**Project Name:** Text Encryption

**Github Link:** https://github.com/projectsforstudents2022/Text\_Encryption.git

**Why was this project created?**

In the field of cryptography, encryption is the process of turning plain text or information into ciphertext, or text that can only be deciphered by the intended recipient. A cypher is the term used to describe the encryption algorithm. It secures communication networks and aids in preventing illegal access to customer information, emails, and other critical data.

**What problem is it solving?**

The objective of this project is to give consumers secure access to accurate data. Some users may experience data loss during the network's transmission process, while others may experience data modification by an unauthorised user. The network may also have additional security issues. The data in the network will be transported from the sender to the recipient using the most up-to-date technology, and our programme will increase network security and reduce data loss.

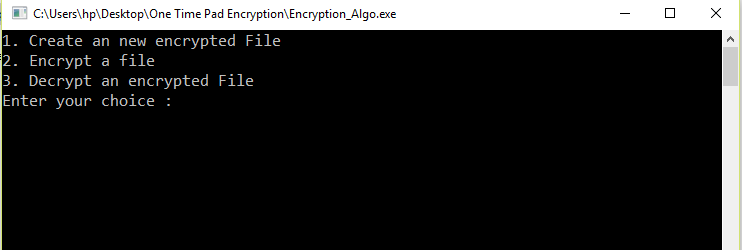
**Entire explanation of project**

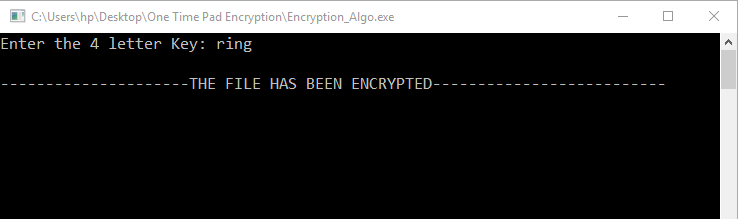
* **PROPOSED APPROACH**

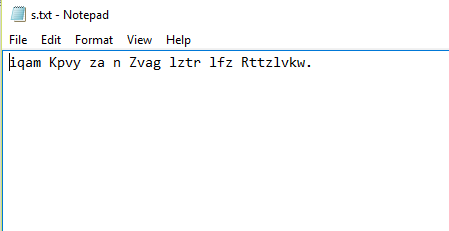
Encrypt() and decrypt are two member methods of the class encdec (). The class member variable contains the name of the file that has to be encrypted. The input file's encryption is handled by the encrypt() method. The encrypt() function includes the file handling code to read and write to the file. The entire encrypted data is placed in a brand-new encrypted file called encrypt.txt. Using a key that the user enters, the encrypted file is encrypted. To read an encrypted file, decrypt the data, and create a new file called decrypt.txt, use the decrypt() function. The user is asked for a key in order to decrypt a file. When the right key is used, then the file is successfully decrypted.

The output stream is used to write to the file while the input stream is used to read from it. In this system, information is encrypted and decrypted using a pair of keys. When encrypting data, a public key is used, and when decrypting data, a private key is used. The private key and the public key are distinct. Even if everyone has access to the public key, only the intended recipient can decode it because only he has access to the private key.

* **RESULT**







**CONCLUSION**

In this project, we discuss the ideas of network-wide digital data communication security. Steganography and cryptography features were used in the design of this project to improve performance. We used a fresh steganography technique in conjunction with the RSA encryption algorithm.