A Project Report

On

**“SecurePass Manager:**

**Password Strength and Encryption Toolkit”**

**Submitted by**

**Shivansh Mittal , 2315002088**

**Rishav Kumar , 2315001838**

**Satyam Dubey , 2315002002**

**Sita Ram Sharma , 2315002169**

**Sameer Kumar , 2315001950**

**Pranjal Gupta , 2315001626**

**Supervisor**

Mr. Asheesh Tiwari

Assistant Professor

**Department of Computer Science & Applications**

**Institute of Engineering & Technology**



**GLA University, Mathura - 281406**



**DECLARATION**

We ***Shivansh Mittal, Btech-CSE 1st Year, 2315002088, Satyam Dubey, Btech-CSE 1 Year, 2315002002, Rishav Kumar, Btech-CSE 1 Year, 2315001838, Sita Ram Sharma, Btech-CSE I Year, 2315002169, Sameer Kumar, Btech-CSE 1st Year, 2315001950, Pranjal Gupta, Btech-CSE 1 Year, 2315001626*** hereby declare that the work presented in this project report entitled “SecurePass Manager: Password Strength and Encryption Toolkit” is an authentic record of our own work carried out under supervision of Mr. Asheesh Tiwari,Assistant Professor.

Shivansh Mittal , 2315002088 Rishav Kumar , 2315001838

Satyam Dubey , 2315002002 Sita Ram Sharma , 2315002169

Sameer Kumar , 2315001950 Pranjal Gupta , 2315001626

**CERTIFICATE**

This is to certify that the above statement made by the students are correct to the best of my knowledge and belief.

Date:14/02/2023

Place: Mathura

Mr. Asheesh Tiwari , Assistant Professor,

Signature :



**Contents**

|  |  |  |
| --- | --- | --- |
| Certificate & Declaration | | ii |
|  |
| Table of Contents | | iii |
| 1. **Introduction, Motivation and Objective** | | **<Page No.>** |
| 1. **Project Description and Work done** | | **<Page No.>** |
| 1. **Geotagged Images of Students at the place of work** | | **<Page No.>** |
| 1. **Findings and Conclusion** | | **<Page No.>** |
| Bibliography/ References | | <Page No.> |



**Chapter - 1**

**Introduction:** In the ever-expanding digital landscape, the prevalence of online activities underscores the critical importance of robust cybersecurity practices. A fundamental aspect of digital security revolves around the management of passwords, the gatekeepers to personal and sensitive information. The Password Management Tool project emerges as a response to the escalating need for sophisticated tools that not only assess and fortify password strength but also provide secure methods for password generation and encryption.

**Motivation:** The motivation behind embarking on the Password Management Tool project stems from the realization that traditional password management practices often fall short in the face of evolving cyber threats. As cybercriminals employ increasingly sophisticated methods, there is a growing urgency to empower users with tools that can adapt and strengthen their defense mechanisms. By developing a comprehensive Password Management Tool, we aim to bridge existing gaps in password security and empower users with a versatile solution that aligns with contemporary digital security standards.

**Objective:**

1) Evaluate and Enhance Password Strength

The tool seeks to provide users with a reliable and accurate Password Strength Checker. By employing advanced algorithms, the tool assesses various parameters, including length, character diversity, and complexity, to deliver precise evaluations of password strength. The objective is to empower users with insights into the robustness of their passwords, fostering a culture of informed password management.

2) Facilitate Secure Password Generation

Recognizing the challenges users face in creating strong yet memorable passwords, the project incorporates a Secure Password Generation feature. This feature aims to simplify the process of generating secure passwords, ensuring randomness and complexity while reducing the cognitive burden on users. The objective is to promote the adoption of secure password practices by offering a user-friendly and efficient password generation mechanism.

3) Implement Advanced Encryption Techniques

Acknowledging the significance of encrypting sensitive information, the project integrates both additive and multiplicative cipher techniques. These encryption options provide users with a choice in securing their passwords and personal data. The objective is to add robust security layers to the password management process, enhancing the overall resilience of the tool against potential security threats.By achieving these objectives, the Password Management Tool endeavors to contribute to a more secure digital environment, where users can navigate the online landscape with confidence, knowing that their sensitive information is well-protect



**Chapter-2**

**Project Description:** The Password Management Tool project is a comprehensive software solution designed to address the evolving challenges associated with password management in the digital era. Recognizing the critical role passwords play in securing personal and sensitive information, the project aims to provide users with a suite of functionalities that go beyond traditional password management practices.

**Work Done:**

The development process followed a systematic approach, encompassing various phases:

1) Requirement Analysis : The project initiation involved a thorough analysis of user requirements. Understanding the expectations, security concerns, and industry best practices laid the foundation for the subsequent development phases.

2) Design and Architecture : A robust and scalable architectural design was crafted, outlining the flow of functionalities and algorithms. Considerations for modularity, scalability, and user-friendliness were paramount in this phase.

3) Implementation : The implementation phase translated the design into functional code using Python. Emphasis was placed on maintaining code modularity, following best coding practices, and ensuring scalability to accommodate future enhancements.

4) User Interface Design : User interface considerations were integral to the project's success. A user-friendly interface was designed, featuring intuitive menus and navigation options to enhance the overall user experience.

5) Testing : Rigorous testing procedures were implemented to validate the correctness, reliability, and security of the Password Management Tool. Various testing phases, including unit testing, integration testing, and user acceptance testing, were conducted to ensure a robust and error-free application. The culmination of these efforts resulted in the creation of the Password Management Tool—an effective, user-friendly, and secure solution for password management in the digital landscape. The project's success is attributed to the collaborative efforts of the project team, drawing on the expertise of team members, insights from seniors, and valuable input from external resources.

**Chapter - 3**

**Geotagged Images of Students at the place of work**

|  |  |
| --- | --- |
| **Geotagged Image 1** | **Geotagged Image 2** |
| **Geotagged Image 3** | **Geotagged Image 4** |



**Chapter - 4**

### Findings: 1) Password Strength Checker Accuracy

The evaluation of the Password Strength Checker revealed its consistent and accurate assessment of password strength. Users benefitted from precise feedback, allowing them to make informed decisions about the robustness of their passwords.

#### 2) Secure Password Generation Effectiveness

The Secure Password Generation feature consistently delivered on its objective of creating strong and secure passwords. Users found the generated passwords to be both complex and memorable, reducing the challenges associated with password creation.

#### 3) Encryption Techniques Security

Both additive and multiplicative cipher techniques were found to add significant security layers to the password management process. Users appreciated the flexibility to choose encryption options based on their preferences, contributing to a more personalized and secure experience.

**Conclusion:** The Password Management Tool project has successfully achieved its objectives, contributing to the enhancement of password security in the digital landscape. The findings from the evaluation phase underscore the effectiveness and reliability of the tool's key features.

#### 1) User Empowerment : The tool empowers users by providing them with accurate insights into password strength, enabling them to make informed decisions about the security of their passwords.

#### 2) Robust Security Measures : The inclusion of encryption techniques—additive and multiplicative ciphers—adds robust security layers to the password management process, safeguarding sensitive data from potential threats.

#### 3) Ease of Use : The user-friendly interface ensures ease of navigation and interaction, making the Password Management Tool accessible and practical for users of varying technical backgrounds.

In conclusion, the Password Management Tool stands as a reliable and efficient solution for addressing the evolving challenges of password security. Its findings highlight its effectiveness in providing users with secure and user-friendly options for managing their passwords in the digital landscape. As technology continues to advance, the Password management Tool is positioned to adapt and evolve, ensuring users stay at the forefront of password security practices.



**Bibliography/ References**

***For making this project, we took help of:***

***Our Seniors and friends,***

***OpenAl. (2023). ChatGPT Documentation.***

***Smith, J. (2020). Secure Coding Practices in Python. Tech Publishing.***

***Python Software Foundation. (2021). Python Documentation. https://docs.python.org/3/***