**Department Of Computer Science and Applications**

**Panjab University**

**Chandigarh**

****

**Project Report on Text Encryption Using RSA**

*(Session 2019-20)*

**SUBMITTED TO: SUBMITTED BY:**

**Prof. M.Syamala Devi Abhay Singh MCA-II (Evening)**

**Roll No. 51**

**CERTIFICATE**

***TO WHOM IT MAY CONCERN***

This is to certify that **ABHAY SINGH** pursuing Master of Computer Applications, at Panjab University, Chandigarh, undertook a project entitled **“Text Encryption Using RSA algorithm**”, the project is a bona fide work carried out by him under our supervision. This work has not been submitted earlier, either in part or in full, to any other university or institute for the award of degree.

***Prof. M.Syamala Devi***

***(Project Guide)***

***DCSA, Panjab University***

***Chandigarh***

**ABOUT THE PROJECT**

The project is about text-encryption using the RSA algorithm. I have started this project by writing the code for creating the menus in the program for switching between the different functionalities, where each option from the menu calls a function to perform a particular task. After creating the menu driven command line interface, I have written the functionalities corresponding to each function call.

The main feature of this program is to encrypt the text data using the private key and decrypt it using the public key, for this I have implemented three function this first one encrypt the data directly from the keyboard input, the second encrypt data of any text file stored in the hard-drive and last one is used to decrypt the data.

The latest version of C++ supports only integer type of size 64 bits only, but to use the RSA algorithm I needed the data-types which can store very large numbers therefore, to solve this problem I have used the boost multiprecision library which has allowed me user the integer data type of the size up to 4096 bits.

The program is very easy to use and can be used by anyone who wants to encrypt their text document & can only be decrypted by providing the right keys. I have tested this program with different set of inputs and text file and remove all the possible bugs came to my notice.

The program can further modified into GUI program to provide more ease of access to the users.

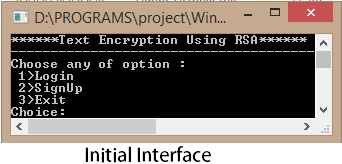
.

**TABLE OF CONTENT**

|  |  |  |
| --- | --- | --- |
| **Sr.no** | **Title** | **Page no.** |
| **1** | **Introduction** |  |
| **2** | **Program Design** |  |
| **3** | **Program Implementation** |  |
| **4** | **Program Testing** |  |
| **5** | **Conclusions & Scope for further Development** |  |
| **6** | **References** |  |

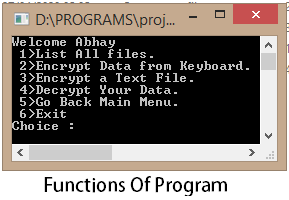
**Teacher’s sign- \_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**1. Introduction**



The Text Encryption program is a command line program developed using the c++ programming language. It implements the RSA algorithm to encrypt the text data character by character.

To use the program, the user is required to create a user-account using the sign up option from the program menu. To create an account the user has to provide a unique username and password after which the program will automatically generate the private and the public keys for the user.



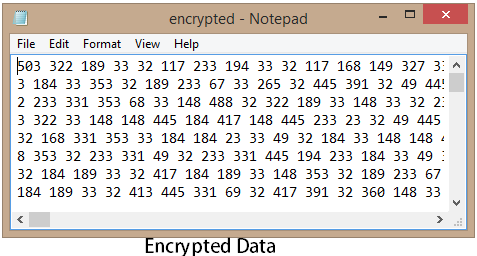
After creating the account, a user can login into the program by providing the username and password. On successful login the user is given six options to use the program, which includes options to encrypt/decrypt data and various other options as show in the picture:

The program is also able to handle any invalid input entered by the user

And prompt the user to enter the correct input till the user enters the correct input or exits the program by choosing the last option and confirming the exit prompt.

***1.1 Goal of the Project***

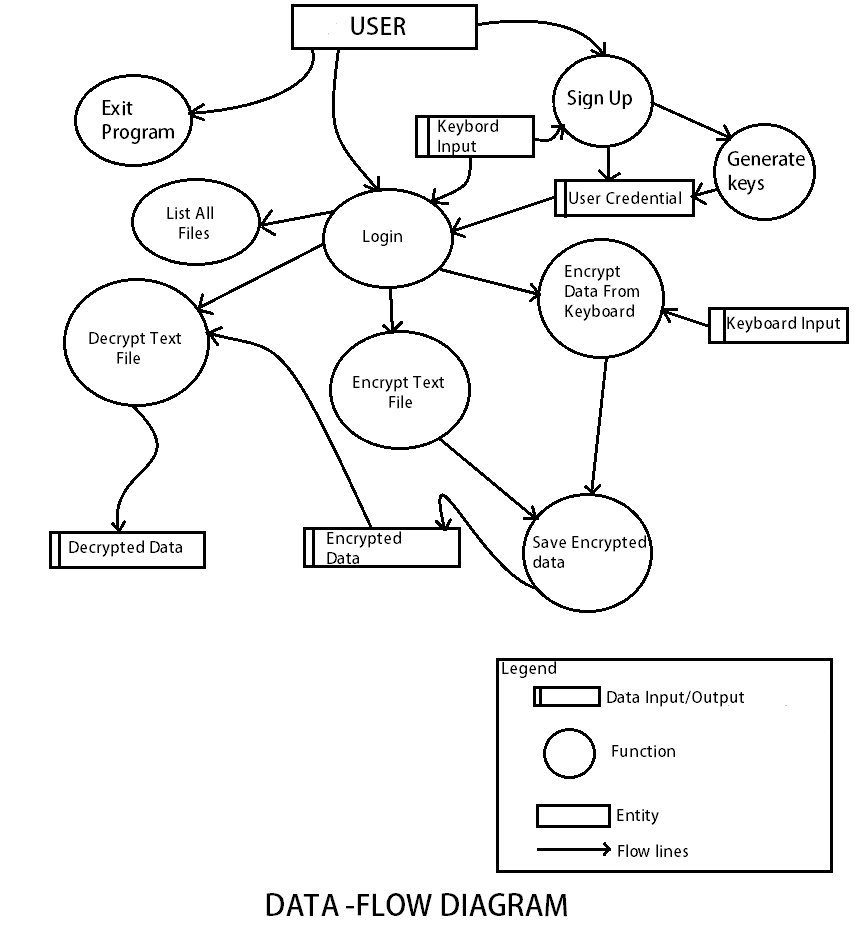
The main goal of the project is to create a very efficient program which can encrypt the text documents providing security and reliability. The encrypted document contains information in unreadable format, since all the information is converted into numerical format by applying the RSA encryption on each character.



***1.2 Objectives of the Project***

* **Implementing RSA algorithm:** One of the main objectives of the program is to show the working of the RSA algorithm for data encryption.
* **Saving The Data:** Another objective of the program is to save the encrypted to files by using the input & output stream class of the c++.
* **Security:** The security objective of the program is met by implementing the user-authentication feature in program.
* **Decrypting The Encrypted Data:** This is another relevant objective of the program to retrieve the data into its original format after proper authentication.

**2. Program Design**



**3. Program Implementation**

***Programming Language Used: C++***

***IDE Used: Code Blocks 17.12***

***Compiler Used: GNU GCC(c++ version 14)***

***Operating System: Microsoft Windows***

Source Code:

**4. Testing the Program**

**Program Initial Interface:**

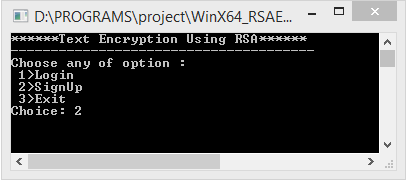


Figure 1 Initial Interface

**Create User Account by Choosing Option 2:**

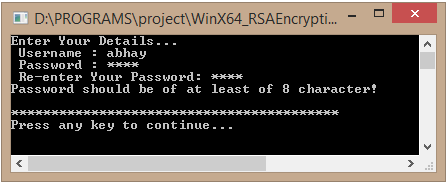


Figure 2 Password Validation

**Choose a Username & Password:**

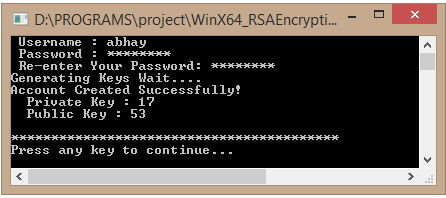


Figure 3 Account Successfully Created

**Login Using the Username & Password:**

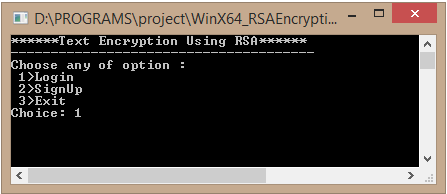


Figure 4 Choosing option 1 For Login

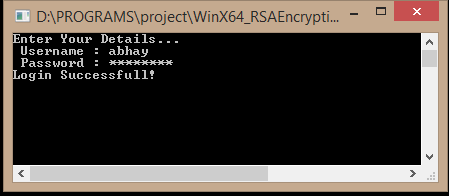


Figure 5 Input Username & Password

**Options Available After Successful Login:**

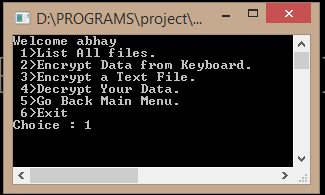


Figure 6 List of Function Available

**Listing the File under Current Directory:**

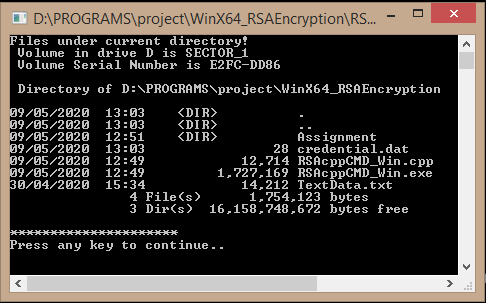


Figure 7 Choose Option 1 to list All Files

**Encrypting Data Entered Through Keyboard:**

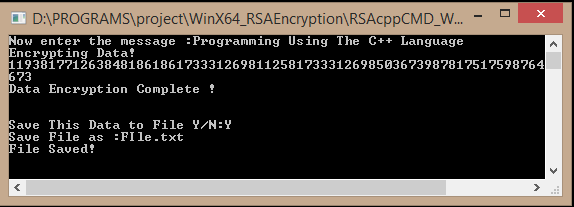


Figure 8 Encrypting & Saving the Data

**Sample Text File MyFile.txt:**

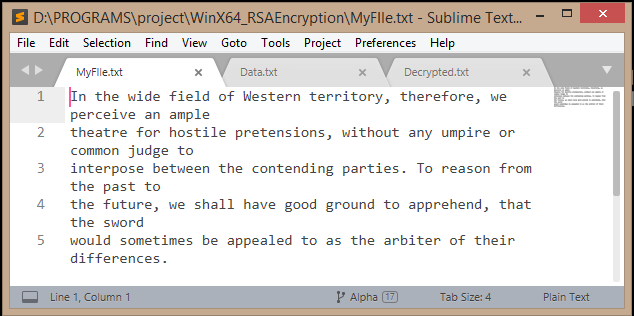
****

Figure 9 MyFile.txt

**Encrypting the Data Stored in text files:**

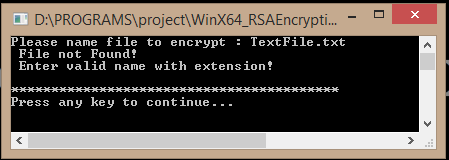


Figure 10 Show Error If File Is Not in Current Directory

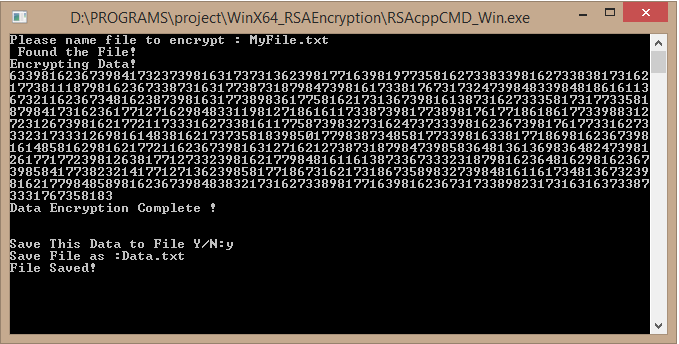
****

Figure 11 Encrypting the MyFile.txt & Saving the Data to Data.txt

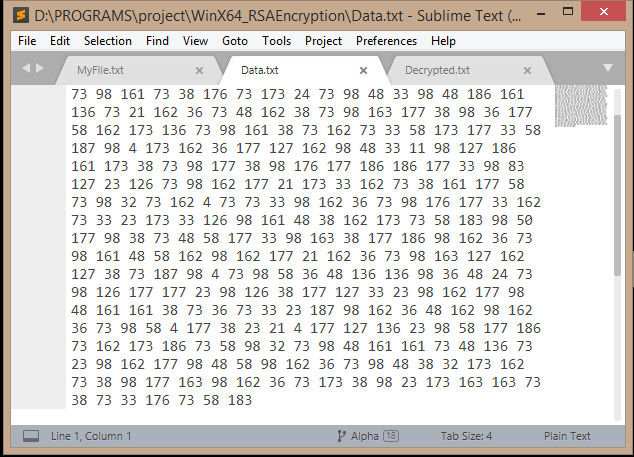
**Saved Data.txt File:**

Figure 12 Encrypted Information In Data.txt File

**Decrypting the Encrypted Data Store in Data.txt File:**

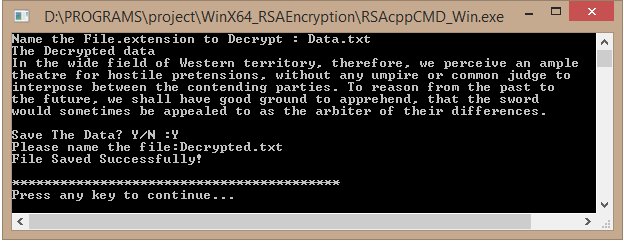


Figure 13 Decrypting & Saving the Data to Decrypted.txt

**Saved Decrypted.txt File:**

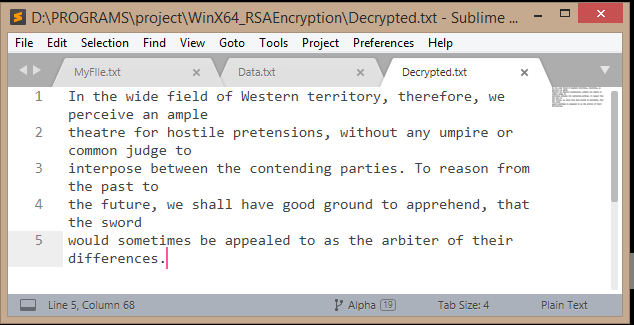
****

Figure 14 Decrypted.txt

**Closing the Program:**

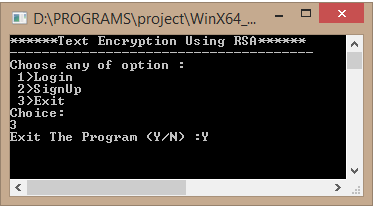


Figure 15 Exit Program

**5. Conclusion & Scope**

**6. References**

Geeksforgeeks.com

Stackoverflow.com

Boostmultiprecision

Tutorialpoint.com