Page No.
Date :

Assignment No. 1

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

→

GCD (99, 78) using Extended euclid algorithm:

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	

Q.2 a) What is Vigenere cipher? Explain it's working using Suitable example.

→ ① Vigenere cipher is a method of encrypting alphabetic text.

② It uses a simple form of polyalphabetic substitution.

③ A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets.

④ The encryption of the original text is done using the Vigenere Square or Vigenere table.

⑤ 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 cipher.

(6) At different points in the encryption process, the cipher uses a different alphabet from one of the rows.

(7) The alphabet used at each point depends on a repeating keyword.

(8) Example:

A	B	C	D	E	F	G	H	I	J	K	L
0	1	2	3	4	5	6	7	8	9	10	11

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

Y	Z
24	25

plaintext: G I V E M O N E Y

6 8 21 4 12 14 13 4 24

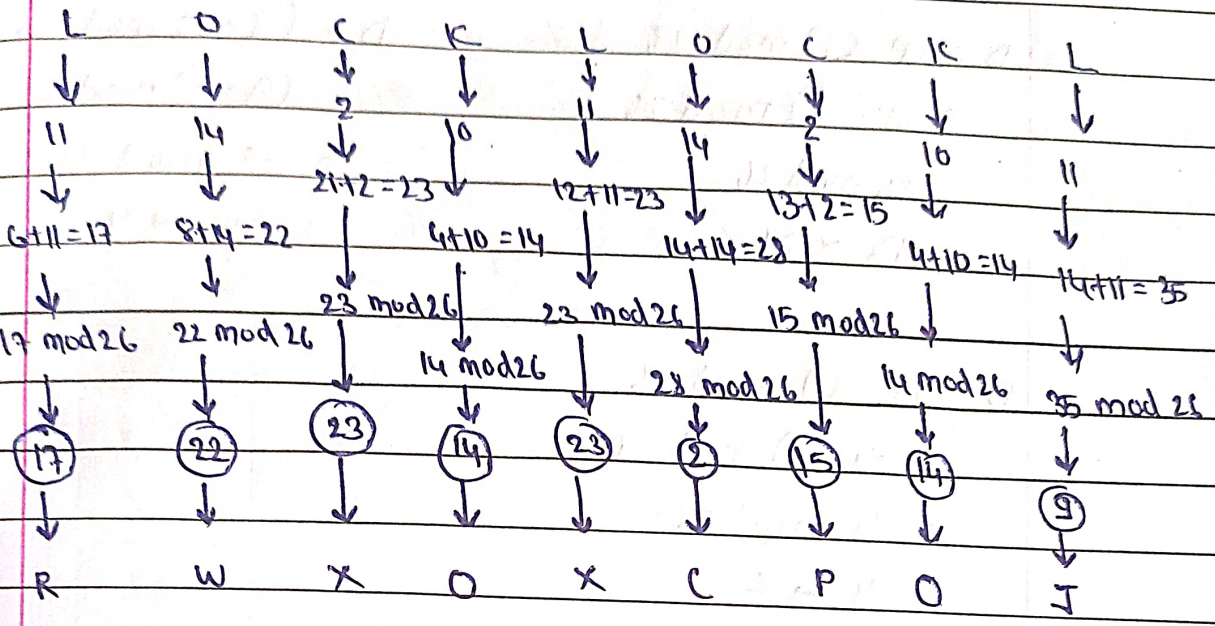
key: L O C K

LOCKLOCKL

11 14 2 10 11 14 2 10 11

Page No.
Date :

Encryption: $E_i = (P_i + K) \bmod 26$



∴ Cipher text : RWXOXCPOJ

Decryption:

R	W	X	O	X	C	P	O	J
17	22	23	14	23	2	15	14	9

$D_i = (E_i - K) \bmod 26$

$= (17 - 11) \bmod 26$

$= 6 \bmod 26$

$= 6 \sim G$

$D_i = (0 - K) \bmod 26$

$= (14 - 10) \bmod 26$

$= 4 \bmod 26$

$= 4 \sim E$

$D_i = (22 - 14) \bmod 26$

$= 8 \bmod 26$

$= 8 \sim I$

$D_i = (X - C) \bmod 26$

$= (26 - 11) \bmod 26$

$= (K \bmod 26) = 12 \sim M$

$D_i = (X - C) \bmod 26$

$= (23 - 2) \bmod 26$

$= 21 \bmod 26$

$= 21 \sim V$

$D_i = (C - O) \bmod 26$

$= (2 - 14) \bmod 26$

$= -12 \bmod 26$

$= 14 \sim O$

Page No.
Date :

$D = (P - C) \bmod 26$
$= (15 - 2) \bmod 26$
$= 13 \bmod 26$
$= 13 \sim N$

$D = (J - L) \bmod 26$
$= (9 - 11) \bmod 26$
$= -2 \bmod 26$
$= 24 \sim Y$

$D = (O - K) \bmod 26$
$= (14 - 10) \bmod 26$
$= 4 \bmod 26$
$= 4 \sim E$

∴ plain text : GIVE MONEY

Q.2 (b) Demonstrate the working of encryption and decryption procedure in Hill cipher w.r.t following parameter :

plaintext : ACOLLEGE

key :

7	8
19	3

→

plain text : AC OL LE GE

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

Encryption :

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

Page No.
Date :

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

$$= \begin{bmatrix} 0 \times 7 + 2 \times 8 \\ 0 \times 19 + 2 \times 3 \end{bmatrix} \text{ mod } 26$$

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

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

ii) For $\begin{bmatrix} 0 \\ L \end{bmatrix} = \begin{bmatrix} 14 \\ 11 \end{bmatrix}$

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

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

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

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

Page No.
Date :

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

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

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

$= \begin{bmatrix} 109 \\ 221 \end{bmatrix} \bmod 26$

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

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

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

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

$= \begin{bmatrix} 74 \\ 126 \end{bmatrix} \bmod 26$

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

∴ Cipher Text = QGENFNWW

Page No.
Date :

Decryption:

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

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

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

$= |21 - 152|$

$= |-131|$

Rule: $-a \bmod b = 1$

$\gcd(a, b) = 1$

$131 \times 1 \bmod 26 = 1$

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

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

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

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

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

To avoid -ve no. just add +26

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

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

Page No.
Date :

i) for $\begin{bmatrix} Q \\ G \end{bmatrix} = \begin{bmatrix} 16 \\ 6 \end{bmatrix}$

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

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

$= \begin{bmatrix} 416 \\ 418 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 0 \\ 2 \end{bmatrix} \sim \begin{bmatrix} A \\ C \end{bmatrix}$

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

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

$= \begin{bmatrix} 4 * 23 + 13 * 8 \\ 4 * 19 + 13 * 19 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 196 \\ 323 \end{bmatrix} \bmod 26$

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

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

Page No.
Date :

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

$$= \begin{bmatrix} 5 \\ 13 \end{bmatrix} \begin{bmatrix} 2 & 8 \\ 19 & 19 \end{bmatrix} \bmod 26$$

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

$$= \begin{bmatrix} 219 \\ 342 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 11 \\ 4 \end{bmatrix} \sim \begin{bmatrix} L \\ E \end{bmatrix}$$

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

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

$$= \begin{bmatrix} 682 \\ 836 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 6 \\ 4 \end{bmatrix} \sim \begin{bmatrix} G \\ E \end{bmatrix}$$

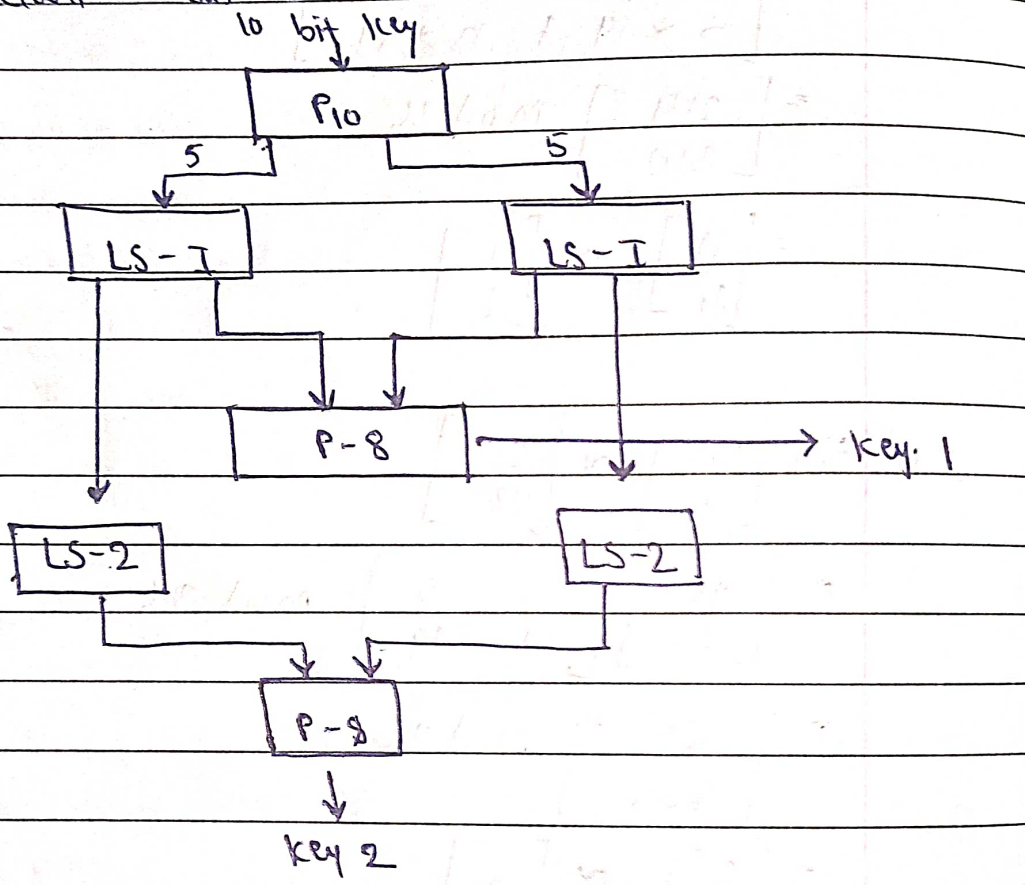
∴ plaintext = $\begin{bmatrix} A \\ C \end{bmatrix} \begin{bmatrix} O \\ L \end{bmatrix} \begin{bmatrix} L \\ E \end{bmatrix} \begin{bmatrix} G \\ E \end{bmatrix}$

ACOLLEGE

Page No.
Date :

Q.3 Explain key calculation procedure in simplified DES algorithm.

→ S-DES is a simplified version of the original Data encryption standard (DES) algo. It uses a shortest key length and fewer rounds for simplicity. Explanation of the key calculation procedure in S- DES :



- Initial 10-Bit key (K):

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

- Permutation P10 :

The first step in key calculation is to

Page No.
Date :

permute the 10 bit key using a fixed permutation called P10. P10 rearranges the bits in the following way: 3 5 2 7 4 10 1 9 8 6

The bits of the initial key are rearranged acc to this permutation. The resulting 10-bit value is divided into two 5-bit halves, often denoted as left and right halves (L0 and R0).

- Key Generation Rounds:
- Round 1:

LSJ: Both L0 and R0 are separately subjected to a left circular shift by one bit. This means that the left most bit is moved to the rightmost position, and the other bits are shifted one position to the left

L0: 3 5 2 7 4 10 1 9 8 6

R0: 5 2 7 4 10 1 9 8 6 3

- 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 halves to generate the first subkey, often denoted as K1.

P8: 6 3 7 4 8 5 10 9.

The bits selected by P8 from L0 and R0 are combined to form K1, which is a 8 bit sub-key.

Page No.
Date :

- Round 2:

Left circular shift 2 : Both L0 and R0 are separately subjected to a left circular shift by two bits this time.

L1 : 2 7 4 10 1 9 8 6 3 5

R1 : 7 4 10 1 9 8 6 3 5 2

- Permutation P8:

After the left circular shift, both L1 and R1 are subjected to the P8 permutation again to generate the second subkey, often denoted as K2.

P8 : 6 3 7 4 8 5 10 9

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

At the end of key calculation procedure, you have generated two 8 bit subkey, K1 and K2, from the original 10-bit key K. These subkeys are used in the S-DES encryption and decryption processes.

Page No.
Date :

Q.4 Explain in detail about encryption procedure in IDEA algorithm.

→ IDEA operates on 64 bit blocks of plaintext and uses a 128 bit key. Here's a step-by-step explanation of the encryption process:

① Key expansion:

The 128-bit encryption key is expanded into 52 round subkeys. These 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 rearrange the bits in the block a/c to a fixed pattern.

③ Rounds:

IDEA consists of 8.5 rounds (16 rounds divided by 2, where 0.5 rounds are applied to the middle of the data block). Each round consists of the following steps:

a) Subkey mixing
b) Substitution (S-Box)
c) permutation (P-Box)
d) Linear Transformation
e) Final permutation.

(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 the final permutation, is the ciphertext.

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

cipher text C = 10

public key (e,n) = (5,35)

→ To demonstrate the RSA decryption algorithm, you'll need the ciphertext (C) and the public key (e,n). The decryption process involves using the private key (d, n) where d is the private exponent.

cipher text = 10

public key (e,n) = (5,35)

RSA Encryption Steps:

(1) Calculate the private key (d):—

To calculate the d, you need to find the modular multiplicative inverse of the public (e) modulo (n). In other words, you

need to find a value for d such that $(d * e) \equiv 1 \pmod{n}$. you can use the extended euclidean algorithm to find d.

First, find the modular multiplicative inverse of 5 modulo 35:

using EEA:

$35 = 5 * 7 + 0$

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 can not decrypt the ciphertext with the provided parameters.

Q.6 Apply the Chinese Remainder Theorem to solve following congruent equation.

$x \equiv 2 \pmod{3}$

$x \equiv 3 \pmod{5}$

$x \equiv 2 \pmod{7}$

→ $m_1 = 3 \quad a_1 = 2$

$m_2 = 5 \quad a_2 = 3$

$m_3 = 7 \quad a_3 = 2$

i) common modulus m:

$M = m_1 * m_2 * m_3$

$= 3 * 5 * 7$

$\therefore M = 105$

Page No.
Date :

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) $M_1^{-1} = 35^{-1} \pmod 3 = 2$

$M_2^{-1} = 21^{-1} \pmod 5 = 1$

$M_3^{-1} = 15^{-1} \pmod 7 = 1$

iv) $x = ((a_1 * M_1 * M_1^{-1}) + (a_2 * M_2 * M_2^{-1}) + (a_3 * M_3 * M_3^{-1})) \bmod M$

$= ((2 * 35 * 2) + (3 * 21 * 1) + (2 * 15 * 1)) \bmod 105$

$= (140 + 63 + 30) \bmod 105$

$= 233 \bmod 105$

$= 23$

Verify: $23 \bmod 3 = 2$

$23 \bmod 5 = 3$

$23 \bmod 7 = 2$