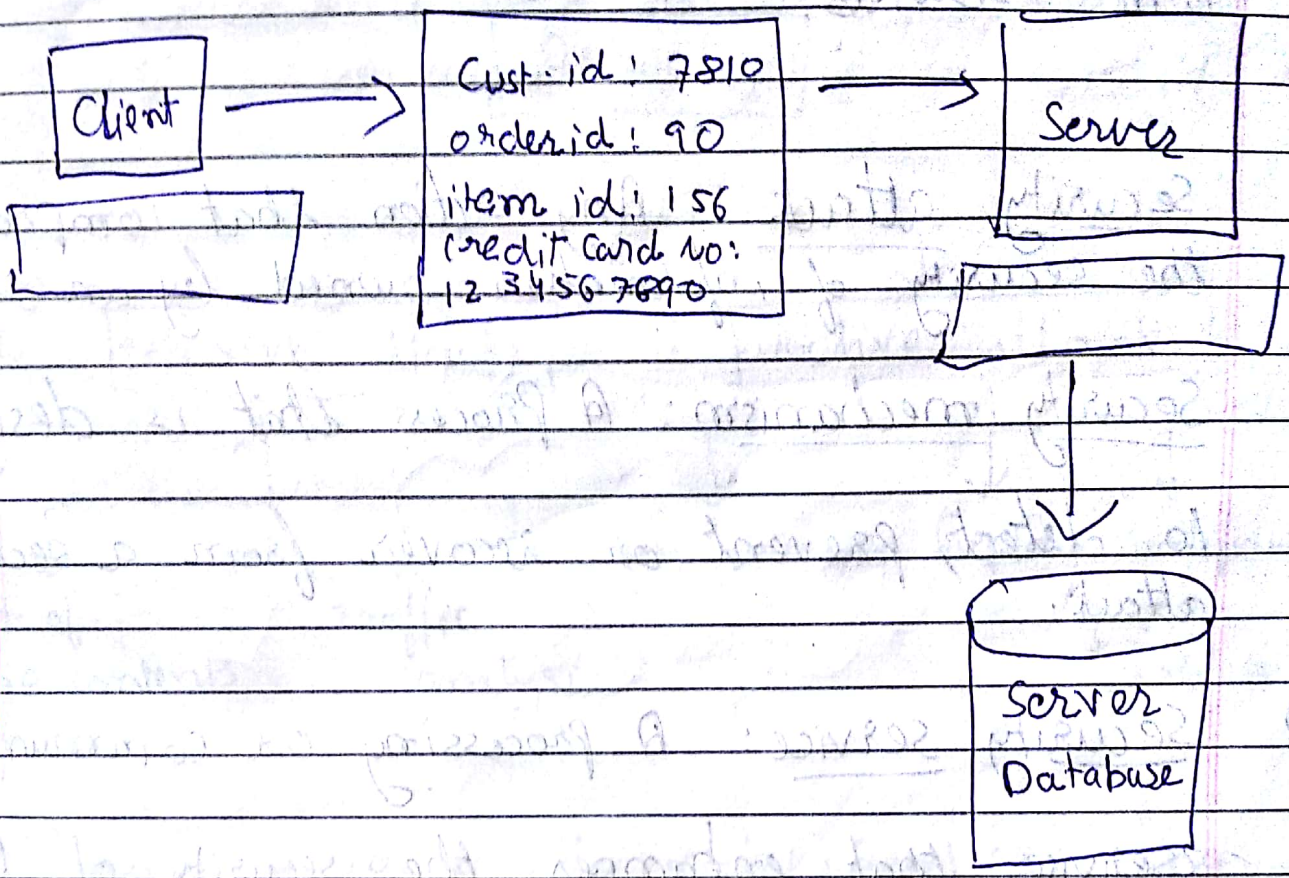
Need for Security:



Modern Nature of Attacks

(1) Automating attacks
(2) Privacy concerns
(3) Distance does not matter

Security Models

(1) No security (2) security through obscurity
(3) Host security (4) N/w security.

Scanned by CamScanner

Date : ...../...../.....

Page : .....

The OSI Security Architecture

- It focuses on security attacks, mechanisms and services.

Security attack : Any action that compromises the security of information owned by an organiz

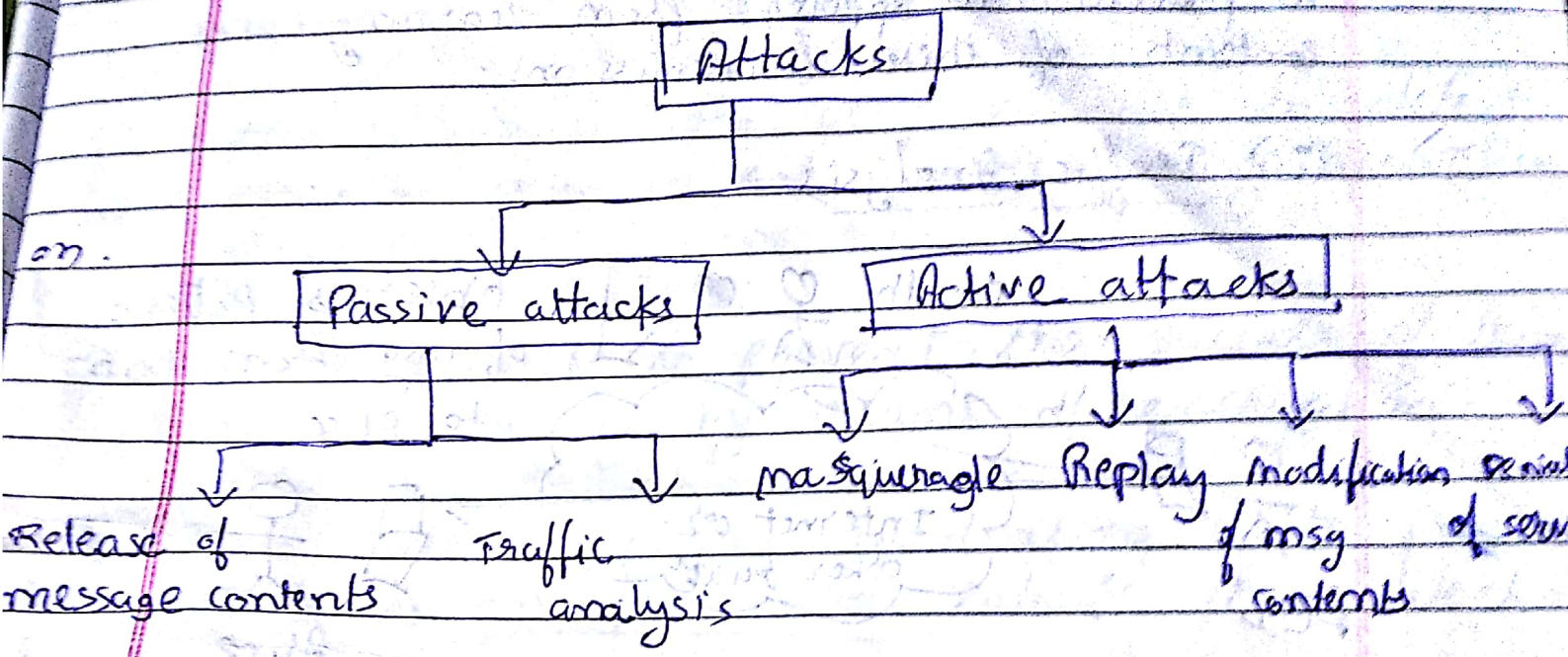
Security mechanism : A process that is designed to detect, prevent or recover from a security attack.

Security service : A processing or communicati service that enhances the security of the data processing systems and the information transfers of the organization.

The services are intended to counter security attacks, and they make use of one or mo security mechanisms to provide the service.

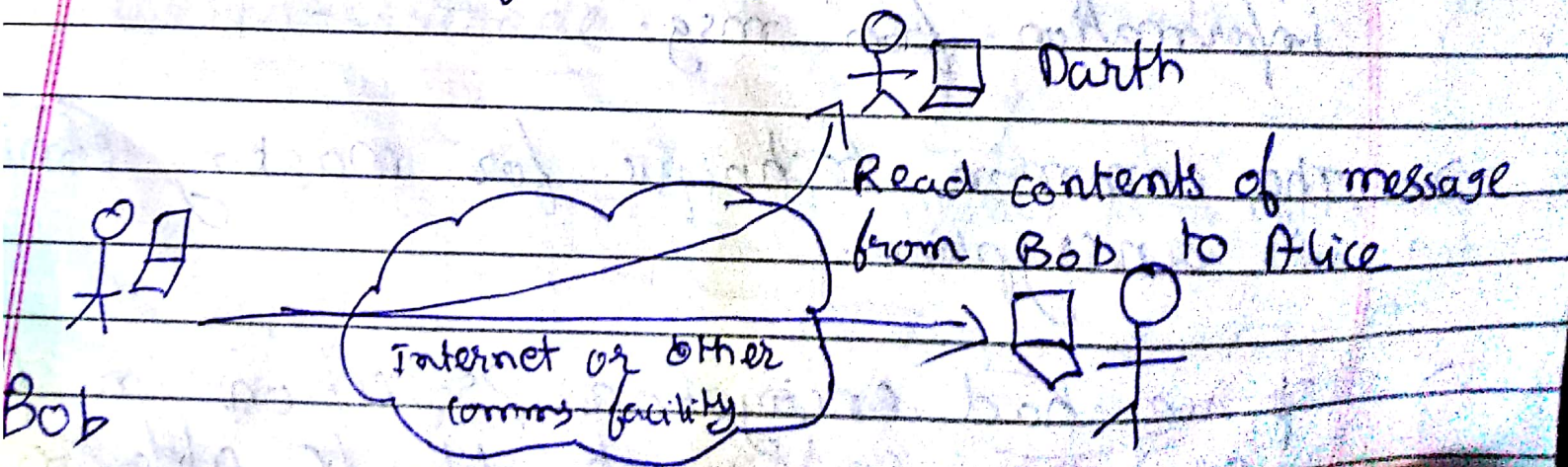
Scanned by CamScanner

* Security Attacks



→ Passive Attacks do not involve any modification to the contents of an original message

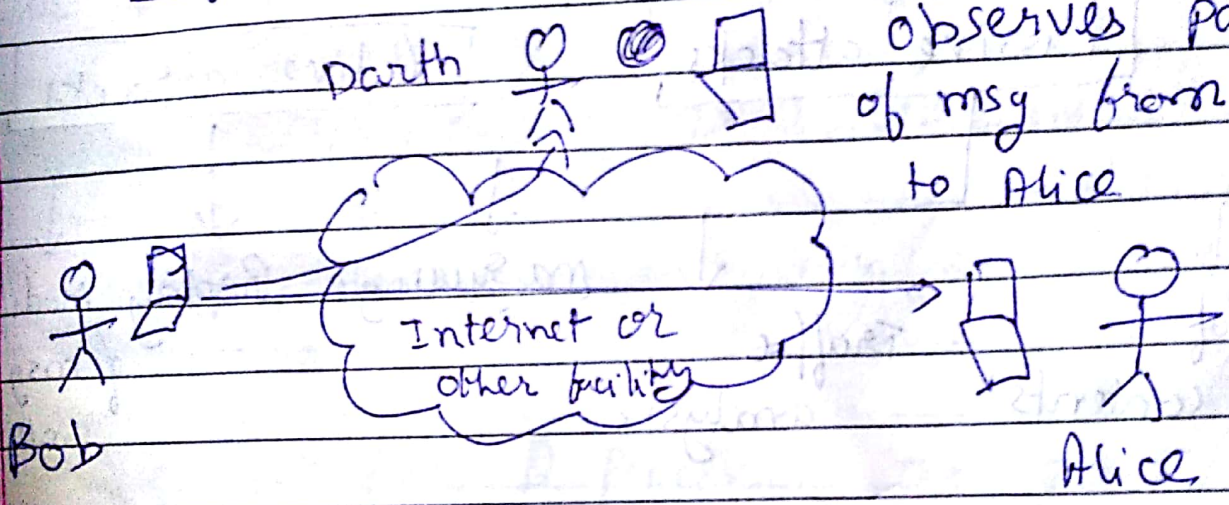
(1) Release of message content



Scanned by CamScanner

→ A telephone conversation, an e-mail, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.

→ (2) Traffic Analysis



→ Suppose that we had a way of masking the contents of messages or other informa traffic so that opponents, even if they captured the message, could not extract t information from msg.

⇒ The common technique for masking conten is encryption.

⇒ If we had encryption protection in plac an opponent might still be able to observe the pattern of these messages.

Scanned by CamScanner

→ The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged.

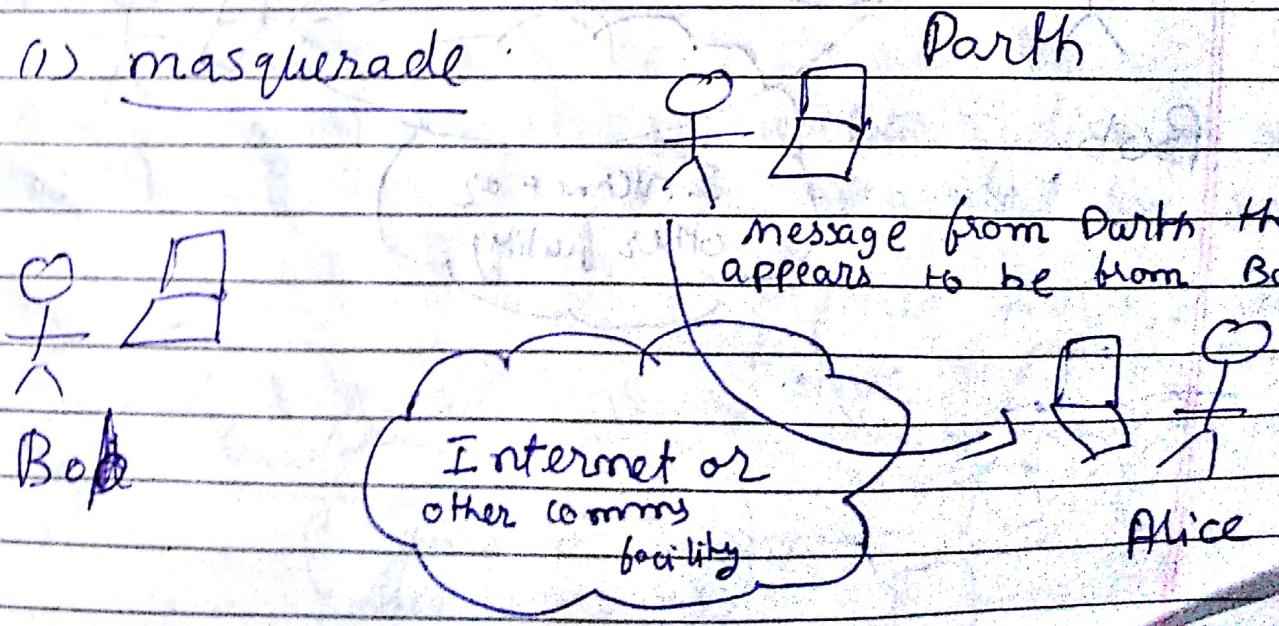
→ Passive attacks are very difficult to detect because they do not involve any alteration of data.

→ It is feasible to prevent the success of these attacks, usually by means of encryption.

→ Thus, the emphasis in dealing with passive attacks is on prevention rather than detection.

→ Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories:

(1) masquerade



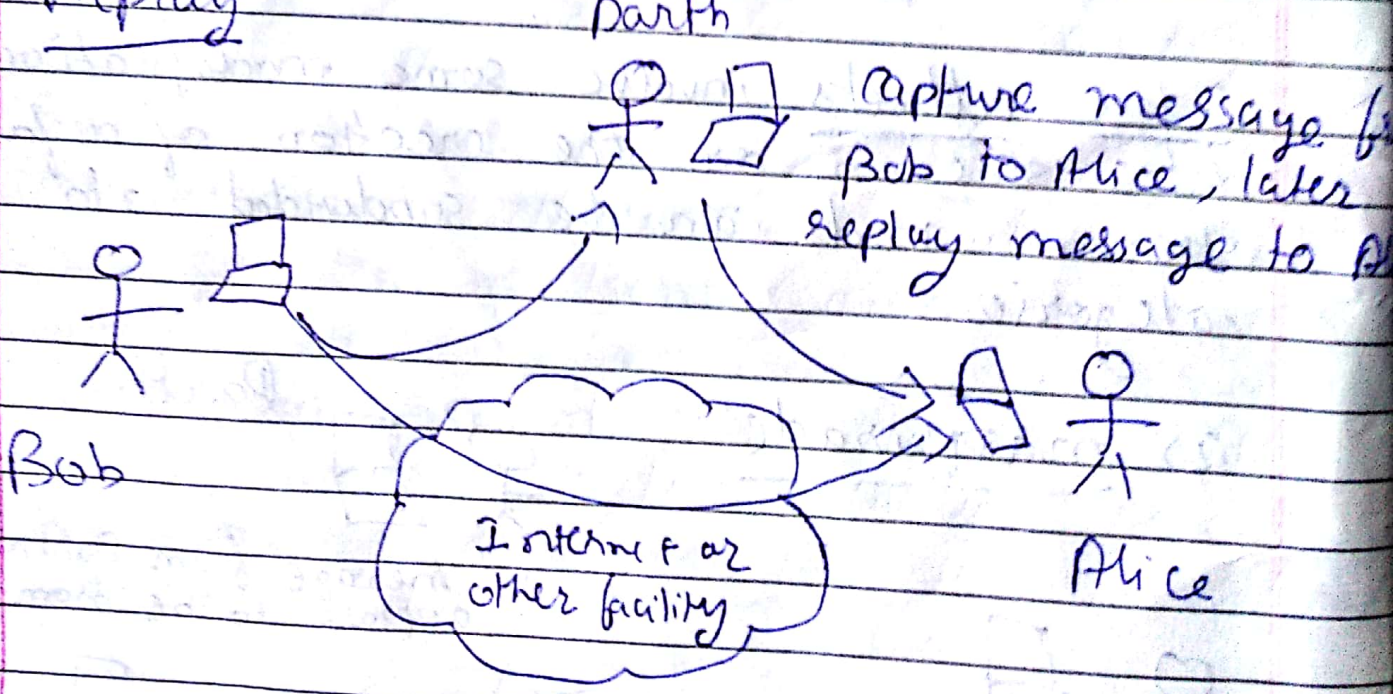
Scanned by CamScanner

→ A masquerade takes place when one entity pretends to be a different entity

→ A masquerade attacks usually includes one of the other forms of active attack.

→ For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonation an entity that has those privileges.

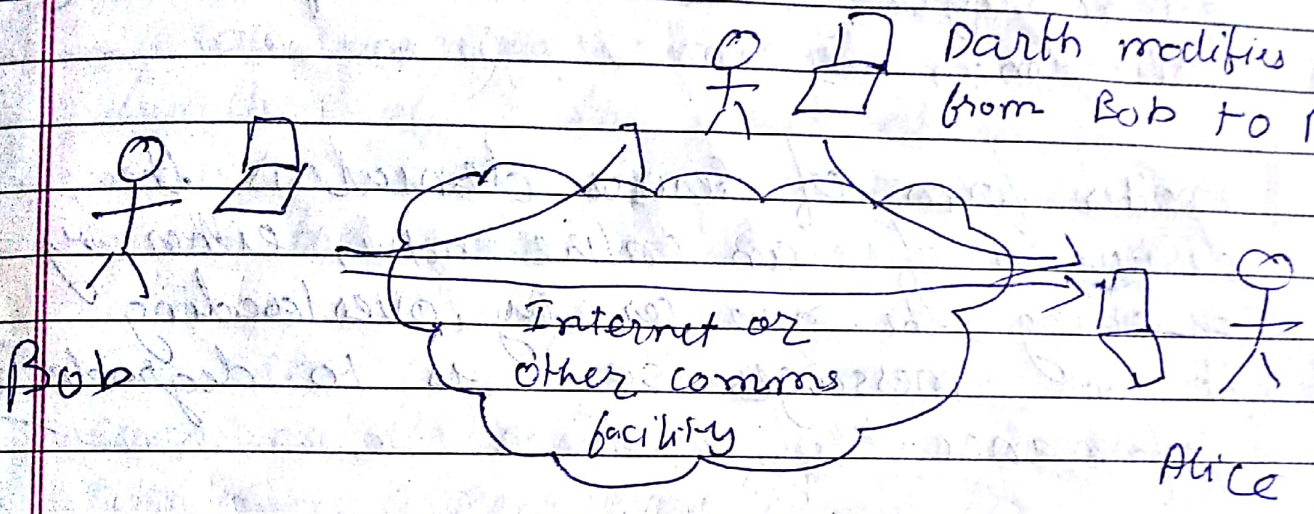
(2) Replay



Scanned by CamScanner

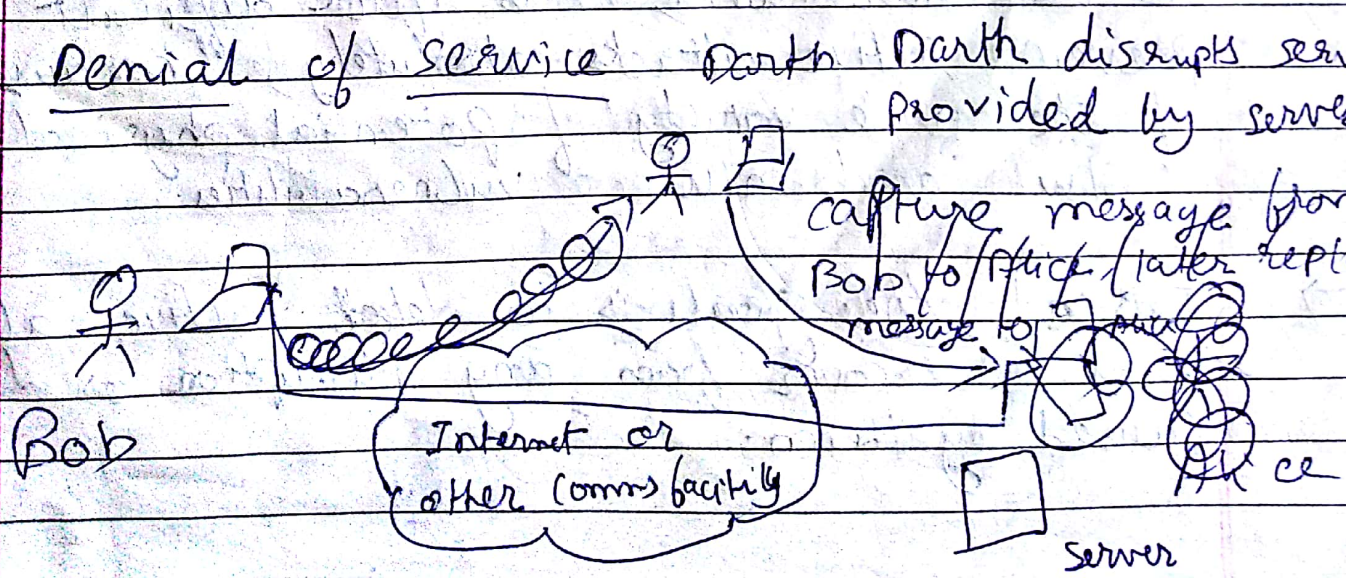
→ It involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

(2) Modification of messages



→ It simply means that some portion of a legitimate message is altered, or that message are delayed or reordered, to produce an unauthorized effect.

(3) Denial of service



Scanned by CamScanner

It prevents or inhibits the normal use or management of communications facilities.

This attack may have a specific target, for example, an entity may suppress all messages directed to a particular destination.

Another form of service denial is the disruption of an entire n/w, either by disabling the n/w or by overloading it with messages so as to degrade performance.

Active attacks present the opposite characteristics of passive attacks.

whereas passive attacks are difficult to detect, measures are available to prevent their success.

On the other hand, it is quite difficult to prevent active attacks absolutely, because of the wide variety of potential physical, S/w and n/w vulnerabilities.

Instead, the goal is to detect active attacks and to recover from any disruption or delays caused by them.

Scanned by CamScanner

* Security Services

(1) Authentication :- The assurance that the communicating entity is the one that it claims to be.

→ In the case of a single message, such as a warning or alarm signal, the function of the authentication service is to assure the recipient that the message is from the source that it claims to be from.

→ In the case of an ongoing interaction, such as the connection of a terminal to a host, two aspects are involved.

→ First, at the time of connection initiation, the service assures that the two entities are authentic, that is, that each is the entity that it claims to be.

→ Second, the service must assure that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties for the purpose of unauthorized transmission or reception.

Scanned by CamScanner

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

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

(c) Access control :- The prevention of unauthorized use of a resource. i.e this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resources are allowed to do.

→ To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.

(3) Data Confidentiality :

Scanned by CamScanner

→ Confidentiality is the protection of transmitted data from passive attacks.

→ (1) Connection Confidentiality
(2) Connectionless Confidentiality
(3) Selective - Field Confidentiality
(4) Traffic Flow Confidentiality

(3) Data Integrity : The assurance that data received are exactly as sent by an authorized entity (i.e contain no modification insertion, deletion, or replay).

(a) Connection Integrity with Recovery
(b) Connection Integrity without Recovery
(c) Selective - Field Connection Integrity
(d) Connectionless Integrity
(e) Selective - Field Connectionless Integrity

(4) Non - Repudiation :- It prevents either sender or receiver from denying a transmitted message.

(a) Nonrepudiation, Origin
(b) Nonrepudiation, Destination

Scanned by CamScanner

(5) Availability service :- Both X.800 and RFC 2828 define availability to be the property of a system or a system resource being accessible and usable upon demand by an authorized system according to performance specifications for the system.

→ A variety of attacks can result in the loss or reduction in availability.

* Security Mechanisms

Specific security mechanisms

(a) Encipherment :- the use of mathematical algorithms to transform data into a form that is not readily intelligible.

→ The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.

(b) Digital Signature :- Data appended to or

Scanned by CamScanner

cryptographic transformation of a data unit that allows a recipient of the data unit to provide the source and integrity of the data unit and protect against forgery (e.g. by the recipient).

by,

(c) Access Control : A variety of mechanisms that enforce access rights to resources.

(d) Data Integrity : A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

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

(f) Traffic Padding : The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

(g) Routing Control : Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.

Scanned by CamScanner

(h) Notarization : The use of a trusted third party to assure certain properties of a data exchange.

Pervasive Security Mechanisms

(a) Trusted Functionality

-> That which is perceived to be correct with respect to some criteria.

(b) Security Label

-> The marking bound to a resource that names or designates the security attributes of that resource.

(c) Event Detection

-> Detection of security relevant events

(d) Security - Audit Trail

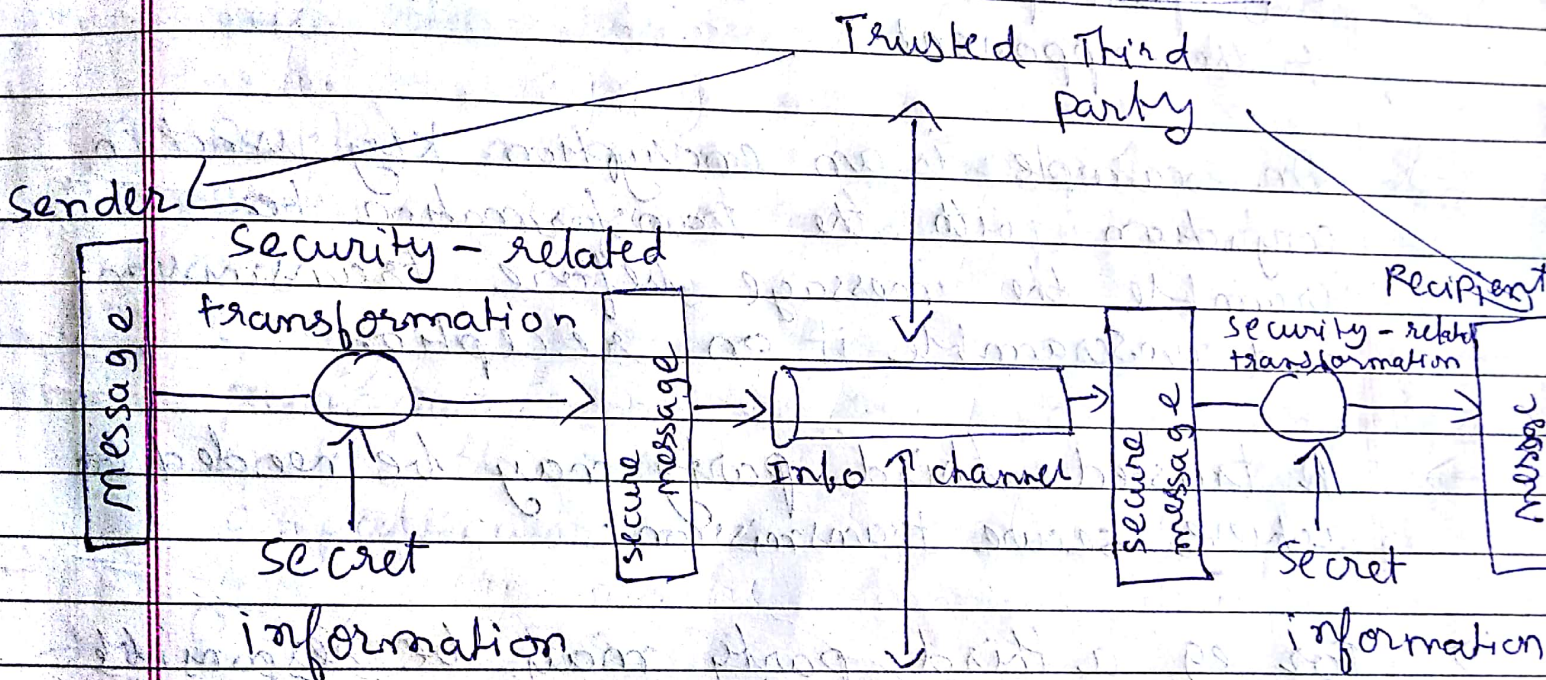
-> Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.

Scanned by CamScanner

(e) Security Recovery:

→ Deals with requests from mechanisms, such as event handling and management functions and takes recovery actions.

* A model For Network Security



→ All the techniques for providing security have two components.

(a) A security - related transformation on the information to be sent.

Scanned by CamScanner

→ Examples include the encryption of message, which scrambles the message so that it is unreadable by the opponent and the addition of a code based on the contents of the message, which can be used to verify the identity of sender.

(b) Some secret information shared by the two principals and, it is hoped, unknown to the opponent.

→ An example is an encryption key used in conjuction with the transformation to scramble the message before transmission and unscramble it on reception.

→ A trusted third party may be needed to achieve secure transmission.

→ For eg, a third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent.

→ Or a third party may be needed to arbitrate disputes between the two principals concerning the authenticity of a message transmission.

Scanned by CamScanner

Page :

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

1) Design an algorithm for performing the security - related transformation. The algo should be such that an opponent cannot defeat its purpose.

2) Generate the secret information to be used with the algorithm.

3) Develop methods for the distribution and sharing of the secret information.

4) Specify a protocol to be used by the two principals that makes use of security algo and the secret information to achieve a particular security service.

-> Programs can pre

Scanned by CamScanner

Page : .....

Vulnerability: It is a weakness in the security system

Threat: It is a potential cause of an incident, that may result in harm systems and organization.

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

Scanned by CamScanner

Date : ..../..../.....

Page : .....

* Symmetric Cipher Model

1) Plaintext : This is the original intelligible message or data that is fed into the algo as input.

2) Encryption algo : The encryption algorithm performs various substitutions and transformations on the plaintext.

3) Secret key : They key is a value independent of the plaintext and of algorithm which is also input to the encryption algorithm.

4) Ciphertext : When a plaintext is codified using any suitable scheme, the resulting message is called as cipher text.

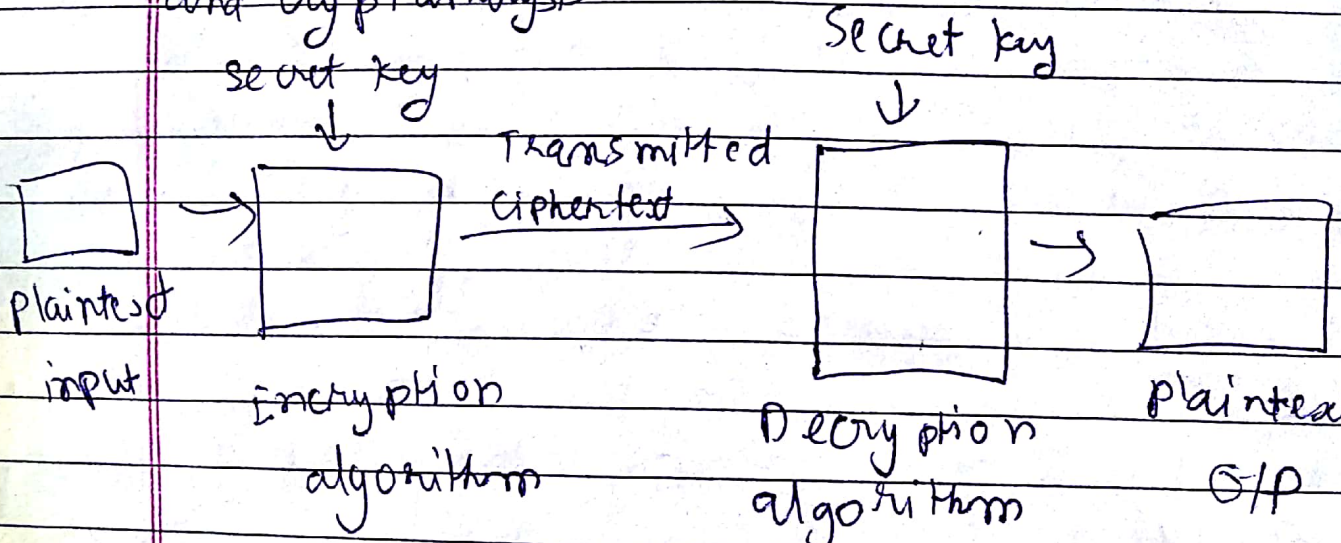
5) Decryption algorithm : This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

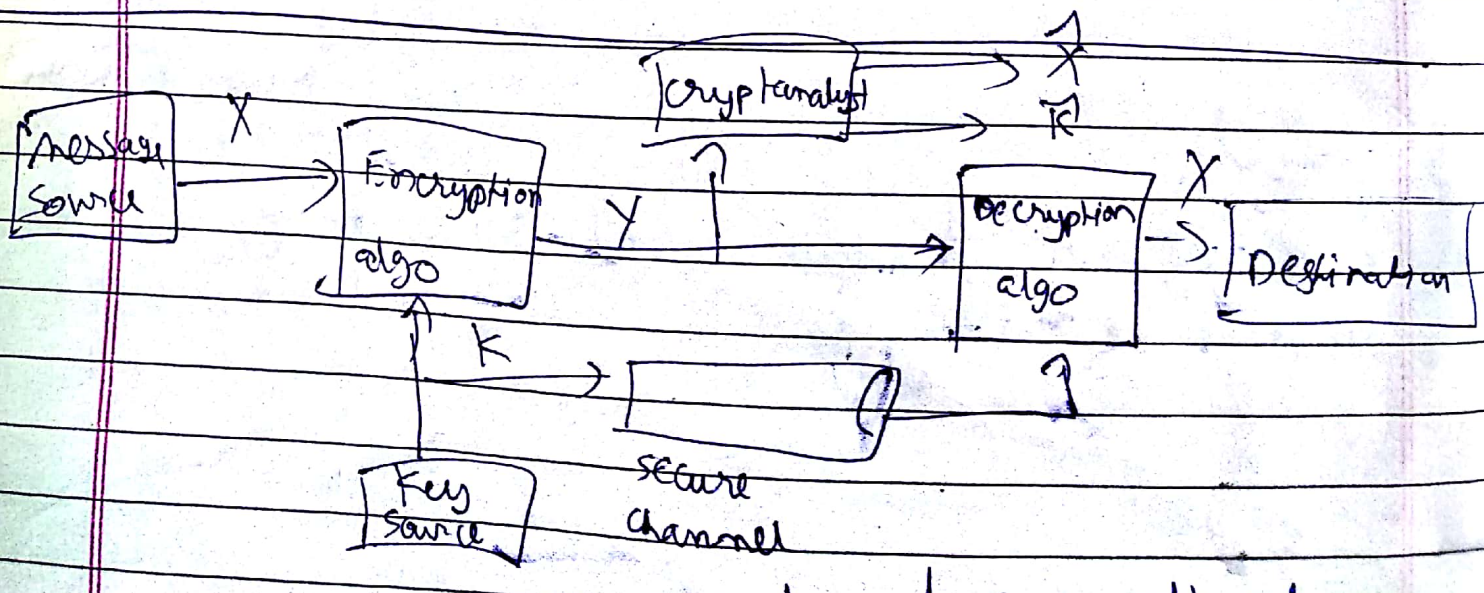
Scanned by CamScanner

→ Cryptography is the art and science of achieving security by encoding messages to make them non-readable.

→ Cryptanalysis is the technique of decoding messages from a non-readable format back to readable format without knowing how they were initially converted from readable format to non-readable format.

→ Cryptology is a combination of cryptography and cryptanalysis.





model of Conventional Cryptosystem

Scanned by CamScanner

Where K = key, Y = Ciphertext, X = Plaintext

$Y = E(K, X)$ → Encryption

$X = D(K, Y)$ → Decryption.

→ Cryptographic systems are characterized along three independent dimensions:

(1) The type of operation used for transforming plaintext to ciphertext.

Eg: Substitution, transposition.

(2) The no. of keys used: If both sender and receiver use the same key, the system is referred to as symmetric, single-key, secret key or conventional encryption. Otherwise it is called Asymmetric key encryption.

(3) The way in which the plaintext is processe

→ A block cipher processes the input one block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing o/p one element at a time, as it goes along.

Scanned by CamScanner

Date : / /

Page :

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

Types of Attacks on Encrypted Messages

Type of Attack	Known to Cryptanalyst
1) Ciphertext only	• Encryption algo • Ciphertext
2) Known plaintext	• Encryption algo, • Ciphertext • one or more plaintext - ciphertext pairs formed with the secret key
3) Chosen plaintext	• Encryption algo • ciphertext • Plaintext message chosen by cryptanalyst together with its corresponding ciphertext generated with secret key.
4) Chosen ciphertext	• Encryption algo • Ciphertext • Purposed ciphertext chosen by cryptanalyst

Scanned by CamScanner

	together with its corresponding decrypted plaintext generated with the secret key.
5) chosen text	• Encryption algorithm • ciphertext • plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with secret key. • purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key.
6)	

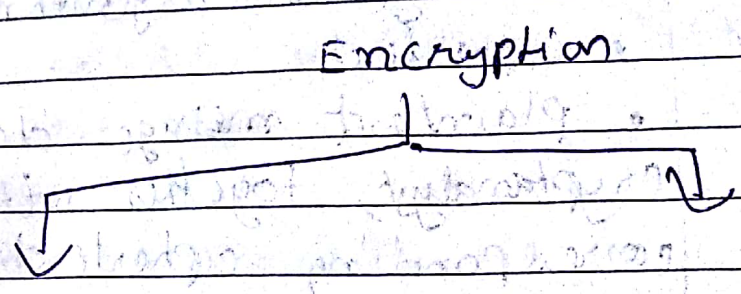
Unconditionally Secure : if the ciphertext generated by the scheme does not contain enough information to determine uniquely the corresponding plaintext, no matter how much ciphertext is available.

- The cost of breaking the cipher exceeds the value of the encrypted information.
- The time required to break the cipher exceeds the useful lifetime of the information.

Scanned by CamScanner

* Computationally secure: If either of the foregoing two criteria are met.

→



1) Caesar Cipher: Proposed by Julius Caesar. It was the first example of substitution cipher.

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

L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Scanned by CamScanner

Plain : Meet me after the Lecture

Ciphertext : P hhw P M D I WHV WKV Oh fwxvh

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

↓

so that substitution alphabet does not exceed 25.

$$p = D(k, C) = (c - 3) \bmod 26$$

→ A shift may be of any amount, so that general caesar algorithm is

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

$$p = D(k, C) = (c - k) \bmod 26$$

→ Disadvantage : Brute-force cryptanalysis is easily performed. Simply try all the 25 possible keys

→ The encryption and decryption algo are known

→ The language is easily recognizable (English alphabet)

Scanned by CamScanner

Monoalphabetic cipher Eg: a→d, b→e, c→f, ..., h→s ..... Date: ... Page: ...

* Monoalphabetic Cipher

→ With only 25 possible keys, the Caesar cipher is far from secure.

→ Increase in the key space can be achieved by allowing an arbitrary substitution.

→ If, instead the "cipher" line can be any permutation of the 26 alphabetic characters, then there are 26!

→ Eliminate brute-force attack.

→ Such an approach is referred to as a monoalphabetic substitution cipher, because a single cipher alphabet is used per message.

→ Disadvantage:

→ Relative frequency of the letters can be determined and compared to a standard frequency distribution for English,

→ If the message were long enough, this technique alone might be sufficient, but because this is a relatively short message, we cannot expect an exact match.

Scanned by CamScanner

P - 13.33, Z - 11.67, S - 8.33 etc.

-> As a result monoalphabetic ciphers are easy to break because they reflect the frequency data of original alphabet.

-> A countermeasure is to provide multiple substitutes, known as homophones, for a single letter.

Playfair Cipher

-> The best-known multiple-letter encryption cipher is the Playfair, which treats digrams in the plaintext as single units and translates these units into ciphertext digrams.

-> The Playfair algorithm is based on the use of a 5 x 5 matrix of letters constructed using a keyword.

Keyword is 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

Scanned by CamScanner

Rules

Plaintext is encrypted two letters at a time according to the following rules:

1) Repeating plaintext letters that are in the same pair are seperated with a filler letter, such as x,

Example ba lx lo on

you can use alphabet as filler as least frequency as O is more

2) Two plaintext letters that fall in the same row of matrix are each replaced by the letter to the right, with the first element of the row circularly following the last.

Eg AR is encryted RM

3) Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last. For example MU is encrypted as CM.

Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter.

Ex: H ur NF

Scanned by CamScanner

→ **Advantage :** There are 26 x 26 = 676 digrams so that identification of individual digrams is more difficult.

→ **Disadvantage :** It is easily to break because it still leaves much of the structure of the plaintext language intact. A few hundred letters of ciphertext are generally sufficient.

[has so is more]

Example :

Given PLAYFAIR EXAMPLE (keyword)

(plaintext)
MY NA ME IS
SI TA

Derived

P L A Y F	XF OL IX MK
I R E X M	KM VP
B C D G H	
K N O Q S	(ciphertext)
T U V W Z	

(matrix)

Scanned by CamScanner

* Hill Cipher: It works on multiple letters at the same time. Hence it is a type of Polygraphic substitution Cipher.

→ Developed by Lester Hill in 1929

→ For m successive plaintext letters it substitutes m ciphertext letters.

For $m = 2$

$$\begin{bmatrix} C_1 \\ C_2 \end{bmatrix} = \begin{bmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \end{bmatrix} \mod 26$$

2×2

And for $m = 3$

$$\begin{bmatrix} C_1 \\ C_2 \\ C_3 \end{bmatrix} = \begin{bmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \\ P_3 \end{bmatrix} \mod 26$$

In short,

$$C = K P \mod 26$$

Scanned by CamScanner

3 x 3

Date : ..../..../.........
Page : ....

Example

plaintext: pay more money

key: $K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$ 3 x 3

for pay we have $\begin{bmatrix} 15 \\ 0 \\ 24 \end{bmatrix}$ derived 3 x 1

by giving numbers to alphabets starting from a = 0 till z = 25

$$\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 15 \\ 0 \\ 24 \end{bmatrix} = \begin{bmatrix} 17(15) + 0(17) + 5(24) \\ 21(15) + 0 + 21(24) \\ 2(15) + 0 + 19(24) \end{bmatrix}$$

3 x 3   3 x 1

$$= \begin{bmatrix} 375 \\ 819 \\ 486 \end{bmatrix} \bmod 26 = \begin{bmatrix} 11 \\ 13 \\ 18 \end{bmatrix}$$

so substitute lns for pay

Similarly if we continue

P: pay mor emo ney

C: lns hdl ewm trw

→ For Decryption we require inverse of matrix K.

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

Note: K^{-1} of a matrix K is defined by the equation $KK^{-1} = K^{-1}K = I$, where I is the identity matrix that contains all zeroes except the main diagonal from upper left to lower right which contains 1.

→ Inverse does not exist if $KK^{-1} \neq I$.

Advantage: Hill cipher hides single letter frequencies and 3x3 Hill cipher hides two-letter frequency information.

Disadvantage:

→ Although Hill cipher is strong against a ciphertext-only attack, it is easily broken with a known plaintext attack.

Scanned by CamScanner

Vigenere cipher

→ Each of the 26 ciphers is laid out horizontally, with the key letter for each cipher to its left.

→ A normal alphabet for the plaintext runs across the top.

→ The process of encryption is simple.

→ Given a key letter x and a plaintext letter y, the ciphertext letter is at the intersection of the row labeled x and the column labeled y; in this case the ciphertext is V.

→ To encrypt a message, a key is needed that is as long as the message. Usually, the key is a repeating keyword.

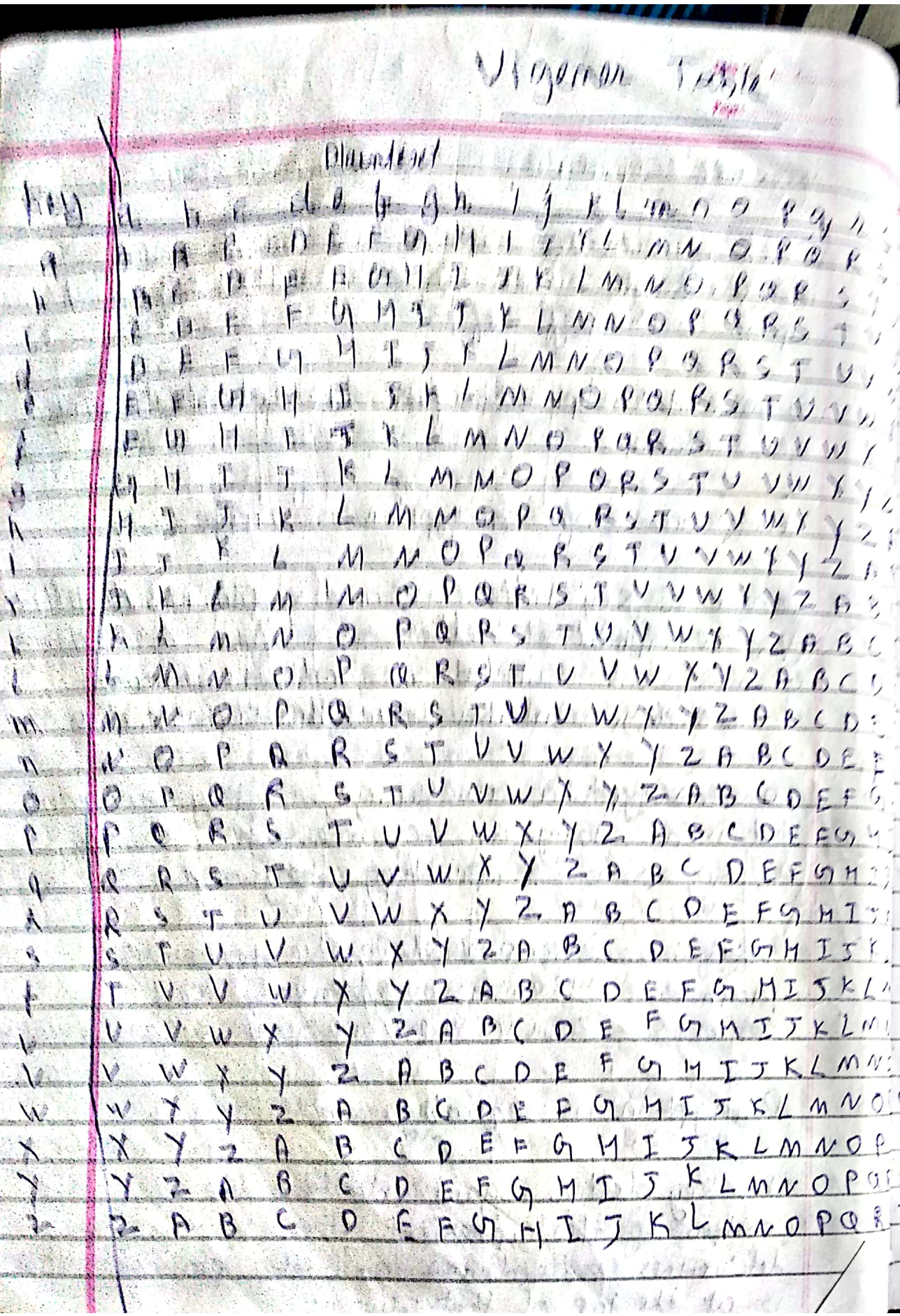
→ key: deceptivedeceptivedeceptive
plain: wearediscoverdsaveyourself
cipher: ZICVTWQNGRZGVTWAZHCQYGLMGJ

→ Decryption is equally simple

→ The key letter again identifies the row. The position of the ciphertext letter in that row determines the column, and the plaintext letter is at the top of that column.

Scanned by CamScanner

Vigenere Table



Scanned by CamScanner

Date : ..../..../....

Page : .....

One time pad / Vernam cipher

→ Implement using a random set of non-repeating characters as the i/p cipher text.

→ The most significant point here is that once an input cipher text for transposition is used, it is never used again for any other message.

Algo :

1) Treat each plaintext alphabet as a no in an increasing sequence i.e A = 0, B = 1 ... Z = 25

2) Do the same for key.

3) Add plaintext and key cipher text.

4) If the sum is greater than 26, subtract 26 from it.

5) Translate each number of the sum back to the corresponding alphabet. This gives the cipher text.

Scanned by CamScanner

Plain:	H	O	W	A	R	E	Y	O	U		
	7	14	22	0	17	4	24	14	20		
one-time Pad:	N	C	B	T	Z	Q	A	R	X		
	13	2	1	19	25	16	0	17	23		
Initial total	20	16	23	19	42	20	24	31	43		
Subtract 26 if >25	20	16	23	19	16	20	24	5	17		
Ciphertext:	U	Q	X	T	Q	U	Y	F	R		
	21										

Transposition Techniques

Rail-fence

Columnar

1) Rail-fence : Plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.

Scanned by CamScanner

Plain text: meet me after lecture

algo { m e m a t r e t r
e t b e t e f l c u e

ciphertext: m e m a t r e t r e t b e f e l c u e

(7) Columnar technique

→ Write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of columns.

→ The order of the columns then becomes the key to the algorithm.

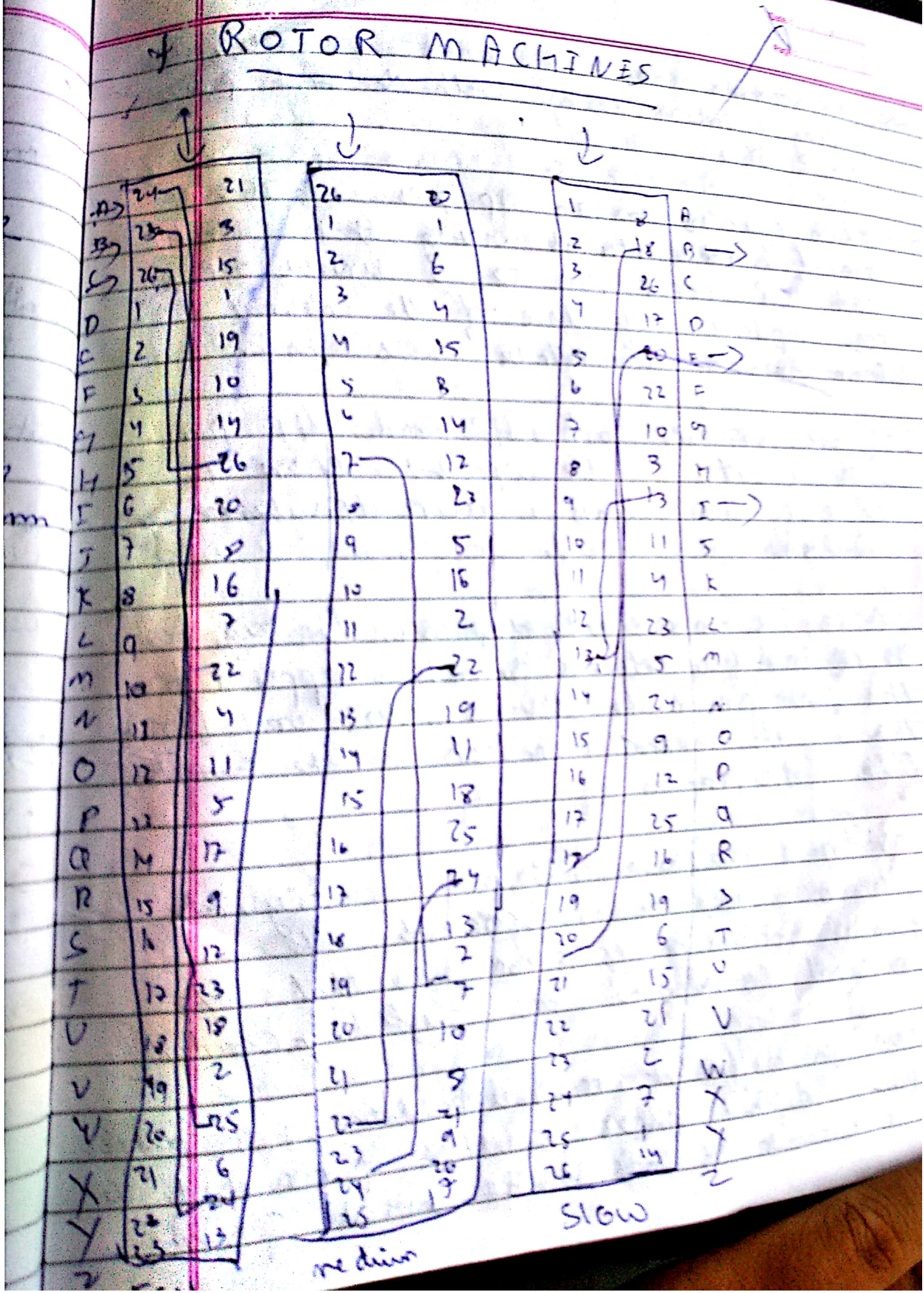
key :	4	3	1	2	5	6	7
Plain :	a	t	t	a	c	k	p
	o	s	t	p	o	n	e
	d	u	n	t	i	l	t
	w	o	a	m	x	y	z

ciphertext : t t n a a p t m t s u o a o d w c o i x k n l y p e t z

If you further encrypt the ciphertext you get stronger ciphertext

Scanned by CamScanner

ROTOR MACHINES



Scanned by CamScanner

Date : ..../..../.....

Page : .....

→ The machine consists of a set of independent rotating cylinders through with electrical pulses can flow.

→ Each cylinder has 26 i/p pins and 26 o/p pins, with internal wiring that connects each i/p input pin to a unique o/p pin. For simplicity, only three of the internal connections in each cylinder are shown.

→ If we associate each i/p and o/p pin with a letter of the alphabet, then a single cylinder defines a monoalphabetic substitution.

→ For eg, if an operator depresses the key for the letter A, an electric signal is applied to the first pin of the first cylinder and flows through the internal connection to the twenty-fifth o/p pin.

→ consider a machine with a single cylinder, after each i/p key is depressed, the cylinder rotates one position, so that the internal connections are shifted accordingly.

→ Thus, a different monoalphabetic substitution cipher is defined. After 26 letters of plaintext, the cylinder would be back to the initial position.

Scanned by CamScanner

=> Thus we have a polyalphabetic substitution algorithm with a period of 26.

=> The power of rotor machine is in the use of multiple cylinders, in which the o/p pins of one cylinder are connected to the i/p pins of the next.

* STEGANOGRAPHY

=> A plaintext message may be hidden in one of two ways. The methods of steganography conceal the existence of the message, whereas the methods of cryptography render the message unintelligible to outsiders by various transformations of the text.

=> A simple form of steganography, is one in which an arrangement of words or letters within an apparently innocuous text spells out the real message.

=> For example, the sequence of first letters of each word of the overall message spells out the hidden message.

Scanned by CamScanner

→ Various other techniques are:

1) Character marking: Selected letters of printed or typewritten text are over-writ in pencil. The marks are ordinarily not v unless the paper is held at an angle to br light.

(2) Invisible ink: A number of substances be used for writing but leave no vis trace until heat or some chemical is ap to the paper.

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

(4) Typewriter Correction ribbon: Used betwee lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light.

→ Hiding a message by using the least significant bits of frames of a photo.

→ LSB can be changed without greatly affecti quality

Scanned by CamScanner

Date : ...../...../.....

Page : .....

Drawbacks

- A lot of overhead to hide a relatively few bits of information.
- Once system is discovered, it becomes worthless.

Scanned by CamScanner

DES

* Stream cipher is one that encrypts a digital data stream one bit or byte at a time.

Eg: Vigenere cipher, Vernam cipher

* A block cipher is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.

Eg: DES

* Feistel Cipher :- Feistel proposed the use of a cipher that alternates substitutions and permutations.

-> Many modern and some old symmetric block ciphers are based on Feistal N/w.

-> For each round $i = 0, 1, \ldots, n$, compute

$$L_{i+1} = R_i$$

$$R_{i+1} = L_i \oplus F(R_i, k_i)$$

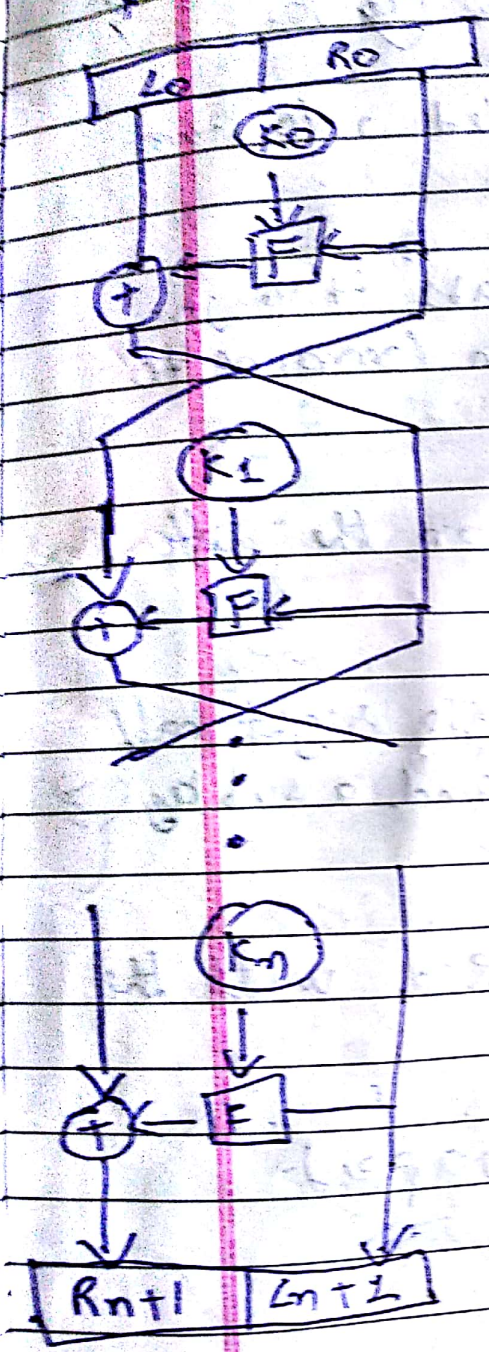
Then the ciphertext is (R_{n+1}, L_{n+1}).

-> Decryption is accomplished by computing for $i = n, n-1, \ldots, 0$: $R_i = L_{i+1}$, $L_i = R_{i+1} \oplus F(\ldots)$

Scanned by CamScanner

Encryption

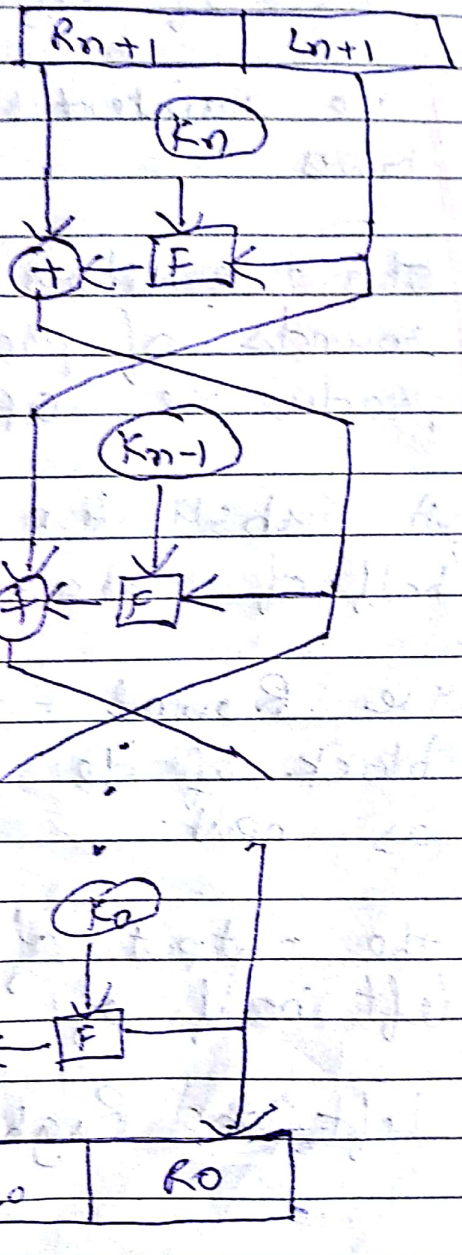
plaintext



Ciphertext

Decryption

Ciphertext



plaintext

Scanned by CamScanner

Encryption

- The input to the encryption algo are a plaintext block of length b bits and a key K.
- The plaintext block is divided into two halves
- The two halves of the data pass through rounds of processing and then combine to produce the ciphertext block.
- A substitution is performed on the left half of data.
- The Round Function F takes the right half block of the previous round and a subkey as input.
- The output of the function XORed with the left half of the data.
- Left and Right halves then swapped.

Scanned by CamScanner

* Feistel N/w depends on these parameters:

(1) Block size : Larger block size means greater security but reduced speed.

(2) key size : Larger key size means greater security but reduced speed.

(3) No. of Rounds : More rounds more

(4) Subkey generation Algo : Greater com greater security

(5) Round Function F: Greater complexity greater security.

Scanned by CamScanner

Data Encryption Standard

→ The origin of DES go back to 1972, when in the US, the National Bureau of Standards now known as the National Institute of Standards and Technology (NIST) embarked upon a project for protecting the data in computers and computer communication.

→ They wanted to develop a single cryptographic algorithm.

→ After two years, NBS realized that IBM's Lucifer could be considered as a serious candidate, rather than developing a fresh algo. from scratch.

→ After a few discussion, in 1975, the NBS published the details of the algorithm. Towards the end of 1976, the US Federal Government decided to adopt this algo and soon, it was renamed as DES.

Scanned by CamScanner

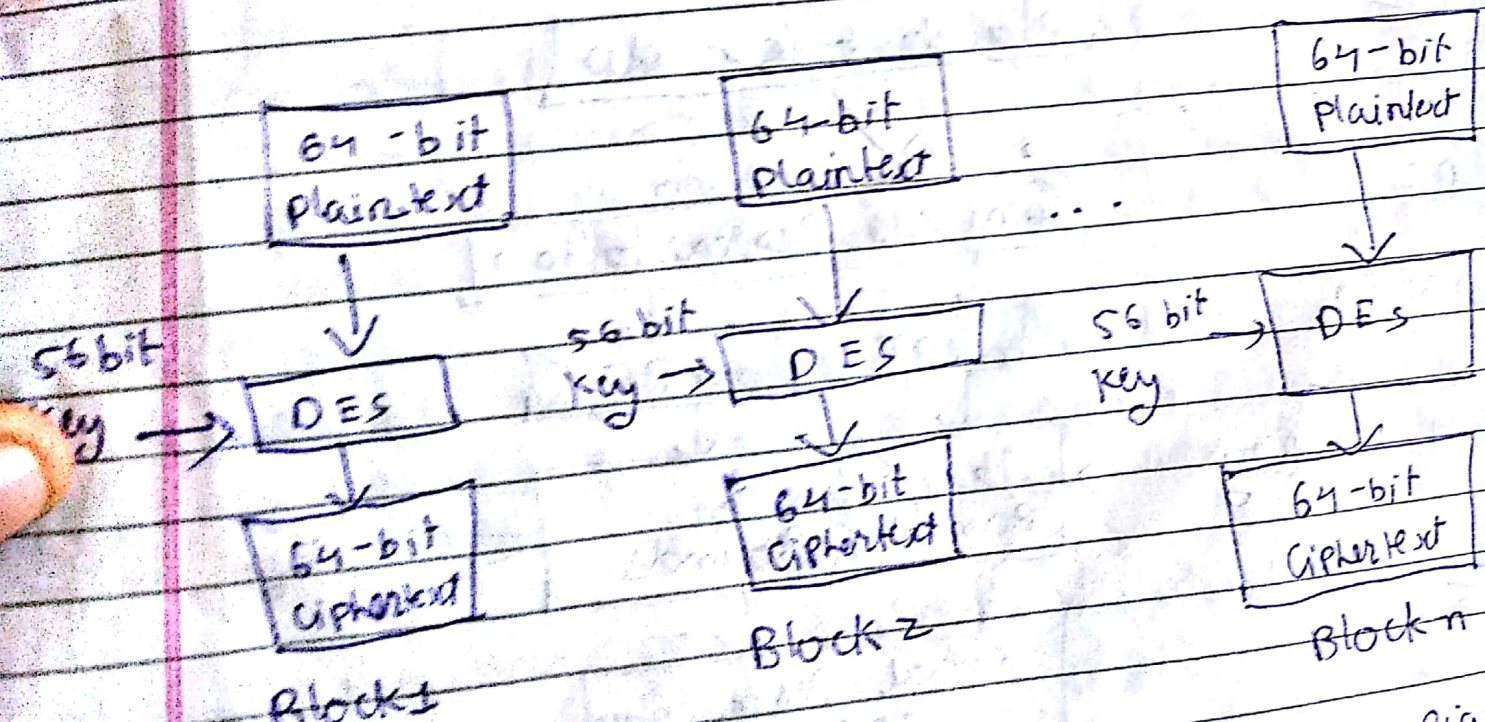
→ Basic principle

→ DES is a block cipher. It encrypts data in blocks of size 64 bits each.

→ That is, 64 bits of plain text goes as the i/p to DES, which produces 64 bits of cipher text

→ The same algorithm and key are used for encryption and decryption with minor difference.

→ The original key is 64 bit which is been converted to 56 bit key.



→ Before DES process even starts, every eighth bit of the key is discarded to produce a 56-bit key. That is bit positions 8, 16, 24, 32, 40, 48, 56 and 64 are discarded.

Scanned by CamScanner

Date : ..../..../....

Page : .....

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

→ Thus we get 56-bit key as shown above

→ Simplistically, DES is based on the two fundamental attributes of cryptography: substitution and transposition.

→ DES consists of 16 steps, each of which is called as a round.

Step 1 — Plaintext (64 bits)

Step 2 — Initial Permutation

Step 3 — LPT | RPT

Step 4 — Key → 16 Rounds | 16 Rounds ← Key

Step 5 — Final Permutation (FP)

Step 6 — Ciphertext (64 bits)

Scanned by CamScanner