KULVIK SINGH.
19BCE2074

(1) $n = 561$

Acc. to Miller Rabin Algorithm.

$n - 1 = 561 - 1$
$= 560$

2	560
2	280
2	140
2	70
	35

$560 = m * 2^k$
$= 35 * 2^4$

$k = 4, \quad m = 35.$

Random integer a, $(1 < a < n-1 \Rightarrow 1 < a < 560)$

Let $a = 2$.

Check : $a^m \bmod n = 1$

LHS $= 2^{35} \bmod 561$
$= 2.(2^{17})^2 \bmod 561$
$= 2(131072)^2 \bmod 561$ [using calculator]
$= 2(20)^2 \bmod 561$ [$131072 \bmod 561 = 20$]
$= 2.400 \bmod 561$
$= 800 \bmod 561$
$= 239 \neq 1$

$\therefore$ Check : $(a^m)^2 \bmod n = n-1$

LHS : $= (2^{35})^2 \bmod 561$
$= 2^{35} \times 2^{35} \bmod 561$
$= (239 \times 239) \bmod 561$
$= 57121 \bmod 561$
$= 460 \neq n-1$

$\therefore$ $\boxed{\text{561 is COMPOSITE}}$

(2) Cipher Text (C) = FWMDIQ = $\begin{bmatrix} F & M & I \\ W & D & Q \end{bmatrix}$

Key (K) = $\begin{bmatrix} 2 & 3 \\ 7 & 8 \end{bmatrix}$

Plain Text (P) = $K^{-1} C \bmod 26$

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

$|K| = (2 \times 8 - 3 \times 7) \bmod 26 = -5 \bmod 26 = 21$

$$\operatorname{adj}(K) = \begin{bmatrix} 8 & -3 \\ -7 & 2 \end{bmatrix}$$

$$\operatorname{inv}(K) = K^{-1} = \frac{1}{21} \begin{bmatrix} 8 & -3 \\ -7 & 2 \end{bmatrix} = \begin{bmatrix} 0.38 & -0.14 \\ -0.34 & 0.09 \end{bmatrix}$$

$$P = K^{-1} C \bmod 26$$

$$= \begin{bmatrix} 0.38 & -0.14 \\ -0.34 & 0.09 \end{bmatrix} \begin{bmatrix} 5 & 12 & 8 \\ 22 & 3 & 16 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} -1.18 & 4.14 & 0.8 \\ 0.28 & -3.81 & -1.28 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 25 & 4 & 1 \\ 0 & 22 & 25 \end{bmatrix}$$

$$= \begin{bmatrix} Z & E & B \\ A & W & Z \end{bmatrix}$$

= ZAEWBZ

Page

(3) $2x^{11} \equiv 22 \bmod 19$

$\because$ $22 \bmod 19 = 3$

$\therefore$ $2x^{11} \equiv 3$

$x^{11} = \dfrac{3}{2}$

Apply logarithm both sides

$\log x^{11} = \log \dfrac{3}{2}$

$\Rightarrow 11 \log x = \log 3 - \log 2$

$\Rightarrow 11 \log x = 0.4771 - 0.3010 = 0.1761$

$\Rightarrow \log x = \dfrac{0.1761}{11} = 0.0160$

$\Rightarrow x = 10^{0.0160}$

$\therefore \boxed{x = 1.0375}$

(4) $x \equiv a_1 \bmod m_1$ $\Rightarrow$ $x \equiv 7 \bmod 13$

$x \equiv a_2 \bmod m_2$ $\Rightarrow$ $x \equiv 11 \bmod 12$

For CRT to hold, $GCD(m_1, m_2) = 1$

$\therefore$ $GCD(13, 12) = 1$ [13, 12 are coprime].

Now,

Acc. to CRT

$$x = (M_1 X_1 a_1 + M_2 X_2 a_2) \bmod M \quad -(1)$$

$$M = m_1 * m_2$$
$$= 13 * 12$$
$$= 156$$

$$M_i = \frac{M}{m_i}$$

$\therefore$ $M_1 = \frac{156}{13} = 12$, $M_2 = \frac{156}{12} = 13$

$M_i X_i \equiv 1 \bmod m_i$

$\Rightarrow M_i X_i \pmod{m_i} = 1$

$\therefore$ $M_1 X_1 \pmod{m_1} = 1$	Similarly
	$M_2 X_2 \pmod{m_2} = 1$
$\Rightarrow 12 X_1 \pmod{13} = 1$	$\Rightarrow 13 X_2 \pmod{12} = 1$
$\Rightarrow X_1 = 12$	$\Rightarrow 1 X_2 \pmod{12} = 1 \Rightarrow X_2 = 1$

Using these values in (1).

$$x = ((12 * 12 * 7) + (13 * 1 * 11)) \bmod 156$$
$$= (1008 + 143) \bmod 156$$
$$= 1151 \bmod 156$$
$$= 59$$

$\boxed{\text{Ans : } x = 59}$

(5) $44^{-1} \bmod 667$

$= 44^{\phi(667)-1} \bmod 667$

$\phi(667) = \phi(29 \times 23)$

$= \phi(29) \times \phi(23)$

$= 28 \times 22$

$= 616$

$= 44^{616-1} \bmod 667$

$= 379.$

6 $\gcd(42828, 6407)$

$42828x + 6407y = d = \gcd(42828, 6407)$

Euclidian Algorithm.	Rewrite
$42828 = 6407(6) + 4386$	$42828 - 6407(6) = 4386$ — 5
$6407 = 4386(1) + 2021$	$6407 - 4386(1) = 2021$ — 4
$4386 = 2021(2) + 344$	$4386 - 2021(2) = 344$ — 3
$2021 = 344(5) + 301$	$2021 - 344(5) = 301$ — 2
$344 = 301(1) + \boxed{43}$	$344 - 301(1) = 43$ — 1
$301 = 43(7) + 0$	

$\therefore \boxed{GCD = 43 = d}$ → Ans.

Build Soln

$42828x + 6407y = d$

$\Rightarrow 42828x + 6407y = 43$ (from euclidean alg.)

$\Rightarrow 344 - 301(1) = 43$ (from 1)

$\Rightarrow 344 - [2021 - 344(5)](1) = 43$ (from 2)

$\Rightarrow 344 - 2021 + 344(5) = 43$

$\Rightarrow 344(6) - 2021 = 43$

$\Rightarrow [4386 - 2021(2)](6) - 2021 = 43$ (from 3)

$\Rightarrow 4386(6) - 2021(13) = 43$

$\Rightarrow 4386(6) - [6407 - 4386(1)](13) = 43$ (from 4)

$\Rightarrow 4386(19) - 6407(13) = 43$

$\Rightarrow [42828 - 6407(6)](19) - 6407(13) = 43$ (from 5)

$\Rightarrow 42828(19) - 6407(127) = 43$

$\Rightarrow 42828(19) + 6407(-127) = 43$

$\therefore \boxed{x = 19, \ y = -127}$ → Ans.

7 a) $55x \equiv 35 \bmod 75$

$\gcd(55, 75) = 5.$

$35 = 5 \times 7$

$55x \equiv 35 \bmod 75$

$11x \equiv 7 \bmod 15$

$-x \equiv 13 \bmod 15$

$x \equiv 2 \bmod 15$

$x = 2, 17, 32, 47, 62 \pmod{75}$

b) $42x \equiv 12 \pmod{90}$

$\gcd(42, 90) = 6.$

$42x \equiv 12 \bmod 90$

$7x \equiv 2 \bmod 15$

$-14x \equiv -4 \bmod 15$

$x \equiv 11 \bmod 15$

$x = 11, 26, 41, 56, 71, 86 \pmod{90}$

(8) a) 20 mod 17

By division algorithm.

$$a = qn + r$$

$$20 = 17 \times (1) + 3.$$

$$\therefore \boxed{20 \text{ mod } 17 = 3.}$$

b) 20 mod −17

By division algorithm

$$a = qn + r$$

$$20 = +17 \times (1) + r$$

$$\therefore r = 3.$$

However when n is negative in a mod n

then, $a \text{ mod} -n = a \text{ mod } n - n$

$$\therefore \boxed{20 \text{ mod } -17 = 3 - 17 = -14}$$

c) −20 mod 17

By division algorithm

$$a = qn + r$$

$$-20 = 17 \times (-2) + r$$

$$\therefore r = 14$$

$$\boxed{-20 \text{ mod } 17 = 14}$$

d) −20 mod −17

By division algorithm

$$a = qn + r$$

$$\Rightarrow -20 = -17 \times (1) + r$$

$$\Rightarrow r = -3$$

$$\boxed{-20 \text{ mod } -17 = -3.}$$

(9) According to Fermat's Theorem,

$$a^p \equiv a \pmod{p}$$

$$a = 9^{794} \pmod{73}$$

73 is prime, we want to break up the exponent 794 into a form of $73q + r$

$$794 = 73 * 10 + 64$$

So,

$$a = 9^{(73*10+64)} \pmod{73}$$

$$= \left[\left(9^{73}\right)^{10}\left(9^{64}\right)\right] \pmod{73}$$

$$= 9^{10} \cdot 9^{64} \pmod{73}$$

$$= 9^{74} \pmod{73}$$

$$= \left[9^{73} * 9\right] \bmod 73$$

$$= 9 * 9 \bmod 73$$

$$= 81 \bmod 73$$

$$\therefore \quad a = 8 \bmod 73.$$

Hence $\boxed{a = 8}$ ← Ans.

(10) By Euler's Theorem

If a and n are co-prime, ie, $GCD(a,n)=1$,

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

where $\phi(n)$ = Euler's Toitent Function.

for $n = 35$

$\therefore$ integer from 0 to 34 that are not co-prime with 35 are $\{5, 7, 10, 14, 15, 20, 21, 25, 28, 30\}$

$\therefore \quad \phi(35) = 34 - 10 = 24$

From Euler's Thm.

$$x^{\phi(35)} = x^{24} \equiv 1 \bmod 35. \quad (1)$$ [24, 35 are co-prim

and

$$x^{85} \equiv x^{(85-3\times24)} \equiv x^{85-72} \equiv x^{13} \equiv 6 \bmod 35 \quad (2)$$

Substituting (1) in (2).

$$x^{12} * x \equiv 6 \bmod 35$$

$$\boxed{x^{24*1/2} \equiv 1 \bmod 35}$$

$$\Rightarrow (+1) * x \equiv 6 \bmod 35$$

$$\Rightarrow x \equiv 6 \bmod 35$$

So

$x = 6$.

$$\therefore \quad 6^{85} \equiv 6 \bmod 35.$$

$\boxed{\text{Ans: } x = 6}$