Bộ Giáo Dục Và Đào Tạo

Trường Đại Học Ngoại Ngữ - Tin Học TP.HCM

KHOA CÔNG NGHỆ THÔNG TIN

BÀI BÁO CÁO

KẾT THÚC HỌC PHẦN HỌC KỲ I

NĂM HỌC 2023-2024

Môn học: Bảo mật hệ thống thông tin

Đề tài:

PHẦN MỀM MÃ HOÁ VĂN BẢN TIẾNG VIỆT

Giảng viên hướng dẫn: **ThS. Phạm Đức Thành**

Nhóm 14: Đặng Trần Hoàng Phú Quý – 21DH112864

Nguyễn Ngọc Kiều Nhi– 21DH112759

Nguyễn Hữu Bình – 21DH113496

Thành Phố Hồ Chí Minh, tháng 11 năm 2023

Mục lục

Danh mục hình

Chương I: Giới thiệu đề tài

I.1. Giới thiệu

I.1.1. Mở đầu

Trong thời đại công nghệ trên toàn thế giới bao gồm cả Việt Nam đang phát triển vượt bậc. Đặc biệt là những sự phát triển của các trang web, các ứng dụng đáp ứng những nhu cầu cần thiết, những tiện ích giúp người dùng sử dụng một cách hiệu quả như tìm kiếm, tra cứu thông tin, thực hiện giao dịch qua ứng dụng, trao đổi, kinh doanh mua bán và nhiều hành động khác. Các trang mạng và ứng dụng được xem là một công cụ thông dụng ở thời điểm hiện tại.

Tuy nhiên, khi các giao dịch trao đổi thông tin qua các ứng dụng và trang mạng thì việc bảo mật và an ninh cho các thông tin đấy cũng rất cần thiết. Việc được bảo đảm an ninh, bảo mật cho những thông tin cá nhân là một vấn đề lớn cho những người sử dụng vì sự đảm bảo về thông tin ở những trang mạng, ứng dụng tràn lan không được xác thực. Một số ví dụ cho những hành động gây tác động ảnh hưởng toàn cầu như Yahoo đã thông báo rằng họ đã bị tấn công vào năm 2013-2014 và thông tin cá nhân của hơn một tỷ tài khoản đã bị đánh cắp. Đây là một trong những cuộc tấn công lớn nhất đối với dữ liệu cá nhân trong lịch sử. Cuộc tấn công của WannaCry vào năm 2017: Đây là một trong những cuộc tấn công ransomware lớn nhất trong lịch sử và gây ra thiệt hại lớn cho nhiều tổ chức trên khắp thế giới.

Theo thống kê của NCS, 6 tháng đầu năm 2023 số lượng tấn công An ninh mạng vào các hệ thống của Việt Nam là 5.100 vụ việc, giảm khoảng 12% so với năm 2022. Tuy nhiên các vụ tấn công có chủ đích APT vào các cơ sở trọng yếu lại tăng khoảng 9% so với cùng kỳ năm 2022. Nguyên nhân là các cơ sở trọng yếu luôn có nhiều dữ liệu quan trọng và ảnh hưởng lớn nên là đích nhắm ưa thích của hacker. Các chuyên gia NCS cho biết, các chiến dịch tấn công APT vào hệ thống mạng tại Việt Nam trong 6 tháng đầu năm tập trung vào 3 hình thức tấn công chính: Tấn công người dùng thông qua email, nội dung email giả mạo có file đính kèm mã độc dạng file văn bản hoặc có đường link đăng nhập giả mạo để chiếm tài khoản người dung. Tấn công thông qua lỗ hổng của phần mềm trên máy chủ, trong đó nhiều nhất là các hệ thống sử dụng phần mềm của Microsoft như Exchange, SharePoint; Tấn công thông qua các lỗ hổng của website, đặc biệt là lỗ hổng SQL Injection hoặc qua dò mật khẩu quản trị website, máy chủ.

Vì vậy trong công cuộc đấu tranh phòng chống về tấn công người dùng vẫn còn rất nhiều hạn chế và vấn đề.

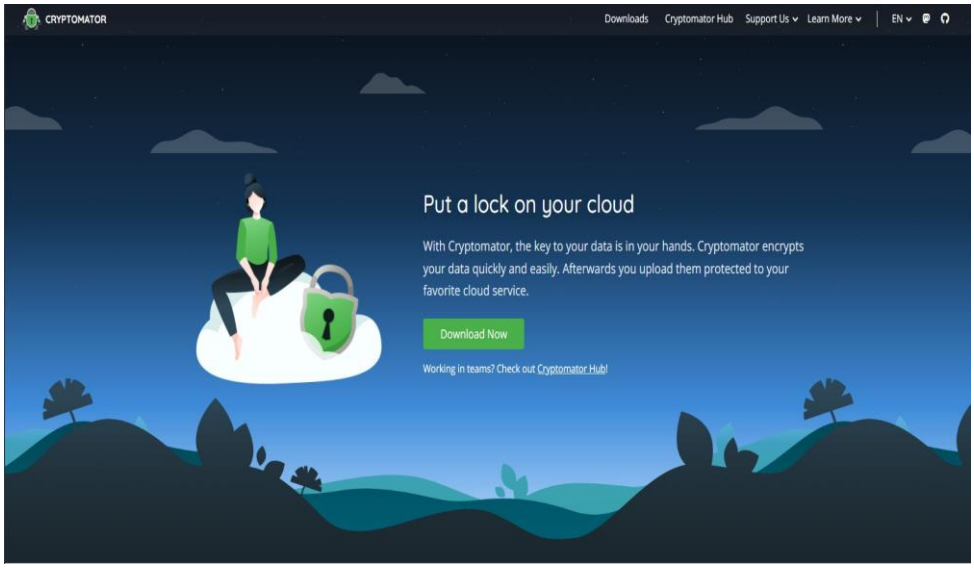
I.1.2. Lý do chọn đề tài

Đề tài được thực hiện nhằm giúp người dùng hiểu rõ cách hoạt động của các phương pháp mã hóa cổ điển và lý do các phương pháp được sử dụng.

I.2. Khảo sát thực tế

I.2.1. Các ứng dụng cụ thể

❖ ***Cryptomator***



Hình 1. Ứng dụng tham khảo Cryptomator

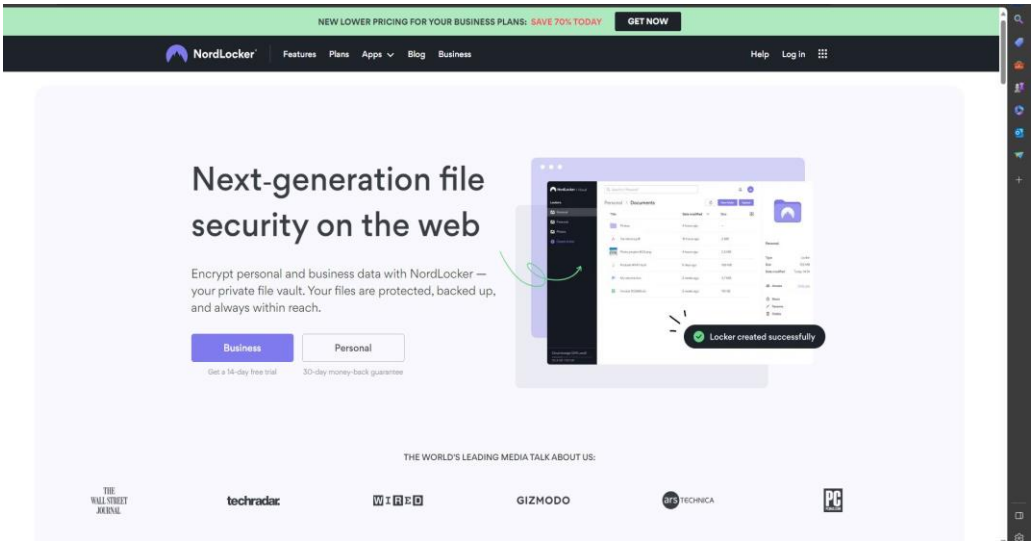
- ***Gồm những thông tin:***
  - Ứng dụng Cryptomator giúp tạo các ổ đĩa được mã hóa. Có thể dễ dàng bảo mật dữ liệu và tránh bị khai thác dữ liệu đó
  - Cryptomator được tạo ra với mục tiêu bảo vệ dữ liệu cá nhân và quyền riêng tư của người dùng trước các mối đe dọa trực tuyến.
- ***Gồm những chức năng:***
  - Mã hóa dữ liệu :Sử dụng mã hóa đối xứng AES với khóa 256-bit để đảm bảo an toàn và bảo mật.
  - Tích hợp với dịch vụ lưu trữ đám mây: Tích hợp chặt chẽ với các dịch vụ lưu trữ đám mây phổ biến như Google Drive, Dropbox, OneDrive, và nhiều dịch vụ khác.

❖ *Boxcryptor*

Hình 2. Ứng dụng tham khảo Boxcryptor

- ***Gồm những thông tin:***
  - Boxcryptor là một ứng dụng mã hóa dữ liệu giúp bảo vệ thông tin cá nhân và quan trọng của người dùng trước các mối đe dọa trực tuyến
- ***Gồm những chức năng:***
  - Hỗ trợ dự án và doanh nghiệp: Cung cấp các tính năng và gói dịch vụ được tối ưu hóa cho doanh nghiệp và môi trường làm việc nhóm, bao gồm quản lý tài khoản và quyền hạn người dùng.
  - Mã nguồn đóng và mã nguồn mở: có một phiên bản mã nguồn đóng cùng với phiên bản mã nguồn mở (Cryptomator), cho phép người dùng kiểm soát mã nguồn và tận dụng tính mở của nó.

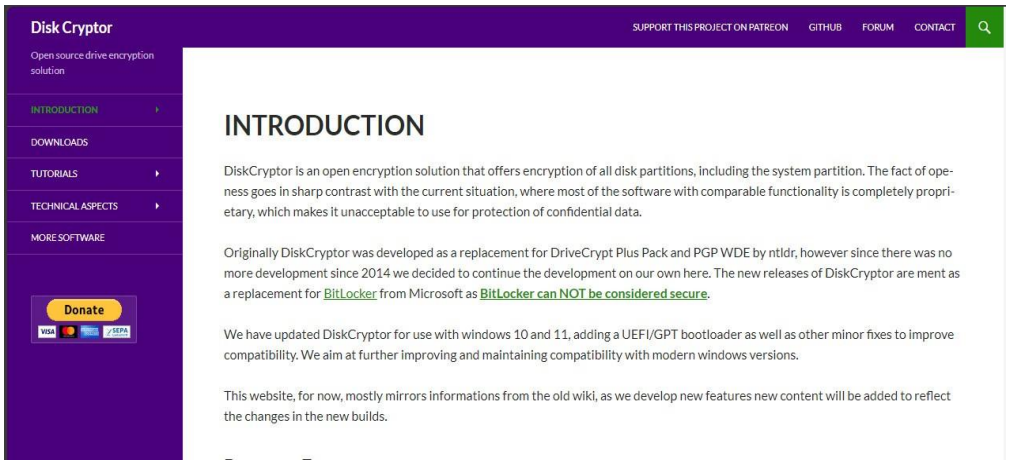
❖ *NordLocker*



Hình 3. Ứng dụng tham khảo NordLocker

- ***Gồm những thông tin:***
  - NordLocker là một dịch vụ mã hóa tệp tin và thư mục của NordVPN, được tạo ra để giúp người dùng bảo vệ dữ liệu cá nhân của họ.
- ***Gồm những chức năng:***
  - Mã hóa dữ liệu: NordLocker cung cấp khả năng mã hóa dữ liệu cá nhân của bạn bằng cách sử dụng mã hóa đối xứng AES với khóa 256-bit.
  - Bảo mật tích hợp với hệ thống tệp tin hiện đại: NordLocker sử dụng cơ sở dữ liệu tệp tin hiện đại như JSON để đảm bảo tính toàn vẹn và bảo mật của dữ liệu.

❖ ***DiskCryptor***

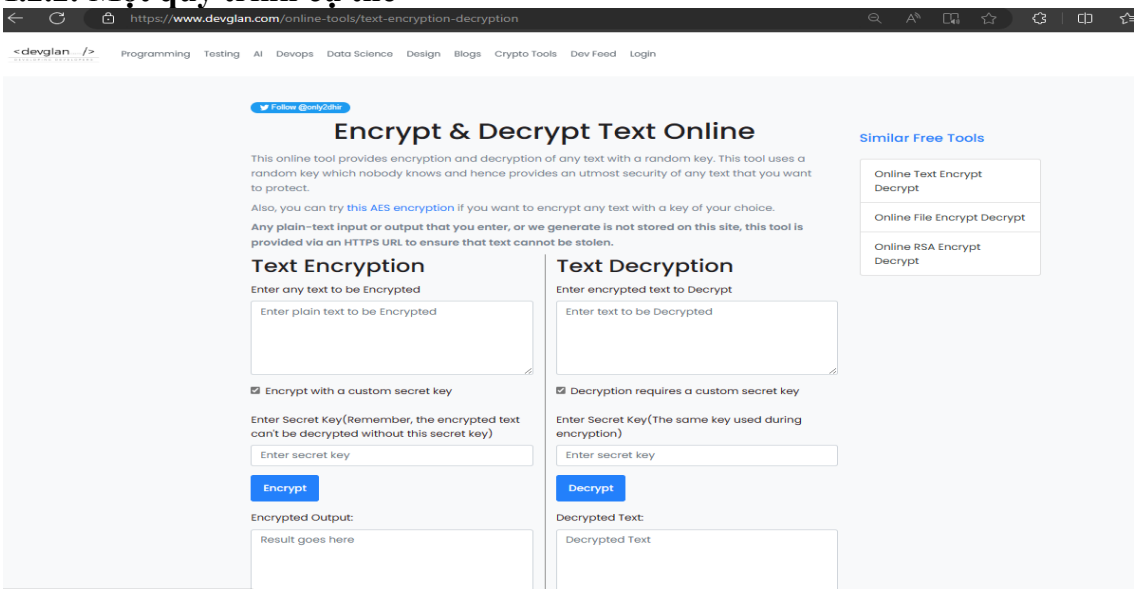


Hình 4. Ứng dụng tham khảo DiskCryptor

- ***Gồm những thông tin:***
  - DiskCryptor là một ứng dụng mã hóa toàn bộ ổ đĩa, được thiết kế để bảo vệ dữ liệu trên cấp độ hệ điều hành.
- ***Gồm những chức năng:***

- Mã hóa toàn bộ ổ đĩa:Chức năng chính của DiskCryptor là mã hóa toàn bộ ổ đĩa, bao gồm cả hệ điều hành, tất cả các tệp tin, và không gian chưa phân bổ trên ổ đĩa
- Hỗ trợ nhiều thuật toán mã hóa: hỗ trợ sử dụng nhiều thuật toán mã hóa khác nhau như AES, Twofish, và Serpent,
- Hỗ trợ Pre-Boot Authentication (PBA): hỗ trợ Pre-Boot Authentication, có nghĩa là bạn phải nhập mật khẩu trước khi hệ thống khởi động.

I.2.2. Một quy trình cụ thể



Hình 5. Màn hình thực hiện quy trình mã hóa – giải mã

- Bước 1: Nhập văn bản cần mã hóa – giải mã vào ô Text
- Bước 2: Nếu chọn tạo với key, nhập key vào ô secret key
- Bước 3: Ấn chọn nút mã hóa – giải mã
- Bước 4: Văn bản đã được mã hóa – giải mã sẽ hiện ở phần output.

I.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, Vignere
  - Dạng mã hóa chuyển vị gồm: chuyển vị 2 dòng và chuyển vị nhiều dòng
  - Dạng mã hóa theo Xor gồm: Caesar, Belasco, Trithemius, Vignere
  - Dạng mã hoá theo DES
  - Dạng mã hoá theo RSA
  - Dạng mã hóa theo AE

I.4. Công nghệ sử dụng

- Qt Designer

- Python
- Visual Studio Code
- Figma

I.5. Phạm vi giới hạn

Đề tài được tổng hợp lý thuyết cơ bản về bảo mật hệ thống thông tin, các phương pháp mã hóa cổ điển và hiện đại phổ biến. Phần ứng dụng demo của đề tài được sử dụng ngôn ngữ Python để triển khai. Trong đề tài này có các chuyển đổi mã hóa – giải mã kí tự Unicode và kí tự đặc biệt trong Character Map.

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 tập hợp nhiều yếu tố được tích hợp và có mối liên hệ mật thiết với nhau. Nó đảm nhiệm vai trò cung cấp, thu thập, xử lý và trao đổi thông tin trên nền tảng mạng dữ liệu.

Nguồn lực được sử dụng trong hệ thống thông tin là con người và công nghệ. sự kết hợp giữa các yếu tố này tạo nên một khối dữ liệu khổng lồ và xử lý, cấu thành các sản phẩm thông tin như một đầu ra của hệ thống thông tin.

Thông qua các hoạt động xử lý thông tin bao gồm: tiếp nhận, truyền, xử lý, lưu trữ, tìm kiếm, hiển thị thông tin; các nguồn dữ liệu nguyên bản thô sơ trở thành các sản phẩm thông tin hữu ích.

Hệ thống thông tin cho phép người dùng nhập dữ liệu vào hệ thống. Thông qua phần mềm, các dữ liệu đã được ghi nhớ sẽ trải qua quá trình xử lý như: phân tích, tính toán, sắp xếp,... thành các thông tin được lưu trữ theo hệ thống. Hệ thống thông tin cho phép người dùng có thể tìm kiếm, xem hoặc in ra các dữ liệu như biểu mẫu, thông báo, đồ thị, báo cáo,...

Vai trò quan trọng nhất của hệ thống thông tin là lưu trữ các thông tin dưới một hệ thống có các định dạng khác nhau, theo các tệp, file riêng biệt theo từng nội dung.

Bên cạnh việc thu thập và quản lý thông tin, hệ thống thông tin trở thành một bộ phận trọng yếu của bất kỳ một hệ thống tổ chức, doanh nghiệp nào. Nó nằm ở trung tâm của tổ chức, doanh nghiệp và là một tài sản vô hình, đem lại sự kết nối giữa tổ chức với môi trường bên ngoài xã hội. Đồng thời, nó cũng đem lại hiệu quả cho hoạt động quản lý cho tổ chức doanh nghiệp.

Các loại hệ thống thông tin thường thấy có thể kể đến hệ thống thông tin quản lý, hệ thống thông tin báo cáo, hệ thống thông tin điều hành,...

II.1.2. Các phương pháp bảo mật 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 nhập trái phép, gián đoạn hoặc phá hủy. InfoSec bao gồm bảo mật vật lý và môi trường, kiểm soát truy nhập và an ninh mạng. Một số ví dụ về các phương pháp bảo mật như:

Network Intrusion Prevention: hay còn được biết đến với tên gọi – **Network IPS** là hệ thống ngăn chặn xâm nhập. Giải pháp được phát triển bởi công ty phần mềm an ninh toàn cầu nổi tiếng của **Mỹ – Trellix**. Dựa trên việc so sánh nội dung với các cuộc xâm nhập đã được biết đến, Network IPS có khả năng phát hiện và phòng chống các cuộc tấn công,

xâm nhập mạng. Công cụ này của Trellix được **Gartner** – công ty nghiên cứu và tư vấn công nghệ thông tin hàng đầu thế giới đánh giá cao. Thị phần dẫn đầu trong mảng thiết bị phát hiện và phòng chống xâm nhập mạng đã chứng minh hiệu quả của **Network IPS**.

Network Access Control (ForeScout NAC): là giải pháp giúp tổ chức, doanh nghiệp bảo mật mạng thông qua việc kiểm soát truy cập. Bằng cách này sẽ ngăn chặn truy cập bất hợp pháp từ máy tính lạ, thiết bị lạ, máy khách hoặc các máy không tuân thủ chính sách truy cập tổ chức. Giải pháp này được Gartner & Forrester đánh giá đứng đầu về công nghệ NAC và khả năng triển khai dễ dàng.

Advanced Malware Analysis và **APT Defense** là bộ công cụ chuyên dụng phục vụ phân tích các mã độc nâng cao. Từ đó phát hiện và định danh các tấn công nâng cao có chủ đích, tấn công Zero-day và Bot.

Web Application Firewall (WAF) – Tường lửa ứng dụng Web được thiết kế bởi hãng **PTsecurity**. Đây là giải pháp giúp bảo vệ hệ thống khỏi những cuộc tấn công khai thác lỗ hổng ứng dụng (Cross-site scripting (XSS), SQL Injection,…), lỗ hổng Zero-day,… WAF sẽ thực thi các chính sách bảo mật dựa trên các dấu hiệu tấn công, triển khai giám sát, phân tích lưu lượng HTTP/ HTTPS ra vào ứng dụng Web.

Check Point Maestro Hyperscale: Là giải pháp đến từ công ty an ninh mạng hàng đầu thế giới Check Point, Maestro Hyperscale tận dụng tất cả tài nguyên phần cứng, tối đa hóa công suất thiết bị và nâng cao hiệu năng của hệ thống.

II.1.3. Thiết lập các biện pháp an toàn thông tin ở mức cơ bản

- Đánh giá rủi ro: Xác định các rủi ro bảo mật trong hệ thống.
- Xây dựng chính sách bảo mật: Lập chính sách chi tiết về bảo mật.
- Xác thực và ủy quyền: Sử dụng xác thực mạnh mẽ và quản lý quyền truy cập.
- Bảo vệ dữ liệu: Mã hóa dữ liệu quan trọng và tạo sao lưu định kỳ.
- Giám sát và phát hiện xâm nhập: Thiết lập hệ thống giám sát và phát hiện xâm nhập.
- Đào tạo và nhận thức bảo mật: Đào tạo nhân viên về bảo mật.
- Cập nhật và bảo trì: Cập nhật hệ thống và phần mềm đầy đủ.
- Kiểm tra thẩm định bảo mật: Thực hiện kiểm tra thẩm định bảo mật định kỳ.
- Giám sát và đánh giá liên tục: Liên tục giám sát và đánh giá hiệu quả của biện pháp an toàn thông tin.

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

II.2.1.1. Python 3.12.0

Python là một ngôn ngữ lập trình dễ học, mạnh mẽ. Nó có cấu trúc dữ liệu cao cấp hiệu quả và một cách tiếp cận đơn giản nhưng hiệu quả đối với lập trình hướng đối tượng. Cú pháp lịch lãm của Python và kiểu dữ liệu động, kết hợp với tính chất thông dịch, khiến nó trở thành một ngôn ngữ lý tưởng cho việc viết mã kịch bản và phát triển ứng dụng nhanh chóng trong nhiều lĩnh vực trên hầu hết các nền tảng.

Trình thông dịch Python và thư viện tiêu chuẩn phong phú có sẵn miễn phí dưới dạng mã nguồn hoặc mã nhị phân cho tất cả các nền tảng chính từ trang web Python và có thể được phân phối miễn phí. Trang web này cũng chứa các bản phân phối và liên kết đến nhiều mô-đun Python bên thứ ba miễn phí, các chương trình và công cụ, cùng với tài liệu bổ sung.

Trình thông dịch Python có thể mở rộng dễ dàng bằng các chức năng và kiểu dữ liệu mới được triển khai bằng C hoặc C++ (hoặc các ngôn ngữ khác có thể gọi từ C). Python cũng thích hợp như một ngôn ngữ mở rộng cho các ứng dụng có thể tùy chỉnh.

Python 3.12 là phiên bản ổn định mới nhất của ngôn ngữ lập trình Python, với sự kết hợp của những thay đổi trong ngôn ngữ và thư viện tiêu chuẩn. Các thay đổi trong thư viện tập trung vào việc làm sạch các API đã bị loại bỏ, tính sử dụng và tính chính xác. Đáng chú ý, gói distutils đã được loại bỏ khỏi thư viện tiêu chuẩn. Hỗ trợ hệ thống tệp trong os và pathlib đã thấy nhiều cải thiện, và một số mô-đun có hiệu suất tốt hơn.

Các thay đổi trong ngôn ngữ tập trung vào tính sử dụng, khi các chuỗi f đã loại bỏ nhiều hạn chế và các đề xuất 'Did you mean ...' tiếp tục cải thiện. Cú pháp tham số kiểu mới và câu lệnh kiểu cải thiện tính tiện lợi trong việc sử dụng kiểu chung và bí danh kiểu với các trình kiểm tra kiểu tĩnh.

II.2.1.2. PyQT6 Designer

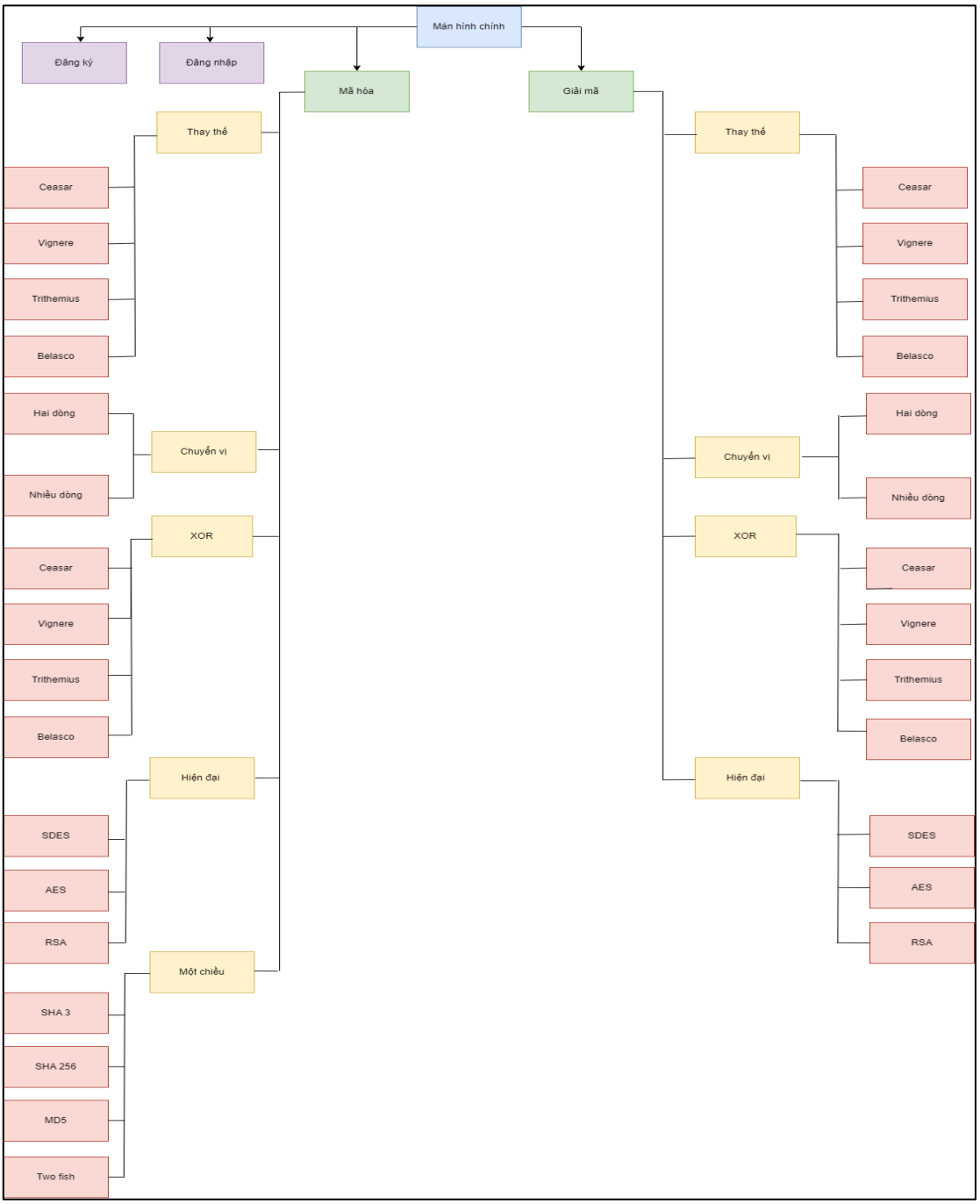
Qt Designer là công cụ Qt dùng để thiết kế và xây dựng giao diện người dùng đồ họa (GUI) bằng Qt Widgets. Bạn có thể tạo và tùy chỉnh cửa sổ hoặc hộp thoại của mình theo kiểu 'what-you-see-is-what-you-get' (WYSIWYG), và kiểm tra chúng bằng các kiểu và độ phân giải khác nhau.

Các Widgets và biểu mẫu được tạo ra bằng Qt Designer tích hợp một cách mượt mà với mã đã được lập trình, sử dụng cơ chế tín hiệu và khe cắm của Qt, giúp bạn dễ dàng gán hành vi cho các phần tử đồ họa. Tất cả các thuộc tính được đặt trong Qt Designer có thể được thay đổi động trong mã. Ngoài ra, các tính năng như thăng cấp widget và các plugin tùy chỉnh cho phép bạn sử dụng các thành phần riêng của bạn cùng với Qt Designer.

Chương III: Phân tích và thiết kế

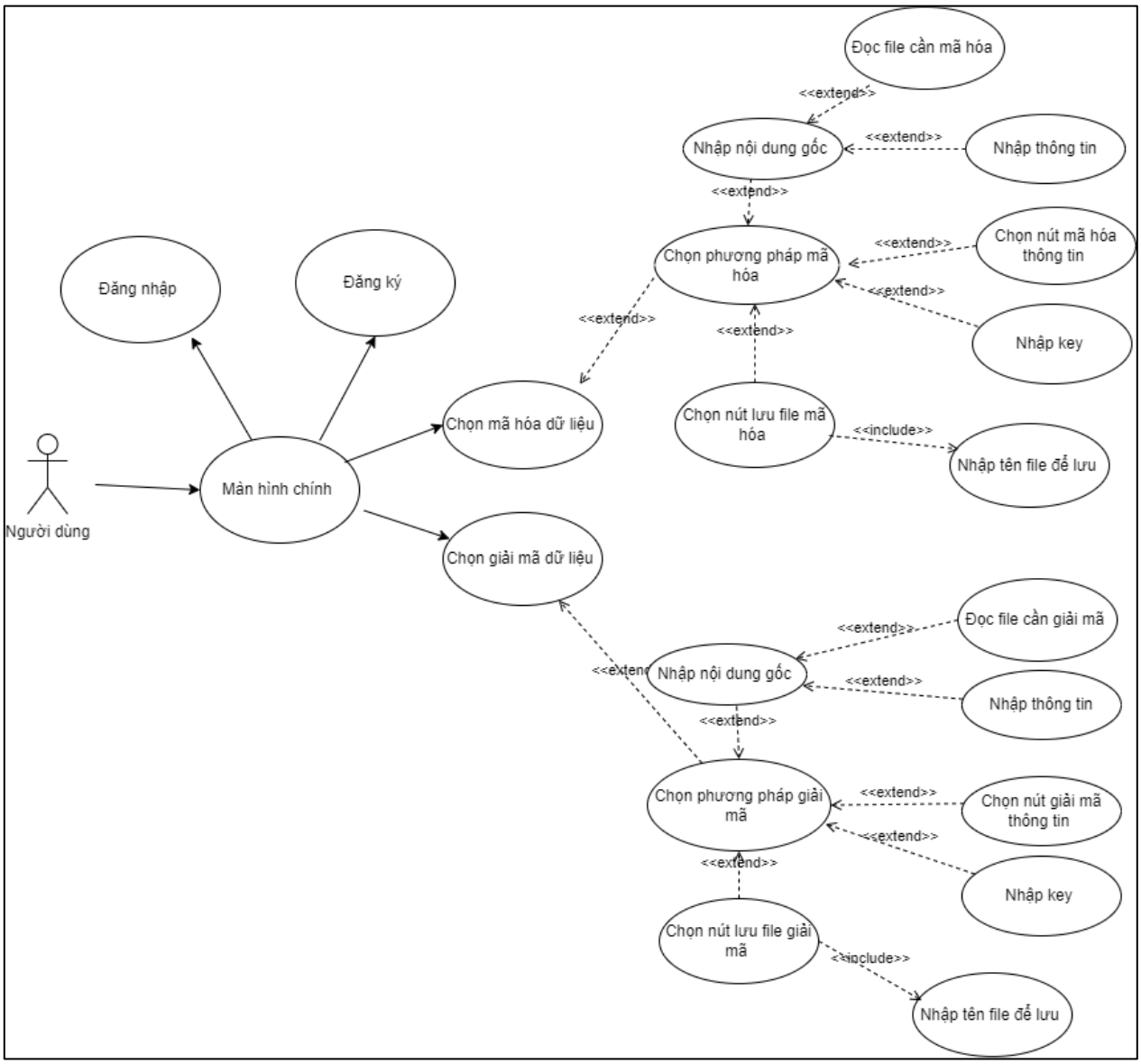
III.1. Phân tích

III.1.1. Sơ đồ chức năng



Hình 6. Sơ đồ chức năng

III.1.2. Usecase Diagram

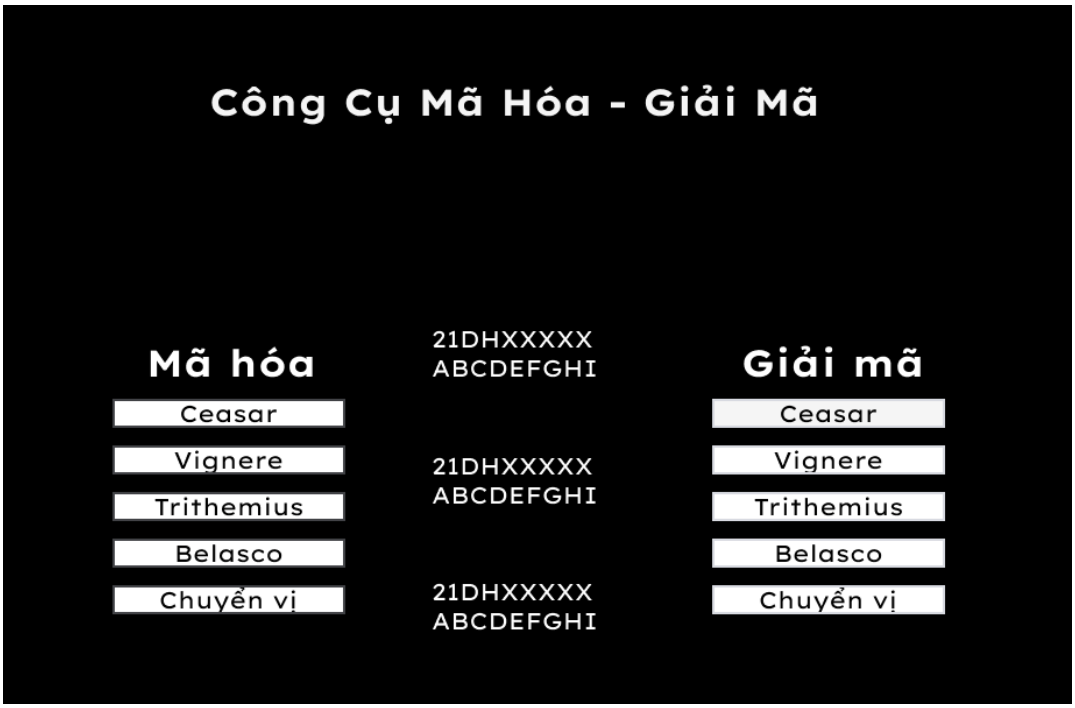


Hình 7. Usecase Diagram

III.2. Thiết kế giao diện

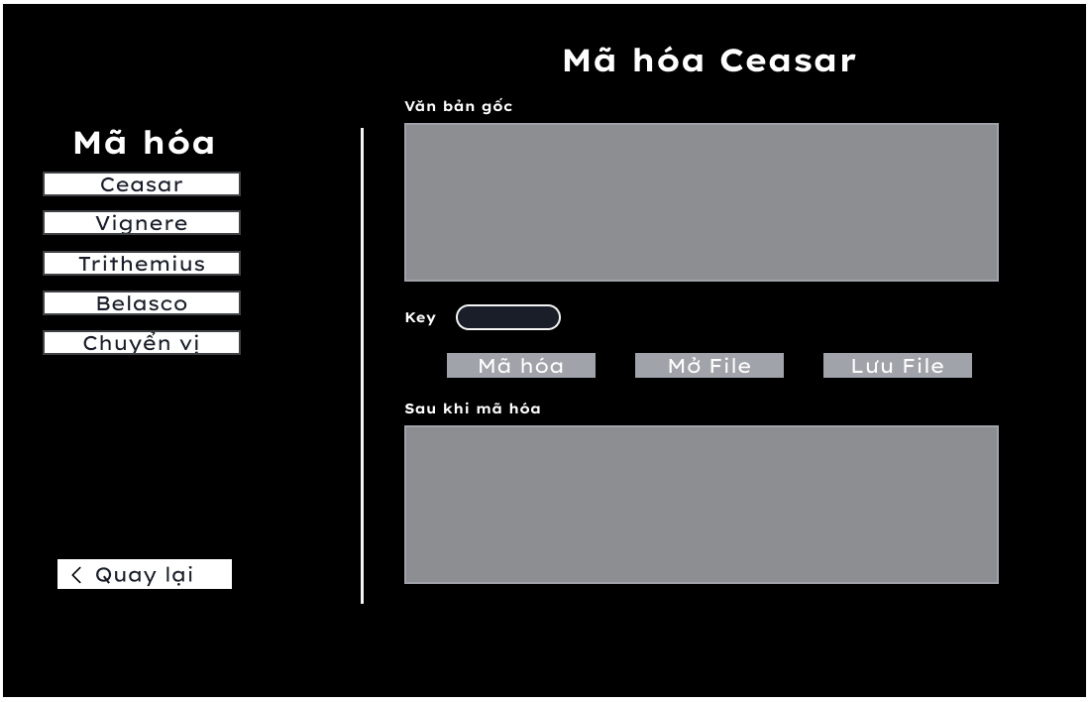
III.2.1. Thiết kế xử lý: (Mô hình 3 lớp)

III.2.1.1. Wireframe giao diện trang chủ



Hình 8. Wireframe giao diện trang chủ

III.2.1.2. Wireframe giao diện trang mã hóa có key

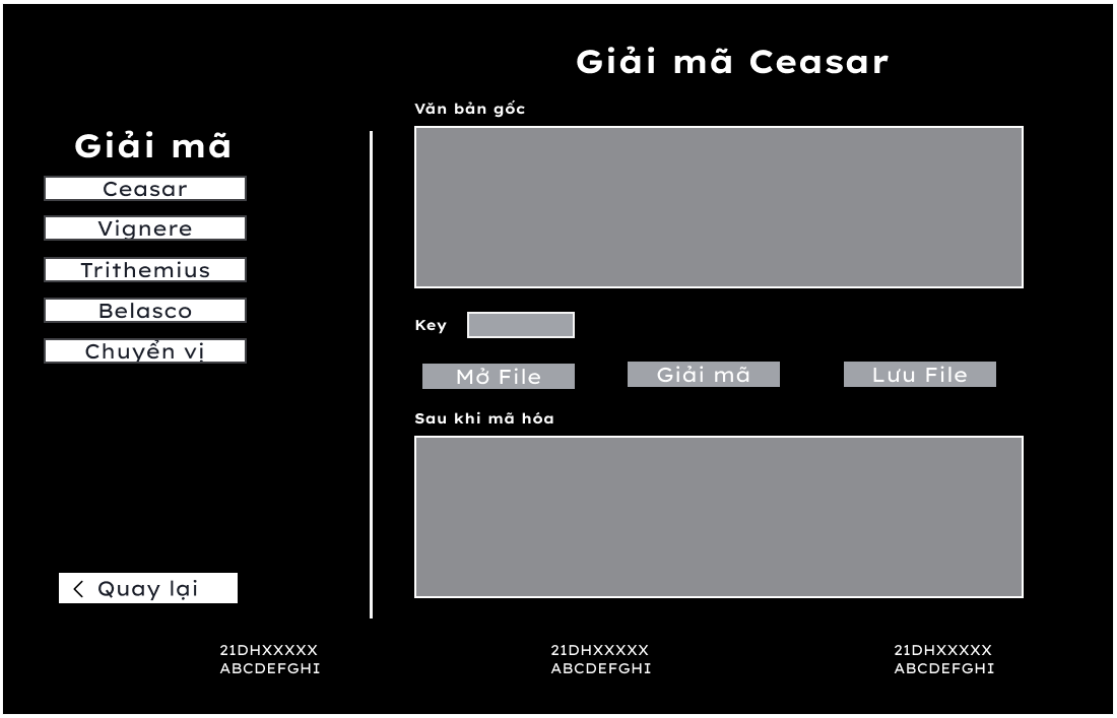


Hình 9. Wireframe giao diện trang mã háo có key

III.2.1.3. Wireframe giao diện trang mã hóa không key

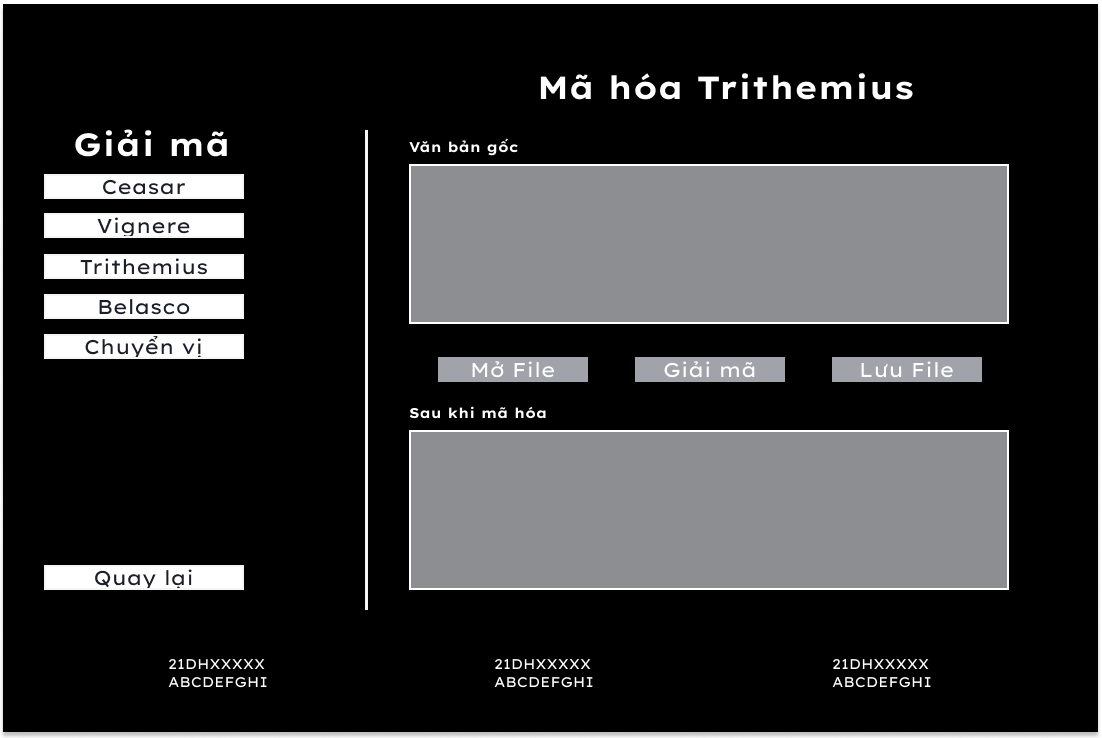
Hình 10. Wireframe giao diện trang mã hóa không key

III.2.1.4. Wireframe giao diện trang giải mã có key



Hình 11. Giao diện trang mã hóa có key

III.2.1.5. Wireframe giao diện trang giải mã không key



Hình 12. Wireframe giao diện trang mã hóa không key

Chương IV: Kết luận

IV.1. Kết quả đạt được

IV.1.1. Màn hình giao diện chính

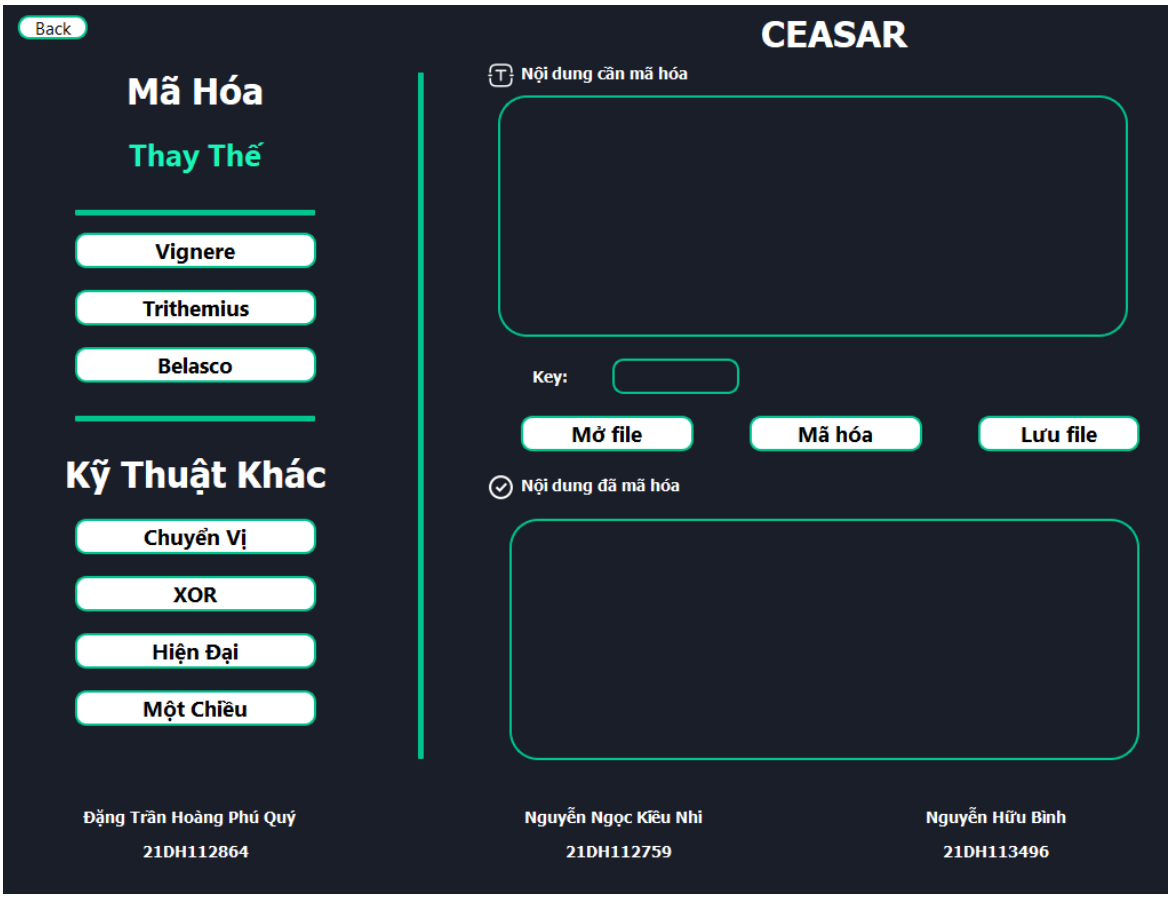
Hình 13. Màn hình giao diện chính

Hướng dẫn sử dụng:

1. Chọn vào các nút Thay Thế, Chuyển Vị, XOR, Hiện Đại của Mã hóa hoặc Giải mã hoặc Mã Hóa Một Chiều tùy theo nhu cầu sử dụng của người dùng.

IV.1.2. Màn hình xử lý mã hoá

➢ ***Màn hình giao diện mã hóa Ceasar có key***

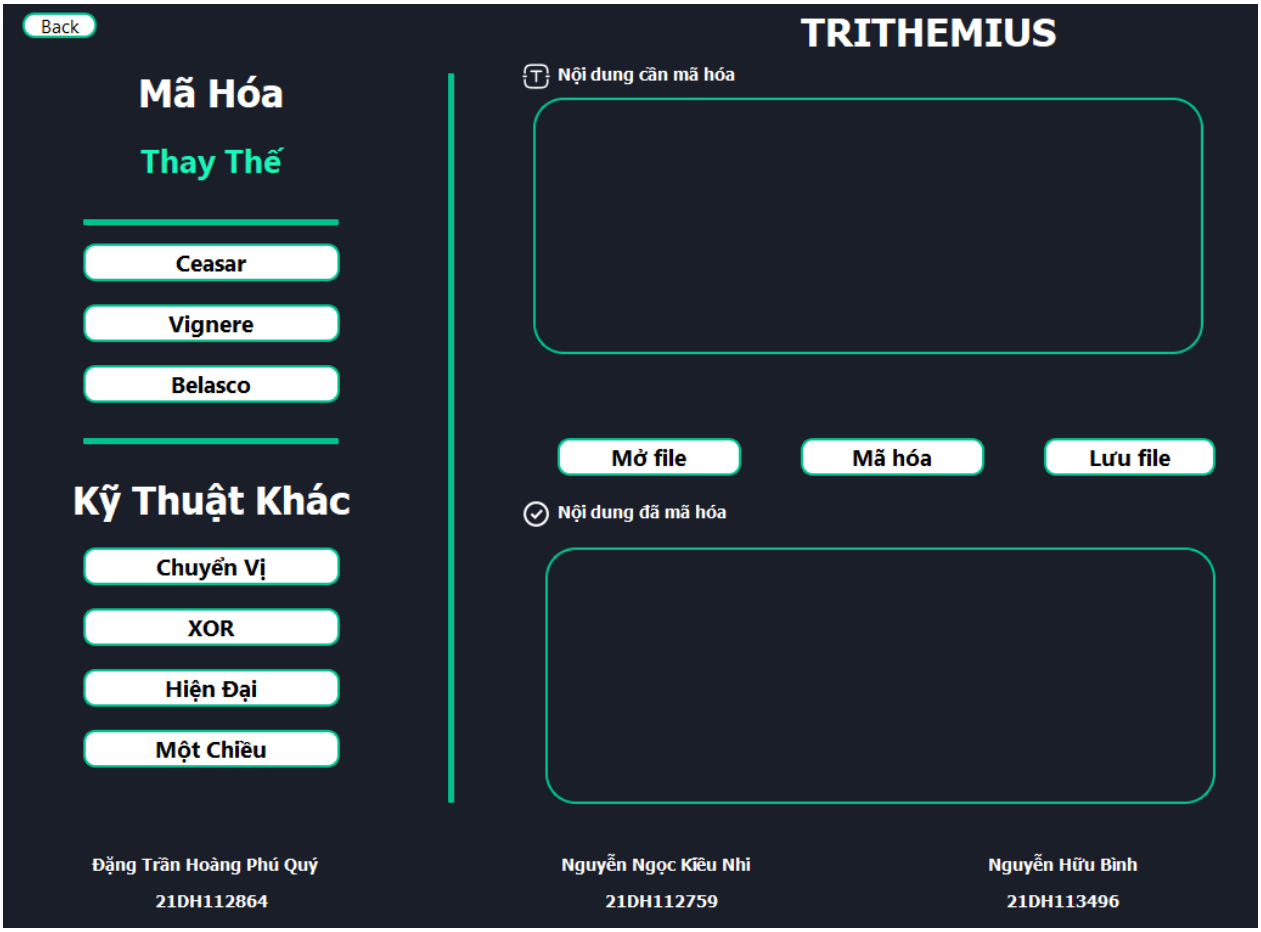


Hình 14. Màn hình giao diện mã hóa Ceasar (có key)

Hướng dẫn sử dụng:

1. Nhập dữ liệu vào ô nội dung cần mã hóa hoặc chọn mở file txt từ máy tính từ nút Mở file để dữ liệu nhập vào khuôn nội dung cần mã hóa.
2. Nhập key bằng số hoặc chữ phù hợp tùy phương pháp mã hóa vào ô Key.
3. Chọn nút Mã hóa để ứng dụng biến văn bản thành văn bản đã được mã hóa
4. Chọn nút Lưu File để lưu dữ liệu đã được mã hóa vào máy tính.

➢ ***Màn hình giao diện mã hóa Trithemius không key***



Hình 15. Màn hình giao diện mã hóa Trithemius (không key)

Hướng dẫn sử dụng:

1. Nhập dữ liệu vào ô nội dung cần mã hóa hoặc chọn mở file txt từ máy tính từ nút Mở file để dữ liệu nhập vào khuôn nội dung cần mã hóa.
2. Chọn nút Mã hóa để ứng dụng biến văn bản thành văn bản đã được mã hóa
3. Chọn nút Lưu File để lưu dữ liệu đã được mã hóa vào máy tính.

IV.1.3. Màn hình xử lý giải mã

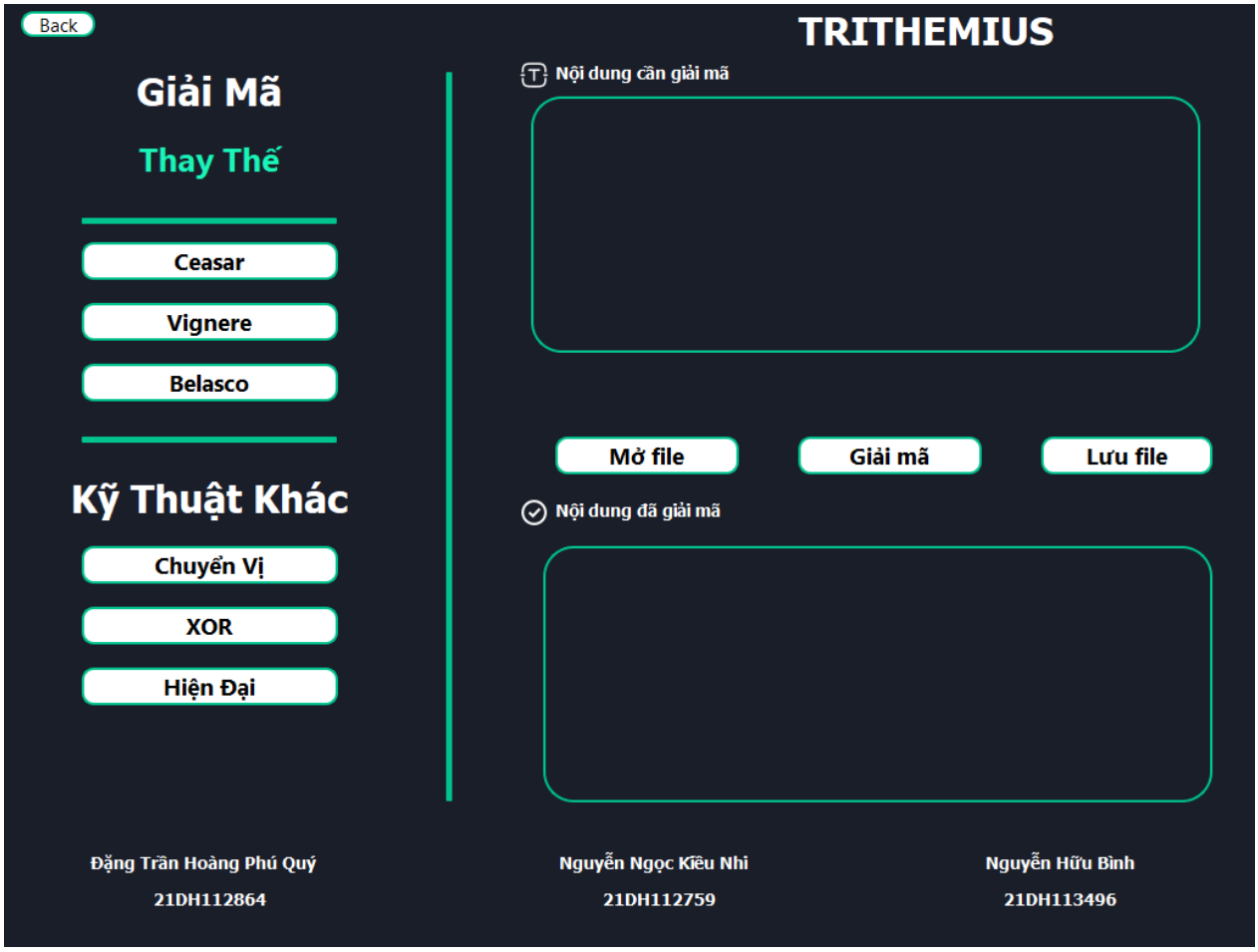
➢ *Màn hình giao diện giải mã ceasar*

Hình 16. Màn hình giao diện giải mã Ceasar

Hướng dẫn sử dụng:

1. Nhập dữ liệu vào ô nội dung cần mã hóa hoặc chọn mở file txt từ máy tính từ nút Mở file để dữ liệu nhập vào khuôn nội dung cần giải mã.
2. Chọn file Key từ máy tính đã lưu trước đó hoặc nhập key bằng tay vào ô Key.
3. Chọn nút Mã hóa để ứng dụng biến văn bản thành văn bản đã được giải mã.
4. Chọn nút Lưu File để lưu dữ liệu đã được giải mã vào máy tính.

➢ ***Màn hình giao diện giải mã Trithemius***



Hình 17. Màn hình giao diện giải mã Trithemius

Hướng dẫn sử dụng:

1. Nhập dữ liệu vào ô nội dung cần mã hóa hoặc chọn mở file txt từ máy tính từ nút Mở file để dữ liệu nhập vào khuôn nội dung cần giải mã.
2. Chọn nút Mã hóa để ứng dụng biến văn bản thành văn bản đã được giải mã.
3. Chọn nút Lưu File để lưu dữ liệu đã được giải mã vào máy tính.

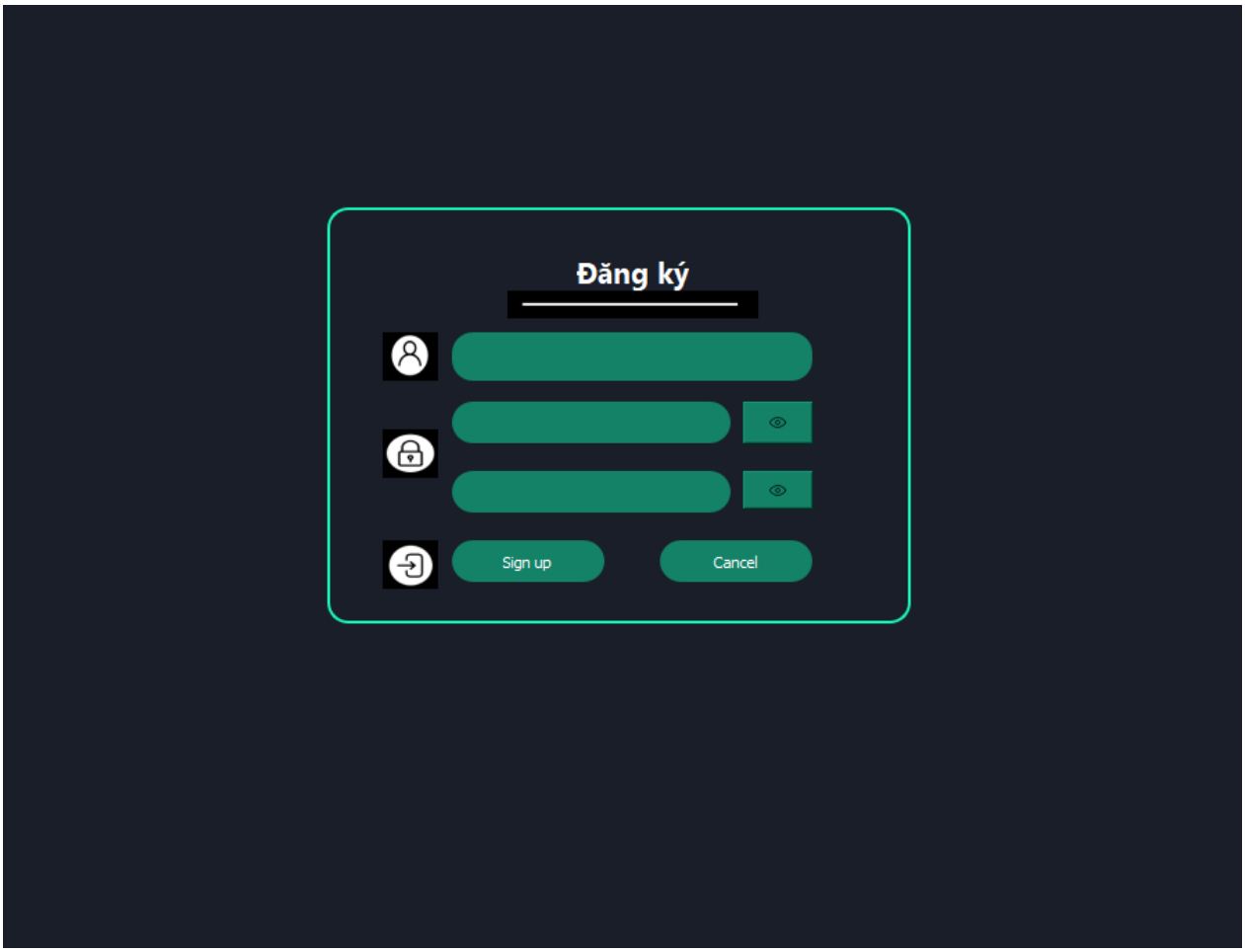
IV.1.4. Màn hình trang đăng nhập

Hình 18. Màn hình trang đăng nhập

Hướng dẫn sử dụng:

1. Nếu chưa có tài khoản ấn vào dòng chữ "Bạn chưa có tài khoản? " Để chuyển qua trang đăng ký.
2. Nếu đã có tài khoản, nhập tài khoản ở trên khung kế icon người dùng
3. Sau đó nhập mật khẩu ở khung kế icon ổ khóa.
4. Nếu muốn xem mật khẩu, ấn vào nút bên cạnh khuôn ổ khóa có hình con mắt để tắt chế độ ẩn mật khẩu.
5. Sau đó ấn vào nút Login để đăng nhập vào màn hình chính.

IV.1.5. Màn hình trang đăng ký



Hình 19. Màn hình trang đăng ký

Hướng dẫn sử dụng:

1. Nhập tài khoản mới ở trên khung kế icon người dùng.
2. Sau đó nhập mật khẩu mới ở khung ở trên kế icon ổ khóa.
3. Sau đó nhập mật khẩu lần 2 ở khung ở dưới kế bên icon ổ khóa.
4. Nếu muốn xem mật khẩu, ấn vào nút bên cạnh khuôn ổ khóa có hình con mắt để tắt chế độ ẩn mật khẩu.
5. Sau đó ấn vào nút Sign up để đăng ký và được chuyển về trang đăng nhập để có thể đăng nhập vào màn hình chính.

Tài Liệu Tham Khảo

Patrick. (2023, 1 1). *How to Decrypt MD5 Passwords in Python?* Retrieved from InfosecScout: https://infosecscout.com/decrypt-md5-python/

Ramakrishna, S. (2021, 9 15). *XOR in Python*. Retrieved from DEV: https://dev.to/itsmycode/xor-in-python-1e5l

Thành, P. Đ. (2020, 2 4). *HUFLIT Moodle*. Retrieved from HUFLIT: https://drive.google.com/drive/folders/1pEXapjk4f2AozyRp9TG3UMKBtDqb039j

BẢNG PHÂN CÔNG CÔNG VIỆC

STT	Nội dung thực hiện	Đặng Trần Hoàng Phú Quý 21DH112864	Nguyễn Ngọc Kiều Nhi 21DH112759	Nguyễn Hữu Bình 21DH113496
1	Có trách nhiệm, tự học tập, trung thực, sử dụng phần mềm hợp pháp	x	x	
2	Đọc tài liệu, nghiên cứu	x	x	
3	Kỹ năng làm việc nhóm	x	x	
4	Thiết kế	x	x	
5	Viết code	x	x	
6	Viết báo cáo	x	x	
7	Đọc hiểu và trình bày báo cáo	x	x	