2) Using extended euclidean algo. to find multiplicative inverse :-

$r_1 \leftarrow n$; $r_2 \leftarrow b$;
$t_1 \leftarrow 0$; $t_2 \leftarrow 1$;

while ($r_2 > 0$) {
$q = r_1 / r_2$;

$r = r_1 - q\, r_2$
$r_1 = r_2$; $r_2 = r$;

$t = t_1 - q\, t_2$
$t_1 = t_2$; $t_2 = t$;
}

if ($r_1 = 1$) then $b^{-1} = t_1$

Q:- Find the multiplicative inv. of 11 in Z_{26} :- $(11 \% 26)$

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

$t_1 = -7$ or 19. Ans

$12 \% 26$

$(12 + n) \% 26$ → does not exist

MINHAAZ

Dt.: 1/2/23
Pg.:

Delta

$a \quad x \quad b \quad n$

Q: $10x \equiv 2 \pmod{15}$

$a = 10, \quad n = 15$

$\gcd(10, 15) = 5$

since 5 does not divide 2, → no soln. Ans

$a \quad x \quad b \quad n$

Q:- $14x \equiv 12 \pmod{18}$

$\Rightarrow \gcd(14, 18) = 2$

$7x \equiv 6 \pmod{9}$

$7^{-1} \bmod 9 \equiv 4$

MINHAAZ

$(6 \times 4) \% 9 =$

MINHAAZ

$7(7^{-1})x = 6 \times 7^{-1} \pmod{9}$

$x = 6 \times 4 \pmod{9}$

$\boxed{x_0 = 6}$

$x_0 = x_0 + k(n/d)$

$= 6 + k(18/2)$

$x = 6 + k(9)$

$x_1 = 15.$ Ans

Dt.:
Pg.:

⇒ Hill Cipher :- (Pg. - 15)

UNIT-2

Dt.:
Pg.:
Delta

106

2) Galois Field (Pg.)

$(x+1)^{-1} \bmod (x^3+x^2+1)$

2) $g^0 = g^0 = g^0 = g^0 \rightarrow g^0 = (0001)$

$g^1 = g^1 = g^1 = g^1 \rightarrow g^1 = (0010)$

$g^2 = g^2 = g^2 = g^2 \rightarrow g^2 = (0100)$

$g^3 = g^3 = g^3 = g^3 \rightarrow g^3 = (1000)$

$g^4 = g^4 = g^4 = g+1 \rightarrow g^4 = (0011)$

Dt.:
Pg.:

$g^{10} = g(g^9) = g(g^3+1) = g^4+g = 1000 + 0010$

$= 1010$

$= g^2(g^4 \cdot g^4) = g^2(g+1)(g+1)$

$= g^2(g^2+g+1)$

$= g^4 + g^2 = g^2+g+1$

$= 0111$

$g^4\ g^3\ g^2\ g^1\ g^0$

$0\ 0\ 0\ 0\ 0$

$0\ 1\ 1\ 1$

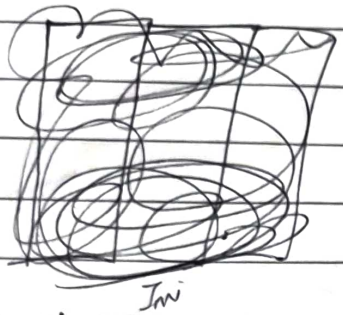
$\left(\frac{5}{3}\right)\%7$ $\Rightarrow (5\times 3) \bmod 7$

$\Rightarrow (5\times 5) \bmod 7 \Rightarrow 4$

Dt.:
Pg.:

⇒ Data Encryption Standard (DES) :-

Initial



Ini

2	4
1	3

Final

3	1
4	2

⇒ Initial permutation (IP) :-

- The bit in the first octate of i/p get spread into the 8 bits of each of the octates.
- The bits in the second octate of the i/p gets spread into the 7th bit of the octate.
- In general the bits of the i^{th} octate get spread into the $(8-i+1)^{th}$ of the octate.
- The pattern of the spreading of the 8^{th} bit in octate 'i' of the i/p among the o/p octate is that even no. bits go into octate 1 to 4.

MINHAAZ.

Dt.:
Pg.:

Delta

· and odd no. bits go into octate 5 to 8.

	1	2	3	4	5	6	7	8
1	58	50	42	34	26	18	10	2
2								
3								
4								
5								
6								
7								
8								

40 8 48 16 56 24 64 32

(Pg.-219)

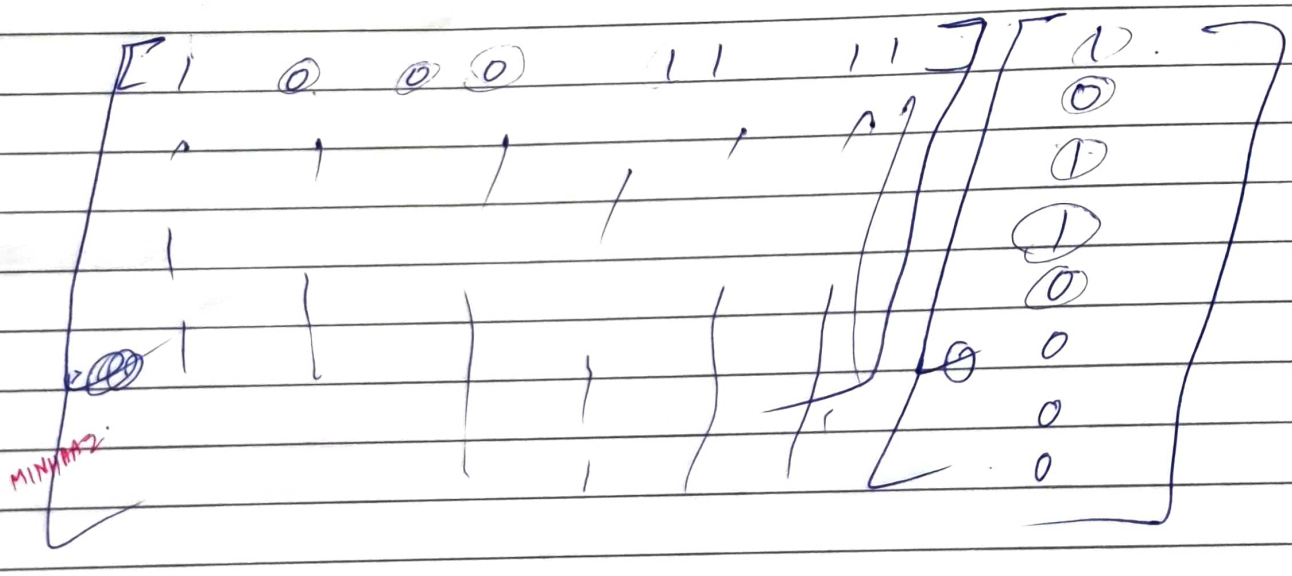
Dt.: 13/02/23
Pg.:

⇒ Advanced Encryption Standard (AES):-

. MINHAAZ

{ 0xC 08 0D 07 00 00 19 }

A	B	C	D	E	F	G	H
00	01	02	03	04	05	06	07
I	J	K	L	M	N	O	P
08	09	0A/10	0B/11	0C/12	0D/13	0E/14	0F/15
Q	R	S	T	U	V	W	X
10/16	11/17	12/18	13/19	14/20	15/21	16/22	17/23
Y	Z						
18/24	19/25						



ip :- $x^8 + x^6 + x^5 + x$

MINHAAZ

Dt.:
Pg.:

Delta

Q:- 03 x6 E

03 ⇒ 00000011 = $x+1$

6E ⇒ 0110 1110 = $x^6+x^5+x^3+x^2+x$

$(x+1) \times (x^6+x^5+x^3+x^2+x)$

⇒ $x^7+x^6+x^4+x^3+x^2+x^6+x^5+x^3+x^2+x$

⇒ $x^7+x^4+x^5+x$

⇒ 1011 0010 ⇒ B2.

10 11 00 10
0001 0101
0100 0110
1010 0110

0100 0111 ⇒ 47.

Dt.: 15/02/23
Pg.: Delta

251

⇒ PRIMES (Pg. - ~~[illegible]~~) :-

Q :- $\phi(10) = \phi(2 \times 5) = \phi(2) \times \phi(5)$

$= 1 \times 4 = 4$. Ans

↳ Tosian fn.

↳ [illegible]

[illegible]

$\phi(49) = \phi(7^2) = 7^2 - 7 \Rightarrow 49 - 7 = 42$. Ans

$\phi(p^e) = p^e - p^{e-1}$

$\phi(240) =$ [illegible] 3×80

↳

[illegible]

$= 2^4 \times 3 \times 5$

$= (2^4 - 2^3) \times (3^1 - 3^0) \times (5 - 5^0)$

$= 8 \times 2 \times 4 = 64$. Ans...

Dt.:
Pg.:

⇒ Fermat's little Theorem :-

- First Version :- p does not divide a.

$$a^{p-1} \equiv 1 \bmod p \quad (p \rightarrow \text{prime})$$

- Second Version :-

$$a^{p} \equiv a \bmod p \quad (p \rightarrow \text{prime})$$

Q :- $6^{10} \bmod 11$

$a = 6, \; p = 11$

$6^{11-1} \bmod 11 \equiv 1 \bmod 11$

Q :- $3^{12} \bmod 11$

~~$3^{10} \bmod 11$~~

$3^{10} \times 3^{2} \bmod 11$

$1 \times 9 \Rightarrow 9.$ Ans

Dt.: Pg.: Delta

Q :- $(145)^{102} \bmod 101$

Q :- $5^{18} \bmod 17$

$\Rightarrow 5^{17-1} \times 5^2 \bmod 17$

$\Rightarrow 1 \times 8 = 8$. Ans.

⇒ Multiplicative Inverse :-

$$a^{-1} \bmod p = a^{p-2} \bmod p$$

⇒ Euler's Theorem :-

~~First version :-~~

If a & n are coprime :-

$$a^{\phi(n)} \equiv 1 \bmod n$$

Q :- $6^{24} \bmod 35$

$\phi(35) = 4 \times 6 = 24$.

$6^{24} \bmod 35 \Rightarrow 1$. Ans

Dt.:
Pg.:

Second Version:-

Q:- $20^{62} \bmod 77$

$\phi(77) \Rightarrow \phi(11) \times \phi(7) \Rightarrow 10 \times 6 = 60$

$20^2 \times (20^{60} \bmod 77)$

$20^2 \bmod 77 = 15$. Ans.

- Second Version:-

$$a^{k \times \phi(m)+1} \equiv a \pmod{m}$$

- Multiplicative Inverse:-

$a^{-1} \bmod m = a^{\phi(m)-1} \bmod m$

(a & m are coprime).