جامعة بيرزيت

Birzeit University

Faculty of Engineering and Technology

Department of Electrical and Computer Engineering

First Semester – 2023/2024

ENCS4320 - Applied Cryptography

Homework # 2

Prepared by: Dana Bornata.

ID: 1200284

Instructor Dr. Mohammed S. Hussein

Date : January 27, 2024

Section #2

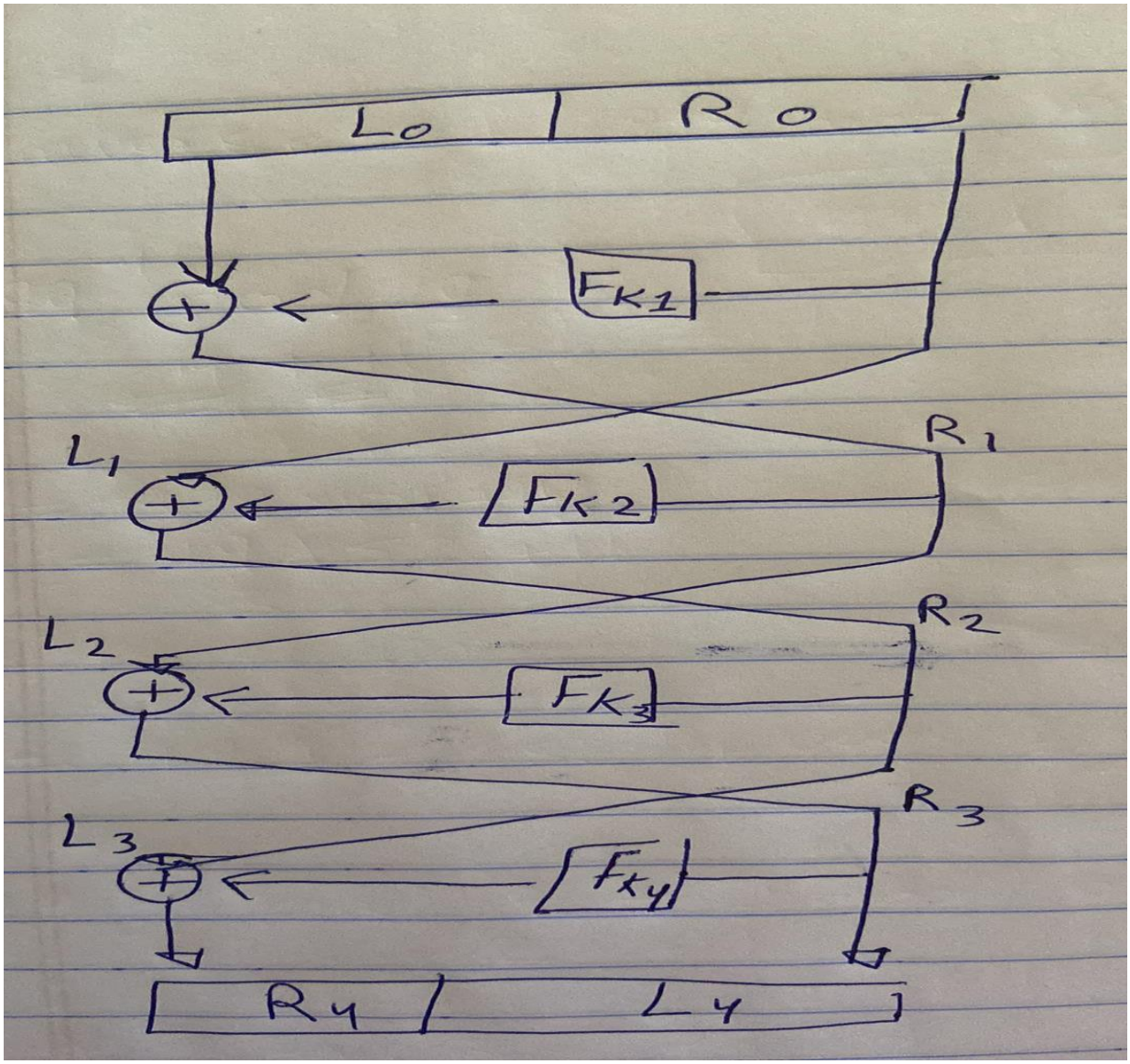
Question 1 (12 points):

Consider a **Feistel cipher** with ***four rounds***. Then the plaintext is denoted as $\boldsymbol{P} = (\boldsymbol{L_0}, \boldsymbol{R_0})$ and the corresponding ciphertext is $\boldsymbol{C} = (\boldsymbol{L_4}, \boldsymbol{R_4})$. What is the **simplest form** of the ciphertext $\boldsymbol{C}$, in terms of $\boldsymbol{L_0}$, $\boldsymbol{R_0}$, and the subkeys, for each of the following round functions? (You should clearly show steps about how you get the answer)

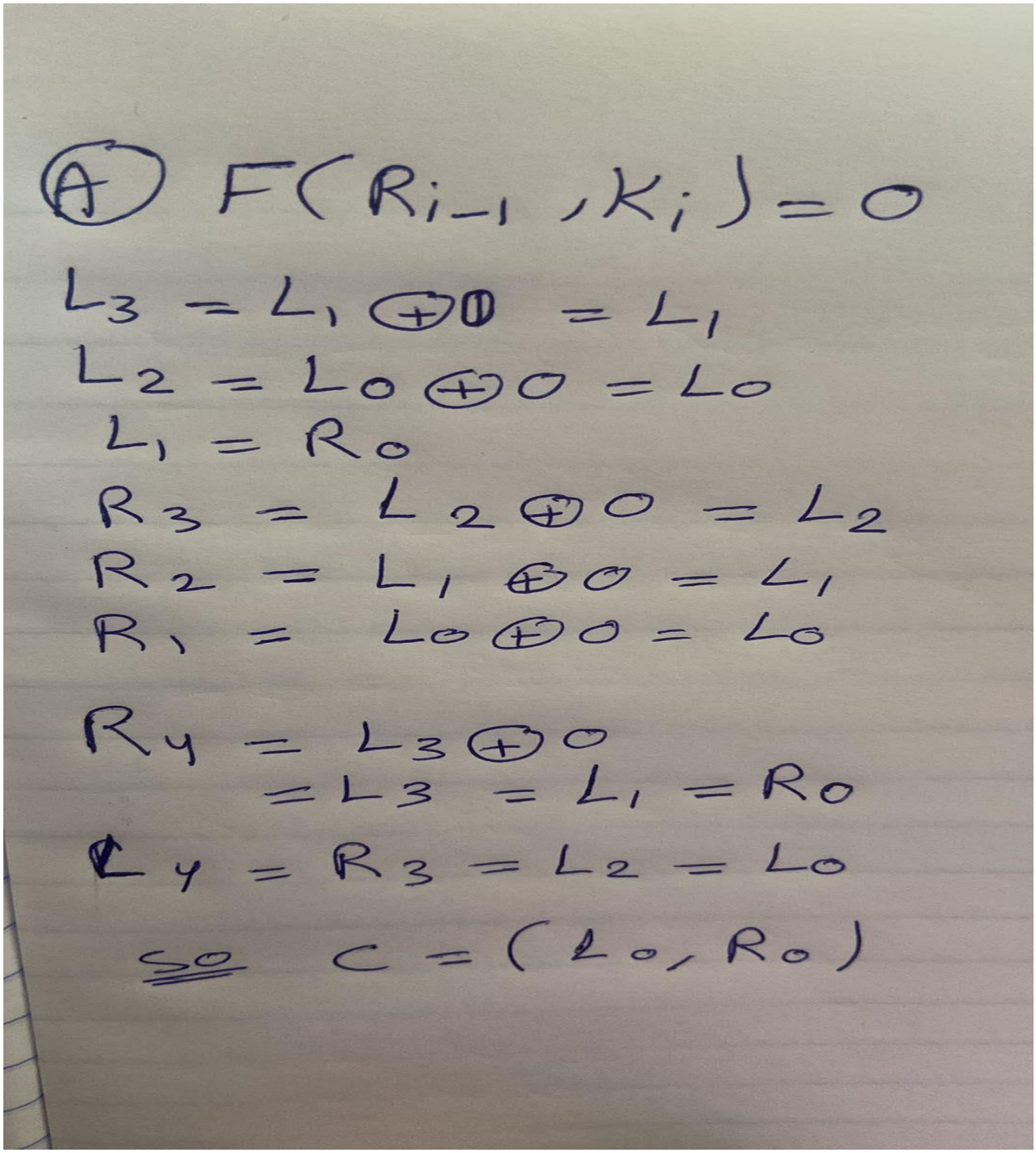
A) $\boldsymbol{F(R_{i-1}, K_i) = 0}$

B) $\boldsymbol{F(R_{i-1}, K_i) = R_{i-1}}$

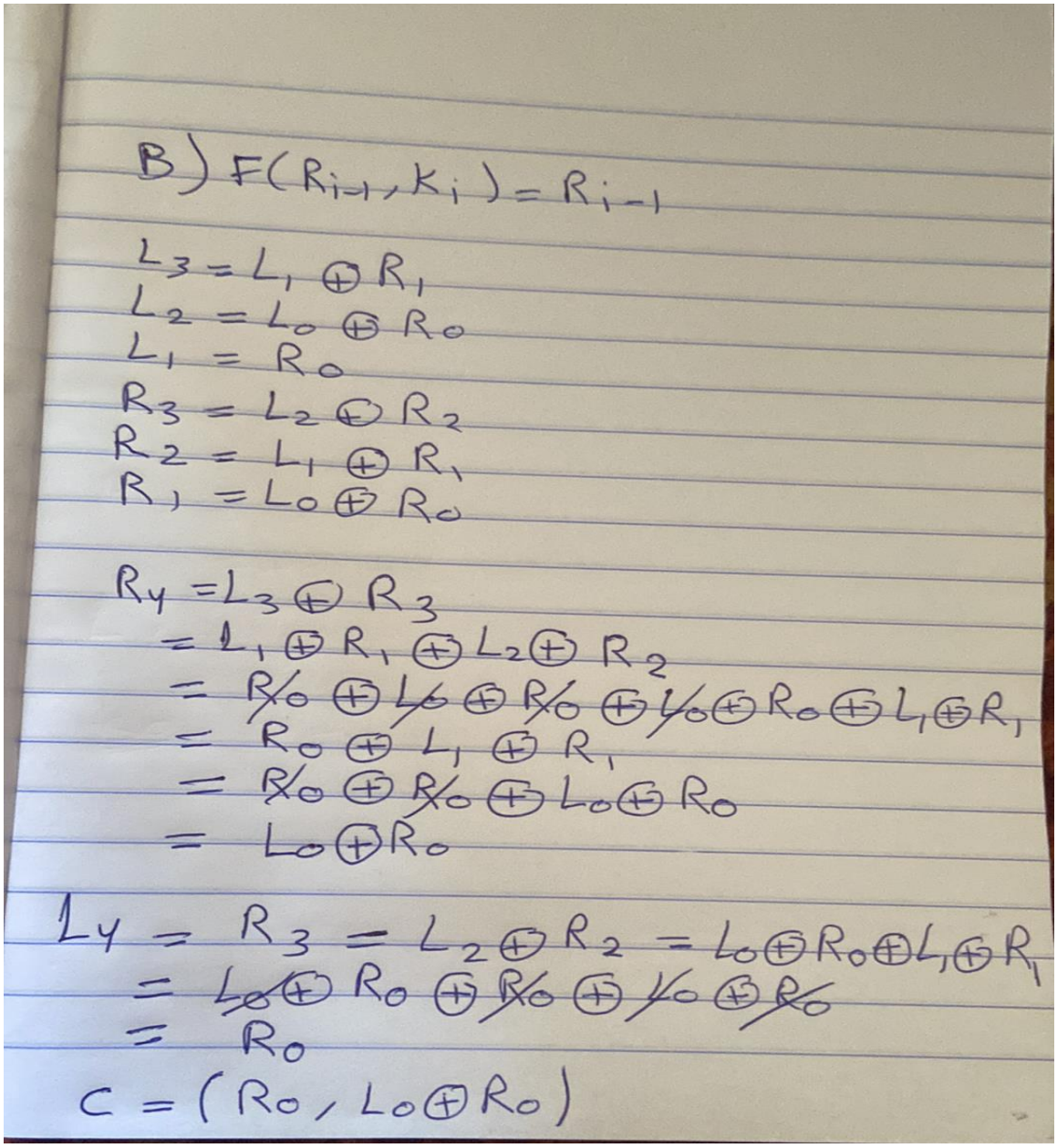
C) $\boldsymbol{F(R_{i-1}, K_i) = R_{i-1} \oplus K_i}$



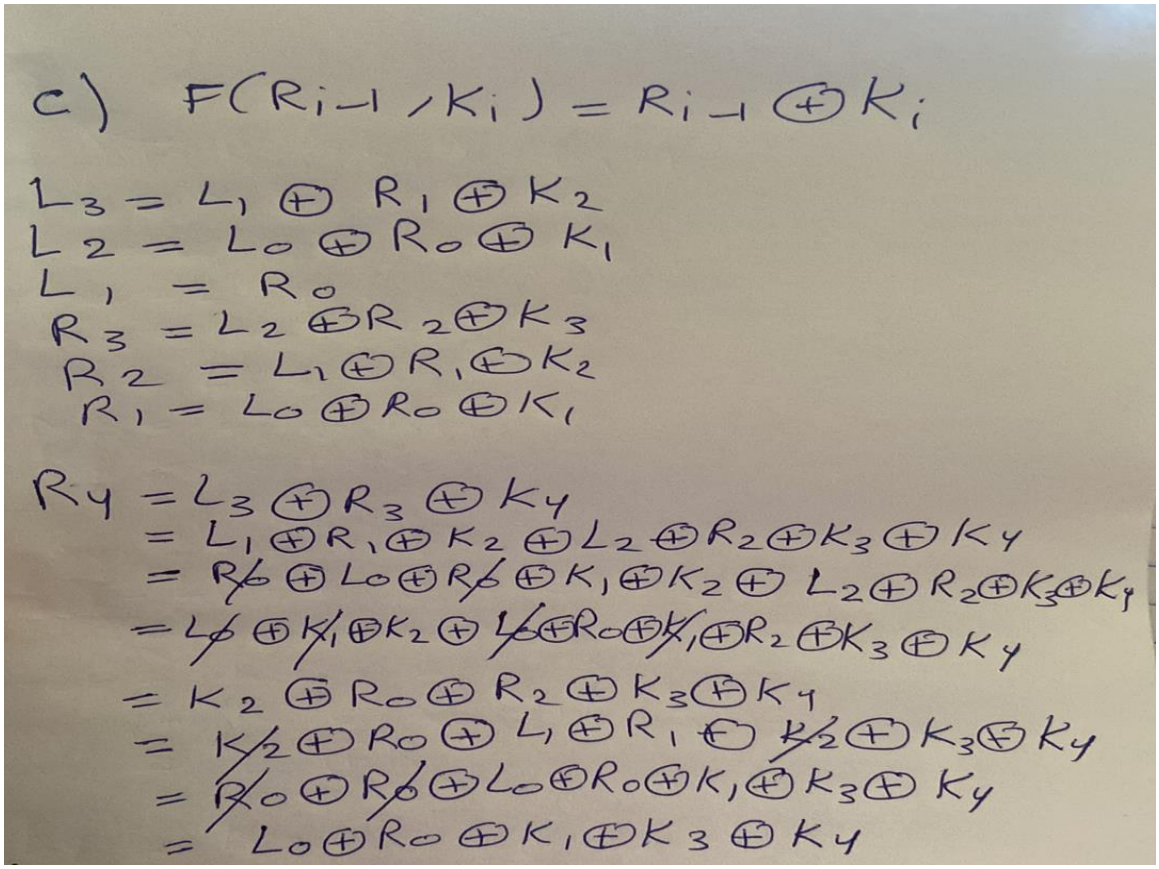
A)

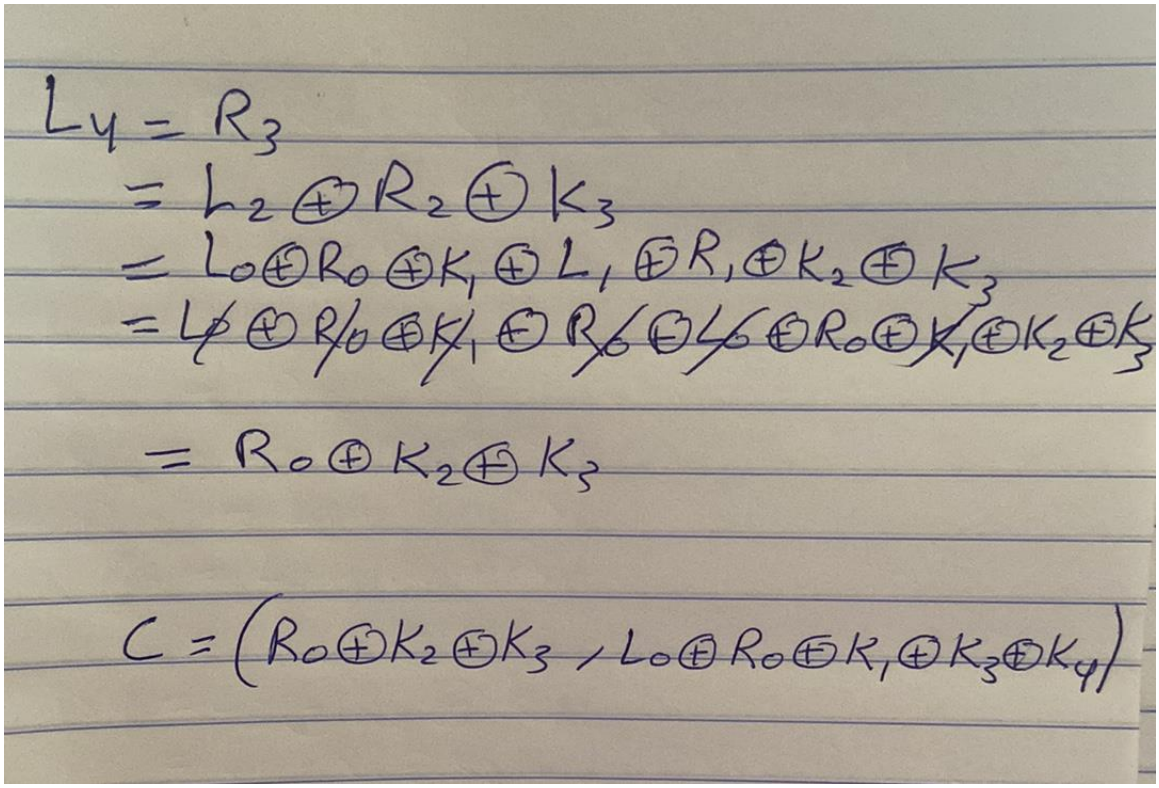

(A) F(Ri-1 , Ki) = 0
L3 = L1 ⊕ 0 = L1
L2 = L0 ⊕ 0 = L0
L1 = R0
R3 = L2 ⊕ 0 = L2
R2 = L1 ⊕ 0 = L1
R1 = L0 ⊕ 0 = L0
R4 = L3 ⊕ 0
= L3 = L1 = R0
L4 = R3 = L2 = L0
So C = (L0, R0)

B)


B) $F(R_{i-1}, K_i) = R_{i-1}$
$L_3 = L_1 \oplus R_1$
$L_2 = L_0 \oplus R_0$
$L_1 = R_0$
$R_3 = L_2 \oplus R_2$
$R_2 = L_1 \oplus R_1$
$R_1 = L_0 \oplus R_0$
$R_4 = L_3 \oplus R_3$
$= L_1 \oplus R_1 \oplus L_2 \oplus R_2$
$= R_0 \oplus L_0 \oplus R_0 \oplus L_0 \oplus R_0 \oplus L_1 \oplus R_1$
$= R_0 \oplus L_1 \oplus R_1$
$= R_0 \oplus R_0 \oplus L_0 \oplus R_0$
$= L_0 \oplus R_0$
$L_4 = R_3 = L_2 \oplus R_2 = L_0 \oplus R_0 \oplus L_1 \oplus R_1$
$= L_0 \oplus R_0 \oplus R_0 \oplus L_0 \oplus R_0$
$= R_0$
$C = (R_0, L_0 \oplus R_0)$

C)


c) $F(R_{i-1}, K_i) = R_{i-1} \oplus K_i$
$L_3 = L_1 \oplus R_1 \oplus K_2$
$L_2 = L_0 \oplus R_0 \oplus K_1$
$L_1 = R_0$
$R_3 = L_2 \oplus R_2 \oplus K_3$
$R_2 = L_1 \oplus R_1 \oplus K_2$
$R_1 = L_0 \oplus R_0 \oplus K_1$
$R_4 = L_3 \oplus R_3 \oplus K_4$
$= L_1 \oplus R_1 \oplus K_2 \oplus L_2 \oplus R_2 \oplus K_3 \oplus K_4$
$= R_0 \oplus L_0 \oplus R_0 \oplus K_1 \oplus K_2 \oplus L_2 \oplus R_2 \oplus K_3 \oplus K_4$
$= L_0 \oplus K_1 \oplus K_2 \oplus L_0 \oplus R_0 \oplus K_1 \oplus R_2 \oplus K_3 \oplus K_4$
$= K_2 \oplus R_0 \oplus R_2 \oplus K_3 \oplus K_4$
$= K_2 \oplus R_0 \oplus L_1 \oplus R_1 \oplus K_2 \oplus K_3 \oplus K_4$
$= R_0 \oplus R_0 \oplus L_0 \oplus R_0 \oplus K_1 \oplus K_3 \oplus K_4$
$= L_0 \oplus R_0 \oplus K_1 \oplus K_3 \oplus K_4$


$L_4 = R_3$
$= L_2 \oplus R_2 \oplus K_3$
$= L_0 \oplus R_0 \oplus K_1 \oplus L_1 \oplus R_1 \oplus K_2 \oplus K_3$
$= L_0 \oplus R_0 \oplus K_1 \oplus R_0 \oplus L_0 \oplus R_0 \oplus K_1 \oplus K_2 \oplus K_3$
$= R_0 \oplus K_2 \oplus K_3$
$C = (R_0 \oplus K_2 \oplus K_3, L_0 \oplus R_0 \oplus K_1 \oplus K_3 \oplus K_4)$

Question 2 (5 points):

Within a single round, the Data Encryption Standard **(DES)** employs both confusion and diffusion.

A) What is the difference between confusion and diffusion in cryptography?

B) Give one source of confusion within a DES round.

C) Give one source of diffusion within a DES round.

A)

Confusion is an encryption operation where the relationship between key and ciphertext is obscured.

Diffusion is an encryption operation where the influence of one plaintext symbol is spread over many ciphertext symbols with the goal of hiding statistical properties of the plaintext.

- Confusion is used to create ignorant cypher text.
- Diffusion is used to make the plain text more redundant.

Confusion	Diffusion
Confusion protects the relationship between the ciphertext and key.	Diffusion protects the relationship between the ciphertext and plaintext.
If an individual bit in the key is changed, some bits in the ciphertext will also be modified.	If an individual symbol in the plaintext is changed, there are some symbols in the ciphertext will also be changed
In confusion, the connection between the data of the ciphertext and the value of the encryption is made difficult. It is completed by substitution.	In diffusion, the numerical mechanism of the plaintext is used up into global statistics of the cipher text. This is achieved by permutation.
vagueness is enhanced in resultant.	redundancy is enhanced in resultant.

B) S-boxes (Substitution boxes)

Confusion: S-boxes are designed to provide confusion by substituting blocks of bits in the plaintext with different blocks of bits in the ciphertext. This substitution is non-linear and complex, making it challenging for an attacker to discern patterns or relationships between the input and output.

DES employs a total of eight S-boxes, and each S-box performs a substitution operation on a 6-bit input to produce a 4-bit output.

c) P-box (Permutation box)

a P-box (Permutation box) is a component used to perform a permutation operation on a set of bits. P-boxes are commonly found in block cipher designs, where they contribute to the diffusion property by rearranging the positions of bits in the data.

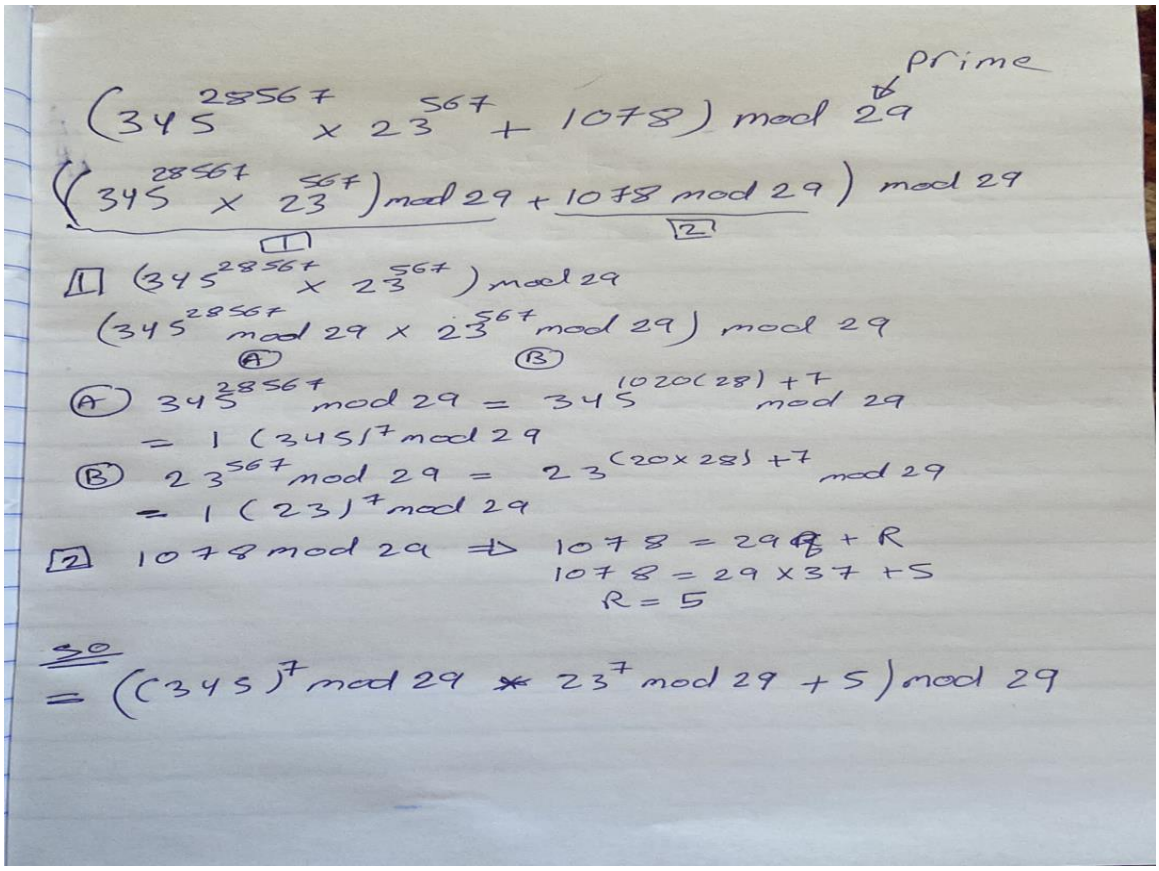
In DES, the P-box is applied after the Feistel function in each round.

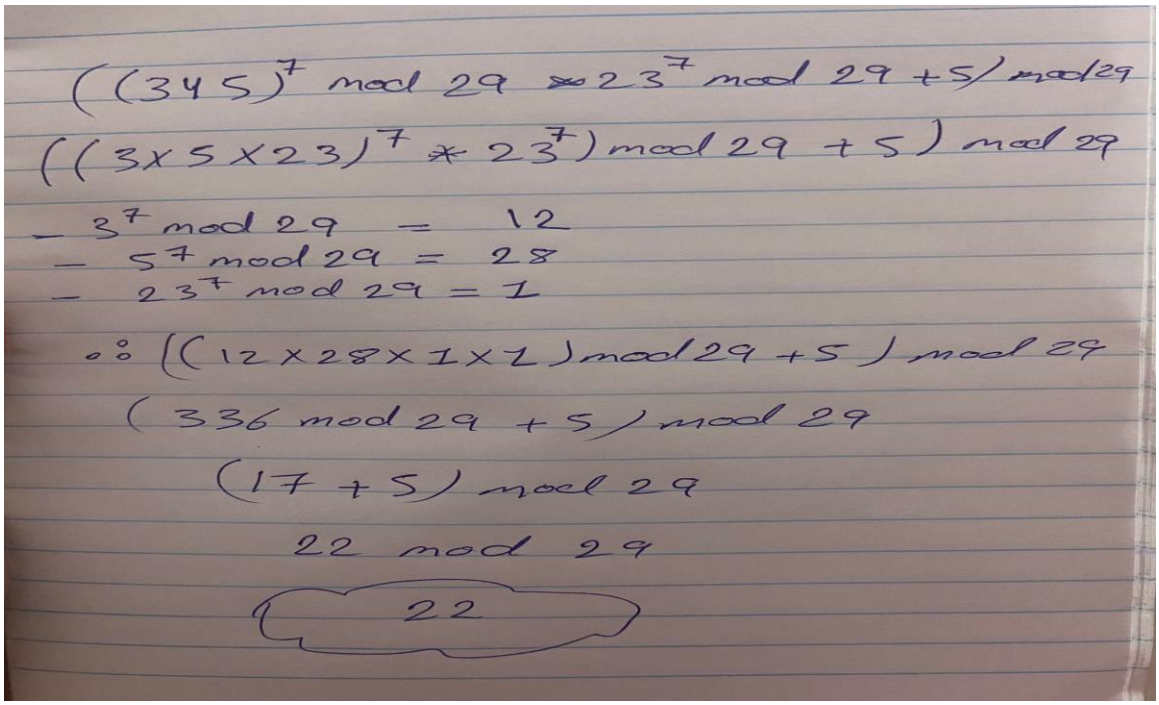
The DES P-box is a fixed permutation that shuffles the bits of the 32-bit output of the Feistel function.

Its purpose is to enhance the security of the algorithm by spreading the influence of each bit across the entire block.

Question 3 (8 points):

Compute ($345^{28567} \times 23^{567} + 1078$) mod 29 given that 29 is a prime.





Question 4 (9 points):

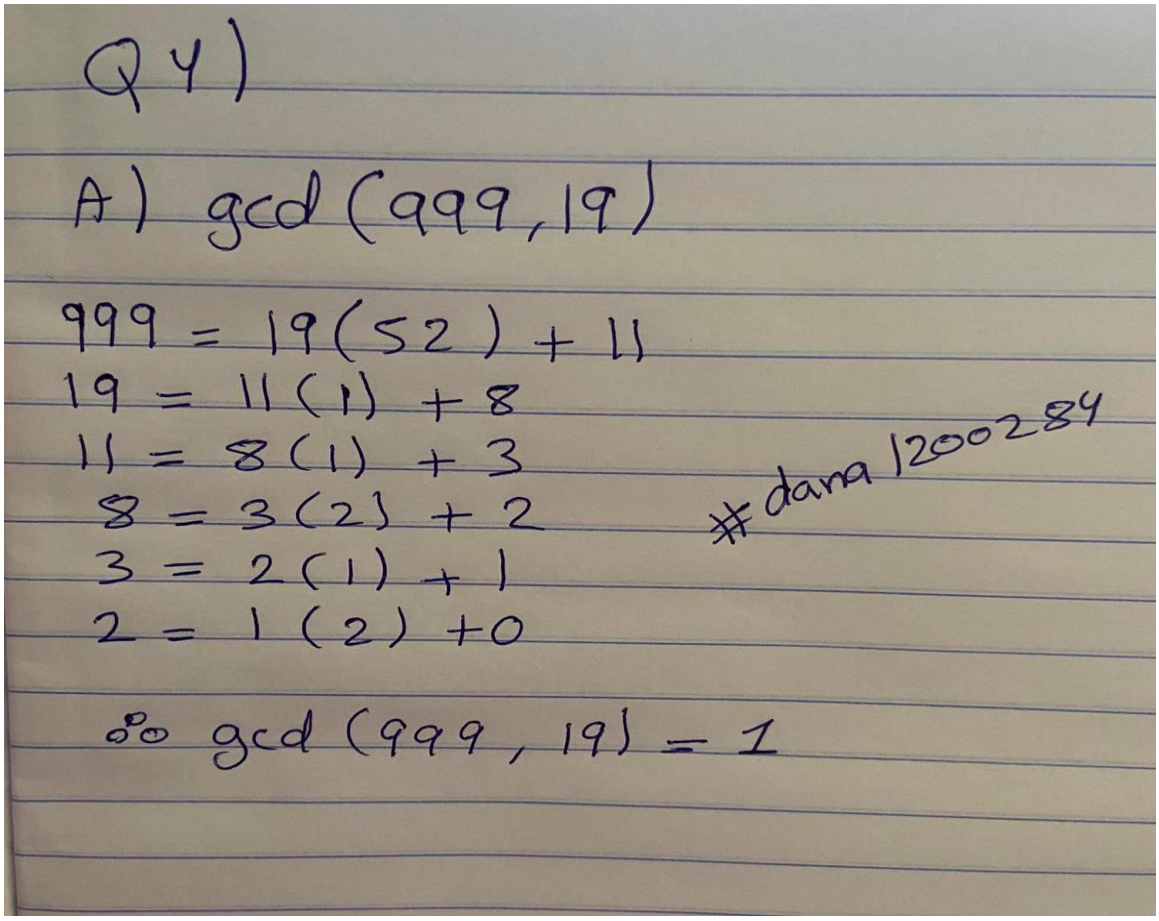
Using the Extended Euclidean algorithm,

A) Find the *greatest common divisor* of **19** and **999**, that is, **gcd(999, 19)**. Show your work clearly step by step.

B) Express the **gcd(999, 19)** as a *linear combination* of **999** and **19**.

C) Compute the *multiplicative inverse* of **19 mod 999**, which is a number between **0** and **998**.

D) Compute the *multiplicative inverse* of **999 mod 19**, which is a number between **0** and **18**.



B) $3 = 2(1) + 1$

1200284

$1 = 3 + 2(-1)$
$1 = 3 + (8 + 3(-2))(-1)$
$1 = 3 + 8(-1) + 3(2)$
$1 = 8(-1) + 3(3)$
$1 = 8(-1) + 3(11 + 8(-1))$
$1 = 8(-4) + 11(3)$
$1 = (19 + 11(-1))(-4) + 11(3)$
$1 = 19(-4) + 11(7)$
$1 = 19(-4) + (999 + 19(-52))(7)$
$1 = 19(-368) + 999(7)$

C) $19^{-1} \bmod 999$

$19x \bmod 999 = 1$

$(1 = 19(-368) + 999(7)) \bmod 999$

$19(-368) \bmod 999 + (7)999 \bmod 999 = 1 \bmod 999$

$= 631$

$19(631) = 1 \bmod 999$

$631 = \frac{1}{19} \bmod 999$

So $X = 631$

D) $999^{-1} \bmod 19$

$999x = 1 \bmod 19$

$(1 = 19(-356) + 999(7)) \bmod 19$

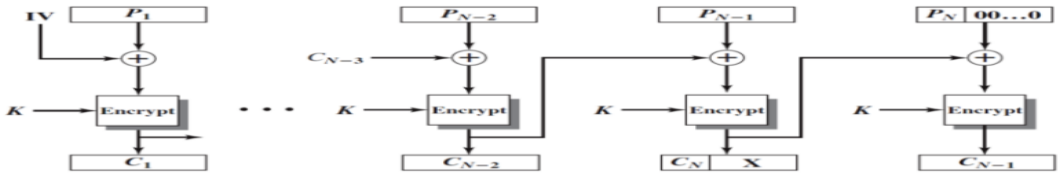
$999(7) \bmod 19 = 1 \bmod 19$

$7 \bmod 19 = 7$

$7 = \frac{1}{999} \bmod 19$

$X = 7$

Question 5:



A) Describe how to decrypt the ciphertext $(C_1, \ldots, C_{N-1}, C_N)$, that is, show the decryption sequence.

B) If a single bit error occurs in the storage of ciphertext C_i, which plaintext blocks, if any, will be correctly restored by the decryption algorithm? Explain your answer.

A)

Dana 1200284

A)

~~*~~ Let || be the concatenation Function.

① $C_{N-1} = Enc((P_N || 00\ldots0) \oplus (C_N || X), K)$

$Dec(C_{N-1}) = (P_N || 00\ldots0) \oplus (C_N || X)$

$(P_N || 00\ldots0) = Dec(C_{N-1}) \oplus (C_N || X)$

So P_N the left-hand answer of result $(P_N || 00\ldots0)$

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

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

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

③ $C_1 = Enc(P_1 \oplus IV, K)$

$Dec(C_1) = P_1 \oplus IV$

$P_1 = Dec(C_1) \oplus IV$

B)

For example, I will take the simple example that we discussed in the lecture:

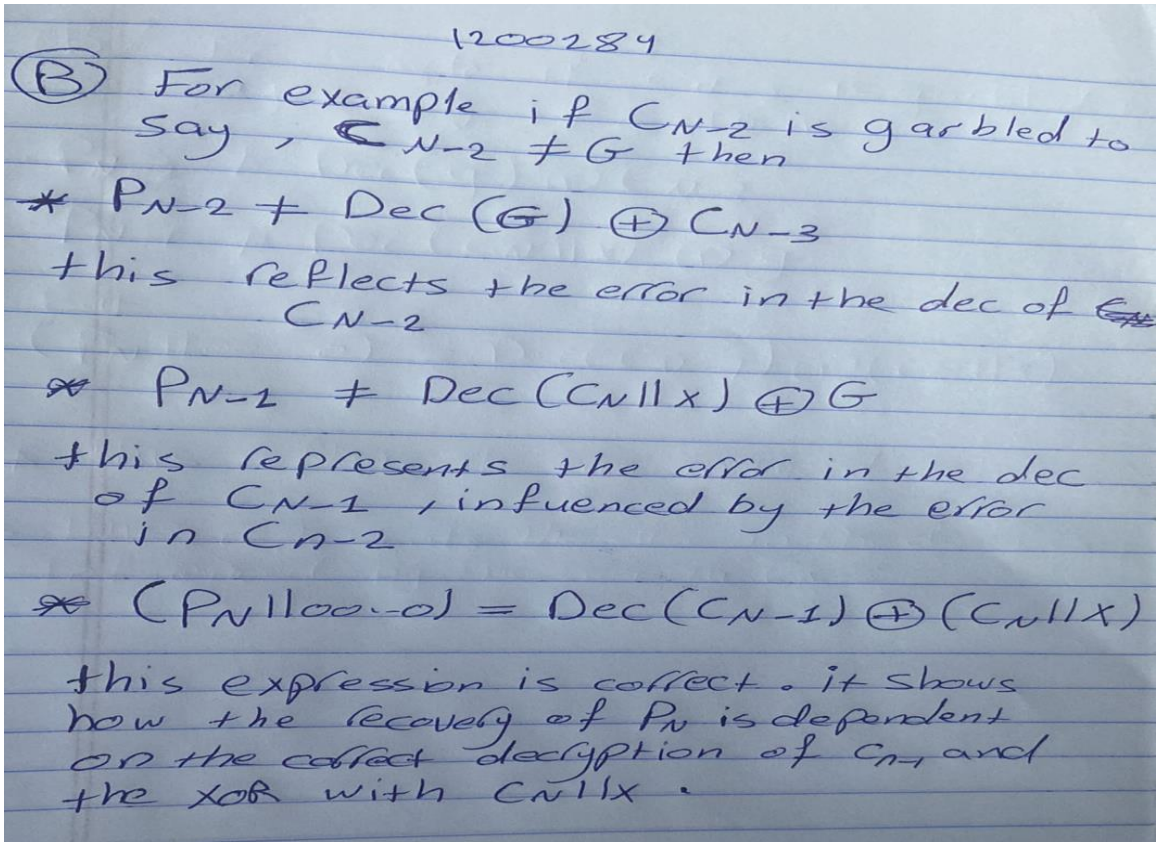
- If C_1 is garbled to, say, $G \neq C_1$ then

  $P_1 \neq C_0 \oplus \text{Dec}(G, K)$, $P_2 \neq G \oplus \text{Dec}(C_2, K)$

- But $P_3 = C_2 \oplus \text{Dec}(C_3, K)$, $P_4 = C_3 \oplus \text{Dec}(C_4, K)$, ...
- Automatically recovers from errors!
  - Each plaintext block only depends on two consecutive ciphertext blocks, so errors do not propagate beyond two blocks

Same idea in this question:

The decryption method in Ciphertext Stealing (CTS) mode is built to recover from ciphert ext faults.
The essential feature is that every block of plaintext depends solely on two blocks of ciph ertext that come after it.



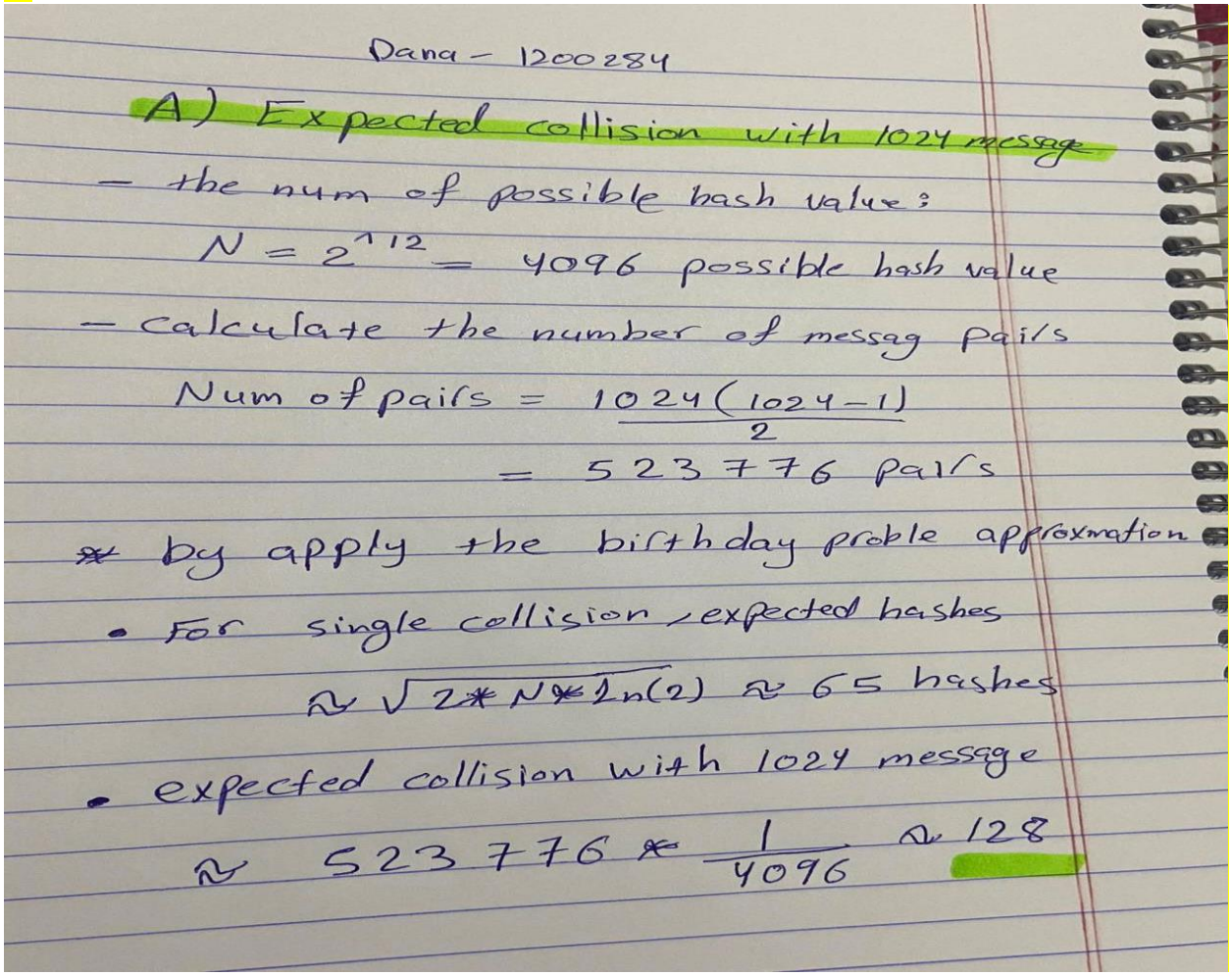
Q)6

Suppose that $H(m)$ is a secure hash function that generates a **12**-bit output.

A) How many collisions would you expect to find if you hash **1024** randomly selected messages?

B) What is the expected number of hashes that must be computed to find **25** collisions? That is, what is the expected number of hashes that must be computed to find pairs (x_i, y_i), $x_i \neq y_i$, with $H(x_i) = H(y_i)$, for $i = 1, 2, \ldots, 25$?

A)

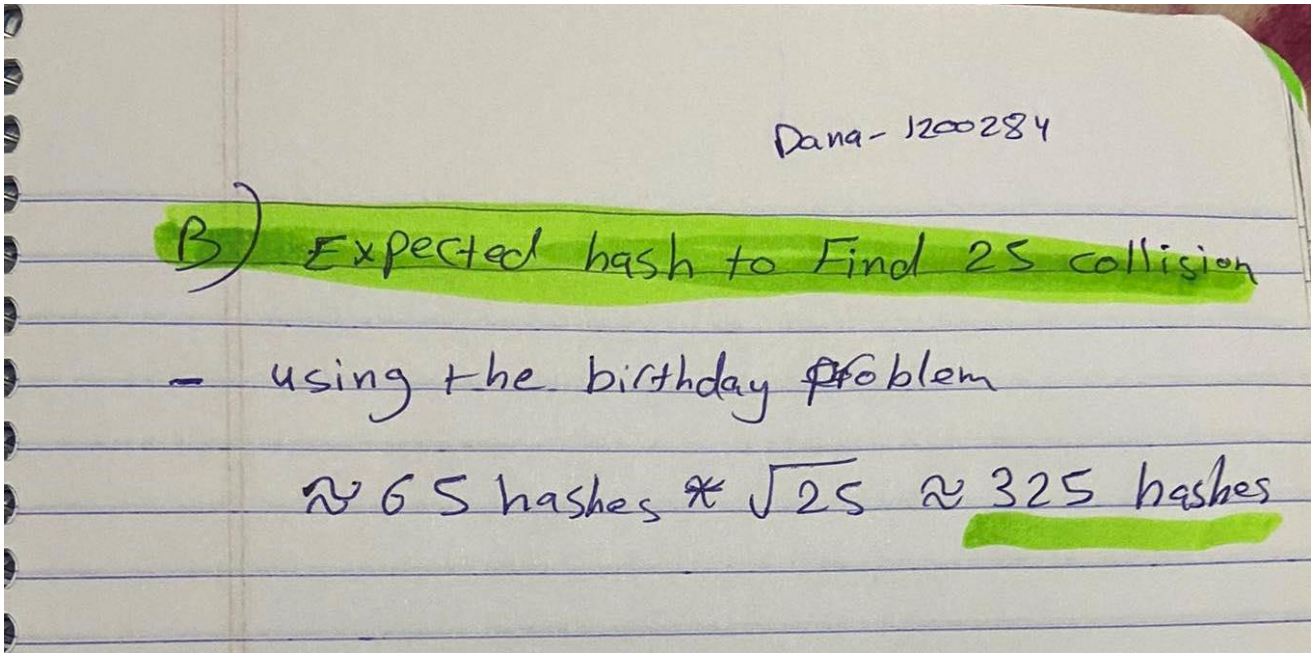


SO:

When hashing 1024 messages with a 12-bit hash function, we can expect approximately 128 collisions on average. This means roughly one out of eight messages will collide with another.

However, due to the randomness of the hashing process, the actual number of collisions in any specific run can be slightly higher or lower than 128.

B)



SO:

To find 25 distinct message pairs with the same hash value (25 collisions), we need to calculate approximately 325 hashes on average.

This implies that simply hashing 1024 messages, while likely surpassing 25 collisions, won't necessarily guarantee finding 25 distinct colliding pairs.

Q)7

Consider the following hash function $H(m)$, which receives as an input a message in the form of a sequence of decimal numbers, $m = (D_1, D_2, \dots, D_I)$.

A) If $H(m)$ is defined as $(\sum_{i=1}^{I} D_i) \bmod n$, for some predefine large value n. Does this hash function satisfy the pre-image resistance (one-way property) requirement? Explain your answer.

B) If $H(m)$ is defined as $(\sum_{i=1}^{I} D_i^2) \bmod n$, for some predefine large value n. Does this hash function satisfy the collision resistance requirement? Explain your answer.

C) Calculate the hash function of part (B) for $m = (189, 632, 900, 722, 349)$ and $n = 989$.

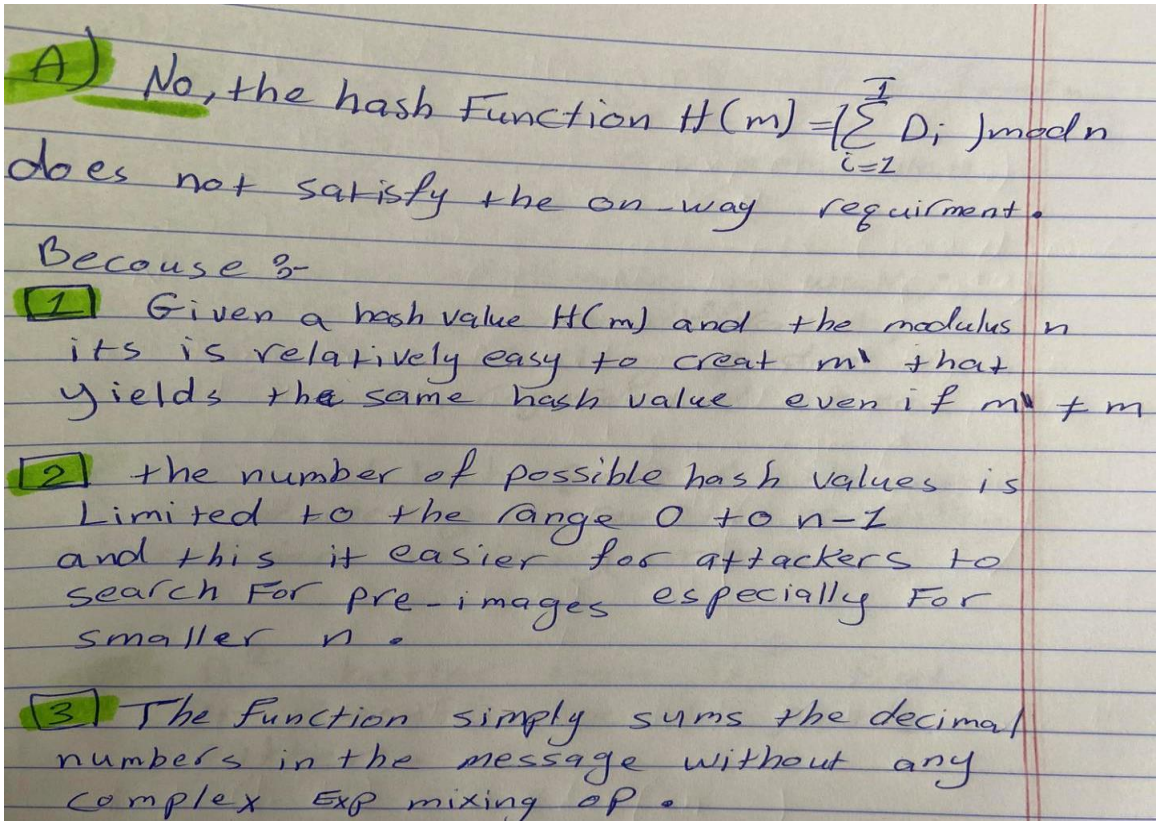
A)

One-way , also known as pre-image resistance, is a property of a hash function that makes it computationally infeasible to reverse the process of hashing and find the original input given its hash value. In other words, it should be difficult to find X given H(X).

$\mathbf{Exp}_H^{ow}(A)$

1. $X \xleftarrow{\$} \mathcal{M}$
2. $Y \leftarrow H(X)$
3. $X' \leftarrow A(Y)$
4. return $H(X') \stackrel{?}{=} Y$

In this q:

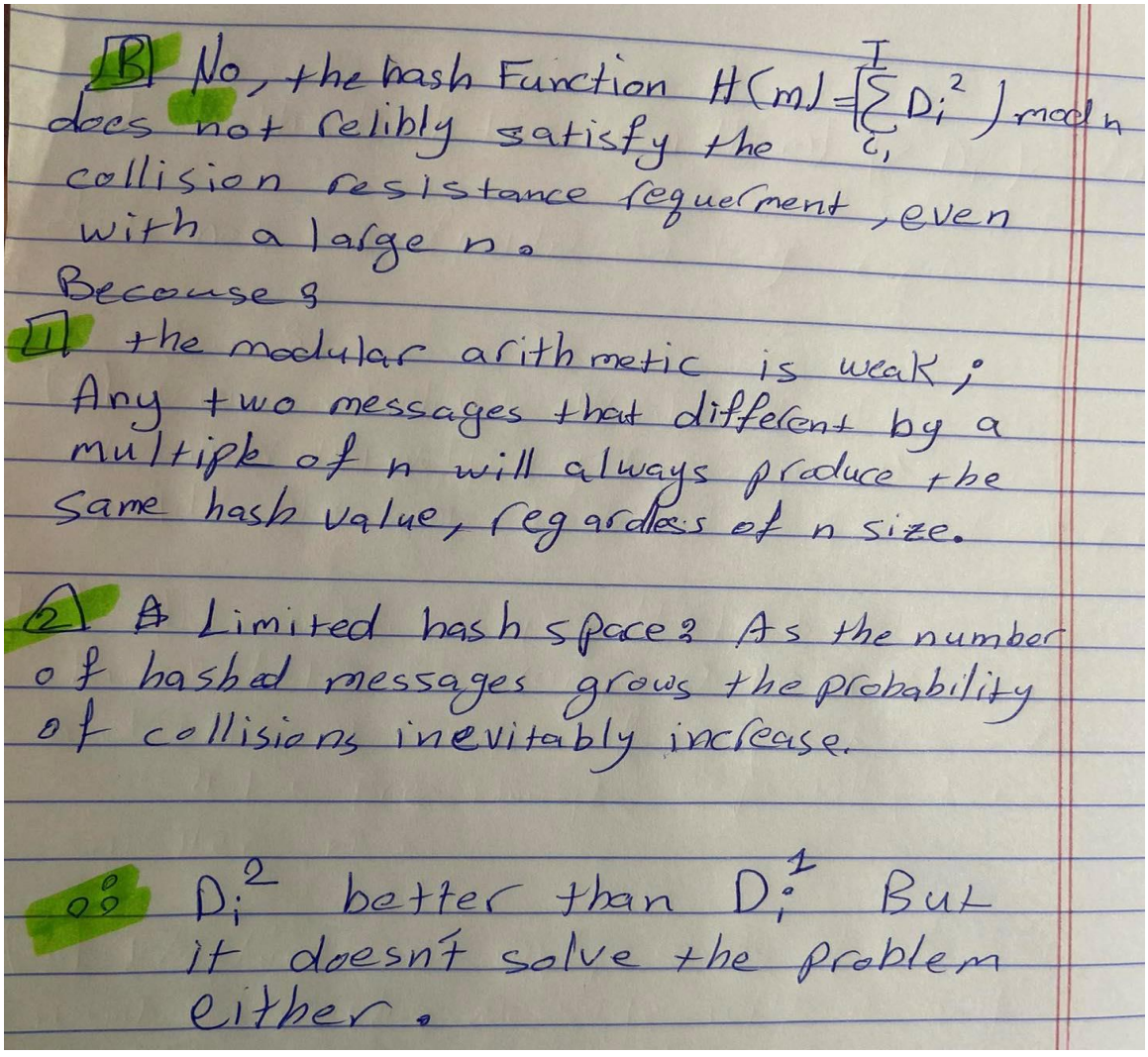


B)

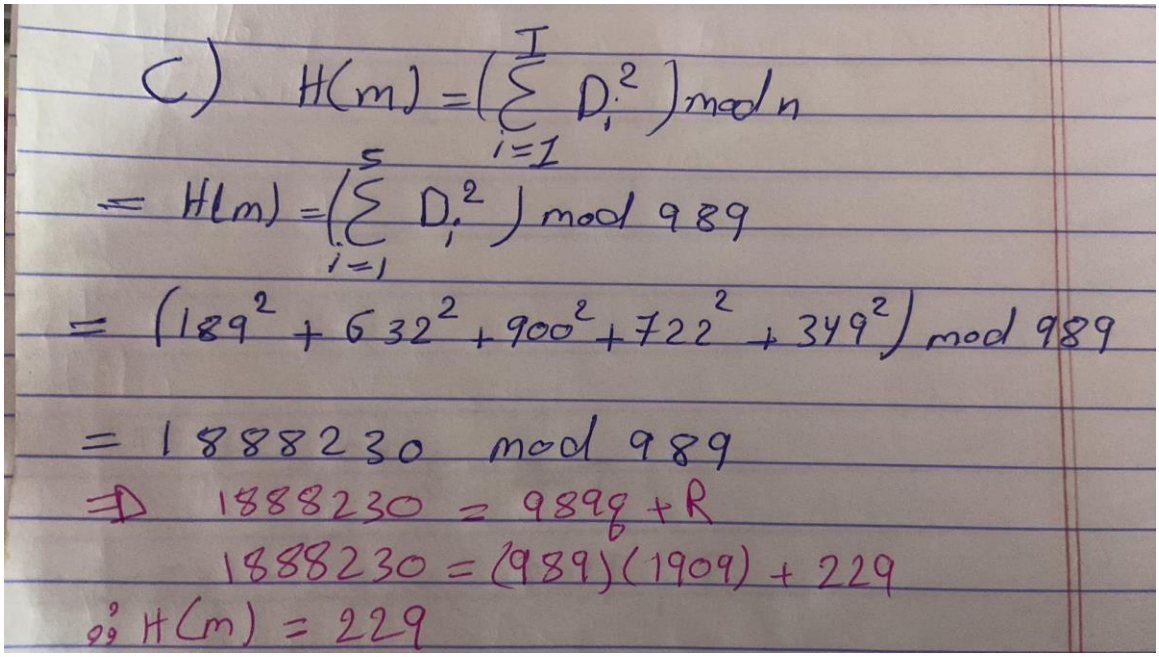
Collision resistance is a property of a hash function that makes it computationally infeasible to find two distinct inputs that produce the same hash value. Collision resistance is crucial in cryptographic applications to prevent adversaries from finding different inputs that map to the same hash value.

$\mathbf{Exp}_H^{cr}(A)$
1. $(X, X') \leftarrow A$
2. **return** $H(X) \stackrel{?}{=} H(X')$ **and** $X \stackrel{?}{\neq} X'$

In this q:



c)


c) $H(m) = \left(\sum_{i=1}^{I} D_i^2\right) \bmod n$
$= H(m) = \left(\sum_{i=1}^{5} D_i^2\right) \bmod 989$
$= (189^2 + 632^2 + 900^2 + 722^2 + 349^2) \bmod 989$
$= 1888230 \bmod 989$
$\Rightarrow 1888230 = 989q + R$
$1888230 = (989)(1909) + 229$
$\therefore H(m) = 229$