Tanuj Saini
2022511141

M T W T F S S
Page No.:
Date:
YOUVA

ASSIGNMENT

(1) π: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 5 & 6 & 9 & 11 & 1 & 8 & 2 & 10 & 4 & 12 & 7 \end{pmatrix}$

a) Plain text : C R Y P T O G R A P H Y
1 2 3 4 5 6 7 8 9 10 11 12

cipher text → Y T O A H C R R P P Y G

b) Yes, we can decrypt it by using inverse permutation

π^{-1}: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 6 & 8 & 1 & 10 & 2 & 3 & 12 & 7 & 4 & 9 & 5 & 11 \end{pmatrix}$

Cipher text : Y T O A H C R R P P Y G
1 2 3 4 5 6 7 8 9 10 11 12

Plain text : C R Y P T O G R A P H Y

(2) plain text : W E A R I N D I A N
22 4 0 17 8 13 3 8 0 13

Encryption : $E(x,4) = (x+4) \% 26$

TANUJ SAINI
2022511411

M	T	W	T	F	S	S
Page No.:					YOUVA	
Date:						

W → (22+4) %.26 = 0	A
E → (4+4) %.26 = 8	I
A → (0+4) %.26 = 4	E
R → (17+4) %.26 = 21	V
I → (8+4) %.26 = 12	M
N → (13+4) %.26 = 17	R
D → (3+4) %.26 = 7	H
I → (8+4) %.26 = 12	M
A → (0+4) %.26 = 4	E
N → (13+4) %.26 = 17	R

Cipher text : AIEVMRHMER

Decryption : D(C,4) = (26+C-4) %.26

A	→ (26+0-4) %.26	= 22	W
I	→ (26+8-4) %.26	= 4	E
E	→ (26+4-4) %.26	= 0	A
V	→ (26+21-4) %.26	= 17	R
M	→ (26+12-4) %.26	= 8	I
R	→ (26+17-4) %.26	= 13	N
H	→ (26+7-4) %.26	= 3	D
M	→ (26+12-4) %.26	= 8	I
E	→ (26+4-4) %.26	= 0	A
R	→ (26+17-4) %.26	= 13	N

Plain text : → WEARINDIAN

TANUJ SAINI
2022511141

M T W T F S S
Page No.:
Date:
YOUVA

(3)

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

- If same Row take the letter to the right
- If same col take the letter below each one
- Else take a letters on the horizontal opp. corner of the rectangle

Encryption:

plain text: WEAR INDIAN

WE AR IN DI AN

ZR HA EL BK FH

cipher text: ZRHA ELBK FH

Decryption

cipher text: ZR HA EL BK FH

WE AR IN DI AN

(4) Decryption is not possible when gcd (0,26) ≠ 1 because a will not have an inverse under modulo 26.

(5) Decrip Decryption:

$$x = (a^{-1}(26 + c - b)) \bmod 26$$

Steps to decrypt

1) Find a^{-1} (only possible if gcd $(a, 26) = 1$)

TANUS SAINZ
(112022511471)

M T W T F S S
Page No.:
Date:
YOUVA

2) Use formula $x = (a^{-1}(26+c-b)) \bmod 26$

Valid a are {1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25}
12 valid values for a
Total Keys $= 12 \times 26 = 312$

No, two different valid keys can generate same cipher text from the same plain text due to unique nature of the affine transformation when a has an inverse. Thus, for each (x, y) there is exactly one unique key.

(3) We know that taking compliment after mapping is same as mapping complimented bits.

Therefore,

$$E(\bar{R_0}) \oplus \bar{K} = \overline{E(R_0)} \oplus \bar{K}$$

$$P(S(E(\bar{R_0}) \oplus \bar{K})) = P(S(\overline{E(R_0)} \oplus \bar{K}))$$

$$f(R_0, K) = f(\bar{R_0}, \bar{K}) \quad \text{--(i)}$$

For message m & key k

$$m = L_0 || R_0$$

$$L_1 = R_0$$

$$R_1 = L_0 \oplus f(R_0, K)$$

$$C_1 = L_1 || R_1$$

TANUS SAINI
2022511141

M T W T F S S
Page No.:
Date:
YOUVA

For message $\bar{m}$ & key $\bar{k}$

$$\bar{m} = \bar{L0} \,||\, \bar{R0}$$

$$L_i = \bar{R_0} = \bar{L_1}$$

$$R_1' = \bar{L_0} \oplus f(\bar{R_0}, \bar{K})$$

$$R_1' = \bar{L_0} \oplus f(R_0, K) \quad \text{from (i)}$$

we know that

$$\bar{A} \oplus B = \overline{A \oplus B}$$

$$R_1' = \overline{L_0 \oplus f(R_0, K)}$$

$$R_1' = \bar{R_1}$$

$$L_1' \,||\, R_1' = \bar{L_1} \,||\, \bar{R_1}$$

$$C_2 = \bar{C_1}$$

Hence, If we compliment the message & the secret key then cipher text will compliments of original CT.

(6)

A F I T I F W F
0 5 8 19 8 5 22 5

Key	Decrypted text
1	ZEHSHEVE
2	YDGRGDUD
3	XCFQFCTC
4	WBEPEBSB
5	VADODARA

Possible Plain text = VADODARA

Secret Key = 5

TANUJ SAINI

2023511141

M	T	W	T	F	S	S
Page No.:						YOUVA
Date:						

⑦ Let Key $K = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

Plain text		Cipher text	
HI	LL	XI	YJ
78	11	23 8	24 9

$$[78] \begin{bmatrix} a & b \\ c & d \end{bmatrix} \bmod 26 = [23\ 8]$$

$$[7a + 8c \quad 7b + 8d] \bmod 26 = [23\ 8]$$

$$[11\ 11] \begin{bmatrix} a & b \\ c & d \end{bmatrix} \bmod 26 = [24\ 9]$$

$$[11a + 11c \quad 11b + 11d] \bmod 26 = [24\ 9]$$

$$(7a + 8a) \bmod 26 = 23 \quad -(i)$$
$$(11a + 11c) \bmod 26 = 24 \quad -(ii)$$

$$11(a+c) \bmod 26 = 24$$
$$11(a+c) \equiv 24 \bmod (26)$$

find inverse of 11 i.e 19

$$19 \times 11\ (a+c) = 24 \times 19 \bmod 26$$
$$a+c = 14 \bmod 26$$
$$a = 14 - c \bmod 26 - (iii)$$

Substitute this into eq (i)

$$7(19-c) + 8c \equiv 23 \bmod (26)$$
$$98 + c = 23 \bmod 26$$
$$98 \bmod 26 = 20$$
$$20 + c \equiv 23 \bmod 26$$
$$c = 3$$

HANUS SAINI
2022511141

$a+3 \equiv 14 \bmod 26$

Now, $(11b+11d) \bmod 26 = 9$

$(7b+8d) \bmod 26 = 8$

$11(b+d) \equiv 9 \bmod 26$

Inverse of $11 = 19$

$b+d \equiv 19 \times 9 \bmod 26$

$\equiv 171 \bmod 26$

$b+d \equiv 15 \bmod 26$

$b \equiv (15-a) \bmod 26$

$7(15-d)+8d \equiv 8 \bmod 26$

$105+d \equiv 8 \bmod 26$

$d+1 = 8 \bmod 26$

$d=7$

$b+7 \equiv 15 \bmod 26$

$b=8$

Key $K = \begin{vmatrix} 11 & 8 \\ 3 & 7 \end{vmatrix}$

(8) (a) gcd (222, 18)

Q	A	B	R
12	222	18	6
3	18	6	0
	6	0	

$\gcd = (222, 18) = 6$

(b) $1 = 33x_0 + 13y_0$

$33 = 13(2) + 7 \Rightarrow 7 = 33 - 13(2)$

$13 = 7(1) + 6 \Rightarrow 6 = 13 - 7(1)$

$7 = 6(1) + 1 \Rightarrow 1 = 7 - 6(1)$

TANUS SAINI
2022511141

$1 = 7 - 6$

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

$= 33(2) - 13(4) - 13$

$1 = 33(2) - 13(5)$

$x_0 = 2 \quad y_0 = 5$

(c) $5x \equiv 1 \bmod 26$

$5x - 1 = 26y$

$5x - 26y = 1$

$26 = 5 \times 5 + 1$ $\quad 1 = 26 - 5 \times 5$

$1 = 5 \times (-5) * 26$

$b = -5 \equiv 21 \bmod 26$

Inverse of 5 is 21

(9) $D_3 = 11010011$

$P(x) = x^7 + x^6 + x^4 + x^1 + 1$

let constant $C = C_7 C_6 C_5 C_4 C_3 C_2 C_1 C_0$

$= (01100011)$

$g(x) = x^8 + x^4 + x^3 + x + 1$

$$x^7+x^6+x^4+x+1 \;\overline{)\; x^8+x^4+x^3+x+1 \;\big|\; x+1}$$

$$\underline{x^8+x^7+x^5+x^2+x}$$

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

$$\underline{x^7+x^6+x^4+x+1}$$

$$x^6+x^5+x^3+x^2+x \;\overline{)\; x^7+x^6+x^4+x+1 \;\big|\; x}$$

$$\underline{x^7+x^6+x^4+x^3+x^2}$$

$$x^3+x^2+x+1 \;\overline{)\; x^6+x^4+x^3+x^2+x \;\big|\; x^3+x+1}$$

$$\underline{x^6+x^5+x^4+x^3}$$

$$x^5+x^2+x$$

$$\underline{x^5+x^4+x^3+x^2+x}$$

$$x^3 \;\overline{)\; x^3+x^2+x+1 \;\big|\; x}$$

$$\underline{x^3+x^2+x}$$

$$1$$

TANUS SAINI

202251141

$1 = x(x^2+x+1) + (x^3+x^2+x+1)$

$1 = x[(x^3+x^2+x+1)(x^3+x+1) + (x^6+x^5+x^3+x^2+x)] + (x^3+x^2+x+1)$

$1 = x(x^6+x^5+x^3+x^2+x) + (x^3+x^2+x+1)(x^4+x^2+x+1)$

$1 = x(x^6+x^5+x^3+x^2+x) + [(x^7+x^6+x^4+x^3+x^2)+(x^2+x^6+x^4+x+1)](x^4+x^2+x+1)$

$1 = (x^7+x^6+x^4+x+1)(x^4+x^2+x+1) + x[(x^7+x^6+x^4+x+1)(x+1)+(x^8+x^4+x^3+x+1)](x^4+x^2+x)$

$1 = P(x)(x^4+x^2+x+1) + P(x)(x^2+x)(x^4+x^2+x) + x(x^4+x^2+x)\,g(x).$

$1 = P(x)(x^4+x^2+x+1+x^6+x^4+x^3+x^5+x^3+x^2) + g(x)(x^5+x^3+x^2)$

$1 = P(x)(x^6+x^5+x+1) + g(x)(x^5+x^3+x^2)$

Inverse of $P(x)$ is x^6+x^5+x+1

$S(11010011) = 01100011$

$= m_7 m_6 m_5 m_4 m_3 m_2 m_1 m_0$

	0	1	2	3	4	5	6	7
m	1	1	0	0	0	1	1	0
c	0	1	0	0	0	1	1	0

$b_0 = 0$

$b_1 = 1$

$b_2 = 1$

$b_3 = 0$

$b_4 = 0$

$b_5 = 1$

$b_6 = 1$

$b_7 = 0$

Subbyte $(11010011) = 01100011$

66

$S(D3) = 66$

Hence, proved

TANUJ SAINI
2022511141

M T W T F S S
Page No.:
Date:
YOUVA

(10) 33 = 100001 = x^5+1

42 = 101010 = x^5+x^3+x

66 = 1000010 = x^6+x

24 = 11000 = x^4+x^3

$$\begin{vmatrix} x & x+1 & 1 & 1 \\ 1 & x & x+1 & 1 \\ 1 & 1 & x & x+1 \\ x+1 & 1 & 1 & x \end{vmatrix} \begin{vmatrix} 33 \\ 42 \\ 66 \\ 24 \end{vmatrix} = \begin{vmatrix} S_0' \\ S_1' \\ S_2' \\ S_3' \end{vmatrix}$$

$$\begin{vmatrix} x & x+1 & 1 & 1 \\ 1 & x & x+1 & 1 \\ 1 & 1 & x & x+1 \\ x+1 & 1 & 1 & x \end{vmatrix} \begin{vmatrix} x^5+1 \\ x^5+x^3+x \\ x^6+x \\ x^4+x^3 \end{vmatrix}$$

For S_0'

$\Rightarrow x^6+x+x^6+x^4+x^2+x^5+x^3+x+x^6+x+x^4+x^3$

$\Rightarrow x^6+x^5+x^2+x$

01100110 = 102

For S_1'

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

$= 10101011$

$= 171$

For S_3'

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

$= x^7+x^5+x^2+x+1$

$= 10100111$

$= 167$

TANUJ SAINI
202251141

M T W T F S S
Page No.:
Date:
YOUVA

for S_4

$x^6 + x^4 + x^5 + x^3 + x^4 + x^6 + x^4 + x^5 + x^4$

$= 01011010$

$= 26$

$$\begin{bmatrix} 102 \\ 171 \\ 187 \\ 26 \end{bmatrix}$$ ans

(11) $ax + b = y \bmod p$ (i)

$ax' + b = y' \bmod p$ (ii)

on solving (i) & (ii)

$a(x - x') \equiv (y - y') \bmod p$

$a \equiv (y - y')(x - x')^{-1} \bmod p$

Thus, we can compute a, given $x \neq x'$.
(ensuring $x - x'$ is invertible)

Substitute value of a on eq(1) & you will get b

$b \equiv y - ax \pmod p$

Yes, it is possible to find a & b given x, x', y, y' as long as $x \neq x'$.