# JAYPEE INSTITUTE OF INFORMATION TECHNOLOGY, NOIDA

# Information Security Lab Project Report

# File Encryption/ Decryption Tool

**SUBMITTED BY**

**AYUSH UPADHYAY**

# Problem Statement

- A Python-based file encryption and decryption tool that allows users to secure sensitive data by encrypting files and later decrypting them when needed.
- The tool should provide a simple and user-friendly interface. Users can choose to encrypt a file by generating a unique key using the Fernet symmetric key encryption algorithm and subsequently decrypt the file using the same key.
- The tool must handle file existence checks, key generation, and user confirmation before overwriting decrypted files ensuring proper error handling, such as notifying users of invalid keys during decryption.
- This project aims to provide a practical solution for users who need to secure and manage their sensitive files with ease.

# Key Concepts

The project involves several key topics and concepts. Here are the main topics used in the project:

File Operations:

- Reading and writing files using Python's open function.
- Checking file existence with os.path.exists.

Cryptography:

- Utilizing the cryptography library for encryption and decryption.
- Fernet symmetric key encryption scheme.

User Input and Interaction:

- Accepting user input using input for choices, filenames, and key confirmation.

Error Handling:

- Using try and except blocks to handle exceptions, such as InvalidToken during decryption.

Control Flow:

- Using if, elif, and else statements for decision-making based on user choices.

Modularization:

- Organizing code into functions (generate_key, load_key, encrypt, decrypt) for modularity and readability.

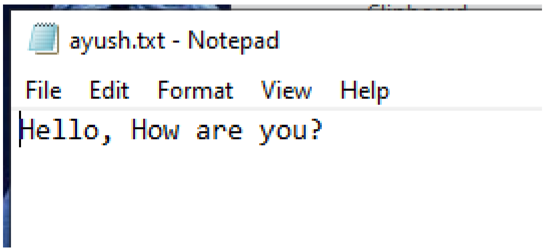
These key topics collectively contribute to the implementation of a secure file encryption and decryption tool.

# Source Code

```python
from cryptography.fernet import Fernet, InvalidToken
import os

def generate_key():
    key = Fernet.generate_key()
    with open("Secret.key", "wb") as key_file:
        key_file.write(key)

def load_key():
    return open("Secret.key", "rb").read()

def encrypt(filename, key):
    f = Fernet(key)
    with open(filename, "rb") as file:
        file_data = file.read()
        encrypted_data = f.encrypt(file_data)
    with open(filename, "wb") as file:
        file.write(encrypted_data)

def decrypt(filename, key):
    f = Fernet(key)
    with open(filename, "rb") as file:
        encrypted_data = file.read()
        try:
            decrypted_data = f.decrypt(encrypted_data)
        except InvalidToken:
            print("Invalid key. Decryption failed.")
            return

    confirm = input(f"Do you want to overwrite the original file '{filename}' with decrypted data? (yes/no): ").lower()
    if confirm == 'yes':
        with open(filename, "wb") as file:
            file.write(decrypted_data)
        print("File Decrypted and Overwritten Successfully!!!")
    else:
        print("Decryption canceled. The original file was not overwritten.")

# Main part of the script
choice = input("Enter 'E' to encrypt or 'D' to decrypt the file: ").lower()
if choice == 'e':
    filename = input("Enter the file name to encrypt (including file extension): ")
    if os.path.exists(filename):
        generate_key()
        key = load_key()
        encrypt(filename, key)
        print("File Encrypted Successfully!!!")
    else:
        print(f"File '{filename}' not found. Please check the file name and try again.")

elif choice == "d":
    filename = input("Enter the file name to decrypt (including file extension): ")
    if os.path.exists(filename):
        key = load_key()
        decrypt(filename, key)
    else:
        print(f"File '{filename}' not found. Please check the file name and try again.")

else:
    print("Invalid choice. Please enter 'E' to encrypt a file or 'D' to decrypt a file.")
```

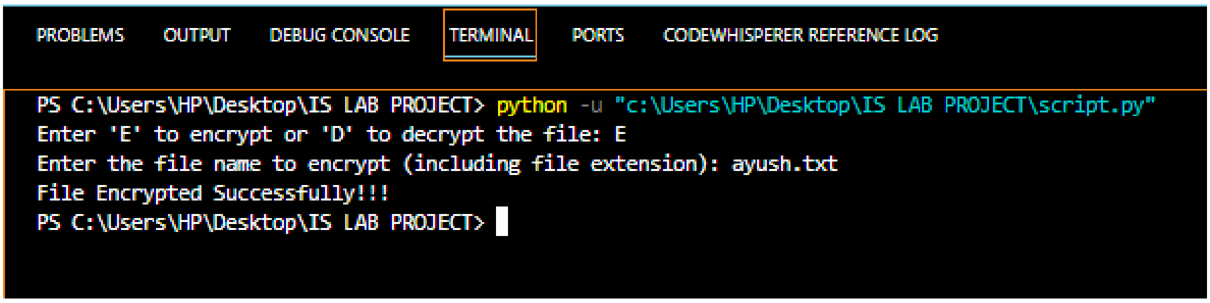
# Implementation Details

## Before encryption



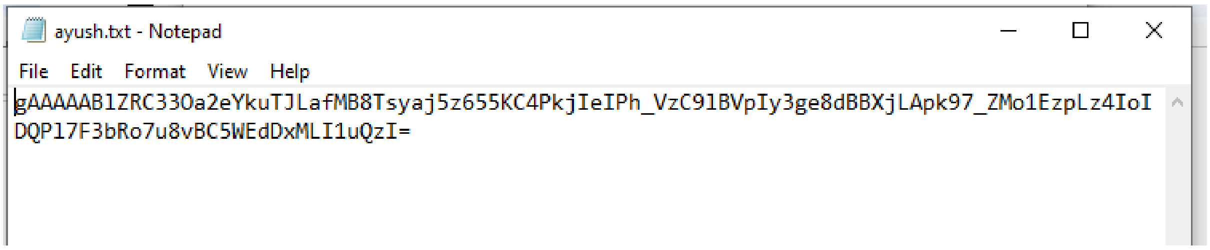
```
Hello, How are you?
```

## Running Program for encryption



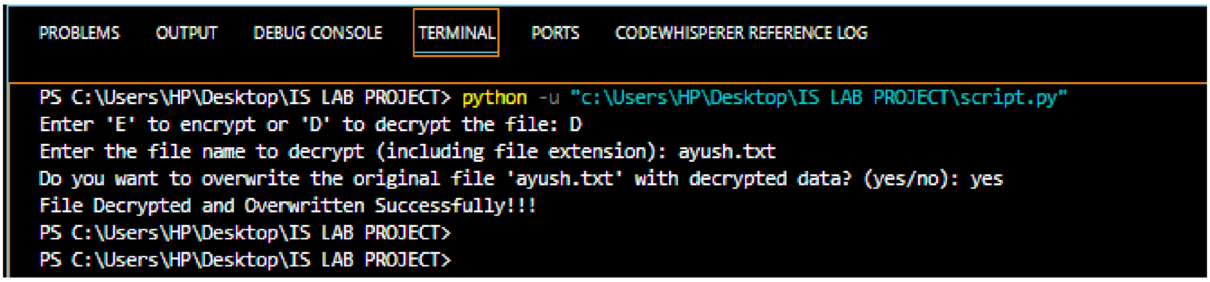
```
PS C:\Users\HP\Desktop\IS LAB PROJECT> python -u "c:\Users\HP\Desktop\IS LAB PROJECT\script.py"
Enter 'E' to encrypt or 'D' to decrypt the file: E
Enter the file name to encrypt (including file extension): ayush.txt
File Encrypted Successfully!!!
PS C:\Users\HP\Desktop\IS LAB PROJECT>
```

## After encryption



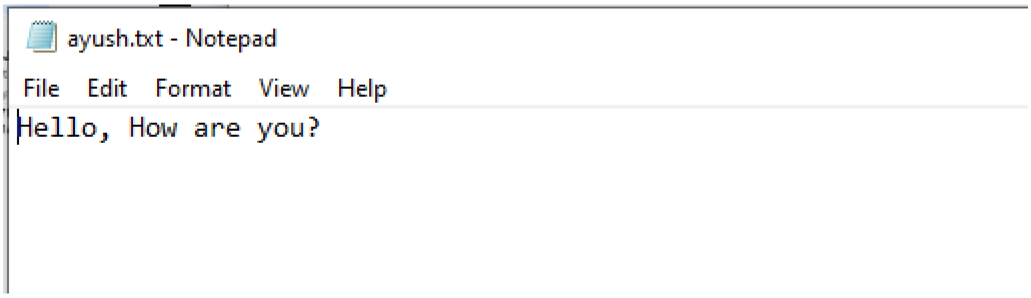
```
gAAAAABlZRC33Oa2eYkuTJLafMB8Tsyaj5z655KC4PkjIeIPh_VzC91BVpIy3ge8dBBXjLApk97_ZMo1EzpLz4IoI
DQP17F3bRo7u8vBC5WEdDxMLI1uQzI=
```

# Running Program for decryption



```
PS C:\Users\HP\Desktop\IS LAB PROJECT> python -u "c:\Users\HP\Desktop\IS LAB PROJECT\script.py"
Enter 'E' to encrypt or 'D' to decrypt the file: D
Enter the file name to decrypt (including file extension): ayush.txt
Do you want to overwrite the original file 'ayush.txt' with decrypted data? (yes/no): yes
File Decrypted and Overwritten Successfully!!!
PS C:\Users\HP\Desktop\IS LAB PROJECT>
PS C:\Users\HP\Desktop\IS LAB PROJECT>
```

# After Decryption



```
Hello, How are you?
```

# References

- https://www.w3schools.com/python/
- https://www.geeksforgeeks.org/cryptography-introduction/
- https://www.tutorialspoint.com/what-is-cryptography-in-computer-network