**Spring**

15

**Al Akhawayn University**

CSC 3355 Project # 1 Report

Meryem M’hamdi

Account Passwords Encryption and Decryption GUI based application

08

**Fall**

There are only two classes in this project. In the first one, I implemented the encryption and decryption methods. I have used AES as my encryption and decryption algorithm. Class EncryptionAlgorithm.java contains the steps used to implement the methods to encrypt and decrypt. The basic steps are as follows:

* Create a Key from a given byte array for a given algorithm.
* Get an instance of Cipher class for a given algorithm transformation. See document of the [Cipher](http://docs.oracle.com/javase/8/docs/api/javax/crypto/Cipher.html" \t "_blank) class for more information regarding supported algorithms and transformations.
* Initialize the Cipher with an appropriate mode (encrypt or decrypt) and the given Key.
* Invoke doFinal(input\_bytes) method of the Cipher class to perform encryption or decryption on the input\_bytes, which returns an encrypted or decrypted byte array.
* Read an input file to a byte array and write the encrypted/decrypted byte array to an output file accordingly.

In the class named EncryptionAlgorithmTested, I have created an user-friendly one comprehensive GUI interface to interact with the user. The interface is composed of three parts which are open existing password file, create a new password file and the table in which the accounts list are displayed. In create new password file part, the user can create a new file which doesn’t exist and has to choose a 16 characters key (64 bits) an error is displayed if a non 16 characters is chosen and the user is reasked to enter it , then the file is created in the chosen location and the user can add, modify and delete entries in the table below. The keys created for each file are stored in a file under the location in line 271 /Users/MeryemMhamdi/Desktop/Keys.txt. Please make sure to change the location accordingly to be able to test the application in another computer. The user can exit the application and renters to reaccess the password file, he should provide the correct necessary information in the open existing password file part (chosing the encrypted file in the file location). The user can add, modify and delete an entry by clicking on the respective buttons. Every change is recorded in the file so that next time the table is refilled considering last changes.