties against each other.



Date ___/___/_____ Saathi

Eg:- Suppose that A sends an authenticated message to B, ~~using one of~~.

→ B may forge a different message and claims that it came from A. B would simply have to create a message and append an authentication code using the key that A & B share.

→ A can deny sending the message. Because it is possible for B to forge a message, there is no way to prove that A did in fact send the message.

In those situations there must be complete trust between sender and reciever, something more than authentication is needed. The most attractive solution to this problem is digital signature.

→ It must verify the author and the date & time of the signature.

→ It must authenticate the contents at the time of the signature.

→ It must be verifiable by third parties, to resolve disputes.

Attacks by Digital Signatures:-

→ Key-only attack:- When C only knows A's public key.

→ Known message attack:- C is given a set of messages & their signatures.

→ Generic chosen message attack:- C chooses a list of messages before attempting to breaks A's signature scheme, independent of A's public key. C then obtain from A valid signatures for the chosen messages. The attack is generic because it does not depend on A's public key.

→ Directed chosen message attack:- Similar to generic attack, except that the list of messages to be signed is chosen after C knows A's public key but before any

Page No. ___

Saathi

Date __ / __ / ____

Signatures are seen.

[redacted]

Requirements for digital signature :-

→ The signature must be a bit pattern that depends on the message being signed

→ It must be relatively easy to produce the digital signature

→ It must be relatively easy to recognize and verify the digital signature.

→ It must be practical to retain a copy of the digital signature in storage.

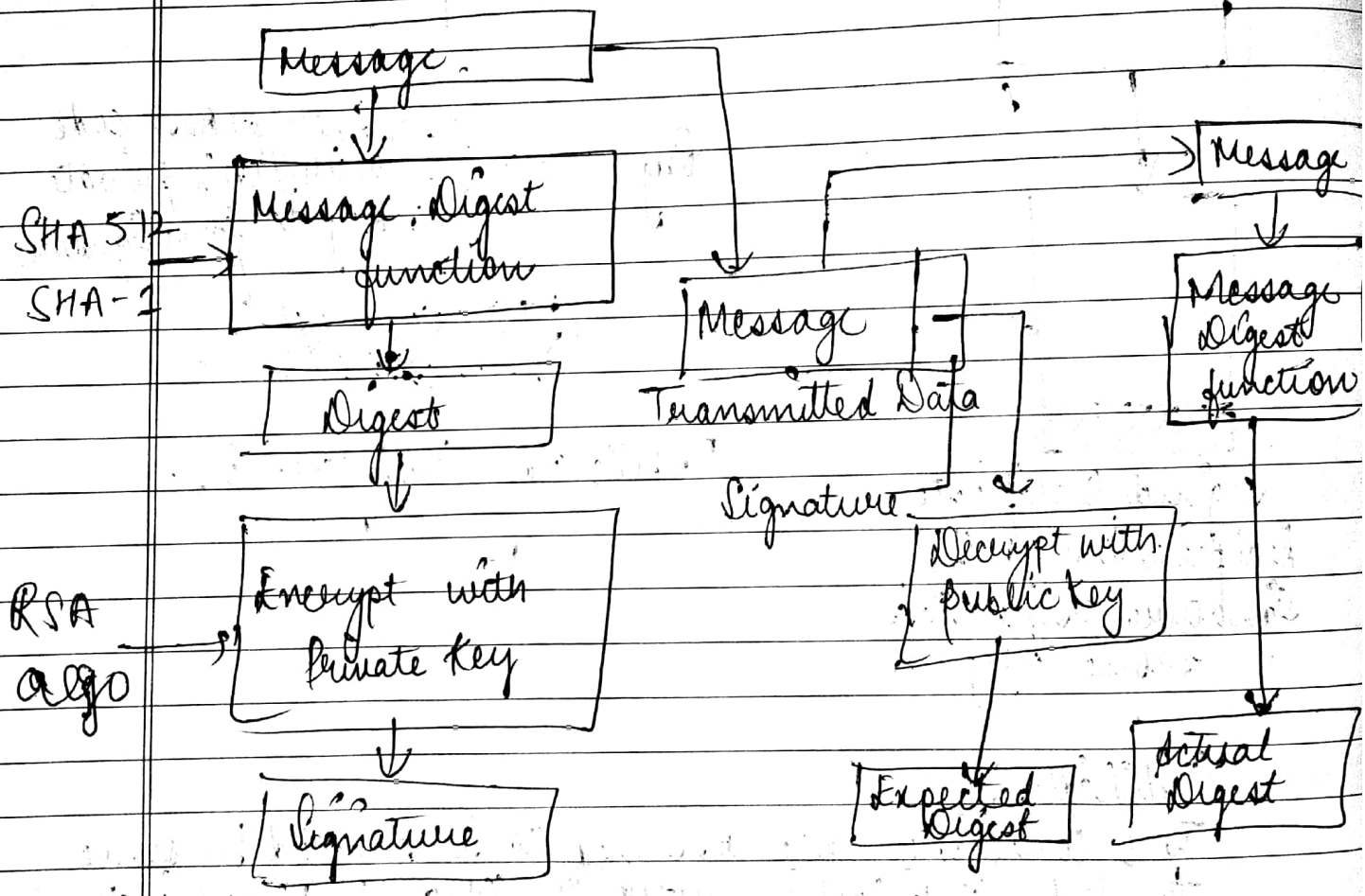
(Saathi)

Date __/__/____

~~MD5~~ ~~(Message Digest 5)~~

RSA Data Security Digital Signature Process :

In RSA digital Signature process, the private key is used to encrypt only the message digest. The encrypted message digest becomes the digital signature and is attached to the original data.



To verify contents of digitally signed data, the recipient generates a new message digest from the data that was recieved, decrypts the original message digest with Originator's public key & compares the decrypted with newly generated

Page No.

Date ___/___/_____

Saathi

Digital Signature Security Standards

The digital signature processes for DSA and RSA are generally considered to be of equal strength. However, DSA requires the use of the SHA-1 message digest function to ensure strong digital signatures. RSA can be used with another message digest function besides SHA-1.

DSA signature verification process increases computer processor load significantly relative to RSA process.

Uses of Digital Signatures

- Authenticate online entities
- Verify the authorship or origin of digital data
- Ensure the integrity of digital data against tampering

Saathi

Date __/__/____

Imp:- MD5 Message digest algorithm.

Hash function :- It is a mathematical function that converts a numerical input value into another compressed numerical value.
↳ O/p is always of fixed length.

Suppose we have a message of any length. When we pass the message through a hash function, we will get an output known as hash value
The output size is always same.

Message (any length)
↓
[Hash function]
↓
[Hash Value]

Hash value size ≠ message size
will size from message

That is why hash functions are also known as compression functions

The hash value generated is called message digest.

Suppose there is a hash function which produces output of 4bit. So, whether input is of 10 or 12 bit the output recieved will always be of 4bit.
Output is constant or of fixed length.

Date __/__/____

Saathi

Features :-

→ fixed length output
→ Compression function because of small size output
→ Since hash is smaller representation of larger data, It is also refered as digest.

Properties :-

→ $M \longrightarrow H$ (Easy)
calculation of hash function through a message is very easy.
$H \rightarrow M$ (Difficult)
Calculation of message through hash function is very difficult, almost impossible.
→ For a perticular message, the hash value will remain constant if calculated n number of times

$M \longrightarrow H$
$\vdots$
$n \text{ - - - } > H$
} Same hash Value for same message everytime

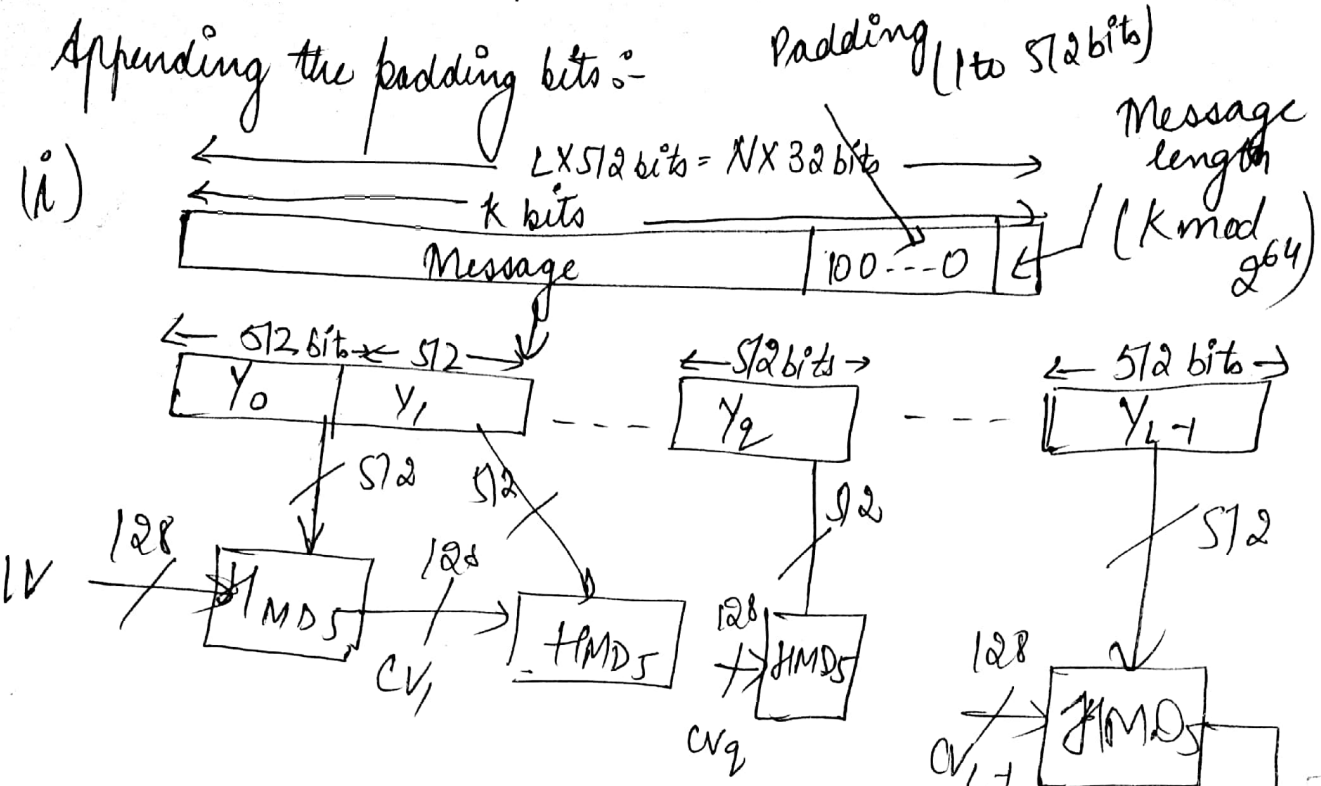
→ Hash values of two different messages can never be same.

$M_1 \rightarrow H_1$
$M_2 \rightarrow H_2$
} $H_1 = H_2$ → should not happen

MD5 logic :- The algorithm takes as input a message of arbitrary length and produces as output a 128-bit message digest. The input is processed in 512-bit blocks.

Appending the padding bits :-

(i)



(ii)

128-bit digest

Saathi

MD5 (MESSAGE DIGEST)

↳ Developed by Ron Rivest

↳ Fast and produces 128-bit message digests

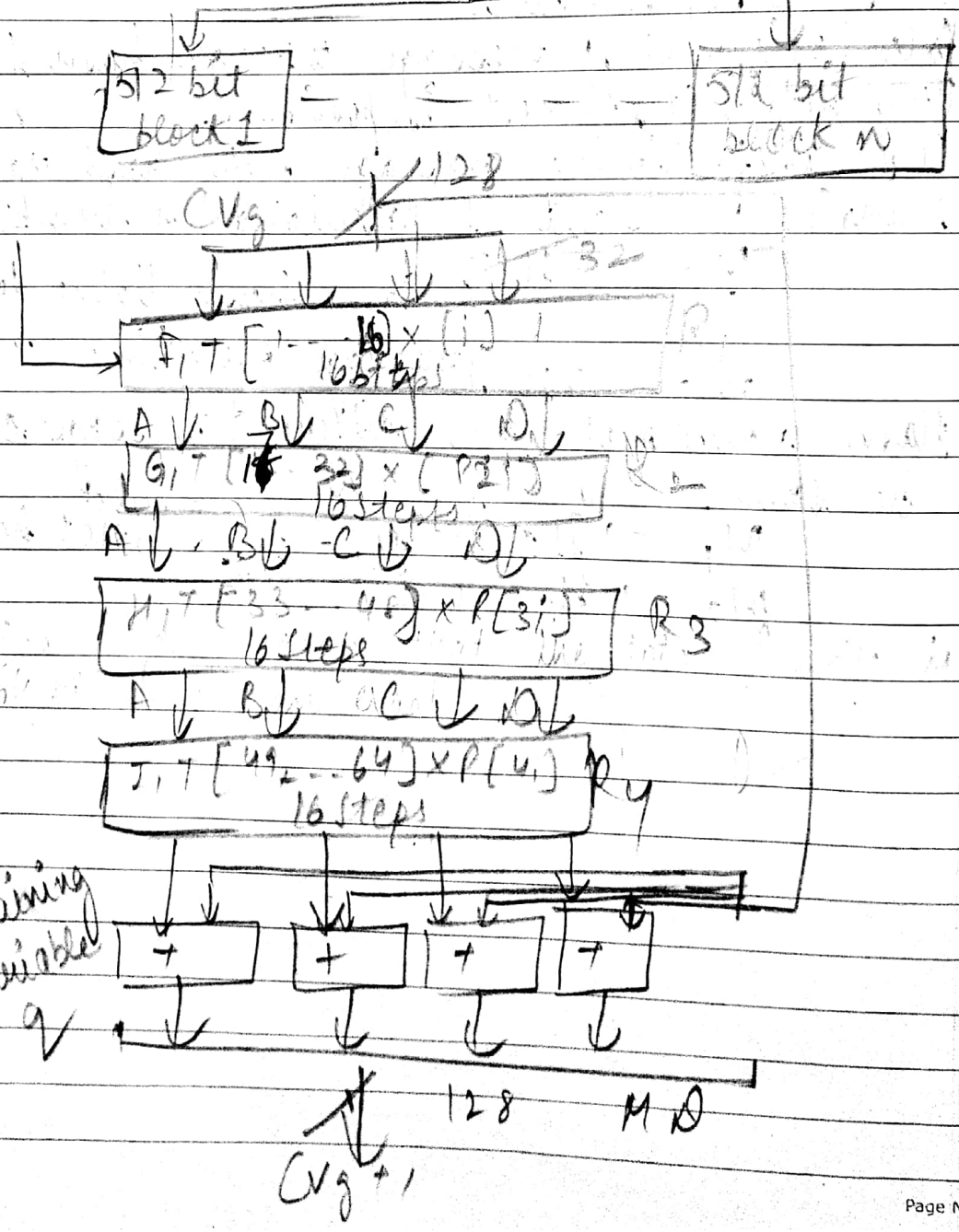
Working :-

Original message / Padding

Exact multiple of 512

Original message / Padding / length

Step (iii)



Date ___/___/_____ Saathi

(i) Padding is done such that the total length is 64 bit less than exact multiple of 512.

Suppose a message of 1000 bits. Now how much bits must be added into it so that it must be 64 bits less than 512 bits.

Size of Buffer = 32 bits.

4 buffer output

Lets see the exact multiple of 512.

$512 \times 2 = 1024$

$512 \times 3 = 1536$

-64

1472

Say → Length = 512 − 64 = 448

mult. of 512, ← 448

Now adding a padding of 472 bits into 1000 bits & it will become 1472 which is 64 bit less than exact multiple of 512.

(ii) Append the original length before padding. (mod 64)

Original length before padding = 1000

1000 || [Length mod 2^{64}]

1000 mod 2^{64} → The value will be added into step2. Generally 64 bits are added, when 64 bits are added into it, it will become an exact multiple of 512

(iii) Divide it in 512 bit blocks

(iv) Initialize 4 chaining variables (32 bit) & denoted by A, B, C, D.

The values of these variables are pre Defined

Page No.

Date ___ / ___ / ____

(v) Process Blocks

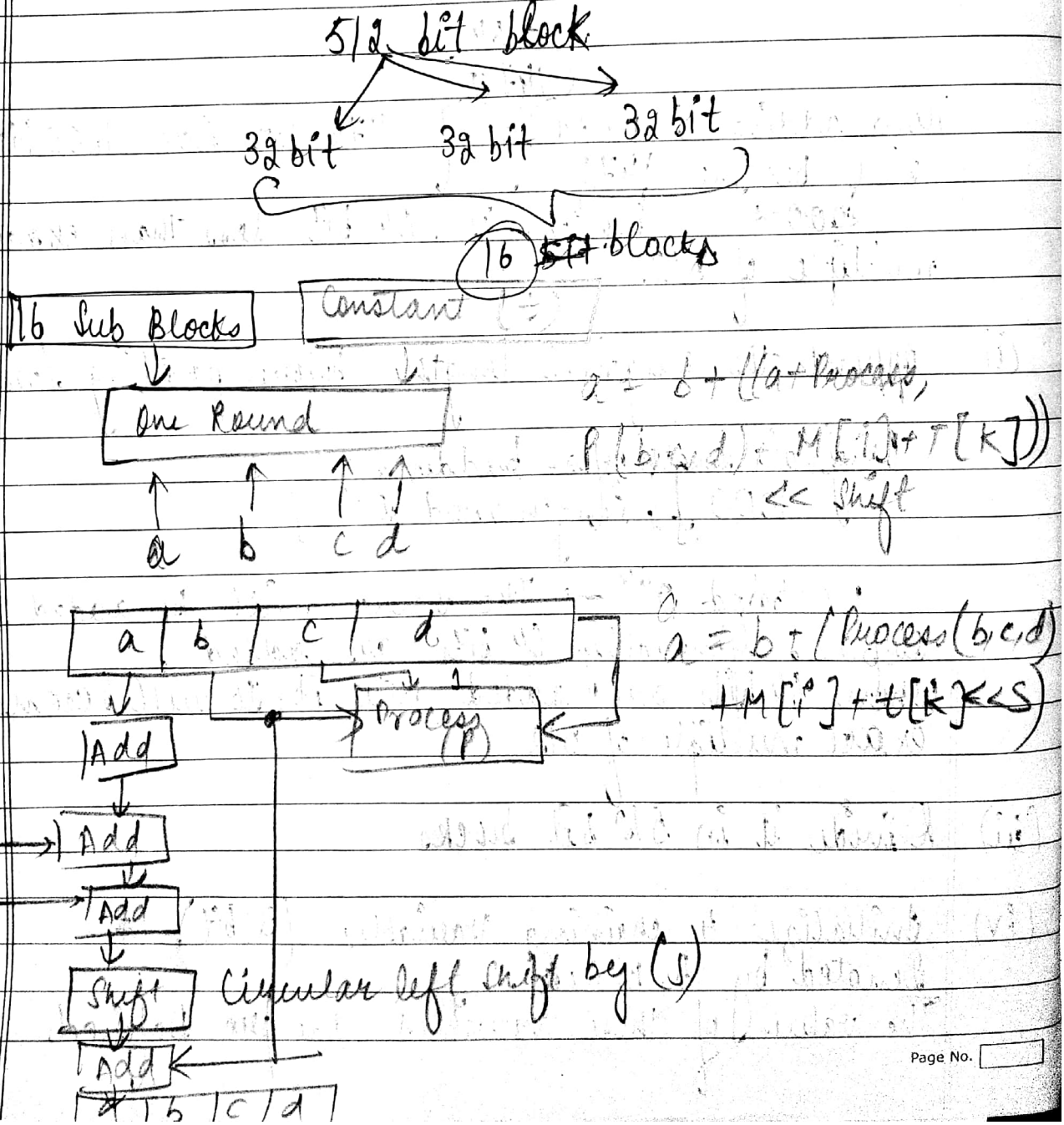
A loop runs for every 512 bit blocks. So copying the 4 chaining variables into 4 corresponding chaining variables & after

↳ Copy four chaining Variables into corresponding variables:

A = a, B = b, C = c, D = d }

↳ Divide 512-bit block into 16 (32 bit blocks)

↳ Four Rounds.



Date __/__/__ Authentication Algorithms

Saathi

~~Hash function~~ SHA 512

SHA → Secure hash algorithm

There are different variants in this SHA algorithm depends upon size of output.

SHA is modified version of MD5.

→ The output is a message digest of 160 bits in length.

Properties :-

(i) Generating original message from digest } Infeasible properties

(ii) Finding two messages generating same digest

Working of SHA :-

(i) Padding : [64 bit less than exact multiple of 512] } exactly same as MD5

(ii) Appending length

(iii) Divide input into 512 bit blocks

(iv) Five chaining variables (A, B, C, D, E)

(v) Process Blocks → copy of chaining variables

(vi) → Divide 512 bit into 16 sub blocks of 32 bit

→ Four rounds (20 steps of each round)

Mathematical Equation :-

$$abcde = (e + \text{Process } P + S^5(a) + W[t] + K[t]),$$
$$a, S^{30}(b), c, d.$$

O/p → 128 bit → SHA-1

256 bit → SHA-256

512 bit → SHA-512

↓

512 bit hash code

$H(M) = h(512\text{-bit})$

Date ___/___/_____

Saathi

Plain Text Block size = 1024 bits

No. of Rounds / steps = 80

Each Round → Output = 64 bit

↳ generated from plain Text

Each Round → K (constant)

Each Round → Buffers = 8 buffers → Store intermediate results & output (hash code)

Each Buffer Size = 64 bits.

→ $\frac{512}{64} = 8$ (buffers)

1 → 2 → 3 → 4 → Suppose there be six (6) blocks of PT & the first block's output is the input to 2nd block, 2nd block's output is the input to 3rd block and so on.

Chain process → 1 → 2 → 3 ↓ 4 ← 5 ← 6 ↓ Hash Code

Output of 6th block is hash code

Steps :-

(1) Pad the bits 100 ... so that length of plain text is 128 Multiple of 1024 bits

(2) Append [128 bit] Representation of original plain Text such that length = Multiple of 1024 bits

(3) Initialize the Buffers (a, b, c, d, e, f, g, h) 64bit in Hexa-Decimal.

(4) Process each block of plain text in 80 rounds/steps

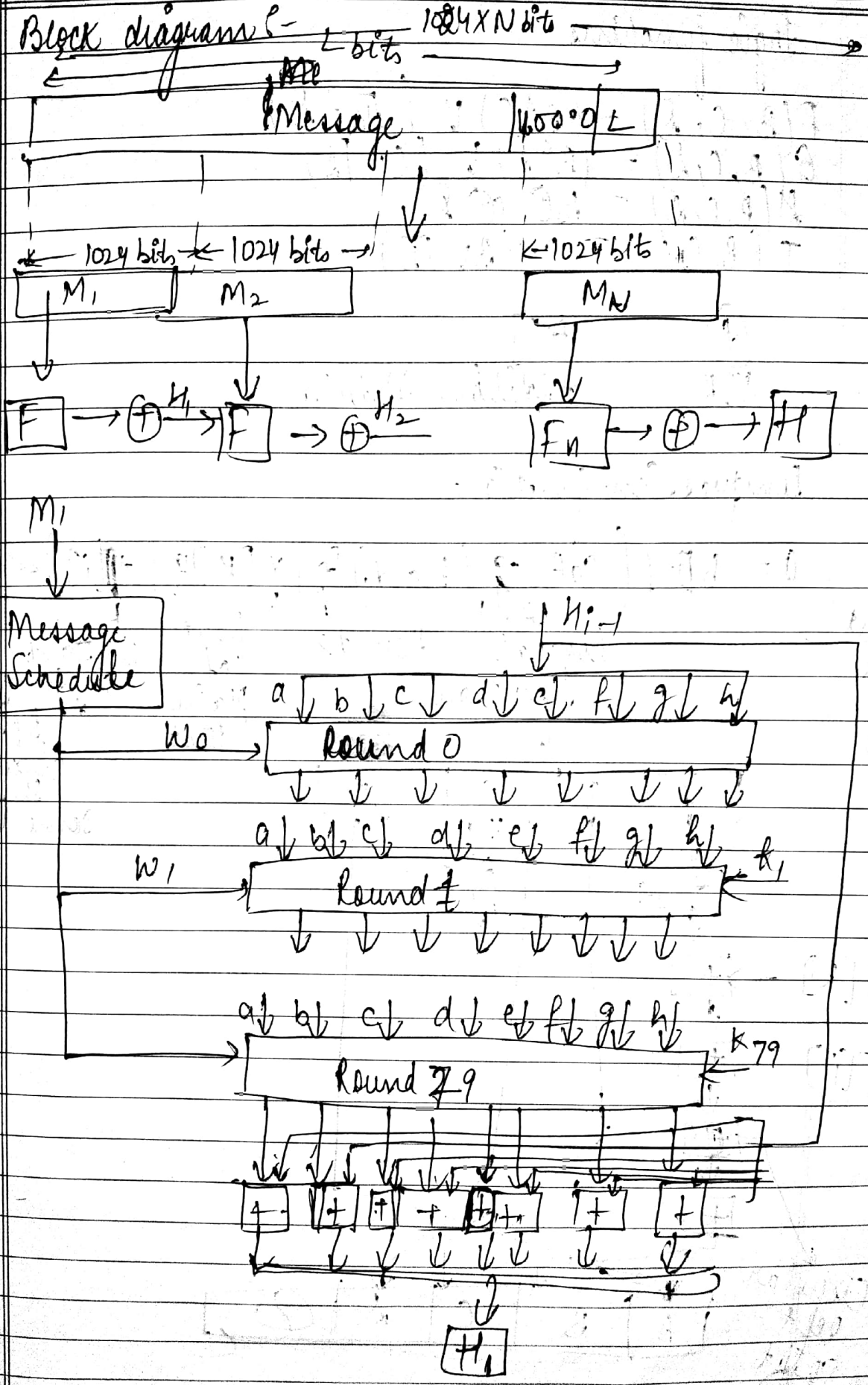
(5) Output in Buffers is hash code (512)

Page No.

Date __/__/____

Saathi

Block diagram :-



Saathi

Date __/__/____

Logic functions

$F(B, C, D) = (B \wedge C) \vee (\neg B \wedge D)$
$G(B, C, D) = (B \wedge D) \vee (C \wedge \neg D)$
$H(B, C, D) = B \oplus C \oplus D$
$I(B, C, D) = C \oplus (B \vee \neg D)$

$\oplus$ XOR $\boxplus$ Addition Modulo

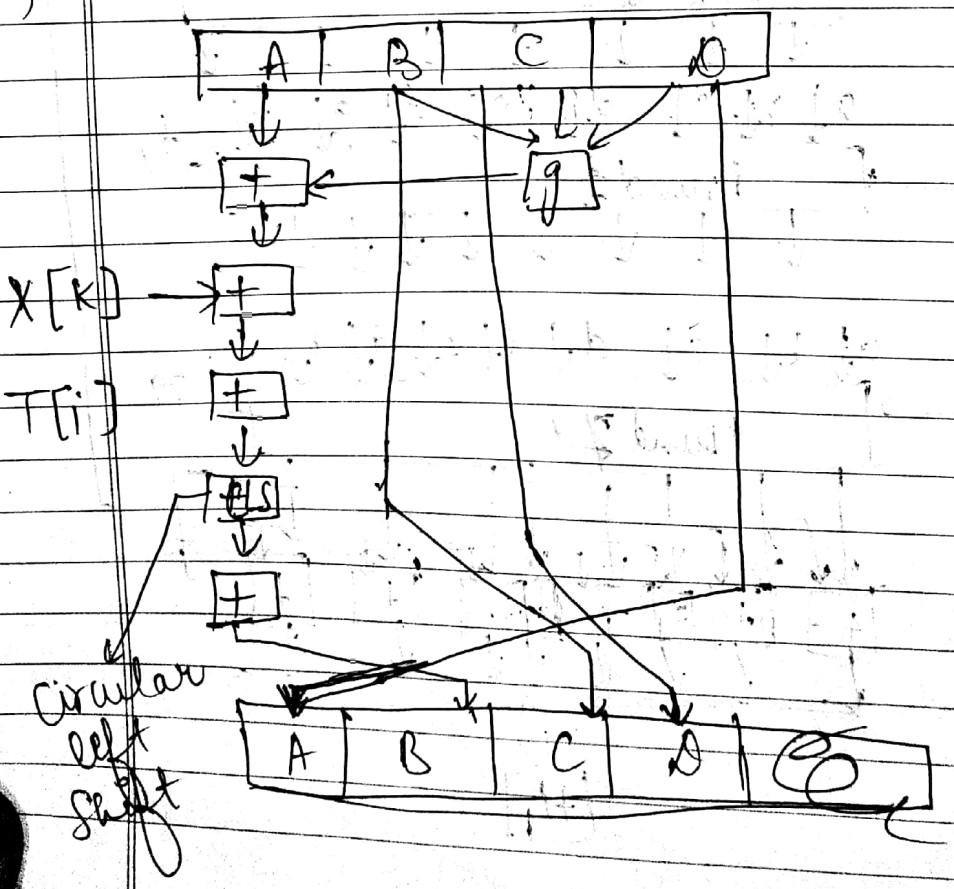
Compression function

$a = b \boxplus (CA \boxplus g(b, c, d) \boxplus X[K] \boxplus T[i]) \lll s$

- g: logical function
- (b, c, d): Round 2
- $X[K]$: part of plain text
- $T[i]$: constant
- $\lll s$: left circular shift of some bits

Output

(V)



Page No.

Date __/__/____

INFORMATION SECURITY

Part IV System
Chapter :- ~~Network~~ Security

System Security :- Security of a computer system is a process of ensuring confidentiality & Integrity of the operating system.
A system is said to be secure if its resources are used and accessed as intended under all the circumstances, but no system can guarantee absolute security from several of various malicious threats and unauthorized access.

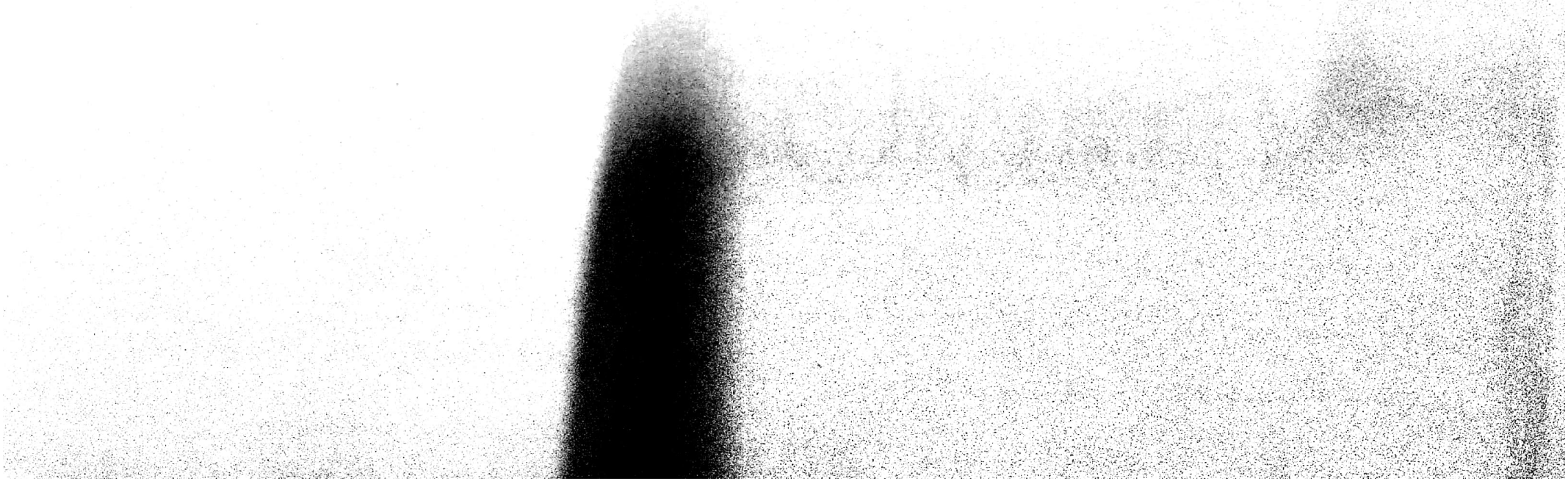
Security System can be threatened via two violations

Threat
(Program causing serious damage to OS)

Attack
(Attempt to break security and make unauthorized use of an asset).

System Security :-

It is defined as various methodologies that help in keeping confidential info safe. It protects info from theft, corruption and other damages.



Date __/__/____

~~Unauthorized~~

System Security Types

- Intruder
- Malicious software
- Virus (counter Measures)
- Firewall

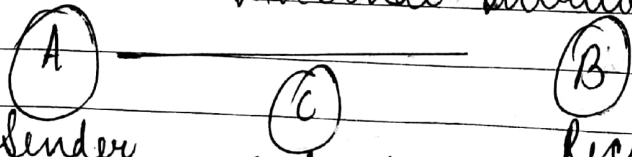
Intruders :- (Hacker / Cracker)
A person trying to gain unauthorized access on the H/W (or systems) with a criminal intension

Types of Intruders
- Masquerader
- Misfeasor
- Clandestine User

~~System~~

Masquerader :- External Intruder.

Eg :-



A sends data to B. That is A must be having its login ID and password. And similarly B as well.
But intruder hacks A's info and C is sending the data to B.

An intruder who is not authorized to use the

Saathi

Date ___ / ___ / _____

Masquerader:- Internal Intruder, computer & who penetrates a system's access controls to exploit a legitimate user's account

Misfeasor:- Internal Intruder
→ More harmful than Masquerader.
→ Very difficult to identify

A legitimate user who accesses data, programs and other resources for which such access is not authorized and
who is authorized for such access, he misuses it.
Eg:- An employee working for a company leaks information about the company outside it.

Clandestine User:- Try to steal & use the credentials of their supervisor.

An individual who seizes supervisory control of system & misuses the control for audit collection.

Date ___/___/___

Saath

Intrusion :- Unauthorized access by intruder

(IDS) Intrusion Detection Systems :-
→ To identify intrusions IDS is used.
→ It monitors the systems / Networks for any unauthorized access.
→ It alerts the admin on detection of any unauthorized activity.

Types
- Host based IDS
- Network based IDS
- Application based IDS

Approaches to Intrusion Detection :-
- Statistical Anomaly Detection
- Rule Based Detection

Statistical Anomaly Detection :-
→ Involves the collection of data relating to behaviour of legitimate users over a time period
→ Statistical tests are applied to observe behaviour to determine whether that is not legitimate user behaviour
  - Threshold Detection
  - Profile based

Page No.

Saathi

Date __/__/____

Rule Based Detection:-

→ Define a set of rules or attack patterns used to decide given behaviour.

(a) Anomaly Detection
(b) Penetration Identification

Malicious Softwares:-

→ A software that is intentionally included or inserted in a system for harmful purpose.

→ Mostly programs / codes causes damage to system.

Malware is a short form for "Malicious Software"

↓

General term for covering all kinds of threats to your computer safety.

Eg: Virus, Spyware, Worms, trojans, horses etc

↓

Damage computer without user consent.

→ These softwares are not developed by their own. They are created and developed by developer / hacker to destroy computer programs

Functions of Malicious Softwares

→ Stealing data
→ Encrypting / Deleting sensitive data
→ Altering or hijacking core computing
→ Monitoring user's computer activity without their permission.

Saath

Date __/__/____

Types of Malware Attacks
- Adware
- Trojan
- Worms
- Viruses
- Spyware
- Ransomware
- Backdoor
- Logic Bomb
- Zombie

Virus :- Vital Info Resource Under Seize

→ Program / code that attaches itself to the application & runs whenever that app is run

→ To modify the program functionality

Eg :- A virus opens Windows media player, it detects the files.
- Text files
- Image files
- Video / audio files

Non-living Virus — Computer / laptop / Mobiles
Living Virus - Human Beings

Phases of Virus
- Dormant phase
- Propagation
- Triggering
- Execution

Types of Virus
- Parasitic
- Memory Resident
- Boot Sector
- Stealth
- Polymorphic
- Metamorphic

Chapter :-
Web Security

Web Security :- Web security is also known as "Cyber Security" which involves protecting website or web application by detecting, preventing and responding to attacks.

Web security Requirements

→ Authentication :- Accepting credentials from the entity and validating them against an authority

→ Authorization :- Determines if service requester is entitled to perform the operation, which can range invoking the web service to executing a certain part of its functionality.

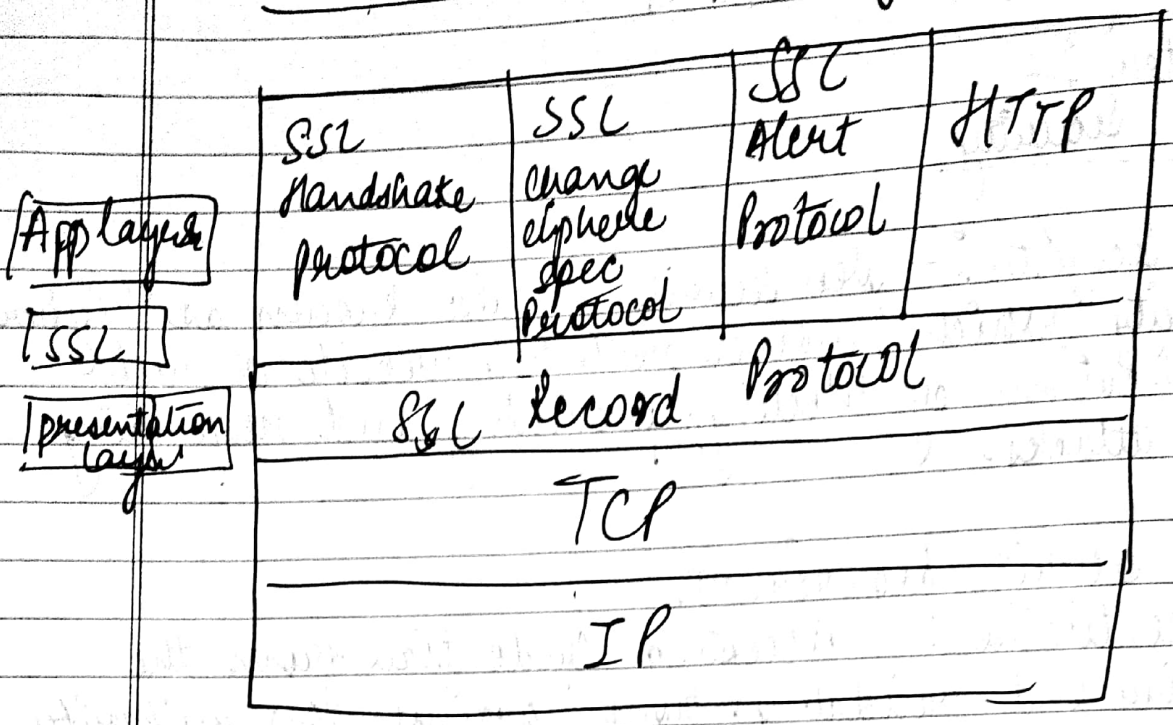
→ Data Protection :- Ensures the request & response have not been tampered with or re-route. It requires securing both data integrity & privacy.

→ Non Repudiation :- Guarantees that the message sender is the same as the creator of the msg.

Saathi

Date __/__/____

SSL - Secure Socket layer



Uses:-

→ Providing security to two entities transferring data through web browser and web server.

→ If client - server communication needs to be secure, the SSL is used in that case.

Type of Security ← Integrity (no. modification in data)
Authentication (Authenticated entities)
Confidentiality (authorized user)

→ If sender ~~needs~~ wants to transfer data to receiver's side, But from application layer the data is not going to transfer directly Firstly it is given to SSL.

Saathi

Date __/__/____

The SSL firstly encrypts the data by using some kind of encryption algo. like DES, Triple DES.
It then attaches the header of the SSL layer to the encrypted data i.e SSL header. And packet is sent to reciever.
After reaching at reciever's end, firstly SSL header is removed. And then encrypted data is decrypted by using same algo. and then original msg is sent to application layer of reciever.

Protocols

SSL Handshake protocol :- Connection establishment, authentication of entities

SSL Record protocol :- Confidentiality, Integrity

(Backbone protocols)

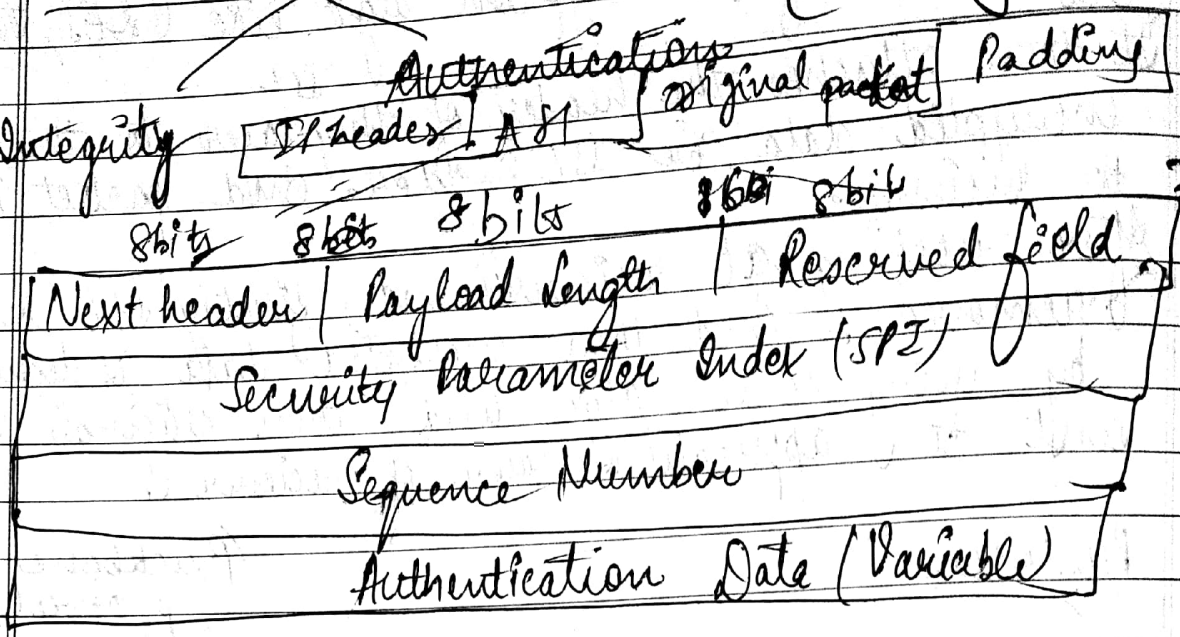
SSL change cipher spec protocol :- Consists of 1 msg, of 1 byte consists of value 1.
[pending state to be get copied into running or current state]

SSL Alert protocol :- Warning, Alert Msg, Error Msg.

Date __/__/____

Authentication Header (AH)

Integrity — Authentication — nothing encrypting



Next header → Type of header which is imidiately next to this header → foll". this header

Payload length → Original data length

Reserved → Used for further Extensions

SPI → Identify particular security association of perticular packet.

Seq No:- Range - $(0 - 2^{32}-1)$

- Increment counter on sending of packets.

Max value - 2^{32}

Dual Role

Authentication data → contains Integrity Check Value (ICV)

Variable length field that tells whether the data reaches to Reciever is modified or not.

Undesired Modifications are made to data or not

Page No.

Date ___/___/___

Saathi

Information Security

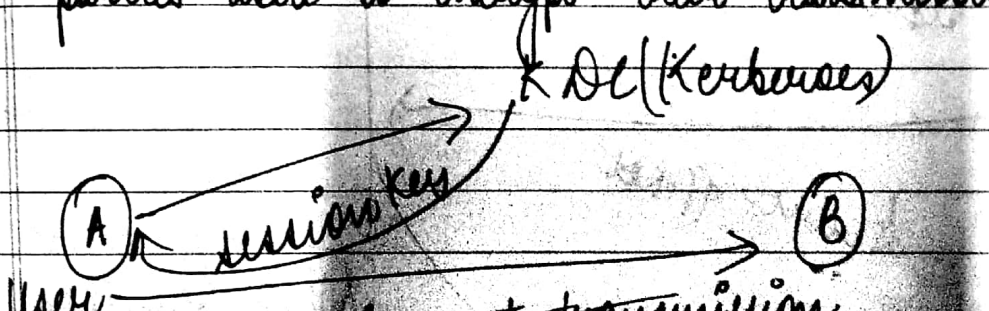
Kerberos

It is a computer n/w authentication protocol which works on basis of tickets to allow nodes communicate over a non-secure n/w to prove their identity to one another in a secure manner.

→ Client-Server Model
→ Symmetric key Model
→ Requires a trusted third party / KDC (contains database of secret keys)

KDC
- Authentication Server (AS)
- Ticket granting Server (TGS)

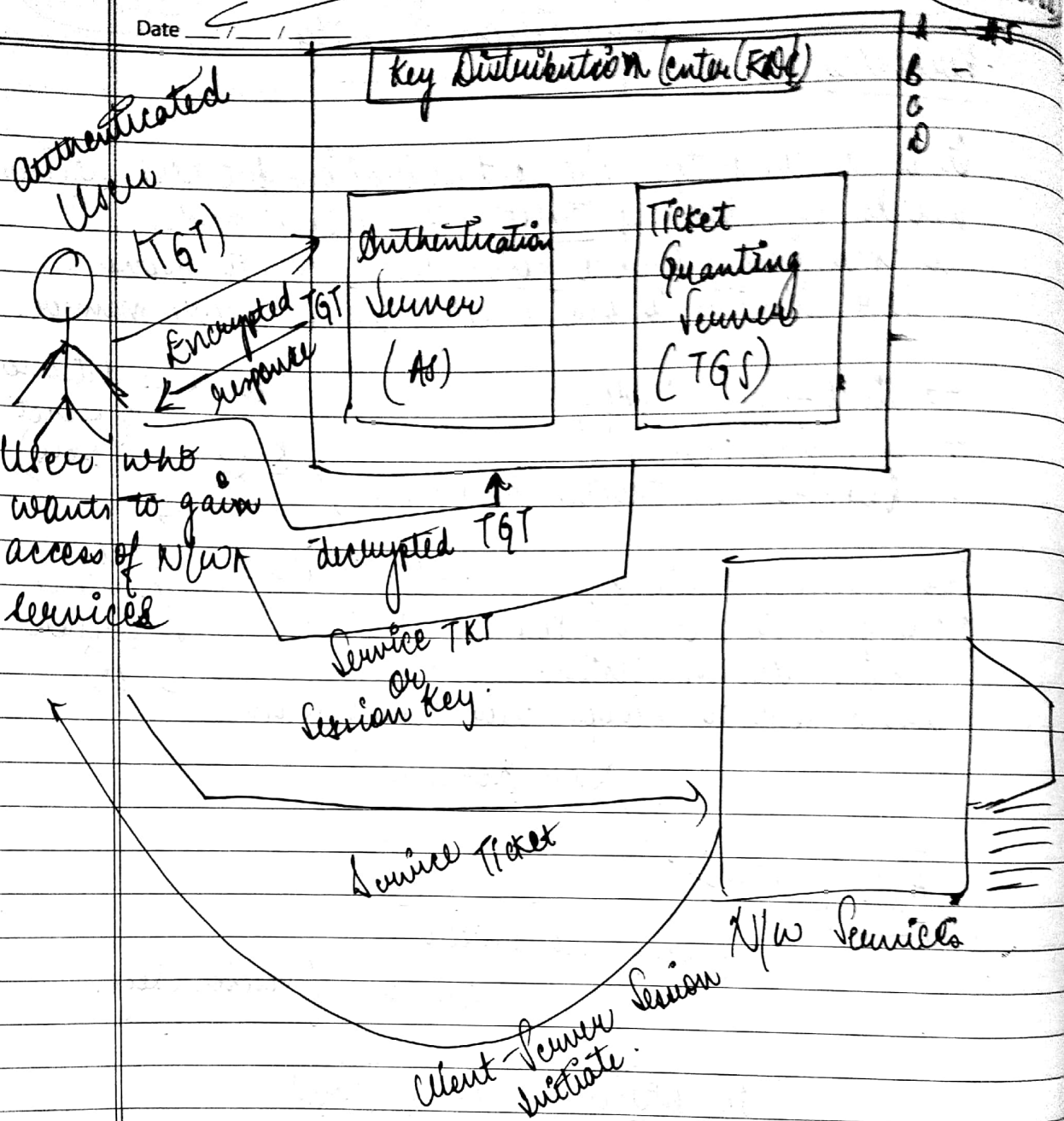
For a communication, KDC generates a session key in which communication parties used to encrypt their transmission



Key Distribution Center (KDC)

Kerberos 4

Date __/__/____



~~To make encryption~~ The user can be anywhere. User make use of a normal internet which is a non-secure channel. So to make encryption of the user to n/w services, Kerberos is used.

Before user gets access to this n/w services, the user need to have one ticket granting ok. That

(saathi)

Date __/__/____

ticket should be present to N/w services it should be authenticated to it. That is authenticated by the third party ie KDC.
Once N/w service recieves ticket from that user which is authenticated by KDC, the network service will provide access to this user.

KDC has database of keys of users.

User demanding Ticket from Ticket granting Server.

Authentication Server will send back a response in the form of TGT ticket granting Ticket and ask the user to decrypt it.

User again sends decrypted TGT to KDC after correct decryption, the KDC will provide a Service Ticket to User.
User will sent service ticket to N/w Server.
After that client-Server session initiate