Page No.
Date / /

→ Cryptography :-
Set of network security protocols to establish the communication to perform the secure data transfer

+ Cryptography and network security

* terminology :-

- Sender :- a sender is a person to creates and generate a message
- Receiver :- a recipient of the message generated by a sender
- message :- a message is a information which is plain text (PT)
- encryption :- it is a process or a function applied over the message or plain text.
- Ciphertext :- the encrypted message is known as ciphertext (CT)
- decryption :- it is a processor function applied over Ciphertext (CT) to get original plain text (PT)
- Cryptography :- the set of technique used to keep the message secure is called as cryptography
- cryptoanalysis :- the techniques used to break the ciphertext is known as cryptoanalysis.

Page No.
Date / /

- Cryptoanalyst :- the person performing Cryptanalysis is known as cryptoanalyst.

- Cryptologists :- the method that used both Cryptoanalysis and cryptograph is known as Cryptologist.

- Cryptosystem :- a system that uses all the possible plain text, secret key information to generate cyphertext is called as Cryptosystem

- Cryptographer :- the person using cryptography is called as cryptographer.

* the plain text is denoted by (PT) plain text or message by M that is to be encrypted.

$$M = PT$$

$$PT = \boxed{E} \longrightarrow \text{keys}$$

keys → symmetric → single key

keys → Assymetric → double key → encryption, decryption

- Ciphertext is denoted by (CT) which is to be decrypted.
- the mathematical notation for :-

- encryption function message M is given by :-

$$E(M) = C$$

~~D(C) = M or D(E(M)) = M~~

- decryption function on C is given by : - D(C) = M or D(E(M)) = M

$$E_K(M) = CT$$

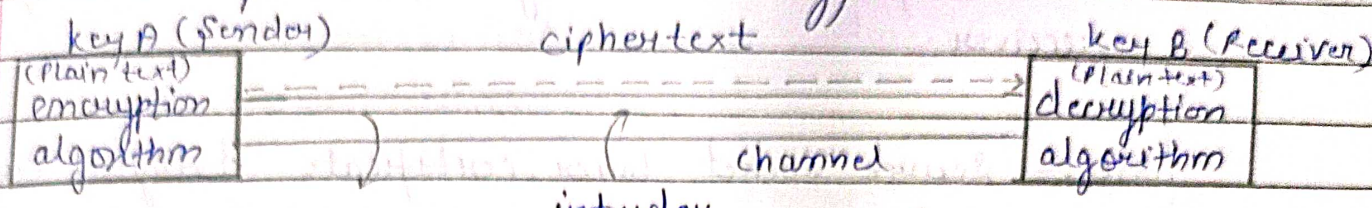
$$D_K(CT) = M \longrightarrow PT$$

k_1, k_2 ——— {keyspace}

Page No.
Date / /

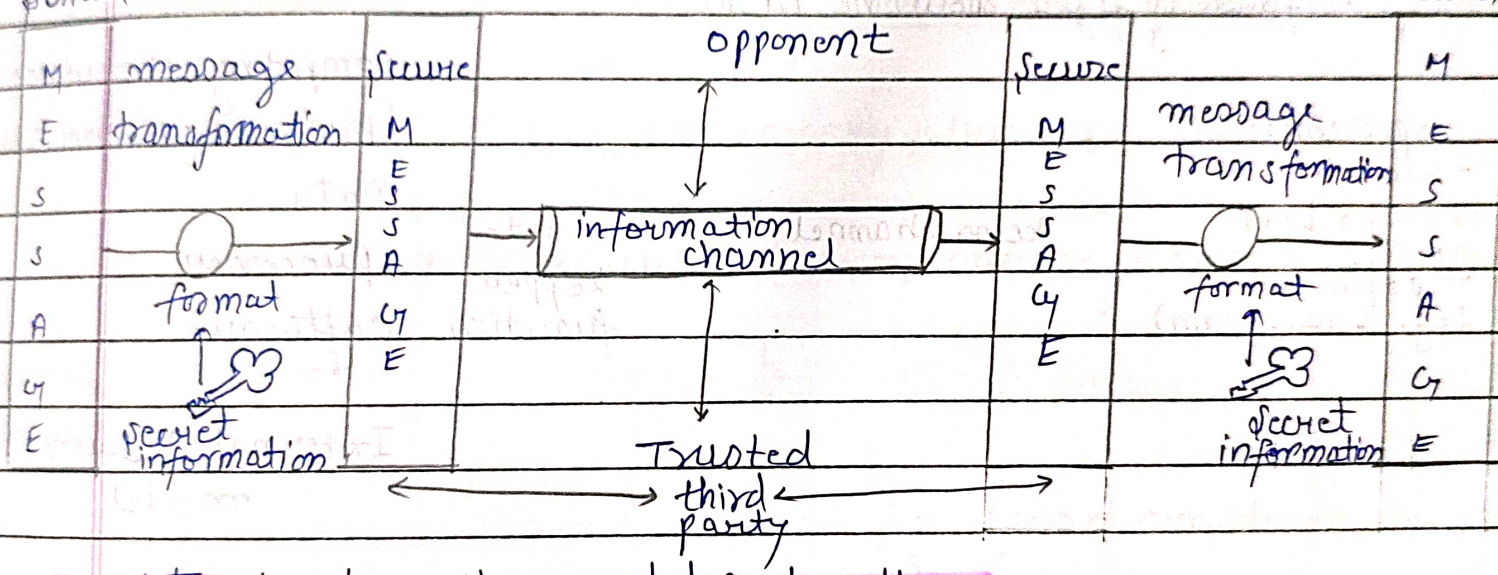
- Cryptography work with concept of key 'k'
- the range of key is called as KEYSPACE

* following figure shows the use of cryptography concept and the terminology:-



{Que:- explain N.S M}

* Network Security model :- {2 & 3M}



* Network Security model explanation:-

• Symmetric (single key) Assymmetric (more than one key)

- As shown in the above figure :-

+ At sender side :-

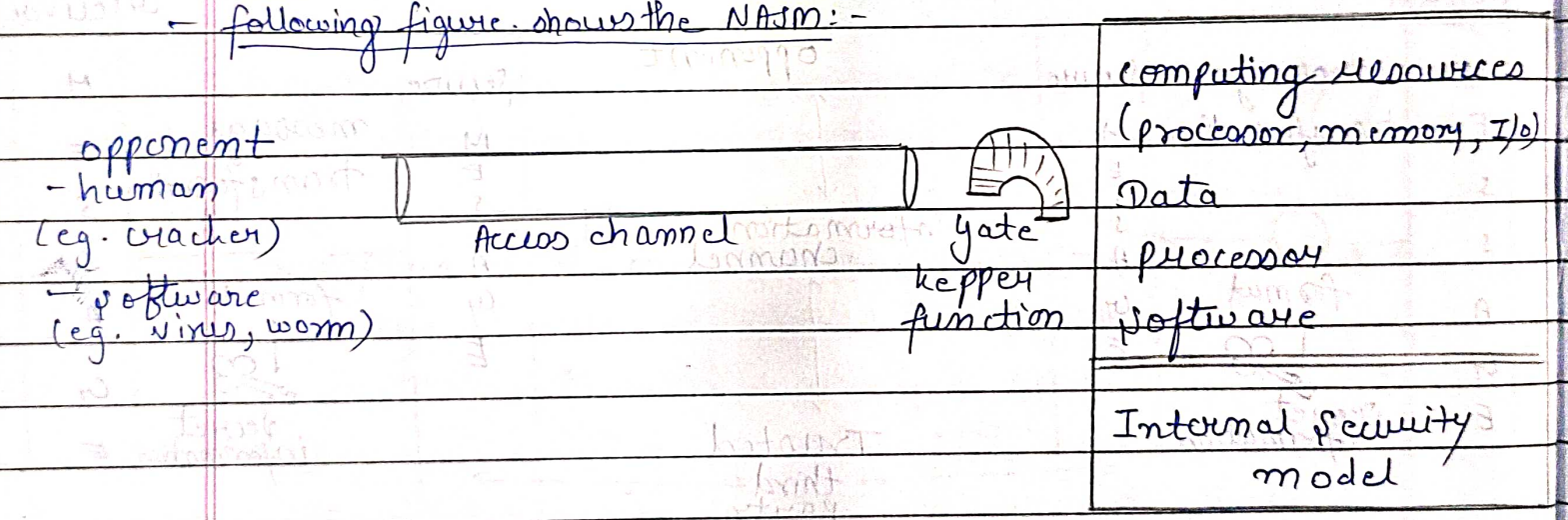
• the sender generate the message which is called as plaintext
• the message is encrypted using the secret information with the help of key which can be symmetric or assymmetric key.
• these encryption leads to generate the secure message and ~~then~~ which is a ciphertext message and then it travel through the information channel which is an open source or internet.
• the information channel as it is an open source the opponent and trusted third party are present to access the message

Page No.
Date / /

+ At receiver side:-
- At receiver side the secure message comes from information channel which is ciphere text message.
- these secure message is decrypted from the secret information using key and receive by the receiver.

{SSL :- Secure Socket layer certificate {digital certificate}}

* Network access security model
- following figure shows the NASM:-



Page No.
Date / /

* Principles of security

- Confidentiality
- Authentication
- Integrity
- Non - repudiation
- Access Control
- Availability

1) Confidentiality :-

- It is the process of preventing disclosure of information to unauthorized individuals or systems.
- examples :- credit card
- Confidentiality is necessary, but not sufficient to maintain privacy.
- Interception causes loss of message confidentiality

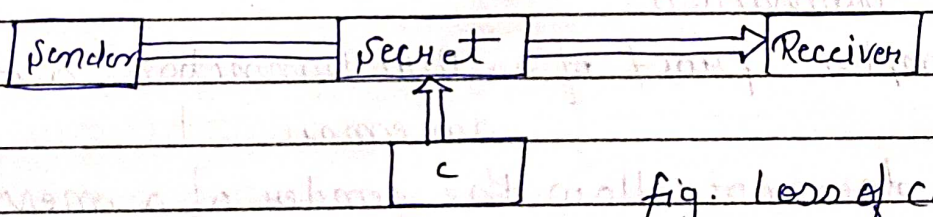


fig. loss of confidentiality.

2) Authenticity :- In computing, e-business and information security it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine (i.e they have not been forged or fabricated).

- examples :- passport, credit card accounts, academic transcripts.
- fabrication is possible in absence of proper authentication.

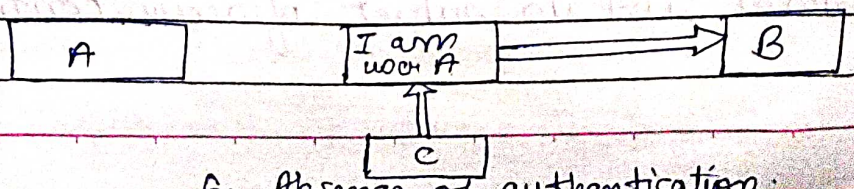


fig. Absence of authentication.

Page No.
Date / /

3) Integrity :-

- It means that data cannot be modified/change without authorization
- examples:- manual deletion or alteration or creation of important data files, Virus infection, website vandalism
- modification causes loss of message integrity

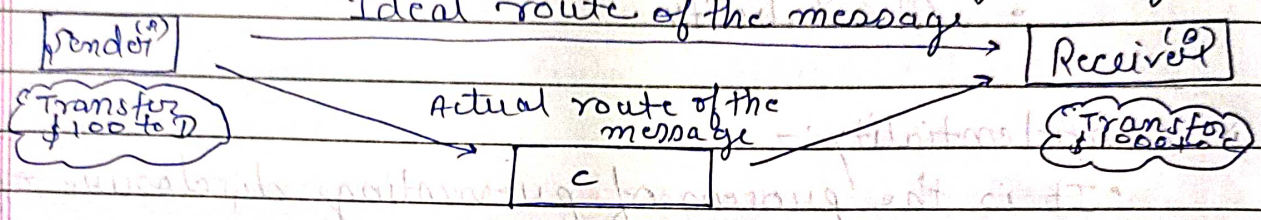


fig. loss of integrity

4) Non-Repudiation :-

- it is a complex term used to describe the lack of deniability of ownership of a message, piece of data, or transaction.
- examples:- proof of an ATM transaction, a stock trade or an email
- It does not allow the sender of a message to refute the claim of not sending that message.

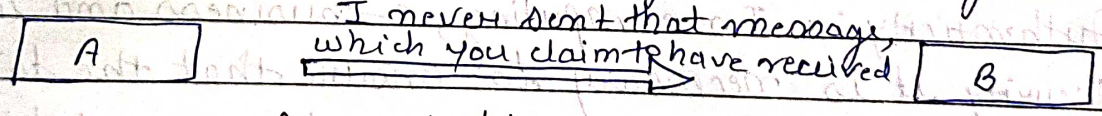


fig. establishing non-repudiation.

5) Access control :-

- Role management → User side → which user can do what
- Rule management → Resource side → which resources are accessible and under what circumstances.
- Access control list is subset of access control matrix.

Page No.
Date / /

6) Availability :-

- for any information / system to serve its purpose,
- the information must be accessible & usable when it is needed.
- Computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly.
- examples: power outages, hardware failures, system upgrades and preventing denial-of-service attack.
- Interruption puts the availability of resources in danger.

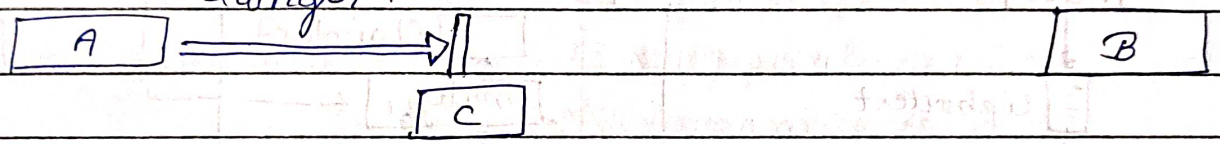


fig: Attack on availability

Security Attacks

- Snooping
  - traffic analysis
  - threat to confidentiality
- modification
  - masquerading
  - replaying
  - repudiation
  - threat to integrity
- denial of service
  - threat to availability

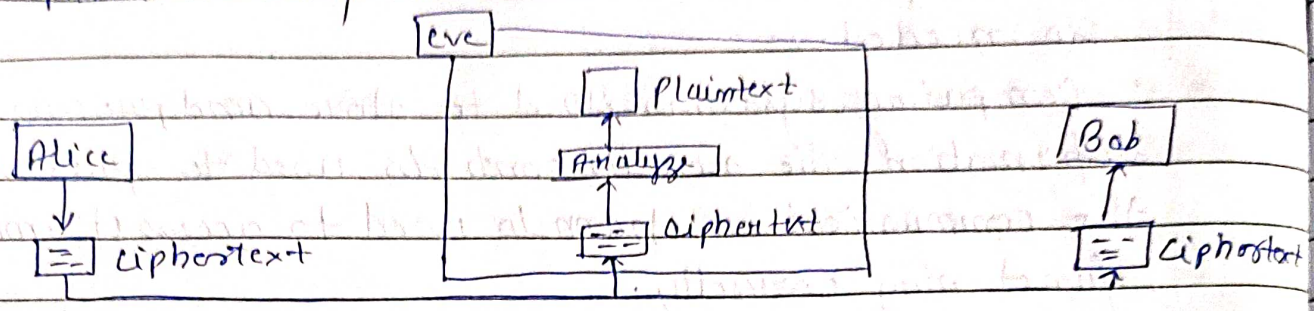
Types of Security attack

- Passive attack
  - release of message content
  - traffic analysis
  - only information is attack
  - Confidentiality
- Active attack
  - masquerade
  - modification of message
  - replay
  - denial of service
  - replay

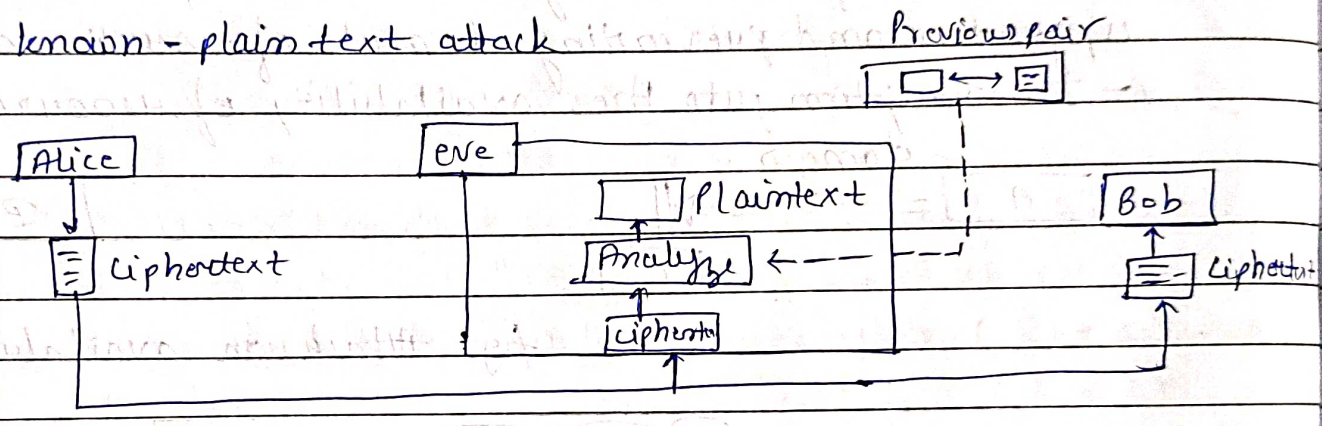
Page No.
Date / /

* Cryptanalysis attacks:-

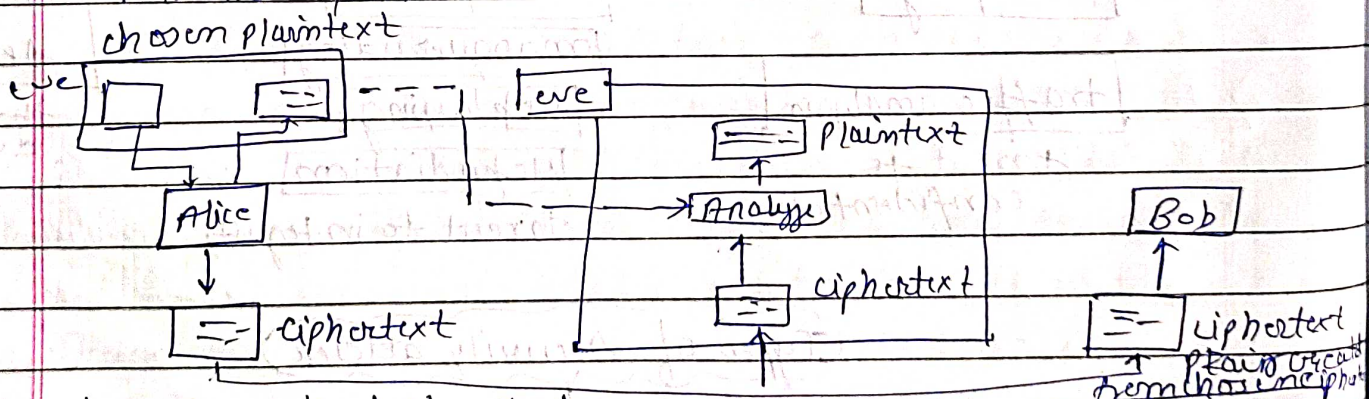
1) Ciphertext-only attack



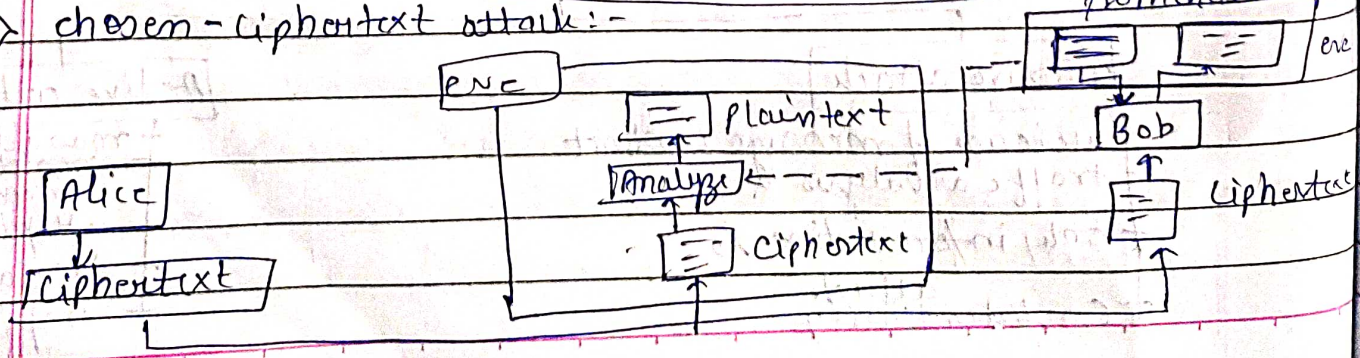
2) known-plaintext attack



3) Chosen-plaintext attack:-



4) chosen-ciphertext attack:-



PT:- plaintext
CT:- ciphertext

Page No.
Date / /

Transforming plaintext to ciphertext

- **Substitution technique**
  - each letter/symbol/char of PT ⇒ replaced/substituted by another symbol/char/letter
  - **monoalphabetic cipher**
    - Caesar cipher
    - modified caesar cipher
    - Homophonic substitution cipher
    - Polygram substitution cipher
  - **Polyalphabetic cipher**
    - Playfair cipher
    - Vigenere cipher
    - Hill cipher
    - Vernam cipher
    - Modified Vernam or one time pad cipher
- **Transposition technique**
  - Re-ordering the position of each symbol/letter/char in the PT into CT

* Substitution cipher:- it replaces one symbol with another.
- ex:- replacing A with letter D or T with letter Z.
- it has been categorized as follows:-

→ monoalphabetic cipher :- a group of substitution ciphers called the monoalphabetic ciphers.
- In these, a character (or a symbol) in the plaintext is always changed to the same character (or symbol) in the ciphertext regardless of its position in the text.
- for ex:- if the algorithm says that letter A in the PT is changed to letter D.
- In monoalphabetic substitution, the relationship between a symbol in the plaintext to a symbol in the ciphertext is always one-to-one.

Page No.
Date / /

- Caesar cipher → Additive cipher / multiplicative cipher / Affine cipher.

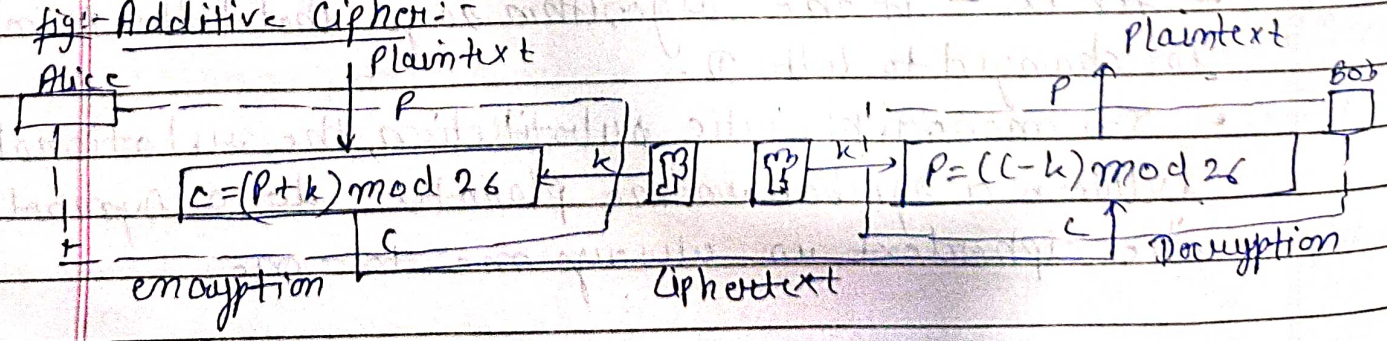
* Caesar cipher :- In these, the key, K is fixed to 3 i.e. K=3, whereas in Additive cipher, the value of K is changed.
- It is also known as modified caesar cipher method.

— Additive cipher :-
- it is simplest monoalphabetic cipher
- it is also called and referred to as a shift cipher or Caesar cipher.
- when the cipher is additive, the plaintext, ciphertext and the key are integers in Z_{26}.
- plaintext → lowercase letter (a to z)
- ciphertext → Uppercase letter (A to z)
- to apply mathematical operation on the PT & CT, we assign numerical values to each other as follows :-

fig :- representation of PT and CT characters in Z_{26}

Plaintext →	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	
Ciphertext →	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	
Value/key →	00	01	02	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	

fig :- Additive cipher :-



Page No.
Date / /

- prove that encryption and decryption are inverse of each other because plaintext created by Bob (P_1) is the same as the one sent by Alice (P)

$P_1 = ((-k) \bmod 26 = (P+k-k) \bmod 26 = P$

Qu- encrypt the message M = "Hello" using caesar cipher method.

→ given :- PT :- [h|e|l|l|o]

Using the mathematical equation :-

encryption $CT = [P+k] \bmod 26$ — ①

decryption $PT = [CT-k] \bmod 26$ — ②

∴ since, it is Cisar cipher method the value of key 'k' that is fixed hence $k=3$

h $CT_1 \Rightarrow (7+3) \bmod 26 = 10 \bmod 26 = 10$ K

e $CT_2 \Rightarrow (4+3) \bmod 26 = 7 \bmod 26 = 7$ H

l $CT_3 \Rightarrow (11+3) \bmod 26 = 14 \bmod 26 = 14$ O

l $CT_4 \Rightarrow (11+3) \bmod 26 = 14 \bmod 26 = 14$ O

o $CT_5 \Rightarrow (14+3) \bmod 26 = 17 \bmod 26 = 17$ R

CT = {KHOOR}

Q — decrypt the above CT using ceaser cipher method.

K $PT_1 = (10-3) \bmod 26 = 7$ h

H $PT_2 = (7-3) \bmod 26 = 4$ e

O $PT_3 = (14-3) \bmod 26 = 11$ l

O $PT_4 = (14-3) \bmod 26 = 11$ l

R $PT_5 = (17-3) \bmod 26 = 14$ O

PT = {hello}

$(3-15) \bmod 26$
$-12 \bmod 26 \longrightarrow$ $\begin{array}{r} 26 \\ -12 \\ \hline 14 \end{array}$
$14 \bmod 26 = 14$

Page No.
Date / /

* example of modified caesar cipher method:-

Que- Use the additive cipher with $k=15$ to encrypt the message 'hello'

→ - additive cipher is also known as modified caesar cipher method.

The given message plain text = | h | e | l | l | o |

using additive cipher encryption mathematical equation

$c = (p+k) \bmod 26$ for key $= 15$

$PT_1 = h = 7$ $\quad CT_1 = (7+15) \bmod 26 = 22 = W$

$PT_2 = e = 4$ $\quad CT_2 = (4+15) \bmod 26 = 19 = T$

$PT_3 = l = 11$ $\quad CT_3 = (11+15) \bmod 26 = 0 = A$

$PT_4 = l = 11$ $\quad CT_4 = (11+15) \bmod 26 = 0 = A$

$PT_5 = o = 14$ $\quad CT_5 = (14+15) \bmod 26 = 3 = D$

$\therefore CT = \{WTAAD\}$

— decrypt $CT = WTAAD$

$CT_1 = W = 22$ $\quad PT_1 = (22-15) \bmod 26 = 7 = h$

$CT_2 = T = 19$ $\quad PT_2 = (19-15) \bmod 26 = 4 = e$

$CT_3 = A = 0$ $\quad PT_3 = (0-15) \bmod 26 = -15 = 11 = l$

$CT_4 = A = 0$ $\quad PT_4 = (0-15) \bmod 26 = -15 = 11 = l$

$CT_5 = D = 3$ $\quad PT_5 = (3-15) \bmod 26 = -12 = 14 = o$

$PT = \{hello\}$

Page No.
Date / /

que- Use Additive cipher for k = 17 & perform encryption for message "network security"

→ The message given in PT :- [n|e|t|w|o|r|k|s|e|c|u|r|i|t|y]

PT1 = n = 13 CT1 = (13+17) mod 26 = 4 E
PT2 = e = 4 CT2 = (4+17) mod 26 = 21 V
PT3 = t = 19 CT3 = (19+17) mod 26 = 10 K
PT4 = w = 22 CT4 = (22+17) mod 26 = 13 N
PT5 = o = 14 CT5 = (14+17) mod 26 = 5 F
PT6 = r = 17 CT6 = (17+17) mod 26 = 8 I
PT7 = k = 10 CT7 = (10+17) mod 26 = 1 B
PT8 = s = 18 CT8 = (18+17) mod 26 = 9 J
PT9 = e = 4 CT9 = (4+17) mod 26 = 21 V
PT10 = c = 2 CT10 = (2+17) mod 26 = 19 T
PT11 = u = 26 CT11 = (20+17) mod 26 = 11 L
PT12 = r = 17 CT12 = (17+17) mod 26 = 8 I
PT13 = i = 8 CT13 = (8+17) mod 26 = 25 Z
PT14 = t = 19 CT14 = (19+17) mod 26 = 10 K
Pt15 = y = 24 CT15 = (24+17) mod 26 = 15 P

The CT = { E V K N F I B J V T L I Z K P

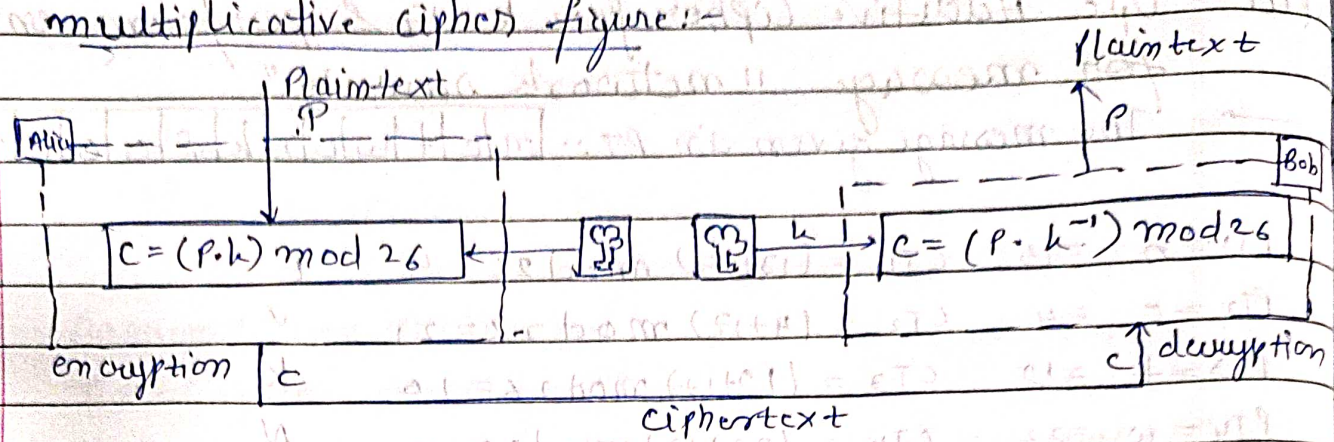
* multiplicative ciphers :-

- A multiplicative cipher, the encryption algorithm specifies multiplication of the plaintext by the key and decryption algorithm specifies division of the ciphertext by the key.
  - Since operations are in Z_{26}, decryption here means multiplying by the multiplicative inverse of the key.

note :- the key needs to belong to the set Z_{26}^* to guarantee that the encryption and decryption are inverse of each other.

Page No.
Date / /

multiplicative cipher figure:-



Que- Eve has interrupted a message CT = "UVACLYFZLJBYL" Now she can use BRUTE force attack method to get the plain text

→ k = 1, 2, 3, 4, 5 ---:

for k = 7 the text is been decrypted as follows:-

The given CT = {"UVACLYFZLJBYL"}

CT_1 = U	20	PT_1 = (20-7) mod 26 = 13	n
CT_2 = V	21	PT_2 = (21-7) mod 26 = 14	o
CT_3 = A	0	PT_3 = (0-7) mod 26 = 19	t
CT_4 = C	2	PT_4 = (2-7) mod 26 = 21	v
CT_5 = L	11	PT_5 = (11-7) mod 26 = 4	e
CT_6 = Y	24	PT_6 = (24-7) mod 26 = 17	r
CT_7 = F	5	PT_7 = (5-7) mod 26 = 24	y
CT_8 = Z	25	PT_8 = (25-7) mod 26 = 18	s
CT_9 = L	11	PT_9 = (11-7) mod 26 = 4	e
CT_{10} = J	9	PT_{10} = (9-7) mod 26 = 2	c
CT_{11} = B	1	PT_{11} = (1-7) mod 26 = 20	U
CT_{12} = Y	24	PT_{12} = (24-7) mod 26 = 17	r
CT_{13} = L	11	PT_{13} = (11-7) mod 26 = 4	e

PT = {not very secure}

To find multiplicative inverse of a no. $\boxed{(a \times b) \bmod n = 1}$

Page No.

Date / /

- Shift cipher ⇒ shift the character down during encryption process
[towards the end of alphabet lines]

- In multiplicative inverse the PT & CT are the integer in Z_{26} whereas the key is an integer in the set Z_{26}^* i.e the key is calculated using GCD.

- Thus the key domain is a set of integers that are relative prime no. or co-prime no. to 26. hence to find the GCD, we use euclidian Algorithm.

Z_{26}^* $\gcd(1,26) = 1$
$\gcd(2,26) = 2$ does not include in set as $\boxed{(a * b) \bmod n \neq 1}$
$\gcd(3,26) = 1$

Que- Use the multiplicative cipher to encrypt the message 'hello' with a key of $k = 7$

→ $PT_1 = h = 7$ $CT_1 = (7 \cdot 7) \bmod 26 = 23 = X$
$PT_2 = e = 4$ $CT_2 = (4 \cdot 7) \bmod 26 = 2 = C$
$PT_3 = l = 11$ $CT_3 = (11 \cdot 7) \bmod 26 = 25 = Z$
$PT_4 = l = 11$ $CT_4 = (11 \cdot 7) \bmod 26 = 25 = Z$
$PT_5 = o = 14$ $CT_5 = (14 \cdot 7) \bmod 26 = 20 = U$

$CT = \{XCZZU\}$

Affine Cipher

Page No.
Date / /

* monoalphabetic drawback:-
  - the repeat symbol are replaced by same.

* Polyalphabetic cipher technique:-
  - In polyalphabetic substitution, each occurence of a characters may have a different substitute.
  - The relationship between a characters in the plaintext to a character in the ciphertext is one-to-many.
  - It has the advantage of hiding the letter frequency of the underlying language.
  - In these method each plain-text character is replaced or substituted by a random letter or symbol / character using the key.
  - the various polyalphabetic cipher technique are as follows:-
    - Vigenere cipher
    - play fair substitution method
    - Hill cipher method
    - One time pad algorithm.

Page No.
Date / /

→ Vignere cipher method:-

Steps:- • In there method the length of the key and the plain text should be of same length or equal length. thus, the key is repeated to match the PT characters.

• following is the mathematical model or equation for the following :-

$E \Rightarrow C_i = [P_i + k_i] \bmod 26$ where, $i = 1$ to n

$D \Rightarrow P_i = [C_i - k_i] \bmod 26$ $k = [k_1, k_2 ---- k_n]$ (key space) domain

- Vigenere cipher method can use the following methods:-
  1) Using mathematical equation
  2) Using the tabular form
  3) Using Vigenere cipher table where CT is obtained through a pair of characters (PT & key)

Que- encrypt the message "she is listening" with the keyword PASCAL used Vignere cipher method to show the process

→ - the size of the keyword ⇒ $k = 6$ [P | A | S | C | A | L]

hence, $k_m = 6$ $\boxed{m = 6}$

- the word is repeated to the length of the plaintext as shown below:-

Plaintext:-

1	2	3	4	5	6	7	8	9	10	11	12	13	14
s	h	e	i	s	L	i	s	t	e	n	i	n	g
P	A	S	C	A	L	P	A	S	C	A	L	P	A
1	2	3	4	5	6	1	2	3	4	5	6	1	2

Now, PT is divided into six different block depending on the size of $k_m = 6$

Page No.
Date / /

- The block size is not fixed.

- the plain text which as '1' as position/key is considered as one block and so on:-

$PT_1 =$	s i n	$PT_4 =$	i e
$PT_2 =$	h s g	$PT_5 =$	s n
$PT_3 =$	e t	$PT_6 =$	l i

- from the above step each sub PT blocked is encrypted with a single key from the keyspace domain as shown below.

- As the plain text are '6' also the km = 6 hence the cipher text for further calculation is given as:-

$PT_1 =$ [s | i | n] $\}$ CT_1 (i → P)

$PT_5 =$ [s | n] $\}$ CT_5 (n → A)

$PT_2 =$ [h | s | g] $\}$ CT_2 (h → A)

$PT_6 =$ [l | i] $\}$ CT_6 (l → L)

$PT_3 =$ [e | t] $\}$ CT_3 (e → S)

$PT_4 =$ [i | e] $\}$ CT_4 (i → C)

Page No.
Date / /

- Using Vigenere mathematical equation:-

- $c_i = \{p_i + k_i\} \bmod 26$ using the Vigenere encryption mathematical equation.

- Convert each PT and k character into an integer value to get the respective CT following shows the above process:

- $PT_1 = \boxed{s \mid i \mid n}$

$\underbrace{s \mid i}_{P} \rightarrow 15$

$CT_{11} = 18 + 15 \bmod 26 = 33 \bmod 26 = 7 = H$

$CT_{12} = 8 + 15 \bmod 26 = 23 \bmod 26 = 23 = X$

$CT_{13} = 13 + 15 \bmod 26 = 28 \bmod 26 = 2 = C$

$CT_1 = \boxed{H \mid X \mid C}$

- $PT_2 = \boxed{h \mid s \mid g}$

$\underbrace{h \mid s}_{A}$

$CT_{21} = 7 + 0 \bmod 26 = 7 = H$

$CT_{22} = 18 + 0 \bmod 26 = 18 = S$

$CT_{23} = 6 + 0 \bmod 26 = 6 = G$

$CT_2 = \boxed{H \mid S \mid G}$

- $PT_3 = \boxed{e \mid t}$

$\underbrace{e \mid t}_{S} \quad 18$

$CT_{31} = 4 + 18 \bmod 26 = 22 = W$

$CT_{32} = 19 + 18 \bmod 26 = 11 = L$

$CT_3 = \boxed{W \mid L}$

- $PT_4 = \boxed{i \mid e}$

$\underbrace{i}_{C}$

$CT_{41} = 8 + 2 \bmod 26 = 10 = K$

$CT_{42} = 4 + 2 \bmod 26 = 6 = G$

$CT_3 = \boxed{K \mid G}$

$PT_5 = \boxed{s \mid n}$

$\underbrace{s}_{A} \quad 0$

$CT_{51} = 18 + 0 \bmod 26 = 18 = S$

$CT_{52} = 13 + 0 \bmod 26 = 13 = N$

$CT_5 = \boxed{S \mid N}$

$PT_6 = \boxed{d \mid i}$

$CT_{61} = 11 + 11 \bmod 26 = 22 = W$

$CT_{62} = 8 + 11 \bmod 26 = 19 = T$

$CT_6 = \boxed{W \mid T}$

* talular method:-

Plain text	s	h	e	i	s	l	i	s	t	e	n	i	n	g
Values	18	7	4	8	18	11	8	18	19	4	13	8	13	6
k values	15	0	18	2	0	11	15	0	18	2	0	11	15	0
ciphertext	H	H	W	K	S	W	X	S	C	G	N	T	C	G

→ play fair cipher method :-

- In these method the key which is made up of 26 alphabets letters are arranged in 5x5 matrix where the alphabets I and J are considered in the same matrix cell.

- As (I/J) during encryption process.
  ex:- let the keywords = MONARCHY

note:- - if there are repeated characters in the given keyword, then it should not be repeated in the matrix.
- rest of the matrix cell are filled with the alphabet 'A' to 'Z' again without repeating the same character or alphabet in the final matrix:-

following shows the example:-

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

Page No.
Date / /

- before encryption the point is ~~observed~~ divided into pair of letters known as ~~Digraph~~ Di-graph.

- before encryption if the 2 letters in a pair are the same, a ___ letter is inserted to seperate them.

- After inserting ___ letter, if the number of characters in the plaintext is odd, one extra ___ character is added at the end to make the no. of characters.

Step: 3:- The Cipher uses a 3 rules for encryption.

a) If the 2 letters in a pair are located in the same row of the secret key, the corresponding encrypted character for each letter in the next letter to the right in the same row (with wrapping to the begining of the row if the plain text letter is the last character in the row)

b) If the 2 letters in a pair are located in the same column of the secret key, the corresponding encrypted character for each letter is the letter beneath it in the same, column (with wrapping to the begining

Page No.
Date / /

of the point the last character in the column)

c) If the 2 letter in a pair are not in the same row or column of the secret, the corresponding encrypted character for each letter is a letter that is in its own row but in the same column as the other letter.

Di-graph → let the point ⇒ Attack

Di-graph →	at	ta	ck
ct →	RS	SR	DE

let the point = MasQuE use the previous key to find the city.

Diagraph →	MO	SQ	UE
ct →	ON	TS	ML

Page No.
Date / /

Que-2) Encrypt the Message = "Hide the gold under the carpet" using play fair technique with the keyword "NETWORK SECURITY"

→ Keyword – NETWORKSECURITY

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

Digraph:- Hp de th eg ol lu nd cr th cc ar pe tx

Ct:- FA YO SV KQ WM MD OI/J NK SV WV I/JS ON WV

Que-

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

Digraph → Th ek ey is Hi dx de nu nd er th ed ox or PA dx

Ct → PO CL BX DR Lg I/JY I/JB CY BY LX PO BI/J LI LT TG I/JY

Page No.
Date / /

Que-3] Encrypt the message the "The key is Hidden under the door password". using key = "GUIDANCE" use playfair technique to get it.

Que-4) encrypt the message = "The House is being sold tonight" use the given key word =

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

Diagraph →	TH	EH	OU	SE	is	be	in	gs	ol	olt	on	pg	Ht
	WE	GE	XI/J	OH	NO								

Page No.
Date / /

Mathematics of Cryptography

1) Integer arithmathic

$Z = \{$ all the values $\}$

- -ve values
- 0 value
- +ve values

2) Modular arithmatic

(a) if we divide 'a' by 'n', we get 'q' and 'r' $\boxed{a = q \times n + r}$ $\{a \bmod n = r\}$

3) if $a \neq 0$ and let $r = 0$ than the division relation we get as $\boxed{a = q \times n}$

* Inverse :-
  - additive inverse :- (relative to an addition operation)
  - multiplicative inverse :- (relative to a multiplication operation)

+ → additive inverse :-

In Z_n, two numbers a and b are additive inverse of each others if $a + b \equiv 0 \pmod{n}$

- In Z_n, the additive inverse of a can be calculated as $b = n - a$.

for ex:- the additive inverse of 4 in Z_{10} is $10 - 4 = 6$.

Page No.
Date / /

→ Multiplicative Inverse:-
In Z_n, two numbers a and b are the multiplicative inverse of each other if
$$a \times b \equiv 1 \pmod{n}$$
for example:- if the modulus is 10, then the multiplicative inverse of 3 is 7. In other words, we have $(3 \times 7) \bmod 10 = 1$.

* greatest common divisor:- [GCD]
  - factorization (prime)
  - co-prime / relative prime no.

- Since we know that to find GCD prime factorization is the manual method at it takes lot of time and space for large numbers

- It was developed by famous mathematician euclid so, as to generate GCD of two large numbers quickly and efficiently.

- the various application of euclidian algorithm are as follows:-
  - to get the distance between two points required for clustering and classification algorithm
  - image processing techniques.
  - to generate shortest route between the nodes
  - antenna & communication systems etc.

Page No.
Date / /

- euclidian algorithm is based on the following facts :-

FACT1 : $\gcd(a, 0) = a$

FACT2 : $\gcd(a,b) = \gcd(b, r)$ - { where 'r' is the remainder of $a|b$ }

for example : - calculate $\gcd(36, 10)$

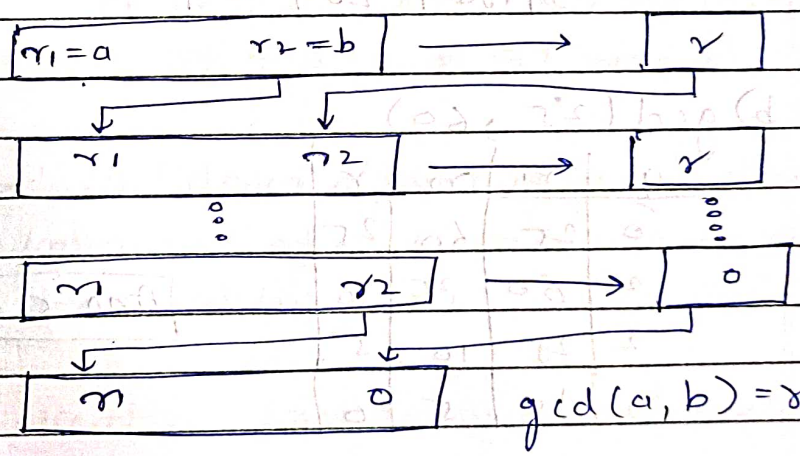
→ using fact 2 :-

$$\gcd(36,10) = \gcd(10,6)$$
$$= \gcd(6,4) = \gcd(4,2)$$
$$\gcd(2,0) = 2$$

$$\boxed{\therefore \gcd(36,10) = 2}$$

* following shows the euclidian algorithm and the process when we need to find gcd of two large numbers

process :- (a)



(b) Algorithm :-

```
r1 ← a ; r2 ← b; (Initialization)
while (r2 > 0)
  { q ← r1/r2;
    r ← r1 - q × r2;
    r1 ← r2 ; r2 ← r;
  }
gcd(a,b) ← r1
```

Page No.
Date / /

Que - find the gcd of 2740 and 1760 using euclidian method :-

a) 2740, 1760
b) 25 & 60
c) 300 & 42
d) 24 & 320
e) 88 & 220
f) 401 & 700

→ a) gcd (2740, 1760)

q	r_1	r_2	r
1	2740	1760	980
2	1760	980	780
1	980	780	200
3	780	200	180
1	200	180	20
9	180	20	0

$\boxed{\text{Ans} - 20}$

b) gcd (25, 60)

q	r_1	r_2	r
0	25	60	25
2	60	25	10
2	25	10	5
2	10	5	0

$\boxed{\text{Ans} - 5}$

c) gcd (88 & 220)

q	r_1	r_2	r
0	88	220	88
2	220	88	44
2	88	44	0

$\boxed{\text{Ans} - 44}$

d) 300 & 42

q	r_1	r_2	r
7	300	42	6
7	42	6	0

$\boxed{\text{Ans} - 6}$

e) gcd (24 & 320)

q	r_1	r_2	r
0	24	320	24
13	320	24	8
3	24	8	0

$\boxed{\text{Ans} - 8}$

Page No.
Date / /

f) gcd(401 & 700)

q	r_1	r_2	r
0	401	700	401
1	700	401	299
1	401	299	102
2	299	102	95
1	102	95	7
13	95	7	4
1	7	4	3
1	4	3	1
3	3	1	0

* extended euclidian algorithm:-

- The integer a in Z_n has a multiplicative inverse if and only if $\gcd(n, a) \equiv 1 \pmod{n}$

- The extended euclidean algorithm finds the multiplicative inverses of b in Z_n when n and b are given and $\gcd(n, b) = 1$

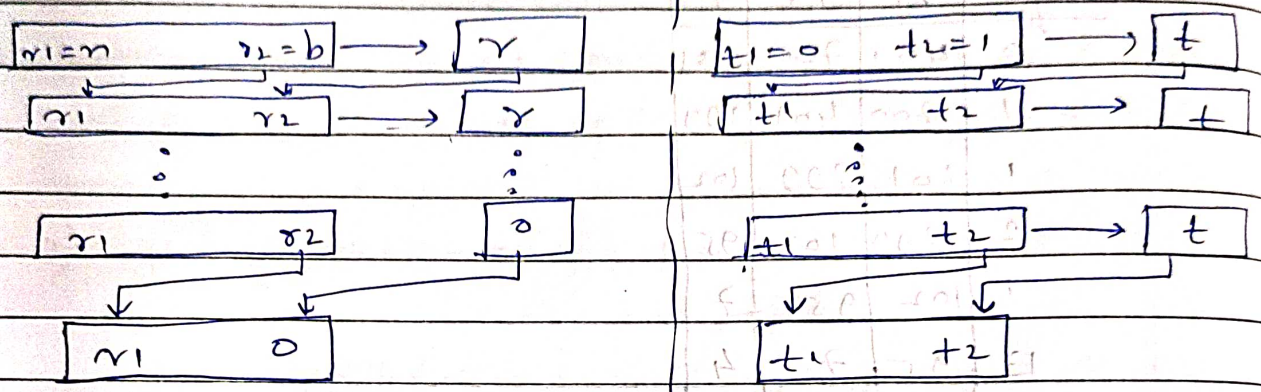
- The multiplicative inverse of b is the value of t after being mapped to Z_n.

- following figure shows how we find the multiplicative inverse of a number using the extended euclidian algorithm :-

Page No.

Date / /

(a) Process:—



$\gcd(n, b) = r_1$

if $r_1 = 1$, $b^{-1} = t_1$

(b) Algorithm:—

```
r1 ← n ; r2 ← b;
t1 ← 0 ; t2 ← 1;
while (r2 > 0)
{ q ← r1/r2;
  r ← r1 − q × r2;
  r1 ← r2 ; r2 ← r;

  t ← t1 − q × t2;
  t1 ← t2 ; t2 ← t;
}
if (r1 = 1) then b^-1 ← t1
```

Page No.
Date / /

Que- find the multiplicative inverse of 11 in Z26

→ gcd (n,b) = 1 n = 26, b = 11

q	r1	r2	r	t1	t2	t
2	26	11	4	0	1	-2
2	11	4	3	1	-2	5
1	4	3	1	-2	5	-7
3	3	1	0	5	-7	26

$\begin{array}{r} 27 \\ -7 \\ \hline 19 \end{array}$

∴ 19 is MI of 11 in Z26

Que- find the multiplicative inverse for the following:-

a) 3 in Z10

3 in Z10 gcd (10, 3) n = 10 b = 3

q	r1	r2	r	t1	t2	t
3	10	3	1	0	1	-3
3	3	1	0	1	-3	10

$\begin{array}{r} 10 \\ -3 \\ \hline 7 \end{array}$

∴ 7 is MI of 10 in Z26

b) 11 in Z13

11 in Z10 gcd (13, 11) n = 13 b = 11

q	r1	r2	r	t1	t	t

Page No.

Date / /

- * Another application of extended euclidian algorithm is used to solve linear diophantine equation of the form $ax + by = c$ where, c is divisible by $\gcd(a,b)$ for performing encryption and decryption of the message.

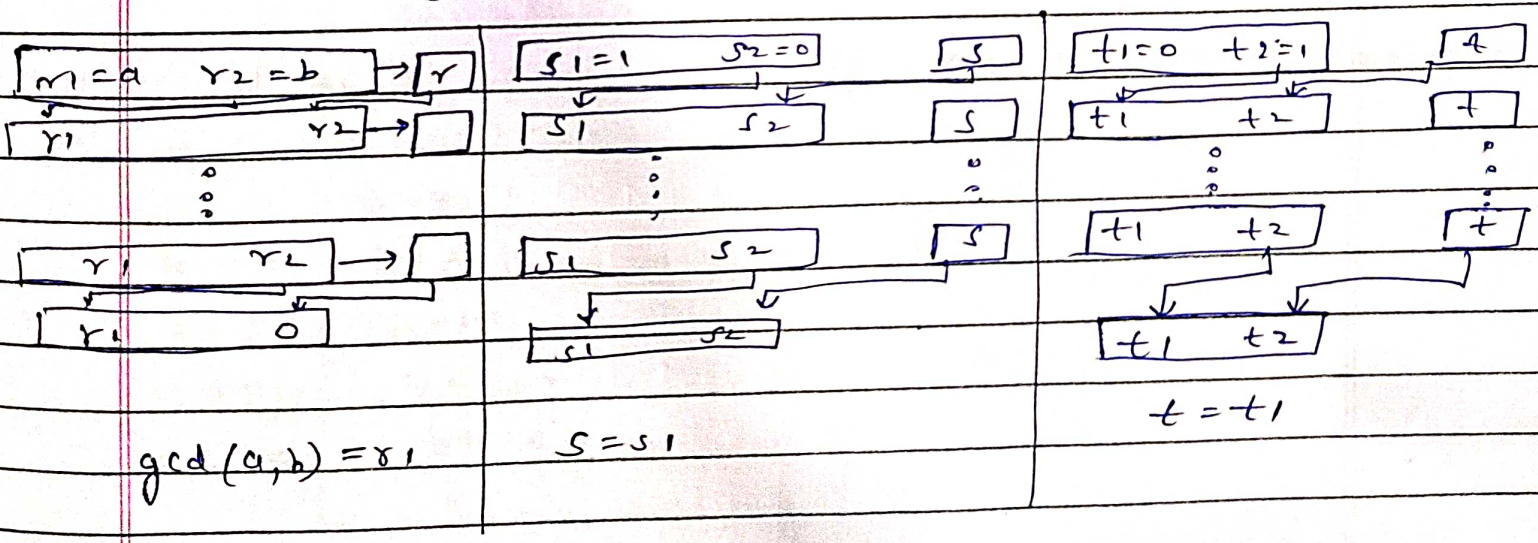
- from the above equations the variables 'x' and 'y' is extended euclidian algorithm is represented by variables 's' and 't' known as Bezout coefficients.

- Given two integers a and b, we often need to find other two integers, s and t, such that:-

$$s \times a + t \times b = \gcd(a,b)$$

the extended euclidean algorithm can calculate the gcd (a,b) and at the same time calculate the value of s and t.

following shows the process:- (a)



Page No.
Date / /

(b) Algorithm:-

$r_1 \leftarrow a$; $r_2 \leftarrow b$;

$s_1 \leftarrow 1$; $s_2 \leftarrow 0$; (Initialization)

$t_1 \leftarrow 0$; $t_2 \leftarrow 1$;

while $(r_2 > 0)$

{ $q \leftarrow r_1 / r_2$;

$r \leftarrow r_1 - q \times r_2$; (updating r's)

$r_1 \leftarrow r_2$; $r_2 \leftarrow r$;

$s \leftarrow s_1 - q \times s_2$; (updating s's)

$s_1 \leftarrow s_2$; $s_2 \leftarrow s$;

$t \leftarrow t_1 - q \times t_2$; (updating t's)

$t_1 \leftarrow t_2$; $t_2 \leftarrow t$;

}

$\gcd(a,b) \leftarrow r_1$; $s \leftarrow s_1$; $t \leftarrow t_1$

Page No.

Date / /

Que- given $a = 161$, $b = 28$ find gcd(a, b) & calculate values of 's' & 't'

→ gcd(161, 28)

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
	161	.							

Que- find gcd(a, b) and values of s and t for the following:-

→ $a = 17$ $b = 0$ — 17

$a = 0$ $b = 45$

$a = 4$ $b = 7$

$a = 291$ $b = 42$

$a = 84$ $b = 320$

$a = 400$ $b = 60$

$* \longrightarrow$ EEA
$+ \longrightarrow$ additive

Page No.
Date / /

* multiplicative cipher :-

encryption: $C = \{P * k\} \bmod 26$ decryption:- $P = \{C * k^{-1}\} \bmod 26$

Que - encrypt the message "PK" using multiplicative cipher method decrypt the same to get the original message {with $k = 7$}

$\longrightarrow$

- encryption :-

$PT = \boxed{P \mid k} \Rightarrow \boxed{15 \mid 10}$

$CT_1 = \{15 * 7\} \bmod 26 = 1$

$CT_2 = \{10 * 7\} \bmod 26 = 18$

$\therefore CT = \boxed{\overset{1}{B} \mid \overset{18}{S}}$

- decryption:- $P = \{C * k^{-1}\} \bmod 26$

{hence, 7^{-1} in $Z_{26} = 15$}

- 7 in Z_{26} is:

q	r_1	r_2	r	t_1	t_2	t

$PT_1 = \{1 * 15\} \bmod 26 = 15$

$PT_2 = \{18 * 15\} \bmod 26 = 10$

$\therefore PT = \boxed{\overset{15}{P} \mid \overset{10}{K}}$

Page No.
Date / /

Que- decrypt the message XCZZU with k = 7 using multiplicative cipher method.

→

given:- CT = | X | C | Z | Z | U | ⇒ | 23 | 2 | 25 | 25 | 20 |

$PT1 = \{23 * 15\} \bmod 26 \Rightarrow 7 \rightarrow H$

$PT2 = \{2 * 15\} \bmod 26 \Rightarrow$

$PT3 = \{25 * 15\} \bmod 26 \Rightarrow$

$PT4 = \{25 * 15\} \bmod 26 \Rightarrow$

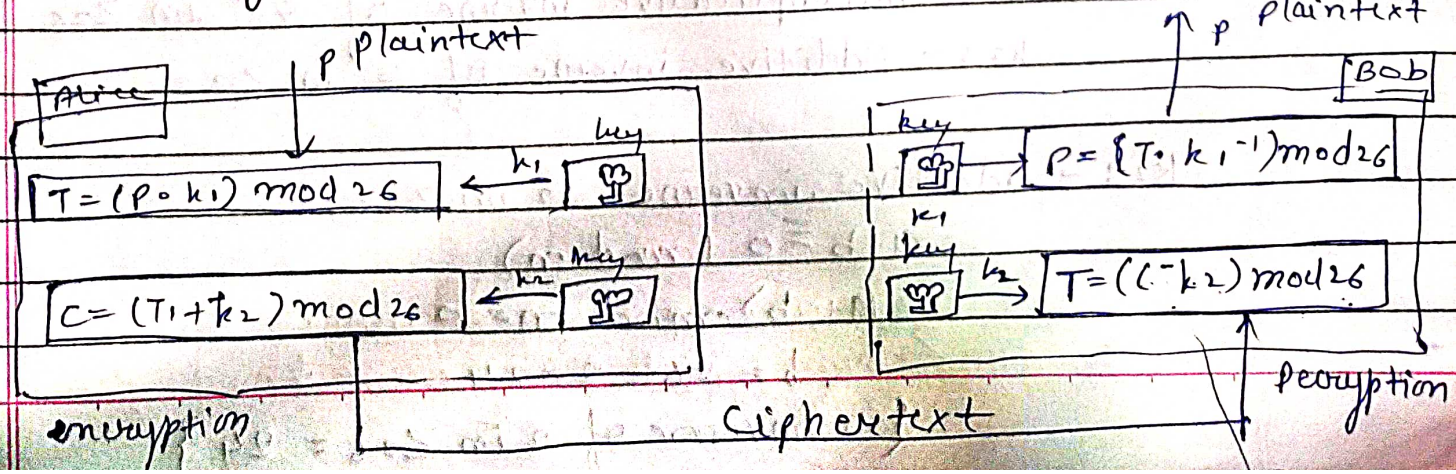
$PT5 = \{20 * 15\} \bmod 26 \Rightarrow$

∴ PT = | | | | | |

* Affine Cipher:-

- it is a combination of additive & multiplicative Cipher.
- Uses a pair of key perform encryption & decryption process ⇒ $k = \{k_1, k_2\} \rightarrow A$
- the first key uses multiplicative cipher and the second key uses additive cipher.
- if $k = \{k_1, k_2\}$ were k_1 = multiplicative, k_2 = additive

- following figure show the above process:-



Page No.
Date / /

- In the affine cipher, the relationship between the plaintext P and the cipher text is:-

$C = (P \times k_1 + k_2) \bmod 26$ $\qquad$ $P = ((C - k_2) \times k_1^{-1}) \bmod 26$

where k_1^{-1} is the multiplicative inverse of k_1 and k_2 is the additive inverse of k_2

Que:- Use an affine cipher to encrypt the message "Hello" with the keypair (7, 2)

→ Step 1:- Integer value of the plaintext:-

PT:- | h | e | l | l | o | ⇒ | 7 | 4 | 11 | 11 | 14 |

encryption:-

$C = (P \times k_1 + k_2) \bmod 26$

$CT_1 = (7 \times 7 + 2) \bmod 26 = (49 + 2) \bmod 26 = 51 \bmod 26 = 25 = Z$

$CT_2 = (4 \times 7 + 2) \bmod 26 = (30) \bmod 26 = 4 = E$

$CT_3 = (11 \times 7 + 2) \bmod 26 = 79 \bmod 26 = 1 = B$

$CT_4 = (11 \times 7 + 2) \bmod 26 = 79 \bmod 26 = 1 = B$

$CT_5 = (14 \times 7 + 2) \bmod 26 = 100 \bmod 26 = 22 = W$

CT = | Z | E | B | B | W |

decryption:-

k_1:- multiplicative inverse of 7^{-1} in Z_{26}

k_2:- Additive inverse of 2 in Z_{26}

k_2:- additive inverse (2 in Z_{26})

$a + b \equiv 0 \pmod n$

$(a + b) \bmod n = 0$

$b = 26 - 2 = 24$

{∴ inverse of 2 in Z_{26} = 24}

Page No.
Date / /

k_1 :- multiplicative inverse of 7^{-1} in 15 :-

q	r_1	r_2	r	t_1	t_2	t
3	26	7	5	0	1	-3
1	7	5	2	1	-3	4
2	5	2	1	-3	4	-11
2	2	1	0	4	-11	26

$$\begin{array}{r} 26 \\ -11 \\ \hline 15 \end{array}$$

Z in Z_{26} = 15

	25	4	1	1	22
CT =	Z	E	B	B	W

formula :- $P = (c + (-k_2)) \bmod 26$

$P^* = (P \cdot k^{-1}) \bmod 26$

$-k_2$:- is the additive inverse which is 24

$-k_1$:- is the multiplicative inverse which is 15

- $CT_1 = Z = 25$

  $PT_1 = (25 + 24) \bmod 26 = 23$

  $PT_1^* = (23 \cdot 15) \bmod 26 = 7$

  $CT_1 = 7$

- $CT_2 = E = 4$

  $PT_2 = (4 + 24) \bmod 26 = 2$

  $PT_2^* = (2 \cdot 15) \bmod 26 = 4$

  $CT_2 = 4$

- $CT_3 = B = 1$

  $PT_3 = (1 + 24) \bmod 26 = 25$

  $PT_3^* = (25 \cdot 15) \bmod 26 = 11$

  $CT_3 = l$

- $CT_4 = B = 1$

  $PT_3 = (1 + 24) \bmod 26 = 25$

  $PT_3^* = (25 \cdot 15) \bmod 26 = 11$

  $CT_4 = l$

- $CT_5 = W = 22$

  $PT_5 = (22 + 24) \bmod 26 = 20$

  $PT_5^* = (20 \cdot 15) \bmod 26$

  $CT_5 = 14$

hence, $PT_I = 4, 11, 11, 14$

h	e	l	l	o

Page No.
Date / /

Que- encrypt the message "this is an exercise" using one of the following ciphers. Ignore the space between words decrypt message to get the original plaintext.

→ a) Affine cipher with key = (15, 20)

$k_1 = 15 \quad k_2 = 20$

k_1 :- multiplicative inverse 15 in Z26

q	r_1	r_2	r	t_1	t_2	t
1	26	15	11	0	1	-1
0	15	26	15	1	-1	2
1	26	15	11	1	2	-1
1	15	11	4	2	-1	3
2	11	4	3	-1	3	-7
1	4	3	1	3	-7	10
3	3	1	0	-7	10	-37

$26 - 7 = 19$

k_2 :- additive inverse 20 in Z26

$(a+b) \bmod 26 = 0$

$b = 26 - 20 = 6$

Page No.
Date / /

* One time pad [OTP] method :-

- These method is an advanced method of Vernam cipher
- In vernam cipher method, length of the keyword length of plain text.
- In these method we work on binary bits rather than character of symbol or letter.
- Same key is used for performing encryption and decryption.
- The mathematical equation for encryption is given as :-

$E \Rightarrow C_i = P_i \oplus k_i$ $\quad \oplus \rightarrow$ 'x' or truth table

$D \Rightarrow P_i = C_i \oplus k_i$

- Thus the bits are Exord during the process:-

0	0	→	0
0	1	→	1
1	0	→	0
1	1	→	0

- In OTP method it also works on the binary bits format the key is randomly generated as long as the length of the PT.

- The key is discarded or use only "one time" during encryption and decryption process. every new message required the use of new key of the same length.

- The values are assigned using ASCII chart code user can build their own chart for communication

Page No.
Date / /

- Hill Cipher method :-
  - In these method, the plaintext divide into blocks(l) of equal size, where each block consist of 'm' charactors.

  - The key is a square matrix of size $m \times m$.
  - Each block is encrypted one at a time.
  - Hill cipher is also known as block cipher.
  - the encryption equation is given by :-

    $C = (P * k) \bmod 26$ were, $C = CT$, $P = PT$, $k = key$

  - the decryption equation is given by :-

    $P = (C * k^{-1}) \bmod 26$

  were k^{-1} is the inverse of the keywords and it should be solved using the following equation.

  $k^{-1} = \left(\frac{1}{|k|} * \text{Adjoint } k \right) \bmod 26$

  $|k| \rightarrow$ determinant

  $\frac{1}{|k|} = |k|^{-1}$ — {EEA}

- After finding k^{-1} it is applied to the decryption equation to get back the original message.

Que :- Encryption PT = "attack" key = $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$ using Hill cipher method. Show the decryption also.

→

Page No.
Date / /

decryption :- $n=15$ $k=5$

CT = MEEEAPATATTRMHR

$n=3$ $r=0$

2	5	3	1	5
M	E	E	T	H
E	A	T	T	M
E	P	A	R	R

PT :- meet me at the park.

* Combining Two approaches or (Hybrid approach) :-

In these method encryption and decryption are done in three steps :-

keyless ✓ 1) The ~~tex~~ plain text is written in a table row-by-row

keyed ✓ 2) permutation is done coloumn by coloum of the given key.

keyless ✓ 3) New table is created and read coloum by coloum

→ from the above steps first and third is a key less approach were as step-2 is keyed approach.

Q— let the plain text be "enemy attacks to night" with the permutation key = 5.

→ Step1 :- PT = enemy attacks to night

e	n	e	m	y		a	t	t	a	c		k	s	t	o	n		i	g	h	t	z

Dummy char

encryption :-

Step2 :- Convert the table into row-by-row.

1	2	3	4	5
e	n	e	m	y
a	t	t	a	c
k	s	t	o	n
i	g	h	t	z

Page No.
Date / /

Step-3] Permutation is done coloumby columby the given key:-

permutation key:-

encryption ↓

3	1	4	5	2
1	2	3	4	5

↑ decryption

3	1	4	5	2
e	e	m	y	n
t	a	a	c	t
t	k	o	n	s
h	i	t	2	g

Step-4] Read ~~row~~ coloum by ~~row~~ coloum as the new table is created and the cipher text is:-

CT:- ETTH EAKI MAOT YCN2NTSG

Step1:-

decryption:- CT:- ETTH EAKI MAOT YCN2NTSG

E	T	T	H	E

A	K	I	A	A

O	T	Y	C	N

2	N	T	S	G

Step2:- convert the table into coloum by column:-

1	E	A	O	2
2	T	K	T	N
3	T	I	Y	T
4	H	M	C	S
5	E	A	N	G

E	E	M	Y	N
T	A	A	C	T
T	K	O	N	S
H	I	T	2	G

Page No.
Date / /

2M/ How can the decryption key be created if the encryption key is given or vice versa

Que - write an algorithm for the key of given key.

- following figure shows the key inversion in a transposition cipher.

encryption key

2	6	3	1	4	7	5

4	1	3	5	7	2	6

decryption key

2	6	3	1	4	7	5	Add
1	2	3	4	5	6	7	index
1	2	3	4	5	6	7	swap
2	6	3	1	4	7	5	
4	1	3	5	7	2	6	sort
1	2	3	4	5	6	7	

(a) Manual process

Page No.
Date / /

(b) Algorithm

given: Enckey [index]

```
index ← 1
while (index ≤ column)
{
    Deckey [Enckey [index]] ← index
    index ← index + 1
}
Return : DecKey [index]
```

(b)

Que - The given encryption key is 3, 2, 6, 1, 5, 4 find the decryption key in the transportation cipher

→

encryption key

3	2	6	1	5	4

4	2	1	6	5	3

3	2	6	1	5	4	Add
1	2	3	4	5	6	index
1	2	3	4	5	6	swap
3	2	6	1	5	4	
4	2	1	6	5	3	sort
1	2	3	4	5	6	

Page No.
Date / /

Encrypt and decrypt process for a transposition cipher using matrix :-

Step 1:- The PT and CT are $l \times m$ matrix representing the numerical value of the given character.

Step 2:- The key is a square matrix of size $m \times n$

Step 3:- The permutation matrix is design in such a way that every row or colour has only ~~one~~ '1' and rest of all zeros.

Step 4:- encryption is performed by multiplying the plaintext by the key matrix to get the cipher text matrix

Step 5:- Decryption is performed by multiplying the CT matrix with the inverse of the key matrix to get PT matrix.

NOTE There is no need to encrypt the matrix hence the encryption key matrix can be simply transpose to get the decryption key matrix

Page No.
Date / /

Que:- encryption key in a transposition cipher is given as 3, 2, 6, 1, 5, 4 design the inverse matrix and represent the same.

→ Key:- 3 2 6 1 5 4

3	2	6	1	5	4

↓

encryption key:

0	0	0	1	0	0
0	1	0	0	0	0
1	0	0	0	0	0
0	0	0	0	0	1
0	0	0	0	1	0
0	0	1	0	0	0

Inverse Decryption key:-

1	0	0	1	0	0	0
2	0	1	0	0	0	0
3	0	0	0	0	0	1
4	1	0	0	0	0	0
5	0	0	0	0	1	0
6	0	0	0	1	0	0

decryption key:- 4 2 1 6 5 3

Que:- the decryption key is given as 2, 5, 1, 3, 4 design the encryption key using matrix method.

→ decryption key:-

2	5	1	3	4
0	0	1	0	0
1	0	0	0	0
0	0	0	1	0
0	0	0	0	1
0	1	0	0	0

⇒

1	0	1	0	0	0
2	0	0	0	0	1
3	1	0	0	0	0
4	0	0	1	0	0
5	0	0	0	1	0

encryption key:- 3 1 4 5 2