ECE627 PROJECT SECURE WEBSITE AND EMAIL PASSOWRDS

Mostafa Mohamed

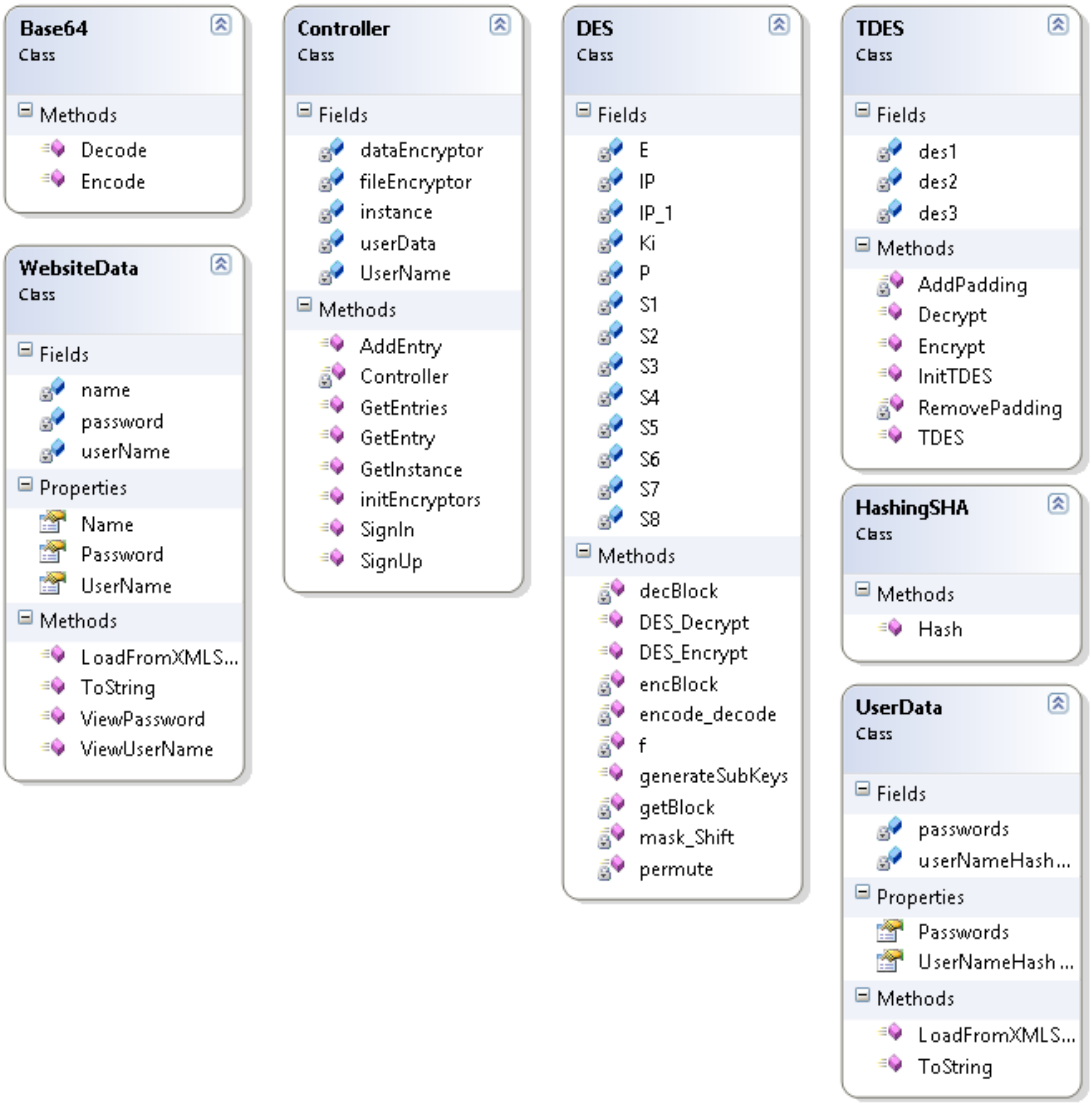
MSECE AT IUPUI

Project Overview

Most of computer users today need to keep track of many of passwords (e.g. Social networks, email, web sites). Some people write the passwords on a piece of paper but they could lose it or at any time someone can find it and get the important data they need to keep secret. Other people choose a master password for everything but again if someone knows the password then everything is vulnerable and not every website accepts every password.

In this project I am trying to create a solution to the passwords problem by creating an application for users to keep all the passwords safe encrypted by Triple DES and not revealing the data to anyone even their own personal computer.

System Architecture



System overview

The system block diagram consists mainly of few blocks plus the GUI data. The main classes in the system are the encryption blocks (DES, Triple DES), the Hashing block, the controller and the utilities (user data, base64 Encoders and website data).

Implementation

The implementation of the project was is in C# using Microsoft Visual Studio 2010. In .NET there is some security libraries so I have used the SHA384 hashing scheme from the library. But I have implemented all other blocks.

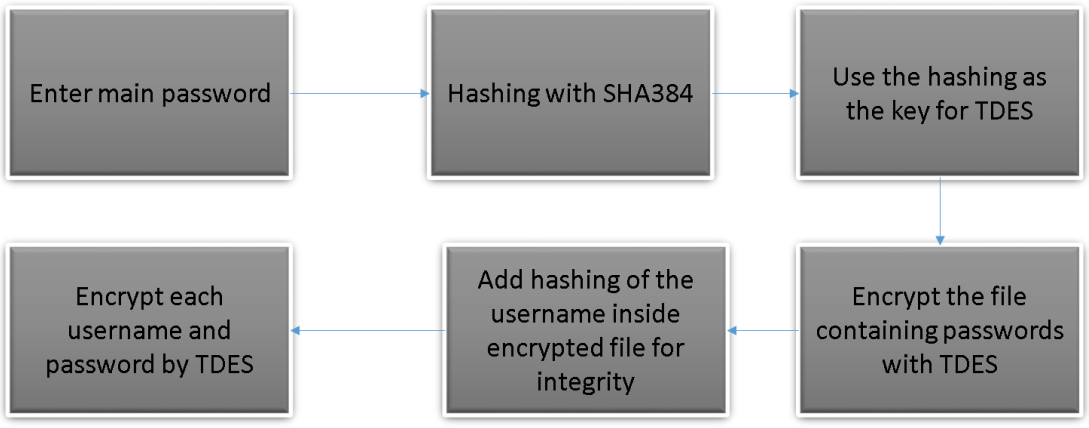
Work Flow

The system is easy to use by first starting the application then writing the username and password and sign up if it is first time otherwise the user just sign in. Then, the user can show the passwords saved or add new passwords through simple interface. The data itself is encrypted in a file. While the master password is not saved on the PC.

Security Design

The system is providing a secure safe for the many website passwords we are using currently. Everyone now has a problem managing the passwords for each website and email. Specially, each website has different requirements for it is own security. And using a master password for all of these passwords cannot guarantee that it will work for each website. Also we cannot keep the passwords online in our emails or in some website because we cannot trust them. The solution presented in this project is to use some offline software that keeps all the passwords safe and only the user can open them.

The security of the system has more than one level. First we need to keep our online passwords safe. So, we could just save them in a file and encrypt the file. But, the need to encrypt the file means that we need to save a private key for the whole process.



Security Flow

The user memorize his own master password for the program and username. Then the program saves a file with his user name encrypted. After entering the username and password the SHA384 hashing scheme is applied to his password and the result is divided into two keys for two Triple DES encryptions. The first encryption is for the whole file to be able to retrieve the data at one in a data structure that organizes everything. The second encryption is applied on individual website data. In the main file the username is hashed and kept inside the encrypted file so that we can verify the file is not modified. One more thing is added to make sure the text in files is safe is the base64 encoding scheme. The base64 encoding scheme is used to convert all binary data to normal characters in base64 and remove all special characters.

Future Directions

There are many future directions in this project. First thing is to extend the project to use different encryption schemes for more security and more options. Second direction is to extend the project to work on different platforms. Third directions is to synchronize the data with online servers that should keep the data but the security of the system still offline only at the user machine. There is one more direction on how to make it more secure even from the user machine itself. Currently, the user is not saving the master password on his own machine instead it is generated on the fly while trying to log-in. But, still it is visible in the memory of the processor.