CS304 Theory Assignment

Name - URMILA

Roll No - RATHORE

(2) Plaintext → WEAREINDIAN

We generate ciphertext using shift cipher enc. eq. with secret key → 4

shift cipher operation. →

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

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

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

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

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

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

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

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

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

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

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

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

So the ciphertext = AIEVIMRHMER

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

$D_1 = (\text{[illegible]})(0+4) \bmod 26 = 22 = W$

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

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

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

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

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

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

Urmila Rathore
20195116

$D_8 = (7 - 4) \bmod 26 = 3 = D$

$D_9 = (12 - 4) \bmod 26 = 8 = I$

$D_{10} = (4 - 4) \bmod 26 = 0 = A$

$D_{11} = (17 - 4) \bmod 26 = 13 = N$

Hence prove our ciphertext is right for the given plaintext.

Urmila Rathod

2019511694

DATE
PAGE

(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 → $m_3 m_5 m_6 m_9 m_{11} m_1 m_8 m_2 m_{10} m_4 m_{12} m_7$

and encry. 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 → CRYPTOGRAPHY.

encrypted msg → YTOAHCRRPPYG.

To find the decryption we need to find

$\pi = \pi^{-1}$

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 → YTOAHCRRPPYG.

decrypted msg → CRYPTOGRAPHY.

URMILA RATHORE

2019S1164

(3) Plaintext → WEAREINDIAN

Key → 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 There are the all pairs

WE → ZR

AR → HA

EI → CK

ND → MF

IA → RB

NZ → VE

So the encryted msg is → ZRHACKMFRBVE

And for the Decryption msg :-

ZR → WE (they are in the same Row)

HA → AR (same column)

CK → EI (same row)

MF → ND (same rectangle.)

RB → IA (same rectangle)

VE → NZ Z not considered)

So → WEAREINDIAN

Vamila Kallore
2019SIIG4

(a) As we know Decryption is not possible when. (a, 26) are not co-prime,
GCD (a, 26) ≠ 1

For i in 1 to 26
if i mod 26 == 1
Inv = i

and, Dec(C) = ((C-b) * inv_a) mod 26

If Inv. is inverse modulo of a, i.e. (a * inv.) mod 26 = 1 then Inv is also inverse modulo of a + n * 6 ∀ n ∈ N.

Thus all the pair of the form (a + n * 26, b + n * 26 ∀ n ∈ N generates same ciphertext where N is Natural numbers.
So, There are Infinite no. of diff. keys.

(b) The given expression of (M, K) results in the same expression as M, K.
Since message and encryption key is same, thus ciphertexts C_1, C_3 are also same.
Let's suppose,

C_1 = Enc (M, K)

C_2 = Enc ($\bar{M}$, $\bar{K}$)

Enc (M, K) = C so Enc ($\bar{M}$, $\bar{K}$) = $\bar{C}$

Umila Rathnayake
2019S116

So from above,

$$C_2 = Enc.(\bar{m}, \bar{k})$$
$$= Enc(\bar{\bar{m}}, \bar{\bar{k}})$$
$$\bar{C}_2 = Enc(m, k)$$
$$\bar{C}_2 = C_1$$

(6) Given Ciphertext is = AFITI FWF

$Y = (X + K) \bmod 26$. For encryption

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

F is given as 3

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

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

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

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

$X_2 = S - K.$

For $K = 5$, $X_1 = 21$

$X_2 = 0$

$X_3 = 3$

$X_4 = 14$

$X_5 = 3$

$X_6 = 0$

$X_7 = 17$

$X_8 = 0$

Urmila Rathore
20195116

(6) So the plaintext is VADODARA
and secret key = 5

(7) let us consider encryption.

→ $y = xK \pmod{26}$

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

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

HI LL

(7, 8) (11, 11)

$$(7, 8)\ (11, 11) \cdot \begin{bmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{bmatrix} \rightarrow \begin{matrix} (23, 8) \\ (24, 9) \end{matrix}$$

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

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

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

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

after solving -

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

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

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

Urmila Rathore
2019511cs

(8) (a) $222 = 18 * 12 + \boxed{6}$

$18 = \boxed{6} * 3 + 0$

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

(b) $1 = 33x_0 + 13y_0 \quad -①$

$33 = 13 * 2 + 7$

$13 = 7 * 1 + 6$

$7 = 6 * 1 + 1$

$6 = 1 * 6 + 0$

gcd (33, 13) = 1

$1 = 7 - 6 * 1$

$= (33 - 13 * 2) - (13 - 7 * 1)$

$= 2 * 33 - 5 * 13 \quad -②$

by comparing eq.n ① and ② we get.

$\boxed{x_0 = 2}$ $\boxed{y_0 = -5}$

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

$5x = 1 \pmod{26}$

$5x = 105 \pmod{26}$

$x = 21 \pmod{26}$

For above eq.n,
Inverse is 21 //

Urmila Rathore
2019511164

(10) mix column → (33, 42, 66, 24)

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

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

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

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

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

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

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

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

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

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

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

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

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

$= 00111001$

$= 39$

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

$= x^7 + x^6 + x^3 + x^2 + x^6 + x^3 + x^5 + x^2 + x^5 + x^4 + x + 1 + x^6 + x$

Urmila Rathore
2019511694

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

$= 11010001$

$= 01$

$T'_{30} = xT_{30} + (x+1)T_{00} + T_{10} + T_{20}$

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

$= (00110001)$

$= 31$

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

Urmila Rathore
2015516

③ AES Subbytes (D3)

D3 = 1101 0011
4 3

∴ x = D y = 3

So according to the table of multiplicative inv. in GF (2^8)

Output = BB = 1011 1011

Affine transformation :-

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

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

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