Bit Lords

**Caesar Cipher**

Version 1.0

**Software Requirements Specification:**

1. Windows 10
2. Python 3.6
3. 2GB RAM

**Project Guide: Ms. Pronika Chawla**

**Members:** 1. Shubh Gaur

2. Harsh Vardhan

3. Shivam Sharma

4. Madhusudhan Mishra

College Name: Manav Rachna International Institute of Research and Studies

Department: Faculty of Engineering and Technology

Table of Contents

1. Introduction 3

1.1 Purpose 3

1.2 Scope 3

1.3 Definitions, Acronyms and Abbreviations 3

1.4 References .

1.5 Technologies to be used .

1.6 Overview .

2. Overall Description .

2.1 Use-Case Model Survey .

2.1 Block Diagram .

2.2 File System Architecture Diagram .

3. Specific Requirements .

3.1 Workflow Diagram .

3.2 Class Diagram .

3.2 Supplementary Requirements .

1. Introduction

## Purpose

## One of the objectives of our project is to come up with a solution to overcome the limitations of the three encryption techniques used in the project and modify their working to enforce them.

## The main purpose of our project is to protect digital data confidentiality using three layered hybrid encryptions implemented by combining three of the popular techniques namely Caesar cipher, Vigenère cipher and Playfair cipher.

## Scope

This tool will secure computer and information technology systemsdata by encrypting it. As cyberattacks are increasing day by day on an exponential rate, this tool will help in mitigating the possible vulnerabilities of data by hiding the original information which will be of use in the case of information leakage (through a cyber-attack or system malfunction) so that the real meaning behind the data could not be identified, which will help in preventing the wrongful use of data.

## Definitions, Acronyms and Abbreviation

**ISPA** – Installable Single Package Architecture.

**CT** – Cipher Text.

**PT** – Plain Text.

**SEC** – Secret Message

**Encryption** – Encryption is the process of converting normal message (plaintext) into meaningless message (Ciphertext).

**Decryption** – Decryption is the process of converting meaningless message (Ciphertext) into its original form (Plaintext).

## References

* Han F et al (2014) A general transformation from KP-ABE to searchable encryption. Future Gener Comput Syst 30:107–115
* Rachmawati Dian and Candra Ade 2015 Implementation of the combination of Caesar Cipher and Affine Cipher for text data security *Informatics Research and Education Journal (JEPIN)*
* Ariyus D. 2008 *Introduction to Cryptography: Theory, analysis and implementation* (Yogyakarta: Andi)
* Basuki, Paranita and Hidayat 2016 Design of Layered Cryptography Applications Using Caesar Algorithms, Transpositions, Vigenere and Block Cipers Based on Mobile *National Seminar on Information and Multimedia Technology. STMIK AMIKOM* *(Yogyakarta,)*
* Bellare, M., Desai, A., Jokipii, E., Rogaway, P.: A concrete security treatment of symmetric encryption: analysis of the DES modes of operation. In: Proceedings of the 38th Symposium on Foundations of Computer Science. IEEE (1997)
* K. Senthil, K. Prasanthi and R. Rajaram, "A modern avatar of Julius Caesar and Vigenere cipher", *Computational Intelligence and Computing Research (ICCIC) 2013 IEEE International Conference*, pp. 1-3, 2013.
* Champakamala B.S, Padmini K and Radhika D.K 2014 Least Significant Bit Algorithm for Steganography *Int. J. of Advance Computer Technology*
* Emam, Marwa M, Aly Abdelmgeid A and Omara Fatma A 2016 An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection *Int.l J. of Advanced Computer Science and Applications* **7** 17-22
* Inan, Y. (2019). Analyzing the Classic Caesar Method Cryptography. 4th International Conference on Computational Mathematics and Engineering Sciences(pp. 213-220)
* Monika,A.,& Pradeep,M. (2012). A Comparative Survey on Symmetric Key Encryption Techniques.International Journal on Computer Science and Engineering (IJCSE), 877-882.
* Senthil, K.,et al. (2013). A modern avatar of Julius Caesar and Vigenere cipher. IEEE International Conference.Computational Intelligence and Computing Research (ICCIC)
* Verma, O.P et al. (2011). Performance Analysis Of Data Encryption Algorithms. IEEE.Delhi Technological University India
* Atish,J.,et al.(2015).Enhancing the Security of Caesar Cipher Substitution Method using a Randomized Approach for more Secure Communication. International Journal of Computer Applications, 129(13),6-11.DOI: 10.5120/ijca201590706
* Sahai A, Waters B (2005) Fuzzy identity-based encryption. In: Annual international conference on the theory and applications of cryptographic techniques. Springer, Berlin, Heidelberg

## Technologies to be used

# Application Architecture - ISPA

# Development tool - VSCode, Jupyter Notebooks

# Designing tool - Tkinter

# Libraries Used - Cryptography,Numpy ,Sys,

# Tkinter, Pygame

## Overview

In our project, we have integrated three encryption algorithms together to generate a hybrid cipher which will not be easy to crack because not only we are integrating the three algorithms but also modifying the working of two encryption algorithms used and using the third encryption as it is in our hybrid cipher.

# Overall Description

## Use-Case Model Survey

Diagram

Description automatically generated

1. Sender: - is responsible for sending the message to the sending module for encryption and encoding.
   1. **Fetch Message Module: -** works as an input module for the project to fetch message from the sender for further processing.
   2. **Encryption Module-** Responsible for encrypting the message with the mentioned technique for safe transmission.
   3. **Encoding Module**: - Responsible for encoding the message so that it is easily accommodated in the medium.
2. Receiver-: responsible for receiving the decoded message after processing by the receiver side module.
   1. **Decoding Module**: - Responsible for catching the encoded message from the channel and decoding it to computer language for further processing.
   2. **Decryption Module: -** Responsible for decryption of the message with the appropriate key provided to the receiver through the sender
   3. **Deliver Message Module: -** delivers the message to the sender after applying checksums to verify for alterations in the original message.

## Block Diagram

**Encryption**

**Diagram

Description automatically generated**

**Decryption**

**Diagram

Description automatically generated**

## File System Architecture Diagram

Caesar Cipher Project/

│

├── Caesar Cipher/

│ ├── \_\_init\_\_.py

│ ├── source.py

│ └── helpers.py

| └──encryption.py

| └──decryption.py

│

├── tests/

│ ├── project\_test1.py

│ └── project\_test2.py

│

├──. gitignore

├── LICENSE

├── README.md

├── requirements.txt

└── setup.py

# Specific Requirements

## Workflow Diagram

**Sender’s Side Receiver’s Side**

A sender wants to send a message.

The application is initiated

The sender enters the message in the application, along with the key

The application encrypts the message first then encodes it and send it via LAN to the receiver.

Decoder receives the encoded message

The application’s decoding module decodes it after running checksum.

Decryption module decrypts the message with appropriate key.

The decrypted message is presented to the receiver in the proper format

## Class Diagram (UML)

Diagram

Description automatically generated

## Supplementary Requirements

* This tool can be run on any modern operating systems viz. Windows, Linux, RedHat CentOS etc.
* The users using this and accessing its methods from this tool should have supporting software and necessary libraries to run them.
* To use the application in the best possible way please read the tips displayed while using the tool.