**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**

In the beginning I have started this project by writing the switch statements for creating the menu’s 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 of the 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. The program can further modified into GUI program to provide more ease of access to the users.

I am thankful to Prof.M.Syamla Devi for her thorough guidance right from day 1st till the end of the Project and giving me the required guidance and removing any difficulties faced by me during the project. Finally I am indebted to my friends who showed tolerance and maturity when I was preoccupied with composition of the project cannot be expressed in words.

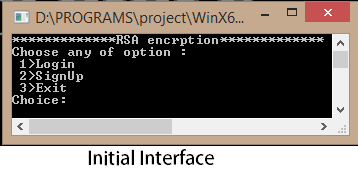
**TABLE OF CONTENT**

|  |  |  |
| --- | --- | --- |
| **Sr.no** | **Title** | **Page no.** |
| **I** | **Introduction** | **1-2** |
| **II** | **Design** | **3-6** |
| **III** | **Implementation** | **7-9** |
| **IV** | **Testing** | **10-20** |
| **V** | **Conclusions & Scope for further Development** | **21** |
| **VI** | **References** | **22** |

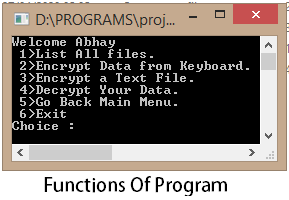
**Teacher’s sign- \_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**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.



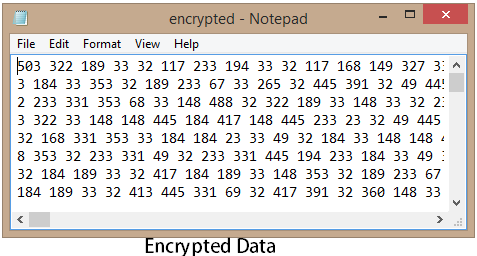
After creating the account, a user can login into the program by providing the username and password. on successful login the user is given six options to use the program, which includes options to encrypt/decrypt data and various other options as show in the picture:

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.

***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.



***Objectives of 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.