



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

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

PHẦN MỀM MÃ HOÁ VĂN BẢN TIẾNG VIỆT

GVHD: ThS. Phạm Đức Thành

Sinh viên thực hiện: Lê Thanh Tân – 21DH114097

Phạm Quang Phát – 21DH113964

Đặng Duy Thái – 21DH111733

Thành Phố Hồ Chí Minh, tháng 11 năm 2023

MỤC LỤC

MỤC LỤC	1
DANH MỤC HÌNH	3
DANH MỤC BẢNG	4
Chương I. Giới thiệu đề tài	5
I.1. Giới thiệu	5
I.1.1. Mở đầu	5
I.1.2. Lý do chọn đề tài	6
I.2. Khảo sát thực tế	6
I.2.1. Các ứng dụng cụ thể	6
I.2.2. Một quy trình cụ thể	16
I.3. Các chức năng dự kiến của đề tài	17
I.4. Công nghệ sử dụng	17
I.5. Phạm vi giới hạn	17
I.6. Bố cục đề tài	17
Chương II. Cơ sở lý thuyết	18
II.1. Lý thuyết về bảo mật thông tin	18
II.1.1. Khái niệm cơ bản về hệ thống thông tin	18
II.1.2. Các phương pháp bảo mật thông tin trong hệ thống thông tin	19
II.2. Ngôn ngữ lập trình và cài đặt môi trường	20
II.2.1. Python 3.11	20
II.2.2. PyQt6 Designer	21
II.3. Mô hình MVC	22
Chương III. Phân tích và thiết kế	23
III.1. Phân tích	23
III.1.1. Sơ đồ chức năng	23
III.1.2. Usecase Diagram	24
III.2. Thiết kế giao diện	25
III.3. Thiết kế xử lý	29
Chương IV. Kết luận	30
IV.1. Kết quả đạt được	30
IV.2. Màn hình giao diện chính	30
IV.3. Màn hình xử lý mã hoá	33
IV.4. Màn hình xử lý giải mã	37
IV.5. Hướng phát triển	39

Tài liệu tham khảo	40
Phụ lục	41

DANH MỤC HÌNH

Hình I.2-1. Phần mềm NordLocker.....	6
Hình I.2-2. Phần mềm AxCrypt	8
Hình I.2-3. Phần mềm Folder Lock	10
Hình I.2-4. Steganos Data Safe	12
Hình I.2-5. Advanced Encryption Packages	14
Hình I.2-6. Quy trình mã hóa cụ thể của Google Admin Toolbox.....	16
Hình III.1-1. Sơ đồ chức năng.....	29
Hình III.1-2. UseCase Diagram	29
Hình III.2-1. Wireframe giao diện màn hình chính (1).....	29
Hình III.2-2. Wireframe giao diện màn hình chính (2).....	29
Hình III.2-3. Wireframe giao diện màn hình xử lý mã hóa	29
Hình III.2-4. Wireframe giao diện màn hình xử lý giải mã	29
Hình III.3-1. Mô hình MVC.....	29
Hình IV.2-1. Màn hình giao diện chính.....	30
Hình IV.2-2. Màn hình giao diện đăng ký.....	31
Hình IV.2-3. Màn hình giao diện đăng nhập.....	32
Hình IV.3-1. Màn hình giao diện xử lý mã hoá phương pháp Ceasar	33
Hình IV.3-2. Màn hình giao diện xử lý mã hoá phương pháp Trithemius	35
Hình IV.4-1. Màn hình giao diện xử lý giải mã theo kỹ thuật Ceasar	37
Hình IV.4-2. Màn hình giao diện xử lý giải mã theo kỹ thuật Trithemius	29

DANH MỤC BẢNG

Bảng 1. Bảng phân công công việc	41
--	----

Chương I. Giới thiệu đề tài

I.1. Giới thiệu

I.1.1. Mở đầu

Khi phải đối mặt với các lỗ hổng, doanh nghiệp không chỉ đặt thông tin của riêng họ vào rủi ro mà còn của khách hàng và đối tác. Các công ty vừa và nhỏ thậm chí còn bị nhầm mục tiêu nhiều hơn so với các doanh nghiệp lớn bởi những tin tặc thấy được lợi nhuận mà họ nhận được là rất lớn trong khi rủi ro phải chịu lại ít hơn so với những công ty lớn.

Vậy, vai trò của bảo mật thông tin đối với các doanh nghiệp vừa và nhỏ cụ thể bao gồm những gì? Hãy cùng chúng tôi tìm hiểu chi tiết qua bài chia sẻ dưới đây.

Các lỗi bảo mật về cơ bản là nguy hiểm vì giá trị của thông tin. Hãy tưởng tượng rằng buổi sáng bạn thức dậy và phát hiện tài khoản email của bạn đã bị tấn công. Kẻ tấn công có quyền truy cập vào một khối lượng lớn dữ liệu cá nhân. Lịch trình, tài liệu bí mật và các cuộc trò chuyện riêng tư của bạn. Điều này thật kinh khủng đúng không?

Với dữ liệu này, tội phạm có thể mạo danh bạn trên các dịch vụ khác, đặt lại mật khẩu và giành quyền kiểm soát vĩnh viễn các tài khoản. Nếu viễn cảnh này là đáng sợ đối với một cá nhân thì đối với doanh nghiệp nó còn tệ hơn rất nhiều.

Theo một cuộc khảo sát cho thấy khoảng 90% các vụ xâm nhập nhằm vào hệ thống của các doanh nghiệp vừa và nhỏ. Chi phí trung bình cho các lỗ hổng bảo mật đủ làm tăng chi phí của các công ty này lên khoảng 36.000 đô la Mỹ hàng năm.

Ngoài các biện pháp an ninh bổ sung cần thiết sau một cuộc tấn công và một nguồn chi phí phụ, các công ty này còn phải chịu thiệt hại về quan hệ công chúng. Đánh mất lòng tin của đối tác và khách hàng. Tệ hơn là một cuộc tấn công mạng có thể đưa công ty này ra khỏi lĩnh vực kinh doanh mãi mãi.

Trong hầu hết các trường hợp, mục đích chính của một cuộc tấn công mạng là đánh cắp thông tin nhạy cảm. Có rất nhiều kỹ thuật được khám phá về vấn đề này và bạn nên biết những kỹ thuật phổ biến nhất để tự bảo vệ mình.

- **Các cuộc tấn công nội bộ:** Những cuộc tấn công này xảy ra khi ai đó có đặc quyền quản trị sử dụng thông tin đăng nhập của bạn với mục đích xấu. Các nhân viên cũ là nguồn chính của kiểu tấn công này và sẽ bị thu hồi tài khoản ngay khi họ rời tổ chức.

- **Phần mềm độc hại:** Vi rút, trojan và các loại phần mềm độc hại khác khai thác các lỗ hổng trong hệ thống và làm rò rỉ thông tin thẳng vào tay tin tặc.

- **Tấn công bằng mật khẩu:** bỏ qua xác thực với sự trợ giúp của các công cụ cụ thể, kỹ thuật xã hội.

- **Tấn công DDoS:** xảy ra khi một máy chủ cố tình bị quá tải với các yêu cầu, với mục đích làm cho quyền truy cập không khả dụng.

I.1.2. Lý do chọn đề tài

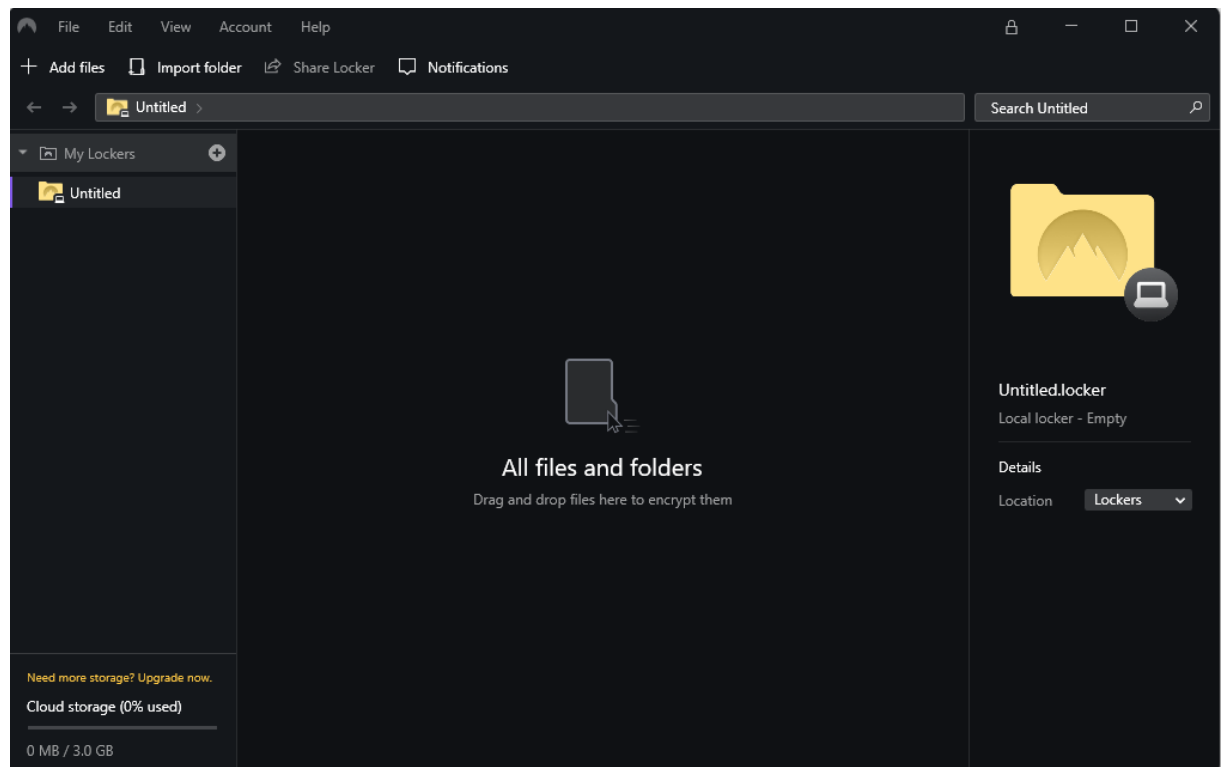
Đề tài được thực hiện với mục đích hiểu rõ hơn về các phương pháp mã hoá cổ điển, hiện đại và cách chúng hoạt động trong việc bảo mật hệ thống thông tin.

Đồng thời nắm bắt được tầm quan trọng trong việc mã hoá và giải mã thông tin trong việc bảo mật thông tin.

I.2. Khảo sát thực tế

I.2.1. Các ứng dụng cụ thể

➤ Phần mềm NordLocker

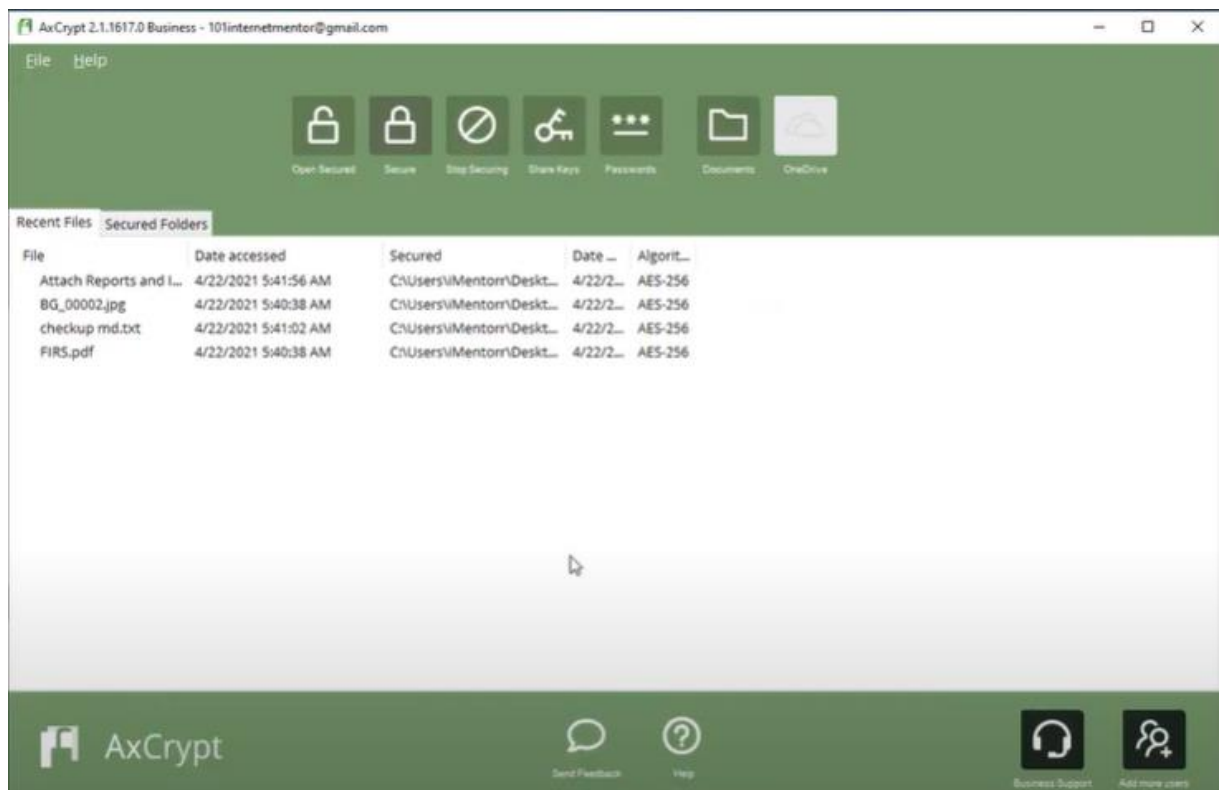


Hình I.2-1. Phần mềm NordLocker

- Thông tin lưu trữ:
 - Các file, tệp
 - Menu: file, tùy chỉnh, màn hình, tài khoản, hỗ trợ
 - Vị trí lưu trữ file
 - Thanh tìm kiếm
 - Các nút: Add files, Import folder, Share Locker, Notification

- Các chức năng:
 - Bảo mật Dữ liệu:
 - NordLocker giúp người dùng mã hóa dữ liệu của họ để bảo vệ khỏi truy cập trái phép. Khi dữ liệu được mã hóa, nó trở nên khó đọc và hiểu mà không có khóa giải mã đúng.
 - Mã Hóa File và Thư Mục:
 - Người dùng có thể mã hóa cả tệp tin và thư mục bằng cách sử dụng NordLocker. Điều này giúp bảo vệ toàn bộ cấu trúc thư mục và tất cả các tệp tin bên trong chúng.
 - Khóa An Toàn:
 - Ứng dụng sử dụng các khóa an toàn để đảm bảo rằng chỉ có người dùng có quyền truy cập mới có thể mở khóa và xem dữ liệu.
 - Integrations với Dịch vụ Lưu Trữ Đám Mây:
 - NordLocker thường tích hợp với các dịch vụ lưu trữ đám mây như Dropbox, Google Drive và OneDrive, giúp người dùng lưu trữ dữ liệu của họ một cách an toàn trên các nền tảng này.
 - Quản lý Dễ Dàng:
 - NordLocker thường có giao diện người dùng thân thiện và dễ sử dụng, giúp người dùng quản lý và kiểm soát dữ liệu của mình một cách hiệu quả.
 - Tính Di Động:
 - Người dùng có thể di chuyển dữ liệu đã mã hóa giữa các thiết bị một cách thuận tiện và an toàn.
 - Hỗ Trợ Đa Nền Tảng:
 - NordLocker thường hỗ trợ nhiều nền tảng, bao gồm cả Windows và macOS, để người dùng có thể trải nghiệm tính năng bảo mật trên nhiều thiết bị khác nhau.

➤ *Phần mềm AxCrypt*

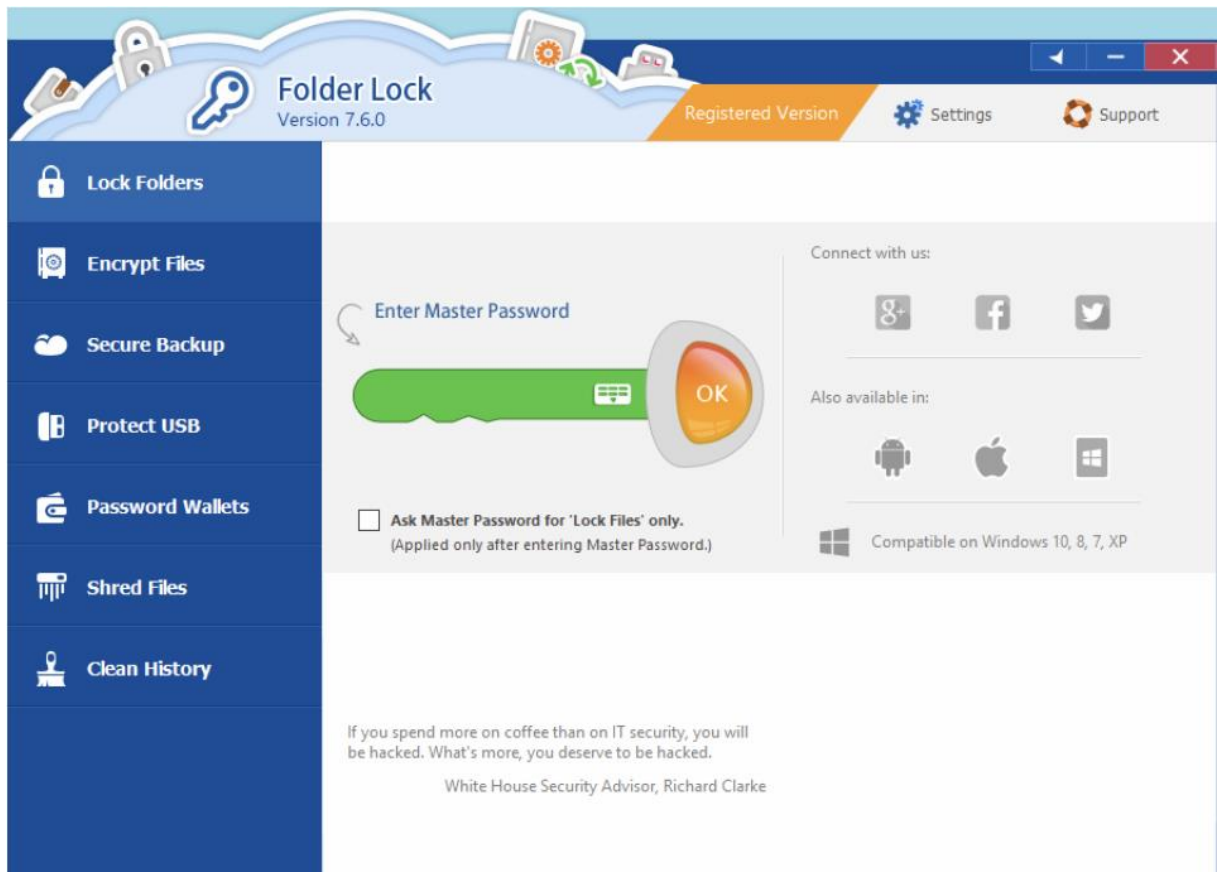


Hình I.2-2. Phần mềm AxCrypt

- Thông tin lưu trữ:
 - Các file, tệp
 - Menu: file, hỗ trợ
 - Vị trí lưu trữ file
 - Các nút: Open Secured, Secure, Stop Securing, Share Keys, Passwords, Documents, Onedrive

- Các chức năng:
 - Mã Hóa Tập Tin:
 - AxCrypt cung cấp khả năng mã hóa tệp tin và thư mục, làm cho chúng trở nên không đọc được cho những người không có khóa mã hóa.
 - Mật khẩu Bảo Vệ:
 - Người dùng có thể đặt mật khẩu để bảo vệ tệp tin đã mã hóa. Mật khẩu này được yêu cầu để mở và truy cập nội dung của tệp tin.
 - Tích Hợp với Windows Explorer:
 - AxCrypt thường tích hợp trực tiếp với Windows Explorer, giúp người dùng dễ dàng thực hiện các thao tác mã hóa và giải mã từ giao diện người dùng của hệ điều hành.
 - Quản Lý Khóa Mã Hóa:
 - Ứng dụng cung cấp quản lý khóa mã hóa để quản lý các khóa mã hóa và mật khẩu. Người dùng có thể thêm, xóa, và quản lý các khóa này theo cách thuận tiện.
 - Tích Hợp với Dịch vụ Lưu Trữ Đám Mây:
 - AxCrypt thường có khả năng tích hợp với các dịch vụ lưu trữ đám mây như Dropbox, Google Drive, và OneDrive, giúp người dùng lưu trữ và chia sẻ tệp tin đã mã hóa trực tuyến.

➤ **Phần mềm Folder Lock**

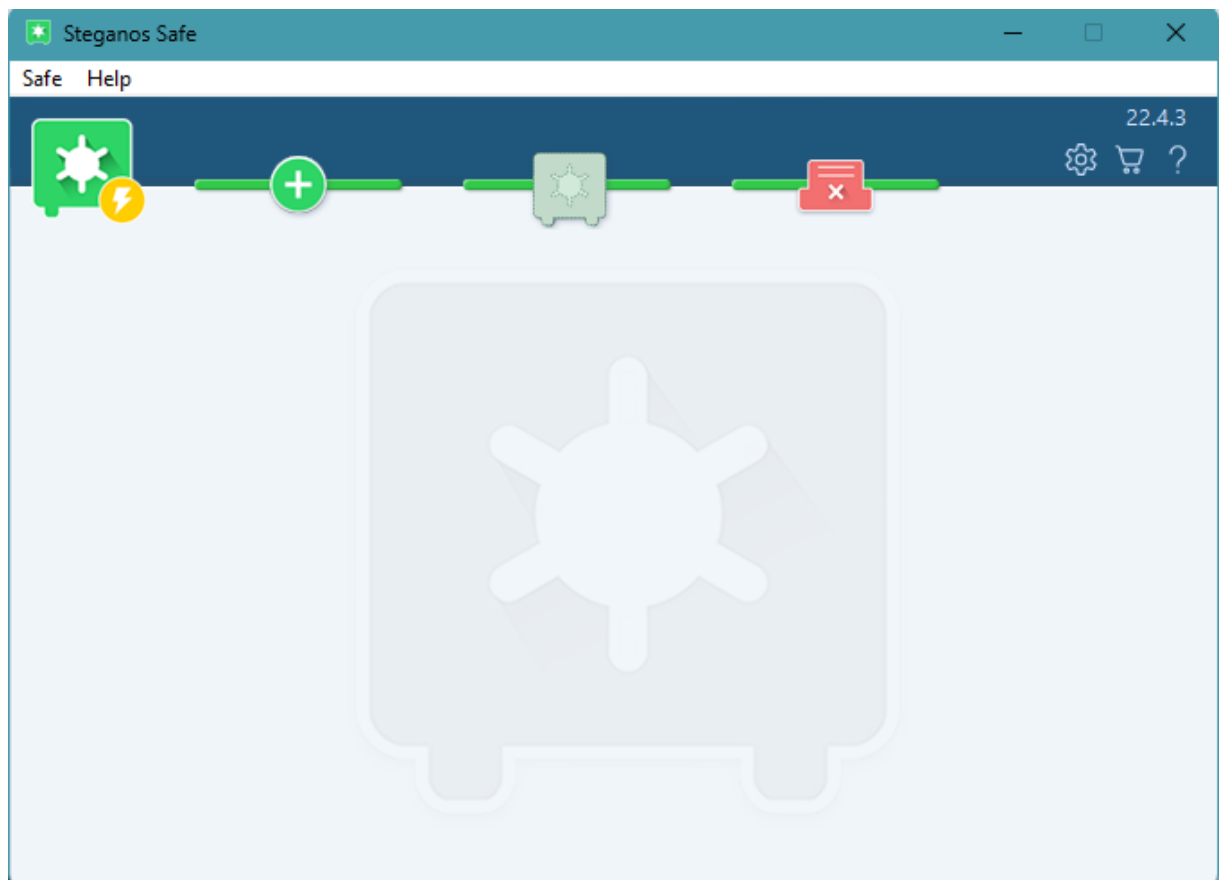


Hình I.2-3. Phần mềm Folder Lock

- Thông tin lưu trữ:
 - Menu: Khóa thư mục, mã hóa thư mục, bảo mật backup, bảo vệ USB, mật khẩu cho ví tiền, xóa lịch sử.
 - Các nút: Cài đặt, hỗ trợ
 - Menu: Khóa thư mục, mã hóa thư mục, bảo mật backup, bảo vệ USB, mật khẩu cho ví tiền, xóa lịch sử.

- Các chức năng:
 - Mã Hóa Tập Tin và Thư Mục:
 - Folder Lock cung cấp khả năng mã hóa tập tin và thư mục để bảo vệ chúng khỏi truy cập trái phép. Người dùng có thể chọn mã hóa và giải mã tập tin một cách dễ dàng.
 - Ẩn và Khóa Thư Mục:
 - Người dùng có thể ẩn thư mục hoặc khóa chúng bằng mật khẩu. Điều này giúp bảo vệ dữ liệu khỏi sự truy cập của những người không mong muốn.
 - Bảo Vệ USB và Ổ Đĩa Di Động:
 - Folder Lock thường hỗ trợ chức năng bảo vệ dữ liệu trên các thiết bị lưu trữ di động như USB và ổ đĩa di động bằng cách mã hóa và mật khẩu bảo vệ.
 - Khóa và Mở Bằng Mật Khẩu:
 - Người dùng có thể thiết lập mật khẩu để khóa và mở các thư mục, tập tin, và các tính năng bảo vệ khác trong ứng dụng.
 - Mã Hóa Email và Tập Tin Wallet:
 - Folder Lock thường có chức năng mã hóa email và tập tin wallet để bảo vệ thông tin cá nhân và những tài liệu quan trọng.
 - Tích Hợp với Dịch vụ Lưu Trữ Đám Mây:
 - Ứng dụng thường có khả năng tích hợp với các dịch vụ lưu trữ đám mây để lưu trữ dữ liệu an toàn trực tuyến.
 - Ghi Chú An Toàn:
 - Folder Lock thường cung cấp chức năng ghi chú an toàn để lưu trữ thông tin quan trọng mà bạn muốn giữ an toàn và bảo mật.
 - Bảo Vệ Trước Ransomware:
 - Folder Lock có thể cung cấp tính năng bảo vệ trước ransomware để ngăn chặn và phòng tránh sự tấn công của các loại phần mềm độc hại này.

➤ ***Steganos Data Safe***

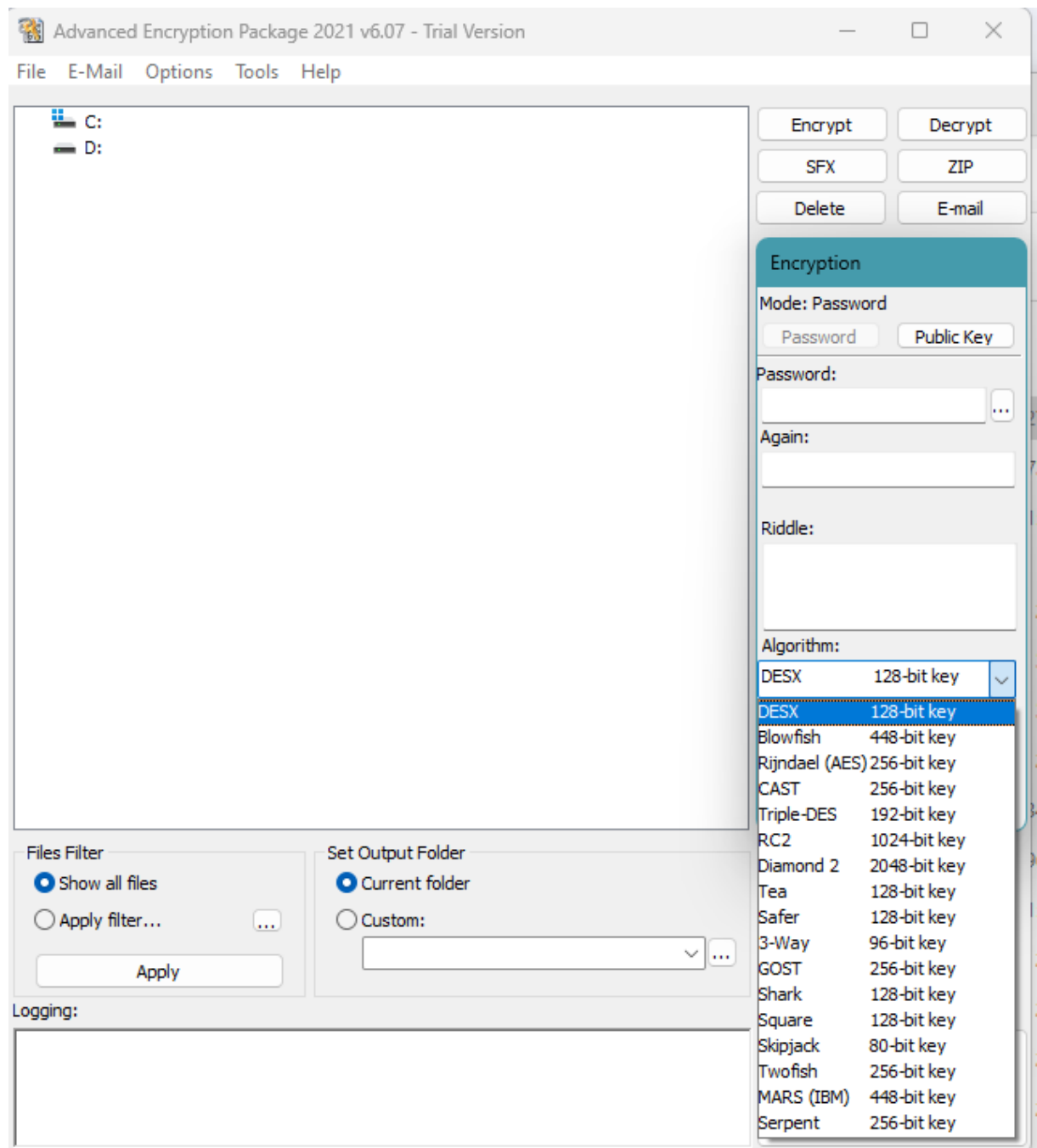


Hình I.2-4. Steganos Data Safe

- Thông tin lưu trữ:
 - Các file, tệp
 - Menu: Safe, Help
 - Các nút: Add files, Import folder, Share Locker, Notification

- Các chức năng:
 - Mã Hóa Dữ Liệu:
 - Steganos Safe sử dụng các thuật toán mã hóa mạnh mẽ để bảo vệ dữ liệu bên trong kho an toàn. Các dữ liệu trong kho an toàn sẽ được mã hóa và chỉ có thể truy cập bằng cách sử dụng mật khẩu chính xác.
 - Tạo Kho An Toàn:
 - Người dùng có thể tạo ra nhiều "kho an toàn" ảo trên máy tính của họ. Mỗi kho an toàn có thể được coi như một ổ đĩa ảo, nơi họ có thể lưu trữ và quản lý các tệp tin và thư mục.
 - Ẩn Dữ Liệu:
 - Steganos Safe thường cung cấp tính năng ẩn dữ liệu, có nghĩa là bạn có thể ẩn đi sự tồn tại của kho an toàn trên hệ thống của bạn. Điều này giúp bảo vệ dữ liệu khỏi sự phát hiện bởi người dùng khác.
 - Mật Khẩu Bảo Vệ:
 - Mỗi kho an toàn yêu cầu một mật khẩu để truy cập. Mật khẩu này đóng vai trò quan trọng trong việc bảo vệ dữ liệu trong kho an toàn.
 - Tích Hợp với Các Dịch Vụ Đám Mây:
 - Steganos Safe thường có khả năng tích hợp với các dịch vụ lưu trữ đám mây như Dropbox, OneDrive, và Google Drive, giúp người dùng lưu trữ và đồng bộ hóa dữ liệu an toàn của họ trên nhiều thiết bị.
 - Tính Di Động:
 - Người dùng có thể chuyển kho an toàn giữa các máy tính hoặc lưu trữ chúng trên các thiết bị di động, giúp họ tiếp cận dữ liệu của mình từ nhiều nơi.
 - Ghi Chú An Toàn:
 - Steganos Safe thường cung cấp chức năng ghi chú an toàn, nơi bạn có thể lưu trữ thông tin nhạy cảm như mật khẩu hoặc ghi chú cá nhân mà không lo sợ mất mát dữ liệu.

➤ *Advanced Encryption Packages*



Hình I.2-5. Advanced Encryption Packages

- Thông tin lưu trữ:
 - Các file, tệp
 - Ô nhập mật khẩu, ô nhập lại mật khẩu.
 - Danh sách phương thức mã hóa
 - Các nút: Proceed, Cancel

- Các chức năng:
 - Mã Hóa Tập Tin và Thư Mục:
 - AEP cho phép người dùng mã hóa cả tập tin và thư mục để bảo vệ chúng khỏi truy cập trái phép. Mã hóa này có thể được thực hiện với nhiều thuật toán mã hóa khác nhau.
 - Mã Hóa USB và Ổ Đĩa Di Động:
 - Ứng dụng hỗ trợ mã hóa dữ liệu trực tiếp trên các thiết bị lưu trữ di động như USB và ổ đĩa di động.
 - Mã Hóa Email:
 - AEP thường cung cấp khả năng mã hóa email, giúp bảo vệ thông tin cá nhân trong các trao đổi email.
 - Tích Hợp với Dịch vụ Lưu Trữ Đám Mây:
 - Ứng dụng có thể tích hợp với các dịch vụ lưu trữ đám mây như Dropbox, Google Drive, và OneDrive để mã hóa và bảo vệ dữ liệu trực tuyến.
 - Bảo Vệ Trước Ransomware:
 - Một số phiên bản của AEP có thể có tính năng bảo vệ trước ransomware để ngăn chặn và phòng tránh sự tấn công của các phần mềm độc hại này.
 - Mật khẩu Bảo Vệ:
 - Người dùng có thể đặt mật khẩu để bảo vệ dữ liệu của mình. Mật khẩu này đóng vai trò quan trọng trong quá trình mã hóa và giải mã.
 - Tích Hợp với Windows Explorer:
 - AEP thường tích hợp trực tiếp với Windows Explorer, giúp người dùng thực hiện các thao tác mã hóa và giải mã từ giao diện người dùng của hệ điều hành.
 - Quản Lý Khóa Mã Hóa:
 - Ứng dụng cung cấp các công cụ để quản lý và lưu trữ các khóa mã hóa, bảo đảm rằng người dùng có thể dễ dàng quản lý các khóa an toàn.

I.2.2. Một quy trình cụ thể

Dưới đây là một bài thơ về quê hương:

****Quê Hương****

Trên nền trời xanh rộng mênh mang,
Là quê hương tôi, vẻ đẹp tràn.
Cánh đồng bát ngát, lúa vàng đang chín,
Núi non xanh biếc, sông nước êm đềm.

Quê hương tôi, những con đường quê thân thương,
Dẫn tôi về nơi tuổi thơ đầu yêu.
Những lời ca dao vang vọng đêm ngày,
Những tiếng cuộc gọi làng quê xa xăm.

Dưới bóng cây xanh, tôi ngồi nhớ về,
Những kỷ niệm xưa, những mối tình đẹp.
Quê hương tôi, hòa bình và hạnh phúc,

☐ Mã hóa Base64
☐ Giải mã Base64
☐ Mã hóa Base64Url
☐ Giải mã Base64Url
☐ Mã hóa URL
☐ Giải mã URL
☐ Hàm băm MD5
☒ Mã hóa SAML
☐ Giải mã SAML
☐ JSON hợp lệ
☐ Mã hóa Quoted-Printable
☐ Giải mã Quoted-Printable
☐ Giải mã UTF16
☐ Giải mã hệ thập lục phân (hex)

Plain Text

bVTNattAE17vU8zZCD9A9j200PRRDoFQuKaAVtdapLRn7aHroqQcTeggml1IoJfLe1bhIo3iXksEbvsW+Sb3Z1Yrc5WLakb2a+nx2fNBtFjnt5vZqSn27pMKZi5ISu8yp1E1NY2dm9LGy
a5LNpq1V9kKITuctP3gdHnQ6Qrwb2rU1Bay1cuJmZU6TWEnCzwUUYG3kopYZZF4gyGH/a10d3mEOdqAhtPbM3SwS9UVr2yNKjwz54A1t15JZbhGIKppjGgOU4TW6UirtLxWJntU5qYEK
w5Pc6Yc0opG9A0R5q5nZdeF7zoquEF7HMRE1nfnNLdFmN+ei59x5xqW0V9DX4iN4vQP3KM52KSaGq5VznxtzTt1+rqiQV1XXdFr+/a9021Mp/GAkwetV+8EqYghcsp1LTokjUwG3Sd
p5QBmnN0e0qTmCa7Tyx1H2V1bXnPebILUeCnUhmOL7RdeLJPIz4485dU7szngibNjN6yAGdhDiX2Z4gB0XSfc0zamxhjGVVMSDrNuZ1Jq9Mqd/CFaFDZ+BbMKocDHgXQjCQ0GMcbLgF
fXxkDAZ6G1HCHTHh+38JcHdgV13B67L1CVIHLI4yf0aAp8Ypef61M3+gaTmIxEuwhWkgA1YrjrOeBvQI1nB0wPvCPSU0wm4pQbZBtV8Mno3QfSVLY5IPfF5R5xSy8FYHL0hpgKXDACrvy
maMKKc0qxtzzPvCp4iEQvqeV89L53eCDt1C0w2PQe/aJ2/D1nyEjp++pX2FJDoiEf4TuIw==

Hình I.2-6. Quy trình mã hóa cụ thể của Google Admin Toolbox

Mã hoá thông tin:

- B1: Chọn thuật toán muốn mã hoá bên phải
- B2: Nhập nội dung văn bản cần mã hoá vào khung nhập
- B3: Chọn kiểu xuất theo nhu cầu
 - + Có 3 dạng xuất sẵn là “Plain Text”, “Hexadecimal Output” và “Binary Output”
 - + Nếu người dùng không lựa chọn trước, giao diện sẽ đặt mặc định “Plain Text” cho việc xuất file
- B4: Chọn gửi để xuất ra nội dung mã hoá
 - + Nếu người dùng không chọn trong những thuật toán ở cột bên phải thì giao diện sẽ báo lỗi “Hãy chọn một thuật toán mã hóa hay giải mã”
 - + Nếu người dùng không nhập nội dung văn bản cần mã hóa thì giao diện sẽ báo lỗi “Đừng bỏ trống ô nhập”

I.3. Các chức năng dự kiến của đề tài

- Đăng nhập và đăng ký tài khoản
- 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, Vigenere
 - Dạng mã hóa chuyển vị gồm: chuyển vị 2 dòng và chuyển vị nhiều dòng
 - Dạng mã hóa theo Xor gồm: Caesar, Belasco, Trithemius, Vigenere
 - Dạng mã hoá theo AES
 - Dạng mã hoá theo RSA
 - Dạng mã hóa theo SDES

I.4. Công nghệ sử dụng

- Qt Designer
- Python
- Wireframe

I.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, đề tài thực hiện việc mã hoá và giải mã các kí tự tiếng việt và các kí tự đặc biệt trong bộ kí tự của Character Map. 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 SDES và mã hoá RSA, AES.

I.6. Bố cục đề tài

- Chương 1: Giới thiệu đề tài
- Chương 2: Cơ sở lý thuyết
- Chương 3: Phân tích và thiết kế
- Chương 4: 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 và rất đa dạng trong lĩnh vực công nghệ thông tin và quản lý. Nó đề cập đến một cấu trúc tổ chức chứa thông tin, dữ liệu, quy trình và tài nguyên, với mục tiêu cung cấp một cơ sở cho việc thu thập, xử lý, lưu trữ và phân phối thông tin để đáp ứng nhu cầu và mục tiêu của một tổ chức hoặc hệ thống cụ thể.

Hệ thống thông tin là một khía cạnh cốt lõi trong môi trường công nghiệp ngày nay, không chỉ ở mức tổ chức mà còn ở mức cá nhân. Để hiểu rõ hơn về khái niệm này, chúng ta có thể xem xét một số thành phần quan trọng của hệ thống thông tin:

Phần mềm: Phần mềm đóng vai trò quan trọng trong hệ thống thông tin. Nó bao gồm các ứng dụng và chương trình máy tính được thiết kế để xử lý và quản lý dữ liệu. Điều này có thể bao gồm hệ thống quản lý cơ sở dữ liệu, ứng dụng văn phòng, phần mềm quản lý dự án và nhiều ứng dụng khác để giúp tổ chức thực hiện các nhiệm vụ cụ thể.

Phần cứng: Phần cứng là thành phần vật lý của hệ thống thông tin. Đây là các máy tính, máy chủ, thiết bị lưu trữ và mạng mà hệ thống dựa vào để đảm bảo dữ liệu và ứng dụng có nơi để tồn tại và chạy.

Dữ liệu: Dữ liệu là tài sản quý báu của hệ thống thông tin. Nó có thể là thông tin văn bản, hình ảnh, âm thanh hoặc dữ liệu số hóa khác. Quản lý và bảo vệ dữ liệu là một phần quan trọng của hệ thống thông tin.

Quy trình: Các quy trình trong hệ thống thông tin định rõ cách thông tin và dữ liệu được xử lý, truyền tải và lưu trữ. Điều này bao gồm các quy trình công việc và quy trình kỹ thuật được thiết lập để đảm bảo hiệu quả và tuân thủ.

Con người: Con người đóng vai trò quan trọng trong việc sử dụng, quản lý và bảo vệ hệ thống thông tin. Họ là người quản lý, người sử dụng và chịu trách nhiệm trong việc đảm bảo hệ thống hoạt động một cách hiệu quả và an toàn.

Hệ thống thông tin có thể tồn tại ở nhiều quy mô khác nhau, từ hệ thống thông tin cá nhân cho đến hệ thống thông tin doanh nghiệp và cả hệ thống thông tin quốc gia. Quản lý và bảo mật hệ thống thông tin là một phần quan trọng để đảm bảo rằng thông tin và dữ liệu được bảo vệ, sử dụng một cách hiệu quả và đáp ứng các mục tiêu tổ chức hoặc hệ thống.

Hệ thống thông tin cũng đóng vai trò quan trọng trong việc cung cấp thông tin cho quyết định. Từ quyết định chi tiêu tài chính cho việc điều hành một doanh nghiệp, thông tin thu thập, xử lý và trình bày qua hệ thống thông tin có thể giúp người quản lý ra quyết định thông minh dựa trên dữ liệu thực tế.

Hệ thống thông tin cũng có thể được tích hợp với các hệ thống khác trong tổ chức, ví dụ, hệ thống sản xuất hoặc hệ thống quản lý khách hàng. Điều này giúp tối ưu hóa quy trình công việc và tạo ra sự thống nhất trong việc quản lý thông tin và tài nguyên.

Trong thế giới kỹ thuật số ngày nay, hệ thống thông tin đóng vai trò quan trọng trong việc kết nối và truyền tải thông tin qua mạng Internet. Các hệ thống thông tin dựa vào mạng có thể cung cấp dịch vụ trực tuyến cho người dùng và cho phép họ truy cập thông tin từ bất kỳ đâu trên thế giới.

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

Bảo mật thông tin là một phần quan trọng của quản lý hệ thống thông tin. Với sự gia tăng của các mối đe dọa mạng và việc lưu trữ thông tin quan trọng trên các thiết bị kỹ thuật số, việc áp dụng các biện pháp bảo mật là cực kỳ quan trọng. Dưới đây là một số phương pháp bảo mật thông tin quan trọng trong hệ thống thông tin:

Mật khẩu mạnh và xác thực đa yếu tố: Sử dụng mật khẩu mạnh và đảm bảo rằng người dùng phải sử dụng xác thực đa yếu tố để truy cập hệ thống. Mật khẩu mạnh bao gồm chữ cái, số, ký tự đặc biệt và đủ dài. Xác thực đa yếu tố bao gồm cung cấp một mật khẩu cùng với mã xác thực tạm thời.

Quản lý quyền truy cập: Hạn chế quyền truy cập thông tin chỉ cho những người cần biết. Sử dụng chính sách quản lý quyền truy cập để đảm bảo rằng người dùng chỉ có quyền truy cập đến thông tin mà họ cần trong công việc của họ.

Mã hóa dữ liệu: Mã hóa dữ liệu là quá trình chuyển đổi dữ liệu thành dạng mã hóa, chỉ có thể giải mã bằng một mã. Điều này đảm bảo rằng dữ liệu không thể đọc được nếu nó rơi vào tay của kẻ tấn công.

Bảo vệ mạng: Sử dụng tường lửa và phần mềm chống virus để ngăn chặn các tấn công mạng từ bên ngoài. Đảm bảo rằng hệ thống mạng được cập nhật và bảo mật để ngăn chặn việc xâm nhập.

Sao lưu và phục hồi dữ liệu: Đảm bảo rằng có quy trình sao lưu dữ liệu định kỳ và khả năng phục hồi dữ liệu nhanh chóng trong trường hợp xảy ra sự cố hoặc tấn công mạng.

Giám sát và phát hiện xâm nhập: Sử dụng các công cụ giám sát và phát hiện xâm nhập để theo dõi hoạt động trên hệ thống và cảnh báo sớm về các hoạt động bất thường.

Chính sách và đào tạo: Thiết lập và thực hiện các chính sách bảo mật thông tin và đào tạo nhân viên về các quy định bảo mật. Điều này đảm bảo rằng tất cả nhân viên hiểu và tuân theo các quy định bảo mật.

Phân loại thông tin: Xác định mức độ quan trọng của thông tin và phân loại nó dựa trên độ nhạy cảm. Thông tin quan trọng hơn cần được bảo vệ mạnh hơn.

Kiểm tra và đánh giá liên tục: Thực hiện kiểm tra bảo mật định kỳ và đánh giá để đảm bảo rằng các biện pháp bảo mật vẫn hiệu quả và đáp ứng các yêu cầu bảo mật mới.

Bảo mật vật lý: Đảm bảo rằng thiết bị lưu trữ và máy chủ cơ sở dữ liệu được bảo vệ vật lý bằng cách sử dụng cửa kín, hệ thống kiểm soát truy cập và môi trường lý tưởng để ngăn chặn truy cập trái phép.

Bảo vệ thiết bị di động: Đối với các thiết bị di động như điện thoại thông minh và máy tính bảng, áp dụng các biện pháp bảo mật như mã hóa dữ liệu và từ chối từ xa để bảo vệ thông tin trong trường hợp thiết bị bị mất hoặc đánh cắp.

Hệ thống bảo mật IoT: Đối với hệ thống thông tin liên quan đến Internet of Things (IoT), cần đảm bảo rằng các thiết bị IoT được bảo mật và thông tin từ chúng được mã hóa và bảo vệ.

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

II.2.1. Python 3.11

Ngôn ngữ lập trình Python là một ngôn ngữ lập trình đa mục đích, thông dịch (interpreted), và dễ đọc dễ viết. Nó được tạo ra bởi Guido van Rossum và lần đầu tiên ra mắt vào năm 1991. Python nổi tiếng với cú pháp đơn giản, dễ hiểu, và linh hoạt, làm cho nó trở thành một trong những ngôn ngữ phát triển phổ biến nhất trên toàn thế giới. Dưới đây là một số đặc điểm chính của ngôn ngữ Python:

Cú Pháp Dễ Đọc và Hiểu: Python được thiết kế với cú pháp gần gũi với ngôn ngữ tự nhiên, làm cho nó dễ đọc và hiểu. Điều này giúp giảm thiểu lỗi trong mã và tạo điều kiện thuận lợi cho việc hợp tác giữa các nhà phát triển.

Tự Động Quản lý Bộ Nhớ: Python sử dụng mô hình quản lý bộ nhớ tự động (garbage collection), giúp giảm thiểu nguy cơ xảy ra lỗi về bộ nhớ như quên giải phóng bộ nhớ đã cấp phát (memory leaks).

Ngôn Ngữ Đa Mục Đích: Python có thể được sử dụng để phát triển một loạt các ứng dụng, bao gồm ứng dụng web, ứng dụng desktop, ứng dụng di động, trí tuệ nhân tạo (AI), khoa học dữ liệu, và nhiều lĩnh vực khác.

Cộng Đồng Lớn Và Hỗ Trợ Đa Dạng: Python có một cộng đồng lập trình lớn, nơi có hàng triệu nhà phát triển và nguồn tài liệu phong phú. Điều này giúp dễ dàng tìm kiếm giải pháp cho các vấn đề lập trình và học hỏi từ cộng đồng.

Thư Viện Và Frameworks: Python có một số thư viện và frameworks mạnh mẽ như NumPy, Pandas, Django, Flask, TensorFlow, và PyTorch. Điều này giúp tăng cường khả năng phát triển và giảm thiểu việc phải viết mã từ đầu.

Tương Tác Tương Tác: Python cho phép tương tác tốt, có nghĩa rằng bạn có thể thử nghiệm mã và kiểm tra các biểu thức một cách trực tiếp trong môi trường Python mà không cần biên dịch lại.

Tích Hợp Dễ Dàng: Python có khả năng tích hợp tốt với các ngôn ngữ khác như C, C++, và Java, cho phép bạn sử dụng các thư viện và mã nguồn từ các ngôn ngữ khác.

Hệ Thống Đa Nền Tảng: Python có sẵn trên hầu hết các hệ điều hành và có thể được sử dụng trên nhiều nền tảng khác nhau.

Phiên Bản và Cộng Đồng Phát Triển Liên Tục: Python có một chu kỳ phát triển liên tục, với các phiên bản mới và cải tiến được phát hành thường xuyên. Cộng đồng phát triển Python luôn đang làm việc để cải thiện ngôn ngữ và thư viện chuẩn.

Tích Hợp Không Giới Hạn: Python cho phép tích hợp không giới hạn, có nghĩa là bạn có thể sử dụng nó cho các loại ứng dụng nhỏ hoặc lớn mà không gặp sự hạn chế về quy mô hoặc loại ứng dụng.

Những đặc điểm này đã làm cho Python trở thành một ngôn ngữ lập trình phổ biến không chỉ trong ngành công nghiệp công nghệ thông tin mà còn trong các lĩnh vực như khoa học dữ liệu, trí tuệ nhân tạo, phân tích dữ liệu, và nhiều ứng dụng khác. Python là một công cụ mạnh mẽ cho các nhà phát triển và người học lập trình.

II.2.2. PyQt6 Designer

PyQt6 Designer là một phần mềm đồ họa được sử dụng để thiết kế giao diện người dùng cho ứng dụng Python bằng PyQt6, một bộ công cụ phát triển ứng dụng đồ họa dựa trên Qt. PyQt6 là một giao diện giữa Python và Qt, cho phép bạn tạo các ứng dụng đồ họa đa nền tảng với giao diện người dùng tương tác.

PyQt6 Designer có những đặc tính nổi bật có thể giúp người dùng tự do thiết kế ứng dụng của mình bằng nhiều cách:

Thiết Kế Giao Diện Người Dùng Một Cách Trực Quan: PyQt6 Designer là một công cụ đồ họa giúp bạn thiết kế giao diện người dùng của ứng dụng một cách trực quan, thay vì phải viết mã giao diện thủ công. Bạn có thể kéo và thả các phần tử giao diện như nút, ô văn bản, hộp kiểm, và cửa sổ để xây dựng giao diện một cách dễ dàng.

Hỗ Trợ Đa Nền Tảng: PyQt6 là một liên kết Python cho Qt, một framework phát triển ứng dụng đa nền tảng mạnh mẽ. Vì vậy, giao diện người dùng bạn thiết kế bằng PyQt6 Designer có thể chạy trên nhiều hệ điều hành như Windows, macOS, và Linux mà không cần sửa đổi nhiều.

Tích Hợp Với PyQt6: PyQt6 Designer hoàn hảo kết hợp với PyQt6 framework. Sau khi bạn đã thiết kế giao diện, bạn có thể sử dụng mã Python để điều khiển các phần tử giao diện và thêm logic vào ứng dụng của bạn.

Hỗ Trợ Chức Năng Gia Công Cao Cấp: PyQt6 Designer cung cấp nhiều tính năng mạnh mẽ như quản lý cửa sổ, sự kiện, đối tượng và thuộc tính. Bạn có thể tùy chỉnh giao diện người dùng của bạn theo cách mà bạn muốn, thêm các tác vụ, tương tác và tính năng phức tạp vào ứng dụng của mình.

Tạo Ứng Dụng Đa Trang: Bạn có thể tạo các ứng dụng đa trang với PyQt6 Designer bằng cách tạo và quản lý nhiều cửa sổ và trang. Điều này cho phép bạn xây dựng ứng dụng có nhiều chức năng và giao diện người dùng phức tạp.

Hỗ Trợ Tích Hợp Dự Án: PyQt6 Designer có khả năng lưu và tải các dự án giao diện. Điều này giúp bạn duyệt và chỉnh sửa lại giao diện khi cần thiết mà không cần bắt đầu từ đầu.

Thư Viện Các Chế Độ Bố Trí: PyQt6 Designer cung cấp nhiều các chế độ bố trí cho việc sắp xếp các phần tử giao diện. Bạn có thể chọn giữa các bố trí như cố định, dọc, ngang, và nhiều bố trí linh hoạt khác.

Thư Viện Các Phần Tử Giao Diện Tùy Chỉnh: PyQt6 Designer cung cấp thư viện các phần tử giao diện tùy chỉnh, cho phép bạn tạo các phần tử độc đáo và tùy chỉnh theo nhu cầu của ứng dụng.

PyQt6 Designer là một công cụ mạnh mẽ cho việc phát triển ứng dụng đồ họa với Python và Qt, giúp bạn tiết kiệm thời gian và nỗ lực trong việc thiết kế giao diện người dùng và tập trung vào việc phát triển logic ứng dụng

II.3. Mô hình MVC

Mô hình MVC (Model-View-Controller) là một mô hình kiến trúc phần mềm được sử dụng rộng rãi trong phát triển ứng dụng. Mô hình này chia ứng dụng thành ba thành phần chính:

Model (Mô hình): Đây là thành phần chịu trách nhiệm cho việc xử lý dữ liệu, logic kinh doanh và tương tác với cơ sở dữ liệu. Mô hình biểu diễn dữ liệu và quản lý trạng thái của ứng dụng. Nó không biết gì về cách hiển thị dữ liệu hoặc giao diện người dùng. Mô hình thường chứa các đối tượng hoặc lớp dữ liệu và phương thức để truy cập và xử lý dữ liệu.

View (Giao diện): View là thành phần mà người dùng tương tác. Nó hiển thị dữ liệu từ mô hình dưới dạng giao diện người dùng. View biểu diễn dữ liệu mô hình theo cách mà người dùng có thể hiểu và tương tác. Một view có thể hiển thị thông tin từ mô hình mà không can thiệp trực tiếp vào dữ liệu.

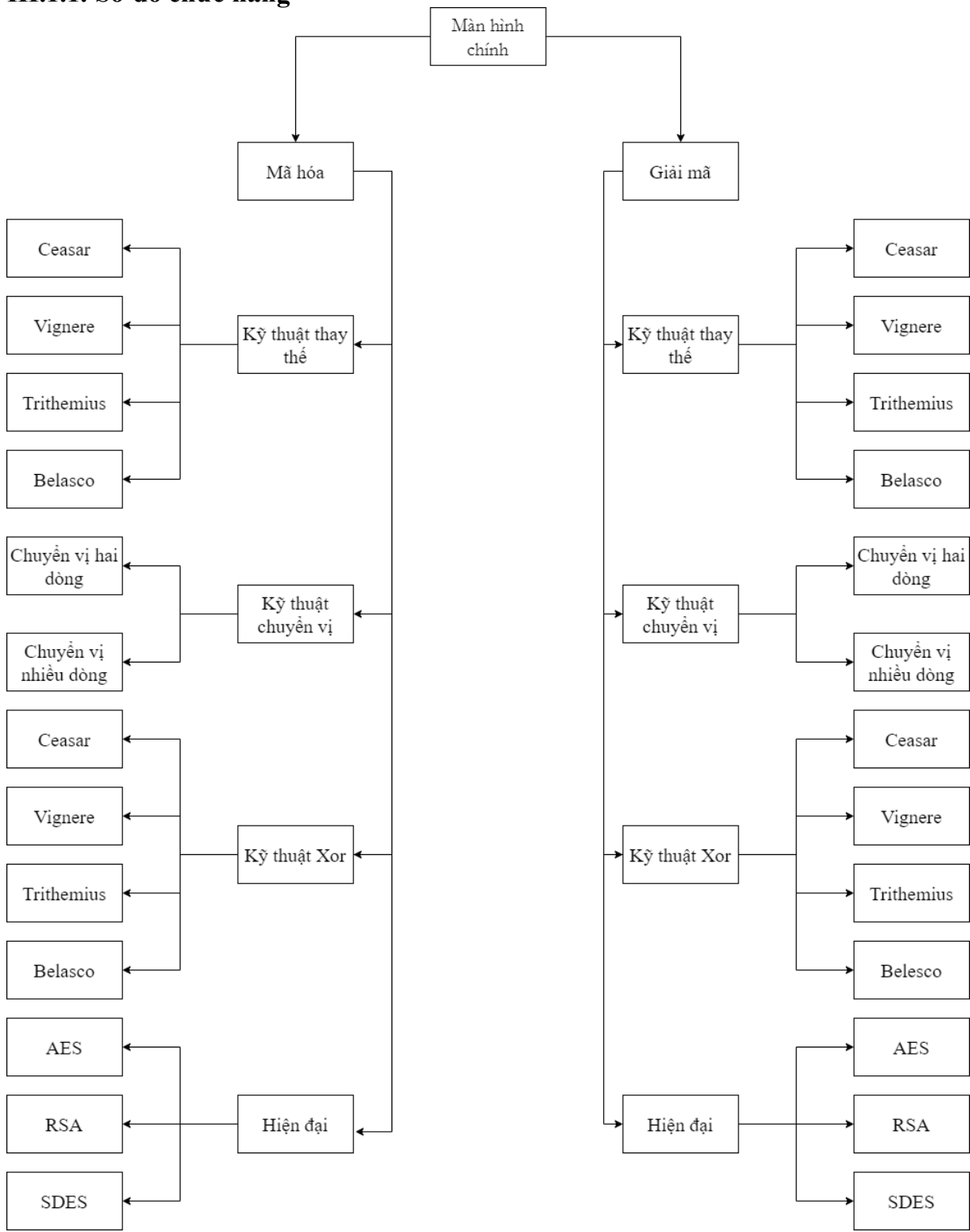
Controller (Bộ điều khiển): Controller là "trung gian" giữa mô hình và giao diện. Nó nhận các yêu cầu từ người dùng thông qua giao diện, xử lý yêu cầu đó và tương tác với mô hình để cập nhật dữ liệu nếu cần. Controller sau đó cập nhật giao diện để hiển thị thông tin mới. Nhiệm vụ của controller là quản lý luồng điều khiển của ứng dụng.

Mô hình MVC giúp tách biệt các phần khác nhau của ứng dụng, tạo điều kiện cho việc phát triển và bảo trì dễ dàng hơn. Nó cũng thúc đẩy tái sử dụng code và tăng khả năng mở rộng của ứng dụng. Với mô hình này, bạn có thể thay đổi giao diện mà không cần thay đổi logic kinh doanh và ngược lại, giúp tăng tính linh hoạt và hiệu quả trong phát triển phần mềm.

Chương III. Phân tích và thiết kế

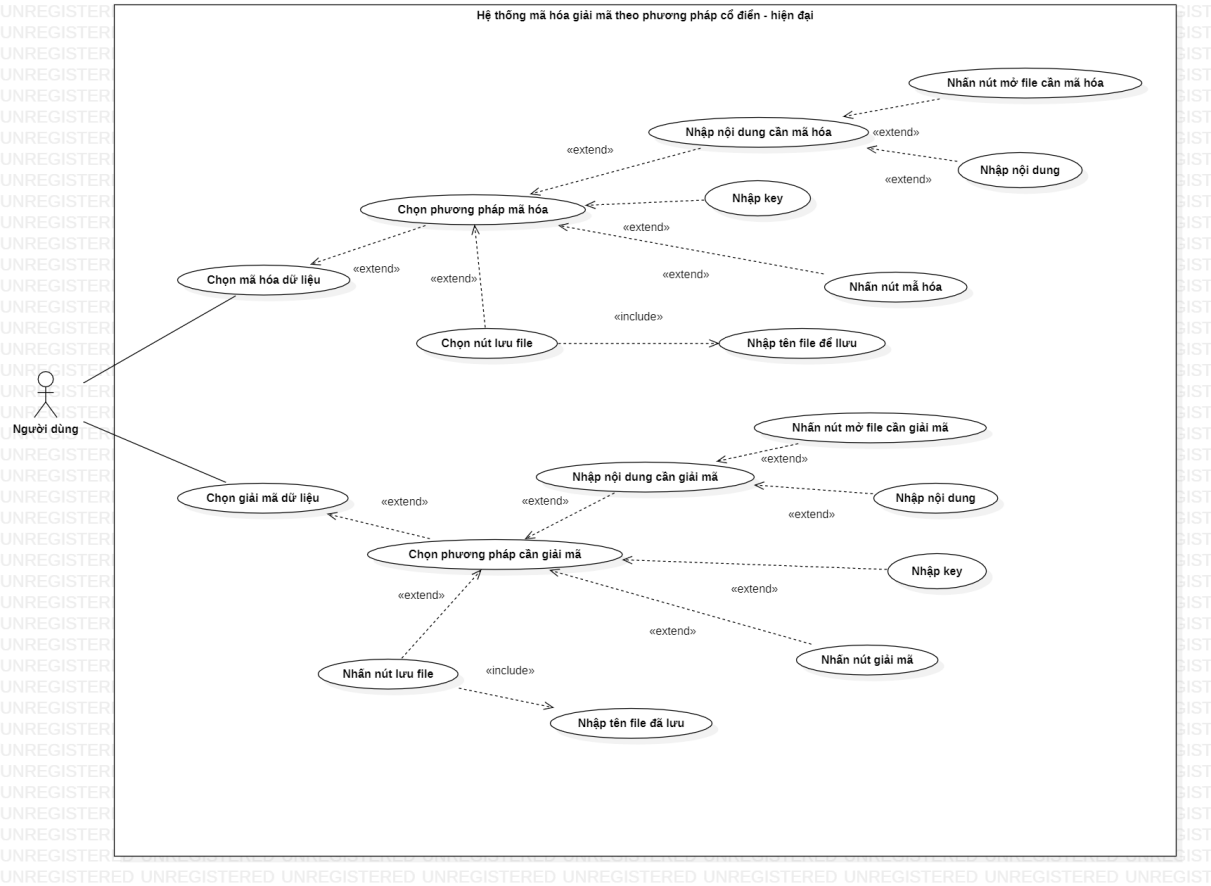
III.1. Phân tích

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.2.1.1. Wireframe giao diện màn hình chính

Giao diện màn hình chính



Hình III.2-1: Wireframe giao diện màn hình chính (1)



Hình III.2-2: Wireframe giao diện màn hình chính (2)

- Nơi thông tin lưu trữ:
 1. Tên màn hình chính, thanh menu
 2. Tên thành viên trong nhóm
 3. Cây thư mục các thuật toán mã hóa, giải mã
- Hướng dẫn xử dụng :
 - + Bước 1: Người dùng phải tiến hành tạo tài khoản và đăng nhập vào ứng dụng
 - + Nếu người dùng chưa đăng nhập vào ứng dụng thì các chức năng mã hóa, giải mã không thể nào kích hoạt
 - + Bước 2: Chọn phương thức mã hóa hoặc giải mã mình muốn

III.2.1.2. Wireframe giao diện xử lý mã hóa

Giao diện trang xử lý

Mã hóa Ceasar

Nhập nội dung cần mã hóa:

Nhập key:

Mở file Mã hóa

Nội dung đã mã hóa:

Lưu file Thoát

Hình III.2-3. Wireframe giao diện màn hình xử lý mã hóa

- Nơi thông tin lưu trữ:
 - 4. Tên màn hình mã hóa, giải mã với phương pháp đã nêu trong menu của màn hình chính
 - 5. Nội dung văn bản gốc
 - 6. Key (nếu có)
 - 7. Nội dung văn bản sau khi mã hóa, giải mã
 - 8. 3 nút (mở file, mã hóa, lưu file, thoát)
- Hướng dẫn xử dụng :
 - + Bước 1: Đọc nội dung từ file ra text editor để xử lý hoặc nhập nội dung từ bàn phím
 - + Bước 2: Nhập key (nếu có)
 - + Bước 3: Nhấn nút mã hóa hoặc giải mã để gọi thực hiện thuật toán.
 - + Bước 4: Nhấn nút lưu file để thực hiện việc lưu nội dung sau khi đã xử lý vào file và key (nếu có)

III.2.1.3. Wireframe giao diện xử lý giải mã***Giao diện trang xử lý***

Giải mã Ceasar

Nhập nội dung cần giải mã:

Nhập key:

Nội dung đã giải mã:

Mở file Giải mã

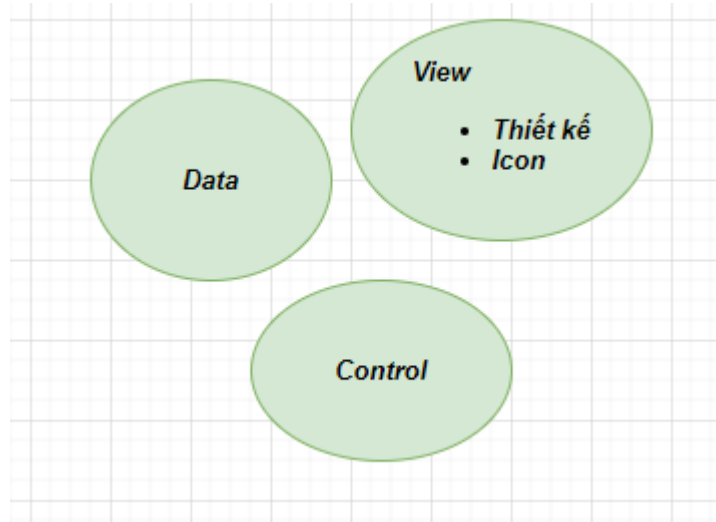
Lưu file Thoát

Hình III.2-4. Wireframe giao diện màn hình xử lý giải mã

- Nơi thông tin lưu trữ:
 1. Tên màn hình mã hóa, giải mã với phương pháp đã nêu trong menu của màn hình chính
 2. Nội dung văn bản cần giải mã
 3. Key (nếu có)
 4. Nội dung văn bản sau khi giải mã
 5. 4 nút (mở file, giải mã, lưu file, thoát)
- Hướng dẫn xử dụng :
 - + Bước 1: Đọc nội dung từ file ra text editor để xử lý hoặc nhập nội dung từ bàn phím
 - + Bước 2: Nhập key (nếu có)
 - + Bước 3: Nhấn nút mã hóa hoặc giải mã để gọi thực hiện thuật toán.
 - + Bước 4: Nhấn nút lưu file để thực hiện việc lưu nội dung sau khi đã xử lý vào file và key (nếu có)

III.3. Thiết kế xử lý

Phần mềm được xây dựng và phát triển theo mô hình 3 lớp MVC.



Hình III.3-1. Mô hình MVC

Trong đó:

- Tầng Data (Model): chứa các file về dữ liệu
- Tầng Control: chứa các file về xử lý, các thuật toán xử lý mã hóa và giải mã
- Tầng View: chứa các file giao diện màn hình chính và các giao diện mạng hình xử lý và gồm 2 thư mục con
 - Thiết kế: gồm các file thiết kế giao diện của các màn hình
 - Icon: chứa các hình ảnh được hiển thị trên màn hình, hình ảnh dùng làm background của màn hình

Chương IV. Kết luận

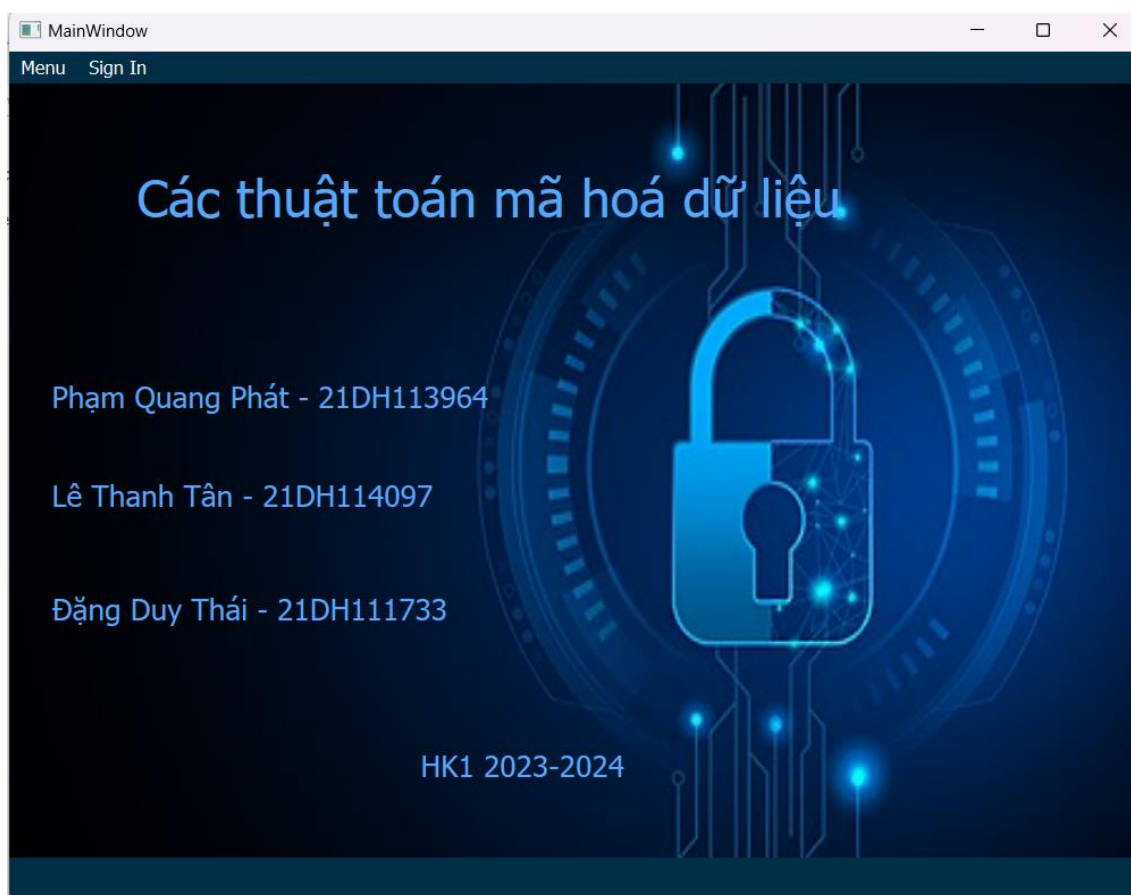
IV.1. Kết quả đạt được

Qua quá trình thực hiện đồ án, chúng em đã phát triển một phần mềm cho việc mã hóa cũng như giải mã các văn bản thông qua việc sử dụng các phương pháp mã hóa cổ điển và hiện đại. Đối với phương pháp mã hóa cổ điển, chúng em đã triển khai thành công nhiều phương pháp mã hóa và giải mã, bao gồm các phương pháp thay thế (như Ceasar, Vignere, Trithemius, Belasco), phương pháp chuyển vị gồm chuyển vị hai dòng và chuyển vị nhiều dòng và phương pháp XOR gồm các thuật toán như XOR Ceasar, XOR Vignere, XOR Trithemius, XOR Belasco.

Ngoài ra, chúng em cũng đã triển khai thành công các phương pháp mã hóa hiện đại như phương pháp mã hóa SDES (Simplified Data Encryption Standard), phương pháp mã hóa RSA (Rivest Shamir Adleman) và phương pháp mã hóa AES (Advanced Encryption Standard). Mỗi khi người dùng thực hiện xong một quy trình mã hóa hay một quá trình giải mã, họ có thể tiến hành lưu file đã được mã hóa và đặt tên cho file theo ý muốn

IV.2. Màn hình giao diện chính

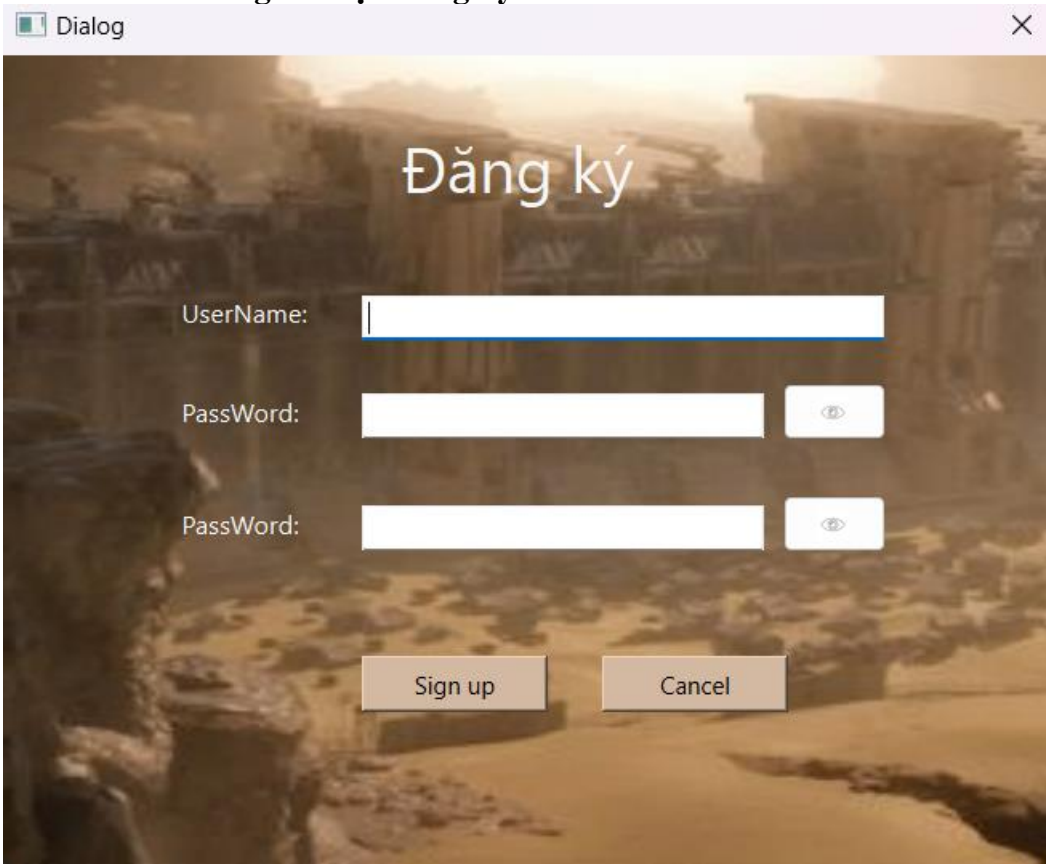
1. Màn hình giao diện giới thiệu



Hình IV.2-1: Màn hình giao diện chính

- Thông tin lưu trữ:
 - Tên màn hình: Giới thiệu.
 - Tên các thành viên của nhóm.
 - Tab mở menu để chọn các phương pháp mã hóa – giải mã.
 - Tab Đăng nhập.
- Hướng dẫn sử dụng:
 - Bước 1: Sign in (Đăng nhập). Nếu chưa đăng nhập thì phải đăng ký tài khoản trước.
 - Bước 2: Nhấn Menu để tiến hành chọn thuật toán muốn sử dụng.
 - Bước 3: Nhấn Menu chọn Thoát nếu muốn thoát ứng dụng.

2. Màn hình giao diện đăng ký



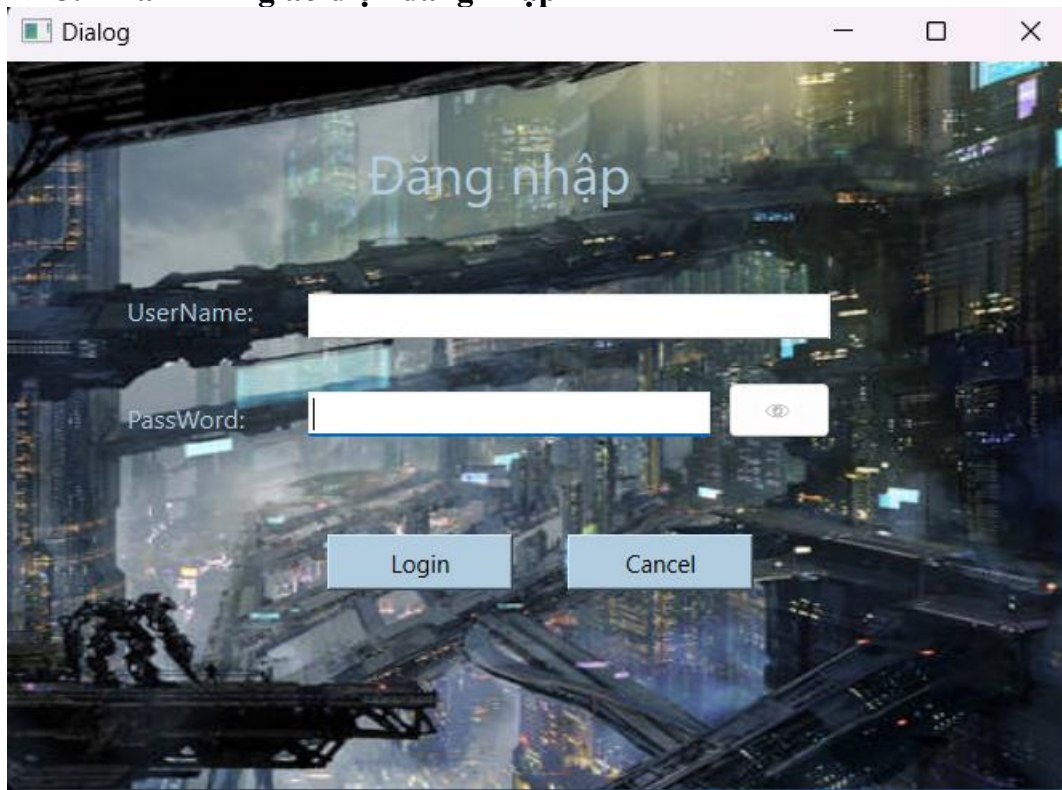
The screenshot shows a registration dialog box titled "Đăng ký". It features a background image of a desert landscape. The dialog contains three input fields: "UserName:", "PassWord:", and "PassWord:". Each field has a corresponding button to its right: a text input button for the first field, and two eye icons for the password fields. At the bottom are two buttons: "Sign up" and "Cancel".

Hình IV.2-2: Màn hình giao diện đăng ký

- Thông tin lưu trữ:
 - Tên màn hình: Đăng ký.
 - Tên người dùng.
 - Mật khẩu
 - Các nút: Sign up, Cancel và nút hiện mật khẩu.
- Hướng dẫn sử dụng:
 - Bước 1: Nhập tên người dùng.
 - Bước 2: Nhập mật khẩu.
 - Bước 3: Nhập lại mật khẩu

- Bước 4: Nhấn sign up để đăng ký hoặc nhấn cancel để hoàn tác.

3. Màn hình giao diện đăng nhập



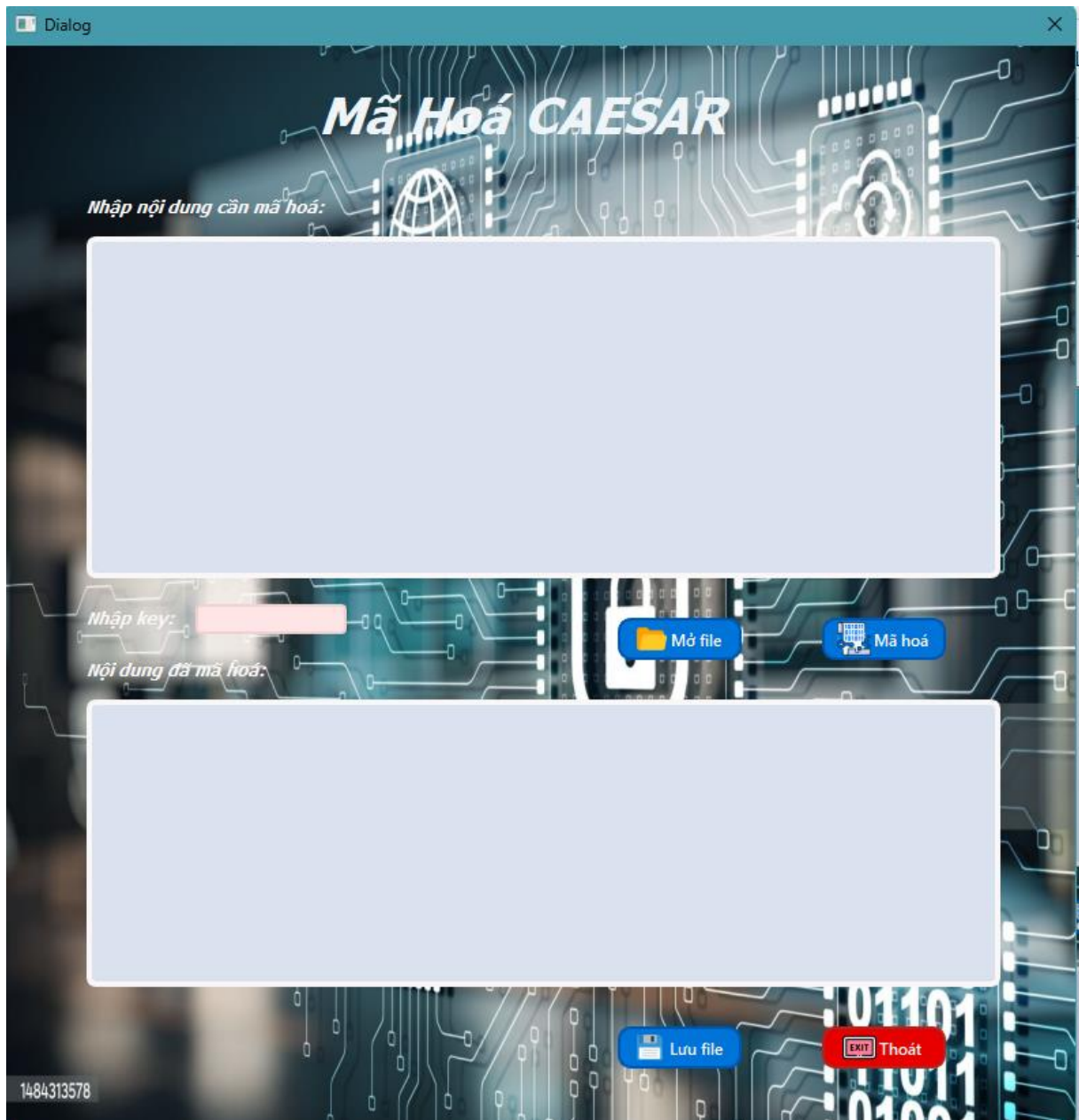
Hình IV.2-3: Màn hình giao diện đăng nhập

- Thông tin lưu trữ:
 - Tên màn hình: Đăng nhập.
 - Tên người dùng.
 - Mật khẩu
 - Các nút: Login, Cancel và nút hiện mật khẩu.
- Hướng dẫn sử dụng:
 - Bước 1: Nhập tên người dùng.
 - Bước 2: Nhập mật khẩu.
 - Bước 3: Nhấn log in để đăng nhập hoặc nhấn cancel để hoàn tác.

IV.3. Màn hình xử lý mã hoá

IV.3.1.1. Màn hình xử lý mã hoá phương pháp Thay thế

1. Màn hình giao diện xử lý mã hóa phương pháp Ceasar

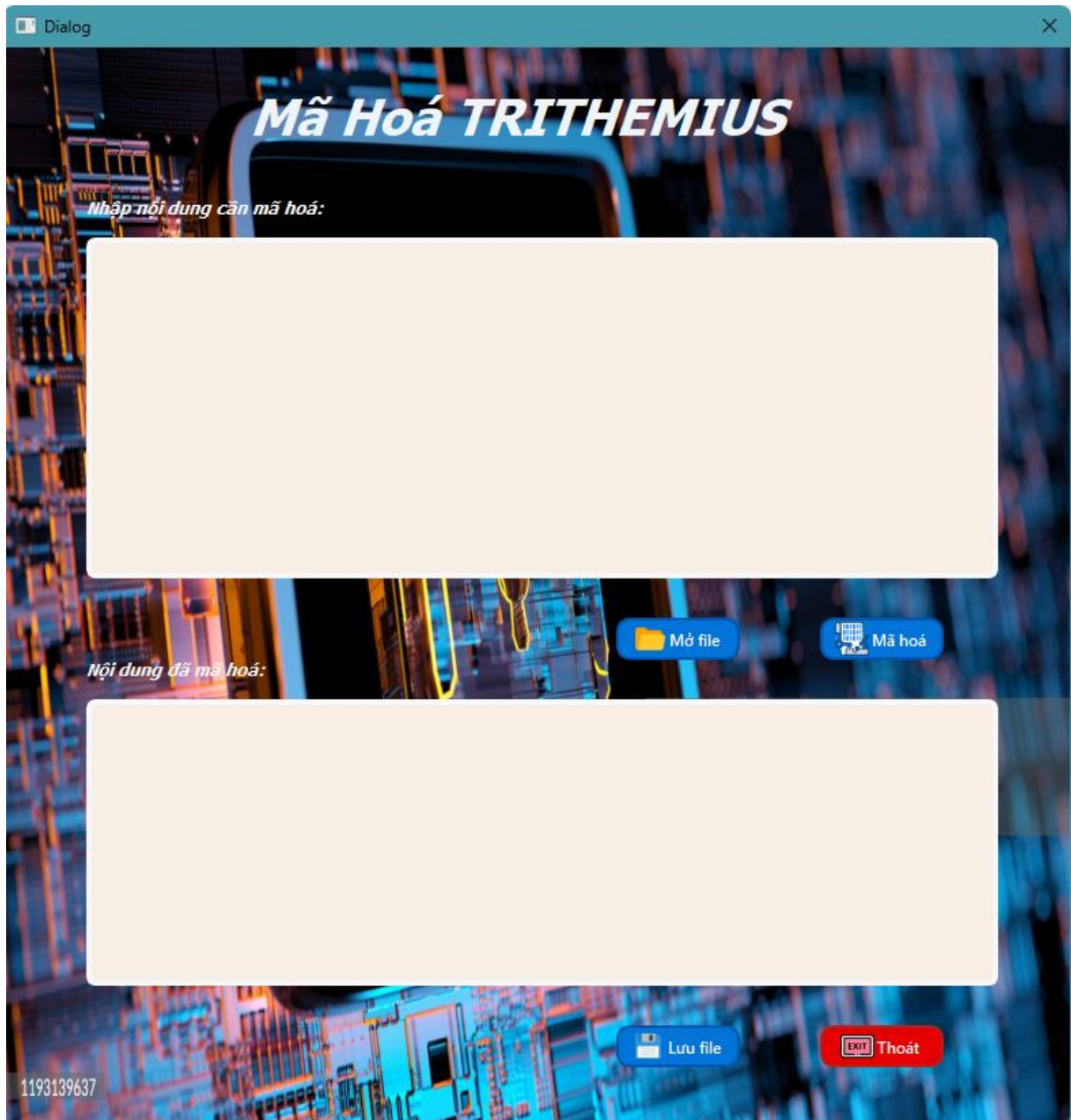


Hình IV.3-1: Màn hình giao diện xử lý mã hoá phương pháp Ceasar

- Thông tin lưu trữ:
 - Tên màn hình: Mã Hóa CAESAR.
 - Nội dung văn bản cần mã hóa nhập trực tiếp từ bàn phím hoặc mở file có sẵn.
 - Nội dung làm Key. (Số nguyên)
 - Nội dung của văn bản sau khi được mã hóa
 - Các nút: Mở file, Mã hóa, Lưu file, Thoát.

- Hướng dẫn sử dụng:
 - Bước 1: Nhập nội dung văn bản cần mã hóa
 - + Nhập trực tiếp từ bàn phím
 - + Nhấn nút Mở file để tiến hành mở file văn bản có sẵn
 - Bước 2: Nhập nội dung làm Key
 - + Nếu nội dung được dùng làm Key không phải là số nguyên thì ứng dụng sẽ không thể tiến hành mã hóa và hiển thị thông báo “Vui lòng nhập một số nguyên hợp lệ vào ô Key!”
 - Bước 3: Nhấn nút mã hóa để tiến hành thao tác mã hóa nội dung của văn bản
 - + Nếu chưa có dữ liệu ở ô Text Edit, ứng dụng sẽ không thể tiến hành mã hóa và hiển thị thông báo “"Bạn chưa nhập dữ liệu để mã hóa!"
 - + Nếu chưa có dữ liệu ở ô Key, ứng dụng sẽ không thể tiến hành mã hóa và hiển thị thông báo “"Bạn chưa nhập key!"
 - Bước 4: Nhấn lưu file để tiến hành lưu nội dung file văn bản đã được mã hóa

2. Màn hình giao diện xử lý mã hóa phương pháp Trithemius



Hình IV.3-2: Màn hình giao diện xử lý mã hoá phương pháp Trithemius

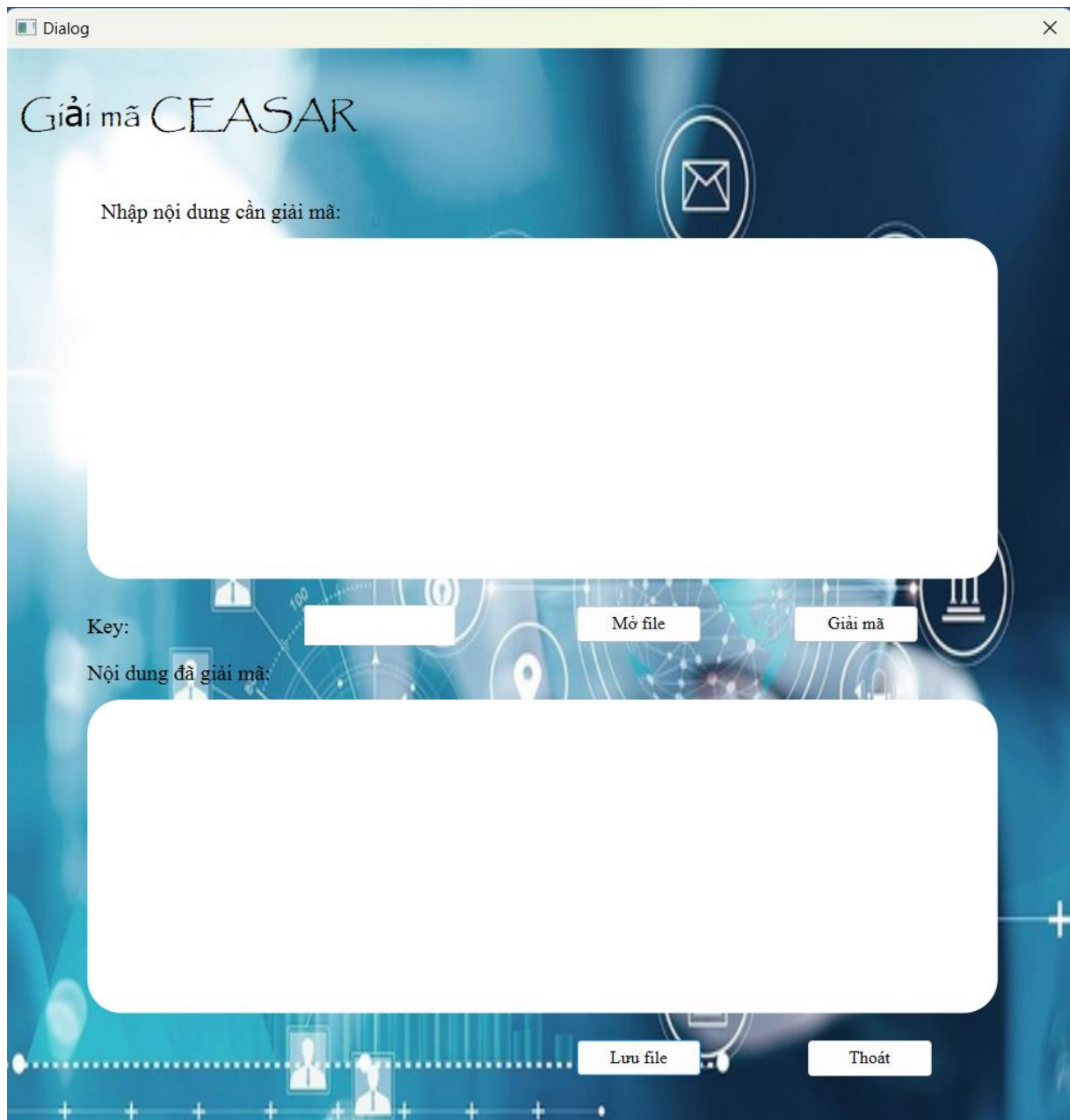
- Thông tin lưu trữ:
 - Tên màn hình: Mã Hóa TRITHEMIUS.
 - Nội dung văn bản cần mã hóa nhập trực tiếp từ bàn phím hoặc mở file có sẵn.
 - Nội dung của văn bản sau khi được mã hóa
 - Các nút: Mở file, Mã hóa, Lưu file và Thoát.

- Hướng dẫn sử dụng:
 - Bước 1: Nhập nội dung văn bản cần mã hóa
 - + Nhập trực tiếp từ bàn phím
 - + Nhấn nút Mở file để tiến hành mở file văn bản có sẵn
 - Bước 2: Nhấn nút mã hóa để tiến hành thao tác mã hóa nội dung của văn bản
 - + Nếu chưa có dữ liệu ở ô Text Edit, ứng dụng sẽ không thể tiến hành mã hóa và hiển thị thông báo ""Bạn chưa nhập dữ liệu để mã hóa!"
 - Bước 3: Nhấn lưu file để tiến hành lưu nội dung file văn bản đã được mã hóa

IV.4. Màn hình xử lý giải mã

IV.4.1.1. Màn hình xử lý giải mã theo kỹ thuật thay thế

1. Màn hình xử lý giải mã theo kỹ thuật Ceasar

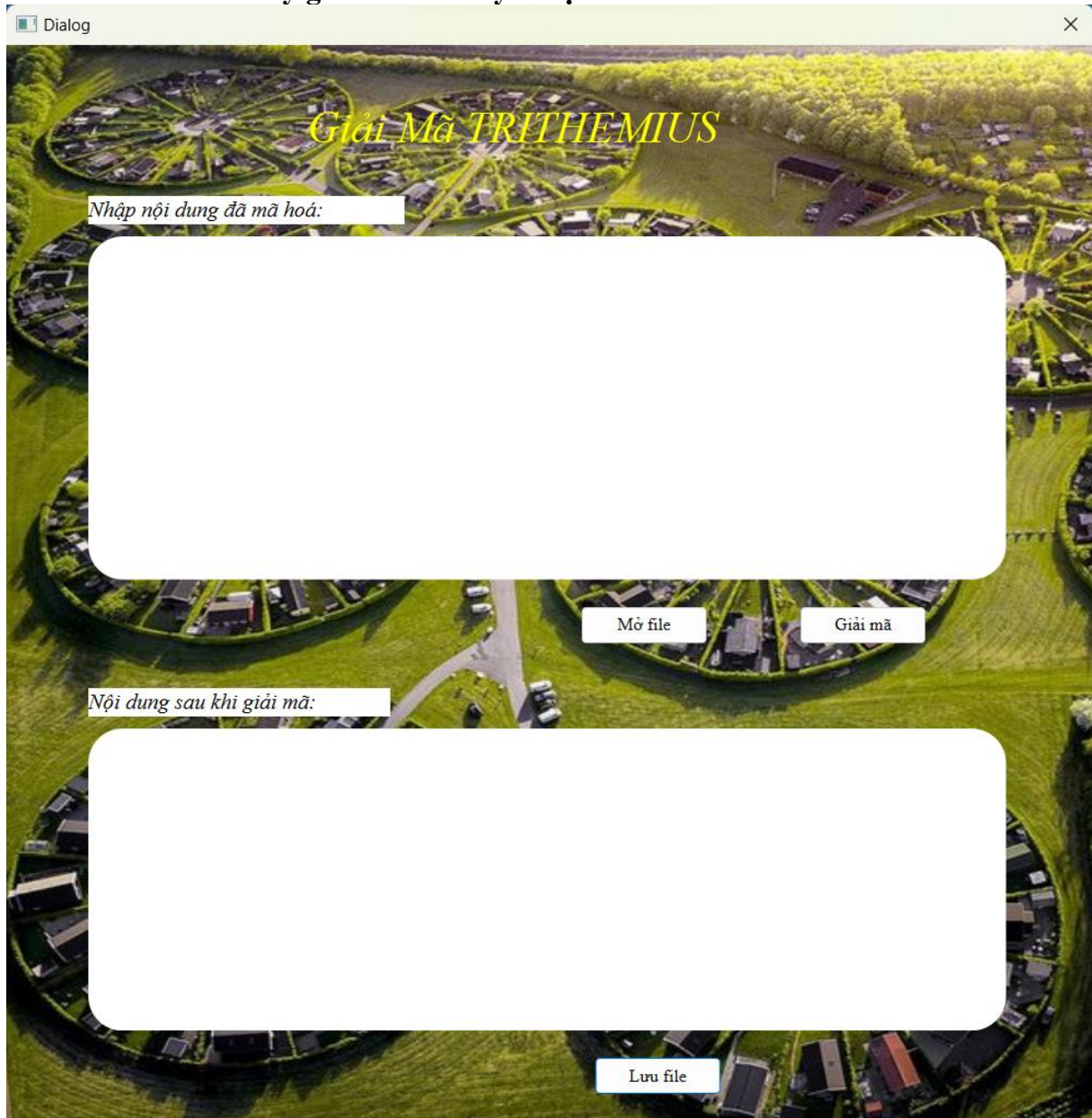


Hình IV.4-1: Màn hình giao diện xử lý giải mã theo kỹ thuật Ceasar

- Thông tin lưu trữ:
 - Tên màn hình: Giải mã Ceasar.
 - Nội dung văn bản đã được mã hóa.
 - Key.
 - Nội dung văn bản sau khi giải mã.
 - Các nút: mở file, giải mã, lưu file, thoát.

- Hướng dẫn sử dụng:
 - + Bước 1: đọc nội dung từ file ra text editor để xử lý
 - + Bước 2: Nhập key
 - + Bước 3: Nhấn nút giải mã để gọi thực hiện thuật toán.
 - + Bước 4: Nhấn nút lưu file để thực hiện việc lưu nội dung sau khi đã xử lý vào file và key

2. Màn hình xử lý giải mã theo kỹ thuật Trithemius



Hình IV.4-2: Màn hình giao diện xử lý giải mã theo kỹ thuật Trithemius

- Thông tin lưu trữ:
 - Tên màn hình: Giải mã Trithemius
 - Nội dung văn bản đã được mã hóa.
 - Nội dung văn bản sau khi giải mã.
 - Các nút: mở file, giải mã, lưu file.

- Hướng dẫn sử dụng:
 - + Bước 1: đọc nội dung từ file ra text editor để xử lý.
 - + Bước 2: Nhấn nút giải mã để gọi thực hiện thuật toán.
 - + Bước 3: Nhấn nút lưu file để thực hiện việc lưu nội dung sau khi đã xử lý vào file

IV.5. Hướng phát triển

Trong tương lai sẽ, nhóm sẽ hướng tới các mục tiêu:

- Cải thiện hiệu suất cho các thuật toán mã hoá, giúp mã hoá và giải mã các tập dữ liệu lớn hơn và nhanh chóng hơn.
- Tăng cường tính an toàn và bảo mật trên hệ thống
- Bổ sung thêm các thuật toán mã hoá hiện đại.
- Cải thiện giao diện người dùng giúp người dùng sử dụng thoải mái, tăng tính thân thiện đối với người dùng.
- Phát triển thêm các chức năng đăng nhập, đăng ký tài khoản cho phép người dùng có thể sử dụng cloud để lưu trữ các tệp mã hoá.
- Phát triển ứng dụng trên cả hai nền tảng Web và Mobile giúp người dùng có thể tự do sử dụng ứng dụng ở bất cứ đâu
- Triển khai thêm hệ thống sao lưu và khôi phục dữ liệu giúp cho người dùng có thể dễ dàng khôi phục dữ liệu trong trường hợp cần thiết

Tài liệu tham khảo

- [1] Britannica, "Information System," Britannica, 3 4 2023. [Online]. Available: <https://www.britannica.com/topic/information-system>.
- [2] 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>.
- [3] 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>.
- [4] Ths. Phạm Đức Thành, "Bài giảng môn Bảo Mật Hệ Thống Thông Tin, Khoa Công Nghệ Thông Tin, Trường Đại Học Tin Học - Ngoại Ngữ TP HCM. 2023
- [5] OpenAI, "Chat GPT (Generative Pre-trained Transformer 3)," 2020. [Online]. Available: <https://chat.openai.com>.
- [6] Nguyễn Quân, "Thuật toán mã hóa và giải mã DES," Nguyễn Quân - ICT Blog, 2017. [Online]. Available: <https://nguyenquanicd.blogspot.com/2017/08/background-thuat-toan-ma-hoa-va-ma-hoa.html>
- [7] Getty Images, "data protection concept," Viblo, 23 2 2017. [Online]. Available: <https://www.gettyimages.com/photos/data-protection-concept?assettype=image&license=rf&alloweduse=availableforalluses&family>
- [8] Color Hunt, "Popular Color Palettes on Color Hunt,".[<https://colorhunt.co/palettes/popular>].
- [9] Viblo, "Cách hoạt động của SHA-256," Zunokie, 9 9 2021. [Online]. Available: <https://viblo.asia/p/cach-hoat-dong-cua-sha-256-1VgZvJPmZAw>.
- [10] Viblo, "Cấu trúc và thuật toán Advanced Encryption Standard (Chuẩn mã hóa nâng cao)," Phạm Hoàng Anh, 17 4 2018. [Online]. Available: <https://viblo.asia/p/cau-truc-va-thuat-toan-advanced-encryption-standard-chuan-ma-hoa-nang-cao-924lJYe8ZPM>.

Phụ lục*Bảng 1. Bảng phân công công việc*

Stt	Nội dung thực hiện	Phạm Quang Phát 21DH113964	Lê Thanh Tân 21DH114097	Đặng Duy Thái 21DH111733
1	Có trách nhiệm tự 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 hiểu và trình bày báo cáo	X	X	X