__/__/____

# Assignment - 1

Name :- Manas Jitendrakumar Ingle
ID :- 202151086

Q1] Plaintext : CRYPTOGRAPHY

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

a] According to the given Permutation, as we know that Secret key in transposition cipher is a permutation.
So, according to the key the 1st Character in the Ciphertext will be the 3rd Character of the plaintext, 2nd Character of Ciphertext will be the 5th Character of the plaintext., The 3rd Character of Ciphertext will be 6th Character of the plaintext.

So, Briefly the permutation gives us the Character Mapping of the transposition within the set of the Message.

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

3 5 6 9 11 1 8 2 10 4 12 7

Ciphertext ⇒ Y T O A H C R R P P Y G

b] As, we know Permutation is a bijection defined on a set from itself to itself.
Therefore, decryption is possible as inverse of $\pi$ exists.
The inverse of $\pi$ can be found out

Manas Jitendrakumar Ingle
202151086.

__/__/____

Out from $\pi$ itself, by remapping the second row of $\pi$ in the order 1 to 12 and correspondingly listing their bijective mappings.

Hence,

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

Hence, Again Applying transposition on our Ciphertext will give us.

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

Dec(Ciphertext) :⇒ C R Y P T O G R A P H Y

Hence, decryption is possible, and can be achieved through $\pi^{-1}$ technique.

Q2] Using the Correspondance :-

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Shift Cipher with general key K can be defined as:

x → Integer corresponding to Alphabet.

- $Enc(x, K) = (x + K) \% 26$
- $Dec(x, K) = (x + 26 - K) \% 26$

We have given key = 4;

Plaintext :- WE ARE INDIAN

So, Encrypting all the unique Characters of the given plaintext.

Manas Jitendrakumar Ingle
20215086

__/__/____

$Enc(W,4) = Enc(22,4) = (22+4)\%26 = 0 = A$

$Enc(E,4) = Enc(4,4) = (4+4)\%26 = 8 = I$

$Enc(A,4) = Enc(0,4) = (0+4)\%26 = 4 = E$

$Enc(R,4) = Enc(17,4) = 21 = V$

$Enc(I,4) = Enc(8,4) = (8+4)\%26 = 12 = M$

$Enc(N,4) = Enc(13,4) = (13+4)\%26 = 17 = R$

$Enc(D,4) = Enc(3,4) = (3+4)\%26 = 7 = H$

Hence, Substituting the Shift Values, we get,

Ciphertext: AIEVIMRHMER

for the plaintext: "WE ARE INDIAN" with key = 4.

Now, let us decrypt the ciphertext to check correctness of our encryption:

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

Manas Jitendrakumar Ingle
202151086

__/__/____

∴ We get WE ARE INDIAN, upon the decryption of AIEVIMR HMER using Shift Cipher with Key 4., Hence, Verified.

Q3] Plaintext: WE ARE INDIAN
Secret Key: CRICKET

Building 5x5 matrix using rules of Playfair Encryption

| | | | | |
|---|---|---|---|---|
| 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 |

# Considering 'I' & 'J' as equals for 5x5 Matrix.

Here we first form diagraphs by dividing plaintext in pairs of two. As, the size is odd to complete the diagraph we add filler(x) at end.

String: WE AR EI ND IA NX

| | | | | |
|---|---|---|---|---|
| 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 every diagraph, taking corresponding values for WE, AR, EI, ND, IA, NX we get corresponding values as:-

ZR HA CK MF RB LZ

Hence,

Ciphertext ⇒ ZR HACK MF RB LZ

Manas Jitendrakumar Ingle
20215086

__/__/____

Decryption ⇒ We again form digraphs and do the inverse of what we did in encryption, i.e, taking diagraphs and getting their corresponding values.

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

for diagraphs,

ZR HA CK MF RB LZ
⇒ WE AR EI ND IA NX

# As we get our playfair text back, we have it cemented that our encryption is validated.

Q4] For Affine Cipher,
Secret key ⇒ $K = (a, b)$, where $0 \leq a, b \leq 25$

$$y = Enc_K(x) = (ax+b) \% 26$$

Decryption of Affine Cipher will be:

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

Hence, we understand that we need $a^{-1}$ is required for decrypting. The $a^{-1}$ is the multiplicative inverse of a. under modulo 26.

Since, $a^{-1}$ exists only iff $\gcd(0, 26) = 1$.

For all (a, b) pair where $\gcd(a, 26)$ is not equal to 1, (a, b) is not a key for Affine Cipher because decryption will not be possible

Manas Jitendrakumar Ingle
202151086.

__/__/____

in such cases.
Therefore for,
$a \in \{2,4,6,8,10,12,13,14,16,18,20,22,24\}$
and $\forall b$ such that $0 \leq b \leq 26$, decryption is not possible.
We need to find different keys for which plaintext and ciphertext is same.

Decryption algorithm when we can have successful decryption is:

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

where $a^{-1}$ is multiplicative inverse of a under modulo 26 . i.e. $a * a^{-1} \equiv 1 \bmod 26$

Pair $(x, y)$, for keys $(a, b)K_1$ and $K_2(a', b')$, assume $K_1 \neq K_2$

$$ax + b \equiv y \bmod 26 \quad \text{---} (1)$$
$$\text{and } a'x + b' \equiv y \bmod 26 \quad \text{---} (2)$$

Substracting (1) from (2), we get,

$$(a'-a)x + (b'-b) \equiv 0 \bmod 26 \quad \text{---} (3)$$

Now, $x \in \{0, 1, \ldots, 25\}$, lets put $x = 0$ in (3)

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

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

Since, $b, b' \in \{0, 1, 2, \ldots 25\}$. Therefore, max value of $(b'-b)$ can be 25.
Hence (4) holds only iff $b' = b$

Manas Jitendrakumar Ingle
2021510B6

__/__/____

equation ③ is reduced to

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

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

$$(a'-a) \equiv 0 \bmod 26 \quad \text{—⑤} \quad (x^{-1} \text{ is also an integer})$$

Again, $a \in \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$, hence, maximum value of $(a'-a)$ is equal to 24, Therfore ⑤ holds only iff $(a' = a)$ Hence, proving that our assumption $K_1 \neq K_2$ is wrong. Hence, two different keys will not result in same plaintext - ciphertext pair.

Therfore, 0 number of different keys will have the same plaintext-ciphertext pair$(x, y)$.

Manas Jitendrakumar Ingle
202151086

__/__/__

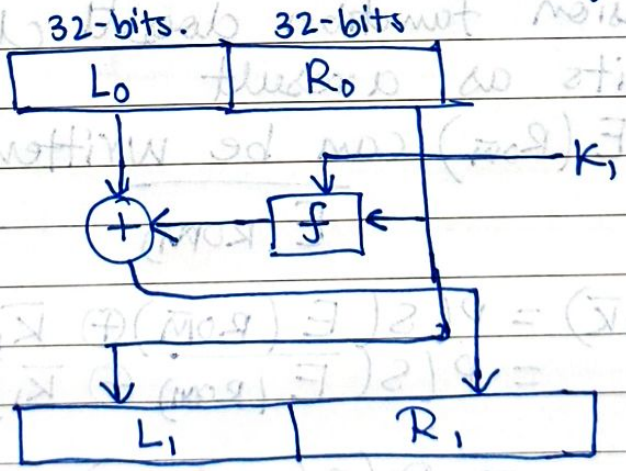
Q5] $\mathcal{E}_{nc}$ is encryption function of DES.

$$C_1 = \mathcal{E}_{nc}(M, K)$$
$$C_2 = \mathcal{E}_{nc}(\overline{M}, \overline{K})$$

Key Scheduling Algorithm of DES, first removes 8 parity bits from 64 bit key, then performs PC-1 permutation. Then, it performs left circular shift & a substitution to generate the round keys. Permutation & substitution doesn't cause any change in individual bit as only positions are changed. As a result complimentary inputs will generate complimentary outputs.

So, if we use K and K' as input to our key schedulling algorithm, the round keys generated will also be complimentary.

1 round fiestal network of DES



Manas Jitendrakumar Ingle
202151086

__/__/____

$\therefore L_1 = R_0$ & $R_1 = f(R_0, K_1) \oplus L_0$

$R_M, L_M \longrightarrow$ denote plaintext M
$R_{\bar{M}}, L_{\bar{M}} \longrightarrow$ denote plaintext $\bar{M}$

Let $(M, K)$ & $(\bar{M}, \bar{K})$ be input to DES.
Therefore, after first round,

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

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

$\therefore L_{1M}$ & $L_{1\bar{M}}$ are complementary
as $R_{0M}$ & $R_{0\bar{M}}$ are complementary.

$f(R_{0M}, K)$ & $f(R_{0\bar{M}}, \bar{K})$

$R_{0M} = X_{32M}\ X_{33M} \ldots\ldots X_{63M}$
$R_{0\bar{M}} = \overline{X_{32M}}\ \overline{X_{33M}} \ldots\ldots \overline{X_{63M}}$

Expansion function doesn't change the individual bits as a result
$E(R_{0\bar{M}})$ can be written as

$$\overline{E(R_{0M})} \quad \text{---} (1)$$

$f(\bar{M}, \bar{K}) = P(S(E(R_{0\bar{M}}) \oplus \bar{K}_1))$
$= P(S(\overline{E(R_{0M})} \oplus \bar{K}_1))$
$= P(S(E(R_{0M}) \oplus K_1))$

Hence,
$A \oplus B = \bar{A} \oplus \bar{B}$

Manas Jitendrakumar Ingle
20215108

__/__/____

$\therefore f(\bar{M}, \bar{K}) = f(M, K)$ —②

$\therefore R_{1M} = (L_{0M} \oplus f(R_{0M}, K))$

$R_{1\bar{M}} = L_{0\bar{M}} \oplus f(R_{0\bar{M}}, \bar{K})$. which can be written as

$R_{1\bar{M}} = L_{0\bar{M}} \oplus f(R_{0M}, K)$

$\therefore R_1\bar{M} = \overline{R_1 M}$

$\therefore L_{1M} || R_{1M}$ is complementary to $L_{1\bar{M}} || R_{1\bar{M}}$

$\therefore$ Outputs of round of DES will also be complementary, given that the provided plaintext and keys are complementary. At last, $IP^{-1}$ does not affect individual bits as a result.

$$C_2 = \overline{C_1}$$

Manas Jitendrakumar Ingle
20215108 6.

__/__/____

Q6]

Given Ciphertext : AFITIFWF

Encryption Algorithm in Shift Cipher.

$$C = (x + K) \% 26.$$

K → secret key
C → Ciphertext
x → plain text

As Shift Cipher has only 25 possible keys, we can enhaustively decrypt using each key and find which key gives as meaningful text.

$$\underset{(x,K)}{Dec} = (x - K) \bmod 26.$$

x → Integer corresponding to English Alphabet.

for K = 1,.

$x_1 = (0 - 1 + 26) \% 26 = 25$
$x_2 = (5 - 1 + 26) \% 26 = 4$
$x_3 = (8 - 1 + 26) \% 26 = 7$
$x_4 = (19 - 1 + 26) \% 26 = 18$
$x_5 = (8 - 1 + 26) \% 26 = 7$
$x_6 = (5 - 1 + 26) \% 26 = 4$
$x_7 = (22 - 1 + 26) \% 26 = 21$
$x_8 = (5 - 1 + 26) \% 26 = 4$

Plaintext ⟹ ZEHSHEVE.
for K = 1

Similarly, we try for other values of K until we find, the meaningful Plaintext.

Manas Jitendrakumar Ingle
20215108 6

__/__/____

Decryption using K=2 ⇒ YDGRGDVD

Decryption using K=3 ⇒ XCFQFCTC

Decryption using K=4 ⇒ WBEPEBSB

Decryption using K=5 ⇒ VADODARA

∴ Using K=5, we get meaningful text i.e, VADODARA.

Hence,

Plaintext is VADODARA

key=5

Q7] In Hill Cipher, if key is nxn matrix, we divide plaintext into n-character blocks. Then we perform matrix multiplication to get the ciphertext.

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

Multiplying both sides by $P^{-1}$ gives

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

⇒ Given plaintext : HILL

⇒ Corresponding Cipher : XIVJ

Let, key $K = \begin{bmatrix} K_1 & K_2 \\ K_3 & K_4 \end{bmatrix}$

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

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

Manas Jitendrakumar Ingle
202151086

__/__/____

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

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

We need to find Multiplicative inverse of 15 and 26

$$\begin{array}{r|l} 15 & 26 \\ -15 & 1 \\ \hline 11 & 15 \\ -11 & 1 \\ \hline 4 & 11 \\ -8 & 2 \\ \hline 3 & 4 \\ -3 & 1 \\ \hline 1 & \end{array}$$

$1 = 4 - 1.3$
$1 = 4 - (11 - 2 \times 4)$
$1 = 3 \times 4 - 11$
$1 = 3(15-11) - 11$
$1 = 3.15 - 4.11$
$1 = 3.15 - 4.(26-15)$
$1 = 7.15 - 4.26.$

∴ Multiplicative inverse of 15 mod 26 is 7.

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

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

Hence, Secret key is $K = \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix}$.

Manas Jitendrakumar Jogi
20215108

__/__/____

98]

a) $18\overline{)222}\,(12$
$\quad 18$
$\quad 42$
$\quad 36$
$\quad 6\overline{)18}\,(3$
$\quad\quad 18$
$\quad\quad 0$

$222 = 18 \times (12) + 6$
$18 = 6 \times (3) + 0$
Hence, gcd $(222, 18) = 6$

GCD(222, 18) is 6

b) $x_0, y_0$ such that $1 = 33(x_0) + 13(y_0)$
Let's first calculate gcd of 13, 33 using Euclidean Algorithm.

$13\overline{)33}\,(2$
$\quad 26$
$\quad 7\overline{)13}\,(1$
$\quad\quad 7$
$\quad\quad 6\overline{)7}\,(1$
$\quad\quad\quad 6$
$\quad\quad\quad 1\overline{)6}\,(6$
$\quad\quad\quad\quad 6$
$\quad\quad\quad\quad 0.$

GCD(13, 33) = 1.

$1 = (33 \times 2) + (13 \times (-5))$

we get $x_0 = 2 \quad y_0 = -5$

through.

$1 = 7 - 1.6$
$1 = 7 - (13 - 1.7)$
$1 = 2.7 - 1.3$
$1 = 2(33 - 2.13) - 1.13$
$1 = 2.33 + (-5).13$
$\therefore x_0 = 2$ and $y_0 = -5.$

Manas Jitendrakumar Jogi
202151086.

__/__/____

98. c) Let's Calculate GCD of 5 and 26.

$$5\overline{)26}\,(5$$
$$\underline{25}$$
$$1\overline{)5}\,(5$$
$$\underline{5}$$
$$0$$

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

The multiplicative inverse of 5 under mod 26 is equal to coefficient of 5 in Bezout's Identity.

$$1 = 5 \cdot x + 26 \cdot y.$$

x and y can be found using Extended Euclidean Algorithm.

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

$\therefore$ Multiplicative inverse of 5 under modulo 26 is $-5$.

We can add or substract multiples of 26 as modulo 26 will not affect it.

We can say multiplicative inverse of 5 under modulo 26 is $-5 + 26 = 21$

Multiplicative inverse of 5 under Modulo 26 = 21

Answer = 21

Manas Jitendrakumar Jogle
202151086.

__/__/____

Q9] for finding Subbyte (D3)
we first compute,

$$(D3)_{16} = (11010011)_2$$

for AES, the constant C is $(63)_{16}$.

Primitive polynomial $= x^8 + x^4 + x^3 + x + 1$

Polynomial generated from binary represent$^n$ of $(D3)_{16}$ is $P(x) = x^7 + x^6 + x^4 + x + 1$

Now, we find inverse of $P(x)$ in $F_2(x)/\langle G(x)\rangle$
We can find it using extended Euclidian Algo.

$x^7+x^6+x^4+x+1 \;\overline{)}\; x^8+x^4+x^3+x+1 \;(x+1$
$x^8+x^7+x^5+x^2+x$
$x^7+x^5+x^4+x^3+x^2+1$
$x^7+x^6+x^4+x+1$
$x^6+x^5+x^3+x^2+x \;\overline{)}\; x^7+x^6+x^4+x+1 \;(x$
$x^7+x^6+x^4+x^3+x^2$
$x^3+x^2+x+1 \;\overline{)}\; x^6+x^5+x^3+x^2+x \;(x^3+x+1$
$x^6+x^5+x^4+x^3$
$x^4+x^2+x$
$x^4+x^3+x^2+x$
$x^3$
$x^3+x^2+x+1$
$x^2+x+1 \;\overline{)}\; x^3+x^2+x+1 \;(x$
$x^3+x^2+x$
$1$

Now, going in reverse direction to find inverse of $P(x)$

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

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

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

Manas Jitendrakumar Ingle
20215086.

__/__/____

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

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

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

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

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

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

∴ Inverse of $P(x)$ in $F_2[x]/\langle G(x)\rangle$ is $(x^6+x^5+x+1)$

binary representation of of inverse of $P(x)$

$P(x) = b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0 = (01100011)_2$

Also, $C = C_7 C_6 C_5 C_4 C_3 C_2 C_1 C_0 = (01100011)_2$

Now, for $i = 0$ to $7$,

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

| | 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 |

$m_0 = (1+0+1+1+0+1) \bmod 2 = 0.$

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

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

$m_3 = (0+0+1+1+0+0) \bmod 2 = 0$

$m_4 = (0+1+1+0+0+0) \bmod 2 = 0$

$m_5 = (1+1+0+0+0+1) \bmod 2 = 1$

$m_6 = (1+0+0+0+1+1) \bmod 2 = 1$

$m_7 = (0+0+0+1+1+0) \bmod 2 = 0.$

Subbyte $(D3) = m_7 m_6 m_5 m_4 m_3 m_2 m_1 m_0 = (01100110)_2$

$= (66)_{16}$

Hence, Proved.

Manas Jitendrakumar Ingle
202151086

__/__/____

Q10] Input: 33, 42, 66, 24 (integer)

$(33)_{10} = (00100001)_2$
$(42)_{10} = (00101010)_2$
$(66)_{10} = (01000010)_2$
$(24)_{10} = (00011000)_2$

∴ Polynomials $t_0, t_1, t_2$ and $t_3$ corresponding to each binary char.

$t_0 = x^5 + 1$
$t_1 = x^5 + x^3 + x$
$t_2 = x^6 + x$
$t_3 = x^4 + x^3$

Now, we will find the polynomial $u_0, u_1, u_2$ and $u_3$, using

$$u_0 = (x.t_0 + (x+1)t_1 + t_2 + t_3) \bmod (x^8 + x^4 + x^3 + x + 1)$$
$$u_0 = \{(x^6 + x) + (x^8 + x^4 + x^2 + x^5 + x^3 + x) + (x^6 + x) + (x^4 + x^3)\} \bmod (x^8 + x^4 + x^3 + x + 1)$$
$$u_0 = (x^6 + x^5 + x^2 + x) \bmod (x^8 + x^4 + x^3 + x + 1)$$
$$\boxed{u_0 = (x^6 + x^5 + x^2 + x)}$$

$$u_1 = (t_0 + x t_1 + (x+1) t_2 + t_3) \bmod (x^8 + x^4 + x^3 + x + 1)$$
$$u_1 = \{(x^5 + 1) + (x^8 + x^4 + x^2) + (x^7 + x^2 + x^6 + x) + (x^4 + x^3)\} \bmod (x^8 + x^4 + x^3 + x + 1)$$
$$\boxed{u_1 = (x^7 + x^5 + x^3 + x + 1)}$$

$$u_2 = (t_0 + t_1 + x t_2 + (x+1) t_3) \bmod (x^8 + x^4 + x^3 + x + 1)$$
$$u_2 = \{(x^5 + 1) + (x^5 + x^3 + x) + (x^7 + x^2) + (x^5 + x^4 + x^4 + x^3)\} \bmod (x^8 + x^4 + x^3 + x + 1)$$
$$\boxed{u_2 = (x^7 + x^5 + x^2 + x + 1)}$$

Manas Jitendrakumar Ingle
20215086.

__/__/____

$$u_3 = ((x+1)t_0 + t_1 + t_2 + x \cdot t_3) \bmod (x^8+x^4+x^3+x+1)$$

$$u_3 = \{(x^6+x+x^5+1) + (x^5+x^3+x) + (x^6+x) + (x^5+x^4)\} \bmod (x^8+x^4+x^3+x+1)$$

$$\boxed{u_3 = (x^5+x^4+x^3+x+1)}$$

Now the binary representations of polynomials $u_0, u_1, u_2$ and $u_3$ be $S_0, S_1, S_2, S_3$ respectively.

$$S_0 = (01100101)_2$$
$$S_1 = (10101011)_2$$
$$S_2 = (10100111)_2$$
$$S_3 = (00111011)_2$$

AES Mix Columns $(33, 42, 66, 24) = (S_0, S_1, S_2, S_3)$

Since, the output is asked in integer, therefore,

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

Manas Jitendrakumar Ingle
202151086

__/__/____

Q11] Eq^n's.

$$ax + b = y \pmod p$$
$$ax' + b = y' \pmod p$$

$$ax = y - b \pmod p \quad \text{——} (1)$$
$$ax' = y' - b \pmod p \quad \text{——} (2)$$

Substract (2) from (1)

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

Since, $x \neq x'$,

Multiplicative inverse of $(x - x') \bmod (p)$

Here p is a prime no, so every no is co-prime with it, so, its multiplicative Inverse exists.

$$a = (y - y')(x - x') \bmod (p) \quad \text{——} (3)$$

Now,

$$ax + b = y \bmod (p)$$
$$(y - y')(x - x')^{-1} \cdot x + b = y \pmod p$$

$$b = (y - (y - y')(x - x')^{-1} \cdot x) \bmod (p) \quad \text{——} (4)$$

So, far given $x, x', y, y'$, 'a' and 'b' are possible to drive and there values are given in equation (3) and (4).

Manas Jitendrakumar Ingle
2021S1086.

__/__/____

Q12] Hash function.

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

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

$$(x_1 + x_2 * x_3 + x_4) \bmod(2) = 0 \quad \text{---} (1)$$
$$(x_2 + x_3 + x_4 + x_5) \bmod(2) = 1 \quad \text{---} (2)$$
$$(x_3 + x_4 + x_5 + x_6) \bmod(2) = 0 \quad \text{---} (3)$$
$$(x_4 + x_5 + x_6 + x_7) \bmod(2) = 1 \quad \text{---} (4)$$

Substracting (2) from (1)

$$x_1 = x_5 + 1 \quad \text{---} (5)$$

Substracting (3) from (2)

$$x_2 = x_6 - 1 \quad \text{---} (6)$$

Substracting (4) from (3)

$$x_3 = x_7 + 1 \quad \text{---} (7)$$

Since, all the operations are under modulo 2, from (4) we can conclude that either a single variable out of $\{x_4, x_5, x_6, x_7\}$ is 1 or any three variables out of $\{x_4\ x_5\ x_6\ x_7\}$ are 1 to satisfy eq$^n$ (4). Therefore, all possible tupples for $(x_4, x_5\ x_6\ x_7)$ are,

$\{(1,0,0,0), (0,1,0,0), (0,0,1,0), (0,0,0,1), (1,1,1,0), (1,1,0,1), (1,0,1,1), (0,1,1,1)\}$

We can find values of $x_1$, $x_2$ and $x_3$ for each tupple above using (5), (6) and (7).

Manas Jitendrakumar Ingle
20215086

__/__/____

Therefore, all the pre-Images of (0,1,0,1) are:

$x_1\ x_2\ x_3\ x_4\ x_5\ x_6\ x_7$

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]
8) [0 0 0 0 1 1 1]

There are these 8 total pre-images for which our image is [0 1 0 1].

Q13] Assuming, that $h_2$ is not collision resistant if there exists $x_1, x_2 \in \{0,1\}^{4m}$ such that $x_1 \neq x_2$ and $h_2(x_1) = h_2(x_2)$.

Let's define $x_1$ and $x_2$ as.

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

where, $x_{11}\ x_{12}\ x_{21}$ and $x_{22} \in \{0,1\}^{2m}$, Since $h_2(x_1) = h_2(x_2)$ from defination of $h_2$, we can write.

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

Since, h is collision resistant, i.e, it is computationally hard to find $x_a \neq x_b$ in ~~given amount~~ feasible amount of time such that $h_1(x_a) = h_1(x_b)$.

Therefore, eq$^n$ (1) can be written as:

$h_1(x_{11}) || h_1(x_{12}) = h_1(x_{21}) || h_1(x_{22})$ (i.e, $x_a = x_b$)

Manas Jitendrakumar Ingle
20215086

__/__/____

Now, using concatenation property of string we can write:

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

Since, $h_1$ is collision resistant again, we can say,

$$x_{11} = x_{21} \quad \text{——} (2)$$
$$x_{12} = x_{22} \quad \text{——} (3)$$

from (2) and (3) we have $x_1 = x_2$, which contradicts our assumption that $x_1 \neq x_2$. Hence, $h_2$ is a collision resistant function.