***Ottendorf Password Encryption***

**AN EXPERIENTIAL LEARNING PROJECT REPORT**

**Submitted in partial fulfilment of the**

**requirement for the award of the degree**

**of**

**BACHELOR OF TECHNOLOGY (B.Tech)**

in

Computer Science and Engineering

by

**Zain Abbas Kazimi**

**199301240**

Under the guidance of

**Manoj Sir**



**Department of Computer Science and Engineering**

**School of Computing and Information Technology**

**Manipal University Jaipur**

**Jaipur, Rajasthan**

**June 2020**

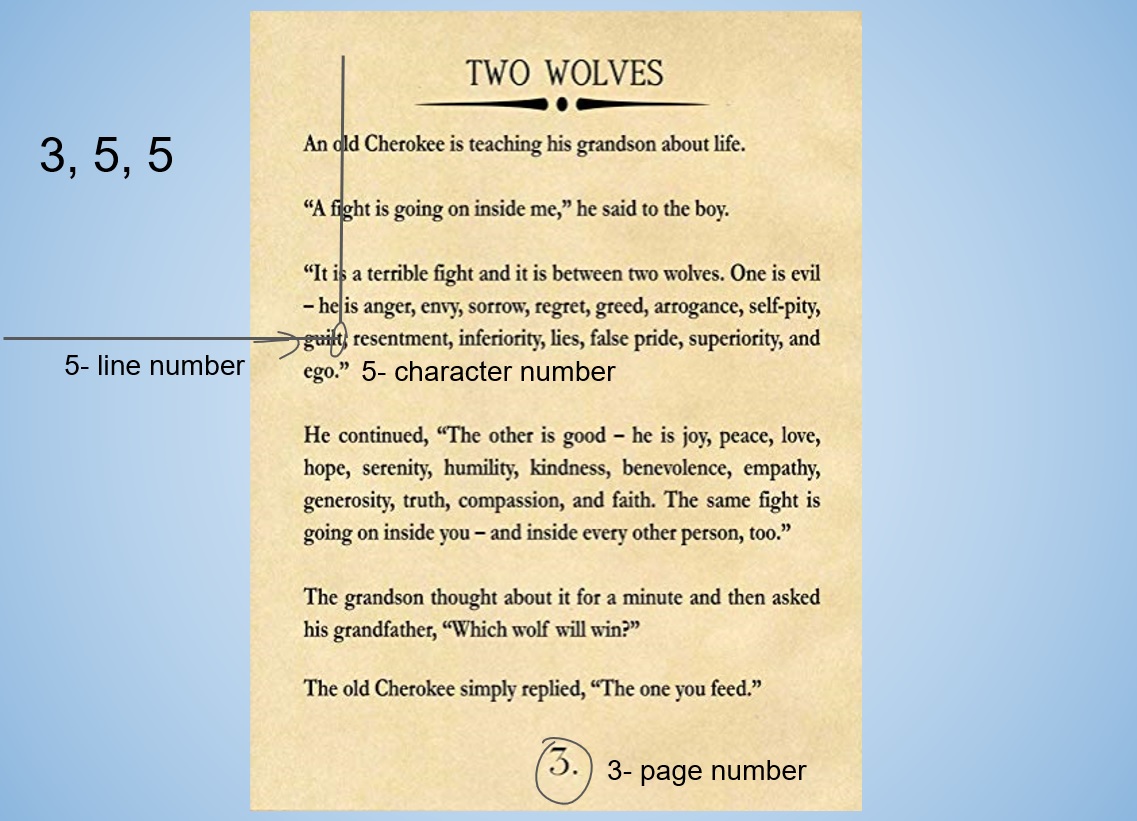
**Table of Contents**

1. Introduction
2. Statement of Problem
3. Motivation and Objectives
4. System Design/Architectural Diagram/Flowchart
5. Methodology of Work
6. Key Learnings / Results / Implementation
7. Conclusion
8. Bibliography / References

Introduction

Our project focuses on making staying cyber secure easier for everyone. Through an innovative application of a centuries old technique, our service allows you to create and store complex passwords in the form of a number series corresponding to the pages in a particular book in such a manner that only you can access them.

An ottendorf cipher is a method of storing individual letters in a phrase as a set of 3 numbers corresponding to the page number, line number, and character number in a particular book. In this manner a password of ‘n’ characters can be stored in a number series of n\*3 numbers.



In this example, the set of numbers (3 5 5) gives us the letter ‘t’ for our password

A number series such as: 3 4 6. 12 6 8. 4 12 5. 16 5 8. 12 6 12. 13 6 19. could give us a password of ‘EL2020’ when referenced with respect to the Agatha Christie novel ‘A mysterious affair at styles’, but would be meaningless when referenced with any other book.

And as such, even with the number key, only the user who would know which book he chose to pair it with.

Statement of Problem

In a world where all of our personal details are stored online, protected behind accounts and passwords, it is extremely important to make long and secure passwords. However, out of laziness, most people just end up using the most simple and predictable keywords such as their name or birthday, out of fear of forgetting the password.

The problem of using multiple passwords and having to store them is another where people feel uncomfortable storing their passwords in an easy to access place, as it would become just as easy for someone else to access it as well.

Objectives

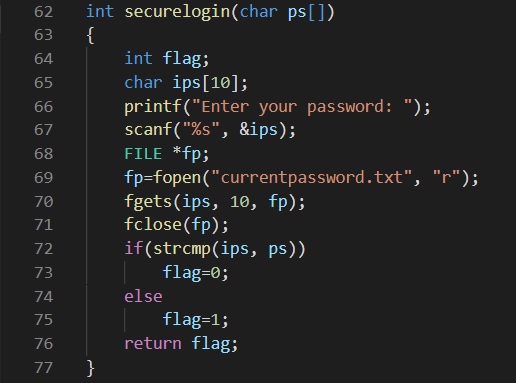
To solve this problem, we sought out a solution that allows the user to store their passwords in an easy to access location, such as their wallet, without the risk of someone else stumbling upon it as only the user can make sense of the number series written on the card.

This service is best used as a backup system to reassure the user that they have a reliable and convenient way of recovering their passwords at a moment’s notice.

System Design

The program is divided into distinct modules that perform certain tasks:

1. Secure login:



This module asks the user for the current password they have set. It stores the currently saved password in a text file and accesses it to check it against the user’s input.

Once it successfully matches the user’s input against the saved password, it moves on to show the menu containing the other features of the program.

After 3 failed attempts, it throws the user out of the program.

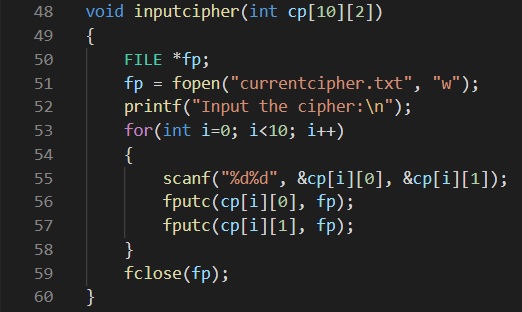
2. Fetching password:



This module takes the argument of the number series and book, and matches the numbers to the corresponding characters in the book, to return us the password.

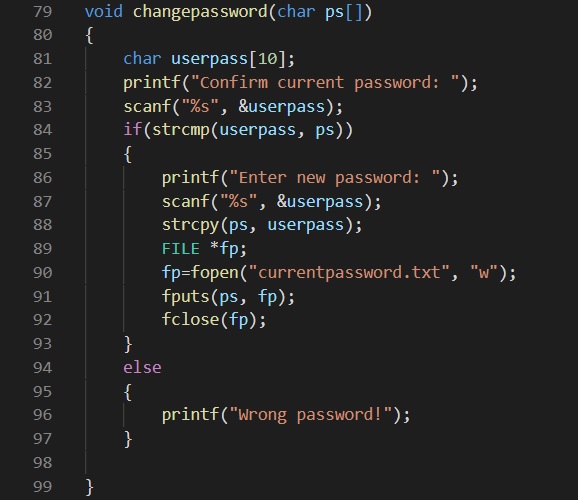
It accesses the book in the form of a text file, which has been formatted to allow the program to distinguish between lines and pages.

3. Input cipher:



This module allows the user to change the number series for their secure passwords.

4. Change password:



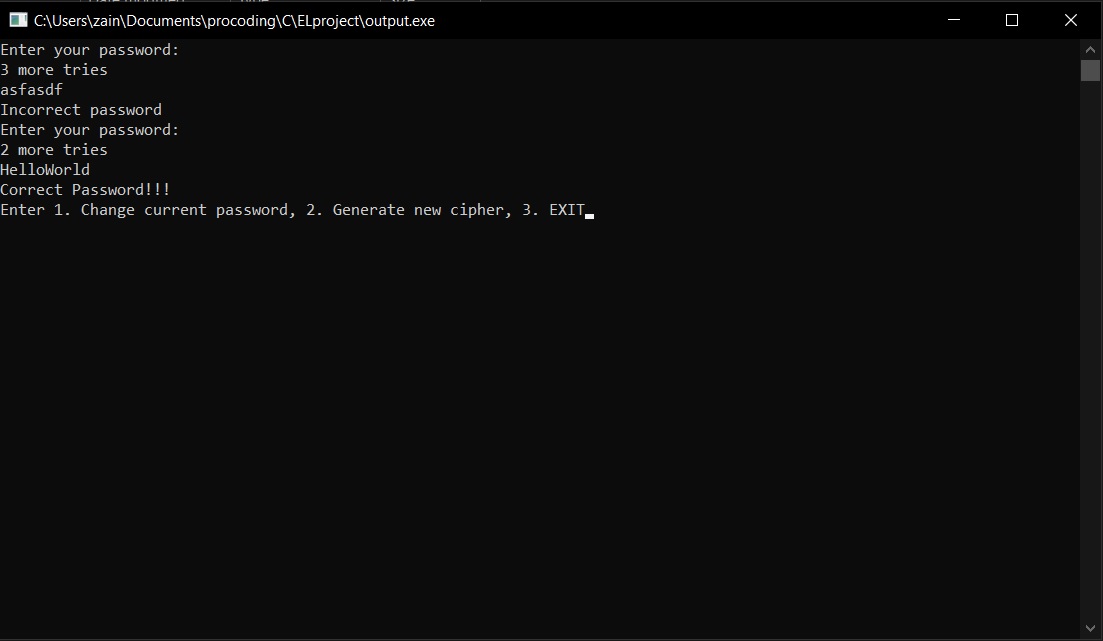
This module allows the user to directly change the password that the program checks for login at launch.

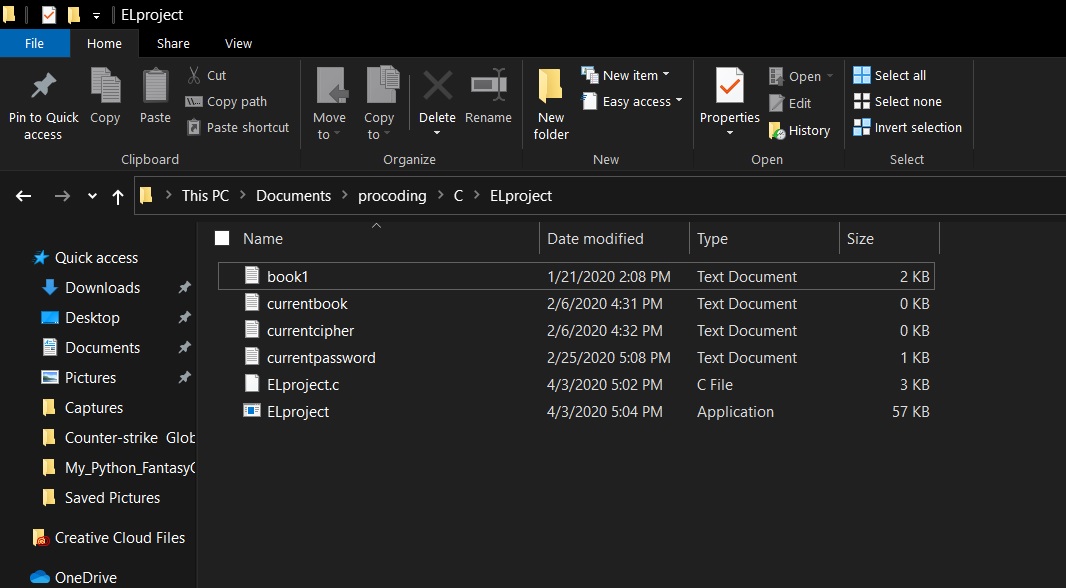
Implementation

The basic algorithm of converting a number series and corresponding book into a password is at the heart of the program.

It would offer an online library for users to store multiple books that they enjoy, allowing them to choose any one book for use in the password encryption without being too obvious about which one it is.

The program itself would not store any data other than the number key, so that even in the event of a data breach, there would be some amount of security.

The user would then be allowed to manually use the core algorithm of the program to manually check their number key against the book that they chose for it.



Conclusion

Ottendorf password security offers an innovative solution to conveniently become cyber secure, it provides the best solution for securely storing strong passwords and has true real world potential as there are many people who experience this dilemma.

References

-www.stackoverflow.com

-The C++ programming language, by Bjarne Stroustrup