

**TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN – ĐHQG HCM**

**KHOA CÔNG NGHỆ THÔNG TIN**

**MÔN AN NINH MÁY TÍNH**



# **BÁO CÁO**

# **ĐỒ ÁN 1**

**Giảng viên lý thuyết:** Lê Giang Thanh

**Giảng viên thực hành:** Lê Hà Minh

**Giảng viên trợ giảng:** Ngô Đình Hy

**Sinh viên thực hiện:**

Võ Minh Tuấn 21127472

Sú Quang Mỹ Phụng 21127674

**Lớp:** 21MMT

*Hồ Chí Minh, ngày 26 tháng 06 năm 2024*

## MỤC LỤC

1. Thông tin thành viên nhóm.....	3
2. Phân chia công việc và tiến độ .....	3
3. Tổng quan chương trình .....	4
4. Chức năng và màn hình .....	4
4.1. Màn hình chính .....	4
4.2. Màn hình mã hóa .....	5
4.3. Màn hình giải mã .....	8
5. Khó khăn gặp phải và giải pháp.....	10
5.1. Mã hóa file bằng AES .....	10
5.2. Mã hóa chuỗi bằng RSA.....	10
Tài liệu tham khảo .....	11

## 1. Thông tin thành viên nhóm

Họ và tên	MSSV	Email
Võ Minh Tuấn	21127472	sqmphung21@clc.fitus.edu.vn
Sú Quang Mỹ Phụng	21127674	vmtuan21@clc.fitus.edu.vn

## 2. Phân chia công việc và tiến độ

Công việc	Người thực hiện	Mô tả nhiệm vụ	Mức độ hoàn thành
AES	Võ Minh Tuấn	Cho phép phát sinh một khoá bí mật Ks của thuật toán AES	100%
	Võ Minh Tuấn	Mã hoá tập tin sử dụng thuật toán AES với khoá Ks	100%
	Võ Minh Tuấn	Giải mã tập tin sử dụng thuật toán AES với khoá Ks	100%
RSA	Sú Quang Mỹ Phụng	Phát sinh một cặp khoá Kprivate và Kpublic của thuật toán RSA	100%
	Sú Quang Mỹ Phụng	Mã hoá một chuỗi sử dụng thuật toán RSA sử dụng khoá Kpublic	100%
	Sú Quang Mỹ Phụng	Giải mã một chuỗi sử dụng thuật toán RSA sử dụng khoá Kprivate	100%
Hash	Võ Minh Tuấn	Tính giá trị hash của một chuỗi sử dụng thuật toán SHA-1, SHA-256	100%
Ứng dụng	Sú Quang Mỹ Phụng	Tạo module	100%
	Sú Quang Mỹ Phụng	Thiết kế màn hình giao diện	100%

<b>Công việc</b>	<b>Người thực hiện</b>	<b>Mô tả nhiệm vụ</b>	<b>Mức độ hoàn thành</b>
	Sú Quang Mỹ Phụng	Xử lý sự kiện màn hình chính	100%
	Sú Quang Mỹ Phụng	Xử lý sự kiện màn hình mã hóa	100%
	Võ Minh Tuấn	Xử lý sự kiện màn hình giải mã	100%
Báo cáo	Võ Minh Tuấn	Viết báo cáo	100%
	Sú Quang Mỹ Phụng	Soát lỗi chính tả và định dạng	100%

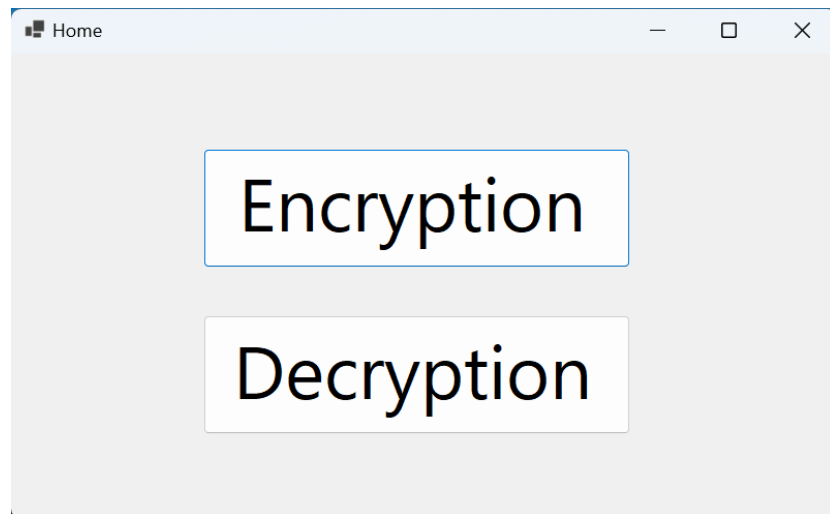
### 3. Tổng quan chương trình

- Ngôn ngữ lập trình: C#, .NET 8.0
- GUI: Winforms
- IDE: Visual Studio 2022
- Hệ điều hành: Windows 11

### 4. Chức năng và màn hình

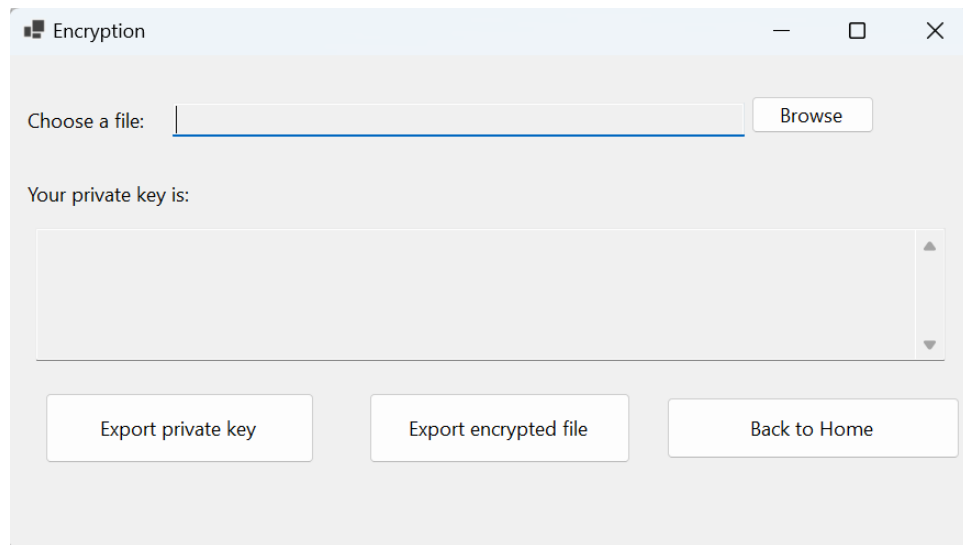
#### 4.1. Màn hình chính

- Màn hình chính cho người dùng chọn 2 chức năng là mã hóa (encryption) hoặc giải mã (decryption).

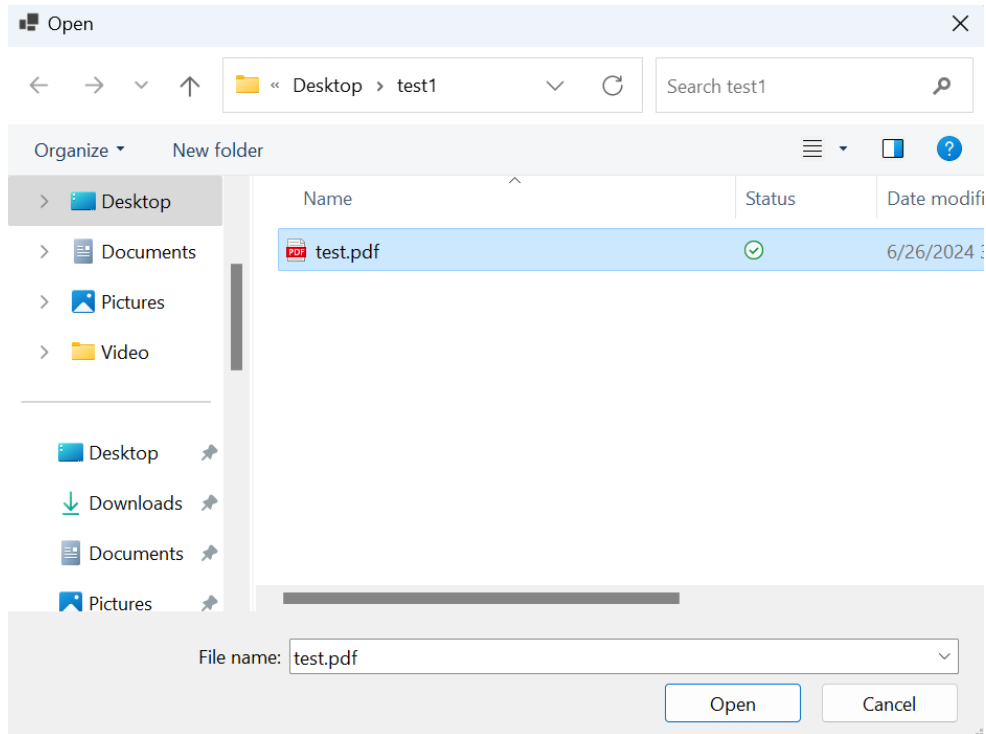


## 4.2. Màn hình mã hóa

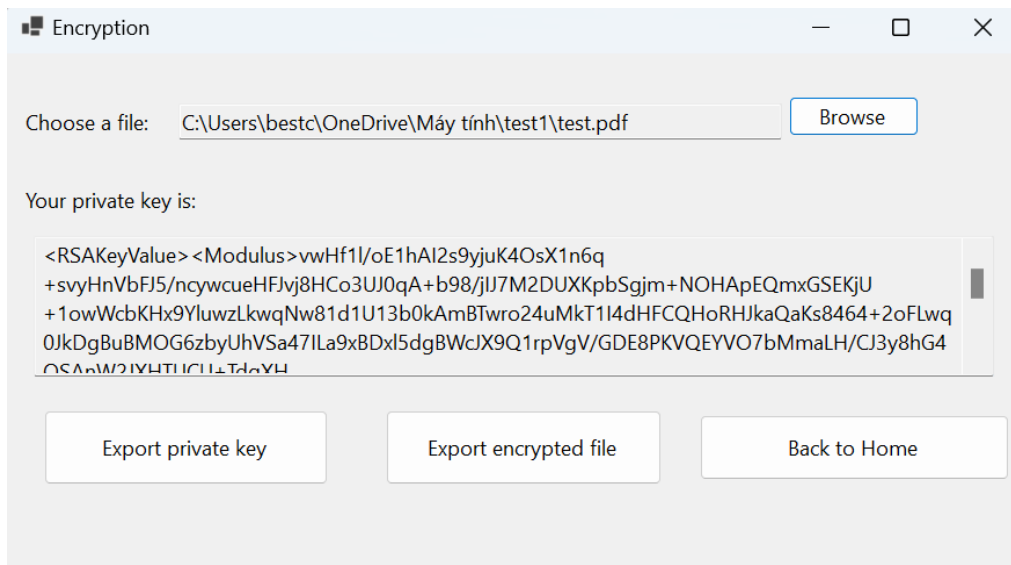
- Khi người dùng chọn chức năng Encryption thì cửa sổ mã hóa sẽ hiển thị:



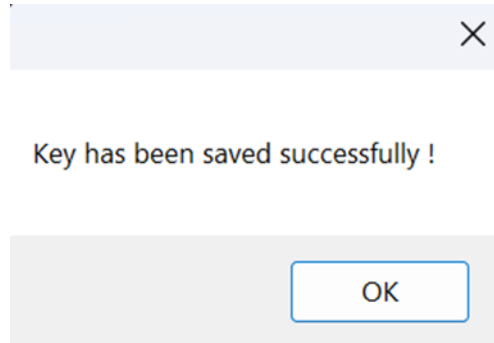
- Các bước sử dụng:
  - o Nhấn Browse để chọn file cần mã hóa từ máy tính:









- Khi chọn file thành công, hệ thống sẽ hiển thị khóa bí mật RSA cho người dùng:



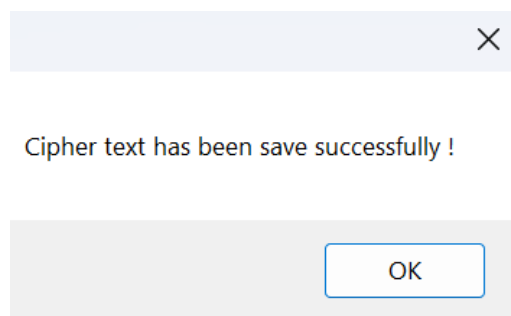
- Người dùng chọn nút “Export private key” để kết xuất khóa ra file (định dạng file là .txt), khi lưu thành công thì hệ thống sẽ hiện thông báo khóa đã lưu thành công:



- Sau đó, người dùng chọn nút “Export encrypted file” để lưu dữ liệu đã mã hóa ra file (định dạng file mã hóa là .metadata), file mã hóa sẽ tự động lưu cùng thư mục với file gốc:

Name	Status	Date modified	Type	Size
 key.txt		6/27/2024 10:22 PM	Text Document	2 KB
 test.metadata		6/27/2024 10:25 PM	METADATA File	157 KB
 test.pdf		6/26/2024 3:46 PM	Microsoft Edge PDF ...	157 KB

- Khi lưu thành công, hệ thống sẽ hiển thị thông báo:

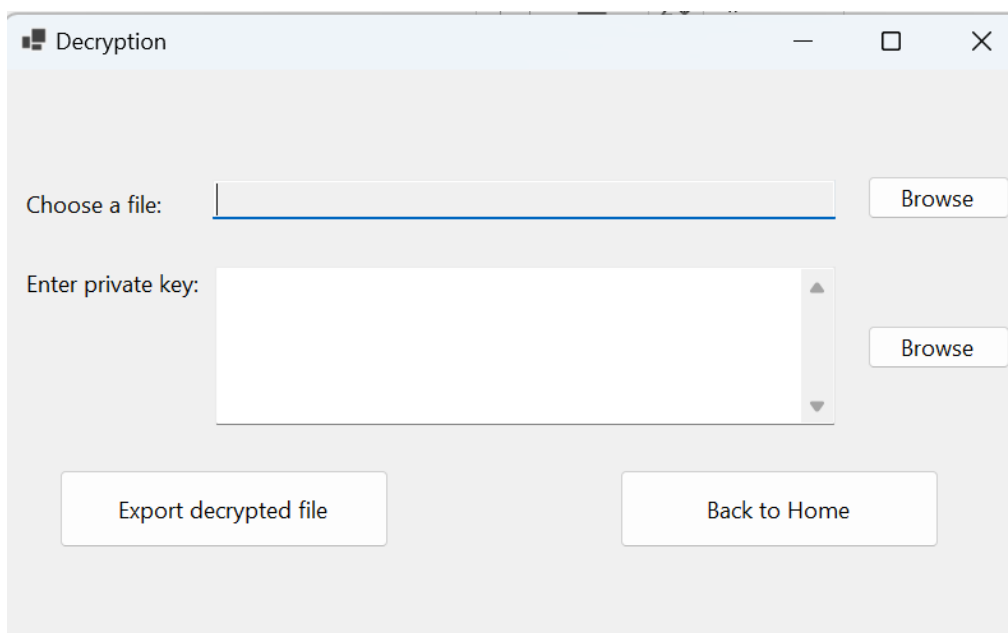


- Hệ thống sẽ tự động tạo ra một file với cấu trúc tên <tên file gốc> \_info.txt để lưu các thông tin gồm: Kx, Hkprivate, IV (để giải mã AES), định dạng của file gốc (tiện cho việc giải mã).

- Nhấn nút “Back to Home” để quay lại màn hình chính

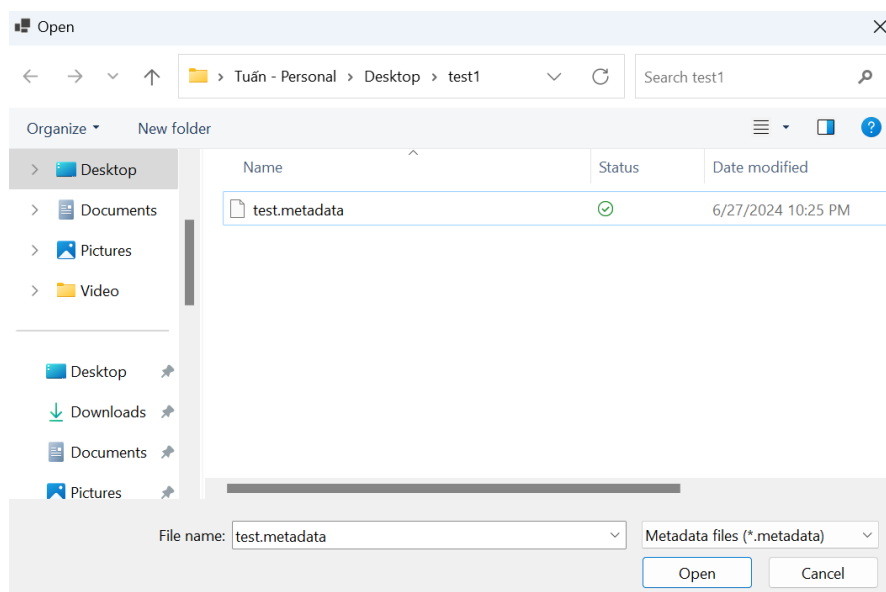
### 4.3. Màn hình giải mã

- Khi người dùng chọn chức năng Decryption thì cửa sổ giải mã sẽ hiển thị:



- Các bước sử dụng:

- Nhấn Browse để chọn file .metadata cần giải mã:





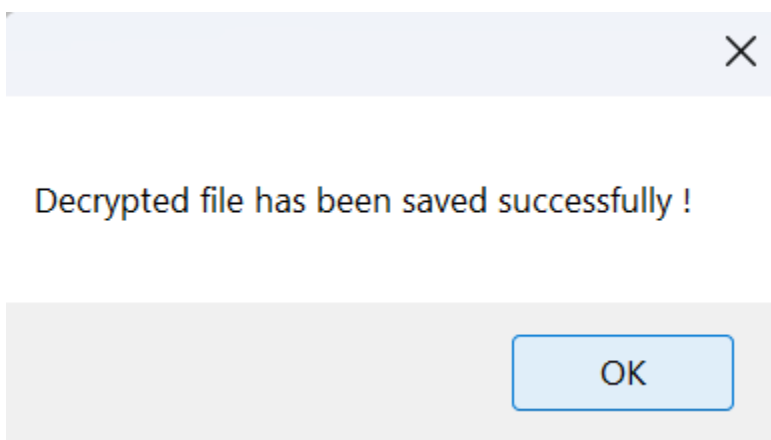
- Sau đó người dùng có thể nhập khóa bí mật hoặc chọn từ file:

Decryption

Choose a file:

Enter private key:

- Chọn nút “Export decrypted file” để tiến hành giải mã, sau khi giải mã thành công thì hệ thống sẽ hiển thị thông báo:



- File sau khi giải mã sẽ có cấu trúc tên là <tên file gốc>\_decrypted.<định dạng file gốc>:

Name	Status	Date modified	Type	Size
key.txt	✓	6/27/2024 10:22 PM	Text Document	2 KB
test.metadata	✓	6/27/2024 10:25 PM	METADATA File	157 KB
test.pdf	✓	6/26/2024 3:46 PM	Microsoft Edge PDF ...	157 KB
test_decrypted.pdf	✓	6/27/2024 10:55 PM	Microsoft Edge PDF ...	157 KB

## 5. Khó khăn gặp phải và giải pháp

### 5.1. Mã hóa file bằng AES

- Vấn đề 1: Hệ thống cần lưu lại IV để dùng cho việc giải mã  
→ Giải pháp: Lưu IV cùng với Hkprivate và Kx ra file và đặt mặc định ở Desktop máy tính của người dùng.
- Vấn đề 2: Mã hóa file. Mã hóa file có cấu trúc phức tạp hơn chứ không chỉ mỗi file text  
→ Giải pháp: sử dụng FileStream để đọc nội dung nhị phân của file, sau đó dùng CryptoStream để mã hóa luồng dữ liệu gốc.

### 5.2. Mã hóa chuỗi bằng RSA

- Dịch vụ mã hoá – giải mã RSA của thư viện Cryptography trong C# không hỗ trợ xử lý trên một chuỗi ký tự nên cần chuyển chuỗi ký tự sang một dãy byte.
- Kết quả sau khi mã hoá – giải mã một chuỗi byte là một chuỗi byte khác.
- Để chuyển bản mã về dạng một chuỗi gồm những ký tự mà người dùng có biết, ta chuyển bản mã về dạng chuỗi base-64.
- Để chuyển bản rõ sau khi giải mã về dạng một chuỗi gồm những ký tự mà người dùng có biết, ta chuyển bản rõ về dạng mã UTF8.

## Tài liệu tham khảo

[1] “cryptography - C# RSA encryption/decryption with transmission.” Stack Overflow, 15 June 2013, <https://stackoverflow.com/questions/17128038/c-sharp-rsa-encryption-decryption-with-transmission>.

[2] “How can I use AES to encrypt files other than text files? PDF, Word, etc.” Stack Overflow, 02 May 2021, <https://stackoverflow.com/questions/67360063/how-can-i-use-aes-to-encrypt-files-other-than-text-files-pdf-word-etc/67360248#67360248>

[3] “Aes class”, [Aes Class \(System.Security.Cryptography\) | Microsoft Learn](#)