CS 304
Cryptography & Network Security
(Assignment)
(1)

Dipean Dasgupta
202151188

Assignment 1
Date 15 03 24

Q1)

(a)

PT = CRYPTOGRAPHY $\quad \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 5 & 6 & 9 & 11 & 1 & 8 & 2 & 10 & 4 & 12 & 7 \end{pmatrix}$

Here, secret key = Permutation of plaintext [in Transposition cipher]

Row 1 = actual positions of the plaintext.

Row 2 = position of characters in ciphertext

So, as per rule. here, 1st char → 3rd position, 2nd → 5th position

∴ Plaintext = CRYPTOGRAPHY

∴ Ciphertext = YTOAHCRRPPYG

(b) $\pi : S \to S$ bijection from S to S.

[S → set of characters in plaintext]

So, its order of elements mapped to different set

Ordering of elements from same set.

Since, bijection → always invertible.

So, through inversion character's position will be mapped back to original positions. (that of the plaintext).

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

So, here, 6th char in CT = 1st character in PT (plaintext) = C

Similarly, all other characters are placed to get the original plaintext

∴ Decryption:

CT : YTOAHCRRPPYG

PT : CRYPTOGRAPHY

Hence, decryption is possible.

Dipsan Dasgupta
20215188

Page No.
Date

Q2)

For shift cipher,

Encryption: $C = (P+k) \bmod 26$ | Decryption: $P = (C-k) \bmod 26$

where, C = ciphertext, P = Plaintext, K = secret key +ve, $P = (26+C-k) \bmod 26$

Here,

Plaintext = WEARINDIAN secret key = 4.

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

Ciphertext(C) = AIEVIMRHMER

= AIEVIMRHMER

Plaintext(P) decrypted = WEAREINDIAN

= WEAREINDIAN

Q3)

Given Plaintext: WEAREINDIAN Secret key: CRICKET.

Step1: Forming the 5×5 matrix using secret key and alternate. Since, 25 elements in matrix, 2 alphabets merged [I=J]

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

Step2:

Since, the plaintext is of odd number characters, so a delimiter 'X' is added at last to make it even.

Processed text: WEAREINDIANX ⇒ WE AR EI ND IA NX

Dipean Dasgupta
20215 1188

Page No.
Date

Step 3

Rules: (Row column cyclic movement).

(1) characters of pair same row:
Cipher pair => immediate next (right) of PT pair.

(2). same column => immediate next down/below.

(3). Different row/column - for cipher text the characters will be of the same row the column will of the other one, and so followed for others also.

	For the 1st 3 pairs			For next 3 pairs		
PT:	WE	AR	EI	ND	IA	NX
CT:	ZR	HA	CK	LF	RB	JZ
	rule 3	rule 2	rule 1		rule 3	

∴ ENC(WEAREINDIANX) = ZRHA CKLF RBJZ

For Decryption,

Done on same matrix with rules reversed:
left move for same row, up move for same column.
=> same rule for different row, column.

So,

1st 3 pairs:			last 3 pairs:		
ZR	HA	CK	LF	RB	JZ
WE	AR	EI	ND	IA	NX
rule 3	rule 2	rule 1		rule 3	

DEC(ZRHACKLFRBJZ) = WEAREINDIANX

So, preprocessed text is retrieved. Now, removing the extra x added as delimiter we get the plaintext:

WEAREINDIAN.

Dipean
20211188

Page No.
Date

Q4)

Key is $K = (a, b)$ $\quad 0 \le a, b \le 25$

$y := Enc(x) = (ax + b) \bmod 26$.

Decryption for the above encryption will be

$x = Dec(y) = ((y - b) \cdot a^{-1}) \bmod 26$.

a^{-1} = mult. inverse of a under modulo 26.

a^{-1} exists iff $gcd(a, 26) = 1$.

∴ For all those pairs where $gcd(a, 26) \neq 1$ (a, b) is not a key for an affine cipher and decryption is also not possible.

Therefore for:

$a \in \{a \in Z$ such that, a even and $-0 \le a \le 26\}$.

and $\forall$ b such that $0 \le b \le 26$, decryption not possible.

② When we have successful decryption:

$x = Dec_K(y) = ((y - b) \cdot a^{-1}) \bmod 26$.

a^{-1} mult. inverse of a under modulo 26.

$\therefore a * a^{-1} \equiv 1 \bmod 26$.

③ It is required to find different number of keys for which PT-CT pair same.

$K_1 (a, b)$ $K_2 (a', b')$ such that $K_1 \neq K_2$.

and PT-CT pair same.

$$ax + b \equiv y \bmod 26 \quad -(i)$$

$$a'x + b' \equiv y \bmod 26 \quad -(ii)$$

(i)-(ii)

$$(a' - a)x + (b' - b) \equiv 0 \bmod 26 \quad -(iii)$$

Now, $x \in \{0, 1, \ldots 25\}$ put $x = 0$ in (iii)

$$(a' - a) \cdot 0 + (b' - b) \equiv 0 \bmod 26.$$

$$\therefore (b' - b) \equiv 0 \bmod 26. \quad -(iv)$$

As $b, b' \in \{0, 1 \ldots 25\}$. Therefore max value of $(b' - b)$ can be 25. Hence (iv)

holds iff $b' = b$. Eqn (iii) reduced to.

$$a'-a)x \equiv n \bmod 26.$$

$$(a'-a) \equiv 0 \cdot x^{-1} \bmod 26.$$

$$(a'-a) \equiv 0 \bmod 26 \quad -(v).$$ x' also an integer.

Again $a \cdot \in \{$odd num. and $1 \le a \le 25\}$. ∴

∴ max value of $(a'-a)$ is equal to 24.

∴ v holds only iff $(a' = a)$.

∴ Our assumption that $k_1 \neq k_2$ is wrong

Hence, 2 different keys will not result in same PT-CT pair (x, y).

Q5/

Enc is encryption function of DES.

$$c_1 = \text{Enc}(m, k). \quad c_2 = \text{Enc}(\bar{m}, \bar{k}).$$

KSA of DES:

1. First removes parity bit of 64 bit key.
2. Performs permutation PC1.
3. a Left circular shift (LCS), and substitution.

LCS. shifts input to left by fixed positions in circular way.

$$\text{LCS}(x_1 \ldots x_{32},) = x_3 x_4 \ldots x_{32} x_1 x_2.$$

and $\text{LCS}(\bar{x}_1, \ldots \bar{x}_{32}, 2) = \bar{x}_3 \bar{x}_4 \ldots \bar{x}_{32}, \bar{x}_1 \bar{x}_2.$

If we input complementary keys k and $\bar{k}$ to KSA round keys generated will be complimentary.

In 1 round of fiestel network:

$$L_1 = R_0 \text{ and } R_1 = f(R_0, k_1) \oplus L_0.$$

Dream
20215188

Page No.
Date

R_{xM}, L_{xM} → denotes about PT M and key k.

$R_{x\bar{M}}, L_{x\bar{M}}$ → " " " PT $\bar{M}$ and " $\bar{k}$.

considering (M,k) & $(\bar{M},\bar{k})$ as input to DES.
Therefore, after first round.

$$M = L_{0M} \| R_{0M} \text{ and } \bar{M} = L_{0\bar{M}} \| R_{0\bar{M}}$$
$$L_{1M} = R_{0M} \text{ and } L_{1\bar{M}} = R_{0\bar{M}}$$

$\therefore L_{1M}$ and $L_{1\bar{M}}$ are complimentary.

$$R_{0M} = x_{32M}\, x_{33M} \cdots x_{63M}$$
$$R_{0\bar{M}} = \bar{x}_{32M}\, \bar{x}_{33M} \cdots \bar{x}_{63M}$$

$$E(R_{0\bar{M}}) = \bar{x}_{63M}\, \bar{x}_{32M} \cdots \bar{x}_{32M} \quad | \quad E(R_{0\bar{M}}) = \overline{x_{63M}\, x_{32M} \cdots x_{32M}}.$$
$$E(R_{0\bar{M}}) = \overline{E(R_{0M})} \quad \text{--- (i)}$$

$$f(\bar{M},\bar{k}) = P(S(E(R_{0\bar{M}} \oplus \bar{k}_1))).$$
$$= P(S(\overline{E(R_{0M})} \oplus \bar{k}_1)).$$
$$= P(S(E(R_{0M} \oplus k_1))).$$
$$f(\bar{M},\bar{k}) = f(M,k) \quad \text{--- (ii)}.$$

Therefore,

$$R_{1M} = f(R_{0M}, k_1) \oplus L_{0M} \text{ and } R_{1\bar{M}} = f(R_{0\bar{M}}, \bar{k}_1) \oplus L_{0\bar{M}}.$$
$$\therefore R_{1\bar{M}} = \overline{R_{1M}}.$$

Therefore, outputs of round of DES will be complimentary given inputs PT and key are complimentary. Applying permutation IP and another IP^{-1} but perm. doesn't alter complimentary property.

$$\therefore C_1 = Enc(M,k).$$
$$C_2 = Enc(\bar{M},\bar{k}).$$
$$C_2 = \bar{C}_1 \text{ (shown)}$$

Dipsam Dasgupta
2021511023.

Page No.
Date

Q6

Ciphertext = AFITIFWF, plaintext and key unknown
As plaintext will be a meaningful word, and secret key not given, so the only way is search on all possible combinations until a meaningful word is attained.
For shift cipher we know.

$ENC(x,k) = (x+k) \bmod 26$
$DEC(x,k) = (x-k) \bmod 26$ x = index of alphabet.

So, Decryption:
Using key(k)=1, we get: ZEHSHEVE (not meaningful)
(shifting alphabet integers by 1).

Using key(k) = 2, we get: YDGRGDUD.
Similarly,
⇒ For k=3 : = XCFQFCTC
⇒ For k=4. = WBEPEBSB
⇒ For k=5, = VADODARA.
∴ Hence at k=5, we get plaintext - VADODARA. which is meaningful and name of a place in India.
Checking the other keys, in a shift cipher decryption code in C, only meaningful word came with key(k)=5.

So, decrypted Plaintext: VADODARA

Dipeam
2021511128.

Page No.
Date

Q.7

In Hill cipher if key is a n×n matrix, we divide PT into n-char blocks. Then do.

$C = K \cdot P \bmod 26$.

Mult. both sides by P^{-1} gives,

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

⇒ Given : PT : HILL.

⇒ corr. Cipher : XIYT.

Key $K = \begin{bmatrix} k_1 & k_2 \\ k_3 & k_4 \end{bmatrix}$

$K = \begin{bmatrix} X & Y \\ I & T \end{bmatrix} \begin{bmatrix} H & L \\ I & L \end{bmatrix}^{-1} \bmod 26$.

$= \begin{bmatrix} 23 & 24 \\ 8 & 19 \end{bmatrix} \cdot \begin{bmatrix} 7 & 11 \\ 8 & 11 \end{bmatrix}^{-1} \bmod 26$.

$K = (-11)^{-1} \cdot \begin{bmatrix} 23 & 24 \\ 8 & 9 \end{bmatrix} \begin{bmatrix} 7 & 15 & -11 \\ -8 & -8 & 7 \end{bmatrix} \bmod 26$.

$= (15)^{-1} \begin{bmatrix} 23 & 24 \\ 8 & 9 \end{bmatrix} \begin{bmatrix} 11 & -11 \\ -8 & 7 \end{bmatrix} \bmod 26$

Mult inverse of 15 mod 26.

$15)26(1$
$\quad 15$
$11)15(1$
$\quad 11$
$4)11(2$
$\quad 8$
$3)4(1$
$\quad 3$
$\quad 1$

$1 = 4 - 1 \cdot 3$
$1 = 4 - (11 - 2 \times 4)$
$1 = 3 \times 4 - 11$
$1 = 3(15 - 11) - 11$
$1 = 3 \cdot 15 - 4 \cdot 11$
$1 = 3 \cdot 15 - 4 \cdot (26 - 15)$
$1 = (7) \cdot 15 - 4 \cdot 26$

mult inverse is 7.

$K = 7 \begin{bmatrix} 61 & -85 \\ 16 & -25 \end{bmatrix} \bmod 26 = \begin{bmatrix} 63 & 133 \\ 112 & 7 \end{bmatrix} \bmod 26 = \begin{bmatrix} 11 & 3 \\ 8 & 7 \end{bmatrix}$

∴ Key K is $\begin{bmatrix} 11 & 3 \\ 8 & 7 \end{bmatrix}$

Dipeam
202151188

Page No.
Date

Q8 soln

(a) Finding gcd (222,18) using euclidean algorithm

```
18)222(12
   18x1
   ----
    42
    36
    --
     6)18(3
       18
       --
        0
```

∴ gcd (222,18) = 6

b) Finding x_0, y_0 such that $1 = 33x_0 + 13y_0$.

Finding gcd (33,13)

```
13)33(2
   26
   --
    7)13(1
      7
      -
      6)7(1
        6
        -
        1)6(6
          6
          -
          0
```

gcd (13,33) = 1

Using bezouts identity, we find x_0, y_0, $\gcd(x,y) = ax+by$

Algo :

$1 = 7 - (1 \times 6) = 7 - (13 - 1 \times 7) = 2 \times 7 - 13 = 2 \times (33 - 2 \times 13) - 13$

$= 2 \times 33 - 5 \times 13$ of form $ax+by$

$\therefore x = x_0 = 2, \quad y_0 = b = -5$

(c) Multiplicative inverse of 5 under modulo 26.

finding gcd : gcd (5,26) is 1. (as 5 = prime number).

$\therefore 1 = 26 - 5 \times 5$

As per bezouts identity: $\gcd(x,y) = ax + by$

By extended euclidian algorithm

$1 = 26 - 5 \times 5 = 26 - (26 - 5 \times 21) \times 5 = 26 \times 1 + (-5) \times 21$

so, we get multiplicative inverse of 5 modulo 26 is 21.

Dipean
2021511128

Page No.
Date

Q9 soln,

Given input $(D3)_{16}$: output = 66.

primitive polynomial = $x^8 + x^4 + x^3 + x + 1$ | $(D3)_{16} = (11010011)_2$

$(D3)_{16} = (11010011)_2$. polynomial = $x^7 + x^6 + x^4 + x + 1$

Finding inverse using extended euclidian algorithm:

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

$x^8+x^7+x^5+x^4+x$

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

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

$x^6+x^5+x^3+x^2+x$

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

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

x^3+x^2+x+1

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

x^3+x^2+x

1

$x^3+x^2+x+1 \overline{)x^6+x^5+x^3+x^2+x} \; (x^3+x+1$

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

x^4+x^2+x

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

x^3

x^3+x^2+x+1

x^2+x+1

$1 = (x^3+x^2+x+1) + (x)(x^2+x+1)$. (+ - same as mod 2)

$= (x^3+x^2+x+1) + x\{(x^6+x^5+x^3+x^2+x) + (x^3+x+1)\cdot(x^3+x^2+x+1)\}$

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

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

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

$= P(x)\{x^4+x^2+x+1\} + (x^6+x^5+x^3+x^2+x)\{x^5+x^3+x^2\}$

$= P(x)\{x^4+x^2+x+1\} + \{(x^8+x^4+x^3+x+1) + P(x)(x+1)\}$

$Q(x)$

$(x^5+x^3+x^2)$.

$= (x^5+x^3+x^2)\,Q(x) + P(x)\{(x^5+x^3+x^2)(x+1) + (x^4+x^2+x+1)\}$

$= (x^5+x^3+x^2)\,Q(x) + (x^6+x^5+x+1)\,P(x)$.

Dipeam
2021511188

Page No.
Date

The inverse found := $x^6+x^5+x+1 = P(x)$

Binary form of $P(x) = (01100011)_2 = b_7 b_6 \cdots b_0$.

$\therefore S(11010011) = 01100011$

Given, C is constant $(63)_{16} = (01100011)_2$

Calculating $m_7 m_6 m_5 m_4 m_3 m_2 m_1 m_0$ ...

for $(i = 0$ to $7)$

$m_i = b_i + b_{(i+4)\%8} + b_{(i+5)\%8} + b_{(i+6)\%8} + b_{(i+7)\%8} + c_i \%2$

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

$m_0 = (b_0+b_4+b_5+b_6+b_7+c_0)\%2 = (1+0+1+1+0+1)\%2 = 0$

In this way,

$m_1 = (1+1+1+0+1+1)\%2 = 1$

$m_2 = (0+1+0+1+1+0)\%2 = 1$

$m_3 = 0$, $m_4 = 0$

$m_5 = 1$, $m_6 = 1$, $m_7 = 0$

$\therefore$ Subbyte $(D3) := m_7 m_6 \cdots m_0 = (01100110)_2$

$\therefore (01100110)_2 = (0110\ 0110)_{16}$

$= 0\times2^7 + 1\times2^6 + 1\times2^5 + 0\times2^4 + 0\times2^3 + 1\times2^2 + 1\times2^1 + 0\times2^0$

$= (66)_{16}$

$\therefore$ Subbyte of $(D3)_{16}$ is $(66)_{16}$. proved.

Dipean
20215128

Page No.
Date

Q.10 soln

Given inputs 33, 42, 66, 24 . for AES mixcolumn.

Converting each of them to binary.

$33 = (00100001)_2$ $42 = (00101010)_2$, $66 = (01000010)_2$.

polynomials corresponding

$33 = t_0 = x^5+1$ $42 = t_1 = x^5+x^3+x$

$66 = t_2 = x^6+x$. $24 = t_3 = x^4+x^3$.

Now for AES mixcolumn.

$$\begin{bmatrix} x & x+1 & 1 & 1 \\ 1 & x & x+1 & 1 \\ 1 & 1 & x & x+1 \\ x+1 & 1 & 1 & x \end{bmatrix} \begin{bmatrix} t_0 \\ t_1 \\ t_2 \\ t_3 \end{bmatrix} = \begin{bmatrix} v_0 \\ v_1 \\ v_2 \\ v_3 \end{bmatrix} \bmod (x^8+x^4+x^3+x+1)$$

$\rightarrow P(x)$

$v_0 = (x.t_0 + (x+1)t_1 + t_2 + t_3) \bmod P(x)$.

$= x(x^5+1) + (x+1)(x^5+x^3+x) + x^6+x + x^4+x^3) \bmod P(x)$

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

$= x^6+x^5+x^2+x$

$v_1 = (t_0 + x t_1 + (x+1) t_2 + t_3) \bmod P(x)$

$= (x^5+1 + x(x^5+x^3+x) + (x+1)(x^6+x) + x^4+x^3) \bmod P(x)$

$= (x^5+1 + x^6+x^4+x^2 + x^7+x^4+x^6+x+x^4+x^3) \bmod P(x)$

$= x^7+x^5+x^3+x+1$

$v_2 = (t_0+t_1+x t_2 + (x+1)t_3) \bmod P(x)$

$= (x^5+1 + x^5+x^3+x + x(x^6+x) + (x+1)(x^4+x^3)) \bmod P(x)$

$= x^5+1 + x^5+x^3+x + x^7+x^2 + x^5+x^4+x^3) \bmod P(x)$

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

$U_3 = \{(x+1)t_0 + t_1 + t_2 + x t_3\} \bmod P(x)$.

$= \{(x+1)(x^5+1) + x^5 + x^3 + x + x^6 + x + x(x^4+x^3)\} \bmod P(x)$

$= (x^6 + x + x^5 + 1 + x^5 - x^3 + x - 1 x^6 + x - 1 x^5 - 1 x^4) \bmod P(x)$

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

Binary corresponding to polynomials.

$U_0 = x^6 + x^5 + x^2 + x = (011\,00110)_2 = 102$

$U_1 = x^7 + x^5 + x^3 + x + 1 = (10101011)_2 = 171$

$U_2 = x^7 + x^5 + x^2 + x + 1 = (10100111)_2 = 167$

$U_3 = x^5 + x^4 + x^3 + x + 1 = (00111011)_2 = 59$

∴ AES MixColumn (33, 42, 66, 24)
$= (102, 171, 167, 59)$

MixCol(33, 42, 66, 24) = (102, 171, 167, 59)

Q.11/

$f(a,b) : Z_p \to Z_p$ by rule $f_{(a,b)}(x) = ax + b \bmod p$.

Given, $f_{(a,b)}(x) = y$ and $f_{(a,b)}(x') = y'$ and $x \neq x'$

We know, x, y, x', y' and we need to prove if (a,b) can be found. It can be said,

$ax + b \equiv y \bmod p$ ... (i) $\quad (ax' + b) \equiv y' \bmod p$ ... (ii)

(i) − (ii)

$a(x' - x) = (y' - y) \bmod p$.

$\because x' \neq x \Rightarrow x' - x \neq 0$.

If inverse of $(x' - x)$ under modulo p, we can find a.

Inverse of $(x' - x)$ under modulo p exists iff $\gcd(x' - x, p) = 1$

∴ p is a prime number ∴ gcd $(x'-x, p)$ will be 1
∴ Inverse of $(x'-x)$ under modulo p

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

once, a is found using above equation, b can be found putting value of a in either (i) or (ii)

Q12/

Let $x = [x_1\ x_2\ x_3\ x_4\ x_5\ x_6\ x_7]$

$$\therefore [x_1\ x_2\ x_3\ x_4\ x_5\ x_6\ x_7] \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \bmod 2 = [0\ 1\ 0\ 1]$$

$$\begin{bmatrix} x_1 + x_2 + x_3 + x_4 \\ x_2 + x_3 + x_4 + x_5 \\ x_3 + x_4 + x_5 + x_6 \\ x_4 + x_5 + x_6 + x_7 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

— (i)
— (ii)
— (iii)
— (iv)

(ii − i) ⇒ $x_1 = x_3 + 1$ — (v)
(iii) − (ii) ⇒ $x_2 = x_6 - 1$ — (vi)
(iv) − (iii) ⇒ $x_3 = x_7 + 1$ — vii

As all operation are under modulo 2, from (iv) we conclude either one or out of x_4, x_5, x_6, x_7 is 1 or any 3 are 1 to satisfy eqn (iv). All possible values
{(1,0,0,0), (0,1,0,0), (0,0,1,0), (0,0,0,1), (1,1,1,0), (1,1,0,1), (1,0,1,1), (0,1,1,1)}.

Dipean
202151188

Page No.
Date

we find value of x_1, x_2, x_3 for each tuple: using v, v_1, v_{11}.

All possible pre image

	x_1	x_2	x_3	x_4	x_5	x_6	x_7
1.	1	1	1	1	0	0	0
2.	0	1	1	0	1	0	0
3.	1	0	1	0	0	1	0
4.	1	1	0	0	0	0	1
5.	0	0	1	1	1	1	0
6.	0	1	0	1	1	0	1
7	1	0	0	1	0	1	1

Tuples mentioned are pre-images of (0,1,0,1) under given rule h.

Q 13

To prove that, let's say h_u is not collision resistant. There exists $x_1, x_2 \in \{0,1\}^{4m}$ such that $x_1 \neq x_2$ and $h_2(x_1) = h_2(x_2)$ Lets define $x_1 \neq x_2$ as:

$$x_1 = x_{11} \,||\, x_{12} \quad x_2 = x_{21} \,||\, x_{22}$$

where, x_{11}, x_{12}, x_{21} and $x_{22} \in \{0,1\}^{2m}$ &
since, $h_2(x_1) = h_2(x_2)$ from def^n.

$$h_1[h_1(x_{11}) \,||\, h_1(x_{12})] = h_1[h_1(x_{21}) \,||\, h_1(x_{22})] \quad (1)$$

Since h_1 is collision resistant, its hard to find.
$x_a \neq x_b$ such that $h_1(x_a) = h_1(x_b)$.
Eq^n (1) →

$$h_1(x_{11}) \,||\, h_1(x_{12}) = [h_1(x_{21}) \,||\, h_1(x_{22})]$$

P.T.O

Dipeam
2021511128

Page No.
Date

Using concatenation property of string we can write:

$$h_1(x_{11}) = h_1(x_{21})$$
$$h_1(x_{12}) = h_1(x_{22})$$

∵ h_1 is collision resistant we can say,

$$x_{11} = x_{21} \quad -(ii)$$
$$x_{12} = x_{22} \quad -(iii)$$

from (ii) and (iii) we have $x_1 = x_2$ which contradicts our assumption that $x_1 \neq x_2$. Hence h_2 is a collision ~~restant~~ resistant function.