Name :- Vedant Ghag   Roll No :- 23   Batch :- A

CSS Assignment - 1

(1) Encrypt "academic committee will meet today" using playfair cipher with key word "ROYAL ENFZELD"

→ ~~Key word~~ Plain text :- "academic committee will meet today"
· Keyword :- "ROYAL ENFZELD"

Playfair grid

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

P.T	AC	AD	EM	IC	CO	MX	MI
C.T	OH	LZ	BU	NH	PN	SU	SE

P.T	TX	IE	FW	ZL	LM	EX	ET
C.T	SZ	MD	FU	DA	RI	ZU	DM

P.T	TO	DA	YX
C.T	PL	ZL	AW

→ Cipher text for given plain text i
"OHCI BUNHPN SUSE SI MDFU DART ZUDM PL ZLAW"

(2) State the Rules for finding Euler's phi func^n

a. $\phi(10)$

$\phi(10) = \phi(2 \times 5)$

$= \phi(2-1)(5-1) \Rightarrow 1 \times 4$

$\phi(10) = 4$

b. $\phi(49)$

$\phi(49) = \phi(7 \times 7)$

$= 49 \times \left(1 - \frac{1}{7}\right)$

$\phi(49) = 42$

c. $\phi(343)$

$\phi(343) = \phi(7 \times 7 \times 7)$

$= 343 \left(1 - \frac{1}{7}\right)$

$\phi(343) = 294.$

(3) Use Hill Cipher to encrypt the text "short". the key to be used is "hill"

$\Rightarrow$ key matrix $= \begin{bmatrix} H & I \\ L & L \end{bmatrix}_{2 \times 2}$

P.T matrix

$\begin{bmatrix} S \\ H \end{bmatrix}_{2 \times 1}$ $\begin{bmatrix} O \\ R \end{bmatrix}_{2 \times 1}$ $\begin{bmatrix} T \\ X \end{bmatrix}_{2 \times 1}$

Now $C_1 = KP \bmod 26$

$$C_1 = \begin{bmatrix} H & Z \\ L & L \end{bmatrix} \cdot \begin{bmatrix} S \\ H \end{bmatrix} \% 26$$

$$C_1 = \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \cdot \begin{bmatrix} 18 \\ 7 \end{bmatrix} \% 26$$

$$C_1 = \begin{bmatrix} 126 + 56 \\ 198 + 77 \end{bmatrix}_{2\times 1} \% 26$$

$$C_1 = \begin{pmatrix} 0 \\ 15 \end{pmatrix}_{2\times 1} = \begin{bmatrix} A \\ P \end{bmatrix}_{2\times 1}$$

$C_3 = KP \bmod 26$

$$C_3 = \begin{bmatrix} H & Z \\ L & L \end{bmatrix} \begin{bmatrix} T \\ X \end{bmatrix} \bmod 26$$

$$C_3 = \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \cdot \begin{bmatrix} 19 \\ 23 \end{bmatrix} \% 26$$

$$C_3 = \begin{bmatrix} 317 \\ 962 \end{bmatrix} \% 26$$

$$C_3 = \begin{bmatrix} 5 \\ 20 \end{bmatrix}_{2\times 1} = \begin{bmatrix} F \\ U \end{bmatrix}_{2\times 1}$$

$C_2 = KP \bmod 26$

$$C_2 = \begin{bmatrix} H & Z \\ L & L \end{bmatrix} \cdot \begin{bmatrix} O \\ R \end{bmatrix} \% 26$$

$$C_2 = \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \cdot \begin{bmatrix} 14 \\ 17 \end{bmatrix} \% 26$$

$$C_2 = \begin{bmatrix} 234 \\ 341 \end{bmatrix} \% 26$$

$$C_2 = \begin{pmatrix} 0 \\ 3 \end{pmatrix}_{2\times 1} = \begin{bmatrix} A \\ D \end{bmatrix}_{2\times 1}$$

∴ For the given plain text "SHORTX" & the key "HZLL" using hill cipher method the cipher text obtained is "APADFU"

Ans: Cipher text: APADFU

(4) A & B whishes to use RSA to communicate securely A choose public key (7, 119) & B chose's public key as (13, 221). Calculate their private key. A wishes to send message m = 10 to B. what will be cipher text? with what key will A encrypt the message "…" if A needs to authenticate itself to B.

⇒ For A :- We know public key = (e, n) = (7, 119)

∴ $e = 7$, $n = 119$

Now we know $n = p \times q$ ... (product of prime no.)

thus through dedication $p = 7$ & $q = 17$
thus checking if $p = 7$, $q = 17$ are true candidates

Two condition:-

(1) $\phi(n) = (p-1) \times (q-1) = 6 \times 16 = 96$. (Euler ...)

Now, $1 < e < \phi(n)$ ⇒ condition satisfied

(2) $\gcd(e, \phi(n)) = 1$ ... (condition approved)

$$d = e^{-1} \bmod \phi(n)$$
$$ed = 1 \bmod \phi(n)$$
$$\therefore d = \frac{1 + k(\phi(n))}{e}$$

Now: * at $k = 1$ ⇒ 13.8 (float) ⇒ reject
* at $k = 2$ ⇒ $d = 27.57$ (float) ⇒ reject
* at $k = 3$ ⇒ $d = 41.28$ (float) ⇒ reject
* at $k = 4$ ⇒ $d = 55$ (int) ⇒ accept

⇒ ∴ Private key of A = (d, n) = (55, 119)

For B :- We know public key = $(e, n) = (13, 221)$
$\therefore e = 13,\ n = 221$
Now we know $n = p \times q$ .. product of prime no.

Thus through deductions $p = 13,\ q = 17$
Thus checking it $p = 13$ & $q = 17$ are true candidates.

Two cond^n :-
(1) $\phi(n) = (p-1) \times (q-1) = 12 \times 16 = 192$ .. Euler's notation fun
Now $1 < e < \phi(n)$ .. cond^n satisfied
(2) $\gcd(e, \phi(n)) = 1$ ...

Now $d = e^{-1} \bmod \phi(n)$
$ed = 1 \bmod \phi(n)$
$d = \dfrac{1 + k\phi(n)}{e}$

$d = 133$ .. accept .. By calculator

Private key of B .. $(d, n) = (133, 221)$

Now, message $\Rightarrow m = 10$.
Now For A to send a ciphertext to B
A would encrypt the message using public key of B

Encrypted text :- Ciphertext $= (10)^e \bmod n$

$$= (10)^{13} \bmod 221$$
$$= (10^5 \times 10^5 \times 10^3) \bmod 221$$
$$= (108 \times 108 \times 116) \bmod 221$$
$$= (172 \times 116) \bmod 221$$

Ciphertext $= 62$

If A would want to authenticate itself to B, it would encrypt the message using its private key

$$\text{Auth} = (m)^d \bmod 119$$
$$S = (10)^{55} \bmod 119$$

$$S = (53 \times 53 \times 53 \times 53 \times 53 \times 10^5) \bmod 119$$

$$S = (8 \times 40 \times 92) \bmod 119$$

$$\boxed{S = 73}$$

Thus B would understand it would A.

$$S_B = (S)^e \bmod 119$$
$$= (73)^7 \bmod 119$$
$$S_B = 10$$

$\boxed{S_B = m}$ Thus B would know A sent the message.