



PASSWORD ENCRYPTION & DECRYPTION

Group members:

Aoun Haider (FA21-BSE-133) (Leader)

Samiullah Sheikh (FA21-BSE-085)

Saram Iftikhar (FA21-BSE-031)

Submitted to:

Sir Atif Saeed

Date:

12/16/2022

Abstract:

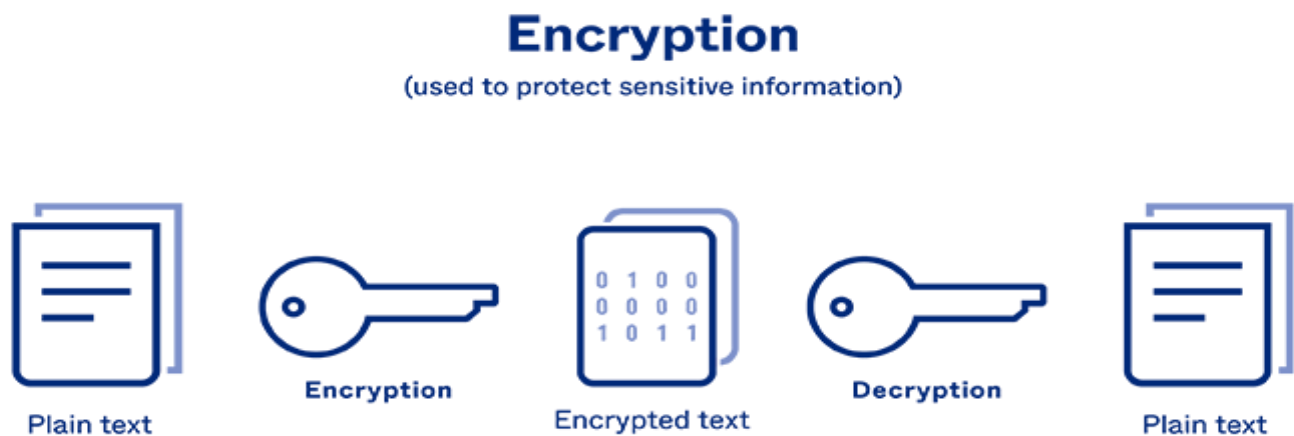
As the technology evolved, people had many accounts that needed a password for authentication. A password is required to access a particular account or information. However, the way they keep their account information expose them to vulnerable threats such as hacking if the password is not protected appropriately.

This Application will help the user to encrypt the password to protect from hackers as well as other unknowns. The user can also generate a unique password with some useful combinations of characters. In the same way, the user will be able to put decrypted message and get the encryption key.

Functionalities:

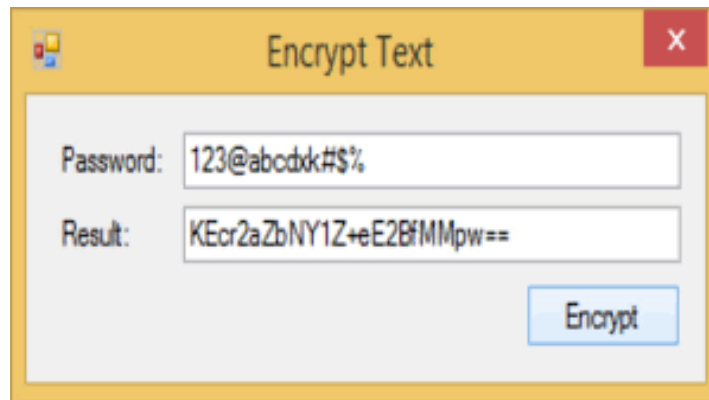
1) Encryption:

The user will provide the password/message which he wants to decrypt. After then, encrypted key will be assigned to user automatically. A proper algorithm will be used in order to provide a strong decryption key.



2) Decryption:

User can get the decoded/decrypted message from entering encrypted password/message. Security will be provided to user information by masking its details.



3) Unique password elicitation:

User can get the strong password with its encryption key to secure the password from hackers.

Conclusion:

This project has been approved to become the solution for user to manage their password more efficient after functionality testing that has been made by a qualified tester. This application can help user manage and keep their password of different account securely.

The secure part is implemented in the application by using an Advance Encryption Standard (AES) algorithm.