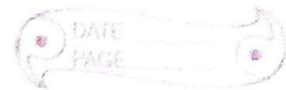


CS304 Theory Assignment

Name - URMILA

Roll No - RATHORE



② Plaintext \rightarrow WEAREINDIAN

We generate ciphertext using shift cipher encryp.
with, Secret Key $\rightarrow 4$

Shift operation, \rightarrow

$$E_n(x) = (x + n) \bmod 26$$

$$E_1 = (4 + 22) \bmod 26 = 0 = A$$

$$E_2 = (4 + 4) \bmod 26 = 8 = I$$

$$E_3 = (4 + 0) \bmod 26 = 4 = E$$

$$E_4 = (4 + 17) \bmod 26 = 21 = V$$

$$E_5 = (4 + 4) \bmod 26 = 8 = I$$

$$E_6 = (4 + 8) \bmod 26 = 12 = M$$

$$E_7 = (4 + 13) \bmod 26 = 17 = R$$

$$E_8 = (4 + 3) \bmod 26 = 7 = H$$

$$E_9 = (4 + 8) \bmod 26 = 12 = M$$

$$E_{10} = (4 + 0) \bmod 26 = 4 = E$$

$$E_{11} = (4 + 13) \bmod 26 = 17 = R$$

So the ciphertext = A I E V I M R H M E R

decryption - $D = (x + n) \bmod 26$

$$D_1 = (22 - 4) \bmod 26 = 18 = W$$

$$D_2 = (8 - 4) \bmod 26 = 4 = E$$

$$D_3 = (4 - 4) \bmod 26 = 0 = A$$

$$D_4 = (21 - 4) \bmod 26 = 17 = R$$

$$D_5 = (8 - 4) \bmod 26 = 4 = E$$

$$D_6 = (12 - 4) \bmod 26 = 8 = I$$

$$D_7 = (17 - 4) \bmod 26 = 13 = N$$

Urmita Rathore

201951164

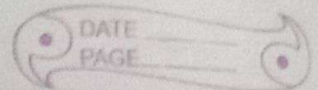


$$\begin{aligned} D_8 &= (7 - 4) \bmod 26 = 3 = D \\ D_9 &= (12 - 4) \bmod 26 = 8 = I \\ D_{10} &= (4 - 4) \bmod 26 = 0 = A \\ D_{11} &= (17 - 4) \bmod 26 = 13 = N \end{aligned}$$

Hence prove our cipher text is right
for the given plain text.

Urmila Rautond

201951164



① we have given the π in the transposition cipher.

π

1	2	3	4	5	6	7	8	9	10	11	12
3	5	6	9	11	1	8	2	10	4	12	7

msg $\rightarrow m_3 m_5 m_6 m_9 m_{11} m_1 m_8 m_2 m_{10} m_4 m_{12} m_7$
and ency. msg = $m_3 m_5 m_6 m_9 m_{11} m_1 m_8 m_2 m_{10} m_4 m_{12} m_7$

~~Plaintext~~ msg \rightarrow CRYPTOGRAPHY.

encrypted msg \rightarrow XTOAHCRRPPYG.

To find the decryption we need to find π^{-1}

which will be,

π^{-1}

1	2	3	4	5	6	7	8	9	10	11	12
6	8	1	10	2	3	12	7	4	9	5	11

Cipher text \rightarrow XTOAHCRRPPYG.

decrypted msg \rightarrow CRYPTOGRAPHY.

③ Plaintext \rightarrow WEAREINDIAN
Key \rightarrow CRICKET

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

WE AR EI ND IA NZ These are the all pairs

WE \rightarrow ZR

AR \rightarrow HA

EI \rightarrow CK

ND \rightarrow MF

IA \rightarrow RA

NZ \rightarrow VE

So the Encrypted msg is
 \rightarrow ZRHACKMFERBVE

And for the Decryption msg :-

ZR \rightarrow WE (they are in the same row)

HA \rightarrow AR (same column)

CK \rightarrow EI (same row)

MF \rightarrow ND (same rectangle)

RA \rightarrow IA (same rectangle)

VE \rightarrow NZ (Z not considered)

So \rightarrow WEAREINDIAN

⑨ As we know Decryption is not possible when $(a, 26)$ are not co-prime,
 $\text{GCD}(a, 26) \neq 1$

For i in 1 to 26
 if $i \bmod 26 == 1$
 $\text{inv} = i$

and, $\text{Dec}(C) = ((C - b) * \text{inv}_a) \bmod 26$

If inv_a is inverse modulo of a , i.e. $(a * \text{inv}_a) \bmod 26 = 1$ then inv_a is also inverse modulo of $a + n * 26 \forall n \in \mathbb{N}$.

Thus all the pairs of the form $(a + n * 26, b + n * 26)$ $\forall n \in \mathbb{N}$ generates same ciphertext where \mathbb{N} is Natural number.

So, There are infinite no. of diff. keys.

⑩ The given expression of (m, k) results in the same expression as m, k .

Since message and encryption key is same, thus ciphertext c_1, c_2 are also same.

Let suppose,

$$c_1 = \text{Enc}(m, k)$$

$$c_2 = \text{Enc}(\bar{m}, \bar{k})$$

$$\text{Enc}(m, k) = c \quad \text{so} \quad \text{Enc}(\bar{m}, \bar{k}) = \bar{c}$$

So from above,

$$\begin{aligned} C_2 &= \text{enc}(\bar{m}, \bar{k}) \\ &= \text{enc}(\bar{m}, \bar{k}) \\ \bar{C}_2 &= \text{enc}(m, k) \\ \bar{C}_2 &= C_1 \end{aligned}$$

⑥ Given ciphertext is = AFITIFWF

$$Y = (X + K) \bmod 26$$

For encryption

$$X = (Y - K) \bmod 26$$

For decryption

F is given as 3

$$(X_2 + K) \bmod 26 = 5$$

$$(5 - K) \bmod 26 = X_2$$

$$\frac{(X_2 + K) \bmod 26}{(5 - K) \bmod 26} = \frac{5}{X_2}$$

$$\Rightarrow (X_2 + 5)(K + X_2 - 5) = 0$$

$$X_2 = 5 - K$$

$$\text{For } K = 5, X_1 = 21$$

$$X_2 = 0$$

$$X_3 = 3$$

$$X_4 = 14$$

$$X_5 = 3$$

$$X_6 = 0$$

$$X_7 = 17$$

$$X_8 = 0$$

Q1 - So the plaintext is VADODARA
and secret key = 5

Q2 - let us consider encryption.

$$y = xK \pmod{26}$$

$$x = yK^{-1} \pmod{26}$$

$$K \cdot K^{-1} = 1 \pmod{26}$$

HI LL

[7, 8] [11, 11]

$$[7, 8] [11, 11] = \begin{bmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{bmatrix} \rightarrow \begin{pmatrix} 23, 8 \\ 24, 9 \end{pmatrix}$$

$$7K_{11} + 8K_{21} = 23$$

$$7K_{12} + 8K_{22} = 8$$

$$11K_{11} + 11K_{21} = 24$$

$$11K_{12} + 11K_{22} = 9$$

after solving -

$$K_{11} = 11, K_{12} = 3$$

$$K_{21} = 8, K_{22} = 7$$

Therefore key $K = \begin{bmatrix} 11 & 3 \\ 8 & 7 \end{bmatrix}$

$$\textcircled{8} \quad (a) \quad \begin{array}{rcl} 222 & = & 18 \times 12 + \boxed{6} \\ 18 & = & \boxed{6} \times 3 + 0 \end{array}$$

$\gcd(222, 18) = 6$ because 6 is the common.

$$(b) \quad 1 = 33x_0 + 13y_0 \quad - \textcircled{1}$$

$$33 = 13 \times 2 + 7$$

$$13 = 7 \times 1 + 6$$

$$7 = 6 \times 1 + 1$$

$$6 = 1 \times 6 + 0$$

$$\gcd(33, 13) = 1$$

$$1 = 7 - 6 \times 1$$

$$= (33 - 13 \times 2) - (13 - 7 \times 1)$$

$$= \cancel{33} \cdot 2 \times 33 - 5 \times 13 \quad - \textcircled{2}$$

by comparing eqⁿ ① and ② we get.

$$\boxed{x_0 = 2}$$

$$\boxed{y_0 = -5}$$

$$(c) \quad x = 5^{-1} \pmod{26}$$

$$5x = 1 \pmod{26}$$

$$5x = 105 \pmod{26}$$

$$x = 21 \pmod{26}$$

For above eqⁿ,

inverse is 21 //

⑩ Mix Column $\rightarrow (33, 42, 66, 24)$

$$\begin{bmatrix} T_{00} \\ T_{10} \\ T_{20} \\ T_{30} \end{bmatrix} = \begin{pmatrix} 33 \\ 42 \\ 66 \\ 24 \end{pmatrix}$$

$$T_{00} = 33 = 00110001 = x^5 + x^4 + x + 1$$

$$T_{10} = 42 = 01000010 = x^6 + x$$

$$T_{20} = 66 = 01100110 = x^6 + x^5 + x^2 + x$$

$$T_{30} = 24 = 00100100 = x^5 + x^2$$

$$T_{00}' = x + T_{00} + (x+1)T_{10} + T_{20} + T_{30}$$

$$x + T_{00} = x^6 + x^5 + x^2 + x$$

$$(x+1)T_{10} = x^7 + x^2 + x^6 + x$$

$$T_{20} = x^6 + x^5 + x^2 + x$$

$$T_{30} = x^5 + x^2$$

$$T_{00}' = x^7 + x^6 + x^5 + x = 11100010 = E2$$

$$T_{10}' = x + T_{10} + (x+1)T_{20} + T_{30} + T_{00}$$

$$= x^5 + x^4 + x^3 + 1$$

$$= 00111001$$

$$= 39$$

$$T_{20}' = xT_{20} + (x+1)T_{30} + T_{00} + T_{10}$$

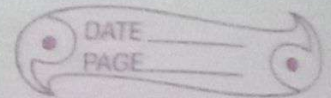
$$= x^7 + x^6 + x^3 + x^2 + x^6 +$$

$$x^3 + x^5 + x^2 + x^5 + x^4 + x$$

$$+ 1 + x^6 + x$$

Vrinda Rathore

201951169



$$= 2^7 + 2^6 + 2^4 + 1$$

$$= 11010001$$

$$= 01$$

$$T_{30}^1 = 2T_{30} + (2+1)T_{00} + T_{10} + T_{20}$$

$$= 2^5 + 2^4 + 1$$

$$= (00110001)$$

$$= 31$$

So the output will be $(E2, 39, D1, 31)$

③ AES Subbytes (D3)

$$D3 = \underbrace{1101}_4 \underbrace{0011}_3$$

$$\therefore x = 0 \quad y = 3$$

So according to the table of multiplicative inverse in GF(2⁸)

$$\text{Output} = BB = 1011 \ 1011$$

Affine transformation :-

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \times \begin{bmatrix} a_7 \\ a_6 \\ a_5 \\ a_4 \\ a_3 \\ a_2 \\ a_1 \\ a_0 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} \Rightarrow \begin{bmatrix} 0 \oplus 0 \\ 0 \oplus 1 \\ 0 \oplus 1 \\ 0 \oplus 0 \\ 0 \oplus 0 \\ 1 \oplus 0 \\ 0 \oplus 1 \\ 1 \oplus 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = 66$$

If we apply AES Subbyte fun. will get 66 as output