Bộ Giáo Dục Và Đào Tạo

**Trường Đại Học Lâm Nghiệp**

****

**BÁO CÁO ĐỒ ÁN**

**TÊN ĐỀ TÀI**

**Mã hoá tập tin**

Ngành : Hệ thống thông tin

Giảng viên hướng dẫn: Mai Hà An

Nhóm sinh viên thực hiện:

Họ và tên: Nguyễn Thị Thu Hoài MSV: 2174801040819

Họ và tên: Nguyễn Thị Vọng MSV: 2174801040565

Họ và tên: Phan Thu Trang MSV: 2174801041090

**MỤC LỤC**

[CHƯƠNG 1: TỔNG QUAN VẤN ĐỀ NGHIÊN CỨU 4](#_Toc137497649)

[I. Vấn đề nghiên cứu: *mã hoá file* 4](#_Toc137497650)

[II. Một số ứng dụng mã hoá file phổ biến hiện nay 4](#_Toc137497651)

[1. Phần mềm NordLocker 4](#_Toc137497652)

[2. Phần mềm AxCrypt 5](#_Toc137497653)

[3. Phần mềm Folder Lock 6](#_Toc137497654)

[4. Phần mềm Advanced Encryption Package 6](#_Toc137497655)

[5. Phần mềm Bitlocker 6](#_Toc137497656)

[6. Phần mềm Challenger 8](#_Toc137497657)

[7. Phần mềm GiliSoft File Lock Pro 8](#_Toc137497658)

[8. Phần mềm Rohos Mini Drive 9](#_Toc137497659)

[9. Phần mềm DiskCryptor 10](#_Toc137497660)

[III. Những vấn đề khó khăn chưa được giải quyết, đề xuất khắc phục 10](#_Toc137497661)

[1. Phần mềm NordLocker 10](#_Toc137497662)

[2. Phần mềm AxCrupt 11](#_Toc137497663)

[3. Phần mềm Bitlocker 11](#_Toc137497664)

[CHƯƠNG 2: NỘI DUNG THỰC HIỆN 11](#_Toc137497665)

[I. Các phương án thực hiện 11](#_Toc137497666)

[1. Phương án 1 11](#_Toc137497667)

[2. Phương án 2 15](#_Toc137497668)

[3. Phương án 3 19](#_Toc137497669)

[II. Phân tích phương án 21](#_Toc137497670)

[1. Phương án 1 21](#_Toc137497671)

[2. Phương án 2 21](#_Toc137497672)

[3. Phương án 3 21](#_Toc137497673)

[III. Lựa chọn phương án phù hợp, lí do chọn 22](#_Toc137497674)

[CHƯƠNG 3: KẾT QUẢ THỰC HIỆN 22](#_Toc137497675)

[I. Giải quyết từng vấn đề của bài toán như thế nào? 22](#_Toc137497676)

[1. Tạo Nơi lưu trữ dữ liệu 22](#_Toc137497677)

[2. Quản lý thông tin tài khoản người dùng 22](#_Toc137497678)

[3. Quản lý kết nối đến CSDL sql server 22](#_Toc137497679)

[4. Truy vấn và đọc dữ liệu trong bảng 22](#_Toc137497680)

[5. Vào form đăng nhập 23](#_Toc137497681)

[6. Với lable\_đăng\_ký 23](#_Toc137497682)

[7. Quản lý việc đăng nhập của người dùng trong ứng dụng 23](#_Toc137497683)

[8. Vào form đăng ký 24](#_Toc137497684)

[9. Kiểm tra xem người dùng nhập có đúng quy định của tên tài khoản, hay định dạng email, email đã được đăng ký hay chưa, 2 mật khẩu nhập vào giống nhau hay không. 24](#_Toc137497685)

[10. Gửi mã xác thực về email người dùng 24](#_Toc137497686)

[11. kiểm tra xem mã code người dùng nhập có giống mã được gửi vào email? 25](#_Toc137497687)

[12. Kiểm tra thông tin tài khoản nhập vào đăng ký hay chưa, nếu chưa điền đúng thì hiển thị đăng ký thành công. 25](#_Toc137497688)

[13. Vào form home giao diện chính 25](#_Toc137497689)

[14. Chọn một tệp từ máy tính 26](#_Toc137497690)

[15. Tạo bảng chữ cái và bảng tra phục vụ cho thuật toán mã hoá 26](#_Toc137497691)

[16. Đảm bảo rằng chỉ một trong hai RadioButton được chọn tại một thời điểm. 26](#_Toc137497692)

[17. Trình tự hoạt động khi click thực hiện 27](#_Toc137497693)

[18. Kiểm tra nếu người dùng nhập không đúng tài khoản hoặc mật khẩu. Nếu mật khẩu sai đến lần thứ 6 thì sẽ gửi file gốc cho người dùng đồng thời xoá file và thông báo có người cố gắng mở tệp của bạn. Khi gửi xong tệp tin sẽ thoát khỏi form Home về form Đăng nhập. 28](#_Toc137497694)

[19. Cick đăng xuất 28](#_Toc137497695)

[20. Mã hoá/giải mã ngay bên ngoài ứng dụng 28](#_Toc137497696)

[21. Chạy thành file exe 28](#_Toc137497697)

[22. Kết quả 29](#_Toc137497698)

[23. Kiểm thử thế nào 29](#_Toc137497699)

[CHƯƠNG 4: KẾT LUẬN, KIẾN NGHỊ 29](#_Toc137497700)

[I. Bạn đã làm được gì? 29](#_Toc137497701)

[II. Còn tồn đọng gì? 30](#_Toc137497702)

[III. Phương hướng triển khai nốt, nâng cấp như thế nào? 30](#_Toc137497703)

[Tài liệu tham khảo 30](#_Toc137497704)

**CHƯƠNG 1: TỔNG QUAN VẤN ĐỀ NGHIÊN CỨU**

1. **Vấn đề nghiên cứu: *mã hoá file***
2. **Một số ứng dụng mã hoá file phổ biến hiện nay**
3. *Phần mềm NordLocker*
4. Định nghĩa

NordLocker là một phần mềm mã hóa tập tin được tích hợp với bộ lưu trữ đám mây được mã hóa end-to-end.

1. Đặc điểm và chức năng

Công cụ mã hoá có cung cấp lưu trữ đám mây được mã hoá, mã hoá là không giới hạn có 2 phiên bản miễn phí và mất phí. Đám mây lưu trữ 500 GB với 3 GB bộ nhớ miễn phí. Thuật toán mã hoá: mã hoá đầu cuối ASE-256 kết hợp với mật mã đường cong Elliptic <thuật toán bất đối xứng>, khoá riêng được mã hoá bằng XchaCha20-Poly1305.

Trước khi bắt đầu mã hoá bất kỳ tệp nào cần tạo một tủ khoá cho chúng. Chỉ cần nhấp vào biểu tượng “thêm” ở bên cạnh “tủ khoá của tôi” trong menu. Sau đó đặt tên cho tủ khoá của mình và được cung cấp tuỳ chọn lưu nó vào đám mây hoặc ổ đĩa cục bộ của mình.

Các tệp và thư mục có thể được tải lên tủ khoá bằng chức năng kéo thả.

Quản lý mật khẩu: ứng dụng yêu cầu tạo mật khẩu chính cho NordLocker. Khoá khôi phục sau đó được tạo tự động cho tài khoản. Sẽ cần khoá khôi phục để khôi phục các tệp của mình nếu quên mật khẩu chính. Có thể duy trì trạng thái đăng nhập vào NordLocker nhưng vẫn phải nhập lại mật khẩu chính để mở khoá tài khoản của mình.

Xác thực đa nhân tố: có thể tuỳ chọn để kích hoạt xác thực nhiều yếu tố, kích hoạt MFA thông qua ứng dụng web và có thể sử dụng ứng dụng xác thực như Google Authenticator, Duo hoặc Authy. NordLocker cũng cung cấp cho mười mã sử dụng một lần khi kích hoạt MFA.

Quyền riêng tư: NordLocker là dịch vụ không có kiến thức, không có quyền truy cập vào tệp cá nhân và ưu tiên quyền riêng tư.

Chia sẻ và cộng tác: chia sẻ bất kỳ loại tệp nào với bao nhiêu người mà bạn muốn.

Sao lưu tự động: tự động sao lưu tất cả các tệp được lưu trữ trong đám mây tuy nhiên tủ khoá cục bộ không thể sao lưu tự động nếu thiết bị bị hỏng hoặc mất, thì sẽ mất các tệp cục bộ. Nếu thiết bị bị đánh cắp hoặc bị hỏng tính năng sao lưu tự động sẽ bảo vệ tệp và quá trình khôi phục sẽ bắt đầu khi đăng nhập lần sau từ máy tính mới và ứng dụng sẽ tải xuống tất cả dữ liệu trên đám mây là đã mất.

1. *Phần mềm AxCrypt*
2. Định nghĩa

AxCrypt là chương trình đơn giản để mã hóa các tập tin và thư mục giúp ngăn chặn truy cập trái phép và bảo vệ tập tin.

1. Đặc điểm và chức năng

Phần mềm mã hoá file nguồn mở để nén, mã hoá, giải mã, lưu trữ, gửi và làm việc với các file riêng lẻ. AxCrypt sử dụng thuật toán mã hoá ASE 128-bit.

AxCrypt cung cấp tính năng 2 chìa khoá, ngoài mật khẩu để truy cập file người dùng có thể chọn 1 file bất kỳ để làm khoá mở dữ liệu. Đó là tính năng sử dụng “file khoá” theo đó người dùng có thể lựa chọn 1 file text (định dạng txt) để dùng làm khoá. Nếu muốn mở khoá những dữ liệu đã mã hoá thì ngoài việc nhập mật khẩu còn phải biết được vị trí chính xác của file khoá nằm ở đâu. Tuy nhiên nếu trong trường hợp file sử dụng làm khoá bị thay đổi nội dung hoặc thất lạc thì sẽ không thể tiếp tục mã hoá dữ liệu đã được bảo vệ.

Làm việc với kho lưu trữ đám mây: AxCrypt tự động phát hiện dịch vụ lưu trữ tệp đám mây nào được cài đặt trên máy tính của bạn và tạo thư mục AxCrypt ở đó. Chương trình cho phép xem và lưu các tệp tin trong các thư mục này.

Cách thức sử dụng phần mềm khá đơn giản:

* Để bảo vệ dữ liệu nào đó (file hoặc thư mục) kích chuột phải vào file dữ liệu chọn AxCrypt 🡪 Encrypt. Sau đó hộp thoại mới hiện ra điền mật khẩu.
* Nếu muốn giải mã hoàn toàn dữ liệu và trả lại trạng thái ban đầu, kích chuột phải và file được mã hoá, chọn AxCrypt 🡪 Decrypt. Từ hộp thoại hiện ra điền mật khẩu xác nhận và chọn “file khoá” (nếu có) rồi nhấn OK để giải mã.

Đặc biệt phần mềm có thêm tính năng tạo file mã hoá dữ liệu định dạng exe, tức là cho phép bạn gửi file đã mã hoá đến bạn bè của mình và họ có thể giải mã file mà không cần phải cài đặt thêm phần mềm AxCrypt. Để thực hiện kích chuột phải vào dữ liệu cần mã hoá chọn AxCrypt 🡪 Encryot copy to .EXE hộp thoại hiện lên xác nhận mật khẩu sau đó phần mềm sẽ tự động tạo ra 1 file có định dạng .exe. Chỉ cần gửi file .exe cho bạn bà kèm mật khẩu khởi tạo và file được sử dụng làm khoá.

Cung cấp thêm tính năng xoá file an toàn mà không thể khôi phục được, đảm bảo dữ liệu xoá một cách triệt để.

1. *Phần mềm Folder Lock*
2. Định nghĩa

Folder Lock là một trong những phần mềm bảo mật dữ liệu và thông tin hàng đầu trên thế giới.

1. Đặc điểm và chức năng

Phần mềm miễn phí bảo vệ tệp tin, thư mục, ổ đĩa bằng mật khẩu, mã hoá những tệp tin quan trọng, sao lưu chúng trong thời gian thực, xoá tệp tin và lịch sử. Phương pháp mã hoá là ASE 256 bit.

Bảo mật sao lưu: nếu PC bị trộm hay dữ liệu bị xoá, người dùng chỉ cần khôi phục lại dữ liệu từ tài khoản online.

Khi người dùng khoá thư mục, nó sẽ ẩn khỏi vị trí trước đó và chỉ có thể truy cập trên giao diện phần mềm.

Không cần mã hoá/giải mã file khi truy cập, đơn giản chỉ cần sao chép chúng lên Locker thế là xong. Chúng sẽ được mã hoá tức thì.

Chia nhỏ tệp tin: Việc chia nhỏ file để đảm báo chúng sẽ biến mất hoàn toàn khỏi ổ đĩa và ngay cả phần mềm khôi phục tệp tin thì cũng không thể lấy lại chúng.

1. *Phần mềm Advanced Encryption Package*
2. Định nghĩa

Phần mềm mã hoá với nhiều thuật toán mã hoá khác nhau.

1. Đặc điểm và chức năng

* Cửa sổ chính bị chi phối bởi 1 cây tệp/thư mục, với một loại các nút điều khiển ở bên phải và dưới nó. Có sáu nút ở trên cùng bên phải: mã hoá, giải mã, SFX(tự giải nén), ZIP, xoá, email. Để mã hoa tệp tin 🡪 Encrypt Now. Sau đó nhập mật khẩu, chọn thuật toán mã hoá có sẵn (17 thuật toán).
* Xoá an toàn: xoá không thể khôi phục.
* Bộ mã hoá Clipboard.

1. *Phần mềm Bitlocker*
2. Định nghĩa

Là một dạng mã hoá và bảo mật thông tin. Khi cài đặt và sử dụng trên các thiết bị windows sẽ giúp ngăn chặn những truy cập trái phép.

1. Đặc điểm và chức năng

Mã hoá ổ đĩa bảo mật tuyệt đối và miễn phí sử dụng thuật toán mã hoá ASE với độ dài khoá mặc định là 128 bit.

Dữ liệu trên một máy tính bị mất hoặc bị đánh cắp rất dễ bị truy cập trái phép, bằng cách chạy một công cụ tấn công phần mềm chống lại nó hoặc bằng cách chuyển đĩa cứng của máy tính sang một máy tính khác. BitLocker giúp giảm thiểu truy cập dữ liệu trái phép bằng cách tăng cường bảo vệ tệp và hệ thống. BitLocker cũng giúp hiển thị dữ liệu không thể truy cập được khi các máy tính được bảo vệ bởi BitLocker ngừng hoạt động hoặc tái chế.

Có hai công cụ bổ sung trong Công cụ quản trị máy chủ từ xa có thể được sử dụng để quản lý BitLocker.

* **Trình xem mật khẩu khôi phục BitLocker** . BitLocker Recovery Password Viewer cho phép định vị và xem các mật khẩu khôi phục BitLocker Drive Encryption đã được sao lưu vào Dịch vụ miền Active Directory (AD DS). Công cụ này có thể được sử dụng để giúp khôi phục dữ liệu được lưu trữ trên ổ đĩa đã được mã hóa bằng BitLocker. Công cụ Trình xem mật khẩu phục hồi BitLocker là một phần mở rộng cho phần đính vào Bảng điều khiển quản lý Microsoft (MMC) của Người dùng Active Directory và Máy tính. **Bằng cách sử dụng công cụ này, hộp thoại Thuộc tính** của đối tượng máy tính có thể được kiểm tra để xem mật khẩu khôi phục BitLocker tương ứng. Ngoài ra, vùng chứa miền có thể được tìm kiếm mật khẩu khôi phục BitLocker trên tất cả các miền trong nhóm Active Directory bằng cách nhấp chuột phải vào vùng chứa miền. Việc xem mật khẩu khôi phục chỉ có thể được xem bởi quản trị viên miền hoặc được quản trị viên miền ủy quyền.
* **Công cụ mã hóa ổ đĩa BitLocker**. Công cụ mã hóa ổ đĩa BitLocker bao gồm các công cụ dòng lệnh, manage-bde và repair-bde cũng như các lệnh ghép ngắn BitLocker cho Windows PowerShell. Cả hai lệnh ghép ngắn manage-bde và BitLocker đều có thể được sử dụng để thực hiện bất kỳ tác vụ nào có thể được thực hiện thông qua bảng điều khiển BitLocker và chúng phù hợp để sử dụng cho triển khai tự động và các kịch bản tập lệnh khác. Repair-bde được cung cấp cho các tình huống khôi phục thảm họa trong đó không thể mở khóa ổ đĩa được bảo vệ bằng BitLocker một cách bình thường hoặc bằng cách sử dụng bảng điều khiển khôi phục.

1. *Phần mềm Challenger*
2. Định nghĩa

Challenger là một phần mềm để mã hóa các tập tin, thư mục và ổ đĩa.

1. Đặc điểm và chức năng

Để cài đặt và thực hiện quyền người dùng đơn giản đủ. Do đó, chương trình cũng có thể được sử dụng trên ổ flash USB. Phần mềm được hình thành để bảo vệ quyền riêng tư dữ liệu cục bộ và cho các vòng kết nối kín. Một mật mã dòng đồng bộ, một sự phát triển từ Đức, cung cấp một mã hóa nhanh.

Chương trình sử dụng một thủ tục hai khóa. Một trong các phím đại diện cho một cụm từ bộ nhớ hoặc mật khẩu thông thường. Khóa thứ hai được tạo bởi một danh sách mở rộng (3 MB) với các số ngẫu nhiên thực. Nó cũng được tạo riêng lẻ và có thể được xử lý như khóa vật liệu (an toàn). Khóa thứ hai có thể được hình thành độc lập với nền tảng PC cho các yêu cầu bảo mật cao. Các cuộc tấn công với keylogger vẫn không hiệu quả vì để theo dõi các cụm từ hộ chiếu để giải mã dữ liệu của bạn không đủ. Dữ liệu gốc bị xóa nhất định (phương pháp an toàn nhất: thủ tục Đức, VSITR)

1. *Phần mềm GiliSoft File Lock Pro*
2. Định nghĩa

GiliSoft File Lock Pro là một phần mềm mạnh mẽ dùng để mã hóa một cách nhanh chóng, an toàn và ẩn các tập tin, thư mục, ổ đĩa.

1. Đặc điểm và chức năng

Có thể sử dụng công nghệ mã hóa 256-bit AES (Encryption Standard Adopted của Chính phủ Mỹ) để bảo vệ các tập tin của bạn trên HDD hoặc bất kỳ phương tiện di động nào như USB**.**

Tính năng và lợi ích của GiliSoft File Lock Pro

**• Ẩn dữ liệu:**

GiliSoft File Lock Pro có thể ẩn các tập tin, thư mục cá nhân và ổ đĩa của bạn, làm cho chúng trở nên “hoàn toàn vô hình” đối với người dùng và chương trình.

**• Khóa dữ liệu:**

Bảo vệ các tập tin/thư mục/ổ đĩa bị khóa không bị truy cập. Người dùng không thể mở, đọc, chỉnh sửa, di chuyển, xóa, sao chép, đổi tên các tập tin/thư mục được bảo vệ mà không cần mật khẩu. Các tập tin và thư mục con trong một thư mục bị khóa cũng được bảo vệ.

**• Mã hóa dữ liệu:**

Chương trình có thể mã hóa bất kỳ tập tin và thư mục nào.

**• Mã hóa di động:**

Gói và mã hóa một thư mục thành một file thực thi (.exe file) với thuật toán mã hóa AES. Bạn có thể mã hóa những dữ liệu quan trọng bằng phương pháp này, và sau đó gửi nó qua mạng hoặc các phương tiện khác để sử dụng trên máy tính mà không cần Gili File Lock Pro.

**• Xóa an toàn:**

GiliSoft File Lock Pro cho phép bạn gỡ bỏ hoàn toàn dữ liệu nhạy cảm từ ổ đĩa cứng của bạn bằng cách ghi đè lên nó nhiều lần với các mẫu lựa chọn cẩn thận. Không ai có thể phục hồi dữ liệu bị xóa từ ổ đĩa cứng của bạn nếu bạn xóa nó an toàn.

**• Mật khẩu bảo vệ:**

GiliSoft File Lock Pro là một phần phềm khóa mật khẩu, điều này để nói lên rằng không có cách nào khác để chạy nó hoặc unistall nó nếu bạn không có mật khẩu.

1. *Phần mềm Rohos Mini Drive*
2. Định nghĩa

[Rohos Mini Drive](https://download.com.vn/rohos-mini-drive-8225)**là một tiện ích an ninh dữ liệu giúp người sử dụng dễ dàng tạo ra các phân vùng ẩn và được mã hóa trên ổ cứng, ổ đĩa flash USB.**

1. Đặc điểm và chức năng

Rohos Mini Drive cho phép người dùng bảo vệ an toàn cho các dữ liệu quan trọng được lưu trên ổ đĩa cứng hoặc trên các thiết bị lưu trữ ngoài như: USB, ổ cứng di động, đĩa mềm….. Phần mềm giúp người dùng phân vùng và tạo mật khẩu cho các thư mục trong vùng được lựa chọn. Chương trình có thể tạo các mật khẩu với thuật toán mã hóa ASE 256 bit. Người dùng cũng có thể thay đổi mật khẩu cho các thư mục khi cần thiết. Ngoài ra, Rohos Mini Drive còn cho phép người dùng thiết lập để cho phép ẩn tất cả hoặc một vài nội dung của tập tin.

Các tập tin trong thư mục được mã hóa sẽ hoàn toàn vô hình đối với những người ngoài. Chỉ khi nhập đúng mật khẩu thì các tập tin mới được hiện lên.

Đặc biệt, Rohos Mini Drive còn có chức năng tạo bàn phím ảo đền nhập mật khẩu. Như vậy người sử dụng có thể tránh được trường hợp mật khẩu bị ăn cắp bởi các phần mềm gián điệp có chức năng đọc ký tự bàn phím.

Các tính năng chính của Rohos Mini Drive:

* Tạo mật khẩu với thuật toán mã hóa ASE 256 bit
* Đổi mật khẩu
* thiết lập để cho phép ẩn tất cả hoặc một vài nội dung của tập tin
* Ẩn tất cả các tập tin
* Nhập mật khẩu bằng bàn phím ảo
* Phân vùng và tạo mật khẩu cho các thư mục trên vùng được chọn

*9. Phần mềm DiskCryptor*

a) Định nghĩa

DiskCryptor là một phần mềm mã hóa toàn ổ đĩa miễn phí và nguồn mở dành cho Windows.

b) Đặc điểm và chức năng

Nó cho phép mã hóa toàn bộ ổ cứng hoặc từng phân vùng của máy tính kể cả ổ cài đặt hệ điều hành.

DiskCryptor được thiết kế để thay thế những phần mềm thương mại như DriveCrypt Plus Pack and PGP Whole Disk Encryption, và sử dụng cả AES-256, Twofish, Serpent hoặc kết hợp các thuật toán xếp tầng (cascaded) trong XTS mode để thực hiện mã hóa.

1. **Những vấn đề khó khăn chưa được giải quyết, đề xuất khắc phục**
2. *Phần mềm NordLocker*

Tạo tài khoản NordLocker trên web dễ nhầm lẫn với tạo tài khoản Nord. Nên tải NordLocker. Nhưng khi tạo tài khoản Nord nó sẽ giúp cho việc khi bạn quên mật khẩu chính Nord sẽ lưu trữ mật khẩu.

Không thể mã hoá tệp ngay lập tức mà phải tạo một tủ khoá. Đề xuất: nên cho mã hoá trực tiếp ở file với điều kiện nhập mật khẩu đúng.

Có thể lấy lại mật khẩu chính khi quên với điện kiện phải nhớ khoá khôi phục được cấp khi tạo tài khoản lần đầu tiên (trường hợp không sử dụng tài khoản Nord). Đề xuất: khi người dùng tạo mật khẩu chính nên đưa ra gợi ý “hãy viết câu hỏi gợi ý về mật khẩu của bạn, gợi ý sẽ được hiện khi bạn quên”.

1. *Phần mềm AxCrupt*

Muốn thoát hoàn toàn chương trình phải vào file chọn exit. Nếu chỉ ấn dấu x thì chương trình sẽ chỉ ẩn dưới thanh Taskbar và người dùng sẽ không thể gỡ khoá bảo mật dữ liệu đươc.

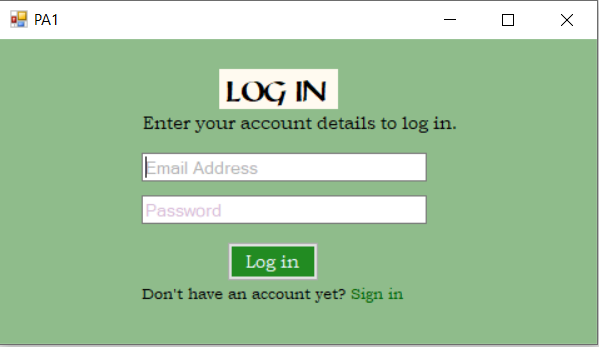
1. *Phần mềm Bitlocker*

Do đây là một chương trình mã hoá dễ sử dụng thuộc sở hữu độc quyền của Microsoft trong hệ điều hành window nên các thao tác thiết lập trước khi mã hoá có vẻ hơi dài dòng khiến cho người dùng khó chịu. Vì vậy nên giảm thiểu số bước để được mã hoá file.

**CHƯƠNG 2: NỘI DUNG THỰC HIỆN**

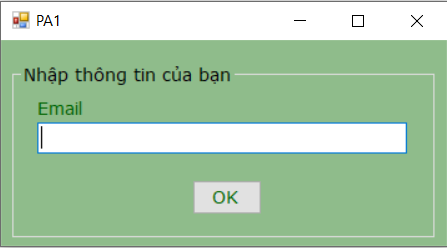
1. **Các phương án thực hiện**
2. *Phương án 1*

a, Khởi động phần mềm sử dụng. Nếu có tài khoản thì đăng nhập



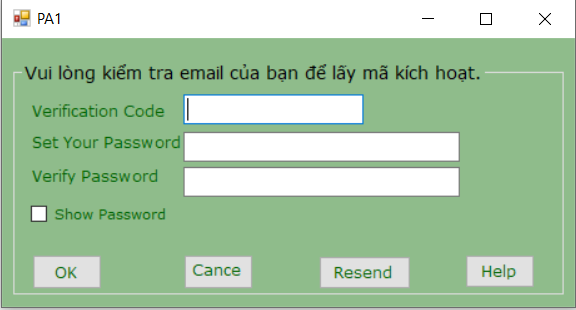
Hình 1.1

Nếu không có thì người dùng cần nhập địa chỉ email để kích hoạt tài khoản



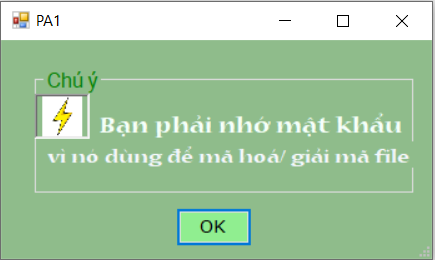
Hình 1.2

b, Phần mềm sẽ gửi tới địa chỉ địa chỉ email mã kích hoạt mà người dùng đăng ký. Bạn mở email của bạn rồi lấy mã nhập vào phần mềm.



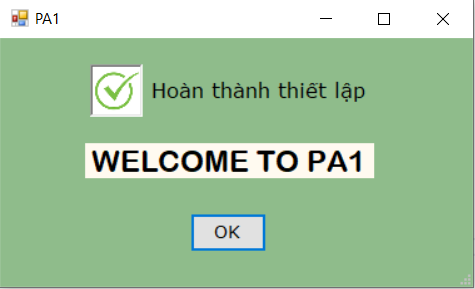
Hình 1.3

c, Phần mềm sẽ gửi tới một lời nhắc nhở



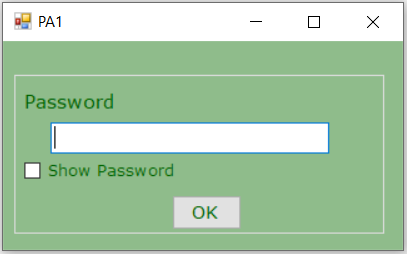
Hình 1.4

d, Khi thấy giao diện hiển thị thôn báo “Welcome PA1” nghĩa là thiết lập mật khẩu thành công.



Hình 1.5

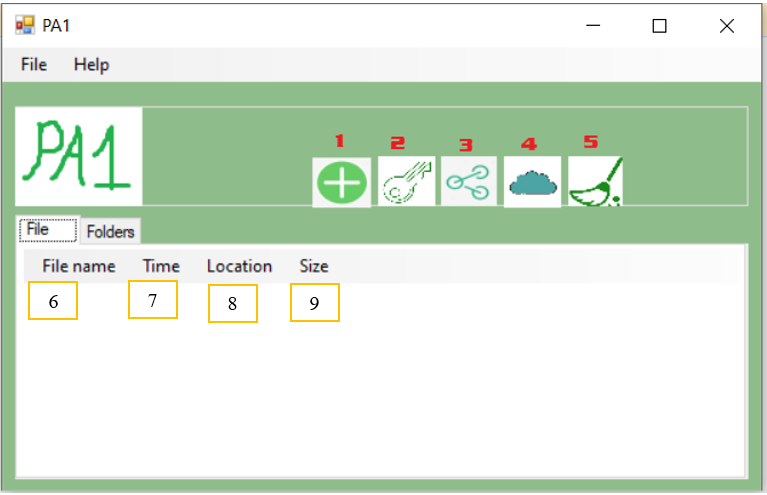
e, Nhập lại mật khẩu để tiếp tục với PA1



Hình 1.6

f, Giao diện chính

Giải thích các số được kí hiệu trong hình 1.7:



Hình 1.7

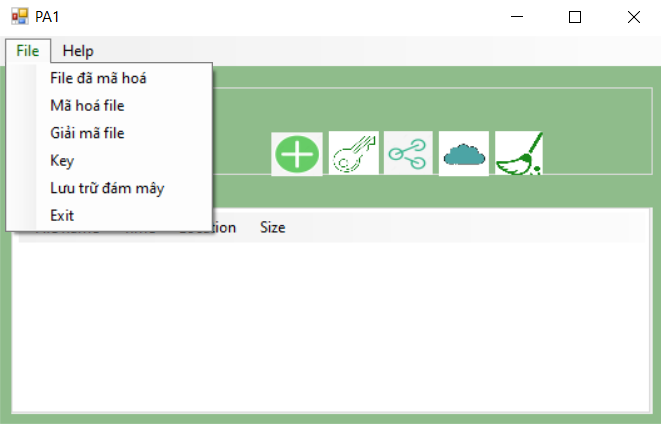
Mã hoá file với thuật toán Ceasar

1. Tạo mật khẩu mới nhưng với file đã mã hoá bằng mật khẩu cũ thì không thể mở bằng mật khẩu mới.
2. Chia sẻ với bạn bè: theo 2 phương thức

* Những người cùng sử dụng ứng dụng PA1
* Những người không sử dụng ứng dụng: file sẽ được mã hoá thành file .exe người dùng có thể chia sẻ file .exe và cung cấp mật khẩu của file cho họ.(bạn phải đổi mật khẩu trước khi mã hoá để không bị lộ mật khẩu nếu gửi mật khẩu cho nười kia)

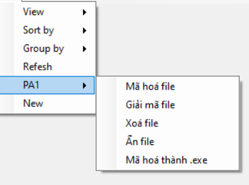
1. Lưu trữ đám mây: cung cấp tối đa 3GB để người dùng có thể lưu trữ dữ liệu trên đó. Khi mất máy tính người dùng có thể tải lại ứng dụng đăng nhập tài khoản và tải dữ liệu từ đám mây xuống.
2. Dọn sạch các file mà bạn chọn. Xoá an toàn khiến người khác không thể dùng phần mềm khác để khôi phục file.
3. File name: tên của file người dùng đưa vào mã hoá.
4. Time: thời điểm (ngày, giờ) mã hoá.
5. Location: đường dẫn tệp.
6. Size: kích thước tệp.

g, Trong thẻ file có menu hiển thị như sau:



Hình 1.8

h, Để mã hoá/giải mã trực tiếp ngay vị trí tệp. Chọn file 🡪 Chuột phải 🡪 PA1.

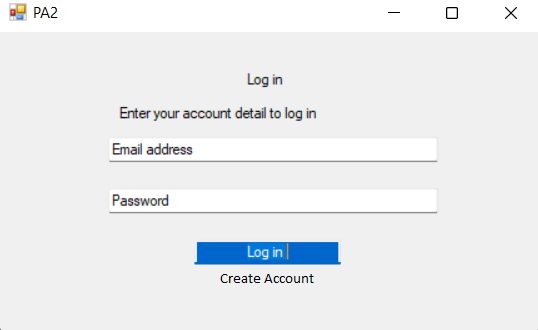


Hình 1.9

Rồi chọn công việc bạn muốn làm với file.

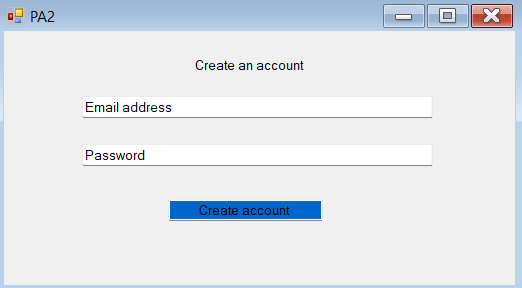
1. *Phương án 2*

a, Khi mở giao diện mới tải. Nếu có tài khoản thì đăng nhập ấn “Log in”. Nếu không có tài khoản để tạo tài khoản ấn Create Account.



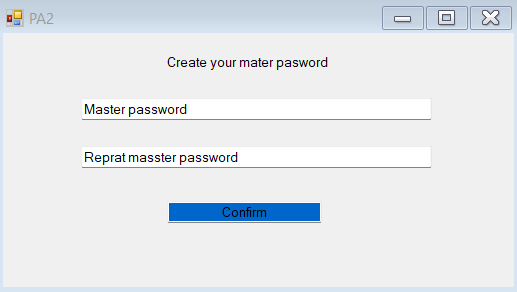
Hình 2.1

Giao diện thiết lập tài khoản.



Hình 2.2

Sau khi nhập email, người dùng sẽ được nhận 1 mã để xác nhận.Sau khi xác nhận, người dùng tạo mật khẩu để đăng nhập khi dùng app. Mật khẩu nhập vào được mã hoá bằng thuật toán MD5.

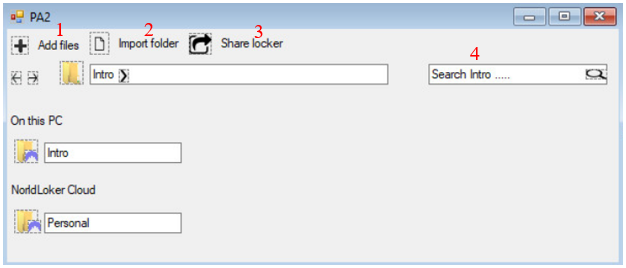


Hình 2.3

b, Giao diện chính.

Mã hoá bằng thuật toán RSA 128 bit.

Giải thích các số được kí hiệu trong hình 2.4:

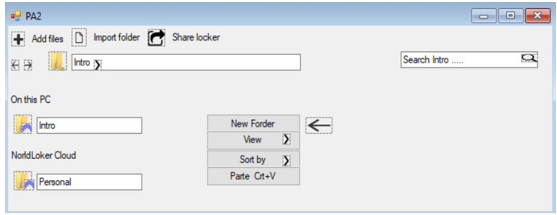


Hình 2.4

1. Tạo file cần mã hoá/giải mã.
2. Tạo folder mã hoá/giải mã.
3. Chia sẻ file với những người cùng sử dụng ứng dụng.
4. Tìm kiếm các folder/file đã mã hoá.

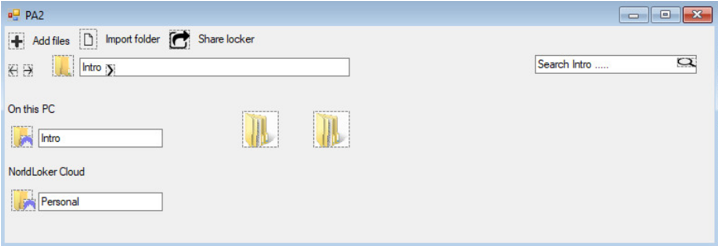
c, Tạo Folder mới trong ứng dụng

Click chuột phải →sau đó chọn New Forder. Sau đó chọn 1 file bất kỳ trong thư mục kéo thả vào Forder. Chọn thư mục có sẵn để bảo mật



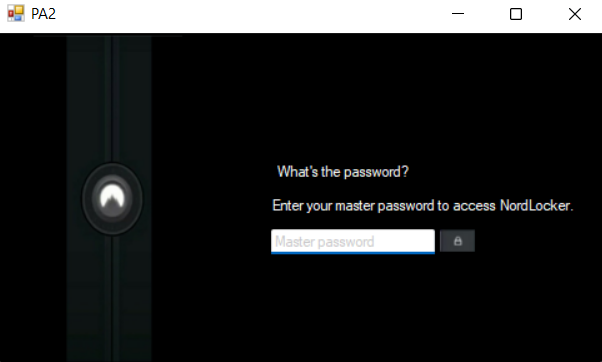
Hình 2.5

Click chuột vào □Import Forder sau hiện ra thư mục →kéo thả thư mục cần chọn vào ứng dụng



Hình 2.6

d, Khi muốn xem filer dữ liệu thì người dùng cần đăng nhập mật khẩu đã tạo ở ứng dụng để mở.



Hình 2.7

e, Quản lý mật khẩu.

Khi người dùng tạo thông tin đăng nhập, nguời dùng được yêu cầu tạo mật khẩu chính cho ứng dụng. Khóa khôi phục sau đó được tạo tự động cho tài khoản. Người dùng sẽ cần khóa khôi phục để khôi phục các tệp của mình nếu tôi quên mật khẩu chính của mình.

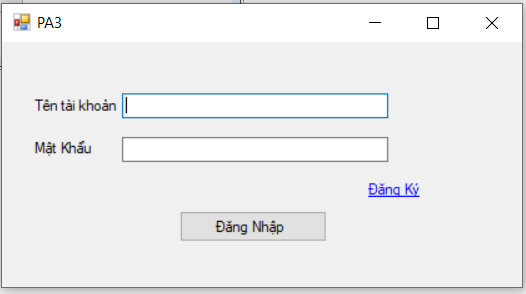


Hình 2.8

Mặc dù có thể duy trì trạng thái đăng nhập vào NordLocker nhưng người dùng vẫn phải nhập lại mật khẩu chính để mở khóa tài khoản của mình.

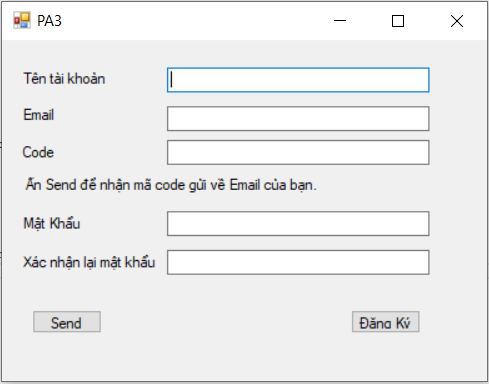
1. *Phương án 3*

a, Khi mở app ứng dụng bắt nhập tài khoản và mật khẩu đã đăng ký. Nếu chưa có tài khoản thì ấn đăng ký.



Hình 2.9

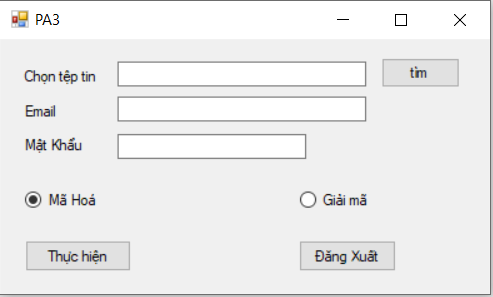
b, Đây là giao diện của người dùng khi ấn đăng ký. Nhập tên tài khoản bao gồm cả chữ và số. Tiếp đó nhập email xong ấn send sẽ có mã gửi về Email. Cuối cùng là nhập mật khẩu và ấn đăng ký.



Hình 2.10

c, Đây là giao diện chính. Người dùng ấn tìm để chọn tệp tin muốn mã hoá/giải mã. Sau đó tiếp tục nhập Email và mật khẩu mà ban đầu người dùng đã đăng ký. Nếu nhập sai mật khẩu 10 lần thì file sẽ bị xoá và file gốc sẽ được gửi và email của người dùng với nội dung có người xâm nhập vào file của bạn. Những file đã mã hoá xong thì sẽ có định dạng không được sao chép. Khi nhập xong các thông tin cần thiết chọn mã hoá/giải mã và ấn thực hiện.

Mã hoá bằng thuật toán Vigenère cipher.



Hình 2.11

Thuật toán mã hoá/giải mã ở đây dùng là thuật toán Vigenère cipher. Thuật toán này được sử dụng để mã hóa và giải mã các thông điệp bằng cách sử dụng một chuỗi khóa. Thuật toán này được xây dựng bằng cách sử dụng nhiều phép thay thế Caesar khác nhau.

d, Mã hoá ngay tệp tin

1. **Phân tích phương án**
2. *Phương án 1*

* Ưu điểm:
* Thao tác dễ dàng đơn giản.
* Có cung cấp bộ nhớ đám mây, và cho phép đồng bộ dữ liệu khi mất thiết bị có thể tải dữ liệu xuống.
* Xoá file an toàn.
* Cho phép thực hiện mã hoá/giải mã trực tiếp.
* Nhược điểm:
* Khi quên mật khẩu cũ thì không thể lấy lại.
* Chỉ có thể lưu trữ tối đa 3GB.
* Mật khẩu khi chia sẻ bằng file .exe có thể bị lộ.

1. *Phương án 2*

* Ưu điểm:
* Thao tác dễ dàng chỉ cần kéo thả file vào trong ứng dụng.
* Khi quên mật khẩu chính có thể khôi phục tệp nhờ khoá khôi phục được cung cấp khi người dùng tạo tài khoản.
* Nhược điểm:
* Không có xác thực đa nhân tố nếu có thì tài khoản sẽ được bảo mật tốt hơn.
* Không có xoá tệp an toàn vẫn có thể bị khôi phục.
* Mật khẩu nhập nên nhập bằng bàn phím ảo tính năng bảo mật mật khẩu sẽ gia tăng.

1. *Phương án 3*

* Ưu điểm:
* Thao tác đơn giản.
* Cho phép thực hiện mã hoá /giải mã trực tiếp.
* Nhược điểm:
* Không cung cấp bộ nhớ đám mây.
* Trong giao diện chính không xem được các file đã mã hoá.
* Thuật toán mã hoá đơn giản Vigenère cipher.
* Chưa mã hoá được thông tin khách hàng nhập vào.

1. **Lựa chọn phương án phù hợp, lí do chọn**

* Phương án 3 là phương án hợp lí phù hợp với tình hình, lực học của nhóm.

**CHƯƠNG 3: KẾT QUẢ THỰC HIỆN**

1. **Giải quyết từng vấn đề của bài toán như thế nào?**
2. *Tạo Nơi lưu trữ dữ liệu*

Chuột phải 🡪 new item 🡪 Service-based Database 🡪 Add.

Để thao tác chọn View 🡪 Server Explorer 🡪 kích đúp vào database vừa tạo 🡪 chọn table 🡪 create new table 🡪 tạo 3 cột TenTaiKhoan varchar(50), MatKhau varchar(50) null, Email varchar(50), null 🡪 update 🡪 update database.

1. *Quản lý thông tin tài khoản người dùng*

Gồm hai thuộc tính riêng tư là tenTaiKhoan và matKhau. Chúng được sử dụng để lưu trữ thông tin về tên tài khoản và mật khẩu của một đối tượng TaiKhoan. Do chúng là thuộc tính riêng tư, chúng chỉ có thể được truy cập và thay đổi giá trị bên trong lớp TaiKhoan. Để truy cập và thay đổi giá trị của chúng từ bên ngoài lớp, lớp này cung cấp hai thuộc tính công khai là TenTaiKhoan và MatKhau tương ứng. Chức năng của hai thuộc tính riêng tư này là để bảo vệ thông tin cá nhân của người dùng và chỉ cho phép truy cập thông qua các phương thức được cung cấp bởi lớp.

*3. Quản lý kết nối đến CSDL sql server*

Thêm môi trường using System.Data.SqlClient. Lớp gồm một thuộc tính tĩnh riêng tư là stringConnection chứa thông tin kết nối đến cơ sở dữ liệu. Lớp này cũng có một phương thức tĩnh công khai là GetSqlConnection để trả về một đối tượng SqlConnection mới được khởi tạo với thông tin kết nối được lưu trong thuộc tính stringConnection.

1. *Truy vấn và đọc dữ liệu trong bảng*

Thêm môi trường using System.Data.SqlClient. Lớp này có hai thuộc tính là sqlCommand và dataReader để truy vấn và đọc dữ liệu từ cơ sở dữ liệu. Lớp này cũng có hai phương thức công khai là TaiKhoans và Command. Phương thức TaiKhoans nhận vào một chuỗi truy vấn và trả về một danh sách các đối tượng TaiKhoan được lấy từ cơ sở dữ liệu. Phương thức Command nhận vào một chuỗi truy vấn và thực thi câu truy vấn đó trên cơ sở dữ liệu.

1. *Vào form đăng nhập*

Trong đây gồm tên label,textbox tên tài khoản và mật khẩu, có linklable\_đăng\_ký và button\_đăng\_nhập



Hình 3.1

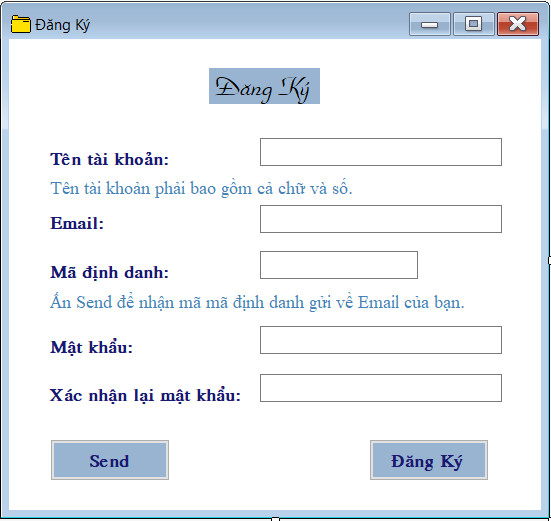
1. *Với lable\_đăng\_ký*

Hiển thị một hộp thoại đăng ký bằng cách gọi phương thức ShowDialog của đối tượng đó.

1. *Quản lý việc đăng nhập của người dùng trong ứng dụng*

Dùng class Modify để lấy thông tin về tên tài khoản và mật khẩu từ các textBox tương ứng, sau đó kiểm tra xem tên tài khoản và mật khẩu có được nhập hay không. Nếu có bất kỳ thông tin nào không được nhập, đoạn code sẽ hiển thị một thông báo lỗi. Nếu cả hai thông tin đều được nhập, đoạn code sẽ kiểm tra xem tên tài khoản và mật khẩu có chính xác hay không bằng cách truy vấn cơ sở dữ liệu. Nếu tên tài khoản và mật khẩu chính xác, đoạn code sẽ hiển thị một thông báo thành công và chuyển sang màn hình Home. Nếu tên tài khoản hoặc mật khẩu không chính xác, đoạn code sẽ hiển thị một thông báo lỗi.

1. *Vào form đăng ký*



Hình 3.2

1. *Kiểm tra xem người dùng nhập có đúng quy định của tên tài khoản, hay định dạng email, email đã được đăng ký hay chưa, 2 mật khẩu nhập vào giống nhau hay không.*

Kiểm tra tính hợp lệ của tên tài khoản và địa chỉ email của người dùng trong một ứng dụng dùng hai phương thức công khai là CheckAccount và CheckEmail. Phương thức CheckAccount nhận vào một chuỗi ac và kiểm tra xem chuỗi đó có phải là một tên tài khoản hợp lệ hay không. Một tên tài khoản hợp lệ là một chuỗi chỉ chứa các ký tự chữ cái và số, có độ dài từ 6 đến 24 ký tự. Phương thức CheckEmail nhận vào một chuỗi em và kiểm tra xem chuỗi đó có phải là một địa chỉ email hợp lệ hay không. Một địa chỉ email hợp lệ là một chuỗi có định dạng theo quy tắc của email.

1. *Gửi mã xác thực về email người dùng*

Người dùng nhấn vào nút btnSend để gửi email thì lấy thông tin về địa chỉ email người nhận từ textBox4\_Email, sau đó tạo ra một đối tượng MailMessage mới và thiết lập các thuộc tính cần thiết cho nó, bao gồm địa chỉ email người nhận, người gửi, tiêu đề và nội dung email. Tiếp đó tạo ra một đối tượng SmtpClient mới và thiết lập các thuộc tính cần thiết cho nó, bao gồm máy chủ SMTP, cổng, thông tin xác thực và bật SSL. Sau đó, đoạn code sẽ gửi email bằng cách gọi phương thức Send của đối tượng SmtpClient. Nếu email được gửi thành công, đoạn code sẽ hiển thị một thông báo thành công. Nếu có lỗi xảy ra trong quá trình gửi email, đoạn code sẽ hiển thị một thông báo lỗi.

1. *kiểm tra xem mã code người dùng nhập có giống mã được gửi vào email?*

Hiện tại nhóm chưa làm được. Đã code nhưng kết quả vẫn không được như đoạn code dưới đây.

if(codeRandom.Text != "" && codeRandom.Text != Numrd\_str)

{

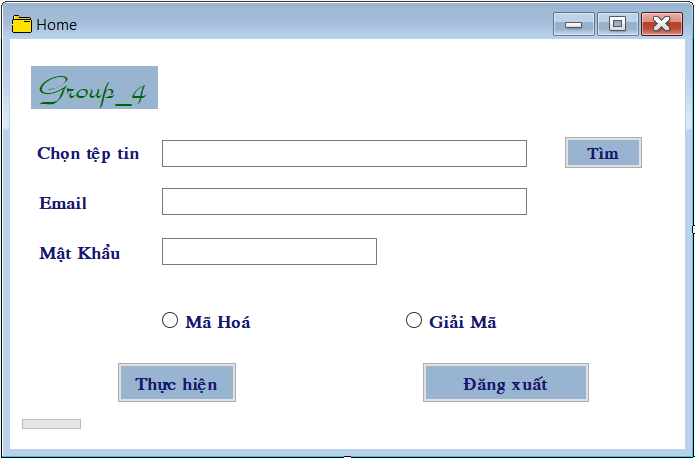
MessageBox.Show("Mã định danh không đúng vui lòng nhập lại.", "Thông báo");

}

1. *Kiểm tra thông tin tài khoản nhập vào đăng ký hay chưa, nếu chưa điền đúng thì hiển thị đăng ký thành công.*

Dùng class Modify để lấy thông tin về tên tài khoản, mật khẩu, xác nhận mật khẩu và email từ các textBox tương ứng, sau đó kiểm tra tính hợp lệ của các thông tin này bằng cách sử dụng các phương thức CheckAccount và CheckEmail. Nếu có bất kỳ thông tin nào không hợp lệ, đoạn code sẽ hiển thị một thông báo lỗi và thoát khỏi phương thức. Nếu tất cả các thông tin đều hợp lệ, đoạn code sẽ kiểm tra xem email đã được đăng ký hay chưa. Nếu email đã được đăng ký, đoạn code sẽ hiển thị một thông báo lỗi và thoát khỏi phương thức. Nếu email chưa được đăng ký, đoạn code sẽ thêm thông tin tài khoản mới vào cơ sở dữ liệu và hiển thị một thông báo thành công.

1. *Vào form home giao diện chính*



Hình 3.3

1. *Chọn một tệp từ máy tính*

Tạo ra một đối tượng OpenFileDialog mới và hiển thị một hộp thoại chọn tệp bằng cách gọi phương thức ShowDialog của đối tượng đó. Thiết lập thuộc tính Multiselect của đối tượng OpenFileDialog thành false để chỉ cho phép người dùng chọn một tệp duy nhất. Nếu người dùng chọn một tệp và nhấn nút OK trên hộp thoại chọn tệp, đoạn code sẽ lấy đường dẫn của tệp được chọn và gán giá trị cho thuộc tính Text của đối tượng tbDuongDan.

1. *Tạo bảng chữ cái và bảng tra phục vụ cho thuật toán mã hoá*

Khởi tạo hai mảng bangChuCai và bangTra khi form Home được tải. Đoạn code này đầu tiên thiết lập thuộc tính Checked của đối tượng rbMaHoa thành true. Sau đó, đoạn code khởi tạo mảng bangChuCai với kích thước 256 và gán giá trị cho các phần tử của mảng bằng cách sử dụng vòng lặp for. Cuối cùng, đoạn code khởi tạo mảng bangTra với kích thước 256x256 và gán giá trị cho các phần tử của mảng bằng cách sử dụng hai vòng lặp for lồng nhau.

1. *Đảm bảo rằng chỉ một trong hai RadioButton được chọn tại một thời điểm.*

Xử lý sự kiện khi người dùng thay đổi trạng thái của các radio button MaHoa và GiaiMa.

Bao gồm 2 phương thức xử lý sự kiện rbMaHoa\_ CheckedChanged và rbGiaiMa\_ CheckedChanged. Phương thức rbMaHoa\_CheckedChanged được gọi khi trạng thái của rbMaHoa thay đổi. Nếu rbMaHoa được chọn, sẽ thiết lập thuộc tính Checked của rbGiaiMa thành false. Phương thức rbGiaiMa\_ CheckedChanged được gọi khi trạng thái của rbGiaiMa thay đổi. Nếu rbGiaiMa được chọn sẽ thiết lập thuộc tính checked của rbMaHoa thành false.

1. *Trình tự hoạt động khi click thực hiện*

Dùng class Modify để lấy thông tin về email và mật khẩu từ các TextBox tương ứng, sau đó kiểm tra xem email và mật khẩu có được nhập hay không. Nếu có bất kỳ thông tin nào không được nhập, đoạn code sẽ hiển thị một thông báo lỗi. Nếu cả hai thông tin đều được nhập, đoạn code sẽ kiểm tra xem email và mật khẩu có chính xác hay không bằng cách truy vấn cơ sở dữ liệu.

Nếu nhập đúng mật khẩu và email và rbMaHoa được chọn thì thực hiện mã hóa một tệp tin bằng cách sử dụng thuật toán Vigenere. Ban đầu đọc nội dung của tệp tin được chọn bởi người dùng và sinh ra một khóa từ mật khẩu được nhập bởi người dùng. Sau đó, sử dụng thuật toán Vigenere để mã hóa nội dung của tệp tin bằng cách sử dụng khóa đã sinh ra. Kết quả mã hóa được lưu vào một mảng ketQua. Để hiển thị tiến trình mã hóa bằng cách cập nhật giá trị của progressBar1 sau mỗi lần lặp. Cuối cùng, hiển thị một hộp thoại lưu tệp để cho phép người dùng lưu kết quả mã hóa vào một tệp tin mới.

Nếu nhập đúng mật khẩu và email và rbGiaiMa được chọn thì thực hiện giải mã một tệp tin bằng cách sử dụng thuật toán Vigenere. Ban đầu đọc nội dung của tệp tin được chọn bởi người dùng và sinh ra một khóa từ mật khẩu được nhập bởi người dùng. Sau đó, sử dụng thuật toán Vigenere để giải mã nội dung của tệp tin bằng cách sử dụng khóa đã sinh ra. Kết quả giải mã được lưu vào một mảng ketQua. Để hiển thị tiến trình giải mã bằng cách cập nhật giá trị của progressBar1 sau mỗi lần lặp. Cuối cùng, hiển thị một hộp thoại lưu tệp để cho phép người dùng lưu kết quả giải mã vào một tệp tin mới.

Ngược lại xử lý ngoại lệ khi có lỗi xảy ra trong quá trình đọc hoặc ghi tệp tin. Đoạn code này sử dụng cấu trúc try-catch để bắt ngoại lệ. Nếu có ngoại lệ xảy ra sẽ hiển thị một thông báo lỗi cho người dùng biết rằng tệp tin đang được sử dụng bởi một chương trình khác và yêu cầu người dùng đóng chương trình đó trước khi thử lại.

1. *Kiểm tra nếu người dùng nhập không đúng tài khoản hoặc mật khẩu. Nếu mật khẩu sai đến lần thứ 6 thì sẽ gửi file gốc cho người dùng đồng thời xoá file và thông báo có người cố gắng mở tệp của bạn. Khi gửi xong tệp tin sẽ thoát khỏi form Home về form Đăng nhập.*

Kiểm tra tính chính xác của email và mật khẩu khi người dùng đăng nhập. sử dụng một câu truy vấn để kiểm tra xem có tài khoản nào khớp với email và mật khẩu được nhập hay không. Nếu không có tài khoản nào khớp, đoạn code sẽ hiển thị một thông báo lỗi cho người dùng biết rằng email hoặc mật khẩu không chính xác. tăng biến đếm count lên 1 và kiểm tra xem giá trị của count có bằng 2 hay không. Nếu count bằng 2, sẽ hiển thị một thông báo cho người dùng biết rằng họ đã nhập sai quá nhiều 5 lần và tệp tin sẽ bị xoá. Tiếp tục đến khi người dùng nhập sai quá 5 lần thì sẽ gửi tệp về email và thông báo có người xâm nhập file đồng thời xoá file gốc đi.

1. *Cick đăng xuất*

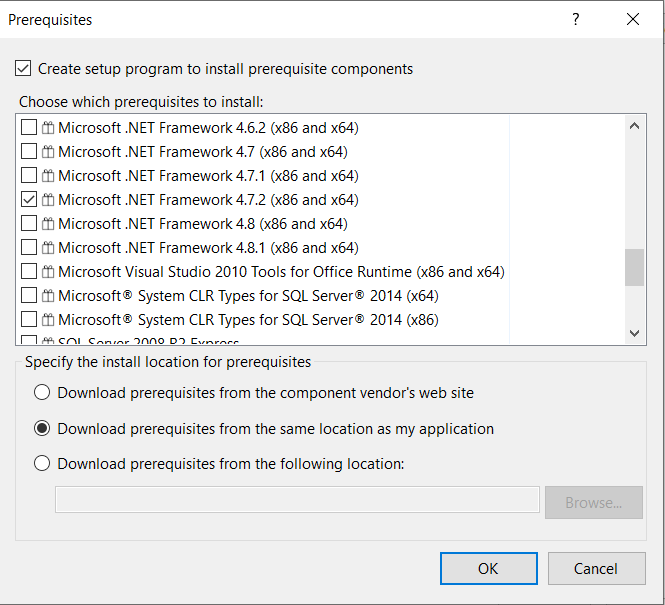
Người dùng nhấn vào nút button1\_DangXuat để đăng xuất. Hiển thị một hộp thoại xác nhận để hỏi người dùng có muốn đăng xuất hay không. Nếu người dùng chọn Yes, đoạn code sẽ ẩn form hiện tại và tạo ra một đối tượng mới của lớp DangNhap. Sau đó, hiển thị form DangNhap bằng cách gọi phương thức ShowDialog của đối tượng DangNhap.

1. *Mã hoá/giải mã ngay bên ngoài ứng dụng*

* Hiện tại nhóm em chưa làm được.

1. *Chạy thành file exe*

* Mở visual studio vào Extentions 🡪 Manage Extentions 🡪 tìm Microsoft Visual Studio Installer Projects 2022 để tải về.
* Chuột phải và Solution chọn Add project 🡪 chọn Setup Project 🡪 đặt tên là FileEncrypt
* Chuột phải vào FileEncrypt 🡪 properties (chỉ định ứng dụng cần cho project)



* Tuỳ chỉnh cho phần mềm sau khi cài: shortcut, icon hiển thị,...
* Sau đó vào build chọn batch build 🡪Solution config 🡪 release|any CPU 🡪 buid
* Mở sql server chọn database xuất thành dòng sript.sql và tạo file thực thi lệnh script

1. *Kết quả*

* Người dùng có thể đăng nhập, đăng ký tài khoản để mã hoá/giải mã tệp tin của mình trong ứng dụng.

1. *Kiểm thử thế nào*

* Chưa kiểm tra được mã định danh, chưa mã hoá/ giải mã ngay tệp tin, file gửi về gmail khi người dùng nhập sai mật khẩu không xem được.
* Nếu má hoá/giải mã trong ứng dụng thì kết quả được coi là ổn.

**CHƯƠNG 4: KẾT LUẬN, KIẾN NGHỊ**

1. **Bạn đã làm được gì?**

* Cho phép người dùng đăng nhập đăng ký tài khoản.
* Mã hoá/ giải mã lưu tệp.
* Sử dụng tiến trình.

1. **Còn tồn đọng gì?**

* Mã định danh gửi về gmail người dùng chưa kiểm tra được, chưa được bảo mật.
* File gửi về gmail người dùng khi nhập mật khẩu sai quá 5 lần bị lỗi file, chưa có tính bảo mật file.

1. **Phương hướng triển khai nốt, nâng cấp như thế nào?**

* Thêm một phần code vào mã hoá mã định danh.
* File gửi về gmail không bị lỗi.
* Thêm lấy lại mật khẩu hoặc đổi mật khẩu nếu người dùng cần.
* Dùng thuật toán mã hoá mạnh mẽ hơn.

**Tài liệu tham khảo**

**Tiếng Việt**

[1] [VB.NET] Sercurity Winform with password - Yêu cầu nhập mật khẩu khi đóng form. (2017, April 17). LaptrinhVB.net. Retrieved April 8, 2023, from <https://laptrinhvb.net/bai-viet/chuyen-de-csharp/--VB-NET---Sercurity-Winform-with-password---Yeu-cau-nhap-mat-khau-khi-dong-form/92493f873d7217e2.html>

[2] Đánh giá NordLocker: Lưu trữ đám mây được mã hóa dễ sử dụng nhất? (2023, March 28). Website Rating. Retrieved April 8, 2023, from <https://www.websiterating.com/vi/cloud-storage/nordlocker-review/>

[3] Bảo vệ dữ liệu riêng tư/quan trọng theo cách an toàn nhất. (2011, June 19). Dân trí. Retrieved April 8, 2023, from <https://dantri.com.vn/suc-manh-so/bao-ve-du-lieu-rieng-tuquan-trong-theo-cach-an-toan-nhat-1308617763.htm>

[4] AxCrypt Premium/Business 2.1.1629.0 Full - Mã hóa và bảo vệ tập tin. (2021, April 17). VN-Zoom. Retrieved April 8, 2023, from <https://vn-z.vn/threads/axcrypt-premium-business-2-1-1629-0-full-ma-hoa-va-bao-ve-tap-tin.39243/>

[5] Symantec Encryption Desktop Professional 10.5.0 MP1 - Mã hóa, bảo vệ dữ liệu. (n.d.). Taiwebs.com. Retrieved April 8, 2023, from <https://taiwebs.com/windows/download-symantec-encryption-desktop-professional-2127.html>

[6] GiliSoft File Lock Pro - Phần mềm mã hóa. (n.d.). Download.com.vn. Retrieved April 8, 2023, from <https://download.com.vn/gilisoft-file-lock-pro-18089>

[7] (2020, August 11). Rohos Mini Drive -Download- Tải về - Bảo mật dữ liệu trên ổ cứng, usb. Retrieved April 8, 2023, from <https://taimienphi.vn/download-rohos-mini-drive-1479>

[8] Home. (n.d.). YouTube. Retrieved April 8, 2023, from <https://progsoft.net/vi/software/challenger>

[9] Đánh giá NordLocker: Lưu trữ đám mây được mã hóa dễ sử dụng nhất? (2023, March 28). Website Rating. Retrieved April 8, 2023, from <https://www.websiterating.com/vi/cloud-storage/nordlocker-review/>

[10] Cách mã hóa dữ liệu bằng phần mềm AxCrypt. (2018, June 15). Quantrimang.com. Retrieved April 8, 2023, from <https://quantrimang.com/cong-nghe/cach-ma-hoa-du-lieu-bang-phan-mem-axcrypt-152920>

[11] Mai, A. H. (2018, July 30). FileEncrypt. github. Retrieved June 10, 2023, from <https://github.com/maihaan/atbmtt/tree/master/ATBMTT/FileEncrypt>

**Tiếng Anh**

[1] Rubenking, N. J. (n.d.). Steganos Safe Review. PCMag. Retrieved April 8, 2023, from <https://www.pcmag.com/reviews/steganos-safe>

[2] Rubenking, N. J. (n.d.). Advanced Encryption Package Review. PCMag. Retrieved April 8, 2023, from <https://www.pcmag.com/reviews/intercrypto-advanced-encryption-package>

[3] Cool MinE. (2012, April 26). How to encrypt and decrypt files in C#. Fluxbytes. Retrieved June 4, 2023, from https://www.fluxbytes.com/csharp/encrypt-and-decrypt-files-in-c/

[4] FoxLearn. (2019, August 7). Windows Forms: How to Encrypt and Decrypt files using AES encryption algorithm in C#. FoxLearn. Retrieved June 4, 2023, from <https://foxlearn.com/windows-forms/windows-forms-how-to-encrypt-and-decrypt-files-using-aes-encryption-algorithm-in-c-396.html>

**Video**

[1] Nguyễn, Đ. (2019, May 7). .[Window Forms Apps] Form Đăng Nhập, Đăng Ký Tài Khoản và Quên Mật Khẩu (SQL Server) - C#. - YouTube. Retrieved May 22, 2023, from https://www.youtube.com/watch?v=fZHW8mEFO9E&list=LL&index=14&t=2042s

[2] KhoaiCodeTV. (2019, May 7). .Gởi Email bằng Gmail xác thực 2 bước | Send Email with Gmail 2 Step Verification | KhoaicodeTV. . - YouTube. Retrieved May 22, 2023, from <https://www.youtube.com/watch?v=YO8EzBimx0U&list=LL&index=15>

[3] Lai. (2019, May 7). .Hướng dẫn kết nối Database Visual Studio với SQL Sever thành công 100%.-YouTube. Retrieved May 22, 2023, from <https://www.youtube.com/watch?v=OKOGQ71MqZ4&list=LL&index=12&t=398s>

[4] Đỗ, Đ. V. (2023, April 15). 004 An toàn bảo mật thông tin Phương pháp mã hóa đa bảng chữ VIGENERE – AUTOKEY. YouTube. Retrieved June 10, 2023, from <https://www.youtube.com/watch?v=p4TOsQ_3L_4>

[5] Chan. (n.d.). Đóng gói phần mềm. youtobe. Retrieved June 10, 2023, from https://www.youtube.com/watch?v=jAYZC\_CU0zE&list=LL&index=2&t=249s

[6] Đóng gói ứng dụng c#. (2018, July 30). YouTube. Retrieved June 10, 2023, from https://www.youtube.com/watch?v=nQDBIh3ojGs&list=LL&index=3&t=598s