A

Mini project Report

on

“Encryption and Decryption using Caesar Cipher”

By

Pavan Bhonde-04
Prathmesh Tiparkar-65

Under the Guidance of

Prof. Tejal Rane

DEPARTMENT OF COMPUTER ENGINEERING

Shalaka Foundation’s Keystone School of Engineering
Near Handewadi Chowk, Pune- 412308

SAVITRIBAI PHULE PUNE UNIVERSITY

2025-26

A

Mini Project Report

on

“Encryption and Decryption using Caesar Cipher”

Successfully Completed

by

Pavan Bhonde
Prathmesh Tiparkar

DEPARTMENT OF COMPUTER ENGINEERING

Shalaka Foundation’s Keystone School of Engineering
Near Handewadi Chowk, Pune-412308

SAVITRIBAI PHULE PUNE UNIVERSITY

2025-26

Prof. Tejal Rane
Project Guide

Prof. Sagar Rajebhosale
HOD

Shalaka Foundation’s

Keystone School of Engineering

Department of Computer Engineering

Certificate

This is to certify that the Project entitled " Encryption and Decryption using Caesar Cipher" Submitted by Pavan Bhonde and Prathmesh Tiparkar is a record of bonafied work carried out by them, in the partial fulfilment of the requirements for the award of Degree of Bachelor of Engineering (Computer Engineering) at Keystone School of Engineering, Pune under the Savitribai Phule Pune University. This work is done during year 2025-2026.

Prof. Tejal Rane	**Prof. Sagar Rajebhosale**
Guide	HOD
Department of Computer Engineering	Department of Computer Engineering

Dr. Sandeep Kadam

Principal

ACKNOWLEDGEMENT

It takes immense pleasure in presenting the complete Mini-Project report on " Encryption and Decryption using Caesar Cipher". We extend our deepest gratitude to my guide, Prof. Tejal Rane for their unwavering support and guidance. We also wish to thank my Head of Department, Prof. Sagar Rajebhosale, for his invaluable insights. Our heartfelt appreciation goes to Dr. Sandeep Kadam, Principal of my institution, and Prof. Y.R. Soman, Director, for their encouragement and cooperation throughout the Mini-Project. This Mini-Project would not have been possible without the support of my faculty members, dear parents, and friends.

Pavan Bhonde
Prathmesh Tiparkar

ABSTRACT

The project “Encryption and Decryption using Caesar Cipher” focuses on implementing a simple yet fundamental cryptographic algorithm that demonstrates the core concept of data security in computer networks. The Caesar Cipher is one of the earliest and most basic encryption techniques, where each letter in the plaintext is shifted by a fixed number of positions in the alphabet to produce the ciphertext. This project aims to provide a clear understanding of how encryption and decryption processes ensure data confidentiality during communication. The system is implemented using Python, offering an easy-to-understand interface for both encryption and decryption operations. Through this project, users can learn how classical ciphers form the foundation for modern cryptographic algorithms used in secure network communications. The successful implementation of the program validates the working principle of symmetric key encryption and highlights the importance of protecting sensitive information in digital systems.

Keywords:- Caesar Cipher, Encryption, Decryption, Python, Cryptography, Network Security, Symmetric Key, Data Confidentiality.

INDEX

CHAPTER 1

INTRODUCTION

1.1 Introduction

In modern digital communication, securing information is a critical aspect of networked systems. Protecting sensitive data from unauthorized access and ensuring confidentiality are fundamental requirements for any organization or individual exchanging information electronically. To address these requirements, the **Encryption and Decryption using Caesar Cipher** project demonstrates the principles of classical cryptography through a simple, practical implementation.

The project implements a functional encryption-decryption system where plaintext messages are transformed into ciphertext using the Caesar Cipher algorithm, and can be decrypted back to their original form with the correct key. The system is developed using **Python**, providing an interactive and user-friendly platform for performing encryption and decryption operations. By simulating the encoding and decoding processes, this project helps users understand the underlying concepts of **symmetric key cryptography** and the importance of data confidentiality in network communications. It also forms a foundational step toward learning more advanced encryption techniques used in modern network security.

Key Elements of Project

- Implementation of Caesar Cipher in Python –
  The project is developed using Python, which provides a simple and powerful platform to demonstrate the working of classical encryption algorithms.

- Encryption and Decryption Logic –
  The system uses the Caesar Cipher technique, where each letter in the plaintext is shifted by a fixed key value to generate ciphertext. The same key is used in reverse for decryption.

- Symmetric Key Encryption Concept –
  Both encryption and decryption processes use the same key, demonstrating the core idea of symmetric cryptography.

- Handling of Characters and Key Management –
  The program effectively handles uppercase, lowercase, and non-alphabetic characters. It also ensures secure key input and proper management during data transformation.

CHAPTER 2

PROBLEM DEFINITION AND OBJECTIVES

2.1 Problem Definition

The problem is to design a system capable of encrypting and decrypting text using Caesar Cipher logic. The goal is to ensure data confidentiality during transmission by transforming readable text into an encoded form that can only be understood with the correct key.

To design a system capable of encrypting and decrypting text using the Caesar Cipher logic, the process involves substituting each letter in the plaintext with another letter that is a fixed number of positions down or up the alphabet. This fixed number is known as the "shift" or "key." For instance, with a shift of 3, 'A' becomes 'D', 'B' becomes 'E', and so on. The Caesar Cipher is one of the simplest and earliest encryption methods, named after Julius Caesar, who used it to protect his military communications.

The encryption process is straightforward: for each letter in the plaintext, determine its position in the alphabet, apply the shift, and replace it with the corresponding letter. Non-alphabetic characters, such as spaces and punctuation, remain unchanged. Decryption is the reverse process, where the shift is applied in the opposite direction to retrieve the original message.

2.2 Objectives

The main objectives of the project are to:

1. Implement Basic Substitution Encryption –

   Develop a system that substitutes each letter in the plaintext with another letter a fixed number of positions down or up the alphabet, based on a user-defined shift value.

2. Ensure Symmetric Encryption and Decryption -

   Design the system so that the same key is used for both encryption and decryption, ensuring that the original message can be accurately retrieved when the correct key is applied.

3. Handle Non-Alphabetic Characters Appropriately

   Ensure that non-alphabetic characters, such as spaces, punctuation, and numbers, are either preserved in their original form or handled according to the system's design specifications.

4. Provide User-Friendly Interface for Key Input

   Create an intuitive interface that allows users to input the shift value (key) easily, ensuring that both the sender and receiver use the same key for successful encryption and decryption.

5. Educate Users on Cryptographic Concepts

   Incorporate educational elements within the system to explain the principles of substitution ciphers, the importance of key management, and the historical context of the Caesar Cipher, enhancing users' .

CHAPTER 3

METHODOLOGY AND REQUIREMENTS

3.1 Requirement Analysis

The **Requirement Analysis** phase is a critical component of the Software Development Life Cycle (SDLC), focusing on identifying, documenting, and validating the specific needs and expectations of stakeholders for a new or modified product.

A. Hardware Requirements

- Computer/Laptop with Python installed
- Minimum 4GB RAM

B. Software Requirements

- Python 3.x
- Text Editor or IDE (VS Code, PyCharm, etc.)
- OS: Windows/Linux/Mac

3.2 System Design

The project involves implementing a Caesar Cipher algorithm that performs encryption and decryption using modular arithmetic. The logic involves shifting characters by a fixed key value.

Algorithm-

1. Input plaintext and key.
2. Convert characters to ASCII.
3. Shift characters by key value (mod 26 for alphabets).
4. Form ciphertext.
5. Reverse process for decryption.

Code-

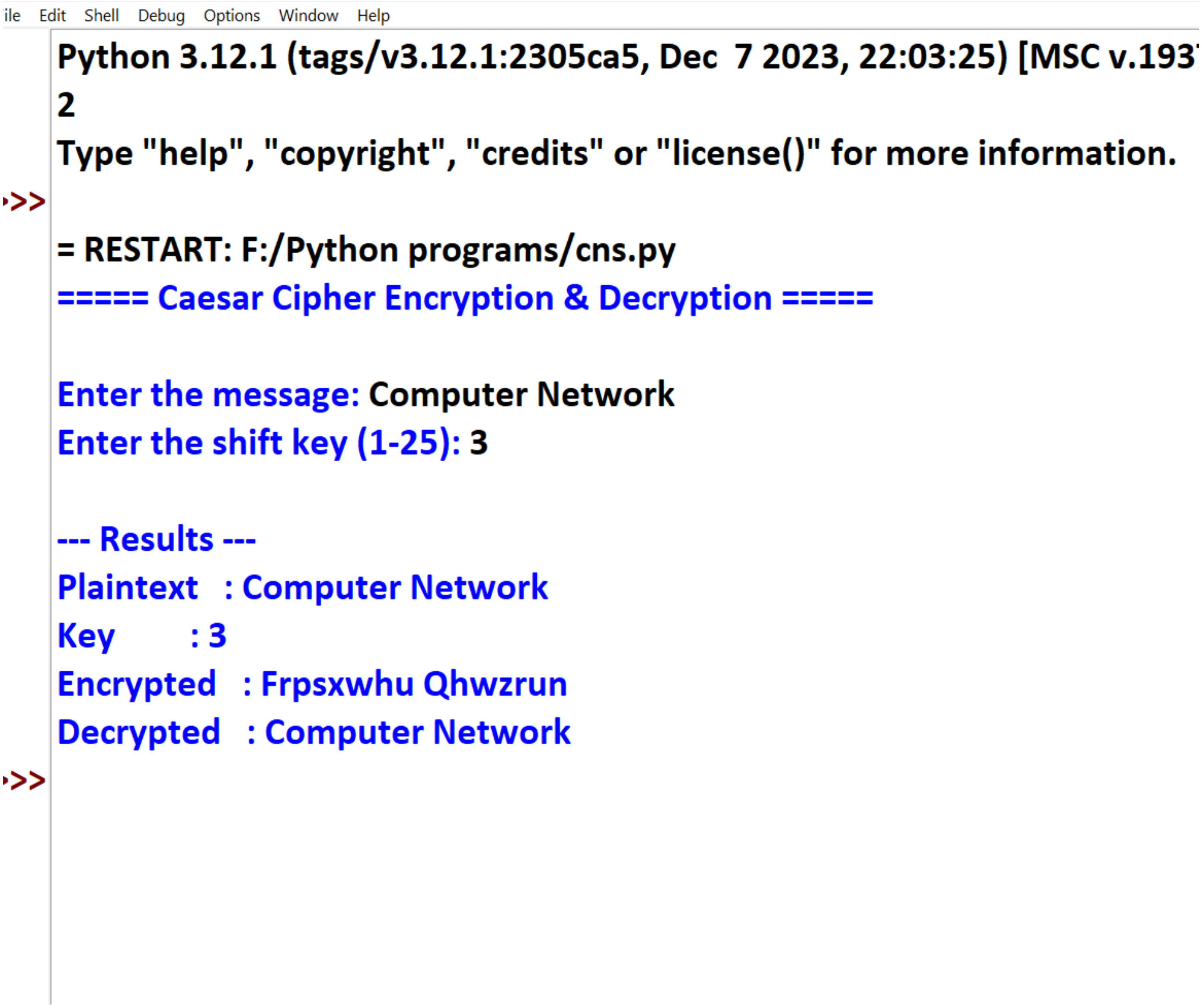
Python Code:

```
def encrypt(text, shift):
    result = ''
    for char in text:
        if char.isalpha():
            start = ord('A') if char.isupper() else ord('a')
            result += chr((ord(char) - start + shift) % 26 + start)
        else:
            result += char
    return result

def decrypt(text, shift):
    return encrypt(text, -shift)

plain_text = 'HELLO WORLD'
key = 3
cipher_text = encrypt(plain_text, key)
print('Encrypted:', cipher_text)
print('Decrypted:', decrypt(cipher_text, key))
```

CHAPTER 4

RESULT AND OUTPUT

Output(Screenshot):



```
Python 3.12.1 (tags/v3.12.1:2305ca5, Dec  7 2023, 22:03:25) [MSC v.193
2
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: F:/Python programs/cns.py
===== Caesar Cipher Encryption & Decryption =====

Enter the message: Computer Network
Enter the shift key (1-25): 3

--- Results ---
Plaintext   : Computer Network
Key         : 3
Encrypted   : Frpsxwhu Qhwzrun
Decrypted   : Computer Network
>>>
```

CONCLUSION

The Caesar Cipher stands as one of the earliest and simplest encryption techniques, dating back to Julius Caesar's era. Its fundamental approach involves shifting letters of the plaintext by a fixed number, making it a straightforward example of substitution cipher logic. This simplicity has made it an invaluable educational tool, helping learners grasp the basic principles of cryptography and the importance of key-based encryption.While not suitable for securing sensitive communications today, the Caesar Cipher remains relevant in various domains. It's employed in puzzles, games, and as a stepping stone for understanding more complex encryption algorithms. Additionally, its principles are often integrated into hybrid encryption methods, enhancing data security in specific applications.

In conclusion, the Caesar Cipher exemplifies the balance between simplicity and security. Its enduring presence in cryptographic education and its influence on subsequent encryption methods underscore its lasting impact on the field of information security.

REFERENCES

1. William Stallings – Cryptography and Network Security, Pearson.
2. Behrouz A. Forouzan – Data Communications and Networking, McGraw-Hill.
3. Charles Pfleeger – Security in Computing, Pearson.
4. Bruce Schneier – Applied Cryptography, Wiley.
5. TutorialsPoint – Python Cryptography Basics.
6. GeeksforGeeks – Caesar Cipher Implementation in Python.
7. NPTEL – Network Security and Cryptography course material.
8. Cryptography and Network Security Research Papers – IEEE Xplore.