

Message Encode Decode using Tkinter

Archana.CV

Computer Science and engineering(Cyber security),
Nehru college of engineering and research centre,
Kerala,India
archanacvcv@gmail.com

Betsy Joy

Computer Science and engineering(Cyber security),
Nehru college of engineering and research centre,
Kerala,India
betsy.lija@gmail.com

Abstract: This article showcases the encode and decode operations on a secure login page, all while maintaining a basic yet reliable website. Using cryptographic techniques, the main objective is to put information security measures into practice in a practical manner. Python provides a variety of GUI (Graphical User Interface) development possibilities. It is a typical Python interface to the Python-shipped Tk GUI toolkit. Python combined with Tkinter provides the quickest and most straightforward method for developing GUI apps. The Tkinter toolkit for creating GUI apps is provided by Python. This programme would encrypt messages using a key and decrypt hashes using the same key.

Keywords: *Vigenere cypher, Tkinter-Python*

I. INTRODUCTION

The purpose of this paper is to design a secure login page for a basic yet reliable website that also demonstrates encode and decode procedures. The main objective is to employ cryptographic techniques to implement a practical demonstration of information security measures. The project functions as a teaching aid, demonstrating how cryptographic techniques improve web application security. Python provides a variety of GUI (Graphical User Interface) development possibilities.

An example of such a project's structure is shown below: Within this framework: 'encodedecode.py' is the primary Python script that includes the logic for encoding and decoding messages, as well as the code for the TkinterGUI programme. - "README.md": This file usually contains pertinent project information, dependencies that must be installed, and usage instructions for the application. 'assets/': Any additional resources needed by the application, including GUI icons or graphics, may be found in this directory. The structure is simple because the project is focused on a single functionality and is somewhat modest. Upon completion of this project, participants will have acquired significant knowledge on the real-world application of encryption techniques to improve web application security.

II. LITERATURE SURVEY

A literature review would also involve investigating existing literature related to the Vigenère Cypher, encryption techniques, and any pertinent studies or resources on encryption techniques, graphical user interface (GUI) development, and Python programming. Knowledge of the Vigenère Cypher: This is a basic technique for encrypting messages using the alphabet. reviewing the literature on the Vignere Cipher's shortcomings, principles, and historical background. looking for sites that cover cryptographic principles, encryption methods, and the application of historical cyphers to contemporary cryptography. Studying the literature on encoding and decoding techniques, especially as they relate to cryptography, is the task at hand. reviewing books, articles, and tutorials that cover secure communication encoding and decoding techniques. Recognising the difficulties and factors to be taken into account while putting encoding and decoding functionalities into practice, such as error management, efficiency, and security. In today's digital environment, common cyber threats like credential stuffing, phishing, and password cracking pose serious risks to people, organisations, and systems. The act of obtaining passwords without authorization through methods such as dictionary attacks, rainbow table assaults, and brute force attacks is known as password cracking. Phishing is a type of social engineering assault where the goal is to fool victims into divulging private information like passwords, usernames, and bank account information.

Encryption methods encode data in a secure manner that can only be decoded by authorised individuals, so safeguarding its integrity throughout transmission between clients and servers. As a result, there is less chance of unapproved changes and data tampering. Additionally, encryption protects user privacy by guaranteeing that private user information is kept secret and shielded from unwanted disclosure. Hashing and salting are two strong encryption techniques that can help reduce credential-based attacks. Organisations can mitigate the likelihood of password compromise and unauthorised access by implementing security measures such as rate restriction and password complexity requirements, in addition to securely storing hashed passwords. Python Programming: Examining Python programming literature, including materials on software engineering concepts, cryptography, and GUI development.

III. SYSTEM REQUIREMENTS

Software Requirements

1. Latest version of Tkinter

The Python GUI (Graphical User Interface) library is called Tkinter. You probably won't need to install it separately because it comes installed with most

Python systems. On the other hand, pip: pip install tk can be used to install it if necessary.

2. Visual Studio Code

Microsoft created Visual Studio Code (VS Code), a free source code editor for Windows, Linux, and macOS. Because of its versatility, ease of use, and vast ecosystem of extensions, it has swiftly emerged as one of the most well-liked options for developers working with a variety of programming languages. The user interface of VS Code is clear and simple to use, with the goal of increasing productivity. To accommodate different tastes, it provides keyboard shortcuts, themes, and layouts that may be customised.

3. Tkinter

Python's main GUI toolkit, tkinter, is another implicit module. It is heavily utilised in the project to create the graphical user interface, which includes widgets like buttons, labels, and entry fields.

4. Encode Decode py

It includes the application logic, such as the event handling functions, the GUI setup using Tkinter widgets, and the Base64 encoding and decoding logic for messages. Here are the main elements of this module: GUI Configuration: This module's portion initialises the Tkinter application window and generates the buttons, labels, and entry fields required for the user interface. Event Handlers: The purpose of event handling routines is to react to user input, like button clicks. For instance, an event handler is called to encode the message entered by the user when the "Encode" button is clicked. Encoding and Decoding Logic: These functions use the Base64 encoding technique to accomplish the actual encoding and decoding of messages.



Fig. 1 Encrypt Window

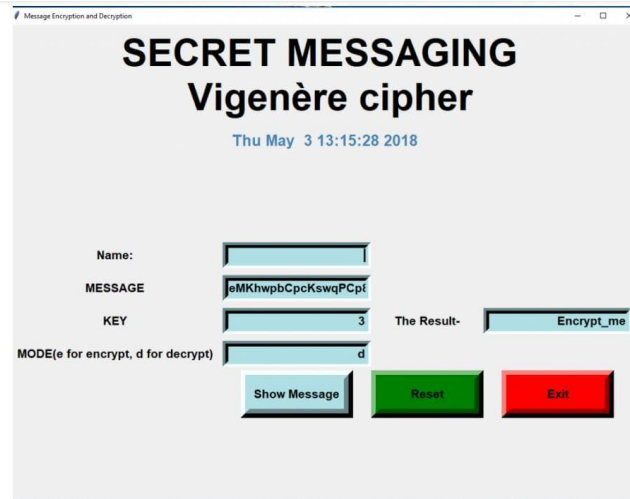


Fig. 2 Decrypt Window

IV. PROPOSED SYSTEM

The general idea behind "Message Encode-Decode using Tkinter and Vigenère Cypher" is to utilise the Python GUI package Tkinter to create a graphical user interface (GUI) application that can encode and decode messages using the Vigenère Cypher encryption technology. The following essential elements could be included in the project: GUI Development: Creating an intuitive Tkinter interface that lets users submit messages, choose between encryption and decryption modes, input a key, and see the result. Vigenère Cypher Implementation: Encoding and decoding messages using the Vigenère Cypher algorithm. To do this, one must comprehend the encryption and decryption procedures used by the polyalphabetic substitution cypher known as the Vigenère Cypher. Combining the Tkinter GUI's implementation of the Vigenère Cypher with it, enabling users to quickly and simply encrypt and decrypt messages using the GUI. Using error-handling mechanisms to deal with faulty inputs, such as invalid keys or empty message fields, is known as error handling.

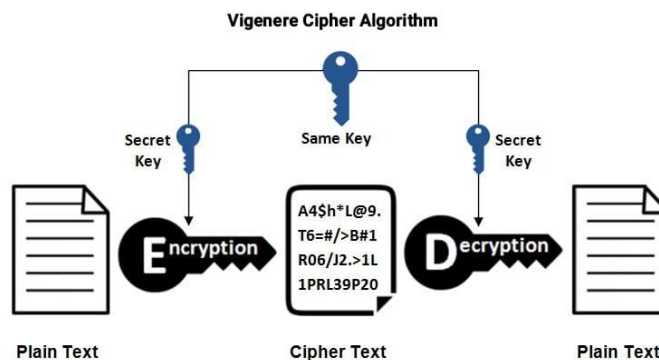


Fig. 3 Architecture Diagram

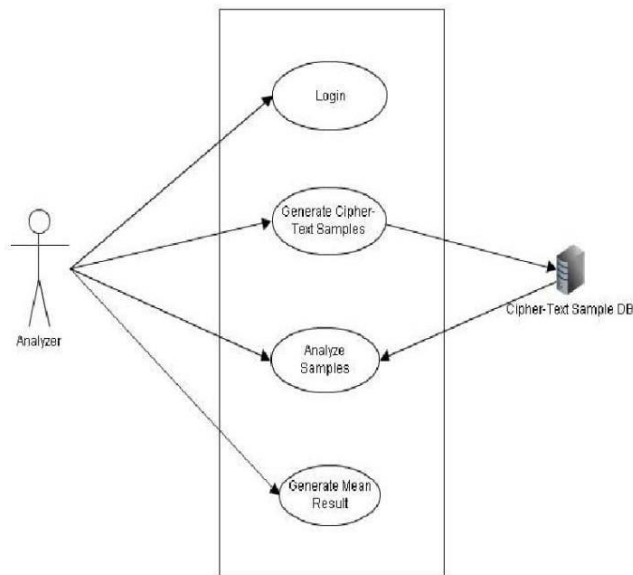


Fig. 4 Use Case Diagram.

V. CONCLUSION

This works well for password encryption in the sign-up and login page with appropriate validation. Every function activity that a user does is completed with sweet alert messages. Appropriate block messages are included to stop the intrusive party's actions, even if they attempt to modify the content via inspect element mechanisms. Therefore, guaranteeing more safety for the user's identity and details. The page's responsiveness shouldn't be compromised in order to make it more user-friendly. Passwords are successfully encrypted and kept in a database. Every time a user logs in, their password needs to match the one in the database in order for them to be the only ones able to access the page; if not, their entry will be blocked right away.

REFERENCES

- [1]. Javier Andres Bargas-Avila, Online Form Validation: Don't Show Errors Right Away. Human
- [2]. Ako Muhammad Abdullah, Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data, Article · June 2011
- [3]. Katha Chanda, Password Security: An Analysis of Password Strengths and Vulnerabilities, July 2016
- [4]. Comparison of Vigenere Cipher and Affine Cipher in Three-pass Protocol for Securing Image, Rahma Isnaini Masya
- [5]. Improve Security Algorithm Cryptography Vigenere Cipher Using Chaos Functions, Budi Triandi; Evri Ekadiansyah
- [6]. Cryptanalysis of Vigenère Cipher: Method Implementation, Aiman Al-Sabaawi
- [7]. Multi character frequency based encoding for efficient text messaging in Indian Languages, Manu Seth