জৱাহৰলাল নেহৰু মহাবিদ্যালয়

JAWAHARLAL NEHRU COLLEGE

*A Project Report*

*On*

# *The Concept of Number theory Applied in Cryptography*

*Master of Science*

*In Mathematics*


*Submitted By-*

**Pronali Borah**

**G.U.ROLL NO: PS-221-019-0005**

**G.U.Reg No: 22004369**

**Session: 2023-24**

*Under the Guidance of*

**Ripunjoy Choudhury**

**Department of Mathematics**

**Jawaharlal Nehru College, Boko**

# ACKNOWLEDGEMENT

I would like to express my sincere gratitude to my project guide, Ripunjoy Choudhury, Department of Mathematics, Jawaharlal Nehru College, Boko for his constant support, inspiration, cordial advice and invaluable guidance throughout the course of this project.

I find myself spellbound to acknowledge Dr. Dipankar Sarma, H.O.D. of Department of Mathematics, Jawaharlal Nehru College, Boko for providing the required facilities from the Department and any kind of academic help needed during the course of this project.

I would also like to extend my thankful note to all the Faculty member staff of Department of Mathematics, Jawaharlal Nehru College, Boko and my fellow batchmates. Last but not the least I am indebted to my parents for their support, patience and understanding.

Date: 26/12/2023

Pronali Borah

Pronali Borah

(PS-221-019-0005)


# CERTIFICATE

It is certified that the work contained in this project report entitled "***A Project Report On The Concept of Number theory Applied in Cryptography***" submitted by **Pronali Borah** for the partial fulfillment of the syllabus for 3rd semester for the degree of Master of Science is absolutely based on her own work carried out under my guidance and this report has not been submitted elsewhere for any degree.

.....

**Dr. Dipankar Sarma(H.O.D)**

Department of Mathematics

Jawaharlal Nehru College, Boko

Ripunjoy Choudhury .....25/12/23

**Ripunjoy Choudhury**

Department of Mathematics

Jawaharlal Nehru College, Boko

## Abstract

This project introduces the fundamental concepts of encryption and decryption through a practical implementation of the classic Caesar cipher. The user interacts with the program by entering a plaintext message and a shift value, triggering encryption and subsequent decryption processes. The program employs modular arithmatic to shift the letters, illustrating the reversible nature of the Caesar cipher.

The initiative behind this project is educational, aiming to provide users with hands-on experience in basic crypto-graphic techniques. By engaging with the program, users gain insights into the workings of encryption algorithms and understand the importance of secure communication.

It is crucial to note the program's limitations - specifically the caesar cipher's susceptibility to attacks and emphasize its role as a foundational learning tool. Aspiring programmers and cryptography enthusiasts can utilize this project as a starting point to delve into more sophisticated encryption methods, reinforcing the significance of robust cryptographic protocols in contemporary security landscapes.

Ultimately, this project offers a practical and accessible entry point for individuals seeking to comprehend encryption and decryption principles, paving the way for further exploration into advanced cryptographic algorithms and their applications in securing sensitive information.

## Contents

1.1

## Introduction :-

Number theory is a branch of pure mathematics that explores the properties and relationships of integer or while numbers. It serves as the foundation for many mathematical concepts and has applications in various fields. It delves into topics like prime numbers divi- -sibility, modular arithmetic.

## 1.2 Primes :-

A positive integer 'p' greater than 1 is called prime if the only positive factors of p are 1 and p. A positive integers that is greater than 1 and is not prime is called composite.

### The fundamental theorem of arithmetic :-

Every a positive integer can be written uniquely as the product of primes, where the prime factors are written in order of increasing size.

Example :—

$15 = 3.5$

$48 = 2.2.2.2.3 = 2^4.3$

$49 = 7.7 = 7^2$

$625 = 5.5.5.5 = 5^4$

## 1.3 Least Common Multiples :-

**Definition :-** The least common multiple of the positive integers a and b is the smallest positive integer that is divisible by both a and b. The least common multiple of a and b is denoted by lcm (a,b)

Example - lcm (5,10) = 10

Least common Multiples using prime factorization :-

$$a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}, \quad b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$$

Where $p_1 < p_2 < \dots < p_n$ and $a_i, b_i \in N$ for $1 \le i \le n$

$$\text{lcm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \dots p_n^{\max(a_n,b_n)}$$

Example :- $a = 80 = 2^4 . 5 . 3^0$

$b = 90 = 2 . 3^2 . 5$

$\text{lcm}(a,b) = 2^4 . 3^2 . 5^1 = 720$

## 1.4 Greatest Common Divisors :-

Let a and b be integers not both zero. The largest integer d such that $d|a$ and $d|b$ is called the greatest common divisor of a and b. The greatest common divisor of a and b is denoted by gcd (a,b).

Example :- gcd (48, 72) = 24

Greatest Common Divisors using prime factorization :-

$$a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}, \quad b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$$

Where $p_1 < p_2 < \dots < p_n$ and $a_i, b_i \in N$ for $1 \le i \le n$

$$\gcd(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \dots p_n^{\min(a_n,b_n)}$$

Example :- $a = 60 = 2^2 . 3 . 5$

$b = 54 = 2^1 . 3^3 . 5^0$

$\gcd(a,b) = 2^1 . 3^1 . 5^0 = 6$

## 1.5 Relation between GCD and LCM:-

$a = 60 = 2^2 \cdot 3^1 \cdot 5^1$

$b = 54 = 2^1 \cdot 3^3 \cdot 5^0$

$\gcd(a,b) = 2^1 \cdot 3^1 \cdot 5^0 = 6$

$\text{lcm}(a,b) = 2^2 \cdot 3^3 \cdot 5^1 = 540$

$a.b = \gcd(a,b)\ \text{lcm}(a,b)$

## 1.6 Relatively Prime integers:-

**Definition:** → Two integers a and b are relatively prime if $\gcd(a,b) = 1$

**Example:** →

① 11 and 13 are relatively prime.

② 17 and 19 are relatively prime.

## 1.7 Modular Arithmetic:-

Let a be an integer and m be a positive integer. We denote by a mod m the remainder when a is divided by m.

**Example:-**

$9 \bmod 3 = 0$

$15 \bmod 2 = 1$

2. Cryptography :-

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information it across insecure networks so that it cannot be read by anyone except the intended recipient. Plaintext ciphertext while plaintext encryption decryption. An introduction to cryptography while cryptography is the science of securing data.

In the age of internet, when we use the internet to conduct business transactions, check our bank account, use credit cards to buy things online, and take cash out of an ATM. The danger with modern internet transactions is that you must send private data through a public network in order to reach its destination, such as your bank. The problem with this is that anyone can intercept read the message you have sent.

An internet-based economy therefore required a new kind of security technology in oreder to protect information people send online. Actually, the field of information protection - known as "cryptography" ore "hidden writing".

Illustration:-

The presented C program offers a foundational exploration into the concepts of encryption and decryption through the lens of a simple implementation of the Caesar cipher. This introductory example aims to provide a tangible understanding of cryptographic processes within the context of a classic algorithm.

At its core, the program invites user interactions by prompting them to input a message and a shift value. The message typically a string of characters, serves as the plaintext to be encrypted and subsequently decrypted, while the shift value dictates the magnitude of the letter shift in the Caesar cipher.

The encryption function employs a straightforward logic, iterating through each character of the input message. It applies a modular arithmetic operation to shift the the letters based on the user-provided value. This process transforms the original message into a seemingly random arrangement of characters, forming the encrypted output.

Conversely the decryption function reverses this processes, restoring the original message from the encrypted text. By employing modular arithmetic to revert the letter shifts, the program demonstrate the reversible nature of the Caesar cipher.

It is crucial to recognize the limitations of the Caesare cipher showcased in this example. while it serves as a didactic tool for understanding basic cryptographic principles, the caesare cipher is unsuitable for secure communication due to its vulnerability to various attaks. This program thus serves as a stepping stone for individuals seeking an introductory grasp of encryption and decryption concepts, laying the groundwork for further exploration into the field of Cryptography.

Input 3.2

```c
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

// Function to encrypt the message
void encrypt(char *message, int shift) {
    int i;
    for (i = 0; i < strlen(message); i++) {
        if (message[i] >= 'a' && message[i] <= 'z') {
            message[i] = 'a' + (message[i] - 'a' + shift) % 26;
        } else if (message[i] >= 'A' && message[i] <= 'Z') {
            message[i] = 'A' + (message[i] - 'A' + shift) % 26;
        }
    }
}

// Function to decrypt the message
void decrypt(char *message, int shift) {
    int i;
    for (i = 0; i < strlen(message); i++) {
        if (message[i] >= 'a' && message[i] <= 'z') {
            message[i] = 'a' + (message[i] - 'a' - shift + 26) % 26;
        } else if (message[i] >= 'A' && message[i] <= 'Z') {
            message[i] = 'A' + (message[i] - 'A' - shift + 26) % 26;
        }
    }
}

int main() {
    char message[100];
    int shift;

    // Get the message from the user
    printf("Enter a message: ");
    fgets(message, sizeof(message), stdin);
```

```
36
37          // Get the shift value from the user
38          printf("Enter a shift value: ");
39          scanf("%d", &shift);
40
41          // Encrypt the message
42          encrypt(message, shift);
43          printf("Encrypted message: %s", message);
44
45          // Decrypt the message
46          decrypt(message, shift);
47          printf("Decrypted message: %s", message);
48
49          return 0;
50      }
```

Output 3.3:-

```
Enter a message: This project introduces the concept of encryption
Enter a shift value: 4
Encrypted message: Xlmw tvsnigx mrxvshygiw xli gsrgitx sj irgvctxmsr
Decrypted message: This project introduces the concept of encryption

--------------------------------

Process exited after 31.54 seconds with return value 0
Press any key to continue . . .
```

## Conclusion

In conclusion, this project has served as a practical exploration into the fundamental concepts of encryption and decryption, using the venerable Caesar cipher as a pedagogical tool. By providing users with an interactive experience, allowing them to input messages and observe the effects of encryption and subsequent decryption, the project aimed to demystify the underlying processes of basic of basic cryptographic techniques.

The project has successfully illustrated the reversible nature of the Caesar ciphere, shedding light on the importance of understanding encryption principles for secure communication However, it is crucial to acknowledgement the limitations of cipher in real-world scenarios.

As an educational initiative, this project serves as a stepping stone for individuals interested in cryptography, offering a hands on approach to learning. It encourage users to delve deeper into the intricate world of encryption providing a solid foundation for exploring more advanced algorithms and cryptographic protocols.

In the dynamic landscape of information security, this project emphasizes the need for continuous learning and adaptation. While the caesar cipher provides a historical context for encryption, it serves as a catalyst for aspiri programmers and enthusiasts to explore modern cryptograp methods, ensuring a comprehensive understanding of secure communication practices in today's digital age.