Graphic Era
HILL UNIVERSITY
Established by an Act of the State Legislature of Uttarakhand (Adhiniyam Sankhya 12 of 2011)

MINI PROJECT

REPORT

On

FILE ENCRYPTION

Submitted by:

Vaibhav Kumar Kapriyal

University Roll. No.: 2018837

Class Roll. No./Section: 60/A

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

GRAPHIC ERA HILL UNIVERSITY, DEHRADUN

ACKNOWLEDGMENT

Here by I am submitting the project report on **"File Encryption"** as per the scheme of Graphic Era Hill University, Dehradun.

I would like to particularly thank ***Ms. Lisa Gopal*** for her guidance, support and encouragement throughout the completion of this Mini Project.

At last, but not the least I greatly indebted to all other persons who directly or indirectly helped me during this project.

Vaibhav Kumar Kapriyal

University. Roll No.- 2018837

B. Tech CSE-A-III Sem

Session: 2021-22

GEHU, Dehradun

CERTIFICATE

Certified that Mr. Vaibhav Kumar Kapriyal (Roll No.- 2018837) has developed mini project on “File Encryption” for the CS III Semester Mini Project Lab in Graphic Era Hill University, Dehradun. The project carried out by Students is their own work as best of my knowledge.

Date: 23 Feb 2022

(Dr Rakesh Patra)
Class Co-ordinator
CSE-A-III-Sem
(CSE Department)
GEHU Dehradun

(Mrs. Lisa Gopal)
Project Guide
Resource Person
(CSE Department)
GEHU Dehradun

INTRODUCTION

The technology enables files to be transparently encrypted to protect confidential data from attackers with physical access to the computer.

Encryption as provided in is a process of converting messages, information, or data into a form unreadable by anyone except the intended recipient.

Encrypted data must be deciphered, or decrypted, before it can be read by the recipient. The root of the word encryption—crypt—comes from the Greek word kryptos, meaning hidden or secret. In its earliest form, people have been attempting to conceal certain information that they wanted to keep to their own possession by substituting parts of the information with symbols, numbers and pictures, this paper highlights in chronology the history of Cryptography throughout centuries. For different reason, humans have been interested in protecting their messages.

Threats to computer and network security increase with each passing day and come from a growing number of sources. No computer or network is immune from attack. A recent concern is the susceptibility of the power grid and other national infrastructure to a systematic, organized attack on the United States from other nations or terrorist organizations. That’s why Data encryption is the most essential element and requirement of todays world.

Objective

This project will meet the following objectives:

- To explore and implement an encryption and digital signature program to use with the aim of providing the user with a basic knowledge of the fundamental techniques of encryption and digital signature.
- To provide the user with authentication, integrity, confidentiality and non-repudiation of the data.
- To provide the user with an enhanced security of their data.
- To provide the user with a way to easily and conveniently protect the data.
- User friendly interface.

Motivation

Real Motivation for doing this project is that now days, digital information and data are being transmitted more often over the internet now than ever before.

Hence information security is becoming more and more important for information and transmission among the people.

So, in order to learn how the digital images, videos and audios ...etc could be protected by writing a piece of code I got very interested in choosing this project in which I learn various things about digital File Encryption and how easily the unauthorized persons from outside used our files without our consult.

Protection of digital data has been provided by a variety of encryption method. However, cryptography is considered as strong method specifically, Fernet methods which is symmetric type of cryptography, so cryptographic techniques play an important role here as it not only protects our digital data and also protecting it from unauthorized access. Storing of data is not enough but protecting it from unauthorized people is very important.
Hence by knowing all these things that data security is very important in present as well as in future, so this all things motivate me to choose “File Encryption” as my mini project and this project also enhance my knowledge in cyber security

Using this project, I was able to secure my files and its transmission among people became more secure than ever before.

Tools Used

1. From cryptography
    - Fernet based tools: -

        ♦ generate_key (): This method generates a new fernet key. The key must be kept safe as it is the most important component to decrypt the file.

        ♦ encrypt(data): It encrypts data passed as a parameter to the method. The outcome of this encryption is known as a “Fernet token” which is basically the ciphertext based file.

        ♦ decrypt (token, ttl=None): This method decrypts the Fernet token passed as a parameter to the method. On successful decryption the original file is obtained as a result, otherwise an exception is thrown.

2. From tkinter
    - Messagebox: Python Tkinter – MessageBox Widget is used to display the message boxes in the python applications. This module is used to display a message using provides a number of functions.

    - Filedialog: Python Tkinter (and TK) offer a set of dialogs that you can use when working with files. By using these you don’t have to design standard dialogs yourself. Example dialogs include an open file dialog, a save file dialog and many others.

    - Other tools based on tkinter for user friendly interface.

Methodology Used

Symmetric Encryption Method

Also called private-key cryptography or a secret key algorithm, this method requires the sender and the receiver to have access to the same key. So, the recipient needs to have the key before the message is decrypted. This method works best for closed systems, which have less risk of a third-party intrusion.

On the positive side, symmetric encryption is faster than asymmetric encryption. However, on the negative side, both parties need to make sure the key is stored securely and available only to the software that needs to use it.

We used the cryptography library to encrypt a file. The cryptography library uses a symmetric algorithm to encrypt the file. In the symmetric algorithm, we use the same key to encrypt and decrypt the file. The fernet module of the cryptography package has inbuilt functions for the generation of the key, encryption of plain text into cipher text, and decryption of cipher text into plain text using the encrypt () and decrypt () methods respectively. The fernet module guarantees that data encrypted using it cannot be further manipulated or read without the key.

Conclusion

The completion of the project went quiet well, I learned much new things while I was building up it, and I get up to know various platforms which help us to learn all this stuff. I was able to learn the practical use of cryptography. Python IDLE provides an open platform for developers to make up projects like this one. I learned many things about python, the libraries that is provided by it .I used tkinter gui in python ,using tkinter I have learned many things ,different features about it .Using python was amazing experience as it provides many inbuilt libraries and graphic user interface like tkinter .Overall working on this project was great fun as I came up with great piece of knowledge and understanding of the topic.

Reference

- Geek for Geek
- Google
- YouTube
- Tutorialpoint
- JavaTpoint