Release Document - Encryption/Decryption with user management utility

Version History

|  |  |  |  |
| --- | --- | --- | --- |
| Version# | Date | Author | Remarks |
| V.1 | Jan 10, 2021 | Neeraj Chhabra |  |

Prepared by: Neeraj Chhabra

Jan 10, 2021

Table of Contents

[Purpose and description 3](#_Toc61138031)

[1.1 Pre-requisites 3](#_Toc61138032)

[1.2 Document Purpose 3](#_Toc61138033)

[Process Flow 3](#_Toc61138034)

[Pre-requisites: 3](#_Toc61138035)

[Call to authorization() with user, pawd, users and Admin 4](#_Toc61138036)

[User selection 4](#_Toc61138037)

[**3.1** AdminModule 4](#_Toc61138038)

[3.2 User Module 4](#_Toc61138039)

[Encryption 4](#_Toc61138040)

[Code 4](#_Toc61138041)

[Unit Testing 5](#_Toc61138042)

# Purpose and description

This document provides details and description of the modules required to implement Encryption, Decryption and user management in the described project

## Pre-requisites

Python version 3.8

OS supported -> iOS, Windows, Linux

Libraries -> sys, Crypto, String, hashlib, base64, getpass

## Document Purpose

This low-level document lays down the steps required to implement the described project:

* User management functionality description and steps
* Encryption/Decryption methods

# Process Flow

This section of the document describes the code flow in the \_\_main\_\_ method is executed

## **Pre-requisites:**

Input username and password as user and pawd

Create a dummy user in users dictionary and Admin user in Admin dictionary for simulation

## **Call to authorization() with user, pawd, users and Admin**

This method acts as an interface for the logged in user,

Admin is given 2 chances to login, if login fails, Admin is asked to enter pin to get the password

User is given 3 chances and if all chances fail, user is asked to reach Admin for password reset

## **User selection**

### **3.1 Admin Module**

Id Admin logs in adminFunc() is called with user, pawd, users, Admin

Admin has special powers and only one user can be Admin, Admin can perform following tasks by choosing below mentioned options:

* d-> delete user
* a-> add user
* u-> update regular user password
* c-> change admin password
* l-> logout
* i-> list all users

### 3.2 User Module

If regular user logs in userFunc is called with user, pawd, users, Admin, newObj

newObj is used to use the access CipherText class for encryption/Decryption of data

User is a regular user which can perform following tasks by choosing below mentioned options:

* c-> change user password
* e-> encrypt data
* d-> decrypt data
* l-> logout

## Encryption

AES encryption technique has been used, when user logs in, a new Key is created that is used to encrypt and decrypt data.

getKey() function is used to create a random key whenever called.

encrypt() is used to encrypt data

decrypt() is used to decrypt data

## Code

Please refer to below document for code:



## 

## Unit Testing

Please refer to Test cases excel sheet.

