

TRƯỜNG ĐẠI HỌC NGOẠI NGỮ - TIN HỌC  
THÀNH PHỐ HỒ CHÍ MINH  
KHOA CÔNG NGHỆ THÔNG TIN



**BÁO CÁO**  
**KẾT THÚC HỌC PHẦN HỌC KỲ I**  
**NĂM HỌC 2023-2024**

**MÔN HỌC: BẢO MẬT HỆ THỐNG THÔNG TIN**

# **PHẦN MỀM MÃ HOÁ VĂN BẢN TIẾNG VIỆT**

Giảng viên hướng dẫn : ThS. Phạm Đức Thành

Sinh viên thực hiện: Cao Thế Anh – 21DH113179

Lê Nguyễn Hồng Phúc – 21DH113995

Trương Văn Quốc Thắng – 21DH114133

*Thành Phố Hồ Chí Minh, tháng 11 năm 2023*



## MỤC LỤC

MỤC LỤC .....	1
DANH MỤC HÌNH .....	3
Chương I. Giới thiệu đề tài .....	4
I.1. Giới thiệu .....	4
I.1.1. Mở đầu .....	4
I.1.2. Lý do chọn đề tài .....	4
I.2. Khảo sát thực tế .....	5
I.2.1. Các ứng dụng cụ thể .....	5
I.2.2. Một quy trình cụ thể .....	10
I.2.3. Các chức năng dự kiến của đề tài .....	12
I.2.4. Công nghệ sử dụng .....	13
I.2.5. Phạm vi giới hạn .....	13
I.2.6. Bố cục đề tài .....	13
Chương II. Cơ sở lý thuyết .....	14
II.1. Lý thuyết về bảo mật thông tin .....	14
II.1.1. Khái niệm cơ bản về hệ thống thông tin .....	14
II.1.2. Các phương pháp bảo mật thông tin trong hệ thống thông tin .....	15
II.1.3. Thiết lập các biện pháp an toàn hệ thống thông tin .....	15
II.2. Ngôn ngữ lập trình và cài đặt môi trường .....	16
II.2.1. Tổng quan về Python .....	16
II.2.2. PyQt5 Designer .....	18
Chương III. Phân tích và thiết kế .....	20
III.1. Phân tích .....	20
III.1.1. Sơ đồ chức năng .....	20
III.1.2. Usecase Diagram .....	21
III.2. Thiết kế giao diện .....	21
III.2.1. Wireframe giao diện màn hình chính .....	21
III.2.2. Wireframe giao diện màn hình đăng nhập .....	22
III.2.3. Wireframe giao diện màn hình đăng ký .....	23
III.2.4. Wireframe giao diện màn hình menu .....	23
III.2.5. Wireframe giao diện màn hình các phương pháp Mã hóa Ceasar .....	24

---

III.2.6. Wireframe giao diện màn hình các phương pháp Mã hóa Trithemius .....	25
III.2.7. Wireframe giao diện màn hình các phương pháp Giải mã với chuyển vị 2 dòng .....	26
III.2.8. Wireframe giao diện màn hình các phương pháp Giải mã với chuyển vị nhiều dòng.....	27
III.3. Thiết kế xử lí: .....	28
Chương IV. Kết luận.....	29
IV.1. Kết quả đạt được.....	29
IV.1.1. Màn hình giao diện chính.....	29
IV.1.2. Màn hình đăng nhập.....	30
IV.1.3. Màn hình đăng ký .....	31
IV.1.4. Màn hình menu .....	32
IV.1.5. Màn hình xử lý mã hoá .....	33
IV.1.6. Màn hình xử lý giải mã .....	35
IV.2. Hạn chế của đề tài .....	36
IV.3. Hướng phát triển.....	37
Tài liệu tham khảo .....	38
Bảng phân công công việc.....	39

**DANH MỤC HÌNH**

Hình I.2- 1: Phần mềm VeraCrypt.....	5
Hình I.2- 2: Phần mềm Cryptomator.....	7
Hình I.2- 4: Phần mềm Cleopatra.....	8
Hình I.2- 5: Phần mềm TMS Cryptography Pack.....	9
Hình I.2- 6: Hình minh họa Text Encryption Tool.....	10
Hình I.2- 7: Hình minh họa Text Encryption Tool.....	11
Hình I.2- 8: Hình minh họa Text Encryption Tool.....	11
Hình I.2- 9: Hình minh họa Text Encryption Tool.....	12
Hình I.2- 10: Hình minh họa Text Encryption Tool.....	12
Hình III.1 - 1: Sơ đồ chức năng.....	20
Hình III.1 - 2: UseCase Diagram.....	21
Hình III.2 - 1: Wireframe giao diện màn hình trang chủ.....	21
Hình III.2 - 2: Wireframe giao diện màn hình đăng nhập.....	22
Hình III.2 - 3: Wireframe giao diện màn hình đăng ký.....	23
Hình III.2 - 4: Wireframe giao diện màn hình menu.....	24
Hình III.2 - 5: Wireframe giao diện màn hình Mã hóa Ceasar.....	24
Hình III.2 - 6: Wireframe giao diện màn hình Mã hóa Trithemius.....	25
Hình III.2 - 7: Wireframe giao diện màn hình Giải mã với chuyển vị 2 dòng.....	26
Hình III.2 - 8: Wireframe giao diện màn hình Giải mã với chuyển vị nhiều dòng.....	27
Hình IV.1 - 1: Màn hình giao diện chính.....	29
Hình IV.1 - 2: Màn hình đăng nhập.....	30
Hình IV.1 - 3: Màn hình đăng ký.....	31
Hình IV.1 - 4: Màn hình Menu.....	32
Hình IV.1 - 5: Màn hình xử lý Mã hóa với Ceasar.....	33
Hình IV.1 - 6: Màn hình xử lý Mã hóa với Trithemius.....	34
Hình IV.1 - 7: Màn hình xử lý giải mã phương pháp Chuyển vị 2 dòng.....	35
Hình IV.1 - 8: Màn hình xử lý giải mã phương pháp Chuyển vị nhiều dòng.....	36

## Chương I. Giới thiệu đề tài

### I.1. Giới thiệu

#### I.1.1. Mở đầu

Trong thời đại của công nghệ thông tin và việc sử dụng mạng Internet phổ biến, việc bảo vệ thông tin cá nhân và dữ liệu trở nên cực kỳ quan trọng. Mã hóa văn bản là một công cụ hiệu quả để đảm bảo tính bảo mật của thông tin. Nó biến đổi văn bản gốc thành một dạng không thể đọc được nếu không biết cách giải mã. Mã hóa thông tin đã tồn tại từ lâu với nhiều thuật toán và phương pháp mã hóa khác nhau.

Với sự phát triển của ngôn ngữ kỹ thuật và việc truyền thông qua Internet, việc xây dựng một phần mềm mã hóa văn bản trở thành một nhiệm vụ quan trọng. Nó giúp bảo vệ thông tin cá nhân của cá nhân và tổ chức khỏi sự xâm nhập trái phép. Trong bối cảnh ngôn ngữ tiếng Việt, việc xây dựng phần mềm mã hóa văn bản tiếng Việt trở nên cực kỳ cần thiết để đáp ứng nhu cầu trong lĩnh vực này.

Đề tài "Xây dựng phần mềm mã hóa văn bản tiếng Việt với các thuật toán cổ điển" ra đời để giải quyết vấn đề bảo vệ thông tin cá nhân và dữ liệu bằng cách cung cấp một công cụ mã hóa văn bản đáng tin cậy trong ngôn ngữ tiếng Việt. Chúng ta sẽ khám phá và phát triển các thuật toán mã hóa cổ điển như Caesar, Vigenère và Substitution để tạo ra một phần mềm mã hóa văn bản đa dạng và hiệu quả. Điều này sẽ giúp người dùng mã hóa và giải mã văn bản tiếng Việt một cách an toàn, đặc biệt trong việc truyền thông qua mạng Internet và lưu trữ dữ liệu trên các thiết bị điện tử.

Chúng ta sẽ đi sâu vào nghiên cứu và phát triển phần mềm này, từ việc triển khai các thuật toán cổ điển đến thiết kế giao diện người dùng thân thiện. Chúng ta cũng sẽ đánh giá hiệu suất của phần mềm và đề xuất hướng phát triển trong tương lai để đảm bảo tính linh hoạt và hiệu quả của nó.

Với mục tiêu này, chúng ta mong muốn đóng góp vào việc bảo vệ thông tin và đảm bảo tính riêng tư trong thế giới số hóa ngày càng phát triển. Phần tiếp theo của luận văn sẽ đi vào chi tiết về các khái niệm cơ bản của mã hóa văn bản và các thuật toán cổ điển, cùng với quá trình phát triển phần mềm và đánh giá hiệu suất của nó.

#### I.1.2. Lý do chọn đề tài

- **Bảo vệ thông tin cá nhân và dữ liệu:**

Trong thời đại số hóa ngày càng phát triển, thông tin cá nhân và dữ liệu trở nên dễ dàng tiếp cận và tiềm ẩn nguy cơ bị xâm nhập. Việc xây dựng phần mềm mã hóa văn bản là một cách quan trọng để đảm bảo rằng thông tin quan trọng của cá nhân và tổ chức được bảo vệ.

- **Yêu cầu đặc biệt cho tiếng Việt:**

Tiếng Việt là ngôn ngữ chính thống tại Việt Nam, và việc sử dụng phần mềm mã hóa văn bản tiếng Việt đặc biệt quan trọng. Các phần mềm mã hóa tiếng Việt cung cấp sự linh hoạt và tiện lợi cho người dùng trong việc bảo vệ thông tin.

- **Giới thiệu các thuật toán cổ điển:**

Việc sử dụng các thuật toán cổ điển như Caesar, Vigenère và Substitution là một cách để tạo sự đa dạng và tăng tính bảo mật trong mã hóa văn bản. Các thuật toán này đã tồn tại trong lịch sử mã hóa và vẫn có giá trị trong việc bảo vệ thông tin.

- **Nhu cầu trong lĩnh vực an ninh thông tin:**

An ninh thông tin là một lĩnh vực ngày càng quan trọng, và việc xây dựng phần mềm mã hóa văn bản là một phần quan trọng trong việc đảm bảo tính an toàn của thông tin và dữ liệu trong môi trường số hóa.

- **Đóng góp cho cộng đồng kỹ thuật:**

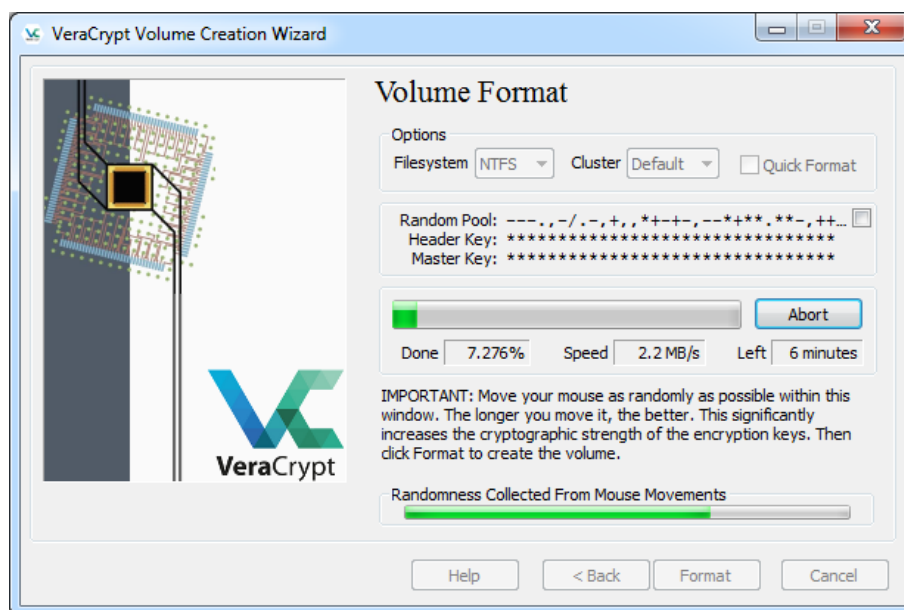
Việc nghiên cứu và phát triển phần mềm mã hóa văn bản là một cách để đóng góp cho cộng đồng kỹ thuật, cung cấp một công cụ hữu ích cho những người cần mã hóa thông tin tiếng Việt.

*Vì những lý do trên, đề tài này trở nên quan trọng và cần thiết trong việc bảo vệ thông tin và đáp ứng nhu cầu ngày càng cao về an ninh thông tin trong môi trường số hóa.*

## I.2. Khảo sát thực tế

### I.2.1. Các ứng dụng cụ thể

➤ *Phần mềm VeraCrypt*



Hình I.2- 1: Phần mềm VeraCrypt

❖ Thông tin lưu trữ:

**Container và Phân Vùng:**

- VeraCrypt tạo ra các "container" hoặc "phân vùng ảo" để chứa dữ liệu đã mã hóa.
- Các container này thường là các tập tin có kích thước cố định và được đặt mật khẩu để bảo vệ.

**Header Mã Hóa:**

- Mỗi container hoặc phân vùng được liên kết với một phần header chứa thông tin về cách dữ liệu đã mã hóa.
- Header bao gồm thông tin như thuật toán mã hóa sử dụng, kích thước container, và các thông tin xác thực.

**Bảng Mã Hóa:**

- Bảng mã hóa chứa danh sách các phần tử được mã hóa trong container và thông tin về cách chúng được tổ chức.
- Nó giúp VeraCrypt xác định vị trí và cách thức để truy xuất dữ liệu đã mã hóa trong container.

❖ Có những chức năng:

**Mã Hóa Toàn Bộ Hệ Thống:**

- VeraCrypt hỗ trợ mã hóa toàn bộ ổ đĩa, bao gồm cả hệ thống và các dữ liệu lưu trữ.
- Việc này giúp bảo vệ dữ liệu ngay cả khi hệ điều hành khởi động.

**Mã Hóa Phân Vùng và Ổ Đĩa Ngoại Vi:**

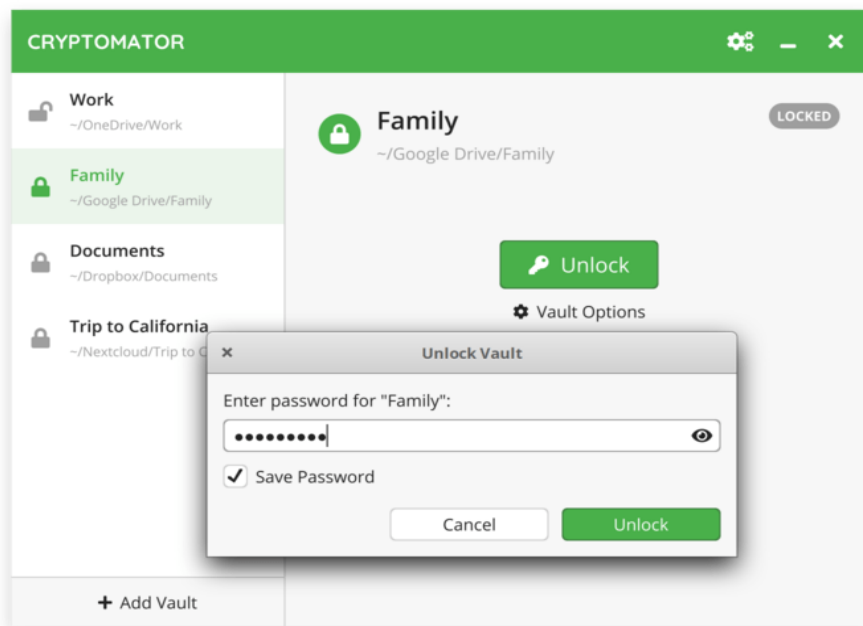
- Có khả năng tạo và quản lý các phân vùng mã hóa trên ổ đĩa hoặc thiết bị lưu trữ ngoại vi như USB và ổ đĩa di động.
- VeraCrypt tạo ra "container" để chứa dữ liệu mã hóa trên các ổ đĩa đã tồn tại.

**Mã Hóa File và Thư Mục:**

- VeraCrypt cung cấp khả năng mã hóa các file và thư mục cụ thể, không cần mã hóa toàn bộ ổ đĩa.
- Điều này cho phép người dùng chỉ mã hóa các phần cần thiết của dữ liệu.



➤ **Phần mềm Cryptomator**



Hình I.2- 2: Phần mềm Cryptomator

❖ Thông tin lưu trữ:

**Master Key và Master Password:**

- Một master key (khóa chính) được tạo ra khi bạn tạo một "vault" (kho chứa) mới trong Cryptomator.
- Master key được mã hóa bằng mật khẩu chính mà bạn xác định.

**Vault (Kho Chứa):**

- Mỗi kho chứa là một thư mục ảo chứa tất cả các tệp và thư mục đã được mã hóa.
- Thư mục và tệp trong kho chứa có thể được quản lý và truy cập như bất kỳ thư mục nào khác.

**Kết Hợp với Dịch Vụ Lưu Trữ Đám Mây:**

- Cryptomator tích hợp trực tiếp với các dịch vụ đám mây phổ biến như Google Drive, Dropbox, OneDrive, và nhiều dịch vụ khác.
- Dữ liệu đã mã hóa được lưu trữ trong các thư mục của dịch vụ đám mây.

❖ Có những chức năng:

**Mã Hóa Dữ Liệu:** Cryptomator mã hóa dữ liệu trước khi lưu trữ nó, đảm bảo rằng dữ liệu chỉ có thể được đọc khi được giải mã.

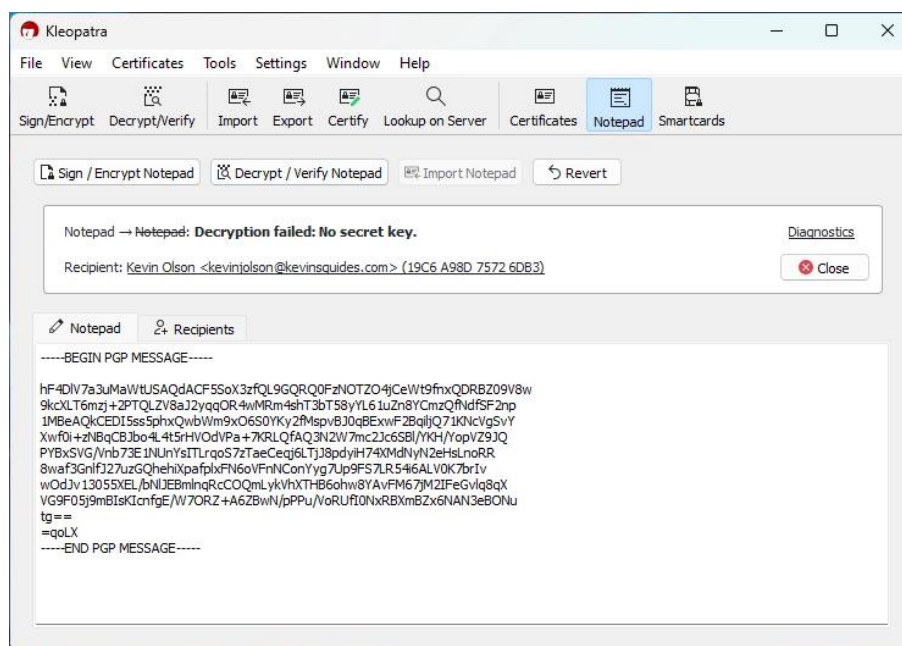
## Mã Hóa Tập và Thư Mục Riêng Biệt:

- Mỗi tập và thư mục trong kho chứa có khóa riêng biệt để tăng cường bảo mật.
- Điều này có nghĩa là thậm chí khi một tập hoặc thư mục bị tấn công, dữ liệu khác vẫn an toàn.

**Tạo Nhiều Vaults:** Người dùng có thể tạo nhiều "vaults" để phân loại và quản lý dữ liệu theo nhóm hoặc mục đích cụ thể.

**Khả Năng Đồng Bộ Dữ Liệu:** Cryptomator không quản lý chức năng đồng bộ hóa dữ liệu, nhưng nó hỗ trợ sự kết hợp với các dịch vụ đám mây để quản lý đồng bộ hóa.

### ➤ *Cleopatra:*



Hình I.2- 3: Phần mềm Cleopatra

### ❖ Thông tin lưu trữ:

**Khóa Mã Hóa và Khóa Ký Số:** Cleopatra hiển thị và quản lý khóa mã hóa và khóa ký số của bạn. Tuy nhiên, thông tin này thực sự được lưu trữ trong hệ thống tệp của GnuPG.

**Sự Kiện và Log:** Cleopatra cũng có thể hiển thị các sự kiện và log liên quan đến các hoạt động mã hóa và xác thực. Thông tin này thường được GnuPG lưu trữ trong các tệp log của nó.

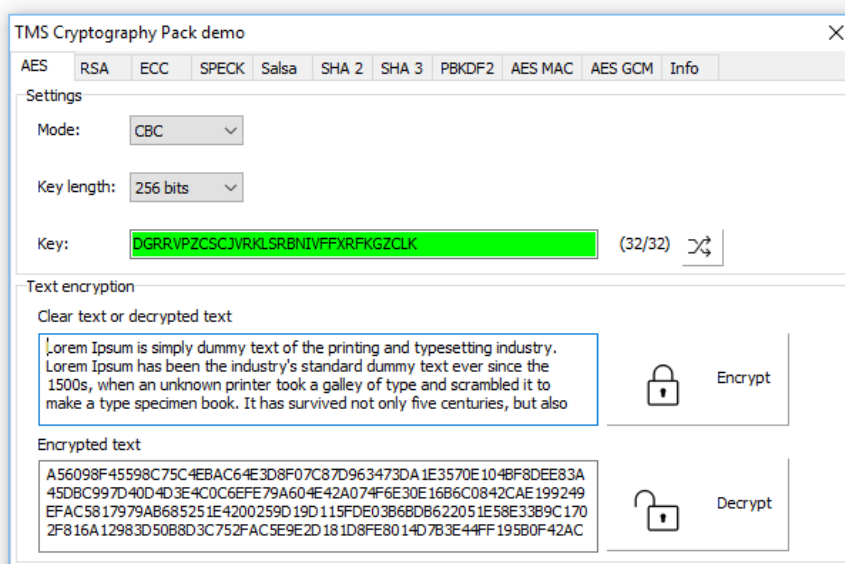
❖ Có những chức năng:

**Quản lý Khóa:** Cleopatra cho phép người dùng tạo mới, xem, xuất, nhập, và quản lý các khóa mã hóa và ký số. Bạn có thể tạo cặp khóa mới, xem thông tin về khóa hiện tại, và thực hiện các hoạt động quản lý khóa.

**Tạo Cặp Khóa:** Cleopatra hỗ trợ quá trình tạo cặp khóa mới, bao gồm cả việc chọn thuật toán mã hóa và cung cấp thông tin khác như tên và email.

**Xác Nhận Khóa:** Người dùng có thể xác nhận tính xác thực của khóa công khai của người khác bằng cách ký số hoặc sử dụng các tính năng xác thực khác.

**Mã Hóa và Giải Mã Tập Tin:** Cleopatra cho phép bạn mã hóa và giải mã tập tin bằng cách sử dụng khóa mã hóa của bạn. Điều này giúp bảo vệ dữ liệu của bạn bằng cách sử dụng mã hóa mạnh mẽ.

➤ *TMS Cryptography Pack:*

Hình I.2- 4: *Phạm mềm TMS Cryptography Pack*

❖ Thông tin lưu trữ:

**Khóa và Chứng Thục:** Dữ liệu liên quan đến khóa và chứng thực có thể được lưu trữ an toàn để đảm bảo tính toàn vẹn và an toàn của chúng.

**Cài Đặt và Tùy Chọn:** Thông tin về cài đặt và tùy chọn của TMS Cryptography Pack có thể được lưu trữ để duy trì cấu hình của ứng dụng.

**Metadata Bảo Mật:** Nếu TMS Cryptography Pack hỗ trợ bảo vệ metadata, thông tin liên quan đến dữ liệu có thể được lưu trữ an toàn.

**Dữ Liệu Ngẫu Nhiên:** Nếu có tính năng tạo dữ liệu ngẫu nhiên, thông tin liên quan đến quá trình tạo và quản lý dữ liệu ngẫu nhiên có thể được lưu trữ.

❖ Có những chức năng:

**Mã Hóa và Giải Mã Dữ Liệu:** Cung cấp khả năng mã hóa và giải mã dữ liệu sử dụng các thuật toán mã hóa mạnh mẽ.

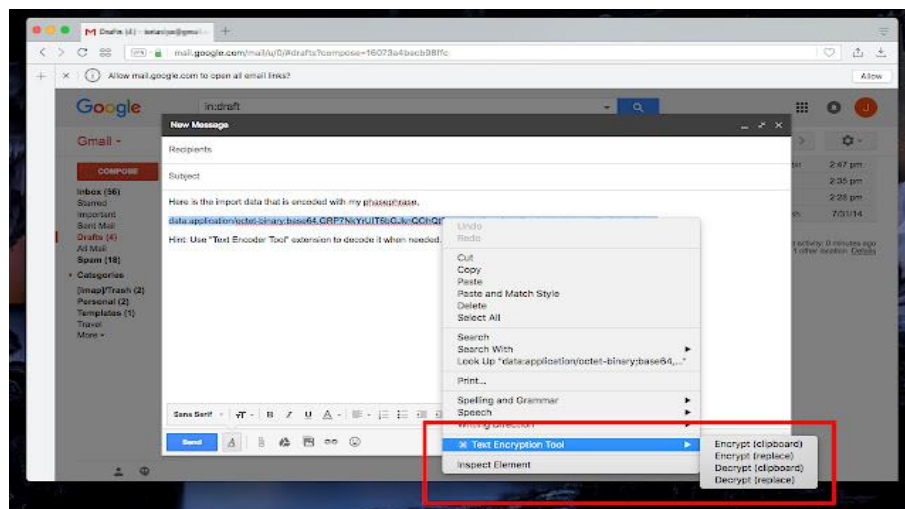
**Chữ Ký Số và Xác Minh:** Hỗ trợ tạo và xác minh chữ ký số, giúp đảm bảo tính toàn vẹn và nguồn gốc của dữ liệu.

**Quản Lý Khóa:** Cung cấp các chức năng quản lý khóa, bao gồm cả sinh khóa và quản lý chuỗi khóa.

**Bảo vệ Dữ Liệu Tại Mức Địa Phương (Local Data Protection):** Các chức năng bảo vệ dữ liệu tại mức địa phương, giúp đảm bảo an toàn dữ liệu lưu trữ trên các thiết bị.

### I.2.2. Một quy trình cụ thể

### ❖ Sử dụng Text Encryption Tool mã hóa văn bản



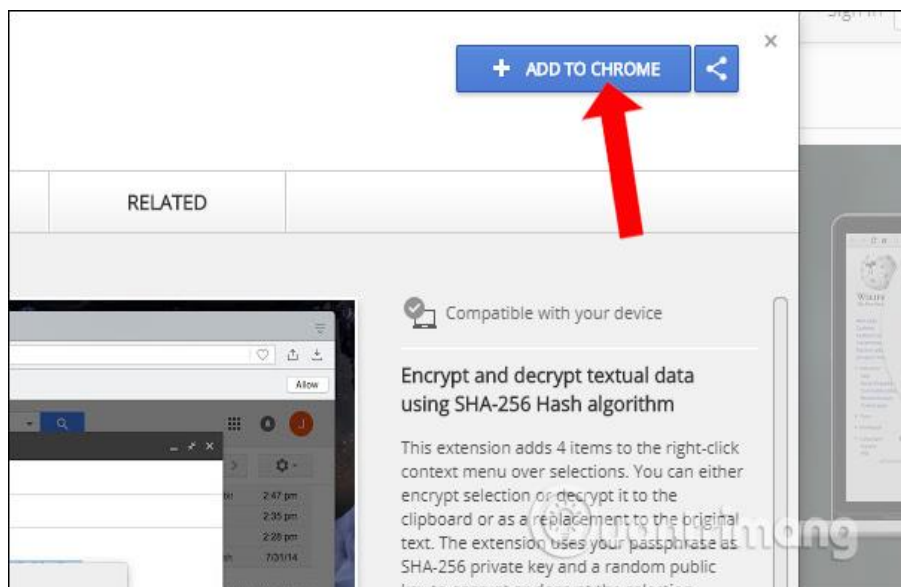
Hình I.2- 5: Hình minh họa Text Encryption Tool

### Mã hoá và giải mã đoạn văn bản:

### Bước 1:

Text Encryption Tool có thể cài đặt trên Google Chrome và Firefox. Nhấp vào link dưới đây để cài đặt tiện ích trên trình duyệt.

- Tải tiện ích [Text Encryption Tool Chrome](#)
- Tải tiện ích [Text Encryption Tool Firefox](#)



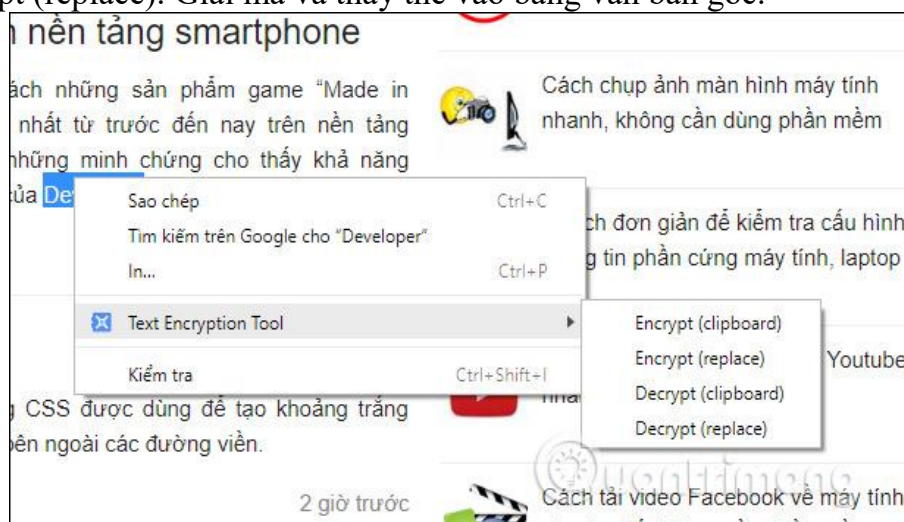
Hình I.2- 6: Hình minh họa Text Encryption Tool

### Bước 2:

Tiếp đến người dùng bôi đen đoạn văn bản muốn tiến hành mã hóa nội dung rồi click chuột phải. Chúng ta sẽ thấy tùy chọn mới Text Encryption Tool để sử dụng. Trong tùy chọn này bạn sẽ được lựa chọn chức năng mã hóa mà mình muốn.

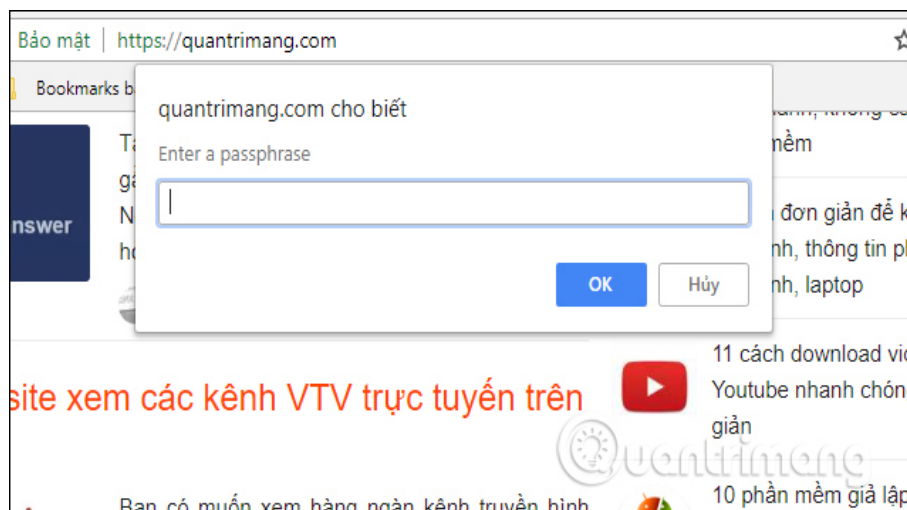
Sẽ có 2 tùy chọn khác nhau với mục đích mã hóa và giải mã dữ liệu khác nhau.

- Encrypt (clipboard): Mã hóa văn bản và sao chép vào clipboard, thông qua mật khẩu bảo mật.
- Encrypt (replace): Mã hóa và thay thế đoạn văn bản này.
- Decrypt (clipboard): Giải mã văn bản và sao chép nội dung văn bản gốc vào bộ nhớ đệm. Bạn nhập mật khẩu bảo vệ sau khi chọn.
- Decrypt (replace): Giải mã và thay thế vào bằng văn bản gốc.



Hình I.2- 7: Hình minh họa Text Encryption Tool

- Xuất hiện giao diện nhập mật khẩu bảo mật dữ liệu. Nhập mật khẩu rồi nhấn OK.



Hình I.2- 8: Hình minh họa Text Encryption Tool

### Bước 3:

Văn bản sau khi được mã hóa sẽ hiển thị dãy mã hóa như hình dưới đây.



Hình I.2- 9: Hình minh họa Text Encryption Tool

Để giải mã người nhận cũng phải sử dụng công cụ Text Encryption Tool và biết mật khẩu bạn đã đặt. Sau đó cũng bôi đen vào dãy ký tự trên chọn chuột phải rồi chọn phương thức giải mã ứng với cách thức mã hóa đã sử dụng.

Chúng ta có thể sử dụng Text Encryption Tool với nhiều trình soạn thảo khác nhau như soạn email, thực hiện trên trang web,... Tuy nhiên hiện tại Text Encryption Tool mới chỉ áp dụng giải mã cho các văn bản tiếng Anh. Với văn bản tiếng Việt sẽ có hiện tượng lỗi font chữ.

#### I.2.3. Các chức năng dự kiến của đề tài

- Đọc file và lưu file
- Mã hóa và giải mã các thuật toán cổ điển – hiện đại như:

- Dạng mã hóa thay thế gồm: Caesar, Belasco, Trithemius, Vgnere
- Dạng mã hóa chuyển vị gồm: chuyển vị 2 dòng và chuyển vị nhiều dòng
- Dạng mã hóa theo Xor gồm: Caesar, Belasco, Trithemius, Vgnere
- Dạng mã hoá theo DES
- Dạng mã hoá theo RSA
- Dạng mã hóa một chiều như MD5, SHA-256, SHA-3

#### **I.2.4. Công nghệ sử dụng**

- Qt Designer
- Python
- PyQt5
- Figma

#### **I.2.5. Phạm vi giới hạn**

Đề tài tổng hợp các lý thuyết cơ bản về bảo mật thông tin, các phương pháp mã hoá cổ điển và hiện đại. Phần Demo đề tài sử dụng ngôn ngữ Python để triển khai, chương trình sẽ thực hiện việc đọc các file, mã hoá và giải mã các kí tự tiếng việt và các kí tự đặc biệt trong bộ kí tự của Character Map, đồng thời là lưu lại các file. Các phương pháp mã hoá và giải mã trong đề tài được giới hạn trong các phương pháp mã hoá cổ điển – hiện đại như mã hoá thay thế, mã hoá chuyển vị, mã hoá theo Xor, mã hoá DES, mã hoá RSA và các phương pháp mã hóa một chiều có tính bảo mật cao như MD5, SHA-256, SHA-3

#### **I.2.6. Bố cục đề tài**

- Chương I: Giới thiệu đề tài
- Chương II: Cơ sở lý thuyết
- Chương III: Phân tích và thiết kế
- Chương IV: Kết luận



## Chương II. Cơ sở lý thuyết

### II.1. Lý thuyết về bảo mật thông tin

#### II.1.1. Khái niệm cơ bản về hệ thống thông tin

Hệ thống thông tin là một khái niệm quan trọng trong lĩnh vực khoa học máy tính và quản lý. Nó thường ám chỉ một tập hợp các thành phần, phần mềm, dữ liệu, quy trình và nguồn lực được tổ chức và tương tác với nhau để thu thập, lưu trữ, xử lý, truyền tải và truy cập thông tin trong một môi trường cụ thể. Hệ thống thông tin đóng một vai trò quan trọng trong nhiều khía cạnh của cuộc sống hiện đại, từ quản lý doanh nghiệp và tổ chức cho đến lĩnh vực giáo dục, y tế, và công nghệ thông tin. Quản lý thông tin hiệu quả đảm bảo rằng thông tin được xử lý, lưu trữ và truyền tải một cách an toàn và có hiệu suất cao để đáp ứng nhu cầu của các tổ chức và cá nhân. Dưới đây là các khái niệm cơ bản liên quan đến hệ thống thông tin:

- + Thông tin: Thông tin là dữ liệu đã qua xử lý để có ý nghĩa và giá trị. Nó có thể bao gồm văn bản, hình ảnh, âm thanh, số liệu, hoặc bất kỳ dạng dữ liệu nào có thể truyền đạt kiến thức hoặc tin tức.
- + Hệ thống: Hệ thống tin là tổ hợp các thành phần, chức năng và quy trình cùng hoạt động để quản lý thông tin. Điều này có thể bao gồm phần cứng máy tính, phần mềm, con người, quy trình và dữ liệu.
- + Phần mềm hệ thống thông tin: Là tập hợp các chương trình và ứng dụng máy tính được thiết kế để xử lý, lưu trữ và quản lý thông tin. Nó bao gồm các ứng dụng doanh nghiệp, hệ thống quản lý cơ sở dữ liệu, phần mềm giao diện người dùng, và nhiều ứng dụng khác.
- + Phần cứng hệ thống thông tin: Là các thành phần vật lý của hệ thống, bao gồm máy tính, máy chủ, thiết bị lưu trữ, mạng, và các thiết bị ngoại vi. Phần cứng cung cấp nền tảng cho việc thực hiện các nhiệm vụ xử lý thông tin.
- + Cơ sở dữ liệu: Là một phần quan trọng trong hệ thống thông tin, cơ sở dữ liệu là nơi lưu trữ dữ liệu cấu trúc một cách hệ thống. Dữ liệu trong cơ sở dữ liệu có thể được truy cập, cập nhật và truy vấn dễ dàng.
- + Người dùng: Người dùng là những cá nhân hoặc tổ chức sử dụng hệ thống thông tin để truy cập, xử lý và quản lý thông tin. Người dùng có thể là nhân viên, khách hàng, hoặc bất kỳ ai có quyền truy cập vào hệ thống.
- + Quy trình: Là chuỗi các bước hoặc quy tắc mà hệ thống theo dõi để xử lý thông tin. Quy trình có thể bao gồm quy trình kinh doanh, quy trình xử lý dữ liệu, và các quy tắc và quy định quản lý.
- + Mạng: Là cơ sở hạ tầng liên kết tất cả các phần của hệ thống thông tin lại với nhau. Điều này cho phép thông tin di chuyển qua lại giữa các thành phần của hệ thống.
- + Bảo mật thông tin: Là việc bảo vệ thông tin quan trọng khỏi sự truy cập trái phép hoặc thay đổi. Bảo mật thông tin là một khía cạnh quan trọng của hệ thống thông tin để đảm bảo tính riêng tư và an toàn của thông tin quan trọng.



### II.1.2. Các phương pháp bảo mật thông tin trong hệ thống thông tin

Bảo mật thông tin, thường được viết tắt là InfoSec, là tập hợp các quy trình và công cụ bảo mật để bảo vệ trên diện rộng thông tin nhạy cảm của doanh nghiệp, tránh để thông tin đó bị lạm dụng, truy cập trái phép, giai đoạn hoặc phá hủy. InfoSec bao gồm bảo mật vật lý và môi trường, kiểm soát truy cập và an ninh mạng. Các phương pháp bảo mật thông tin như sau:

- **Mã hóa dữ liệu:** Mã hóa dữ liệu là quá trình biến đổi thông tin gốc thành một dạng khác sao cho chỉ có người được ủy quyền mới có thể đọc được nó. Sử dụng mã hóa, bạn có thể bảo vệ dữ liệu cả trong trạng thái lưu trữ và truyền tải.
- **Xác thực và ủy quyền:** Xác thực đảm bảo rằng người dùng hoặc hệ thống chỉ có quyền truy cập thông tin nếu họ có đủ quyền. Ủy quyền xác định loại quyền họ có, bao gồm quyền truy cập, sửa đổi, xóa, hay chỉ đọc dữ liệu.
- **Firewalls:** Firewall là một phần cứng hoặc phần mềm được sử dụng để kiểm soát lưu lượng mạng vào và ra khỏi hệ thống. Nó giúp ngăn chặn các truy cập trái phép hoặc tấn công từ bên ngoài.
- **Phân tách mạng:** Sử dụng việc phân tách mạng, bạn có thể tạo ra các mạng con riêng biệt trong hệ thống, mỗi mạng có quyền truy cập riêng và được kiểm soát độc lập. Điều này giúp hạn chế tiềm ẩn sự xâm nhập từ mạng nội bộ.
- **Cơ sở dữ liệu an toàn:** Sử dụng cơ sở dữ liệu an toàn để bảo vệ dữ liệu quan trọng. Điều này bao gồm việc thực hiện các biện pháp bảo mật như kiểm tra dữ liệu đầu vào, sử dụng quyền truy cập cơ sở dữ liệu cụ thể và sao lưu dữ liệu định kỳ.
- **Quản lý danh tính:** Đảm bảo rằng bạn quản lý danh tính người dùng một cách chặt chẽ. Điều này bao gồm việc quản lý tài khoản, mật khẩu mạnh, và chính sách thay đổi mật khẩu định kỳ.
- **Giám sát và ghi lại hoạt động:** Việc giám sát hệ thống và ghi lại các hoạt động là một phần quan trọng trong bảo mật thông tin. Nó giúp xác định các hoạt động bất thường và tấn công tiềm ẩn.
- **Chính sách và quy trình bảo mật:** Xây dựng và thực hiện các chính sách và quy trình bảo mật rõ ràng trong tổ chức để đảm bảo rằng mọi người trong tổ chức hiểu và tuân thủ các biện pháp bảo mật.
- **Mạng riêng ảo (VPN):** Sử dụng VPN cho phép người dùng truy cập mạng công nghiệp từ xa một cách an toàn và ẩn danh.
- **Kiểm tra an ninh và kiểm tra thâm nhập:** Thường xuyên kiểm tra an ninh hệ thống và thực hiện kiểm tra thâm nhập để xác định các lỗ hổng bảo mật và tìm cách khắc phục chúng.

### II.1.3. Thiết lập các biện pháp an toàn hệ thống thông tin

- **Firewall (Tường lửa):** Ngăn chặn các kết nối không mong muốn giữa mạng nội bộ và mạng ngoại vi. Có tường lửa phần cứng và phần mềm để bảo vệ cả tại mức cổng (port) và tại mức ứng dụng.
- **Mã hóa dữ liệu:** Bảo vệ thông tin bằng cách chuyển đổi nó thành dạng không đọc được nếu không có khóa giải mã. Mã hóa có thể áp dụng cho dữ liệu lưu trữ và truyền qua mạng.

- **Chính sách an ninh thông tin:** Xác định quy tắc và hướng dẫn về cách thông tin được quản lý và bảo vệ. Bao gồm cả việc quản lý mật khẩu, quyền truy cập, và các biện pháp an ninh khác.
- **Mật khẩu mạnh và quản lý mật khẩu:** Yêu cầu người dùng sử dụng mật khẩu mạnh, và triển khai các phương tiện để quản lý và bảo vệ mật khẩu, như hệ thống xác thực hai yếu tố.
- **Cập nhật và vá lỗ hổng bảo mật:** Giữ cho hệ thống luôn được cập nhật với các bản vá mới nhất để bảo vệ chống lại các lỗ hổng bảo mật tiềm ẩn.
- **Kiểm tra và giám sát liên tục:** Thực hiện kiểm tra bảo mật định kỳ để phát hiện và ngăn chặn các mối đe dọa. Hệ thống giám sát theo thời gian thực có thể cảnh báo về các hoạt động đáng ngờ.
- **Backup và phục hồi dữ liệu:** Tạo bản sao lưu định kỳ của dữ liệu quan trọng để đảm bảo khả năng phục hồi sau một sự cố.
- **Giáo dục và đào tạo người dùng:** Người dùng là một phần quan trọng trong chuỗi an ninh, nên họ cần được đào tạo để nhận biết và tránh các mối đe dọa bảo mật.
- **Quản lý rủi ro:** Đánh giá và quản lý rủi ro để xác định những điểm yếu và triển khai biện pháp bảo mật hiệu quả.
- **Quản lý và giám sát danh sách kiểm tra quy trình an ninh:** Đảm bảo rằng các biện pháp bảo mật được triển khai đúng cách và theo dõi chúng theo thời gian.

## II.2. Ngôn ngữ lập trình và cài đặt môi trường

### II.2.1. Tổng quan về Python

#### ❖ Ngôn ngữ Python

Python là ngôn ngữ lập trình máy tính bậc cao thường được sử dụng để xây dựng trang web và phần mềm, tự động hóa các tác vụ và tiến hành phân tích dữ liệu. Python là ngôn ngữ có mục đích chung, nghĩa là nó có thể được sử dụng để tạo nhiều chương trình khác nhau và không chuyên biệt cho bất kỳ vấn đề cụ thể nào.

- Các đặc điểm tạo nên sự độc đáo của ngôn ngữ lập trình Python:
- Python là một ngôn ngữ thông tin: Python là một ngôn ngữ thông dịch, điều này nghĩa là ngôn ngữ này trực tiếp chạy từng dòng mã. Nếu có lỗi trong mã chương trình, nó sẽ ngừng chạy. Do đó, lập trình viên có thể nhanh chóng tìm ra lỗi trong đoạn mã.
- Python là ngôn ngữ dễ sử dụng: Python sử dụng từ ngữ giống trong tiếng Anh. Không giống như các ngôn ngữ lập trình khác, Python không sử dụng dấu ngoặc ôm. Thay vào đó, ngôn ngữ này sử dụng thụt đầu dòng.
- Python là ngôn ngữ linh hoạt: Các lập trình viên không cần phải khai báo loại biến khi viết mã bởi vì Python sẽ xác định chúng vào thời điểm chạy. Vì vậy, bạn có thể viết các chương trình Python một cách nhanh chóng hơn.

- Python là ngôn ngữ cấp cao: Python gần gũi với ngôn ngữ con người hơn các ngôn ngữ lập trình khác. Do đó, các lập trình viên không cần phải lo lắng về những chức năng cơ bản của nó như kiến trúc và quản lý bộ nhớ.
- Python là ngôn ngữ lập trình hướng đối tượng: Python coi mọi thứ đều là đối tượng, nhưng ngôn ngữ này cũng hỗ trợ các phương thức lập trình khác như lập trình hàm và lập trình cấu trúc.

Môi trường phát triển tích hợp (IDE) là phần mềm cung cấp cho các nhà phát triển công cụ duy nhất họ cần để viết, chỉnh sửa, kiểm tra và gỡ lỗi mã. Môi trường phát triển và học hỏi tích hợp (IDLE) là Python IDE được cài đặt theo mặc định. Nó chỉ được phát triển với Python bằng bộ công cụ Tkinter GUI và cung cấp các tính năng sau:

Hoạt động trên nhiều hệ điều hành như Windows, Unix và macOS

- Cung cấp một cửa sổ shell để chạy các lệnh và hiển thị kết quả
- Cung cấp trình soạn thảo văn bản trên nhiều cửa sổ với khả năng đánh dấu cú pháp mã và hoàn thành mã tự động
- Có trình gỡ lỗi riêng

### ❖ ***Python 3.11***

Python 3.11 là phiên bản mới nhất của ngôn ngữ lập trình Python, được phát hành vào ngày 14 tháng 10 năm 2022. Phiên bản này mang đến nhiều tính năng mới và cải tiến, giúp Python trở nên mạnh mẽ và linh hoạt hơn.

#### \* **Những điểm mới đáng chú ý:**

- Hiệu suất được cải thiện đáng kể: Python 3.11 có những cải tiến đáng kể về hiệu suất, giúp các chương trình Python chạy nhanh hơn. Những cải tiến này bao gồm:
  - Sử dụng bộ đệm bộ nhớ hiệu quả hơn
  - Tối ưu hóa việc biên dịch mã
  - Sử dụng các mô hình toán học tiên tiến để tối ưu hóa thời gian chạy
- Tích hợp với thư viện NumPy và SciPy: Python 3.11 tích hợp chặt chẽ hơn với thư viện NumPy và SciPy, giúp các nhà khoa học dữ liệu và kỹ sư máy học dễ dàng sử dụng các thư viện này.
- Cải tiến về cú pháp và tính năng: Python 3.11 có một số cải tiến về cú pháp và tính năng, bao gồm:
  - Thêm các biểu thức lambda ngắn gọn hơn
  - Thêm các hàm thư viện chuẩn mới
  - Sửa một số lỗi và thiếu sót trong các phiên bản trước

#### \* **Những cải tiến về hiệu suất:**

- Python 3.11 có những cải tiến đáng kể về hiệu suất, giúp các chương trình Python chạy nhanh hơn. Những cải tiến này bao gồm:
  - Sử dụng bộ đệm bộ nhớ hiệu quả hơn: Python 3.11 sử dụng bộ đệm bộ nhớ hiệu quả hơn, giúp giảm thời gian truy cập bộ nhớ.
  - Tối ưu hóa việc biên dịch mã: Python 3.11 đã được tối ưu hóa để biên dịch mã nhanh hơn.

- Sử dụng các mô hình toán học tiên tiến để tối ưu hóa thời gian chạy: Python 3.11 sử dụng các mô hình toán học tiên tiến để tối ưu hóa thời gian chạy của các chương trình.
- Những cải tiến này giúp Python 3.11 chạy nhanh hơn từ 10% đến 60% so với Python 3.10.
- Tích hợp với thư viện NumPy và SciPy
- Python 3.11 tích hợp chặt chẽ hơn với thư viện NumPy và SciPy, giúp các nhà khoa học dữ liệu và kỹ sư máy học dễ dàng sử dụng các thư viện này.
- Python 3.11 cung cấp các hàm thư viện chuẩn mới để làm việc với NumPy và SciPy. Ngoài ra, Python 3.11 cũng cải thiện khả năng tương thích với các thư viện này.

\* **Cải tiến về cú pháp và tính năng:**

Python 3.11 có một số cải tiến về cú pháp và tính năng, bao gồm:

- Thêm các biểu thức lambda ngắn gọn hơn: Python 3.11 thêm các biểu thức lambda ngắn gọn hơn, giúp viết mã ngắn gọn và dễ hiểu hơn.
- Thêm các hàm thư viện chuẩn mới: Python 3.11 thêm các hàm thư viện chuẩn mới để hỗ trợ các tính năng mới.
- Sửa một số lỗi và thiếu sót trong các phiên bản trước: Python 3.11 sửa một số lỗi và thiếu sót trong các phiên bản trước.

\* **Kết luận:**

Python 3.11 là một phiên bản nâng cấp đáng giá của ngôn ngữ lập trình Python. Phiên bản này mang đến nhiều tính năng mới và cải tiến, giúp Python trở nên mạnh mẽ và linh hoạt hơn.

## II.2.2. PyQt5 Designer

PyQt5 Designer là một công cụ giúp bạn thiết kế giao diện đồ họa cho ứng dụng sử dụng PyQt5. PyQt5 là một giao diện Python cho toolkit đồ họa Qt, cho phép bạn tạo các ứng dụng đồ họa đa năng trên nhiều nền tảng.

**Cơ sở lý thuyết của PyQt5 Designer bao gồm:**

**Qt và PyQt5:** Qt là một toolkit đồ họa nổi tiếng và mạnh mẽ được viết bằng C++. PyQt5 là một giao diện Python cho Qt, cho phép bạn sử dụng Qt trong Python. PyQt5 cung cấp các lớp và phương thức để tạo giao diện đồ họa, xử lý sự kiện và tương tác với ứng dụng.

**Widget-based Design:** PyQt5 Designer là một công cụ thiết kế dựa trên cơ sở widget. Bạn có thể kéo và thả các widget từ thư viện widget có sẵn vào khung làm việc để tạo giao diện đồ họa. Các widget có thể là các phần tử như nút bấm, hộp văn bản, danh sách thả xuống, và nhiều loại widget khác.

**Sự kiện và kết nối:** PyQt5 Designer cho phép bạn thiết lập kết nối giữa các widget và các phương thức xử lý sự kiện trong mã Python của bạn. Điều này cho phép bạn xác định hành vi của ứng dụng khi người dùng tương tác với giao diện.

**MVC Architecture:** PyQt5 thường được xây dựng dựa trên kiến trúc Model-View-Controller (MVC). Bạn có thể sử dụng các lớp mô hình để quản lý dữ liệu ứng dụng, và thiết kế giao diện đồ họa để hiển thị và tương tác với dữ liệu này.

**Tạo mã Python:** Sau khi bạn đã thiết kế giao diện trong PyQt5 Designer, công cụ này sẽ tạo một tệp UI XML. Bạn sau đó có thể sử dụng công cụ pyuic5 để chuyển

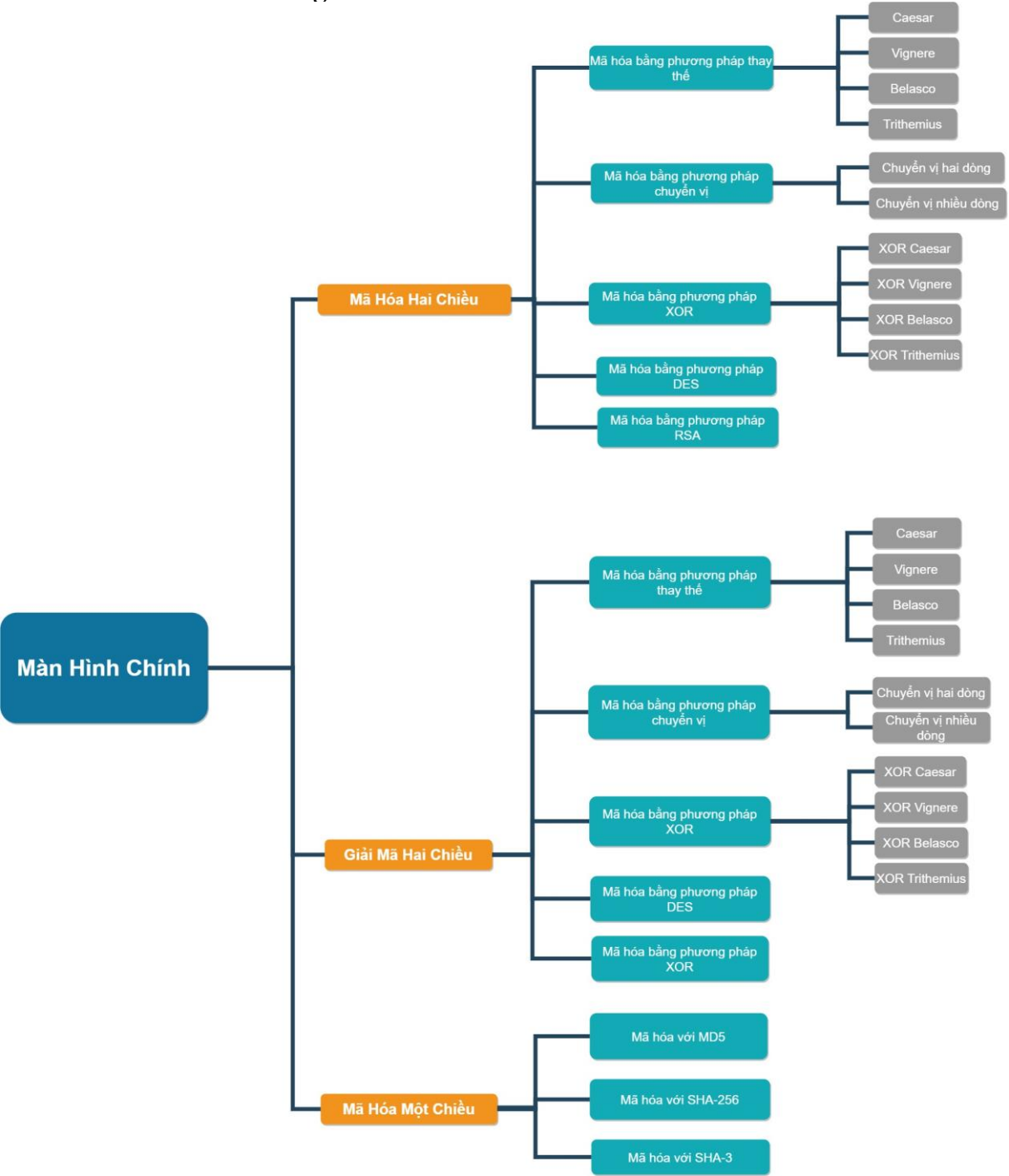
đổi tệp UI XML này thành mã Python, và sau đó sử dụng mã Python này để xây dựng ứng dụng thực tế.

PyQt5 Designer cung cấp một cách trực quan để thiết kế giao diện đồ họa cho ứng dụng của bạn mà không cần phải viết mã Python từ đầu. Nó tích hợp tốt với PyQt5, giúp bạn tiết kiệm thời gian và công sức trong việc phát triển ứng dụng đồ họa.

### Chương III. Phân tích và thiết kế

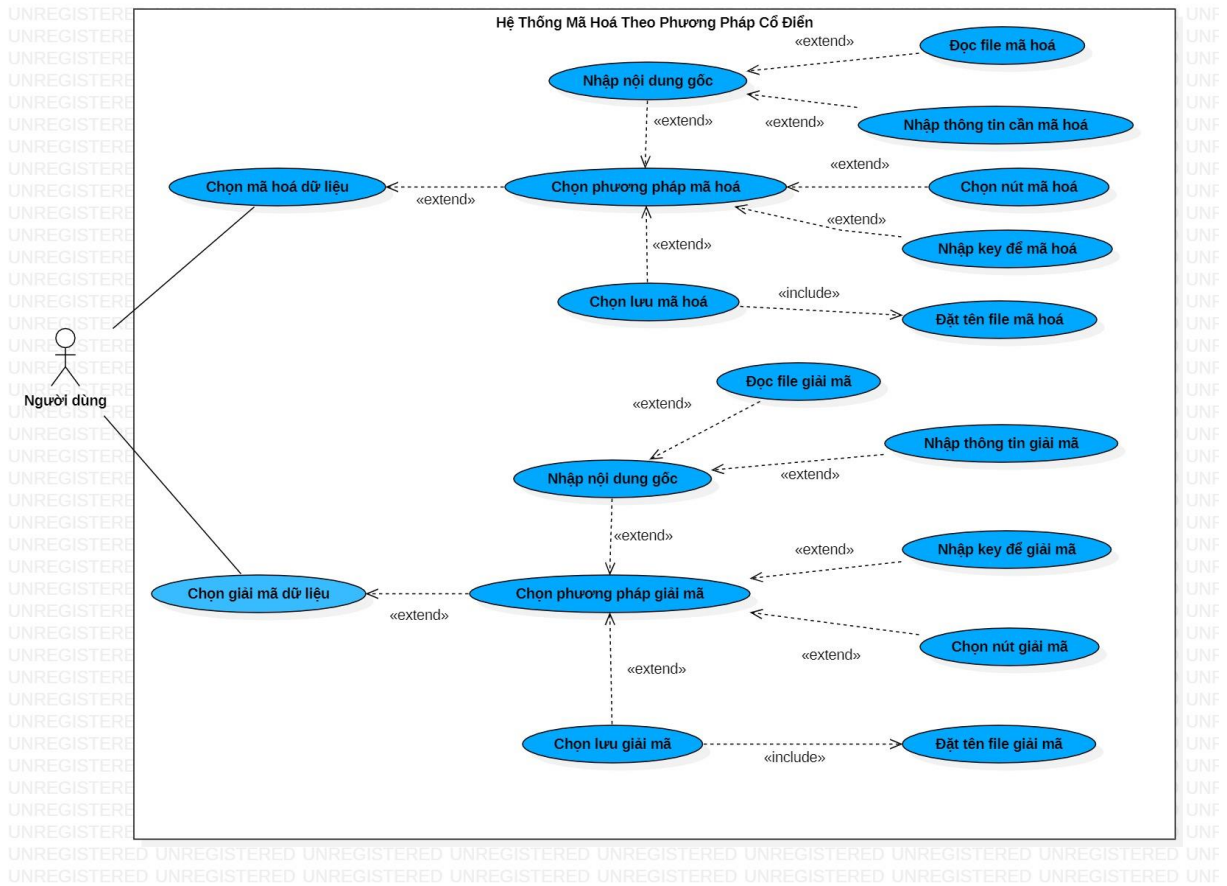
III.1. Phân tích

III.1.1. Sơ đồ chức năng



Hình III.1 - 1: Sơ đồ chức năng

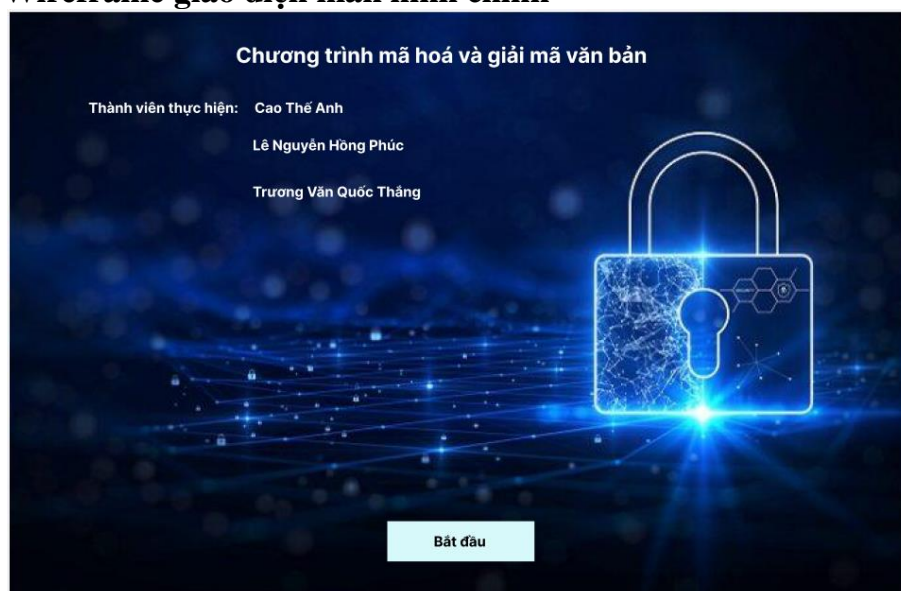
### III.1.2. Usecase Diagram



Hình III.1 - 2: UseCase Diagram

## III.2. Thiết kế giao diện

### III.2.1. Wireframe giao diện màn hình chính

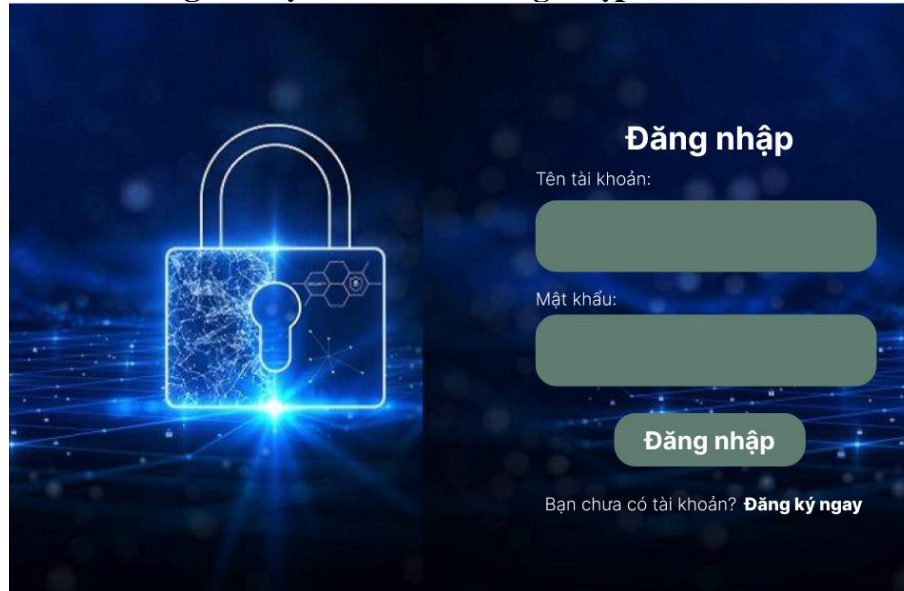


Hình III.2 - 1: Wireframe giao diện màn hình trang chủ

- Thông tin lưu trữ:
  - o Tên đề tài.

- Danh sách các thành viên.
- Nút bắt đầu.
- Chức năng:  
Mở khóa bắt đầu chương trình.

### III.2.2. Wireframe giao diện màn hình đăng nhập

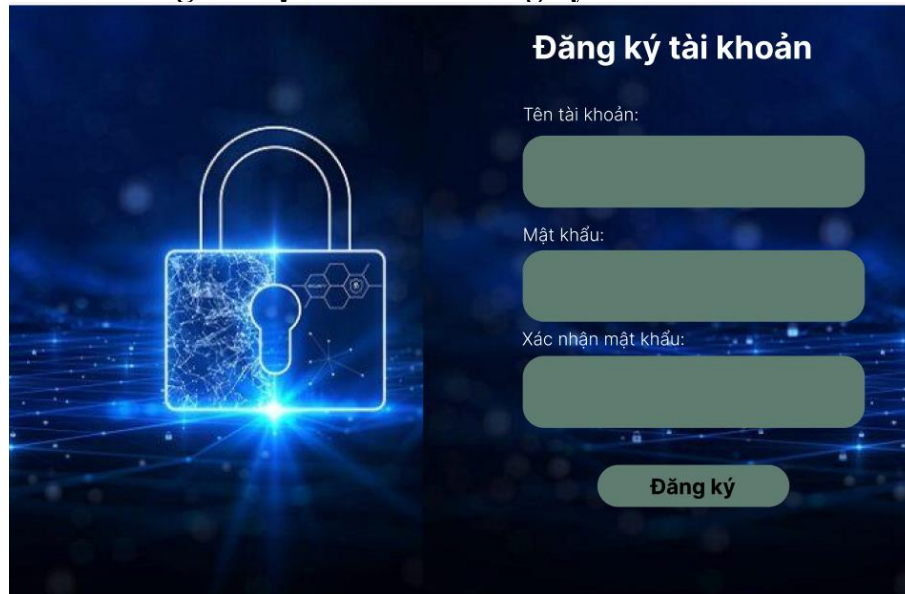


Hình III.2 - 2: Wireframe giao diện màn hình đăng nhập

- Thông tin lưu trữ:
  - Tên tài khoản đăng nhập.
  - Mật khẩu đăng nhập tài khoản.
  - Nút đăng nhập.
  - Mục đăng ký tài khoản.
- Chức năng:
  - Đăng nhập: nhập tên tài khoản và mật khẩu đã được đăng ký để đăng nhập vào tài khoản.
  - Đăng ký: nhấp vào mục “Đăng ký ngay” để tiến hành đăng ký tài khoản nếu chưa có tài khoản.



### III.2.3. Wireframe giao diện màn hình đăng ký



**Đăng ký tài khoản**

Tên tài khoản:

Mật khẩu:

Xác nhận mật khẩu:

**Đăng ký**

Hình III.2 - 3: Wireframe giao diện màn hình đăng ký

- Thông tin lưu trữ:
  - Tên tài khoản đăng ký.
  - Mật khẩu đăng ký tài khoản.
  - Xác nhận lại mật khẩu đã nhập.
  - Nút đăng ký tài khoản.
- Chức năng:
  - Nhập tên tài khoản vào ô trống.
  - Nhập mật khẩu vào ô trống.
  - Xác nhận mật khẩu đã nhập phía trên.
  - Nhấn nút đăng ký để đăng ký tài khoản.

### III.2.4. Wireframe giao diện màn hình menu



**Các phương pháp mã hoá và giải mã**

Mã hoá bằng phương pháp thay thế	Giải mã bằng phương pháp thay thế
Mã hoá bằng phương pháp chuyển vị	Giải mã bằng phương pháp chuyển vị
Mã hoá bằng phương pháp XOR	Giải mã bằng phương pháp XOR
Mã hoá bằng phương pháp DES	Giải mã bằng phương pháp DES
Mã hoá bằng phương pháp RSA	Giải mã bằng phương pháp RSA

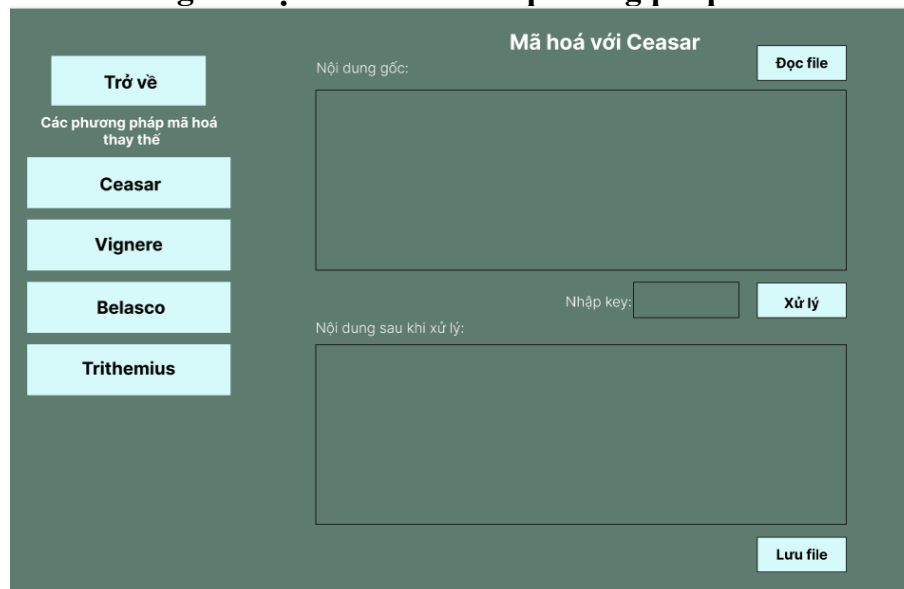
**Các phương pháp mã hoá một chiều**

Mã hoá bằng phương pháp MD5	Mã hoá bằng phương pháp SHA-256	Mã hoá bằng phương pháp SHA-3
-----------------------------	---------------------------------	-------------------------------

Hình III.2 - 4: Wireframe giao diện màn hình menu

- Thông tin lưu trữ:
  - Màn hình menu các phương pháp mã hóa và giải mã, các phương pháp mã hóa một chiều
  - 5 nút mã hóa: mã hóa bằng phương pháp thay thế, mã hóa bằng phương pháp chuyển vị, mã hóa bằng phương pháp XOR, mã hóa bằng phương pháp DES, mã hóa bằng phương pháp RSA.
  - 5 nút giải mã: giải mã bằng phương pháp thay thế, giải mã bằng phương pháp chuyển vị, giải mã bằng phương pháp XOR, giải mã bằng phương pháp DES, giải mã bằng phương pháp RSA.
  - 3 nút mã hóa một chiều: mã hóa bằng phương pháp MD5, mã hóa bằng phương pháp SHA-256, mã hóa bằng phương pháp SHA-3.
- Chức năng:
  - Chọn các chức năng giải mã hoặc mã hóa để xử lý các văn bản

### III.2.5. Wireframe giao diện màn hình các phương pháp Mã hóa Caesar

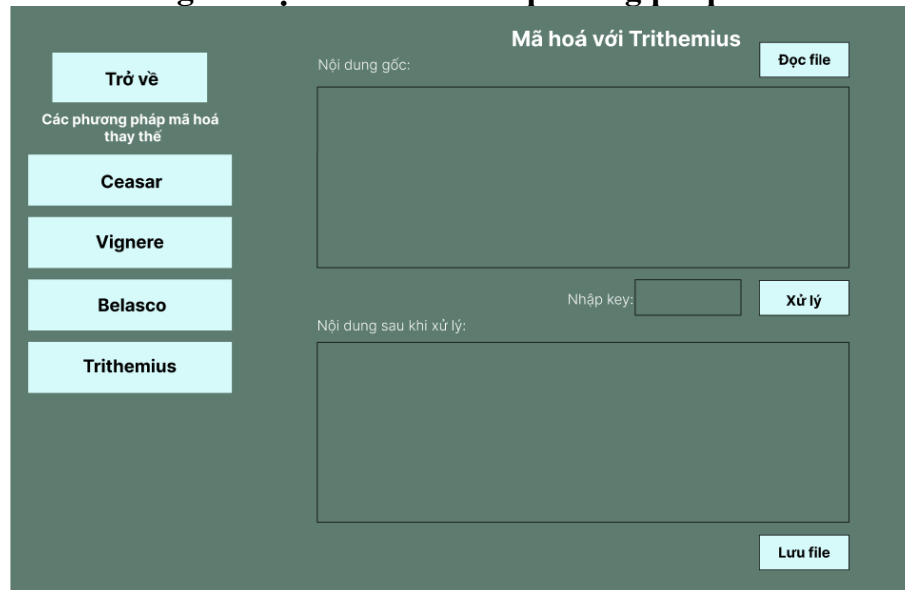


Hình III.2 - 5: Wireframe giao diện màn hình Mã hóa Caesar

- Thông tin lưu trữ:
  - Màn hình mã hóa với Caesar \_ Các phương pháp mã hóa thay thế.
  - Nút trở lại trang trước chọn lại phương pháp mã hóa hoặc giải mã.
  - Nội dung văn bản gốc.
  - Key.
  - Nội dung văn bản sau khi được xử lý .
  - 3 nút: đọc file, xử lý, lưu file.
  - 4 nút: 4 thuật toán có trong phương pháp mã hóa thay thế gồm Caesar, Vignere, Belasco, Trithemius.
- Chức năng:

- Đọc file: đọc nội dung từ file ra text editor để xử lí/ nhập nội dung từ bàn phím.
- Đọc file: đọc nội dung của key file ra text editor để xử lí/ nhập nội dung từ bàn phím.
- Nhấn nút xử lí để gọi thực hiện thuật toán. Xuất ra nội dung đã xử lí ra text editor nội dung đã xử lí.
- Nhấn nút lưu file để thực hiện lưu nội dung đã xử lí vào file.
- Nhấn nút trở lại để quay trở lại trang menu các phương pháp giải mã và mã hóa.

### III.2.6. Wireframe giao diện màn hình các phương pháp Mã hóa Trithemius



Hình III.2 - 6: Wireframe giao diện màn hình Mã hóa Trithemius

- Thông tin lưu trữ:
  - Màn hình mã hóa với Trithemius \_ Các phương pháp mã hóa thay thế.
  - Nút trở lại trang trước chọn lại phương pháp mã hóa hoặc giải mã.
  - Nội dung văn bản gốc.
  - Key.
  - Nội dung văn bản sau khi được xử lí .
  - 3 nút: đọc file, xử lý, lưu file.
  - 4 nút: 4 thuật toán có trong phương pháp mã hóa thay thế gồm Ceasar, Vignere, Belasco, Trithemius.
- Chức năng:
  - Đọc file: đọc nội dung từ file ra text editor để xử lí/ nhập nội dung từ bàn phím.
  - Đọc file: đọc nội dung của key file ra text editor để xử lí/ nhập nội dung từ bàn phím.
  - Nhấn nút xử lí để gọi thực hiện thuật toán. Xuất ra nội dung đã xử lí ra text editor nội dung đã xử lí.
  - Nhấn nút lưu file để thực hiện lưu nội dung đã xử lí vào file.
  - Nhấn nút trở lại để quay trở lại trang menu các phương pháp giải mã và mã hóa.

### III.2.7. Wireframe giao diện màn hình các phương pháp Giải mã với chuyển vị 2 dòng



Hình III.2 - 7: Wireframe giao diện màn hình Giải mã với chuyển vị 2 dòng

- Thông tin lưu trữ:
  - Màn hình giải mã với chuyển vị 2 dòng \_ các phương pháp giải mã chuyển vị.
  - Nút trở lại trang trước chọn lại phương pháp mã hóa hoặc giải mã.
  - Nội dung văn bản gốc.
  - Key.
  - Nội dung văn bản đã được xử lý .
  - 3 nút: đọc file, xử lý, lưu file.
  - 2 nút: 2 thuật toán có trong phương pháp giải mã chuyển vị gồm chuyển vị 2 dòng, chuyển vị nhiều dòng.
- Chức năng:
  - Đọc file: đọc nội dung từ file ra text editor để xử lý/ nhập nội dung từ bàn phím.
  - Đọc file: đọc nội dung của key file ra text editor để xử lý/ nhập nội dung từ bàn phím.
  - Nhấn nút xử lý để gọi thực hiện thuật toán. Xuất ra nội dung đã xử lý ra text editor nội dung đã xử lý.
  - Nhấn nút lưu file để thực hiện lưu nội dung đã xử lý vào file.
  - Nhấn nút trở lại để quay trở lại trang menu các phương pháp giải mã và mã hóa.

### III.2.8. Wireframe giao diện màn hình các phương pháp Giải mã với chuyển vị nhiều dòng



Hình III.2 - 8: Wireframe giao diện màn hình Giải mã với chuyển vị nhiều dòng

- Thông tin lưu trữ:
  - Màn hình giải mã với chuyển vị nhiều dòng \_ các phương pháp giải mã chuyển vị.
  - Nút trở lại trang trước chọn lại phương pháp mã hóa hoặc giải mã.
  - Nội dung văn bản gốc.
  - Key.
  - Nội dung văn bản đã được xử lý .
  - 3 nút: đọc file, xử lý, lưu file.
  - 2 nút: 2 thuật toán có trong phương pháp giải mã chuyển vị gồm chuyển vị 2 dòng, chuyển vị nhiều dòng.
- Chức năng:
  - Đọc file: đọc nội dung từ file ra text editor để xử lý/ nhập nội dung từ bàn phím.
  - Đọc file: đọc nội dung của key file ra text editor để xử lý/ nhập nội dung từ bàn phím.
  - Nhấn nút xử lý để gọi thực hiện thuật toán. Xuất ra nội dung đã xử lý ra text editor nội dung đã xử lý.
  - Nhấn nút lưu file để thực hiện lưu nội dung đã xử lý vào file.
  - Nhấn nút trở lại để quay trở lại trang menu các phương pháp giải mã và mã hóa.

### III.3. Thiết kế xử lý:

#### ❖ Mô hình MVC:

Mô hình MVC (Model-View-Controller) là một kiến trúc thiết kế phần mềm được sử dụng rộng rãi trong phát triển ứng dụng web và các ứng dụng khác. Nó giúp tách biệt logic dữ liệu, giao diện người dùng và quản lý luồng điều khiển trong một ứng dụng. Dưới đây là giải thích chi tiết về từng thành phần của mô hình MVC:

- **Data :** Đại diện cho dữ liệu và logic xử lý dữ liệu.
- **View (Giao diện):**
  - Lưu trữ các file giao diện màn hình.
  - Hai thư mục con:
    - Icon: lưu trữ các file icon
    - Image: lưu trữ các file image
- **Controller (Bộ điều khiển):** Lưu trữ các file xử lý thuật toán.

## Chương IV. Kết luận

### IV.1. Kết quả đạt được

Đồ án đã tạo thành công một phần mềm mã hóa và giải mã bằng các phương pháp mã hóa cổ điển và hiện đại. Cụ thể, đối với các phương pháp mã hóa cổ điển, phần mềm đã thực hiện được các phương pháp mã hóa và giải mã sau:

- Phương pháp thay thế: Caesar, Vigenère, Trithemius, Belasco
- Phương pháp chuyển vị: chuyển vị 2 dòng và chuyển vị nhiều dòng
- Phương pháp XOR: XOR Caesar, XOR Vigenère, XOR Trithemius, XOR Belasco

Đối với các phương pháp mã hóa hiện đại, phần mềm đã thực hiện được phương pháp DES (Data Encryption Standard) và phương pháp RSA (Rivest-Shamir-Adleman). Ngoài ra cũng có thể thực hiện các phương pháp mã hóa một chiều như: MD5, SHA-3, SHA-256. Sau mỗi lần mã hóa/giải mã, người dùng được yêu cầu đặt tên và lưu file.

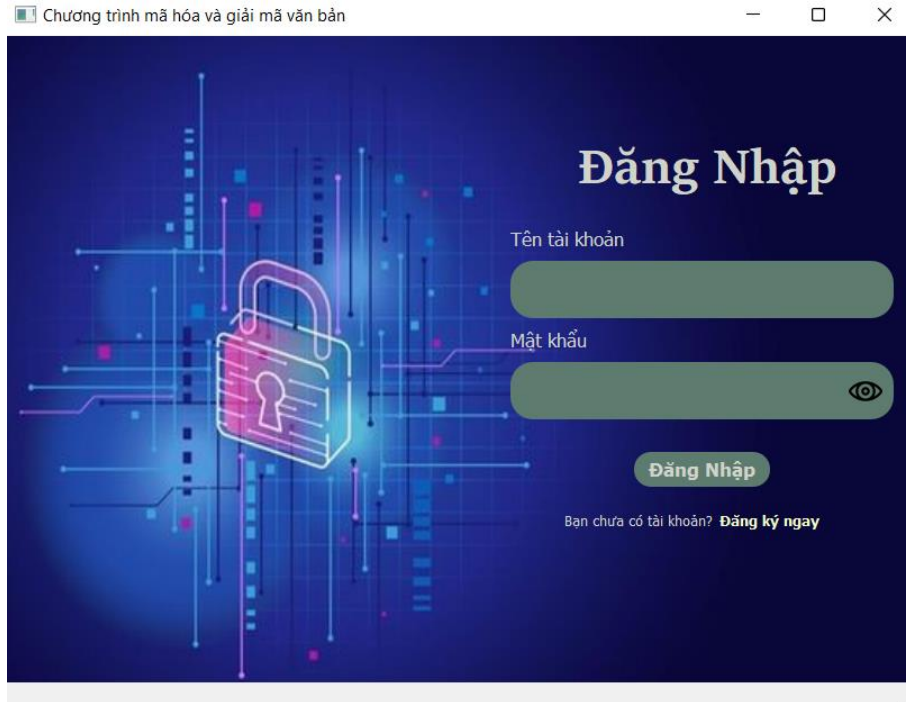
#### IV.1.1. Màn hình giao diện chính



Hình IV.1 - 1: Màn hình giao diện chính

- Gồm có những thông tin lưu trữ:
  - Tên đề tài.
  - Danh sách các thành viên.
  - Nút bắt đầu.
- Hướng dẫn sử dụng:
  - Ấn chọn nút bắt đầu để bắt đầu chương trình

### IV.1.2. Màn hình đăng nhập



Hình IV.1 - 2: Màn hình đăng nhập

- Gồm có những thông tin lưu trữ:
  - Tên tài khoản đăng nhập.
  - Mật khẩu đăng nhập tài khoản.
  - Nút đăng nhập.
  - Mục đăng ký tài khoản.
- Hướng dẫn sử dụng:
  - Bước 1 - 1: Nếu chưa có tài khoản thì thực hiện nhấp vào mục “Đăng ký ngay” đăng ký tài khoản.
  - Bước 1 - 2: Nhấp vào ô tên tài khoản và nhập tên tài khoản đã đăng ký.
  - Bước 2: Nhấp vào ô mật khẩu và nhập mật khẩu đã đăng ký với tên tài khoản.
  - Bước 3: Nhấp vào nút đăng nhập để đăng nhập.



### IV.1.3. Màn hình đăng ký

Chương trình mã hóa và giải mã văn bản

Trở về

## Đăng ký tài khoản

Tên tài khoản

Mật khẩu

Xác nhận mật khẩu

Đăng ký

Hình IV.1 - 3: Màn hình đăng ký

- Thông tin lưu trữ:
  - Tên tài khoản đăng ký.
  - Mật khẩu đăng ký tài khoản.
  - Xác nhận lại mật khẩu đã nhập.
  - Nút đăng ký tài khoản.
- Hướng dẫn sử dụng:
  - Bước 1: Nhấp vào ô tên tài khoản và nhập tên tài khoản muốn tạo.
  - Bước 2: Nhấp vào ô mật khẩu và nhập mật khẩu muốn tạo.
  - Bước 3: Nhấp vào ô xác nhận mật khẩu và nhập lại mật khẩu vừa tạo.
  - Bước 4: Nhấp chọn nút đăng ký và thực hiện đăng nhập vào tài khoản vừa tạo.

#### IV.1.4. Màn hình menu

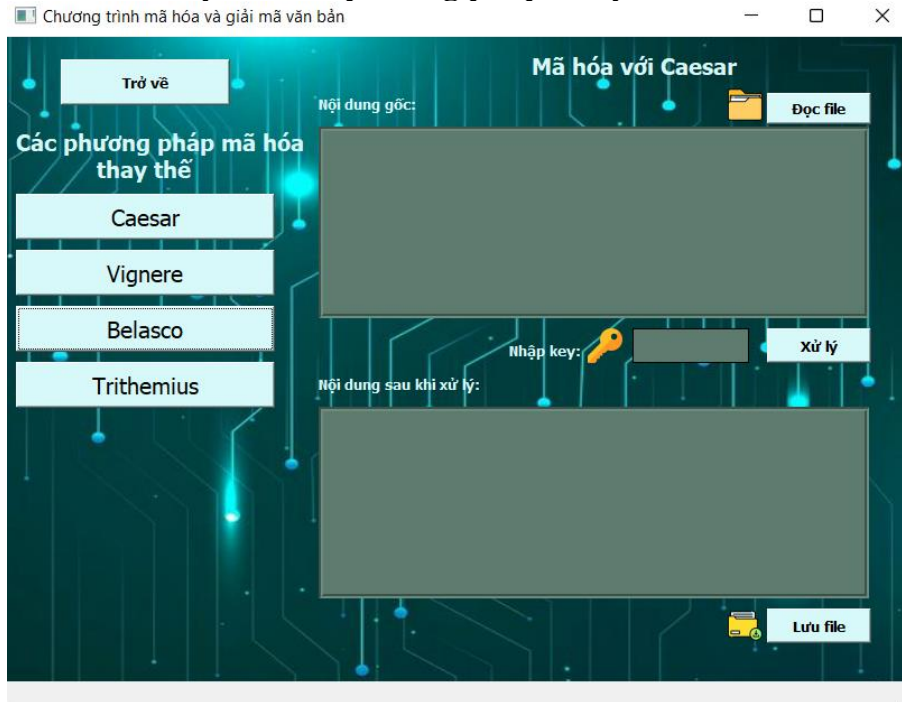


Hình IV.1 - 4: Màn hình Menu

- Thông tin lưu trữ:
  - Màn hình menu các phương pháp mã hóa và giải mã, các phương pháp mã hóa một chiều
  - 5 nút mã hóa: mã hóa bằng phương pháp thay thế, mã hóa bằng phương pháp chuyển vị, mã hóa bằng phương pháp XOR, mã hóa bằng phương pháp DES, mã hóa bằng phương pháp RSA.
  - 5 nút giải mã: giải mã bằng phương pháp thay thế, giải mã bằng phương pháp chuyển vị, giải mã bằng phương pháp XOR, giải mã bằng phương pháp DES, giải mã bằng phương pháp RSA.
  - 3 nút mã hóa một chiều: mã hóa bằng phương pháp MD5, mã hóa bằng phương pháp SHA-256, mã hóa bằng phương pháp SHA-3.
- Hướng dẫn sử dụng:  
Nhấp chọn phương pháp mã hóa hoặc giải mã muốn sử dụng

### IV.1.5. Màn hình xử lý mã hoá

#### IV.1.5.1. Màn hình xử lý mã hoá phương pháp Thay thế \_ Mã hóa với Caesar



Hình IV.1 - 5: Màn hình xử lý Mã hóa với Caesar

- Thông tin lưu trữ:
  - Màn hình xử lý mã hoá phương pháp Thay thế \_ Mã hóa với Caesar.
  - Nút trở lại trang trước chọn lại phương pháp mã hóa hoặc giải mã.
  - Nội dung văn bản gốc.
  - Key.
  - Nội dung văn bản sau khi được xử lý .
  - 3 nút: đọc file, xử lý, lưu file.
  - 4 nút: 4 thuật toán có trong phương pháp mã hóa thay thế gồm Caesar, Vignere, Belasco, Trithemius.
- Hướng dẫn sử dụng:
  - Bước 1: Nhập nội dung muốn mã hóa và ô “Nội dung gốc” hoặc nhấp vào nút “Đọc file” để chọn nội dung có sẵn.
  - Bước 2: Nhập key vào ô “Nhập key”.
  - Bước 3: Ấn nút “Xử lý” để thực hiện mã hóa.
  - Bước 4: Ấn nút “Lưu file” để tiến hành lưu lại file đã mã hóa.

#### IV.1.5.2. Màn hình xử lý mã hoá phương pháp Thay thế \_ Mã hóa với Trithemius (Không key)

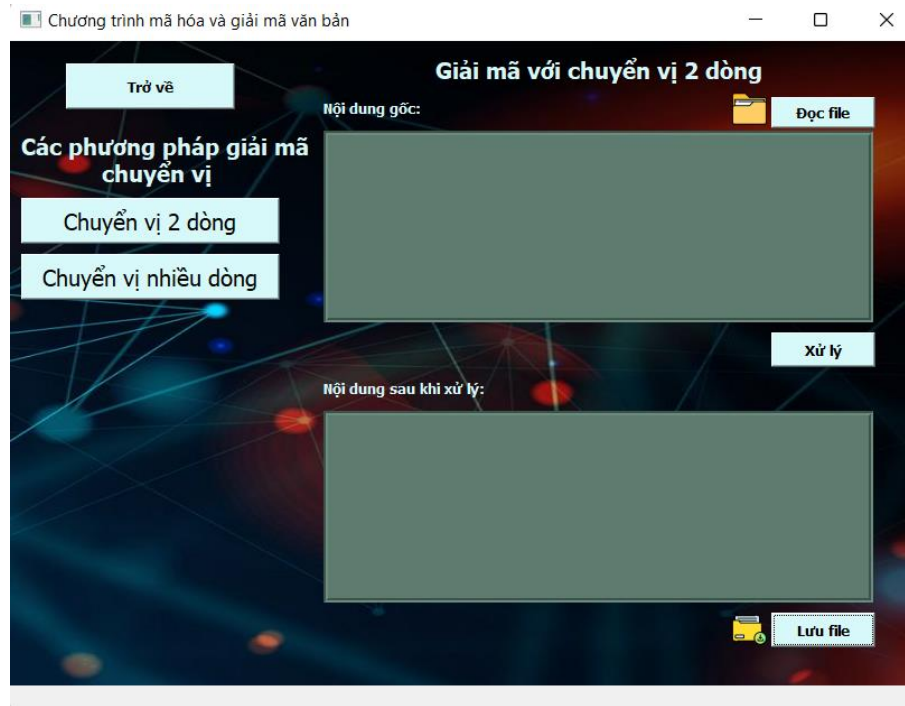


Hình IV.1 - 6: Màn hình xử lý Mã hóa với Trithemius

- Thông tin lưu trữ:
  - Màn hình xử lý mã hoá phương pháp Thay thế \_ Mã hóa với Trithemius.
  - Nút trở lại trang trước chọn lại phương pháp mã hóa hoặc giải mã.
  - Nội dung văn bản gốc.
  - Nội dung văn bản sau khi được xử lý .
  - 3 nút: đọc file, xử lý, lưu file.
  - 4 nút: 4 thuật toán có trong phương pháp mã hóa thay thế gồm Caesar, Vignere, Belasco, Trithemius.
- Hướng dẫn sử dụng:
  - Bước 1: Nhập nội dung muốn mã hóa vào ô “Nội dung gốc” hoặc nhấp vào nút “Đọc file” để chọn nội dung có sẵn.
  - Bước 2: Ấn nút “Xử lý” để thực hiện mã hóa.
  - Bước 3: Ấn nút “Lưu file” để tiến hành lưu lại file đã mã hóa.

#### IV.1.6. Màn hình xử lý giải mã

##### IV.1.6.1. Màn hình xử lý giải mã phương pháp Chuyển vị \_ Giải mã với chuyển vị 2 dòng



Hình IV.1 - 7: Màn hình xử lý giải mã phương pháp Chuyển vị 2 dòng

- Thông tin lưu trữ:
  - Màn hình xử lý giải mã phương pháp Chuyển vị \_ Giải mã với chuyển vị 2 dòng.
  - Nút trở lại trang trước chọn lại phương pháp mã hóa hoặc giải mã.
  - Nội dung văn bản gốc.
  - Nội dung văn bản sau khi được xử lý .
  - 3 nút: đọc file, xử lý, lưu file.
  - 2 nút: 2 thuật toán có trong phương pháp mã hóa chuyển vị gồm chuyển vị 2 dòng, chuyển vị nhiều dòng.
- Hướng dẫn sử dụng:
  - Bước 1: Nhập nội dung muốn mã hóa và ô “Nội dung gốc” hoặc nhấp vào nút “Đọc file” để chọn nội dung có sẵn.
  - Bước 2: Ấn nút “Xử lý” để thực hiện giải mã.
  - Bước 3: Ấn nút “Lưu file” để tiến hành lưu lại file đã giải mã.

#### IV.1.6.2. Màn hình xử lý giải mã phương pháp Chuyển vị \_ Giải mã với chuyển vị nhiều dòng



Hình IV.1 - 8: Màn hình xử lý giải mã phương pháp Chuyển vị nhiều dòng

- Thông tin lưu trữ:
  - Màn hình xử lý giải phương pháp Chuyển vị \_ Giải mã với chuyển vị nhiều dòng.
  - Nút trở lại trang trước chọn lại phương pháp mã hóa hoặc giải mã.
  - Nội dung văn bản gốc.
  - Key
  - Nội dung văn bản sau khi được xử lý .
  - 3 nút: đọc file, xử lý, lưu file.
  - 2 nút: 2 nút: 2 thuật toán có trong phương pháp mã hóa chuyển vị gồm chuyển vị 2 dòng, chuyển vị nhiều dòng.
- Hướng dẫn sử dụng:
  - Bước 1: Nhập nội dung muốn mã hóa và ô “Nội dung gốc” hoặc nhấp vào nút “Đọc file” để chọn nội dung có sẵn.
  - Bước 2: Nhập key vào ô “Nhập key”.
  - Bước 3: Ấn nút “Xử lý” để thực hiện giải mã.
  - Bước 4: Ấn nút “Lưu file” để tiến hành lưu lại file đã giải mã.

#### IV.2. Hạn chế của đề tài

Mặc dù có nhiều cố gắng, nỗ lực trong quá trình thực hiện nghiên cứu đề tài này nhưng do thời gian ngắn, khả năng nghiên cứu có hạn, nên nhóm em nhận thấy đề tài này còn một số hạn chế như:

- Chưa tối ưu hóa được giao diện người dùng
- Chưa khai thác hết các thuật toán mã hóa hiện đại như TrippleDes, Twofish ...



**IV.3. Hướng phát triển**

Trong tương lai sẽ:

- Cải thiện hiệu suất cho các thuật toán mã hoá, giúp mã hoá và giải mã các tập dữ liệu lớn nhanh chóng hơn.
- Bổ sung thêm các thuật toán mã hoá hiện đại.
- Cải thiện về giao diện giúp thân thiện hơn với người dùng.
- Triển khai chương trình chạy thành các ứng dụng có thể sử dụng trực tiếp trên điện thoại thông minh

## Tài liệu tham khảo

- [1] T. đ. s. V. Nam, "Giải pháp bảo mật thông tin các hệ cơ sở dữ liệu," Thời đại số Việt Nam, 4 7 2021. [Online]. Available: <https://www.thoidaisovn.com/2021/07/6-giai-phap-bao-mat-thong-tin-cac-he-co-so-du-lieu.html>.
- [2] Viblo, "Hệ mã hoá RSA và chữ ký số," Viblo, 23 2 2017. [Online]. Available: <https://viblo.asia/p/he-ma-hoa-rsa-va-chu-ky-so-6J3ZgkgMZmB>.
- [3] Made Ari Dwi Suta Atmaja; Nyoman Gede Arya Astawa; Ni Wayan Wisswani; Made Riyan Adi Nugroho; Putu Wijaya Sunu; Komang Wira, "Document Encryption Through Asymmetric RSA Cryptography," 2020. [Online]. Available: <https://ieeexplore.ieee.org/document/9557723/authors>. [Accessed 20 10 2023].
- [4] M. Lutz, Learning Python, O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472., 2009.
- [5] J. M. Willman, Beginning PyQt A Hands-on Approach to GUI Programming, 2020.
- [6] U. S. N. B. o. Standards, Data Encryption Standard (Des), Forgotten Books, 2018.
- [7] J. Holden, The Mathematics of Secrets: Cryptography from Caesar Ciphers to Digital Encryption, 10: Princeton University Press; Illustrated edition , 2018.
- [8] T. Linh, "Mã Hoá Dữ Liệu Là Gì? 4 Phương Pháp Mã Hoá Dữ Liệu Phổ Biến Nhất Hiện Nay," Feb 2023. [Online]. Available: <https://locker.io/vi/blog/ma-hoa-du-lieu-2>. [Accessed 1 Nov 2023].
- [9] N. M. Duc, "Giới thiệu các loại thuật toán mã hoá dữ liệu," 15 7 2019. [Online]. Available: <https://viblo.asia/p/gioi-thieu-cac-loai-thuat-toan-ma-hoa-du-lieu-07LKXBW8IV4>. [Accessed 10 10 2023].
- [10] Kate Brush, Linda Rosencrance, Michael Cobb, "asymmetric cryptography (public key cryptography)," [Online]. Available: <https://www.techtarget.com/searchsecurity/definition/asymmetric-cryptography>. [Accessed 20 10 2023].
- [11] A. P. D. Ouk, XOR encryption NDecryption, 2020.
- [12] P. Training, "Python XOR and Bitwise Operators Tutorial," 4 April 2023. [Online]. Available: <https://pierantraining.com/python-xor-and-bitwise-operators-tutorial/>. [Accessed 20 Nov 2023].
- [13] "How to Decrypt MD5 Passwords in Python?," [Online]. Available: <https://infosecscout.com/decrypt-md5-python/>.



**Bảng phân công công việc**

STT	Nội dung	Cao Thế Anh	Lê Nguyễn Hong Phúc	Trương Văn Quốc Thắng
1	Có trách nhiệm trong học tập, trung thực, sử dụng phần mềm hợp pháp.	X	X	X
2	Đọc tài liệu nghiên cứu.	X	X	X
3	Kỹ năng làm việc nhóm.	X	X	X
4	Thiết kế.	X	X	X
5	Viết Code.	X	X	X
6	Viết báo cáo.	X	X	X
7	Đọc và hiểu thành hướng báo cáo.	X	X	X