Faculty of Engineering & Technology Electrical & Computer Engineering Department

Applied Cryptography– ENCS4320

HW #2

Prepared by:

Maha Maher Mali 1200746

Instructor: Dr. Mohammed Hussein

Section: 2

Date: 20-1-2024

Table of Contents

Table of Figures

Acronyms and Abbreviations

E	Encryption Process
D	Decryption Process
M	Message
P	Plaintext (Same Message)
K	Key
V	OR Operation Symbol
$\oplus$	XOR Operation Symbol
$\|\|$	Concatenation

Section A
Question 1

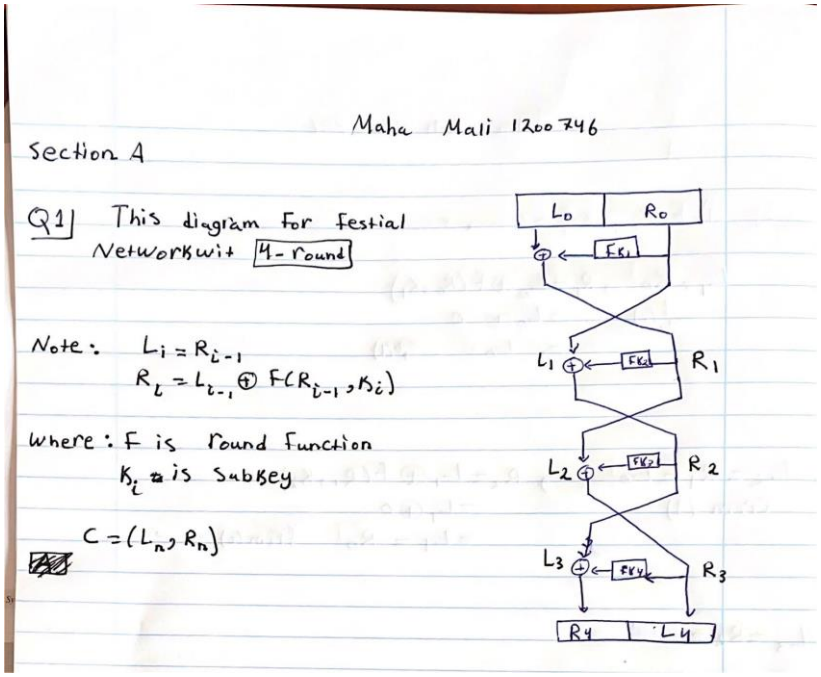


Figure 1:Feistel Network With 4 Round

Part A

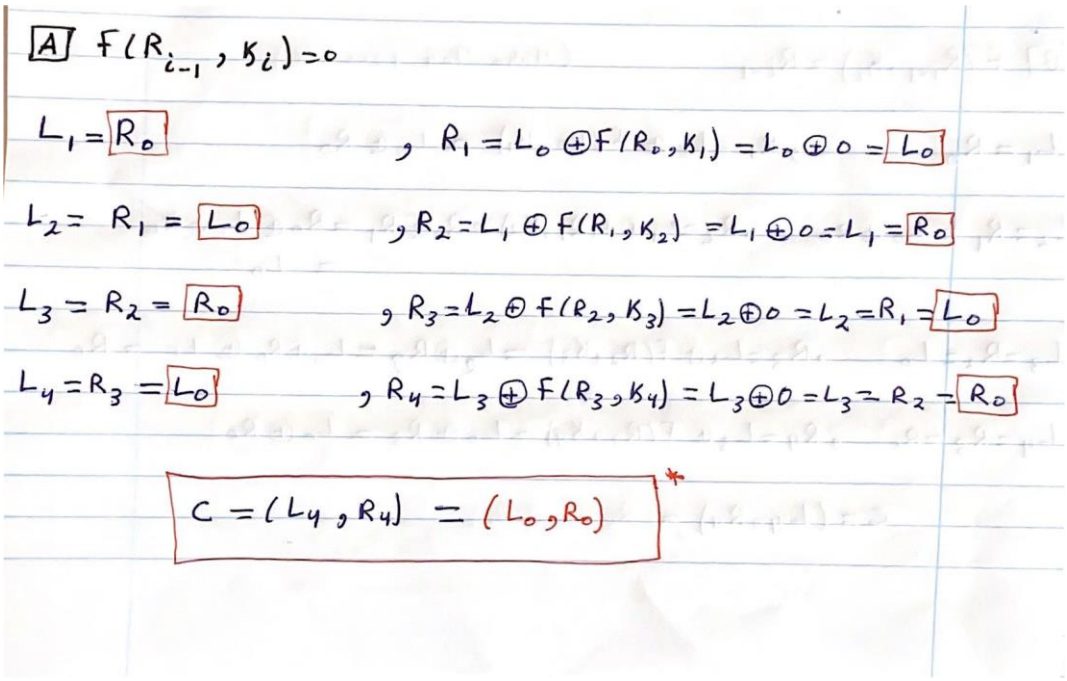


Figure 2: Question 1 Part-A

Part B

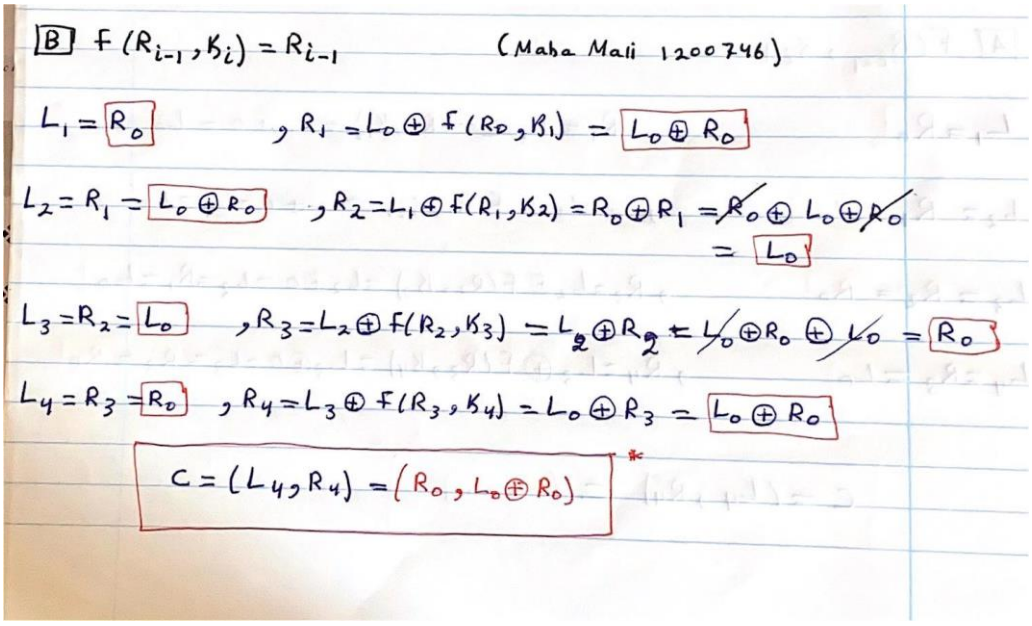


Figure 3: Question 1 Part-B

Part C

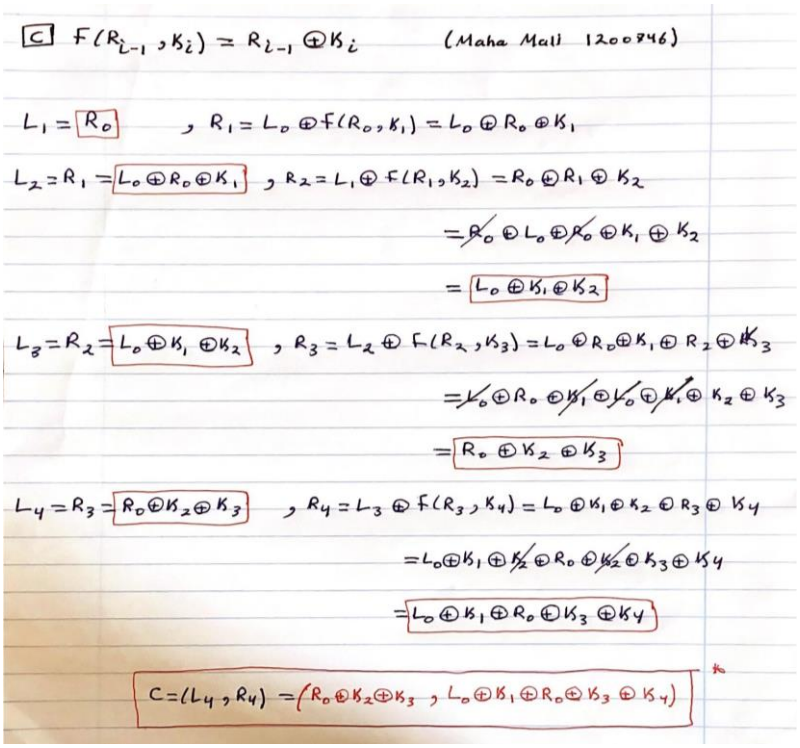


Figure 4: Question 1 Part-C

Question 2
Part A

Diffusion and confusion are two characteristics that help to create a safe encryption. Both confusion and diffusion are employed to stop the original message from being sent or to stop the encryption key from being discovered.[1]

Confusion: confusion is a cryptography method designed to make the cipher text more complex. The approach makes sure that the ciphertext hides any information about the plaintext. The provided approach maintains as complex of a link as possible between the value of the encryption key and the statistics of the encrypted text.[1]

The way the key was utilized to create the ciphertext is so complex that even with some control over the ciphertext statistics, so the attacker would not be able to find out the key.[1]

Diffusion: A cryptographic method known as diffusion was developed to make the plaintext more redundant and hidden its statistical structure in order to prevent attempts to figure out the key.[1]

No one can figure out the original key because of the complex relationship between the long-range statistics of the ciphertext and the statistical structure of the plaintext which might disappear during diffusion. [1]

This is done by distributing each plaintext digit across a large number of ciphertext digits. For example, if a single bit of the plaintext changes the entire ciphertext must be affected or the change must occur on the entire ciphertext.[1]

Features	Confusion	Diffusion
Definition	It is a cryptography technique utilized to create vague ciphertext.	It is employed to generate cryptic plain texts.
Achieved through	It is achieved via the substitution technique.	It is achieved via the transposition technique.
Seeks to	The relationship between the ciphertext statistics and the encryption key value is complicated.	The plain text's statistical structure is dispersed into the ciphertext's long-range statistics.
Used by	It utilizes only block cipher.	It utilizes both stream and block cipher.
Modifications	If one bit in secret is changed, most bits in the cipher text will be changed.	If one image within the plain text changes, most images within the cipher text will also change.
Resultant	Vagueness is increased	Redundancy is increased
Relations	It conceals the relation between the key and the ciphertext.	It conceals the relation between the plaintext and the ciphertext.

Figure 5:Difference Between Confusion &Diffusion [2]

Part B

Confusion in DES is caused by unique boxes known as **S-boxes**. These boxes take in a group of 6 bits and give out a completely other set of 4 bits. This procedure is similar to a secret in that the output may be completely changed through changing a small number of bits in the input. Anyone trying to estimate the output without knowing the secret key will find it extremely difficult to do. So, DES confusion might be compared to a challenge in which one small change in the initial picture gives an entirely different solution.

Part C

In DES diffusion is accomplished by use of permutation operations. Diffusion is built into DES by the **Expansion boxes** which is applied in permutation**,** which distribute each bit's effect over a number of bits in the achieving success rounds. In order to guarantee that a change in one bit of the input affects several bits in the output, the permutation operation rearranges the bits. This enables the information's spread across the ciphertext and dissipation of the statistical structure.

Question 3

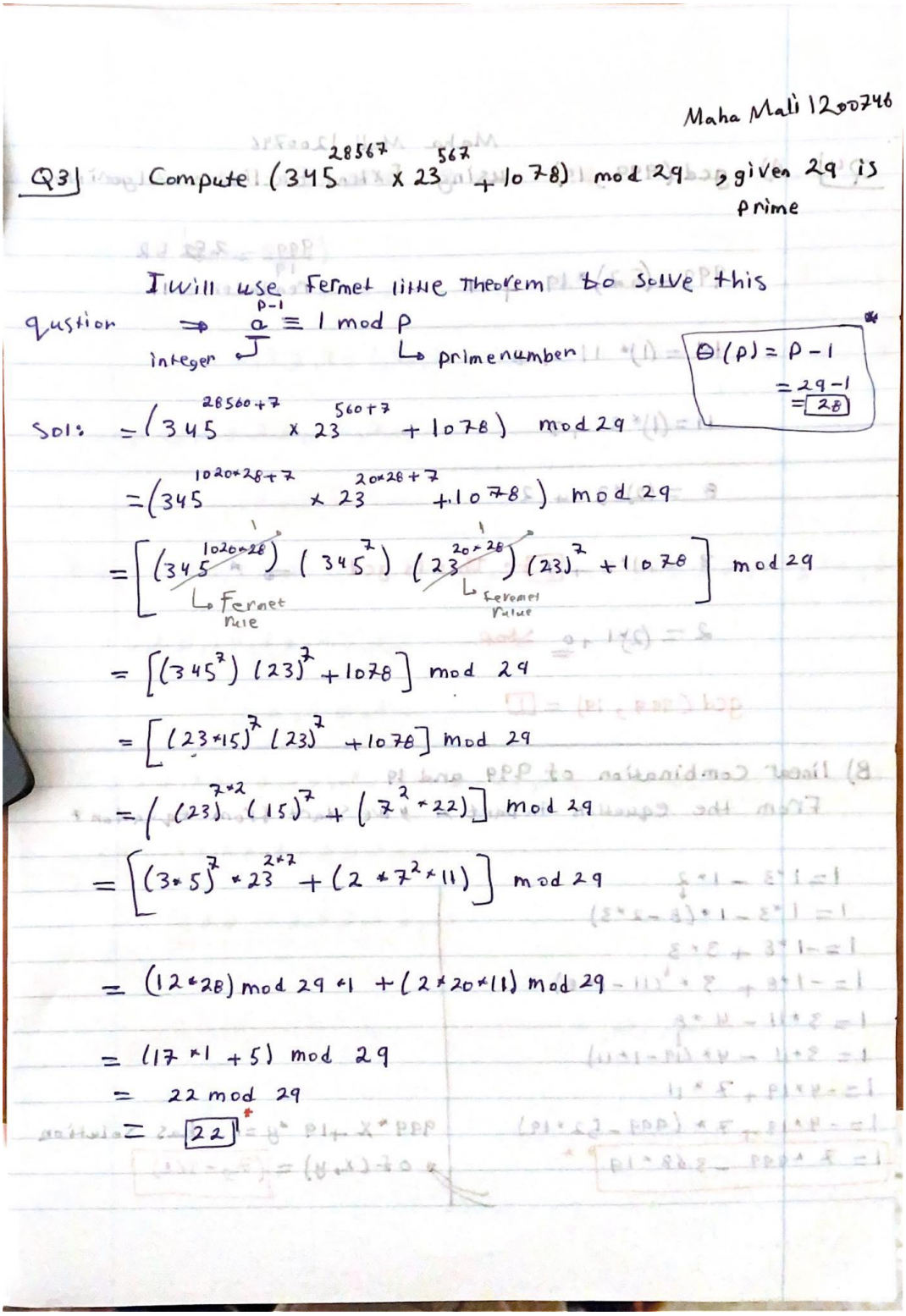


Figure 6: Question 3 Solution

Question 4

Part A

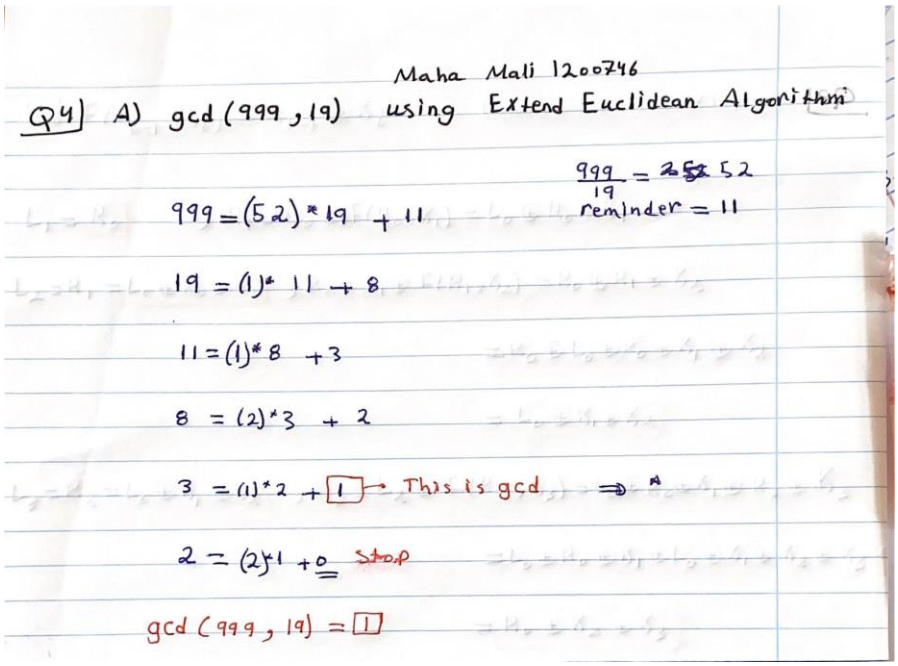


Figure 7: Question 4-part A Solution

Part B

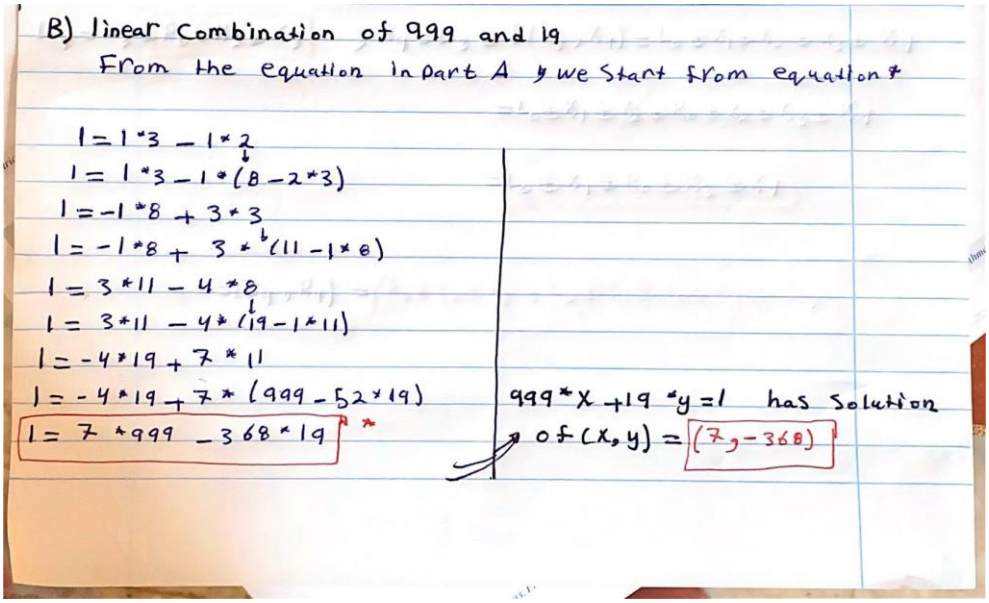
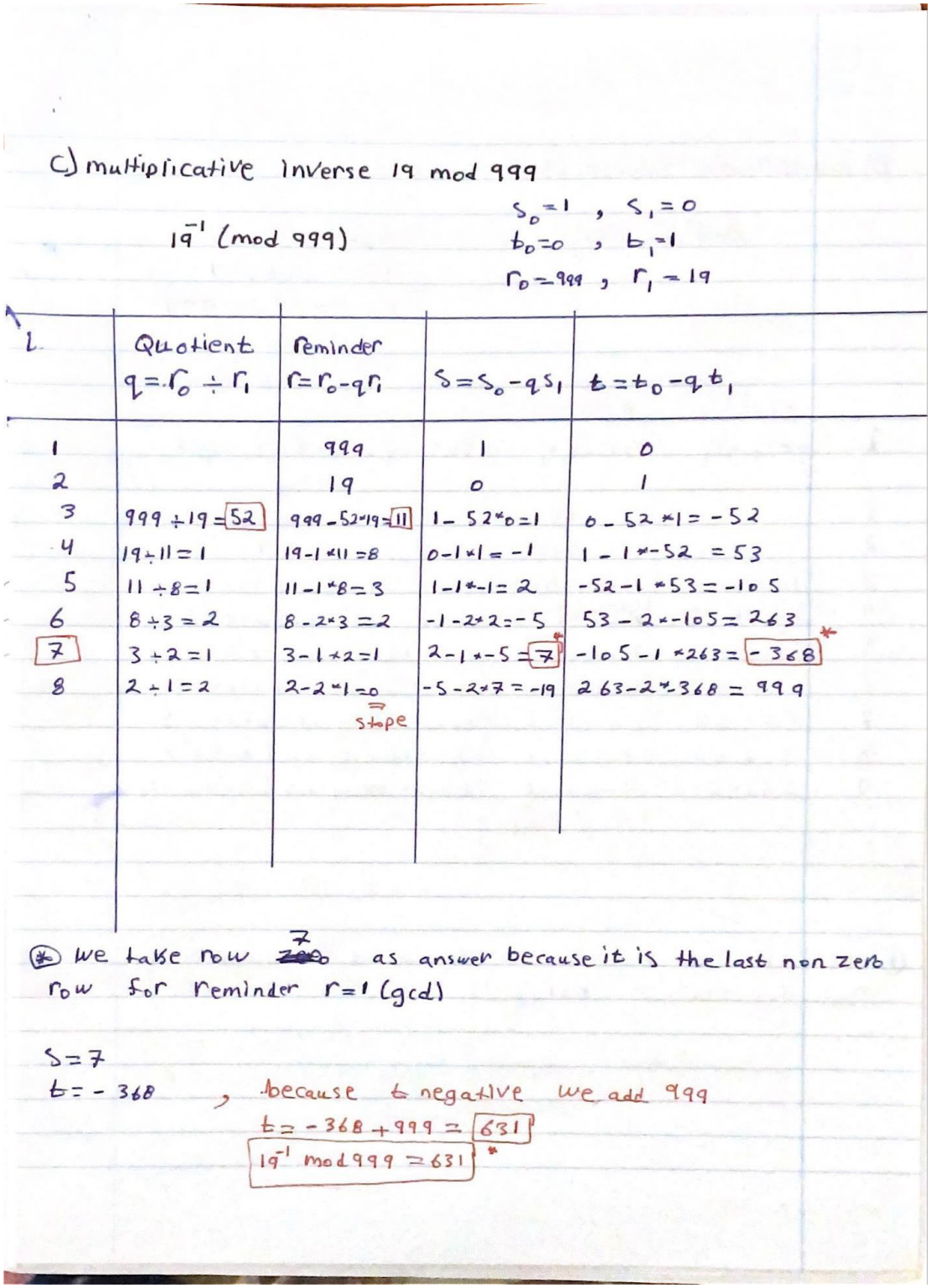


Figure 8 :Question 4-part B Solution

Part C



c) multiplicative inverse 19 mod 999

$19^{-1} \pmod{999}$

$s_0 = 1$, $s_1 = 0$
$t_0 = 0$, $t_1 = 1$
$r_0 = 999$, $r_1 = 19$

i	Quotient $q = r_0 \div r_1$	Reminder $r = r_0 - q r_1$	$s = s_0 - q s_1$	$t = t_0 - q t_1$
1		999	1	0
2		19	0	1
3	$999 \div 19 = 52$	$999 - 52 * 19 = 11$	$1 - 52 * 0 = 1$	$0 - 52 * 1 = -52$
4	$19 \div 11 = 1$	$19 - 1 * 11 = 8$	$0 - 1 * 1 = -1$	$1 - 1 * -52 = 53$
5	$11 \div 8 = 1$	$11 - 1 * 8 = 3$	$1 - 1 * -1 = 2$	$-52 - 1 * 53 = -105$
6	$8 \div 3 = 2$	$8 - 2 * 3 = 2$	$-1 - 2 * 2 = -5$	$53 - 2 * -105 = 263$
7	$3 \div 2 = 1$	$3 - 1 * 2 = 1$	$2 - 1 * -5 = 7$ *	$-105 - 1 * 263 = -368$ *
8	$2 \div 1 = 2$	$2 - 2 * 1 = 0$ ⇒ stop	$-5 - 2 * 7 = -19$	$263 - 2 * -368 = 999$

(*) we take row 7 as answer because it is the last non zero row for reminder $r = 1$ (gcd)

$s = 7$
$t = -368$, because t negative we add 999
$t = -368 + 999 = 631$
$19^{-1} \bmod 999 = 631$ *

Figure 9: Question 4-part C Solution

Part D

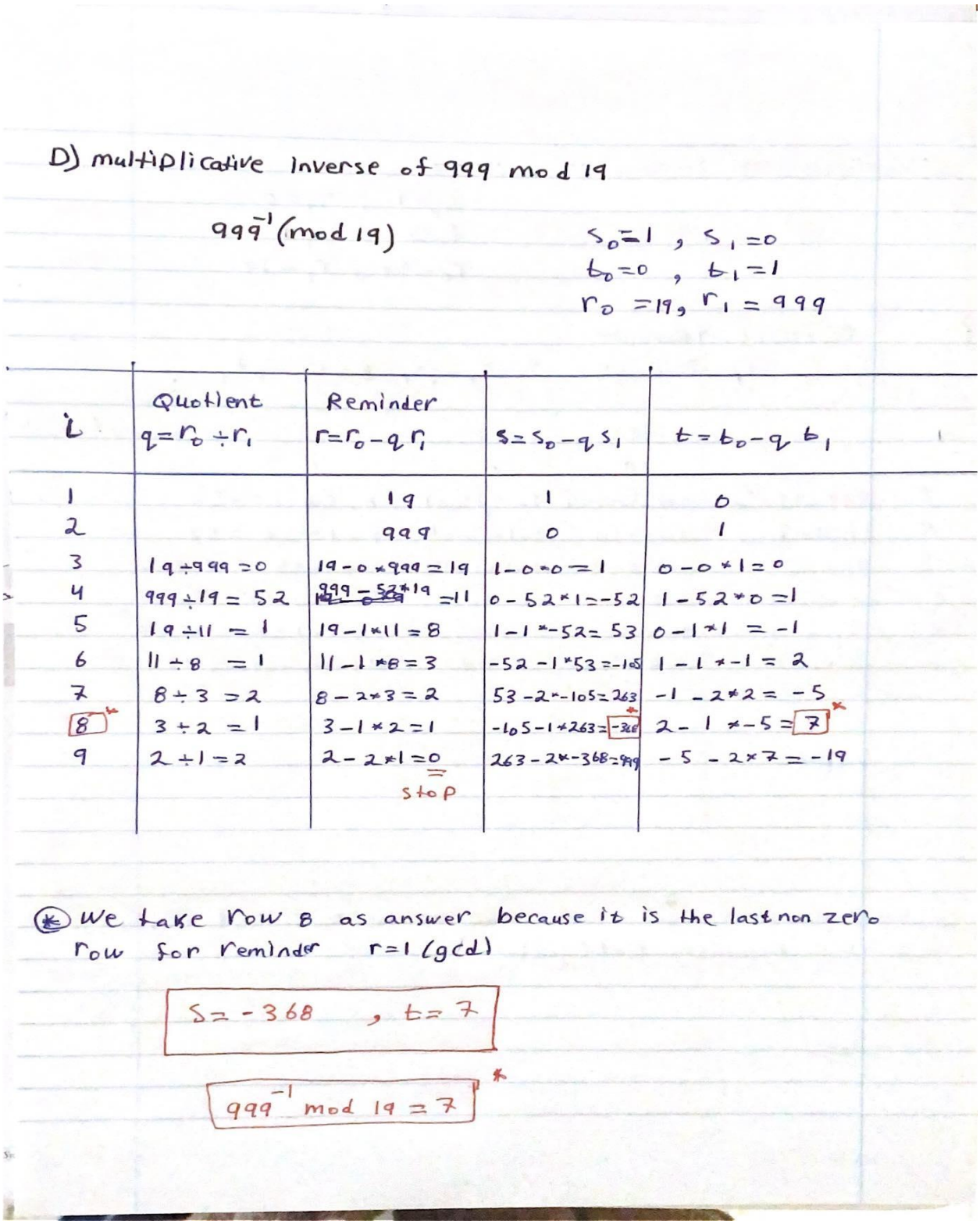
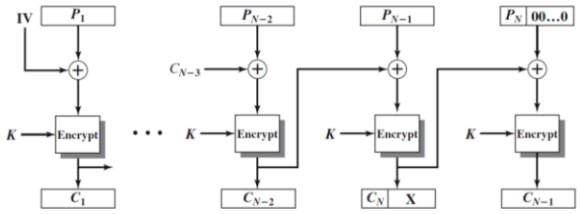


Figure 10: Question 4-part D Solution

Section B
Question 5



* Decryption Sequence:

$$P_i = C_{i-1} \oplus Dec(C_i, K)$$

Part A

Maha Mali 1200746

Q5) A) To find P_N

$C_{N-1} = Enc((P_N || 000..0) \oplus (C_N || X), K)$ $\quad || \Rightarrow$ concatination

Decryption each side:

$DEC(C_{N-1}, K) = (P_N || 000...0) \oplus (C_N || X)$

We need $P_N \Rightarrow$ $P_N || 000...0 = DEC(C_{N-1}, K) \oplus (C_N || X)$ *

We take left part to find P_N (P_N is the left hand portion of $P_N || 000..0$)

To find P_{N-1}:

$C_N || X = Enc((P_{N-1} \oplus C_{N-2}), K)$

Decryption each side:

$DEC(C_N || X) = P_{N-1} \oplus C_{N-2}$

$P_{N-1} = DEC(C_N || X, K) \oplus C_{N-2}$ *

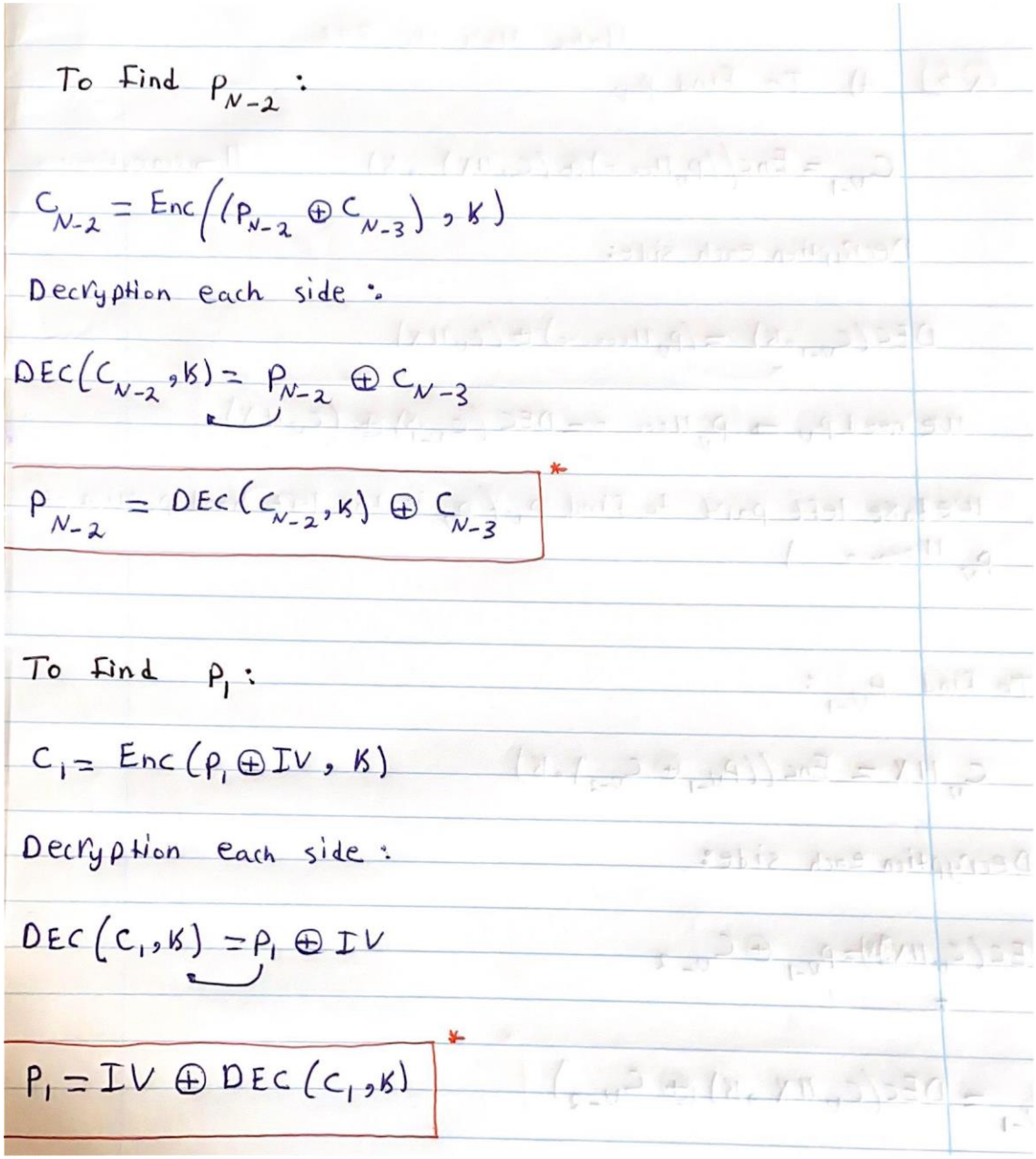
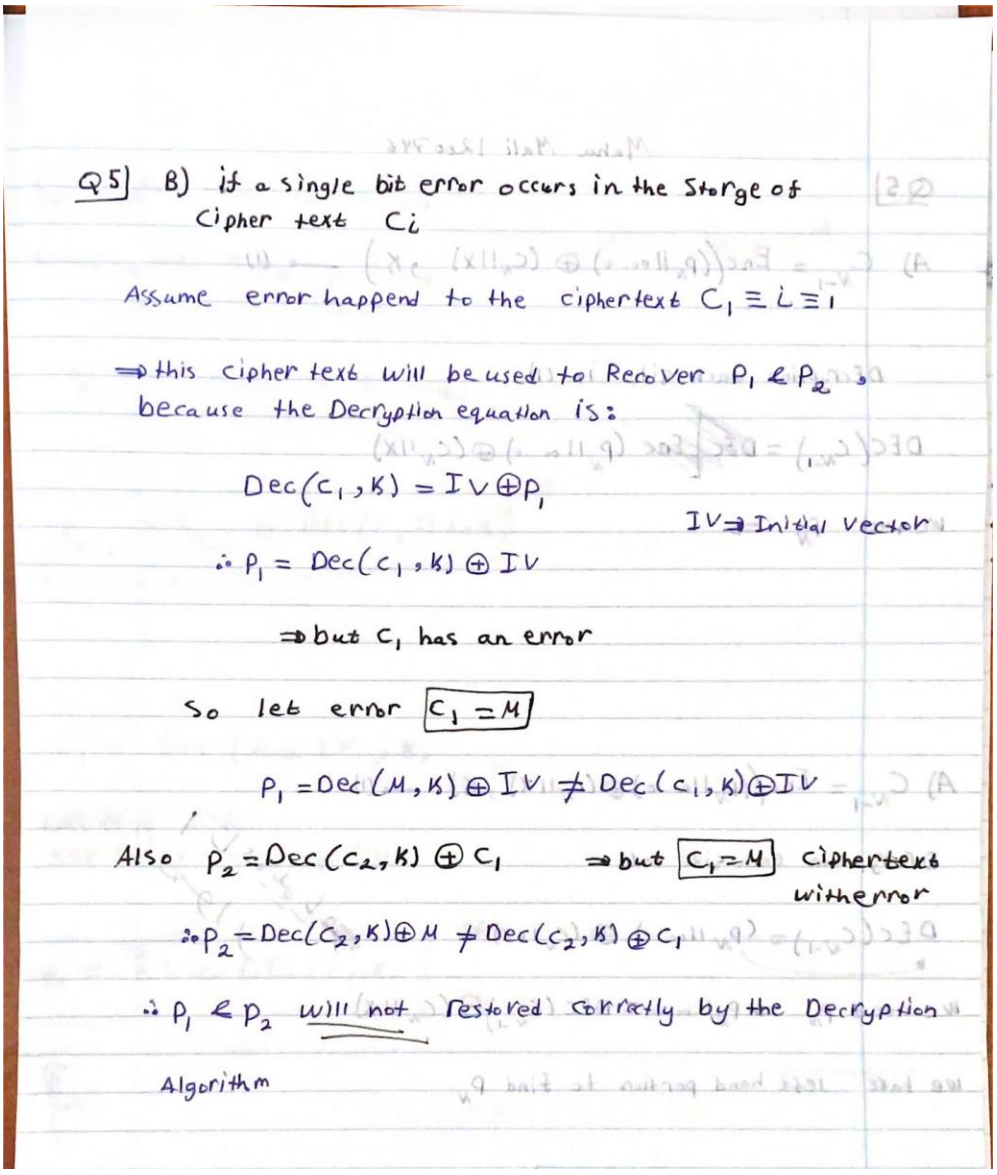


Figure 11: Question 5-part A solution

Part B



Q5] B) if a single bit error occurs in the Storge of Cipher text C_i

Assume error happend to the ciphertext $C_1 \equiv i \equiv 1$

⇒ this cipher text will be used to Recover P_1 & P_2, because the Decryption equation is:

$$Dec(C_1, K) = IV \oplus P_1$$

IV ⇒ Initial Vector

$$\therefore P_1 = Dec(C_1, K) \oplus IV$$

⇒ but C_1 has an error

So let error $\boxed{C_1 = M}$

$$P_1 = Dec(M, K) \oplus IV \neq Dec(C_1, K) \oplus IV$$

Also $P_2 = Dec(C_2, K) \oplus C_1$ ⇒ but $\boxed{C_1 = M}$ ciphertext with error

$$\therefore P_2 = Dec(C_2, K) \oplus M \neq Dec(C_2, K) \oplus C_1$$

$\therefore P_1$ & P_2 will not restored correctly by the Decryption Algorithm

Figure 12: Question 5-part B solution

Section C
Question 6

Part A

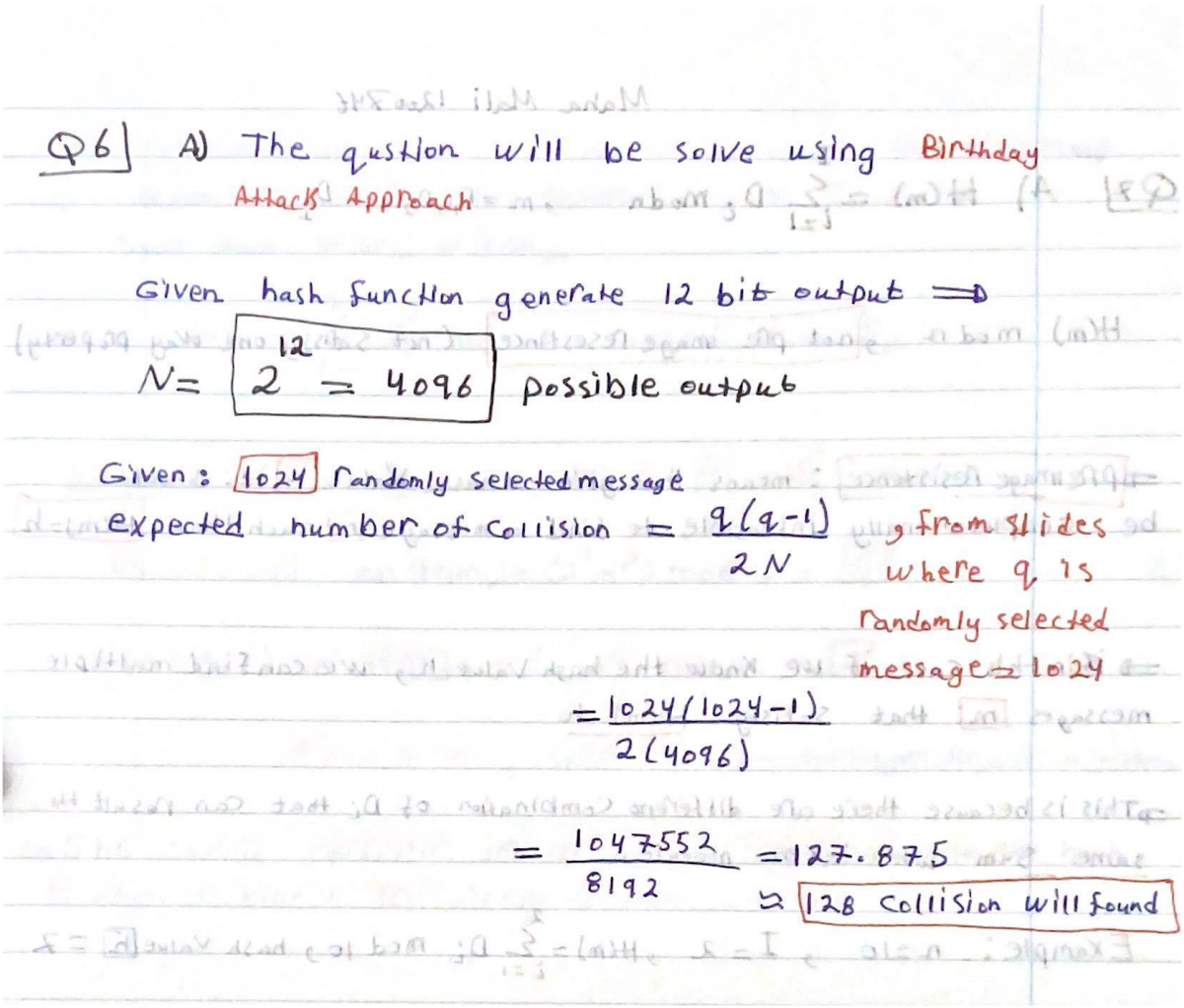


Figure 13: Question 6-part A solution

Part B

Q6] B) What is the expected number of hashes that must be computed to find 25 collisions?

Given number of collision = 25 collisions

Given Hash function generates 12 bit output $\Rightarrow N = 2^{12}$

Required to find number of hashes which is q

number of collision $= \frac{q(q-1)}{2N}$

$q = \sqrt{2N * \text{number of collision}} = \sqrt{2 * 2^{12} * 25}$

$= \sqrt{204800}$

$= 452.54 \approx 453$ number of hashes

Figure 14: Question 6-part B Solution

Question 7
Part A

Maha Mali 1200746

Q7] A) $H(m) = \sum_{i=1}^{I} D_i \bmod n$, $m = D_1, D_2 \dots D_I$

H(m) mod n , not pre image resesitnce (not satisfy one way property)

⇒ preimage resistence : means that given a hash Value h it should be computationally infeasible to find a message m such that H(m)=h

⇒ in this case if we know the hash value h, we can find multiple messages m that satisfy H(m)=h

⇒ This is because there are different combination of D_i that can result the same sum when taken modulo n

Example: n=10 , I=2 , $H(m) = \sum_{i=1}^{2} D_i \bmod 10$, hash Value h = 7

Sol: There are multiple solutions :-

1) if $D_1=3, D_2=4 \Rightarrow H(m) = (3+4) \bmod 10 = 7$

2) if $D_1=5, D_2=2 \Rightarrow H(m) = (5+2) \bmod 10 = 7$

⇒ we have two different message $m_1 = (3,4)$ and $m_2 = (5,2)$ that hash the same value h=7. So this function not pre image because it is not satisfy the preimage condition. if n is not large enough.

⇒ An Attacker could easily find multiple message that hash the same Value

Figure 15: Question 7-part A solution

Part B

B) **Collision Resistance**: hash function should be computationally infeasible to find two different inputs $m_1 \neq m_2$ such that $H(m_1) = H(m_2)$

$$H(m) = \sum_{i=1}^{I} D_i^2 \bmod n \quad , m = D_1, D_2 \cdots D_I$$

Example: $n=10$, $I=2$, $H(m) = (D_1^2 + D_2^2) \bmod 10$

$m_1 = (2,1) \Rightarrow H(m_1) = (2^2+1^2) \bmod 10 = \boxed{5}$

$m_2 = (3,1) \Rightarrow H(m_2) = (3^2+1^2) \bmod 10 = \boxed{2}$

$H(m_1) \neq H(m_2)$ ⇒ so these two messages do not collision

⇒ The square operation introduce a **non linearity** into the hash function making it **less** likely to find collision

⇒ The collision resistence of the hash function depends on the specifics of the **mathmatical operations** and the size n

⇒ if **n** is large this most likely have satisfy collision Resistance.

Figure 16: Question 7-part B solution

Part C

Q7] C) $m = (189, 632, 900, 722, 349)$, $n = 989$

$$H(m) = \sum_{i=1}^{I} D_i^2 \mod n$$

$$H(m) = (189^2 + 632^2 + 900^2 + 722^2 + 349^2) \mod 989$$

$$H(m) = (35721 + 399424 + 810000 + 521284 + 121801) \mod 989$$

$$= 1888230 \mod 989$$

$$H(m) = 229$$

Figure 17: Question 7-part C solution

References

[1] https://techdifferences.com/difference-between-confusion-and-diffusion.html .
Accessed on 18-1-2024 at 10:50 AM.

[2] https://www.javatpoint.com/difference-between-confusion-and-diffusion-in-cryptography .

Accessed on 18-1-2024 at 11:50 AM.

[3] https://www.youtube.com/watch?v=3Cb0ys-jppU .
Accessed on 20-1-2024 at 11:30 AM.