Assignment 1

Page No.
Date :

1. Apply Extended Euclid algorithm to compute GCD (99, 78). Show all the computations.

Ans GCD(99, 78) using EEA

Q	A	B	R
1	99	78	21
3	78	21	15
1	21	15	6
2	15	6	3
1	6	3	0
	3	0	

⇒ Computations

$a = b * q + r$

→ $99 = 78 \times 1 + 21$

→ $78 = 21 \times 3 + 15$

→ $21 = 15 \times 1 + 6$

→ $15 = 6 \times 2 + 3$

→ $6 = 3 \times 2 + 0$

2 a) What is Vigenere Cipher ? Explain its working using suitable example.

Ans • Vigenere Cipher is a method of encrypting alphabetic text.

• It uses a simple form of polyalphabetic substitution

• A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets.

• The encryption of the original text is done using the Vigenere square or Vigenere table

— The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar Ciphers.

— At different points in the encryption process, the cipher uses a different alphabet

from one of the rows.

- The alphabet used at each point depends on a repeating keyword.

Example

Plain Text : GIVE MONEY

Key : LOCK

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

Encryption

PT: G I V E M O N E Y
6 8 21 4 12 14 13 4 24

K: L O C K L O C K L
11 14 2 10 11 14 2 10 11

17 22 23 14 23 28 mod 26 15 14 35 mod 26

9

R W X O X Z P O I

Z

Page No.
Date :

Cipher Text: RWXOXCPOJ

Decryption

CT:	R	W	X	O	X	C	P	O	J
	17	22	23	14	23	2	15	14	9
K:	L	O	C	K	L	O	C	K	L
	11	14	2	10	11	14	2	10	11
	6	8	21	4	12	-12	13	4	-2
						mod 26			mod 26
	G	I	V	E	M	14	N	E	24
						O			Y

Plain Text: GIVE MONEY

2b) Demonstrate the working of encryption and decryption procedure in Hill Cipher with respect to following parameters:

Key: $\begin{bmatrix} 7 & 8 \\ 19 & 3 \end{bmatrix}$

Plain Text: ACOLLEGE

Sol $K = \begin{bmatrix} 7 & 8 \\ 19 & 3 \end{bmatrix}$

Plain Text: AC OL LE GE

$\begin{bmatrix} A \\ C \end{bmatrix} \begin{bmatrix} O \\ L \end{bmatrix} \begin{bmatrix} L \\ E \end{bmatrix} \begin{bmatrix} G \\ E \end{bmatrix}$

* Hill Cipher – Encryption

$\Rightarrow CT = PT * K \bmod 26$

i) For $\begin{bmatrix} A \\ C \end{bmatrix} \rightarrow \begin{bmatrix} 0 \\ 2 \end{bmatrix}$

$= \begin{bmatrix} 0 \\ 2 \end{bmatrix} \begin{bmatrix} 7 & 8 \\ 19 & 3 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 0*7 + 2\times8 \\ 0\times19 + 2\times3 \end{bmatrix} \bmod 26$

$$= \begin{bmatrix} 16 \\ 6 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 16 \\ 6 \end{bmatrix} \Rightarrow \begin{bmatrix} Q \\ G \end{bmatrix}$$

ii) For $\begin{bmatrix} O \\ L \end{bmatrix} \rightarrow \begin{bmatrix} 14 \\ 11 \end{bmatrix}$

$$= \begin{bmatrix} 14 \\ 11 \end{bmatrix} \begin{bmatrix} 7 & 8 \\ 19 & 3 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 14 \times 7 + 11 \times 8 \\ 14 \times 19 + 11 \times 3 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 186 \\ 299 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 4 \\ 13 \end{bmatrix} \Rightarrow \begin{bmatrix} E \\ N \end{bmatrix}$$

Page No.
Date :

iii) For $\begin{bmatrix} L \\ E \end{bmatrix} \rightarrow \begin{bmatrix} 11 \\ 4 \end{bmatrix}$

$= \begin{bmatrix} 11 \\ 4 \end{bmatrix} \begin{bmatrix} 7 & 8 \\ 19 & 3 \end{bmatrix} \text{ mod } 26$

$= \begin{bmatrix} 11 \times 7 & +4 \times 8 \\ 11 \times 19 & +4 \times 3 \end{bmatrix} \text{ mod } 26$

$= \begin{bmatrix} 109 \\ 221 \end{bmatrix} \text{ mod } 26$

$= \begin{bmatrix} 5 \\ 13 \end{bmatrix} \Rightarrow \begin{bmatrix} F \\ N \end{bmatrix}$

iv) For $\begin{bmatrix} G \\ E \end{bmatrix} \Rightarrow \begin{bmatrix} 6 \\ 4 \end{bmatrix}$

$= \begin{bmatrix} 6 \\ 4 \end{bmatrix} \begin{bmatrix} 7 & 8 \\ 19 & 3 \end{bmatrix} \text{ mod } 26$

$= \begin{bmatrix} 6 \times 7 & +4 \times 8 \\ 6 \times 19 & +4 \times 3 \end{bmatrix} \text{ mod } 26$

$= \begin{bmatrix} 74 \\ 126 \end{bmatrix} \text{ mod } 26$

$= \begin{bmatrix} 22 \\ 22 \end{bmatrix} \Rightarrow \begin{bmatrix} W \\ W \end{bmatrix}$

Cipher Text ⇒ Q G E N F N W W

* Hill Cipher – Decryption

$PT = CT * K^{-1} \bmod 26$

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

$|K| = \begin{vmatrix} 7 & 8 \\ 19 & 3 \end{vmatrix} = |21 - 152|$

$= |-131|$

$|K| = -131$

* Rule – $a \bmod b = 1$

$gcd(a, b) = 1$

$131 \times (1) \bmod 26 = 1$

$\frac{1}{|K|} = -1 * 1 = -1$

adj(K)

$$K = \begin{bmatrix} 7 & 8 \\ 19 & 3 \end{bmatrix}$$

$$adj(K) = \begin{bmatrix} 3 & -8 \\ -19 & 7 \end{bmatrix}$$

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

$$= -1 * \begin{bmatrix} 3 & -8 \\ -19 & 7 \end{bmatrix} = -1 \begin{bmatrix} 3 & -8 \\ -19 & 7 \end{bmatrix}$$

$$K^{-1} = \begin{bmatrix} -3 & +8 \\ +19 & -7 \end{bmatrix} \times -1 = \begin{bmatrix} -3 & 8 \\ 19 & -7 \end{bmatrix}$$

to avoid -ve no just add +20 to -ve no.

$$K^{-1} = \begin{bmatrix} -3+26 & +8+26 \\ +19+26 & -7+26 \end{bmatrix} = \begin{bmatrix} -3+26 & 8 \\ 19 & -7+26 \end{bmatrix}$$

$$K^{-1} = \begin{bmatrix} 23 & 8 \\ 19 & 19 \end{bmatrix}$$

i) For $\begin{bmatrix} Q \\ G \end{bmatrix} \Rightarrow \begin{bmatrix} 16 \\ 6 \end{bmatrix}$

$$= \begin{bmatrix} 16 \\ 6 \end{bmatrix} \begin{bmatrix} 23 & 8 \\ 19 & 19 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 16 * 23 + 6 * 8 \\ 16 * 19 + 6 * 19 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 416 \\ 418 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 0 \\ 2 \end{bmatrix}$$

$$= \begin{bmatrix} A \\ C \end{bmatrix}$$

ii) For $\begin{bmatrix} E \\ N \end{bmatrix} \rightarrow \begin{bmatrix} 4 \\ 13 \end{bmatrix}$

$$= \begin{bmatrix} 4 \\ 13 \end{bmatrix} \begin{bmatrix} 23 & 8 \\ 19 & 19 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 4 * 23 + 13 * 8 \\ 4 * 19 + 13 * 19 \end{bmatrix}$$

$$= \begin{bmatrix} 196 \\ 323 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 14 \\ 11 \end{bmatrix}$$

$$= \begin{bmatrix} O \\ L \end{bmatrix}$$

iii) For $\begin{bmatrix} F \\ N \end{bmatrix} \rightarrow \begin{bmatrix} 5 \\ 13 \end{bmatrix}$

$$= \begin{bmatrix} 5 \\ 13 \end{bmatrix} \begin{bmatrix} 23 & 8 \\ 19 & 19 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 5*23 + 13*8 \\ 5*19 + 13*19 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 219 \\ 342 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 11 \\ 4 \end{bmatrix}$$

$$= \begin{bmatrix} L \\ E \end{bmatrix}$$

iv) For $\begin{bmatrix} W \\ W \end{bmatrix} \rightarrow \begin{bmatrix} 22 \\ 22 \end{bmatrix}$

$$= \begin{bmatrix} 22 \\ 22 \end{bmatrix} \begin{bmatrix} 23 & 8 \\ 19 & 19 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 22 * 23 + 22 * 8 \\ 22 * 19 + 22 * 19 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 682 \\ 836 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 6 \\ 4 \end{bmatrix}$$

$$= \begin{bmatrix} G \\ E \end{bmatrix}$$

Decrypted / Plain Text = "A COLLEGE"

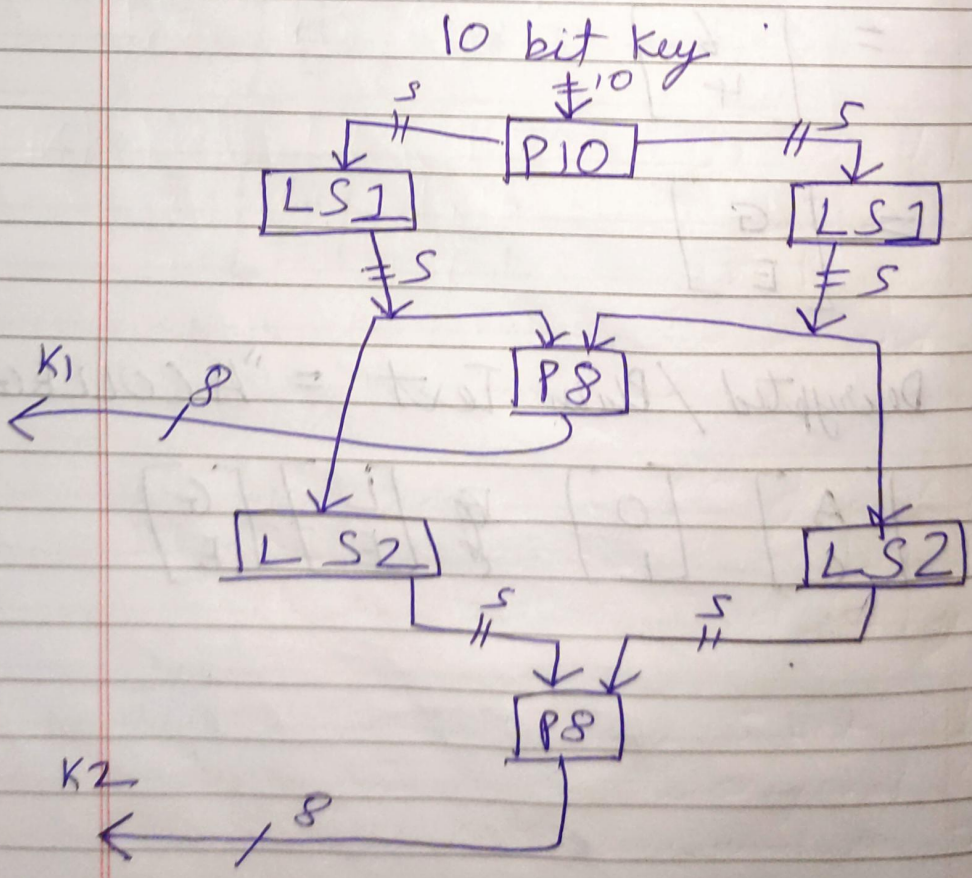
$\begin{bmatrix} A \\ C \end{bmatrix} \begin{bmatrix} O \\ L \end{bmatrix} \begin{bmatrix} L \\ E \end{bmatrix} \begin{bmatrix} G \\ E \end{bmatrix}$

3. Explain Key Calculation Procedure in Simplified DES Algorithm

Ans Simplified DES Algorithm

→ Key Calculation Procedure

- It accept the 10 bit key and convert it into 8 bit key. This key is shared between both sender and receiver



i) Initial 10 Bit Key (K)

The S-DES algorithm starts with an initial 10-bit key, represented as K. This key is provided as input to the encryption and decryption processes.

ii) Permutation P10: The first step in key calculation is to permute the 10 bit key using a fixed permutation called P10.

iii) Key Generation Round

I] Round 1:
Left Circular Shift (LS1): Both L0 & R0 are separately subjected to a left circular shift by one bit. This means that the leftmost bit is moved to the rightmost position, and other bits are shifted one position to the ~~to~~ left.

II] Permutation P8: After the left circular shift, both L0 and R0 are subjected to another fixed permutation called P8.

P8 selects and permutes specific bits from the 10 bit values to generate the first subkey., often denoted as

The bit selected by P8 from both L0 and R0 are combined to form K1, which is a 8 bit subkey.

III] Round 2:
Left Circular shift (LS-2): Both L0 and R0 are separately subjected to a left circular shift by two bits this time.

IV] Permutation P8: After the left circular shift, both L1 & R1 are subjected to the P8 permutation again to generate the second subkey often denoted as K2.

The bits selected by P8 from both L1 & R1 are combined to form K2, which is another 8 bit subkey

It have generated two 8 bit subkeys K1 and K2, from the original 10 bit key K. These subkeys are used in S-DES encryption & decryption processes

4. Explain ~~in detail~~

4. Explain in detail about encryption procedure in IDEA algorithm

Ans IDEA Encryption Procedure

It operates on 64 bit blocks of plain text and uses a 128 bit key.

1. Key Expansion

The 128 bit encryption key is expanded into 52 round subkeys. These ~~round~~ round subkeys will be used in each of the 8.5 rounds of the encryption process. Each subkey is 16 bits in length

2. Initial Permutation :

The 64 bit block of plaintext is subjected to an initial permutation. This permutation rearranges the bits in the block according to a fixed pattern.

3. ~~8~~ Rounds :

IDEA consists of 8.5 rounds. Each ~~round~~ round consists of the ~~following~~ following steps.

a) subkey mixing

b) Substitution (S-Box)

c) Permutations (P-box)

d) Linear Transformation

4. Final Permutation:
After all rounds are completed the resulting data block is subjected to a final permutation, which is the inverse of the initial permutation

5. Output:
The final 64 bit block, after final permutation, ~~which is~~ is the ciphertext.

5. Demonstrate the working of RSA decryption algorithm with following parameters:

Cipher Text $C = 10$ Public key $(e, n) = (5, 35)$

Sol. To demonstrate the RSA decryption algorithm, it needs the cipher text (C) and public key (e, n). The decryption process involves using the private key (d, n) where d is the private exponent. In order to decrypt you need to calculate the private key (d) first.

$C = 10$

$(e, n) = 5, 35$

RSA Decryption Steps

→ Calculate the private key (d):

The modular multiplicative inverse of the public exponent (e) modulo (n)

$(d * e) \equiv 1 \pmod{n}$

Page No.
Date :

Modular
Multiplicative inverse of 5 modulo 35

$35 = 5 * 7 + 0$

Since the GCD (5, 35) is 5, there is no modular multiplicative inverse because 5 does not have an inverse modulo 35. This means that the given public key is not valid; and you cannot decrypt the cypher text with the provided parameters. RSA encryption and decryption require a valid public - private key pair where the chosen values of e, d and n satisfy certain conditions, including having an modular multicative inverse for e modulo (n).

Therefore, if the public key not valid, it is not possible to perform RSA decryption

6. Apply the Chinese Remainder Theorem to solve following congruent equations.

$x \equiv 2 \pmod 3$
$x \equiv 3 \pmod 5$
$x \equiv 2 \pmod 7$

Sol i) Common Modulus M

$$M = m_1 * m_2 * * m_3$$
$$= 3 \times 5 \times 7$$
$$= 105$$

ii) $$M_1 = \frac{M}{m_1} = \frac{105}{3} = 35$$

$$M_2 = \frac{M}{m_2} = \frac{105}{5} = 21$$

$$M_3 = \frac{M}{m_3} = \frac{105}{7} = 15$$

iii) $M_1^{-1} = (2 * 35) \bmod 3 \Rightarrow 2$

$M_2^{-1} = (1 * 21) \bmod 5 \Rightarrow 1$

$M_3^{-1} = (1 * 15) \bmod 7 \Rightarrow 1$

* Rule for M^{-1}

$(y_n * M_n) \bmod m_n = 1$

y = smallest natural no. possible according to the condition

$$M_n^{-1} = y_n$$

$a_1 = 2$	$m_1 = 3$	$M_1 = 35$	$M_1^{-1} = 2$
$a_2 = 3$	$m_2 = 5$	$M_2 = 21$	$M_2^{-1} = 1$
$a_3 = 2$	$m_3 = 7$	$M_3 = 15$	$M_3^{-1} = 1$

iv) $x = \sum_{i=1}^{n} (a_n M_n M_n^{-1}) \bmod M$

$a_1 M_1 M_1^{-1} = 2 \times 35 \times 2 = 140$

$a_2 M_2 M_2^{-1} = 3 \times 21 \times 1 = 63$

$a_3 M_2 M_3^{-1} = 2 \times 15 \times 1 = 30$

Page No.
Date :

$x = 23$

Check:

$23 \bmod 3 = 2$

$23 \bmod 5 = 3$

$23 \bmod 7 = 2$