CS304: INTRODUCTION TO CRYPTOGRAPHY AND NETWORK SECURITY

Assignment 1

Ardit Agrawal
20205123

Problem 1:

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) Secret key in transposition cipher is a permutation. The key given says that 1st character in ciphertext will be the third character in plaintext, second character in ciphertext will be fifth character in plaintext and so on. Therefore,

Ciphertext : YTOAHCRRPPYG

(b) Since, π is a permutation and permutation is a bijection defined on a set from itself to itself. Therefore, inverse of π exists and hence decryption is possible. The inverse of π is given as:

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

Using the π^{-1}, if we decrypt the ciphertext generated in part (a), we should get back the plaintext.

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

∴ Dec(Ciphertext): CRYPTOGRAPHY

Hence, we can see that we got our plaintext back. Therefore, the decryption technique is π^{-1}.

Problem 2:

We use the following correspondence A→0, B→1, ..., Z→25.
Shift cipher with key K is defined as:

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

where x is integer corresponding to english alphabets.

Plaintext: WEAREINDIAN

Key : 4

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) = 12 = M
Enc(N,4) = Enc(13,4) = 17 = R
Enc(D,4) = Enc(3,4) = 7 = H

∴ Encryption of 'WEAREINDIAN' using shift cipher with key 4 is

Ciphertext: AIEVIMRHMER

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) = 4 = E
Dec(E,4) = Dec(4,4) = 0 = A
Dec(V,4) = Dec(21,4) = 17 = R
Dec(M,4) = Dec(12,4) = 8 = I
Dec(R,4) = Dec(17,4) = 13 = N
Dec(H,4) = Dec(7,4) = 3 = D

∴ Decryption of AIEVIMRHMER using shift cipher with key 4 is WEAREINDIAN
Hence, verified.

Problem 3:

Aadit Agrawal
2020512B

Encryption Algorithm : Playfair Cipher

Plaintext : WEAREINDIAN

Secret Key : CRICKET

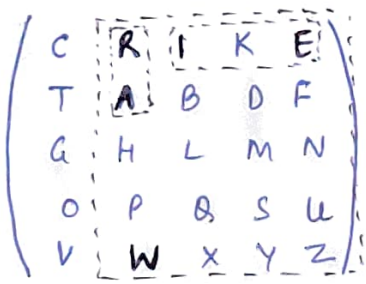
Building 5x5 matrix using rules of Playfair Encryption

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

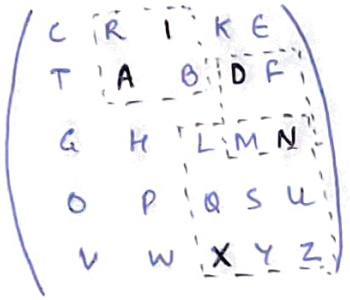
Dividing plaintext into groups of two and adding 'X' according to playfair rules.

Playfair String : WE AR EI ND IA NX

The rectangle or row or column is highlighted for each pair of characters in the matrix below.



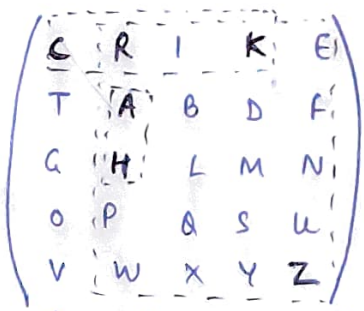
for WE, AR and EI



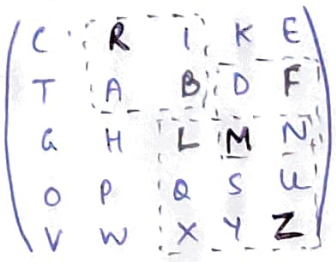
for ND, IA and NX

∴ Ciphertext : ZR HA CK MF RB LZ

On decryption, we should get the playfair string back.



for ZR, HA and CK



for MF, RB and LZ

Archit Agrawal
2020512 13

Cipher text: ZR HA CK Mf RB LZ

Decrypted text: WE AR EI ND IA NX

As we can see, on decryption, we got the playfair string back. Hence, our encryption is validated.

Problem 4

Arduit Agrawal
2020051213

key is $K=(a,b)$, where $0 \le a,b \le 25$

and, $y = Enc_K(x) = (ax+b) \bmod 26$.

The decryption for the above encryption will be,

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

where a^{-1} is multiplicative inverse of a under modulo 26. Since, a^{-1} exists only iff $\gcd(a,26) = 1$. Therefore, for all the (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 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 $0 \le b \le 26$, decryption is not possible.

Decryption algorithm when we can have successful decryption is:

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

where a^{-1} is multiplicative inverse of a under modulo 26

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

Now, we need to find different number of keys for which we will have same plaintext - ciphertext pair (x,y). For keys $K_1(a,b)$ and $K_2(a',b')$, assume $K_1 \neq K_2$ and plaintext and ciphertext pair is same. That is,

$$ax + b \equiv y \bmod 26 \quad \text{---(I)}$$

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

Arclit Agrawal
20205 1213

Subtracting (I) from (II), we get,

~~$(a'-a)x + b - b'$~~

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

Now, $x \in \{0, 1 \cdots, 25\}$. Let's put $x = 0$ in (III),

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

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

Since $b, b' \in \{0, 1, \cdots, 25\}$. Therefore, maximum value of $(b'-b)$ can be 25. Hence, (IV) holds only iff $b' = b$.

$\therefore$ equation (III) is reduced to

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

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

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

($\because x^{-1}$ 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. Therefore (V) holds only iff $(a' = a)$. Therefore our assumption that $K_1 \neq K_2$ is wrong. Hence, two different keys will not result in same plaintext-ciphertext pair. Therefore, 0 number of different keys will ~~generate~~ have the same plaintext-ciphertext pair (x, y).

Archit Agrawal
2020512B

Problem 5

Enc is encryption function of DES.

$$C_1 = Enc(M, K)$$

$$C_2 = Enc(\overline{M}, \overline{K})$$

The key scheduling algorithm of DES, first removes the parity bits out of the 64-bit key. Then, it performs a permutation PC1. Then, it performs left circular shift and a substitution to generate the round keys.

→ Permutation and substitution do not have any effect on individual bits. They either transpose or remove some bits from the given input. Therefore, complementary inputs to these functions will generate complementary outputs.

→ Left circular shift shifts the input to left by fixed positions in circular way.

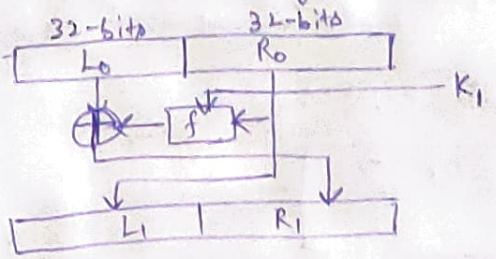
$$LCS(x_1 \cdots x_{32}, 2) = x_3 x_4 \cdots x_{32} x_1 x_2$$

and $LCS(\overline{x_1}, \cdots \overline{x_{32}}, 2) = \overline{x_3}\ \overline{x_4} \cdots \overline{x_{32}}\ \overline{x_1}\ \overline{x_2}$

Again complementary inputs to left circular shift will generate complementary outputs.

∴ If we input complementary keys K and $\overline{K}$ to key scheduling algorithm of DES, the round keys generated will be complementary.

Now, consider one round of Feistel Network of DES.



Ardit Agrawal
2020S1213

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

R_{xM}, L_{xM} → denotes about plaintext M and key K

$R_{x\bar{M}}, L_{x\bar{M}}$ → denotes about plaintext $\bar{M}$ and key $\bar{K}$.

Consider (M,K) and $(\bar{M},\bar{K})$ as 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 $L_{1\bar{M}} = R_{0\bar{M}}$

$\therefore L_{1M}$ and $L_{1\bar{M}}$ are complementary (Since, $R_{0\bar{M}}$ and $R_{0\bar{M}}$ are complementary).

Now, let's look at $f(R_{0M}, K)$ and $f(R_{0\bar{M}}, \bar{K})$.

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

$R_{0\bar{M}} = \overline{x_{32M}}\ \overline{x_{33M}} \cdots \overline{x_{63M}}$

$\therefore E(R_{0\bar{M}}) = \overline{x_{63M}}\ \overline{x_{32M}} \cdots \overline{x_{32M}}$

$E(R_{0\bar{M}}) = \overline{x_{63M}\, x_{32M} \cdots x_{32M}}$

$E(R_{0\bar{M}}) = \overline{E(R_{0M})}$ — (I)

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

$= P(S(\overline{E(R_{0M})} \oplus \bar{K}_1))$ (from (I))

$= P(S(E(R_{0M}) \oplus K_1))$ (complementary keys generated by key schedule algo)

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

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

Therefore,

$R_{1M} = f(R_{0M}, K_1) \oplus L_{0M}$ and $R_{1\bar{M}} = f(R_{0\bar{M}}, \bar{K}_1) \oplus L_{0\bar{M}}$

$R_{1M} = f(R_{0M}, K_1) \oplus L_{0M}$ and $R_{1\bar{M}} = f(R_{0M}, K_1) \oplus L_{0\bar{M}}$ (from (II))

$\therefore R_{1\bar{M}} = \overline{R_{1M}}$

$(\because A \oplus C = \overline{\bar{A} \oplus C}$ as L_{0M} and $L_{0\bar{M}}$ are complementary)

Arduit Agrawal
20205123

$\therefore$ $L_{0M} || R_{0M}$ is complementary to $L_{1\bar{M}} || R_{1\bar{M}}$

Therefore, outputs of round of DES will be complementary given inputs plaintext and keys are complementary.

Since, we apply a permutation IP before round functions and another IP^{-1} after round functions, but permutation does not alter complementary property of inputs.

$$\therefore \quad C_1 = Enc(M, K)$$
$$C_2 = Enc(\bar{M}, \bar{K})$$

$\therefore$ $C_2 = \bar{C_1}$. Hence, shown.

Arclit Agrawal
20205123

Problem 6

Ardit Agrawal
2020 51213

Given ciphertext: AFITIFWF

Encryption Algorithm used is shift cipher.

∵ Shift cipher has only 25 possible keys, we can exhaustively decrypt using each key and find which key gives us meaningful text.

Decryption is given as:

$$Dec(x, K) = (x - K) \bmod 26$$

where x is integer corresponding to english alphabet

∴ Decryption using K=1: ZEHSHEVE

Decryption using K=2: YDGRGDUD

Decryption using K=3: XCFQFCTC

Decryption using K=4: WBEPEDSB

Decryption using K=5: VADODARA

∴ using key K=5, we get meaningful text ie VADODARA.

Hence, plaintext is **VADODARA** and **key is 5.**

Problem 7

Arclit Agrawal 2020512U

In Hill Cipher, if key is a $n \times n$ matrix, we divide the plaintext into n-character blocks. Then we perform matrix multiplication to get the ciphertext.

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

Multiplying both sides by P^{-1} gives

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

⇒ Given plaintext: HILL

⇒ corresponding cipher: XIYJ

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

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

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

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

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

∴ we need to find multiplicative inverse of 15 mod 26

$$\begin{array}{r|l} 15 \overline{)\,26\,(1} & 1 = 4 - 1 \cdot 3 \\ \underline{15} & 1 = 4 - (11 - 2 \times 4) \\ 11 \overline{)\,15\,(1} & 1 = 3 \times 4 - 11 \\ \underline{11} & 1 = 3(15 - 11) - 11 \\ 4 \overline{)\,11\,(2} & 1 = 3 \cdot 15 - 4 \cdot 11 \\ \underline{8} & 1 = 3 \cdot 15 - 4 \cdot (26 - 15) \\ 3 \overline{)\,4\,(1} & 1 = 7 \cdot 15 - 4 \cdot 26 \\ \underline{3} & \\ 1 & \end{array}$$

∴ multiplicative inverse of 15 mod 26 is 7.

$$K = 7 \begin{bmatrix} 61 & -85 \\ 16 & -25 \end{bmatrix} \bmod 26 = \begin{bmatrix} 63 & 183 \\ 112 & 7 \end{bmatrix} \bmod 126 = \boxed{\begin{bmatrix} 11 & 3 \\ 8 & 7 \end{bmatrix}}$$

Answer

Problem 8

Arclit Agrawal
2020512213

(a)

$$18 \overline{)222} \; 12$$
$$18$$
$$42$$
$$36$$
$$6 \overline{)18} \; 3$$
$$18$$
$$0$$

When remainder is 0, the divisor is gcd.

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

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

Let's first calculate gcd of 13, 33 using Euclidean Algorithm.

$$13 \overline{)33} \; 2$$
$$26$$
$$7 \overline{)13} \; 1$$
$$7$$
$$6 \overline{)7} \; 1$$
$$6$$
$$1 \overline{)6} \; 6$$
$$6$$
$$0$$

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

Bezout's Identity states that integer a and b with $d = \gcd(a, b)$, then integer x and y exists such that

$$d = ax + by$$

and x and y can be found using Extended Euclidean Algorithm.

$$\therefore \quad 1 = 7 - 1 \cdot 6$$
$$1 = 7 - (13 - 1 \cdot 7)$$
$$1 = 2 \cdot 7 - 1 \cdot 13$$
$$1 = 2(33 - 2 \cdot 13) - 1 \cdot 13$$
$$1 = 2 \cdot 33 + (-5) \cdot 13$$

$\therefore x_0 = 2$ and $y_0 = -5$

Arclit Agrawal
20205213

(c) Let's calculate GCD of 5 and 26,

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

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

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

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

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 subtract multiples of 26 as modulo 26 will not affect it.

$\therefore$ we can say multiplicative inverse of 5 under modulo 26 is $-5 + 26 = 21$.

multiplicative inverse of 5 under modulo 26 = 21

Problem 9

Akshit Agrawal 2020512213

For AES, the constant C is $(63)_{16}$. Also, the primitive polynomial for AES is $G(x) = x^8 + x^4 + x^3 + x + 1$.

Let us apply Subbyte function of AES to $(D3)_{16}$.

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

∴ polynomial P(x) generated from binary representation of $(D3)_{16}$ is,

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

Now, we need to find inverse of P(x) in $F_2[x]/\langle G(x)\rangle$. We can find it using Extended Euclidean Algorithm.

$$x^8 + x^4 + x^3 + x + 1 = (x+1)(x^7 + x^6 + x^4 + x + 1) + (x^6 + x^5 + x^3 + x^2 + x)$$

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

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

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

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

$$1 = (x^3 + x^2 + x + 1) + (x)(x^2 + x + 1) \quad \{\text{as } + \text{ and } - \text{ are same } \oplus \text{ in } F_2[x]\}$$

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

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

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

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

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

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

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

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

$\therefore$ inverse of $P(x)$ in $\mathbb{Z}_2[x]/\langle G(x)\rangle$ is (x^6+x^5+x+1)

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

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

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

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

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

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

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

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

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

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

$\therefore$ Seedbyte (D3) $= m_7 m_6 m_5 m_4 m_3 m_2 m_1 m_0 = (01100110)_2 = (66)_{16}$

Hence, proved.

Problem 10

Arduit Agrawal
2020512 13

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, AES (33, 42, 66, 24) =~~

Now, we will find the polynomials u_0, u_1, u_2 and u_3, where

$$u_0 = (x \cdot t_0 + (x+1) t_1 + t_2 + t_3) \bmod (x^8 + x^4 + x^3 + x + 1)$$

$$\Rightarrow u_0 = \{(x^6 + x) + (x^6 + x^4 + x^2 + x^5 + x^3 + x) + (x^6 + x) + (x^4 + x^3)\} \bmod (x^8 + x^4 + x^3 + x + 1)$$

$$u_0 = (x^6 + x^5 + x^2 + x) \bmod (x^8 + x^4 + x^3 + x + 1)$$

$$\boxed{u_0 = (x^6 + x^5 + x^2 + x)}$$

$$u_1 = (t_0 + x \cdot t_1 + (x+1) t_2 + t_3) \bmod (x^8 + x^4 + x^3 + x + 1)$$

$$\Rightarrow u_1 = \{(x^5 + 1) + (x^6 + x^4 + x^2) + (x^7 + x^2 + x^6 + x) + (x^4 + x^3)\} \bmod (x^8 + x^4 + x^3 + x + 1)$$

$$\boxed{u_1 = (x^7 + x^5 + x^3 + x + 1)}$$

$$u_2 = (t_0 + t_1 + x t_2 + (x+1) t_3) \bmod (x^8 + x^4 + x^3 + x + 1)$$

$$u_2 = \{(x^5 + 1) + (x^5 + x^3 + x) + (x^7 + x^2) + (x^5 + x^4 + x^4 + x^3)\} \bmod (x^8 + x^4 + x^3 + x + 1)$$

$$\boxed{u_2 = (x^7 + x^5 + x^2 + x + 1)}$$

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

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

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

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

$$S_0 = (01100100)_2$$

$$S_1 = (10101011)_2$$

$$S_2 = (10100111)_2$$

$$S_3 = (00111011)_2$$

~~AES (33, 42,~~

AES MixColumn (33, 42, 66, 24) = (S_0, S_1, S_2, S_3)

Since, the output is asked in integer, therefore,

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

Ardiet Agrawal 20205713

Problem 11

$f_{(a,b)} : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ by the 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' and y', and we need to prove if (a,b) can be found. Using the given rule we can say,

$$(ax + b) \equiv y \bmod p \quad \text{---(I)}$$

and, $$(ax' + b) \equiv y' \bmod p \quad \text{---(II)}$$

Subtracting (I) from (II),

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

$\because x' \neq x \Rightarrow x' - x \neq 0$. Now, if we know inverse of $(x' - x)$ under modulo p, we can find 'a'. Inverse of $(x' - x)$ under modulo p exists iff $\gcd(x' - x, p) = 1$.

$\because p$ is a prime number, therefore $\gcd(x' - x, p)$ will be 1. Therefore, inverse of $(x' - x)$ under modulo p exists.

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

Once, we find a using above equation, b can be found by putting value of a in either (I) or (II).

Arclit Agrawal
2020512B

Problem 12

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

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

$$\begin{bmatrix} x_1 + x_2 + x_3 + x_4 \\ x_2 + x_3 + x_4 + x_5 \\ x_3 + x_4 + x_5 + x_6 \\ x_4 + x_5 + x_6 + x_7 \end{bmatrix}^T = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}^T \quad \text{— (I)}$$

— (II)

— (III)

— (IV)

Subtracting (II) from (I),

$$x_1 = x_5 + 1 \quad \text{— (V)}$$

Subtracting (III) from (II),

$$x_2 = x_6 - 1 \quad \text{— (VI)}$$

Subtracting (IV) from (III),

$$x_3 = x_7 + 1 \quad \text{— (VII)}$$

Since, all the operations are under modulo 2, from (IV), we 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 equation (IV). Therefore, all possible tuples 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 tuple above using (V), (VI) and (VII). Therefore, all the possible pre-images of $(0,1,0,1)$ are:

Arclit Agrawal
2020051213

	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

The 8 tuples mentioned above are pre-images of (0,1,0,1) under the given ~~rule~~ h.

Problem 13

Archit Agrawal
20205213

Let us assume that h_2 is not collision resistant i.e 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 definition of h_2, we can write:

$$h_1\left[h_1(x_{11}) \,||\, h_1(x_{12})\right] = h_1\left[h_1(x_{21}) \,||\, h_1(x_{22})\right] \quad \text{---(I)}$$

Since, h_1 is collision resistant, i.e., it is ~~impossible~~ computationally hard to find $x_a \neq x_b$ such that $h_1(x_a) = h_1(x_b)$.

Therefore, equation (I) can be written as:

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

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

$$x_{11} = x_{21} \quad \text{---(II)}$$

$$x_{12} = x_{22} \quad \text{---(III)}$$

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 resistant function.