CS3002
CYBER SECURITY

Instructor: Sir Fahad Samad

Group Members

- Amman Soomro (K191048)
- Naba Jafri (K191118)
- Abdullah Ansari (K191042)

Introduction

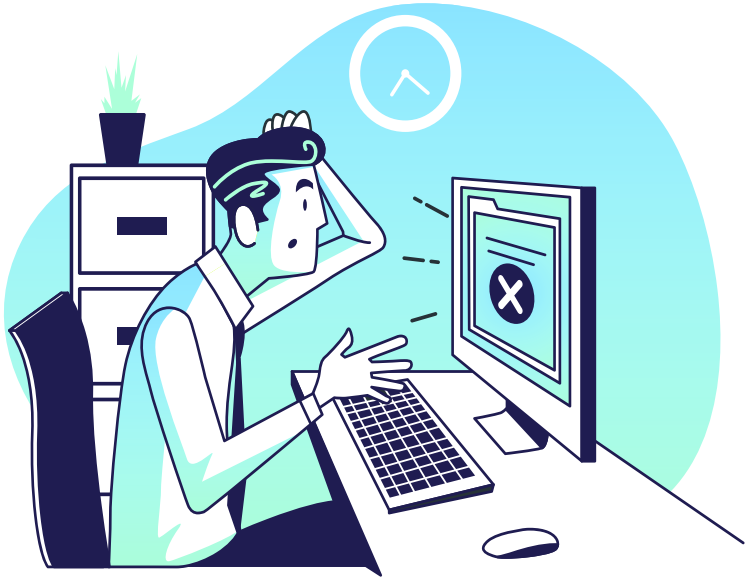
A type of encryption known as symmetric encryption uses a single secret key to both encrypt and decrypt digital data. To be used in the decryption procedure, the key must be exchanged between the parties communicating via symmetric encryption. This encryption technique is distinct from asymmetric encryption, which encrypts and decrypts data using a pair of keys—one public and one private.

In our project the user will first register himself/herself and will receive a private key after the registration process is done successfully. The user will have an option to share the key with anyone they want, the key will be shared using the Diffie Helman Key Exchange. Only the users with the key can see and decrypt the files/data.

Problem Statement

In this modern era, many organizations that don’t focus on their security has left themselves open to cyber-attacks and breaches, which them lead to severe effects on the organizations and businesses.

Often the leaked information or data, in any form, such as i.e., Hard Document, or a soft copy leads to serious and catastrophic issues such as, Confidential or private data leakage, financial losses, identity theft, blackmailing etc.



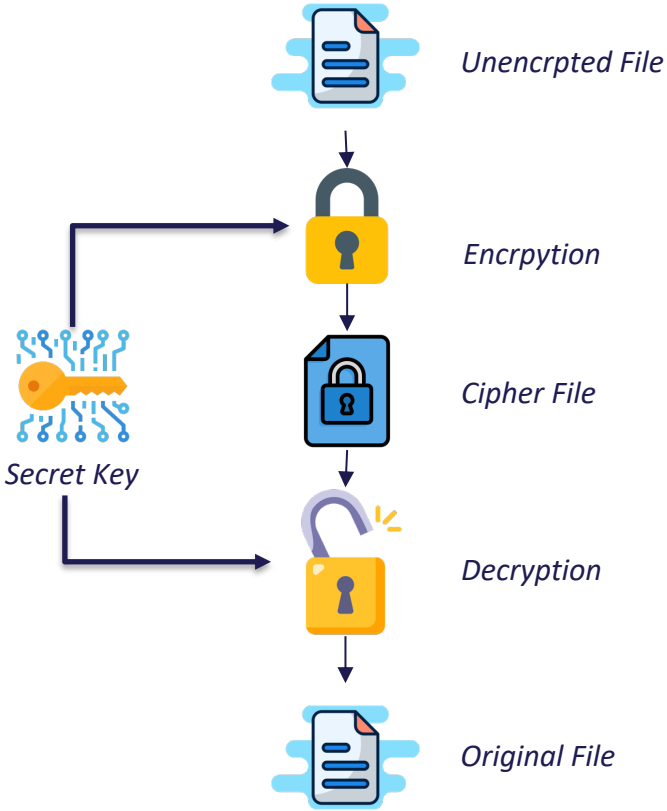
Solution

It is essential for everyone to have a secure way to share desired data among themselves in a secure, fast and easy way in this modern era, where it’s common for hackers to intrude your data.

We propose a solution to the above mentioned proposed in which the user will be provided with a user-friendly interface where user can easily register and acquire a secret key, upload and encrypt any (size limited) file they want, and have a way to share their key with anyone their want using a secure Diffie Helman Key Exchange method

To decrypt an encrypted file, the user will have to upload the file and enter the secret key.

Diagram


Unencrpted File
Encrpytion
Cipher File
Secret Key
Decryption
Original File