Assignment-1

DATE: | | PAGE:

1) Define Cryptography and explain Symmetric cipher model

(or)

Draw the simplified model of symmetric encryption & explain it.

→

Cryptography:

Cryptographic systems are characterized along three independent dimensions.

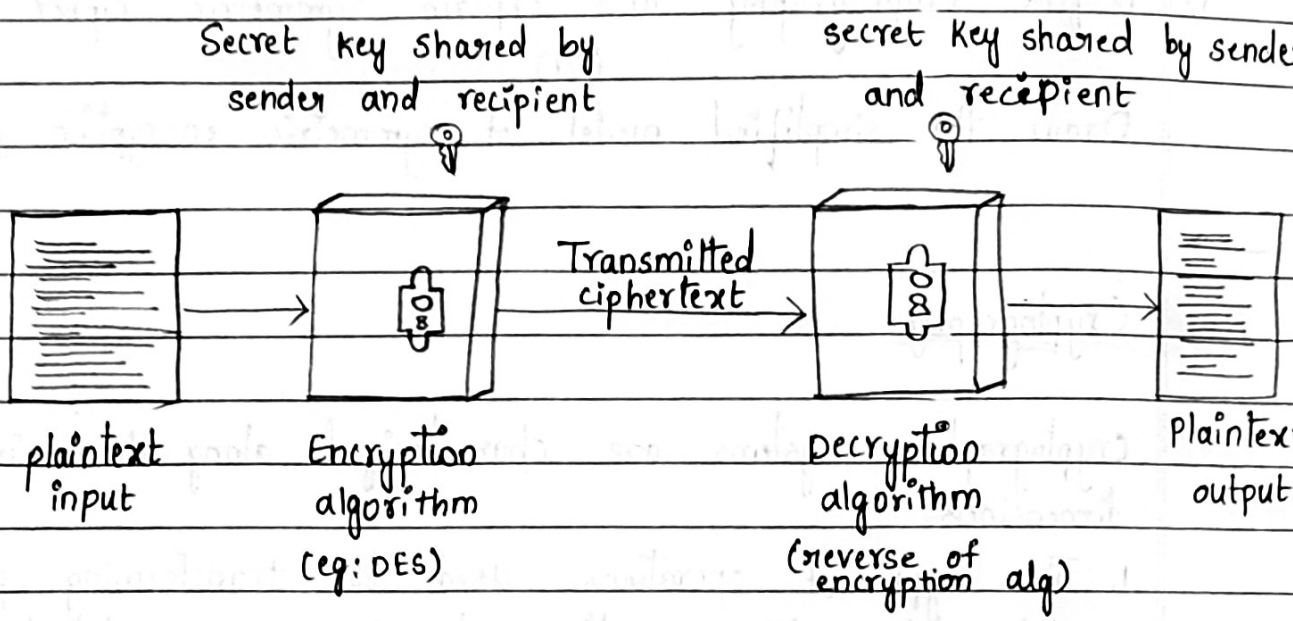
1. The type of operations used for transforming plaintext to ciphertext. All encryption algorithms are based on 2 general principles: Substitution, in which each element in the plaintext is mapped into another element and transposition, in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost.

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. If the sender and receiver use different keys, the system is referred to as asymmetric, 2-key or public-key encryption.

3. The way in which the plaintext is processed. 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 output of one element at a time, as it goes along.

DATE: | | PAGE:

Symmetric cipher model:



A Symmetric encryption scheme has five ingredients

1. Plain-text: This is the original intelligible message or data that is fed into the algorithm as input.

2. Encryption algorithm: The encryption algorithm performs various substitution and transformations on the plaintext.

3. Secret key: The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time.

4. Ciphertext: This is the scrambled message produced as output. It depends on the plaintext and the secret key.

5. Decryption algorithm: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secretkey and

DATE : | | PAGE :

produces the original plaintext.

These are 2 requirements for secure use of conventional encryption:

1. We need a strong encryption algorithm. At a minimum, we would like the algorithm to be such that an opponent who knows the algorithm and has access to one or more ciphertexts would be unable to decipher the ciphertext or figure out the key.

2. Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure.

2. Define following terms :

a) Cryptography :

Cryptographic systems are characterized along 3 independent dimensions

1. The type of operations used for transforming plaintext to ciphertext
2. The number of keys used.
3. The way in which the plaintext is processed.

b) Ciphertext :

This is the scrambled message produced as output. It depends on the plaintext and the secretkey. For a given message, 2 different keys will produce 2 different ciphertexts. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible

DATE: / / PAGE:

c) Encryption:

The process of converting from plaintext to ciphertext is known as encryption or enciphering. The encryption algorithm performs various substitution and transformations on the plaintext.

d) Decryption:

Restoring the plaintext from the ciphertext is called decryption or deciphering. The decryption algorithm is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secretkey and produces the original plaintext.

e) Cryptanalysis:

Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of cryptanalysis. It is what the layperson calls "breaking the code".

cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext.

3. List and explain the 3 independent dimensions of cryptographic system.

Cryptographic systems are characterized by the following 3 independent dimensions:

1. The type of operations used for transforming plaintext to cipher text.
2. The no. of keys used.

DATE : | | PAGE :

3. The way in which the plaintext is processed.

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

All encryption algorithms are based on 2 general principles: Substitution, in which each element in the plaintext is mapped into another element, and Transposition in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost. Most systems, referred to as product systems, involve multiple stages of substitutions and transpositions.

2. The no. of keys used:

If both sender and receiver use the same key, the system is reffered to a symmetric, single-key, secret-key or conventional encryption.

If Sender and receiver use different keys, the system is referred to as asymmetric, 2-key or public-key encryption.

3. The way in which plaintext is processed:

A block-cipher processes the input one block of elements at a time, producing an output block for each input block. A steam cipher processes the input element continuously, producing output one element at a time, as it goes along.

4. List and briefly define types of cryptanalytic attacks based on what is known to attackers.

Types of cryptanalytic attacks based on what is known to attackers are:

1. ciphertext only
2. Known plaintext
3. chosen plaintext
4. chosen ciphertext
5. chosen text

Type of attack	Known to cryptanalyst
1. ciphertext only	* Encryption algorithm * ciphertext
2. Known plaintext	* Encryption algorithm * ciphertext * one or more plaintext - ciphertext pairs formed with the secret key
3. chosen plaintext	* Encryption algorithm * ciphertext * Plaintext msg chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key.
4. chosen ciphertext	* Encryption algorithm * ciphertext * ciphertext chosen by cryptanalyst, together with its decrypted plaintext generated with secret key.

DATE : | | PAGE :

5. chosen text	* Encryption algorithm * ciphertext * Plaintext msg chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key. * ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key.

* The cipher-text-only attack is the easiest to defend against because the opponent has the least amount of information to work with.
* A file that is encoded in the post script format always begin with same pattern or there may be ~~able to deduce~~ the standardized header or banner to an electronic funds transfer msg are examples of known plaintext.
* If the analyst is able somehow to get the source system to insert into the system a msg chosen by the analyst, then a choosen plaintext attack is possible.
* chosen ciphertext and chosen text are less commonly employed as cryptanalytical techniques but are nevertheless possible avenues of attack.

DATE: | | PAGE:

5. Explain Caesar cipher with example.

Caesar Cipher:

* The earliest known & the simplest, use of a substitution cipher was by julius Caesar.
* The Caesar cipher involves replacing each letter of the alphabet with the letter standing 3 places further down the alphabet
* Note that the alphabet is wrapped around, so that the letter following Z is A. we can define the transformation by listing all possibilities as follows:

plain: a b c d e f g h i j k l m n o p q r s t u v w x y z
cipher: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

For example:

plain: meet me after the party
cipher: PHHW PH DIWHU WKH SDUWB

Let us assign a numerical equivalent to each letter:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	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

Then the algorithm can be expressed as follows. For each plaintext letter P, substitute the ciphertext letter C

$$C = E(K, P) = (P + K) \bmod 26 \quad \text{(for encryption)}$$

$$P = D(K, C) = (C - K) \bmod 26 \quad \text{(for decryption)}$$

DATE : / / PAGE :

Example : Use shift of 5 right, to encrypt the msg and write final code. using caesar cipher

plain : " meet me after the party ", K = 5

m = (P+K) mod 26 = (12+5) mod 26 = 17 ⇒ R
e = (4+5) mod 26 = 9 mod 26 = 9 ⇒ J
e = (4+5) mod 26 = 9 mod 26 = 9 ⇒ J
t = (19+5) mod 26 = 24 mod 26 = 24 ⇒ Y

m = (12+5) mod 26 = 17 mod 26 = 17 ⇒ R
e = (4+5) mod 26 = 9 mod 26 = 9 ⇒ J

a = (0+5) mod 26 = 05 mod 26 = 5 ⇒ F
f = (5+5) mod 26 = 10 mod 26 = 10 ⇒ K
t = (19+5) mod 26 = 24 mod 26 = 24 ⇒ Y
e = (4+5) mod 26 = 9 mod 26 = 9 ⇒ J
r = (17+5) mod 26 = 22 mod 26 = 22 ⇒ W

t = (19+5) mod 26 = 24 mod 26 = 24 ⇒ Y
h = (7+5) mod 26 = 12 mod 26 = 12 ⇒ M
e = (4+5) mod 26 = 9 mod 26 = 9 ⇒ J

P = (15+5) mod 26 = 20 mod 26 = 20 ⇒ U
a = (0+5) mod 26 = 5 mod 26 = 5 ⇒ F
r = (17+5) mod 26 = 22 mod 26 = 22 ⇒ W
t = (19+5) mod 26 = 24 mod 26 = 24 ⇒ Y
y = (24+5) mod 26 = 29 mod 26 = 3 ⇒ D

∴ Cipher : RJJY RJ FKYJW YMJ UFWYD

DATE: / / PAGE:

6. Find the ciphertext for plaintext "MEET ME AFTER THE TOGA PARTY" with key = 3, using caesar cipher algorithm, assign a numerical equivalent to each ~~three~~ letter.

Plaintext: "MEET ME AFTER THE TOGA PARTY", Key = 3

Numerical equivalent to each letter

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	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
																		-2	-1						

Formula to convert plaintext to ciphertext (encryption)

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

$m = (P+K) \bmod 26 = (12+3) \bmod 26 = 15 \bmod 26 = 15 \Rightarrow P$

$e = (4+3) \bmod 26 = 7 \bmod 26 = 7 \Rightarrow H$

$t = (19+3) \bmod 26 = 22 \bmod 26 = 22 \Rightarrow W$

$a = (0+3) \bmod 26 = 3 \bmod 26 = 3 \Rightarrow D$

$f = (5+3) \bmod 26 = 8 \bmod 26 = 8 \Rightarrow I$

$r = (17+3) \bmod 26 = 20 \bmod 26 = 20 \Rightarrow U$

$h = (7+3) \bmod 26 = 10 \bmod 26 = 10 \Rightarrow K$

$o = (14+3) \bmod 26 = 17 \bmod 26 = 17 \Rightarrow R$

$g = (6+3) \bmod 26 = 9 \bmod 26 = 9 \Rightarrow J$

$P = (15+3) \bmod 26 = 18 \bmod 26 = 18 \Rightarrow S$

$y = (24+3) \bmod 26 = 27 \bmod 26 = 1 \Rightarrow B$

∴ ciphertext: PHHW PH DIWHU WKH WRJD SDUWB

DATE : | | PAGE :

Formula to convert ciphertext to plaintext (decryption)

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

ciphertext: PHHW PH DIWHU WKH WRJD SDUWB

$P = (C-K) \bmod 26 = (15-3) \bmod 26 = 12 \bmod 26 = 12 \Rightarrow M$

$h = (7-3) \bmod 26 = 4 \bmod 26 = 4 \Rightarrow E$

$w = (22-3) \bmod 26 = 19 \bmod 26 = 19 \Rightarrow T$

$d = (3-3) \bmod 26 = 0 \bmod 26 = 0 \Rightarrow A$

$i = (8-3) \bmod 26 = 5 \bmod 26 = 5 \Rightarrow F$

$u = (20-3) \bmod 26 = 17 \bmod 26 = 17 \Rightarrow R$

$K = (10-3) \bmod 26 = 7 \bmod 26 = 7 \Rightarrow H$

$r = (17-3) \bmod 26 = 14 \bmod 26 = 14 \Rightarrow O$

$j = (9-3) \bmod 26 = 6 \bmod 26 = 6 \Rightarrow G$

$S = (18-3) \bmod 26 = 15 \bmod 26 = 15 \Rightarrow P$

$b = (1-3) \bmod 26 = -2 \bmod 26 = -2 \Rightarrow Y$

∴ ciphertext : PHHW PH DIWHU WKH WRJD SDUWB

plaintext : MEET ME AFTER THE TOGA PARTY

7. Explain Monalphabetic cipher with example.

* With only 25 possible keys, the caesar cipher is far from secure.
* In general, there are n! permutations of a set of n elements, because the first element can be chose in one of n ways, the second in n-1 ways, the third in n-2 ways and so on.
* If, instead, the "cipher" line can be any permutation of the 26 alphabetic characters, then there are 26! or greater than 4×10^{26} possible keys.
* This is 10 orders of magnitude greater than the key space for DES and would seem to eliminate brute-force techniques for cryptanalysis. Such an approach is referred to as a monalphabetic substitution cipher, because a single cipher alphabet is used per message.
* If the cryptanalyst knows the nature of plaintext, then the analyst can exploit the regularities of the language, the relative frequency of the letters can be determined and compared to a standard frequency distribution for English
* In monalphabetic cipher rather than just shifting the alphabet, could shuffle the letters arbitrarily.
* Each plaintext letter maps to different random ciphertext letter.
* Key is 26 letters long.

Example :

plain : abcdefghijklmnopqrstuvwxyz
cipher: DKVQFIBJWPESCXHTMYAUOLRGZN

Plaintext: if we wish to replace letters
ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA

8. Explain playfair cipher algorithm. Find the ciphertext for plaintext "INSTRUMENTS" with key = "MONARCHY"

* The Playfair algorithm is based on the use of a 5x5 matrix of letters constructed using a keyword.

Ex:

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

* Repeating plaintext letters that are in the same pair are seperated with a filler letter such as x, so that balloon would be treated as ba lx lo on.
* Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last. For example, ar is encrypted as RM.
* 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. 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. Thus, hs becomes BP and ea becomes IM (or JM, as the encipherer wishes).

DATE : | | PAGE:

Given

Key = MONARCHY

plaintext = INSTRUMENTS

IN ST RU ME NT SZ → Dummy letter

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

IN ⇒ GA

ST ⇒ TL

RU ⇒ MZ

ME ⇒ CL

NT ⇒ RQ

SZ ⇒ TX

∴ plaintext = INSTRUMENTS

ciphertext = GA TL MZ CL RQ TX

DATE : | | PAGE :

9. Encrypt the plaintext "CRYPTOGRAPHY" using Hill cipher algorithm with key $K = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$ and decrypt the same.

Given Plaintext = CRYPTOGRAPHY

Key = $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$

CR	YP	TO	GR	AP	HY
P_1	P_2	P_3	P_4	P_5	P_6

Encryption

1. $\begin{bmatrix} C \\ R \end{bmatrix} = \begin{bmatrix} 2 \\ 17 \end{bmatrix}$

$C = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 2 \\ 17 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 9\times2 + 4\times17 \\ 5\times2 + 7\times17 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 86 \\ 129 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 8 \\ 25 \end{bmatrix} \Rightarrow \begin{bmatrix} I \\ Z \end{bmatrix}$

$\therefore \begin{matrix} C \\ R \end{matrix} = \begin{matrix} I \\ Z \end{matrix}$

2. $\begin{bmatrix} Y \\ P \end{bmatrix} = \begin{bmatrix} 24 \\ 15 \end{bmatrix}$

$= \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 24 \\ 15 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 9\times24 + 4\times15 \\ 5\times24 + 7\times15 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 276 \\ 225 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 16 \\ 17 \end{bmatrix} \Rightarrow \begin{matrix} Q \\ R \end{matrix}$

$\therefore \begin{matrix} Y \\ P \end{matrix} = \begin{matrix} Q \\ R \end{matrix}$

3. $\begin{bmatrix} T \\ O \end{bmatrix} = \begin{bmatrix} 19 \\ 14 \end{bmatrix}$

$= \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 19 \\ 14 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 9\times19 + 4\times14 \\ 5\times19 + 7\times14 \end{bmatrix} \bmod 26$

4. $\begin{bmatrix} G \\ R \end{bmatrix} = \begin{bmatrix} 6 \\ 17 \end{bmatrix}$

$= \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 6 \\ 17 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 9\times6 + 4\times17 \\ 5\times6 + 7\times17 \end{bmatrix} \bmod 26$

DATE: | | PAGE:

$= \begin{bmatrix} 227 \\ 193 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 19 \\ 11 \end{bmatrix} \Rightarrow \begin{matrix} T \\ L \end{matrix}$

$\therefore \begin{matrix} T \\ O \end{matrix} = \begin{matrix} T \\ L \end{matrix}$

$= \begin{bmatrix} 122 \\ 149 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 18 \\ 19 \end{bmatrix} \Rightarrow \begin{matrix} S \\ T \end{matrix}$

$\therefore \begin{matrix} G \\ R \end{matrix} = \begin{matrix} S \\ T \end{matrix}$

5. $\begin{bmatrix} A \\ P \end{bmatrix} = \begin{bmatrix} 0 \\ 15 \end{bmatrix}$

$= \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 0 \\ 15 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 9\times0 + 4\times15 \\ 5\times0 + 7\times15 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 60 \\ 105 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 8 \\ 1 \end{bmatrix} \Rightarrow \begin{matrix} I \\ B \end{matrix}$

$\therefore \begin{matrix} A \\ P \end{matrix} = \begin{matrix} I \\ B \end{matrix}$

6. $\begin{bmatrix} H \\ Y \end{bmatrix} = \begin{bmatrix} 7 \\ 24 \end{bmatrix}$

$= \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 7 \\ 24 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 9\times7 + 4\times24 \\ 5\times7 + 7\times24 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 159 \\ 203 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 3 \\ 21 \end{bmatrix} \Rightarrow \begin{matrix} D \\ V \end{matrix}$

$\therefore \begin{matrix} H \\ Y \end{matrix} = \begin{matrix} D \\ V \end{matrix}$

$\therefore$ P = CR YP TO GR AP HY

C = IZ QR TL ST IB DV

Decryption

$\frac{1}{|K|} = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$

$= (9\times7) - (5\times4) = 43$

$43 * X \bmod 26 = 1$

$43 * 23 \bmod 26 = 1$

$989 \bmod 26 = 1$

$\therefore \frac{1}{|K|} = 23$

DATE : | | PAGE :

$K^{-1} = \frac{1}{|K|} * adj(K) = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$

$= \begin{bmatrix} 7 & -4 \\ -5 & 9 \end{bmatrix} * 23$

$= \begin{bmatrix} 161 & -92 \\ -115 & 207 \end{bmatrix}$ $\begin{bmatrix} \because \text{add } 26, 4 \text{ times to } 92 \\ \text{add } 26, 5 \text{ times to } 115 \end{bmatrix}$

$\therefore K^{-1} = \begin{bmatrix} 161 & 12 \\ 15 & 207 \end{bmatrix}$

1. $\begin{bmatrix} I \\ Z \end{bmatrix} = \begin{bmatrix} 8 \\ 25 \end{bmatrix}$

$= \begin{bmatrix} 161 & 12 \\ 15 & 207 \end{bmatrix} \begin{bmatrix} 8 \\ 25 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 1588 \\ 5295 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 2 \\ 17 \end{bmatrix} \Rightarrow \begin{matrix} C \\ R \end{matrix}$

2. $\begin{bmatrix} Q \\ R \end{bmatrix} = \begin{bmatrix} 16 \\ 17 \end{bmatrix}$

$= \begin{bmatrix} 161 & 12 \\ 15 & 207 \end{bmatrix} \begin{bmatrix} 16 \\ 17 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 2780 \\ 3759 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 24 \\ 15 \end{bmatrix} \Rightarrow \begin{matrix} Y \\ P \end{matrix}$

3. $\begin{bmatrix} T \\ L \end{bmatrix} = \begin{bmatrix} 19 \\ 11 \end{bmatrix}$

$= \begin{bmatrix} 161 & 12 \\ 15 & 207 \end{bmatrix} \begin{bmatrix} 19 \\ 11 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 3191 \\ 2562 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 19 \\ 14 \end{bmatrix} \Rightarrow \begin{matrix} T \\ O \end{matrix}$

4. $\begin{bmatrix} S \\ T \end{bmatrix} = \begin{bmatrix} 18 \\ 19 \end{bmatrix}$

$= \begin{bmatrix} 161 & 12 \\ 15 & 207 \end{bmatrix} \begin{bmatrix} 18 \\ 19 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 3126 \\ 4203 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 6 \\ 17 \end{bmatrix} = \begin{bmatrix} G \\ R \end{bmatrix}$

5. $\begin{bmatrix} I \\ B \end{bmatrix} = \begin{bmatrix} 8 \\ 1 \end{bmatrix}$

$= \begin{bmatrix} 161 & 12 \\ 15 & 207 \end{bmatrix} \begin{bmatrix} 8 \\ 1 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 1300 \\ 327 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 0 \\ 15 \end{bmatrix} = \begin{matrix} A \\ P \end{matrix}$

6. $\begin{bmatrix} D \\ V \end{bmatrix} = \begin{bmatrix} 3 \\ 21 \end{bmatrix}$

$= \begin{bmatrix} 161 & 12 \\ 15 & 207 \end{bmatrix} \begin{bmatrix} 3 \\ 21 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 735 \\ 4392 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 7 \\ 24 \end{bmatrix} = \begin{matrix} H \\ Y \end{matrix}$

$\therefore$ Plaintext = CRYPTOGRAPHY

ciphertext = IZQR TLST IBDV

DATE: | | PAGE:

10. Explain Polyalphabetic and one Time Pad cipher with example

Polyalphabetic ciphers :

* one of the way to improve on the simple monoalphabetic technique is to use different monoalphabetic substitutions as one proceeds through the plaintext.
* The general name for this approach is polyalphabetic substitution cipher. All these techniques have the following features in common
  1. A set of related monoalphabetic substitution rules is used.
  2. A key determines which particular rule is chosen for a given transformation.

1. Vigenere ciphere :

* one of the simplest, polyalphabetic cipher is vigenere cipher
* A general equation of the encryption process is

$$C_i = (P_i + K_i \bmod m) \bmod 26$$

* similarly, decryption is a generalization of equation

$$P_i = (C_i - K_{i \bmod m}) \bmod 26$$

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

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

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

Ex:

Consider plaintext : "WE ARE DISCOVERED SAVE"

Key : DECEPTIVE

DATE : / / PAGE :

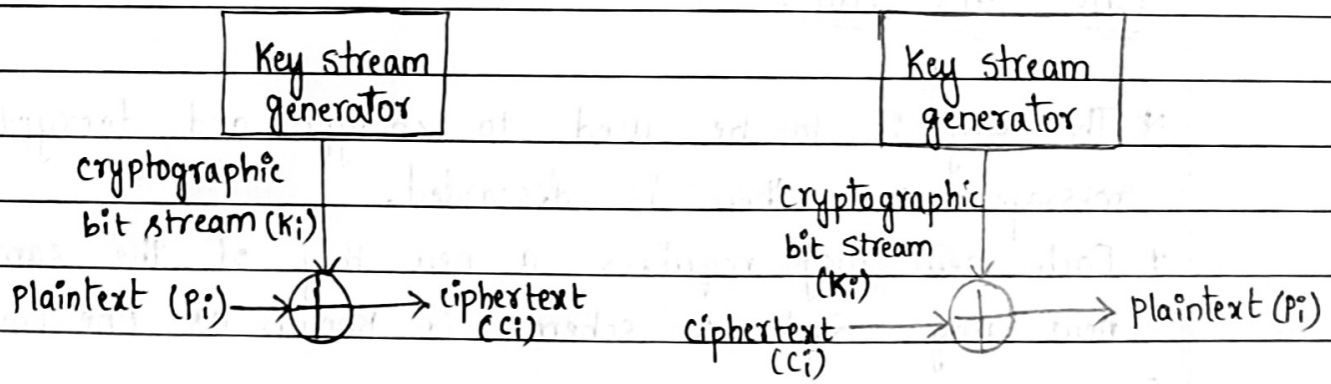
Encryption

Plaintext =	W	E		A	R	E		D	I	S	C	O	V	E	R	E	D		S	A	V	E
Key =	D	E		C	E	P		T	I	V	E	D	E	C	E	P	T		I	V	E	D
$(P_i + K_i)$ =	25	8		2	21	19		22	16	39	6	17	25	6	21	19	22		26	21	25	7
$(P_i + K_i) \bmod 26$ =	25	8		2	21	19		22	16	13	6	17	25	6	21	19	22		0	21	25	7
	Z	I		C	V	T		W	Q	N	G	R	Z	G	V	T	W		A	V	Z	H

∴ Plaintext : WE ARE DISCOVERED SAVE
ciphertext : ZI CVT WQNGRZGVTW AVZH

2. Vernam Cipher :

* The ultimate defense against such a cryptanalysis is to choose a keyword that is as long as the plaintext and has no statistical relationship to it. Such a system was introduced by an AT&T engineer named Gilbert Vernam in 1918



* The system can be expressed as follows : $C_i = P_i \oplus K_i$

where P_i = ith binary digit of plaintext
K_i = ith binary digit of key
C_i = ith binary digit of ciphertext
$\oplus$ = exclusive-OR (XOR) operation

* Thus, the ciphertext is generated by performing the bitwise XOR of the plaintext and the key. Because of the property of the XOR, decryption simply involves the same Bitwise Operation : $P_i = C_i \oplus K_i$

Example :

Consider P = 1101 K = 1011

Encryption : $C_i = P_i \oplus K_i$

P_i K_i

$C_1 = 1 \oplus 1 = 0$

$C_2 = 1 \oplus 0 = 1$

$C_3 = 0 \oplus 1 = 1$

$C_4 = 1 \oplus 1 = 0$

$\therefore C = 0110$

Decryption : $P_i = C_i \oplus K_i$

C_i K_i

$P_1 = 0 \oplus 1 = 1$

$P_2 = 1 \oplus 0 = 1$

$P_3 = 1 \oplus 1 = 0$

$P_4 = 0 \oplus 1 = 1$

$\therefore P = 1101$

One Time Pad :

* The key is to be used to encrypt and decrypt a single message, and then is discarded.
* Each new msg requires a new key of the same length as new msg. Such a scheme is known as One Time Pad.

Ex:

Consider Plaintext = A P P L E

Random key = X M P S B

P = A P P L E

0 15 15 11 4

K = X M P S B

23 12 15 18 1

DATE : / / PAGE :

ciphertext = 0 + 23 = 23 = X

15 + 12 = 27 = B

15 + 15 = 30 = E

11 + 18 = 29 = D

4 + 1 = 5 = F

∴ plaintext = A P P L E

ciphertext = X B E D F

11. Distinguish between a) confusion and diffusion

Feature	Confusion	Diffusion
Definition	obscures the relationship btwn the ciphertext and the encryption key	spreads the influence of one plaintext bit over many ciphertext bits
Goal	Make it difficult to deduce the key from ciphertext	Hide statistical patterns of the plaintext
Method	Achieved through substitution	Achieved through permutation/ transportation
Effect	Key-ciphertext relationship becomes highly complex	A single change in plaintext affects many ciphertexts bits
Example in AES	S-box (Substitution box)	Shift Rows and Mix Columns
Main Protection	Protects against key guessing	Protects against frequency/ statistical analysis.

DATE: | | PAGE:

b. Block cipher and Stream cipher.

Feature	Stream cipher	Block cipher
Basic operation	Encrypts data one bit or one byte at a time.	Encrypts a fixed-size block of plaintext at once.
Key stream	uses a bit-stream generator to produce a key stream that is XORed with plaintext	Uses a fixed encryption algo with the key to transform plaintext block to ciphertext block
Key Requirement	Sender and Receiver share only the generating key, from which the keystream is produced	Sender and receiver share the symmetric key used directly in the block algorithm.
Randomness	Security depends on the keystream being unpredictable	Security depends on strong block transformations
Error propogation	An error in one bit usually affects only that bit	An error in one block may corrupt the entire block of cipher text during decryption
speed	Generally faster and suitable for real-time applications	Usually slower due to complex block transformations.
Examples	Vernam cipher, RC4 and Autokeyed Vigenere	DES, AES, Blowfish
Use Cases	Streaming data, secure video/ Voice, light weight encryption	File encryption, database encryption, most network security protocols.

DATE : | | PAGE :

12. Explain Feistel encryption and decryption algorithm, with neat diagram.

Feistel encryption algorithm:

* The inputs to the encryption algorithm are a plaintext block of length 2w bits and key K. The plaintext block is divided into 2 halves, L_0 and R_0
* The 2 halves of the data pass through n rounds of processing and then combine to produce the ciphertext block.
* Each round i has inputs L_{i-1} and R_{i-1}, derived from the previous round, as well as a subkey K_i, derived from the overall K.
* In general, the subkeys K_i are different from K and from each other.
* A substitution is performed on the left half of the data. This is done by applying around function F to the right half of the data and then taking the exclusive-OR of the output of that function and the left half of the data.
* Following this substitution, a permutation is performed that consists of the interchange of the 2 halves of the data.
* The exact realization of a Feistel network depends on the choice of the following parameters and design features
1. block size, 2. key size, 3. No. of rounds, 4. Subkey generation algorithm and 5. Round function.

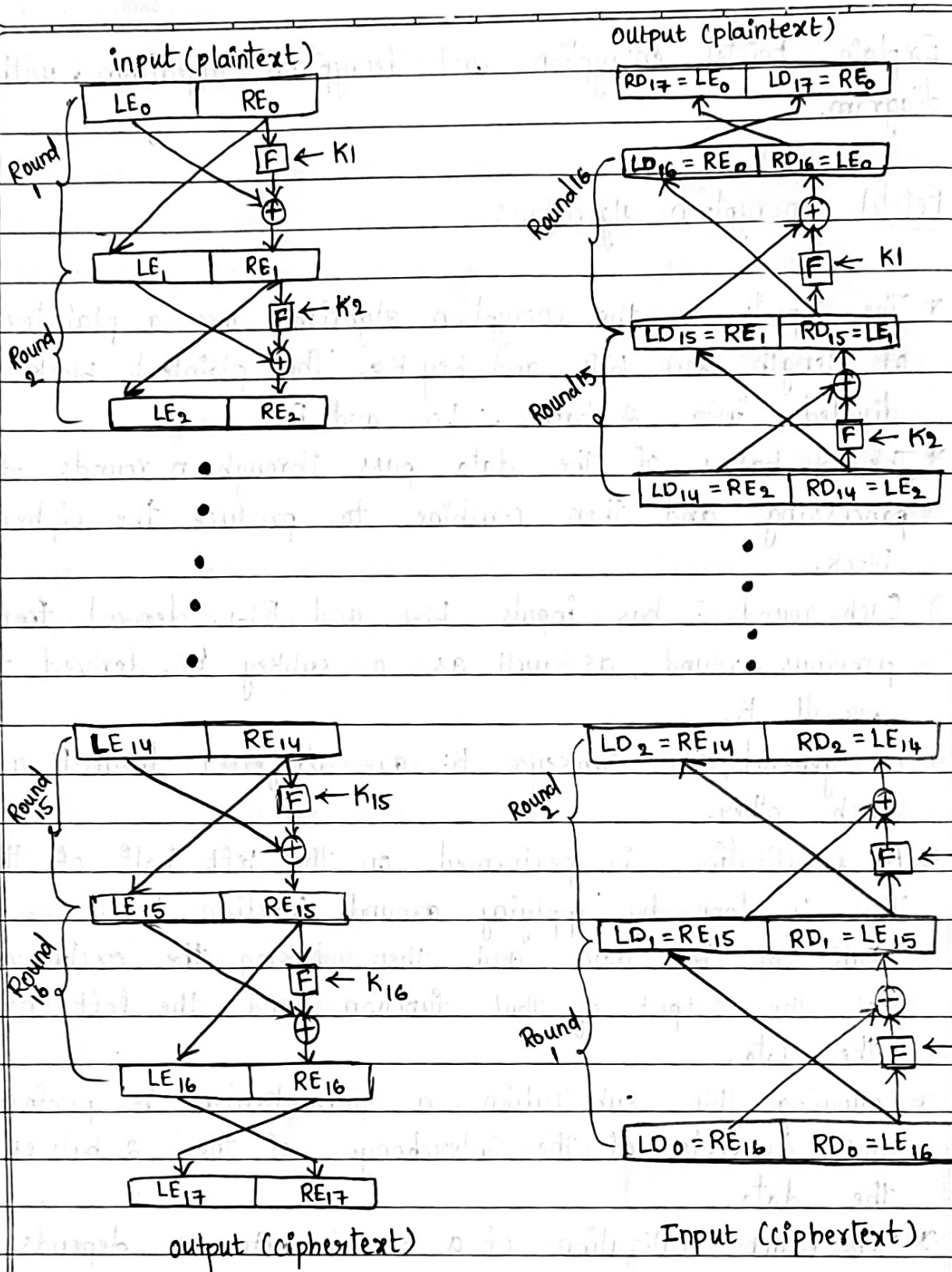


fig: Feistel Encryption and Decryption (16 rounds)

DATE: | | PAGE:

Feistel Decryption Algorithm:

* The process of decryption with a Feistel cipher is essentially the same as the encryption process.
* The rule is as follows: use the ciphertext as input to the algorithm, but use the subkeys K_i in reverse order. That is, use K_n in the first round, K_{n-1} in the second round and so on until K_1 is used in the last round.
* Now we would like to show that the output of the first round of the decryptn process is equal to a 32-bit swap of the input to the sixteenth round of the encryption process. First consider the encryption process. we see that

$$LE_{16} = RE_{15}$$

$$RE_{16} = LE_{15} \times F(RE_{15}, K_{16}) \qquad [\because here \ X = \oplus]$$

on the decryption side, LD_1

$$= RD_0 = LE_{16} = RE_{15}$$

$$RD_1 = LD_0 \times F(RD_0, K_{16})$$

$$= RE_{16} \times F(RE_{15}, K_{16})$$

$$= [LE_{15} \times F(RE_{15}, K_{16})] \times F(RE_{15}, K_{16})$$

The XOR has the following properties:

$$[A \times B] \times C = A \times [B \times C]$$

$$D \times D = 0$$

$$E \times 0 = E$$

* Thus we have $LD_1 = RE_{15}$ and $RD_1 = LE_{15}$. Therefore, the output of the first round of the decryption process is $LE_{15} || RE_{15}$, which is the 32-bit swap of the input to the sixteenth round of the encryption. This correspondence holds all the way through the 16 iterations, as is easily shown. we can cast this process in general terms. For the ith iteration of the encryption algorithm.

$LE_i = RE_{i-1}$

$RE_i = LE_{i-1} \times F(RE_{i-1}, K_i)$

Re arranging terms,

$RE_{i-1} = LE_i$

$LE_{i-1} = RE_i \times F(RE_{i-1}, K_i) = RE_i \times F(LE_i, K_i)$

13. Explain with neat diagram DES encryption and decryption algorithm

* The overall scheme for DES encryption is illustrated in the below figure.
* As with any encryption scheme, there are 2 inputs to the encryption function : the plaintext to be encrypted and the key.
* In this case, the plaintext must be 64 bits in length and the key is 56 bits in length.
* looking at the left-hand side of the figure, we can see that the processing of the plaintext proceeds in three phases.
* First, the 64-bit plaintext passes through an initial permutation (IP) that rearranges the bits to produce the permuted input.
* This is followed by a phase consisting 16 rounds of same function, which involves both permutation and substitution functions.
* The output of last round consists of 64 bits that are a function of the input plaintext and the key.
* The left and right halves of the output are swapped to produce the pre output.
* Finally, the preoutput is passed through a permutation [IP^{-1}] that is the inverse of the initial permutation function, to

produce the 64-bit ciphertext.

* with the exception of the initial and final permutations, DES has the exact structure of a Feistel cipher as shown in figure.
* The right-hand portion of figure shows the way in which the 56-bit key is used.
* Initially, the key is passed through a permutation function. Then, for each of the 16 rounds, a subkey (K_i) is produced by the combination of a left circular shift and a permutation.
* The permutation function is the same for each round, but a different subkey is produced because of the repeated shifts of the key bits.

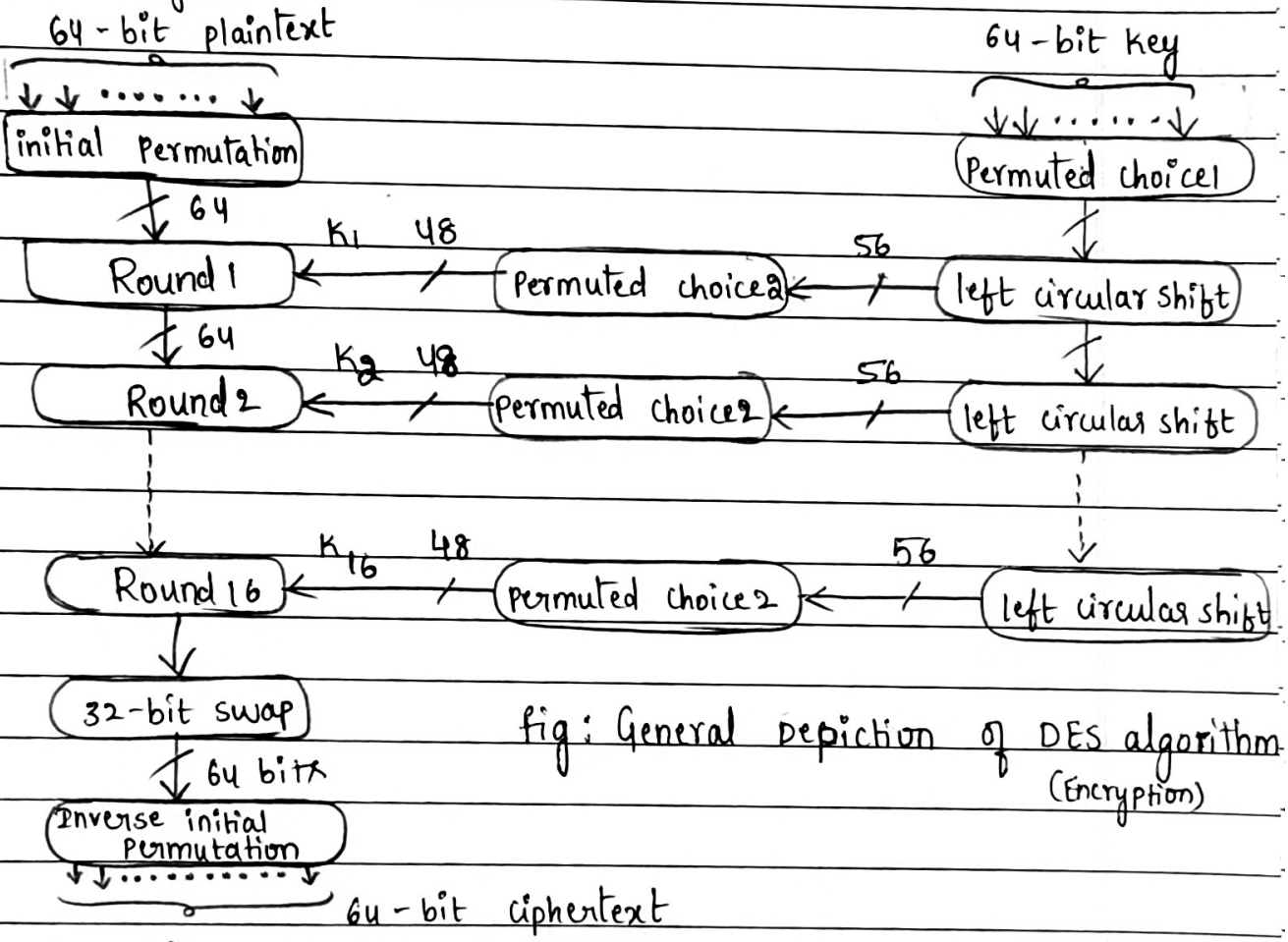


fig: General depiction of DES algorithm (Encryption)

DES decryption: decryption uses the same algorithm as encryption, except that the application of the subkeys is reversed. Additionally, the initial and final permutations are reversed.