2023510311 Patil Dhruv
CS-309

Q1)

Msg = C R Y P T O G R A P H Y
Y T O A H C R R P P Y G

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

∴ Final Msg = CRYPTOGRAPHY

∴ Our Msg and final Msg are equal. So our encryption is correct.

∴ in π corresponding pair $\pi(a, u)$. i.e. $a \rightarrow u$ and in π^{-1} $\pi^{-1}(a, u)$ i.e $u \rightarrow a$.

Q-2] Message: W E A R E I N D I A N
22 4 0 17 4 8 13 3 8 0 13

∴ $C_i = (P(i) + Key) \bmod 26$.

∴ Key = 4

2023503031
Patil Dhruv.

Date
Page

∴ Encryption: W E A R E I N D I A N
↓
22 4 0 17 4 8 13 3 8 0 13
↓
0 8 4 21 8 12 17 7 12 4 17
A I E V I M R H M E R

C = AIEVIMRHMER.
Pi = (Ci - Key) mod 26

⇒ Decryption: A I E V I M R H M E R
22 4 0 17 4 8 13 3 8 0 13
W E A R E I N D I A N.

Q-3] P = WE ARE INDIAN
Secret Key = CRICKET

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

WE AR EI ND IA NX

C = ZR HA CK MF RB LZ.

20235[031

Patel Dhruv.

Date
Page

∴ CI = 2R HA CK MF RB 22

P = WE AR EI ND IA NX

as if we rename x from last then:

P = WE AR E INDIAN.

Q4] a) $E(x) = (ax+b) \bmod 26$

$\Rightarrow D(x) = ((E(x)-b) \cdot a^{-1}) \bmod 26$

* for a^{-1}, we need to find

$a \cdot a^{-1} = 1 \bmod 26$.

as Here a is coprime i.e $\gcd(a, 26) = 1$.

as if $\gcd(a, 26) \neq 1$, then unique D(x) is not possible.

b) if $\gcd(a, 26) = 1$, then D(x) is possible

so for D(x) we compute a^{-1} as follows $a \cdot a^{-1} = 1 \bmod 26$.

if we get a^{-1} then we can easily compute $D(x) = a^{-1}(E(x)-b) \bmod 26$.

c). If $P = x$, $C = y$.

$y = (ax+b) \bmod 26$

$b = (y - ax) \bmod 26$

2023570311
Patil Dhruv

Date
Page

⇒ we can choose b from range [0, 25].

⇒ But we had to choose a that is invertible

$a \in \{1, 3, 5, 7, 9, 11, 13, 17, 19, 21, 23, 25\}$.

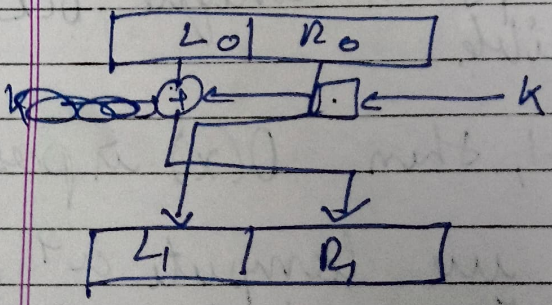
∴ 12 possible ways are there

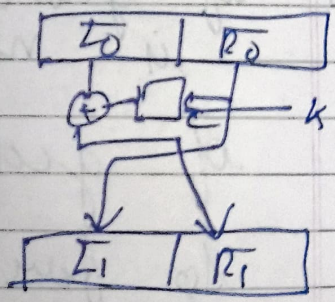
Q-5]

$C_1 = E(M, K)$
$C_2 = E(\bar{M}, K)$

Key scheduling $(K_1)_2$ $K_1, K_2, K_3, \dots, K_{16}$

Key scheduling $(\bar{K}_1) = \bar{K_1}, \bar{K_2}, \bar{K_3}, \dots, \bar{K_{16}}$





$R_1 = L_0 \oplus f(R_0, K_1)$.

$\bar{R_1} = \bar{L_0} \cdot \oplus \cdot f(\bar{R_0}, \bar{K_1})$.

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

∴ so we can see both L & R are

20235031

Patil Dhruv.

Date
Page

Complemented when M & K are complemented cipher text will be complemented

$C_2 = \bar{C}$

Q-6] C = A F I I I F W F

0 5 8 14 8 5 22 5

P = (C − K) mod 26

K_0 = AFIIIFWF

K_1 = 0 5 8 14 5 22 5

↓ ↓ ↓ ↓ ↓ ↓ ↓

26 4 7 18 4 21 4

P = ZEHSHEVE

K_2 = 0 5 8 14 8 5 22 5

↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓

24 3 6 17 6 3 20 3

P = YDGRGDUD

K_3 = 0 5 8 19 8 5 22 5

↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓

23 2 5 16 5 2 19 2

P = XCFQFCTC

20235031

Patil Dhruv

Date
Page

K_4 = 0 5 8 14 8 5 22 5

↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓

22 1 4 15 4 1 18 1

P = WBEPE BSB

K_5 = 0 5 8 14 8 5 22 5

↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓

21 0 3 14 3 0 14 0

P = VADODARA

Q-7] HILL ⟶ [X I 4 S]

7 8 11 11 23 8 24 9

$P = \begin{bmatrix} 7 & 4 \\ 8 & 11 \end{bmatrix}$ $C = \begin{bmatrix} 23 & 24 \\ 8 & 9 \end{bmatrix}$

$C = KP \bmod 26$

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

$|P| = 77 - 88 = -11 = 15$

P^{-1} exist as $|P| \neq 0$

$P^{-1} = \frac{Adj(P)}{|P|}$

$|P|^{-1} = |P|(P)^{-1} \bmod 26$

2023503031

Patel Dhruv.

Date
Page

∴ We know $15 \times 7 \bmod 26 = 1$

∴ 7 is the inv. of 15

Cofactor Matrix = $C = \begin{bmatrix} 11 & -8 \\ -11 & 7 \end{bmatrix}$

Adj matrix = $C^T = \begin{bmatrix} 11 & -11 \\ -8 & 7 \end{bmatrix}$

$P^{-1} = \det^{-1} \times \text{adj}(P) \bmod 26$

$= 7 \times \begin{bmatrix} 11 & -11 \\ -8 & 7 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 25 & 1 \\ 22 & 23 \end{bmatrix}$

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

$= \begin{bmatrix} 23 & 24 \\ 8 & 9 \end{bmatrix} \begin{bmatrix} 25 & 1 \\ 22 & 23 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 1103 & 575 \\ 398 & 215 \end{bmatrix} \bmod 26$

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

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

20235 1031
Patel Dhruv.

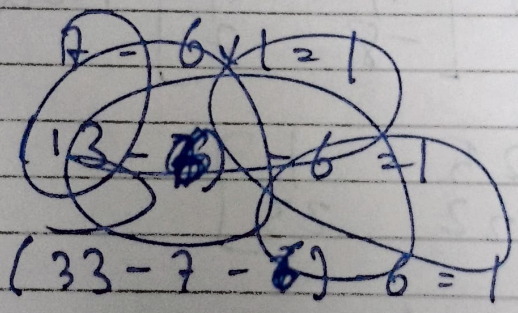
Q-8] Euclidean algo

a) gcd (222, 18) = 6

b) $33x + 13y = 1$

$33 = 13 \times 2 + 7$
$13 = 1 \times 7 + 6$
$7 = 6 \times 1 + 1$
$6 = 1 \times 6 + 0$

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



$7 - 6 \times 1 = 1$
$7 - (13 - 7) = 1$
$7 - 13 + 7 = 1$
$2.7 - 13 = 1$
$2.(33 - 2.13) - 13 = 1$

$2.33 - 4.13 - 13 = 1$

$2.33 + (-5)13 = 1$

$\therefore x = 2, \quad y = -5.$

20235031
Patil Dhruv.

Date
Page

1) $5y = 1 \bmod 26$.

$\therefore \gcd(5, 26) = 1$

$26 - 5 \times 5 = 1$

2) Take mod 26 on both side.

$26 \bmod 26 - 25 \bmod 26 = 1 \bmod 26$

$0 - 5 \times 5 \bmod 26 = 1 \bmod 26$

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

$5 \times 21 \bmod 26 = 1 \bmod 26$

$\therefore$ 21 is the multiplicative inverse of 5.

2023503 1

Patil Dhruv

Date
Page

Q-4)

q	a	b	r
$x+1$	$x^4+x^4+x^3+x+1$	$x^8+x^6+x^4+0+1$	$x^6+x^5+x^3+x^2+x$
x	$x^7+x^6+x^5+x+1$	$x^6+x^5+x^3+x^2+x$	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	x^2+x+1
x	x^3+x^2+x+1	x^2+x+1	1
x^2+x+1	x^2+x+1	1	0

q	t_1	t_2	$t = t_1 - q t_2$
$x+1$	0	1	$x+1$
x	1	$x+1$	x^2+x+1
x^3+x+1	$x+1$	x^2+x+1	x^5+x^4+x
x	x^2+x+1	x^5+x^4+x	x^6+x^5+x+1
x^2+x+1	x^5+x^4+1	$x^6+x^5+x^2+1$	

⇒ Stop

⇒ Multiplicative Inverse (D3) = (63).

20235031

Patel Dhruv

Date
Page

Now,

$S = 0\,11000\,11$

$C = 0\,11000\,11$

$\therefore S_i' = S_i \oplus S_{i+1 \bmod 8} \oplus S_{i+5 \bmod 8} \oplus S_{i+6 \bmod 8} \oplus S_{i+7 \bmod 8} \oplus C_i$

$\therefore S_0' = 1 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 1$
$= 0$

$S_1' = 1 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \oplus 1$
$= 1$

$S_2' = 0 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \oplus 0$
$= 1$

$S_3' = 0 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 0$
$= 0$

$S_4' = 0 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0$
$= 0$

$S_5' = 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 1$
$= 1$

$S_6' = 1 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 1$
$= 1$

$S_7' = 0 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \oplus 0$
$= 0$

$S' = 0110\,0110$
$= 66$

2023BCD031

Patel Dhruv

Date
Page

∴ Sub-byte of (D3) = 66

∴ Hence proved.

Q-10) Mix column C = (33, 42, 66, 24)

$33 = 32 + 1 = 0010\ 0001 = (21)_{16}$

$42 = 0010\ 1010 = (2A)_{16}$

$66 = 64 + 2 = 0100\ 0010 = (42)_{16}$

$24 = 0001\ 1000 = (18)_{16}$

$(01)_{16} = 0000\ 0001 = 1$
$(02)_{16} = 0000\ 0010 = x$
$(03)_{16} = 0000\ 0011 = x+1$

$$\therefore C1 = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} C$$

$C_0' = 02 \times 21 + 03 + 2A + 01 \times 42 + 01 \times 18$

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

$= x^6 + x^5 + x^2 + x = 0110\ 0110 = (66)$

20235031
Patel Dhruv.

Date
Page

$C_1' = 01 \times 21 + 01 \times 2A + 02 \times 42 + 03 \times 18$

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

$= x^7 + x^5 + x^2 + x + 1 = 10100111$

$= (A7)_{16}$

$C_2' = 01 \times 21 + 02 \times 2A + 03 \times 42 + 01 \times 18$

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

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

$= 10101011 \quad (AB)_{16}$

$C_3' = 03 \times 21 + 01 \times 2A + 01 \times 42 + 02 \times 18$

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

$= x^5 + x^4 + x^3 + x + 1 = 00111011$

$= (3B)_{16}$

$$\begin{bmatrix} (66)_{16} \\ (AB)_{16} \\ (A7)_{16} \\ (3B)_{16} \end{bmatrix} = \begin{bmatrix} 102 \\ 171 \\ 167 \\ 59 \end{bmatrix}$$

20235031
Patel Dhruv

Date
Page

Q-11] P is prime

$f_{(a,b)}(x) = ax + b \bmod p$

$f_{(a,b)}(x) = y$

$x \neq x' \in \mathbb{Z}_p$

⇒ $\mathbb{Z}_p$ is a field as it satisfies the below axioms

(1) closure $a, b \in \mathbb{Z}_p$

$(a+b) \bmod p \in \mathbb{Z}_p$

(2) associativity

$(a+b)+c = a+(b+c)$

(3) Commutative

$a+b = a+b$

(4) Identity

$a+0 = a$

(5) Additive Inverse :

$a + (p-a) = 0 \bmod p.$

20235031
Patel Dhruvi

Date
Page

(6) Closure Multiplication

ab mod p ∈ Zp

(7) Associativity

(ab)c = a.(bc) ∈ Zp

(8) Commutative

ab = ba.

(9) Identity

a×1 = a mod p

(10) Multiplicative inverse

for a ∈ Zp with a ≠ 0, gcd(a,p) = 1

(11) Distributive a,b,c ∈ Zp

a.(b+c) = ab+ac

(Zp, +) & (Zp\{0}, ×) are abelian.

∴ Zp is a field.

$f_{a,b}(x) = y$ $f_{a,b}(x') = y'$

$ax+b = y \bmod p$

20235031

Patel Dhruvin

Date
Page

$ax' + b - ax - b = y' - y \mod p$

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

$\therefore$ Since $x \neq x' \Rightarrow x - x' \neq 0$

$\therefore$ $a = (y' - y)(x' - x)^{-1} \mod p$

Q-12] $h : (Z_2)^7 \longrightarrow (Z_2)^4$ $h(x) = xA$

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

$xA = (0,1,0,1)\,y$

$y_1\ y_2\ y_3\ y_4$

$\therefore$ $x' = (x_1\ x_2\ x_3\ x_4\ x_5\ x_6\ x_7)$

$\Rightarrow$ y_1 :

$C_1 = (1\ 1\ 1\ 1\ 0\ 0\ 0)^T$

$y_1 = xC_1 = x_1 + x_2 + x_3 + x_4 = 0$ — (1)

2023/5/03/

Patil Dhruv.

Date
Page

(2) $y_2 = x_2 + x_3 + x_4 + x_5 = 1$ ——— (2)

y_3 :-

$y_3 = x_3 + x_4 + x_5 + x_6 = 0$ ——— (3)

y_4 :-

$xC_4 = x_4 + x_5 + x_6 + x_7 = 1$ ——— (4)

⇒ from (1), (2), (3) & (4)

$x_1 + x_2 + x_3 + x_4 = 0$
$x_2 + x_3 + x_4 + x_5 = 1$
$x_3 + x_4 + x_5 + x_6 = 0$
$x_4 + x_5 + x_6 + x_7 = 1$

⇓

∴ after solving.

$x_1 = 1 + x_5$

$x_2 = 1 + x_6$

$x_3 = 1 + x_7$

$x_4 = 1 + x_5 + x_6 + x_7$

20235031

Patel Dhruv

Date
Page

x_5	x_6	x_7	x_1	x_2	x_3	x_4
0	0	0	1	1	1	1
0	0	1	1	1	0	0
0	1	0	1	0	1	0
0	1	1	1	0	0	1
1	0	0	0	1	1	0
1	0	1	0	1	0	1
1	1	0	0	0	1	1
1	1	1	0	0	0	0

⇒ Soln are

(1111 0000)
(1100 0011)
(1010 0101)
(1001 0110)
(0110 1001)
(0101 1010)
(0011 1100)
(0000 1111)

Q13)

a) $x = x_1 || x_2$ $\quad x_1, x_2 \in \{0,1\}^2$

b) $h_2(x) = h_1(h_1(x_1) || h_1(x_2))$.

2023b2031

Patel Dhruv.

Date
Page

∴ let us assume h_2 is not a collision resistant.

$$x' = x_1 || x_2 \quad \& \quad x'' = x_1' || x_2'$$

$$h_1(h_1(x_1) || h_1(x_2)) = h_1(h_1(x_1') || h_1(x_2'))$$

∴ $a = h_1(x_1) || h_1(x_2)$

$b = h_1(x_1') || h_1(x_2')$

∴ $h_1(a) = h_1(b)$ with $a \neq b$

∴ This is the collision case and h_1 is collision resistant.

∴ our assumption may wrong.

∴ we can conclude that h_2 is collision resistant.