

Đại học Quốc gia Thành phố Hồ Chí Minh
Trường đại học Khoa học Tự nhiên
Khoa Công nghệ Thông tin



Môn: Thực tập Mạng máy tính

Project 1

Sinh viên

21127322 - Hoàng Xuân Khôi
21127105 - Bùi Nguyễn Nhật Minh

Giảng viên

Lê Giang Thanh
Ngô Đình Hy
Lê Hà Minh

TPHCM, 21.6.2024

Mục lục

1. Thông tin chung.....	2
2. Phân công.....	2
3. Các chức năng đã thực hiện.....	2
a. Cho phép phát sinh một khoá bí mật K_s của thuật toán AES.....	2
b. Mã hoá tập tin sử dụng thuật toán AES với khoá K_s	2
e. Mã hoá một chuỗi sử dụng thuật toán RSA sử dụng khoá K_{public} .	3
f. Giải mã một chuỗi sử dụng thuật toán RSA sử dụng khoá $K_{private}$	3
g. Tính giá trị hash của một chuỗi sử dụng thuật toán SHA-1, SHA-256.....	3
h. Xây dựng GUI.....	3
4. Demo sản phẩm.....	4
a. Encrypt.....	4
b. Decrypt.....	6
5. Tham khảo.....	8

1. Thông tin chung

MSSV	Họ tên	Email
21127322	Hoàng Xuân Khôi	hxkhoi21@clc.fitus.edu.vn
21127105	Bùi Nguyễn Nhật Minh	bnnminh21@clc.fitus.edu.vn

2. Phân công

Công việc	Thực hiện	Hoàn thành
Phần A - Module cho các thuật toán mã hóa	BNNMinh ▾	100%
Phần B - Xây dựng ứng dụng GUI để sử dụng các chức năng ở phần A	HXKhôi ▾	100%

3. Các chức năng đã thực hiện

a. Cho phép phát sinh một khoá bí mật Ks của thuật toán AES

- Hàm: generate_aes_key(length=32)
- Mô tả: Hàm này sử dụng os.urandom(length) để tạo ra một khoá AES ngẫu nhiên.

b. Mã hoá tập tin sử dụng thuật toán AES với khoá Ks

- Hàm: encrypt_file_aes(key, input_file, output_file)
- Mô tả: Hàm này sử dụng các hàm Cipher, algorithms.AES, modes.CFB, và encryptor.update từ thư viện cryptography để mã hoá dữ liệu trong tệp tin.

c. Giải mã tập tin sử dụng thuật toán AES với khoá Ks

- Hàm: decrypt_file_aes(key, input_file, output_file)
- Mô tả: Hàm này sử dụng các hàm Cipher, algorithms.AES, modes.CFB, và decryptor.update từ thư viện cryptography để giải mã dữ liệu trong tệp tin.

d. Phát sinh một cặp khoá Kprivate và Kpublic của thuật toán RSA

- Hàm: generate_rsa_key_pair()

- Mô tả: Hàm này sử dụng `rsa.generate_private_key` và `private_key.public_key()` từ thư viện `cryptography` để phát sinh cặp khoá RSA.

e. Mã hoá một chuỗi sử dụng thuật toán RSA sử dụng khoá `Kpublic`

- Hàm: `encrypt_string_rsa(public_key, message)`
- Mô tả: Hàm này sử dụng `public_key.encrypt` với `padding.OAEP` và `hashes.SHA256` từ thư viện `cryptography` để mã hoá một chuỗi.

f. Giải mã một chuỗi sử dụng thuật toán RSA sử dụng khoá `Kprivate`

- Hàm: `decrypt_string_rsa(private_key, encrypted_message)`
- Mô tả: Hàm này sử dụng `private_key.decrypt` với `padding.OAEP` và `hashes.SHA256` từ thư viện `cryptography` để giải mã một chuỗi.

g. Tính giá trị hash của một chuỗi sử dụng thuật toán `SHA-1`, `SHA-256`

- Hàm: `hash_private_key_sha1(private_key)`
- Mô tả: Hàm này sử dụng `hashlib.sha1` và `private_key.private_bytes` từ thư viện `cryptography` để tính toán giá trị hash `SHA-1` của khoá riêng tư RSA và trả về giá trị này dưới dạng chuỗi hex.
- Hàm: `hash_private_key_sha256(private_key)`
- Mô tả: Hàm này sử dụng `hashlib.sha256` và `private_key.private_bytes` từ thư viện `cryptography` để tính toán giá trị hash `SHA-256` của khoá riêng tư RSA và trả về giá trị này dưới dạng chuỗi hex.

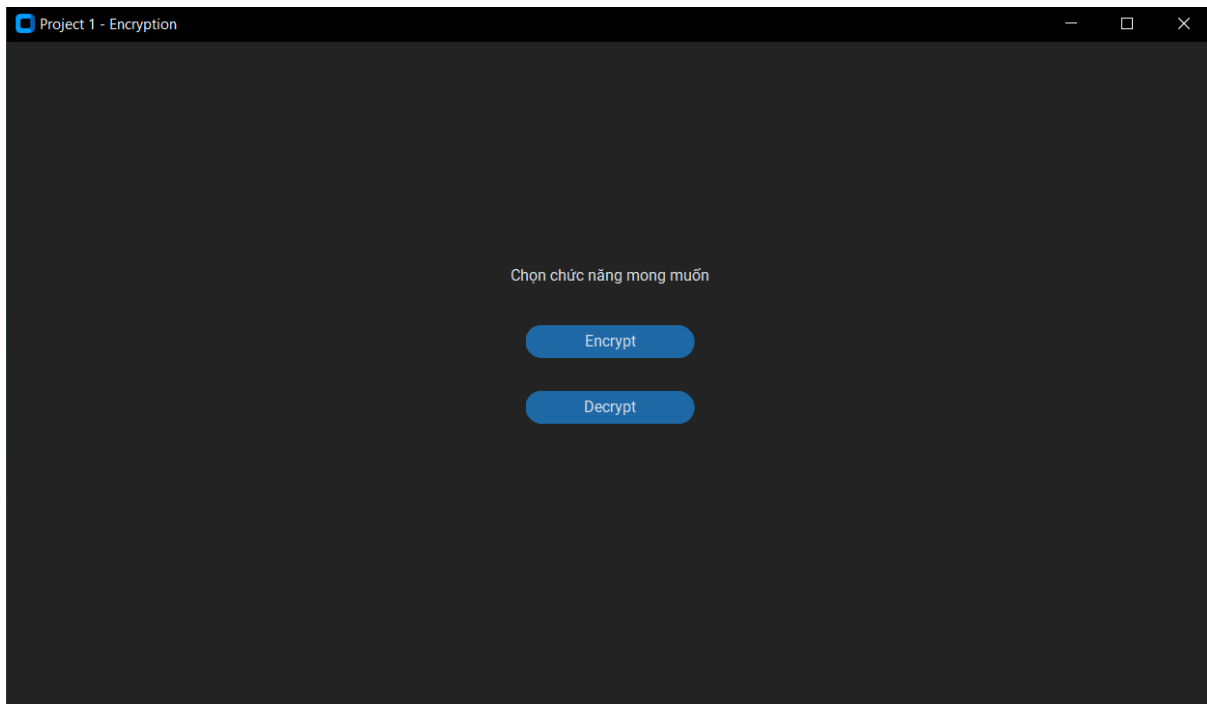
h. Xây dựng GUI

- GUI sử dụng thư viện `customtkinter` để hiện màn hình, các nút bấm và label
- Ở giao diện GUI người dùng có thể chọn file thông qua `filedialog` thuộc thư viện `tkinter`
- Sau khi chọn các file cần thiết thì ở mỗi bước (Encrypt hay Decrypt), các hàm trong `main.py` sẽ gọi các hàm tương ứng trong `module.py` để thực hiện các bước cần thiết

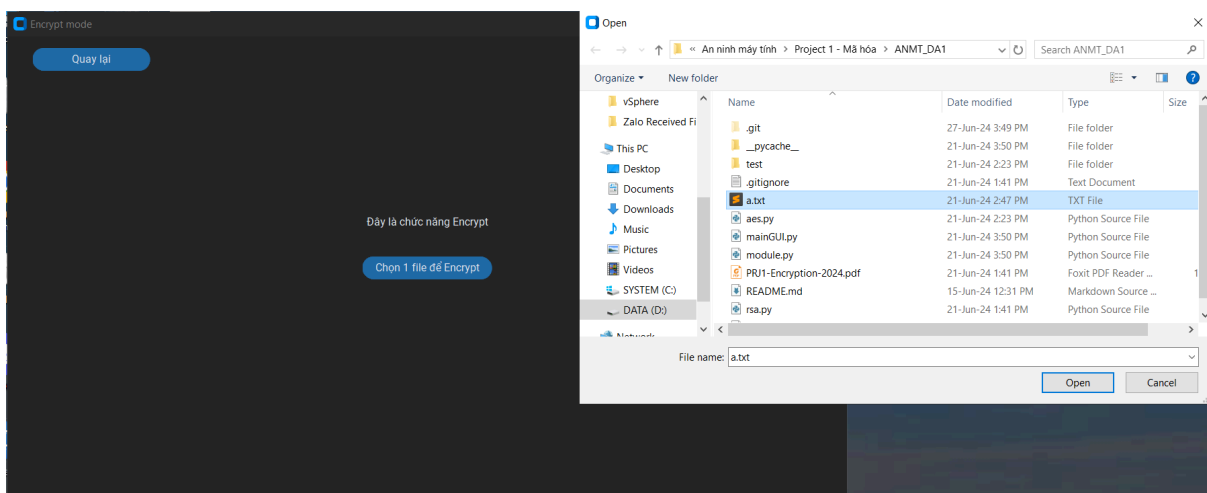
4. Demo sản phẩm

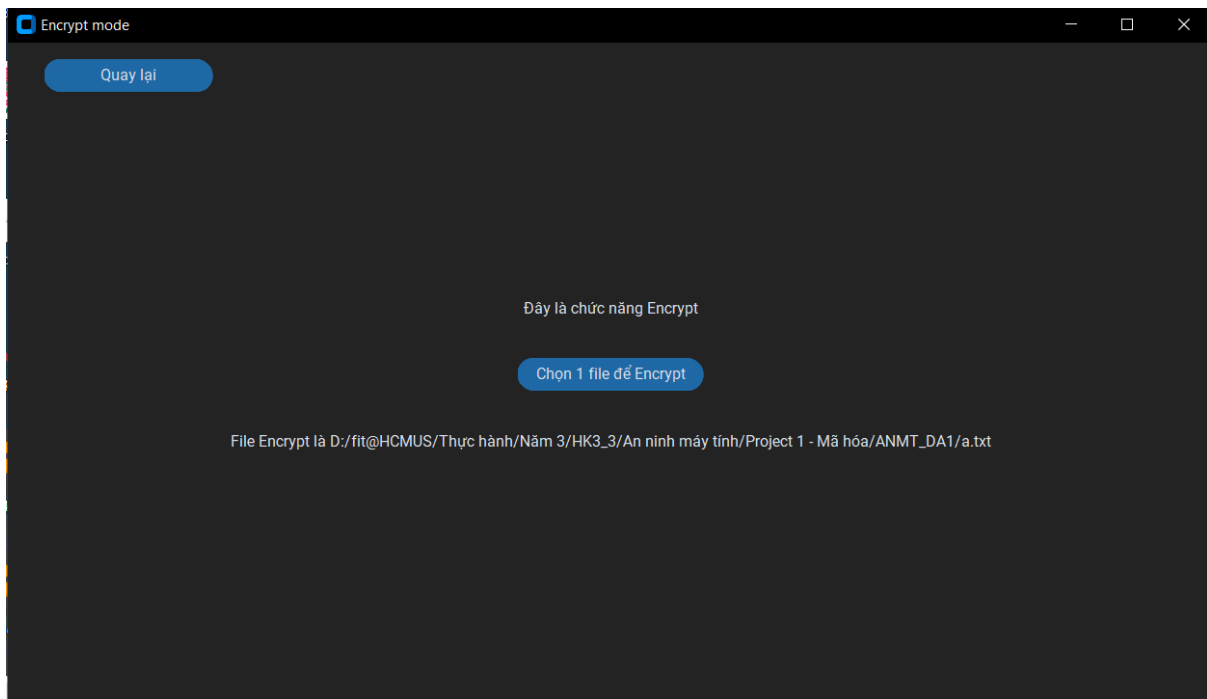
a. Encrypt

- Đầu tiên sẽ là trang chính để người dùng chọn Encrypt và Decrypt

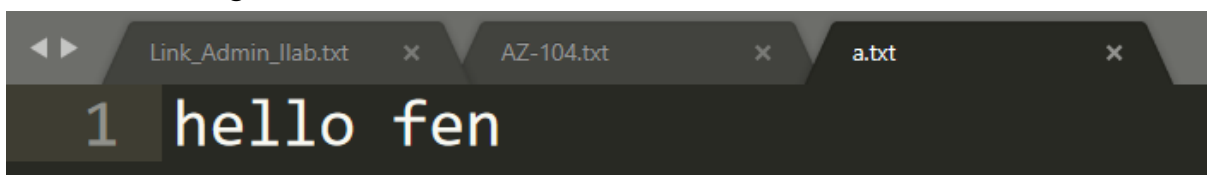


- Người dùng chọn Encrypt sau đó chọn tập tin mà mình muốn mã hóa








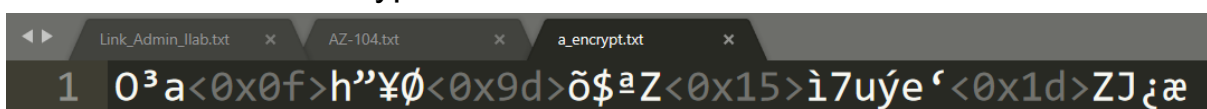
- Nội dung file a.txt



- Sau đó thì hệ thống sẽ tạo ra các file: encrypt (file sau khi encrypt), private_key (file chứa Kprivate) và secret.json (file chứa chuỗi Kx kèm theo giá trị hash SHA-1)

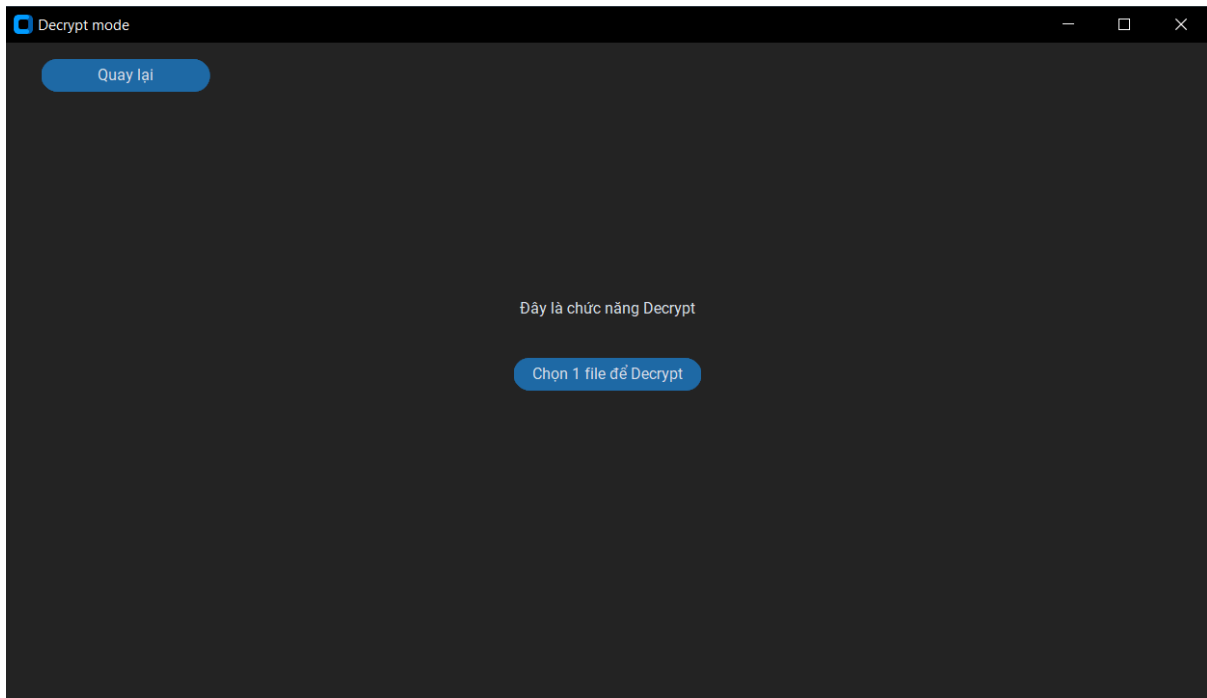
 a_encrypt.txt	27-Jun-24 3:53 PM	TXT File	1 KB
 a_private_key.pem	27-Jun-24 3:53 PM	PEM File	2 KB
 secret.json	27-Jun-24 3:53 PM	JSON Source File	2 KB

- File sau khi Encrypt

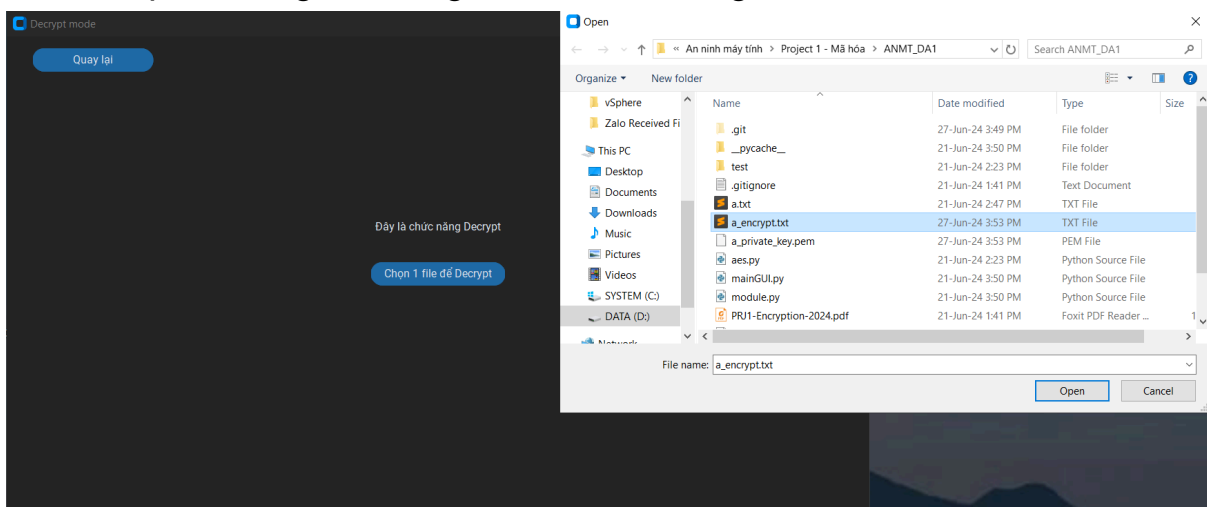


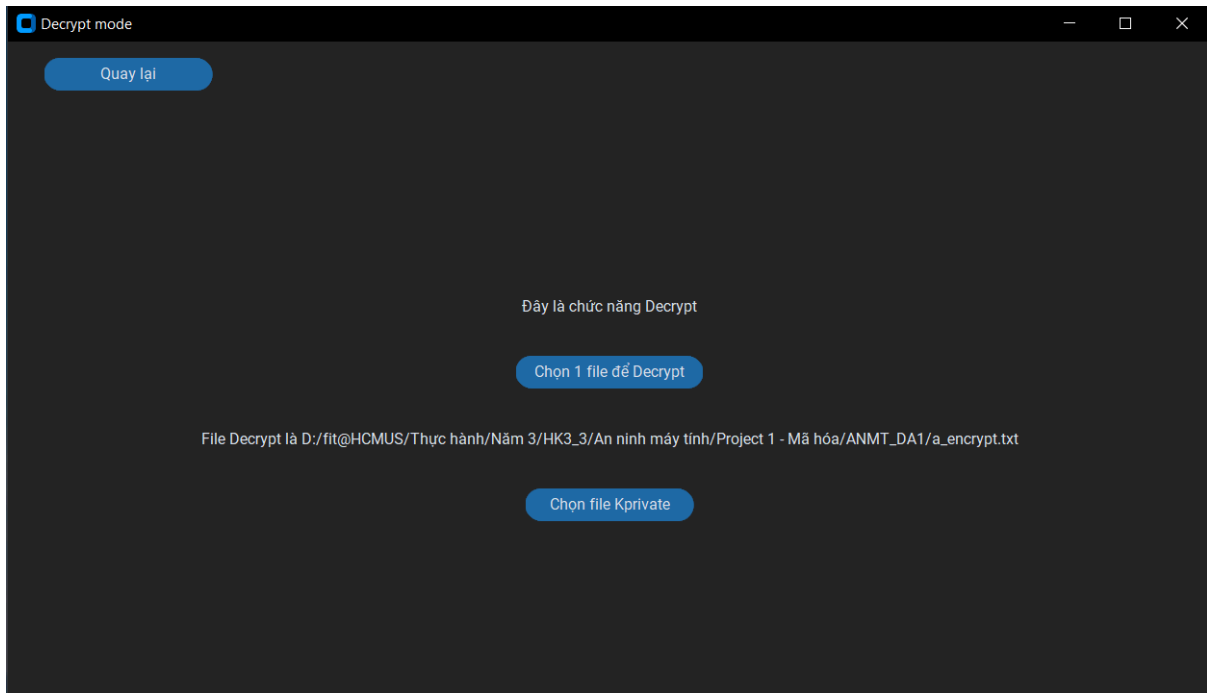
b. Decrypt

- Người dùng bấm nút Quay lại và chọn Decrypt

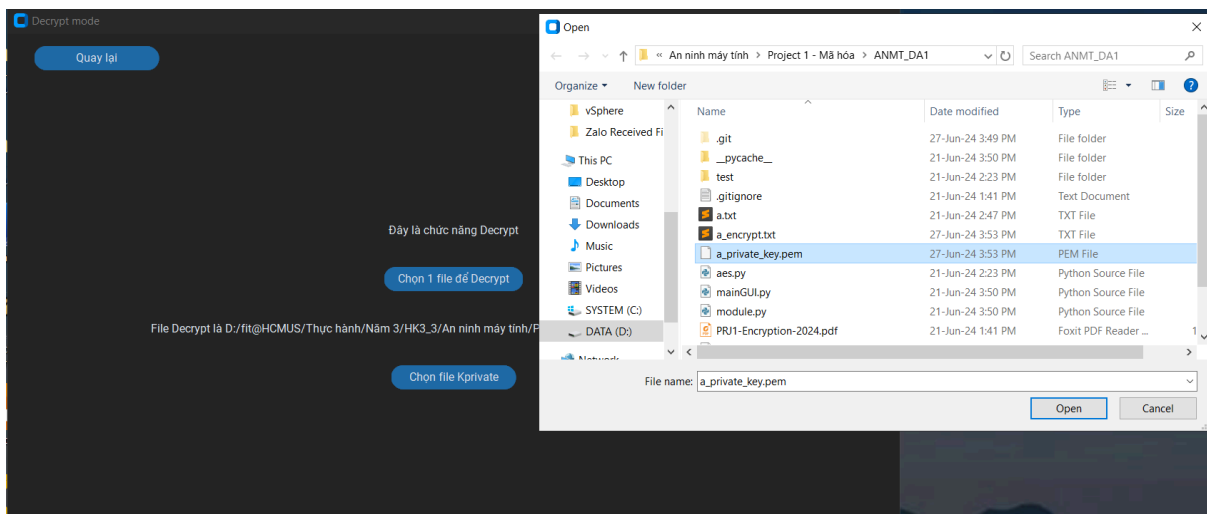


- Tiếp theo, người dùng chọn file muốn giải mã

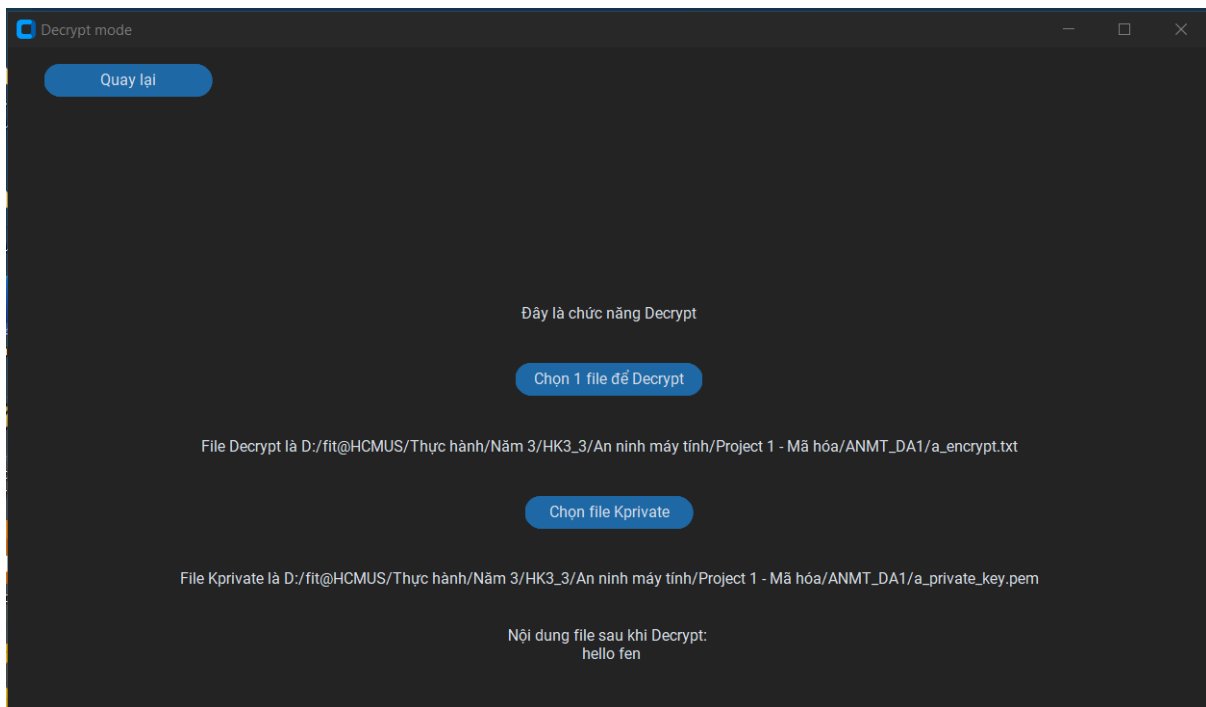




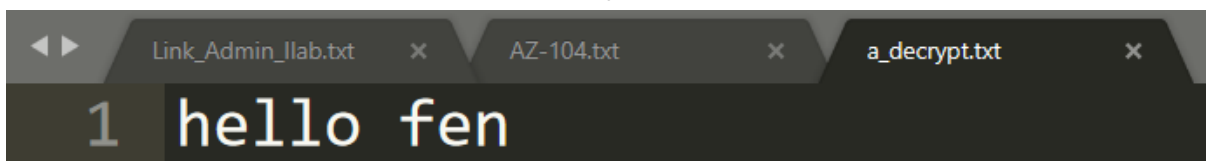
- Sau khi chọn file muốn giải mã, người dùng chọn file chứa khóa Kprivate



- Hệ thống sẽ giải mã và in ra kết quả sau khi giải mã ra màn hình, cũng như là file decrypt chứa kết quả



- File chứa kết quả sau khi Decrypt



5. Tham khảo

- Customtkinter: https://www.youtube.com/playlist?list=PLMi6KgK4_mk0P9FWD1ULjzhzspu23h-Br
- cryptography: [cryptography · PyPI](#)
- AES: [Professional Data Encryption in Python \(youtube.com\)](#)
- RSA: [RSA Private & Public Key Encryption in Python \(youtube.com\)](#)