2021511138

Sanidhya Kumar

CS304

Date 15/3/24

Assignment 1

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

Plaintext : CRYPTOGRAPHY

(a) In transposition cipher we basically permute the plaintext as per the given secret key, which is essentially a permutation π. The 1st row represents position of the final encrypted text and the 2nd row represents those positions that would be used to construct the encrypted text.

For example, $\begin{pmatrix} 1 & 2 & 3 & 4 & \cdots \\ \downarrow & \downarrow & \downarrow & \downarrow & \\ 3 & 5 & 6 & 9 & \cdots \end{pmatrix}$

This means, 3rd character of plaintext will become 1st character in encrypted text and so on.

Using this logic, encrypted text = **YTOAHCRRPPYG**

(b) Permutation π is basically a bijective mapping from set $S \rightarrow S$. [S = set of characters in plaintext] It is essentially a mapping and hence it is always invertible. (∵ Bijections are invertible).

For decryption, we would use the following inverse permutation.

20215138

Sowidhya Kumar

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

Lets understand this mapping, this mapping means that the 6th character from the ciphertext will become the 1st character in the decrypted text and so on..

Using this logic, decrypted text = **CRYPTOGRAPHY**

20215138
Sanidhya Kumar

classmate
Date
Page

Q.2) Shift cipher is basically shifting each character of the plaintext by a fixed no. of characters keeping in mind that it is mod 26.

So, $Enc(x, k) = (x+k) \bmod 26$

and $Dec(c, k) = (c+26-k) \bmod 26$

x = plaintext

k = key (positions to be shifted)

c = ciphertext

It is important to note that A=0, B=1, ---- Z=25.

Using this logic, ciphertext for WEAREINDIAN is-

	W	E	A	R	E	I	N	D	I	A	N
$(22+4) \% 26$ ↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
	A	I	E	V	I	M	R	H	M	E	R

Hence, ciphertext = **AIEVIMRHMER**

Now, lets decrypt using method defined above—

	A	I	E	V	I	M	R	H	M	E	R
$(0+26-4) \% 26$ ↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
	W	E	A	R	E	I	N	D	I	A	N

Hence, decrypted text = **WEAREINDIAN** Hence, correct!

2021511138
Saidhya Kumar

Q.3) Plaintext : WEARE INDIAN
Secret Key : CRICKET

First of all, lets build the 5×5 playfair Matrix using all the rules of playfair cipher. (I=J)

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

Next step is to add a delimiter 'X' b/w repeated characters but since we do not have any repeated characters, we skip this step and move on to making length of plaintext even by adding a 'x' at last

∴ Processed text = WEAREINDIANX

Now, lets break it into blocks of two :-

WE	AR	EI	ND	IA	NX
1	2	3	4	5	6

2021S1138

Sanidhya Kumar

Let us now encrypt it using the 5×5 matrix—

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

→ for blocks 1, 2, 3, 4

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

→ for block 5, 6

∴ Ciphertext = ZR HA CK MF RB LZ

Let us now decrypt it using the rules for decryption for playfair cipher & the 5×5 matrix —

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

ZR HA CK MF RB LZ
1 2 3 4 5 6

→ for blocks 1, 2, 3, 4

2021S1138
Sanidhya Kumar

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

→ for blocks 5, 6

∴ Decrypted text = WEAREINDIANX

We got our preprocessed string back, hence verified playfair cipher!

20215138
Sanidhya Kumar

Q.4) In Affine cipher, $K = (a, b)$ —— $0 \leq a, b \leq 25$
and $Enc(x) = (ax + b) \% 26$

In case of affine cipher, decryption is not possible when the key a is not relatively prime (co-prime) to 26. This means that a and 26 have a common factor other than 1. If a and 26 have a common factor, there exists some letters that cannot be decrypted unambiguously because multiple letters would map to the same ciphertext.

$\gcd(a, 26) \neq 1$

The decryption algorithm for Affine cipher is —

1. Find the modular multiplicative inverse of $a \% 26$
Lets denote this as a^{-1}.
2. Calculate $x = a^{-1}(y - b) \% 26$.

Here, the condition is $\gcd(a, 26) = 1$

Now, we have to find combination of a & b for which they will result same (x, y)

$k_1 (a, b)$ and $k_2 (a', b')$

$k_1 \neq k_2$

$ax + b \equiv y \pmod{26}$ —— (1)

$a'x + b' \equiv y \pmod{26}$ —— (2)

$(a - a')x + (b - b') \equiv 0 \pmod{26}$ —— (3)

As we know x can take any value b/w 0 to 25, lets say $x = 0$

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

$$(b - b') \equiv 0 \bmod 26 \quad \text{——} (4)$$

b and b' can also take any value b/w 0 to 25.

To satisfy eqn (4) lets $\rightarrow b' = b$

So eq" (3) becomes —

$$(a - a')x \equiv 0 \bmod 26$$

$$(a - a') \equiv 0 \bmod 26 \quad \text{——} (5)$$

There are 12 possible values. ($\gcd(a, 26) = 1$)

for a to satisfy eqn (5), $a' = a$ will be true

As $a' = a$ & $b' = b$ So $k_1 = k_2$

∴ Our assumption was wrong.

So, for any value of (x, y), two diff. keys never result in same pair of plaintext-ciphertext (x, y).

So, answer is [0].

2021511138
Saidhya Kumar

Q.5) Given that $C_1 = Enc(m, K)$ ... (1)

$C_2 = Enc(\bar{m}, K)$ ... (2)

where, Enc is encryption fn of DES.

$X = (x_1, \dots x_n)$

$\bar{X} = (1 \oplus \bar{x_1} \oplus \dots 1 \oplus \bar{x_n})$

We have to find relation b/w C_1 and C_2.

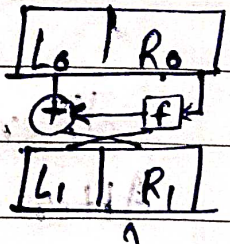
⇒ Case 1 – Complement as Normal Way –

The key scheduling algo produced round keys $K_1, K_2, K_3 \dots K_{16}$ while the complemented key scheduling algo produces round keys $\bar{K_1}, \bar{K_2}, \dots, \bar{K_{16}}$.

This complementation part is not affected by PC1, PC2 and left shift operations used in Enc. fn of DES. Let us jump into round fn. and see what happens there –

Consider the initial setup as follows:

	$\bar{m}$	$\bar{m}$
Got:	$L_0 \| R_0$	$\bar{L_0} \| \bar{R_0}$
To prove:	$L_1 \| R_1$	$\bar{L_1} \| \bar{R_1}$



In the first round: $L_1 = R_0$

$R_1 = L_0 \oplus f(R_0)$

and: $\bar{L_1} = \bar{R_0}$

$\bar{R_1} = \bar{L_0} \oplus f(\bar{R_0})$ — (A)

Let see what happens inside $f(\cdot)$

$$f(B) = f(R_i, k) = P(S(E(R_0) \oplus k))$$

Lets check f for $\overline{R_0}$

$$f(\overline{R_0}) = f(\overline{R_0}, \overline{k})$$
$$= P(S(E(\overline{R_0}) \oplus \overline{k}))$$
$$= P(S(\overline{E(R_0)} \oplus \overline{k})) \quad \because E(\overline{R_0}) = \overline{E(R_0)}$$
$$= P(S(E(R_0) \oplus k)) \quad \because \overline{A} \oplus \overline{B} = A \oplus B$$

This is actually $f(R_0)$

$\because$ (A) becomes as follows—

$$\overline{R_1} = \overline{L_0} \oplus f(\overline{R_0})$$
$$= \overline{L_0 \oplus f(R_0)} \longrightarrow \text{from above}$$
$$= L_0 \oplus f(R_0) \quad \because \overline{A} \oplus B = \overline{A \oplus B}$$
$$= R_1$$

Therefore, after 1 round we get $\overline{L_1} \,||\, \overline{R_1}$
After 16 such rounds, final $\overline{L_{16}} \,||\, \overline{R_{16}}$
Then again we apply IP^{-1} which has no effect and is also complemented.
Consequently, $\boxed{C_1 = \overline{C_2}}$ at the end.

2021511138

Sowidhya Kumar

More clearly,

for Enc (m, k) we get C_1 as $L_{16} \| R_{16}$ then apply IP^{-1}

for Enc $(\bar{m}, \bar{k})$, we get C_2 as $\bar{L}_{16} \| \bar{R}_{16}$ then apply IP^{-1}

IP^{-1} has no role $\therefore$ does not affect complement.

Therefore, finally,

$$\boxed{\begin{aligned} Enc(m, k) &= C_1 \\ Enc(\bar{m}, \bar{k}) &= \bar{C_1} = C_2 \end{aligned}}$$ final conclusion.

$$\boxed{\therefore C_1 = \bar{C_2}}$$

⇒ Case 2: Complement as per Sir's method given in question. $\bar{X} = (1 \oplus \bar{x} \oplus \cdots \oplus \bar{x}_n)$

we get, $X = \bar{X}$ $\therefore \boxed{C_1 = C_2}$

↓

eg $X = 1010$

$(\bar{X}) = 1010$

↓

Sir's way of defining.

Q.6) In shift cipher, we have a plaintext which gets shifted character by character by a fixed key k.

Now, to decrypt the same, we shift each character in the opposite direction by same amount k. We will do this until we find a meaningful plaintext back (in case, we don't know k).

Enc $(x, k) = (x+k) \% 26$

Dec $(x, k) = (x-k) \% 26$

Note that A=0, B=1, ... Z=25 here, for x.

We will use bruteforce, ~~until~~ and vary k from 1 to 25 until we get a meaningful decryption.

1) k=1 decryption—

Ciphertext : AFITIFWF

Plaintext decrypted : ZEHSHEVE

∵ decrypted text has no meaning, move forward.

2) k=2 decryption—

Ciphertext : AFITIFWE

decrypted : YDGRGDUD

20215 1138

Sowidhya Kumar

classmate
Date
Page

∴ decrypted text has no meaning, move forward.

3) k = 3 decryption –

Ciphertext : AFITIFWF

decrypted : XCFQFCTC

∴ decrypted text has no meaning, move forward.

4) k = 4 decryption –

Ciphertext : AFITIFWF

decrypted : WBEPEBSB

∴ decrypted text has no meaning, move forward

5) k = 5, decryption –

Ciphertext : AFITIFWF

decrypted : VADODARA

∴ decrypted text makes sense and has a meaning, we finall stop here.

∴ Plaintext = **VADODARA**

Secret key = **5**

2021511138
Sanidhya

Q.7) In Hill Cipher, we have a secret key $A = (a_{ij})_{n \times n}$ such that A is invertible and $M = [m_1\ m_2\ m_3 \cdots m_n]$

Hence, ciphertext $C = AM$ (mod 26)

$\therefore C_i = \sum_{j=1}^{n} a_{ij} m_j$

lets see C and M now. Here given

$M = HILL = \begin{bmatrix} 7 \\ 8 \\ 11 \\ 11 \end{bmatrix}$ and $C = XIYJ = \begin{bmatrix} 23 \\ 8 \\ 24 \\ 9 \end{bmatrix}$

using the mapping A = 0, B = 1, C = 2, ... Z = 25

lets assume $A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix}$

$\Rightarrow \begin{bmatrix} 23 \\ 8 \\ 24 \\ 9 \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix} \begin{bmatrix} 7 \\ 8 \\ 11 \\ 11 \end{bmatrix}$

From this, we will get four eq^s :-

$$7a_{11} + 8a_{12} + 11a_{13} + 11a_{14} = 23$$

~~$7a_{12} + 8a_{13}$~~

$$7a_{21} + 8a_{22} + 11a_{23} + 11a_{24} = 8$$
$$7a_{31} + 8a_{32} + 11a_{33} + 11a_{34} = 24$$
$$7a_{41} + 8a_{42} + 11a_{43} + 11a_{44} = 11$$

All eqns are under modulo 26, so we will add 26 to RHS since we are not getting soln's with this →

$$7a_{11} + 8a_{12} + 11a_{13} + 11a_{14} = 49$$
$$7a_{21} + 8a_{22} + 11a_{23} + 11a_{24} = 34$$
$$7a_{31} + 8a_{32} + 11a_{33} + 11a_{34} = 50$$
$$7a_{41} + 8a_{42} + 11a_{43} + 11a_{44} = 35$$

Now, we will solve these eq's and find a solution such that A is invertible, there may be multiple soln's but we have to choose the one which is invertible. We have used online calculator for this since it is complicated. We get,

$$A = \begin{bmatrix} 0 & 2 & 0 & 3 \\ 1 & 2 & 1 & 0 \\ 1 & 4 & 0 & 1 \\ 0 & 3 & 0 & 1 \end{bmatrix}$$

202 IS 1138

Sowidhya

classmate Date Page

Q.8) (a) gcd (222, 18) using Euclidean Algorithm—

18	222	12
	−18↓	
	42	
	−36	
6	18	3
	−18	
	0	

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

(b) x_0, y_0 s.t. $1 = 33x_0 + 13y_0$ using Euclidean—Extended Euclidean Algo—

13	33	2
	−26	
7	13	1
	− 7	
6	7	1
	−6	
1	6	6
	−6	
	0	

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

Now, $\gcd(x, y) = ax + by$ → Using Bezout's Identity

Traceback in the division –

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

$= 2 \times 7 - 13$

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

$= 2 \times 33 - 5 \times 13$

This is of the form $ax + by$

$\therefore \boxed{x_0 = a = 2 \\ y_0 = b = -5}$

(c) Mul. inv. of 5 under mod 26

lets check if mul. inv. is possible or not

$\gcd(5, 26) = 1$

$\therefore$ possible

Now, $1 = 26 - 5 \times 5$

According to Bezout's identity, $\gcd(x, y) = ax + by$

lets see –

By, extended euclidean algorithm as well

multiplicative inverse of 5 :–

5	26	5
	−25	
	1	5
		5
		0

20215138

Sandhya

classmate

Date

Page

$1 = 5x + 26y \longrightarrow$ Bezout's identity.

$1 = 1 \cdot 26 - 5 \cdot 5$

∴ Multiplicative inverse of 5 under mod 26 = −5

∵ It is mod 26, we add 26 to −5 to make it positive:

$-5 + 26 = 21$

Therefore, mul. inv of 5 under mod 26 = **21**

Q.9) Input = $[D3]_{16}$
Output = 66

Convert D3 to polynomial form

$[D3]_{16} = [1\ 1\ 0\ 1\ 0\ 0\ 1\ 1]_2$

$\therefore$ Polynomial = $x^7 + x^6 + x^4 + x + 1$

Find inverse of $x^7 + x^6 + x^4 + x + 1$ under mod $x^8 + x^4 + x^3 + x + 1$

$x^7 + x^6 + x^4 + x + 1 \;\big|\; x^8 + x^4 + x^3 + x + 1 \;\big|\; x + 1$

$(-)\ x^8 + x^7 + x^5 + x^2 + x$

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

$(-)\ x^7 + x^6 + x^4 + x + 1$

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

$x^6 + x^5 + x^3 + x^2 + x \;\big|\; x^7 + x^6 + x^4 + x + 1 \;\big|\; x$

$(-)\ x^7 + x^6 + x^4 + x^3 + x^2$

$x^3 + x^2 + x + 1 \;\big|\; x^6 + x^5 + x^3 + x^2 + x \;\big|\; x^3 + x + 1$

$(-)\ x^6 + x^5 + x^4 + x^3$

$x^4 + x^2 + x$

$(-)\ x^4 + x^3 + x^2 + x$

x^3

$(-)\ x^3 + x^2 + x + 1$

$x^2 + x + 1$

20215138

Sowidhya

classmate
Date
Page

$x^2+x+1 \;\big|\; x^3+x^2+x+1 \;\big|\; x$

x^3+x^2+x

1

Note:
All under qo 2
⇓

Now, $1 \Rightarrow (x^3+x^2+x+1) + (x)(x^2+x+1)$

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

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

$\Rightarrow \{\underbrace{(x^7+x^6+x^4+x+1)}_{P(x)} + x(x^6+x^5+x^3+x^2+x)\} \cdot (x^4+x^2+x+1) + x(x^6+x^5+x^3+x^2+x)$

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

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

$\Rightarrow P(x)(x^4+x^2+x+1) + \{\underbrace{(x^8+x^4+x^3+x+1)}_{Q(x)} + P(x)\cdot(x+1)\}$ (-III)

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

$\Rightarrow (x^5+x^3+x^2)Q(x) + (x^6+x^5+x+1)P(x)$

Form is satisfied

$\therefore$ Inverse $= P(x) = x^6+x^5+x+1$

In Binary $= [01100011]_2$

$\therefore S(11010011) = 01100011$

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

lets calculate $m_7\ m_6\ m_5\ m_4\ m_3\ m_2\ m_1\ m_0$

for $i = 0$ to 7

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

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

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

$$= 0$$

$m_1 = 1$

$m_2 = 1$

$m_3 = 0$

$m_4 = 0$

$m_5 = 1$

$m_6 = 1$

$m_7 = 0$

Calculated by same logic as above

$\therefore$ Subbyte $(D3) = m_7\ m_6\ m_5 \dots m_0$

$= (01100110)_2$

$= [66]_{16}$

Hence, Proved !

2021S1138
Sowidhya

Q.10) Given → 33, 42, 66, 24

First step is converting each of them to their binary —

$33 = (00100001)_2 \rightarrow x^5 + 1$

$42 = (00101010)_2 \rightarrow x^5 + x^3 + x$

$66 = (01000010)_2 \rightarrow x^6 + x$

$24 = (00011000)_2 \rightarrow x^4 + x^3$

All under mod $x^8 + x^4 + x^3 + x + 1$

lets say output is x, y, z, w

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

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

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

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

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

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

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

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

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

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

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

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

Now, convert to binary ←

$v = x^6 + x^5 + x^2 + x \rightarrow 01100110 \rightarrow 102$

$y = x^7 + x^5 + x^3 + x + 1 \rightarrow 10101011 \rightarrow 171$

$z = x^7 + x^5 + x^2 + x + 1 \rightarrow 10100111 \rightarrow 167$

$w = x^5 + x^4 + x^3 + x + 1 \rightarrow 00111011 \rightarrow 59$

∴ AES Mix Column (33, 42, 66, 24) = (102, 171, 167, 59)

2021511138

Sawidhya

Q.11) $p \rightarrow$ prime number $a, b \in Z_p$

$f(a,b) : Z_p \rightarrow Z_p$; $f(a,b)(x) = (ax+b) \bmod p$

$x \neq x' \in Z_p$. $f(a,b)(x) = y$

$f(a,b)(x') = y'$

$(ax+b) \equiv y \bmod p$ — (A)

$(ax'+b) \equiv y' \bmod p$ — (B)

(A) − (B)

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

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

$x - x' \neq 0$ as $x \neq x' \rightarrow$ Given

So, for checking if we can find a and b we need to check if $(x-x')^{-1}$ exists or not. ie, if $(x-x')$ is invertible or not under $\% p$.

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

As $p \rightarrow$ prime no, $\Rightarrow \gcd(x-x', p) = 1$

∴ Inverse of $(x-x')$ $\% p$ exists.

So, we can find a and b.

For a –

$a \equiv (y_1 - y)(x_1 - x)^{-1} \pmod{p}$

Put this value of a in (A) and (B) to find b

Hence, we can derive a, b.

20215138

Sanidhya

Q.12) Hash function $h : (Z_2)^7 \to (Z_2)^4$

$h(x) = xA$

To find all pre-images of $[0\ 1\ 0\ 1]$

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

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

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

$\therefore$ Eqns $\to$ $x_1 + x_2 + x_3 + x_4 = 0$ ——— A

$x_2 + x_3 + x_4 + x_5 = 1$ ——— B

$x_3 + x_4 + x_5 + x_6 = 0$ ——— C

$x_4 + x_5 + x_6 + x_7 = 1$ ——— D

A — B $\Rightarrow$ $x_1 = x_5 + 1 \longrightarrow E$

B — C $\Rightarrow$ $x_2 = x_6 - 1 \longrightarrow F$

C — D $\Rightarrow$ $x_3 = x_7 + 1 \longrightarrow G$

As all x_i are binary (since q%2)
From eq^n D it is clear that one x_i out of (x_4, x_5, x_6, x_7) will be =1

OR

any three x_i out of (x_4, x_5, x_6, x_7) will be =1

So, all possible cases are listed below :—

$(x_4, x_5, x_6, x_7) \equiv \{(0,1,1,1), (1,0,1,1), (1,1,0,1), (1,1,1,0), (0,0,0,1), (0,0,1,0), (0,1,0,0), (1,0,0,0)\}$

By looking at eqns E, F, G we can find values of x_1, x_2, x_3.

A C Code was used to implement this tedious task (took permission from Sir).

20215138

Samidhya

Therefore, all possible pre-images of (0,1,0,1) are as follows :-

1. (0, 0, 0, 0, 1, 1, 1)
2. (1, 0, 0, 1, 0, 1, 1)
3. (0, 1, 0, 1, 1, 0, 1)
4. (0, 0, 1, 1, 1, 1, 0)
5. (1, 1, 0, 0, 0, 0, 1)
6. (1, 0, 1, 0, 0, 1, 0)
7. (0, 1, 1, 0, 1, 0, 0)
8. (1, 1, 1, 1, 0, 0, 0)

Q.13) $h_1 : \{0,1\}^{2m} \longrightarrow \{0,1\}^m$

↳ Collision Resistant Function.

$h_2 : \{0,1\}^{4m} \longrightarrow \{0,1\}^m$

TP — h_2 is collision resistant

Assume h_2 is not collision resistant

∴ there exists x and x'

such that $x \neq x'$

and $h_2(x) = h_2(x')$

$x = x_1 \,||\, x_2$

and $x' = x_1' \,||\, x_2'$

} all $x_1, x_2, x_1', x_2' \in \{0,1\}^{2m}$

$h_2(x) = h_2(x')$

$h_1[\underbrace{h_1(x_1) \,||\, h_1(x_2)}_{\alpha}] = h_1[\underbrace{h_1(x_1') \,||\, h_1(x_2')}_{\beta}]$

We know h_1 is collision resistant ∴ it is difficult to find α and β such that

$\alpha \neq \beta$

and $h_1(\alpha) = h_2(\beta)$

∴ $\alpha = \beta$

20215138

Sanidhya Kumar

classmate
Date
Page

$\Rightarrow h_1(x_1) \,||\, h_1(x_2) = h_1(x_1') \,||\, h_1(x_2')$

So, $h_1(x_1) = h_1(x_1')$

$h_1(x_2) = h_1(x_2')$

We know h_1 is collision resistant

so, $x_1 = x_1'$

$x_2 = x_2'$

$\therefore$ We say $\boxed{x = x'}$

But this is a contradiction to our assumption that $x \neq x'$.

Hence, proved by contradiction that h_2 is also collision resistant function.