MÃ HOÁ THÔNG TIN & ỨNG DỤNG

Đồ án thực hành

Nhóm:

- Phan Trọng Đạt 1512102
- Nguyễn Văn Quang Huy 1512205

Khoa Công nghệ thông tin

Đại học Khoa học tự nhiên TP HCM

MỤC LỤC

Báo cáo

Các nội dung chính

1. Thông tin nhóm.
2. Các chức năng.
3. Các vấn đề và giải pháp.
4. Bảng tổng hợp chức năng.

1 Thông tin nhóm

Thông tin các thành viên trong nhóm:

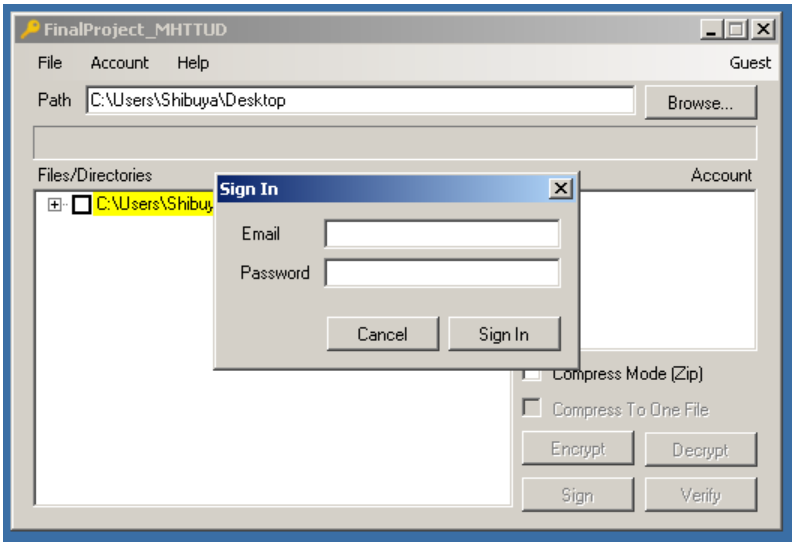
Họ tên	*MSSV*	*Điện thoại*	*Email*
Phan Trọng Đạt	1512102	01646182803	1512102@student.hcmus.edu.vn
Nguyễn Văn Quang Huy	1512205	01648733588	1512205@student.hcmus.edu.vn

2 Các chức năng

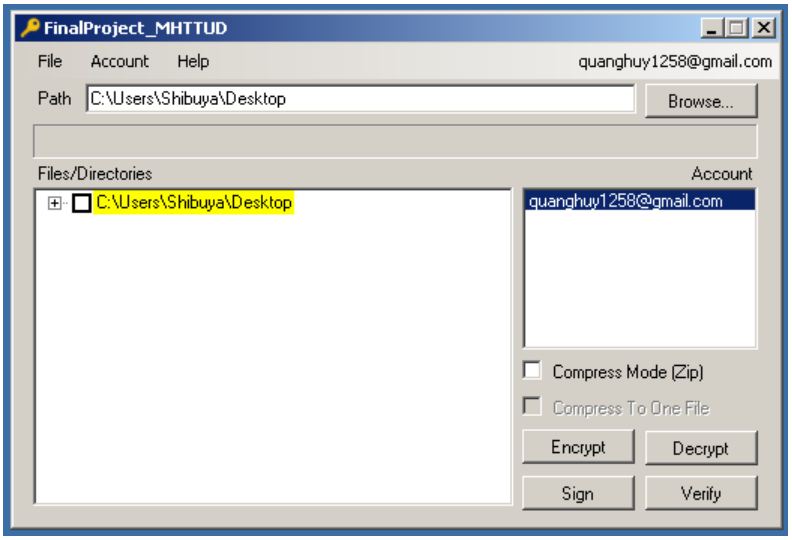
2.1. Các chức năng liên quan đến tài khoản

2.1.1. Đăng nhập tài khoản

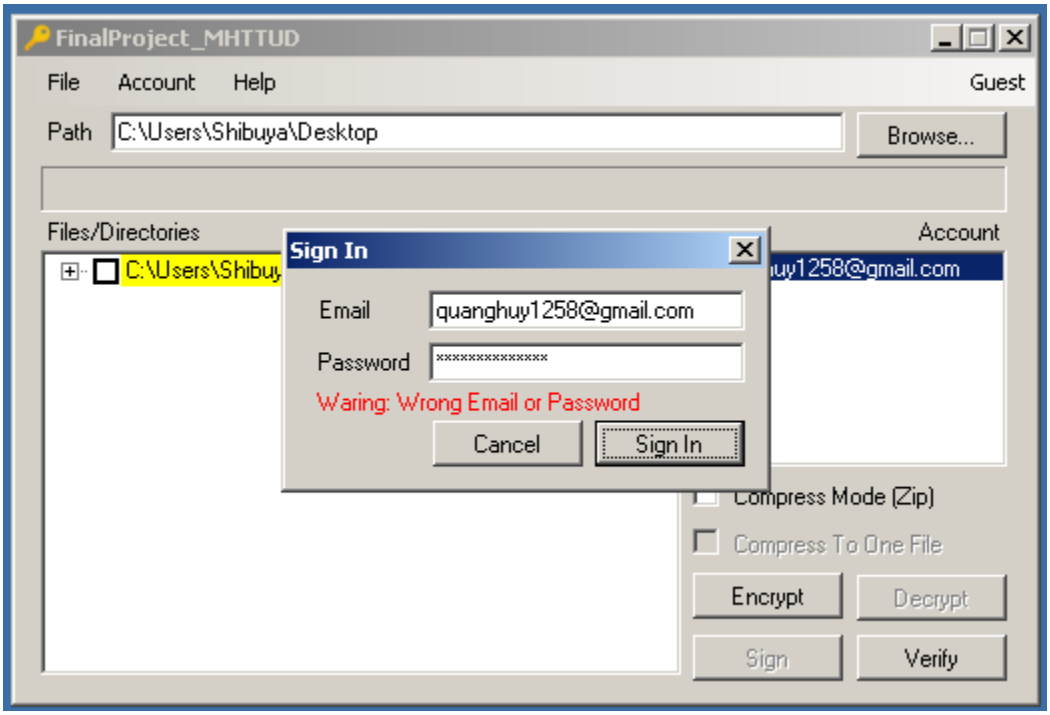
- Đây là màn hình giao diện khi đăng nhập vào tài khoản. Khi không có ai đăng nhập trước đó hoặc những người đăng nhập trước đó đã đăng xuất hết, tức là người dùng sử dụng chương trình với vai trò là khách (guest) thì mới dùng được chức năng này.



- Sau khi đăng nhập thành công thì đây là hình ảnh giao diện. Email đăng nhập của người dùng sẽ hiện ở góc trên bên phải của màn hình.

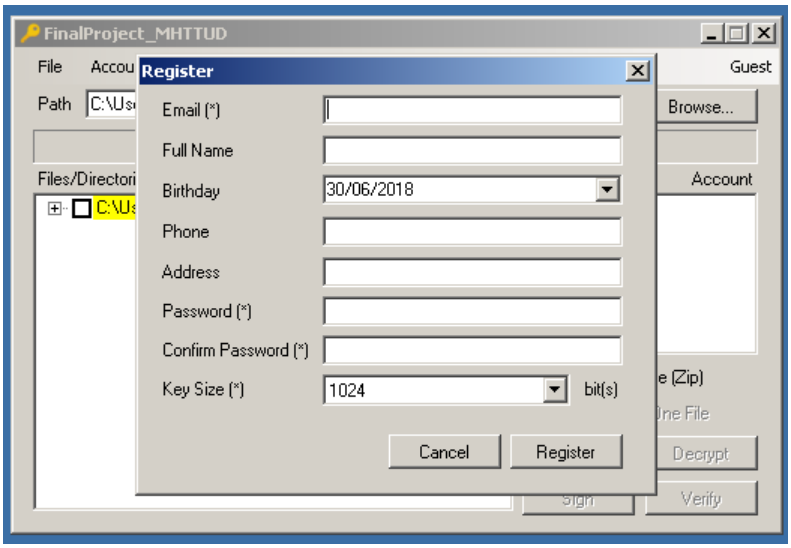


- Nếu người dùng nhập sai email hoặc password đăng nhập thì không thể nào đăng nhập được và chương trình sẽ hiển thị dòng chữ cảnh báo màu đỏ để thông báo cho người dùng.



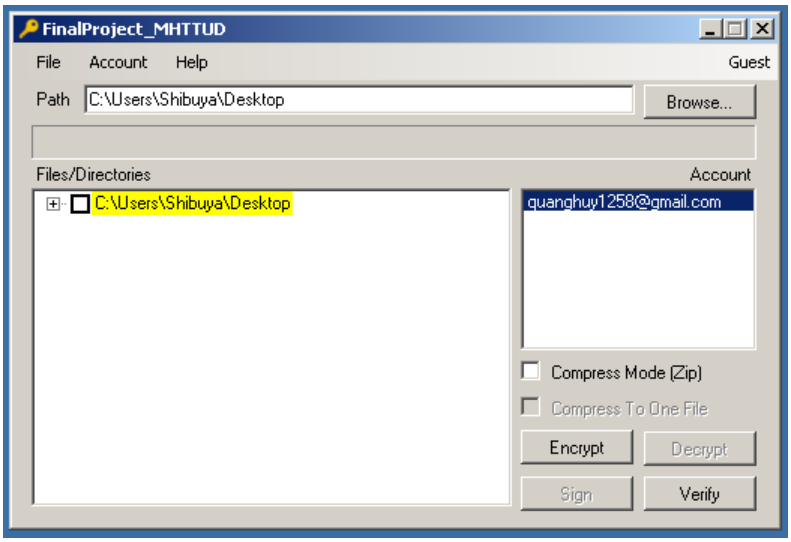
2.1.2. Đăng ký tài khoản

- Đây là màn hình giao diện khi đăng ký tài khoản. Khi không có ai đăng nhập trước đó hoặc những người đăng nhập trước đó đã đăng xuất hết, tức là người dùng sử dụng chương trình với vai trò là khách (guest) thì mới dùng được chức năng này.



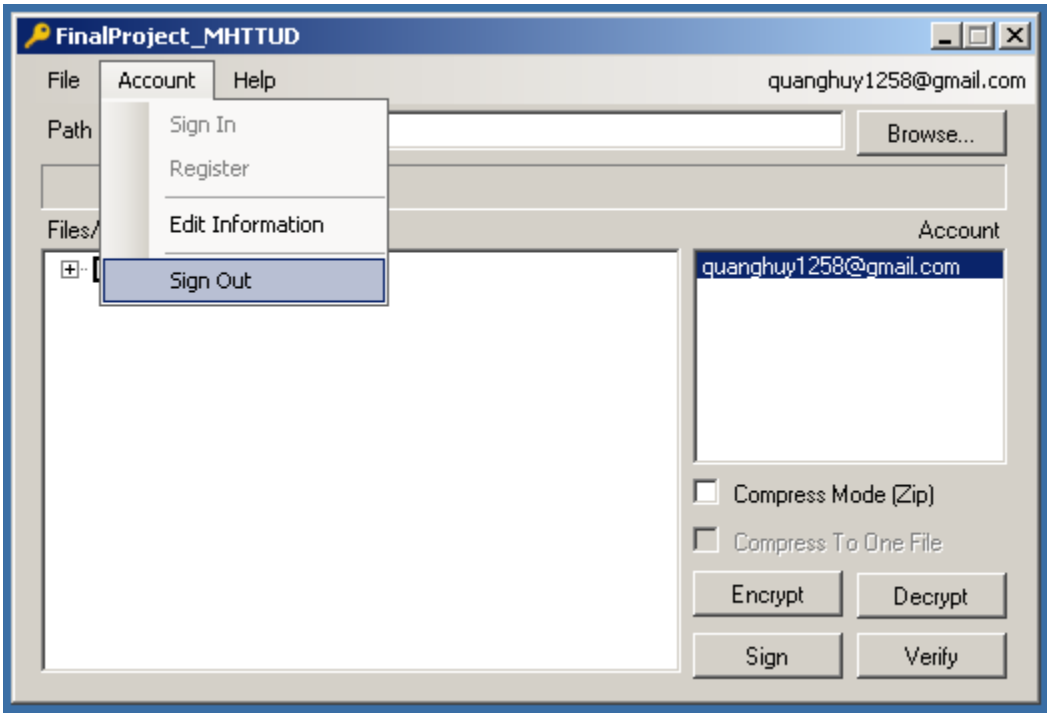
- Khi đăng ký tài khoản, các trường email, password, confirm password và key size bắt buộc phải khác rỗng. Mặc định, key size là 1024 bit. Riêng đối với password và confirm password phải giống nhau để đảm bảo người dùng nhập đúng password. Email đăng ký không được trùng với bất kỳ tài khoản nào trước đó.

- Sau khi đăng ký thành công, tài khoản mới sẽ được hiện ở phía bên phải, trong mục Account.



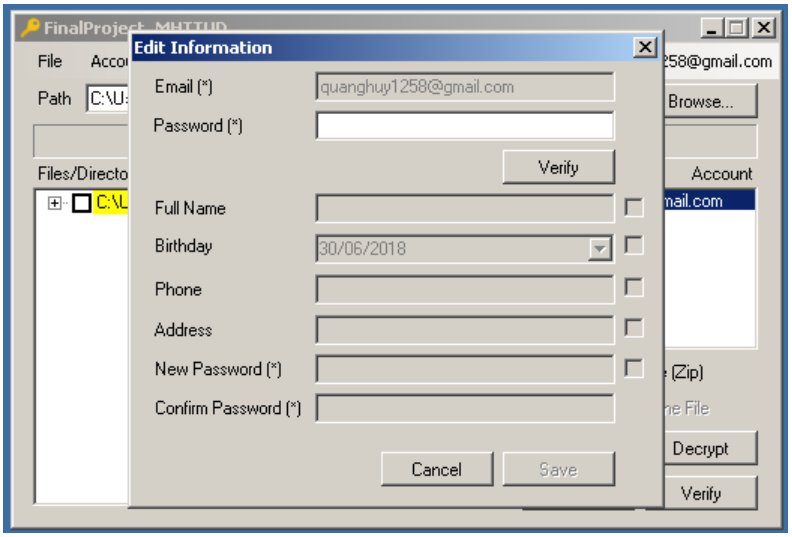
2.1.3. Đăng xuất

- Sau khi đăng nhập thành công, nếu người dùng muốn đăng xuất thì chỉ cần nhấn vào nút Sign out như màn hình giao diện ở dưới.



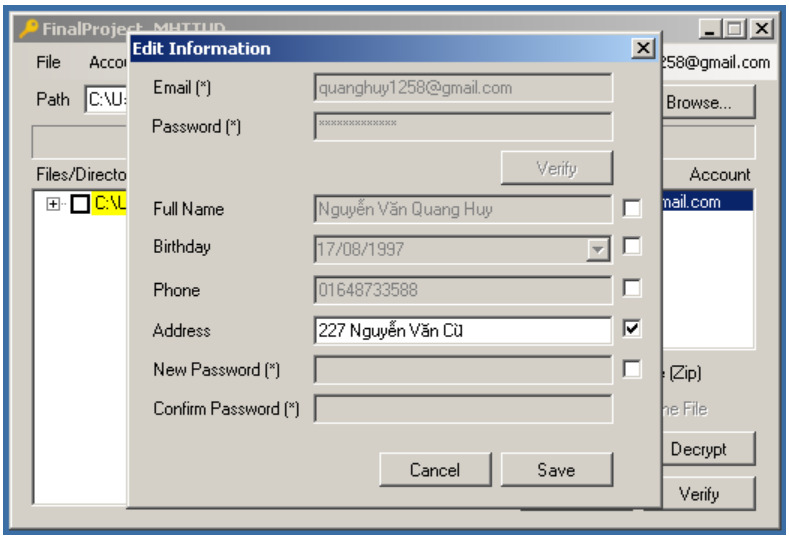
2.1.4. Cập nhật thông tin tài khoản

- Sau khi đăng nhập thành công, người dùng có thể chỉnh sửa các thông tin cá nhân của mình hoặc thay đổi password. Đây là màn hình giao diện khi cập nhật thông tin tài khoản.



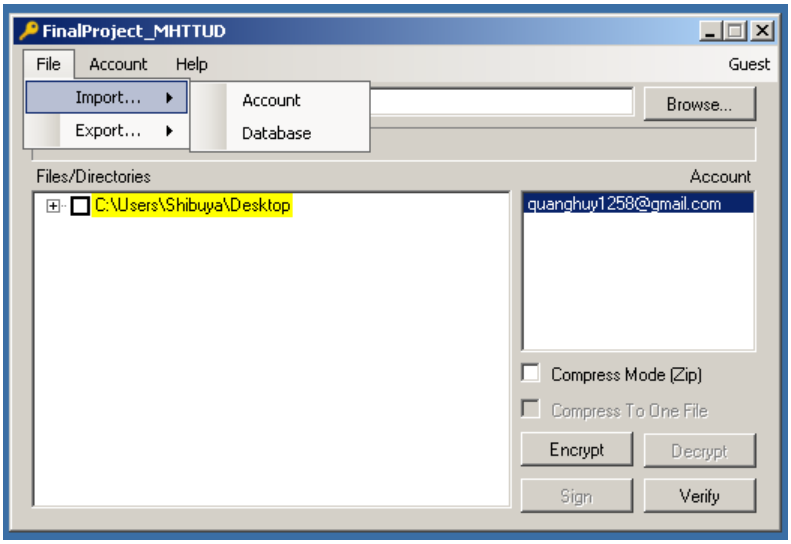
- Đầu tiên, người dùng phải nhập chính xác password của mình thì mới có thể tiến hành cập nhật thông tin tài khoản. Sau khi nhập, người dùng nhấn Verify để chương trình tiến hành kiểm tra.

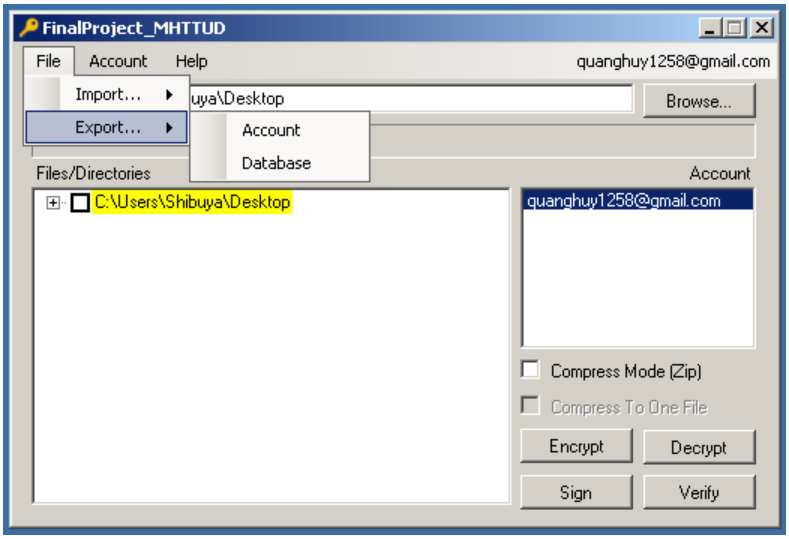
- Sau khi người dùng nhập đúng password thì chương trình hiển thị các thông tin cá nhân hiện tại của người dùng. Người dùng chọn các trường mình muốn và tiến hành chỉnh sửa. Cuối cùng, người dùng nhấn Save để lưu lại.



2.1.5. Export và Import dữ liệu về các thông tin tài khoản

- Chương trình có thể export hoặc import thông tin của 1 tài khoản hoặc toàn bộ cơ sở dữ liệu.





- Thông tin của 1 tài khoản được lưu trữ trong file có phần mở rộng là .acc

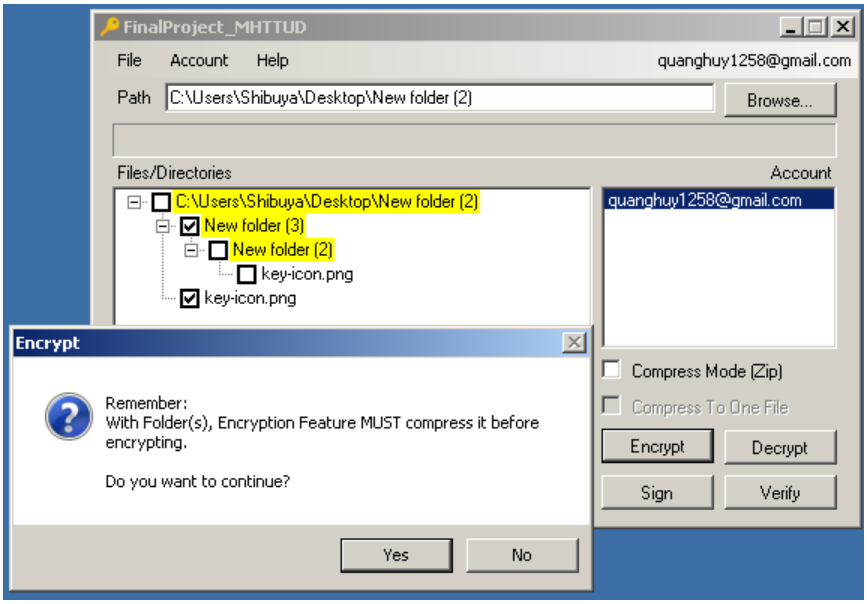
Thông tin các tài khoản của cơ sở dữ liệu được lưu trữ trong file có phần mở rộng là .dbacc

- Thông tin của mỗi tài khoản khi export hoặc import gồm email, họ tên, ngày sinh, điện thoại, địa chỉ, hash của (password + salt) và salt, private key (được mã lại bằng hash của password), public key.

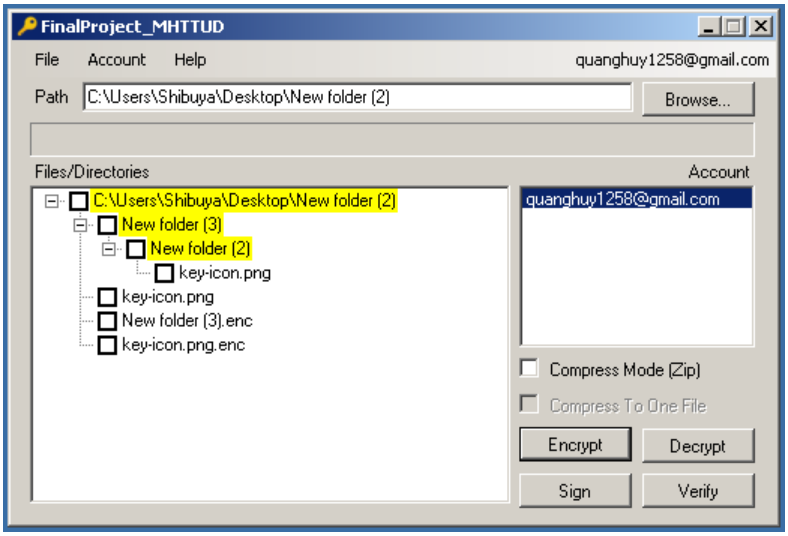
2.2. Mã hoá và giải mã

2.2.1. Mã hoá

- Bất kỳ người dùng nào (kể cả Khách) cũng có thể sử dụng chức năng mã hoá. Đây là màn hình giao diện khi thực hiện mã hoá. Người nhận sẽ được người dùng chọn trong danh sách các tài khoản được hiển thị ở phía bên phải, phần Account.



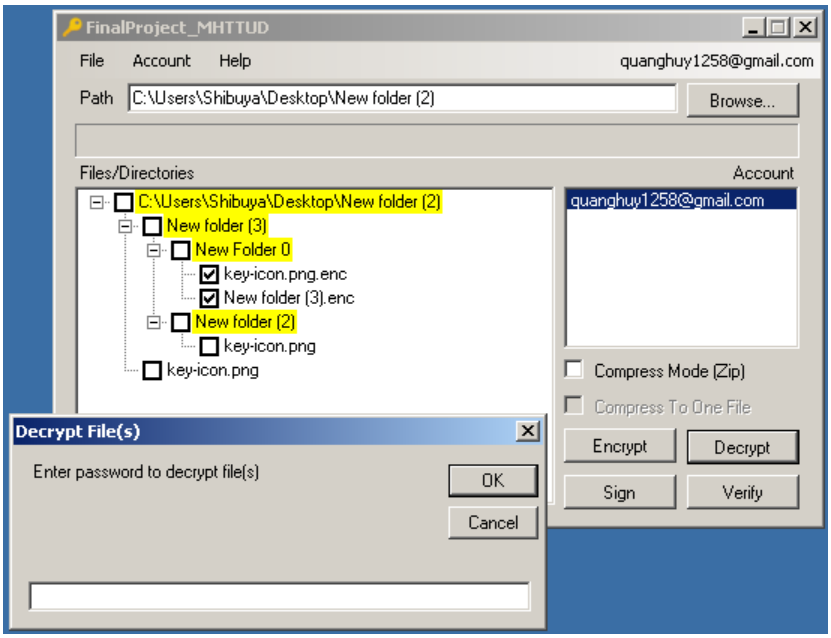
- Đối với chức năng mã hoá, chương trình có thể cho phép người dùng mã hoá cùng lúc nhiều file hoặc thư mục. Đối với file, chương trình có thể cho phép người dùng thực hiện nén file trước hoặc không rồi mới mã hoá. Đối với thư mục, chương trình sẽ nén thư mục lại rồi mới mã hoá. Ngoài ra, chương trình có thể cho phép người dùng nén nhiều file hoặc thư mục vào chung 1 tập tin rồi mới tiến hành mã hoá. Sau khi mã hoá, các tệp tin mã hoá sẽ có phần mở rộng là .enc



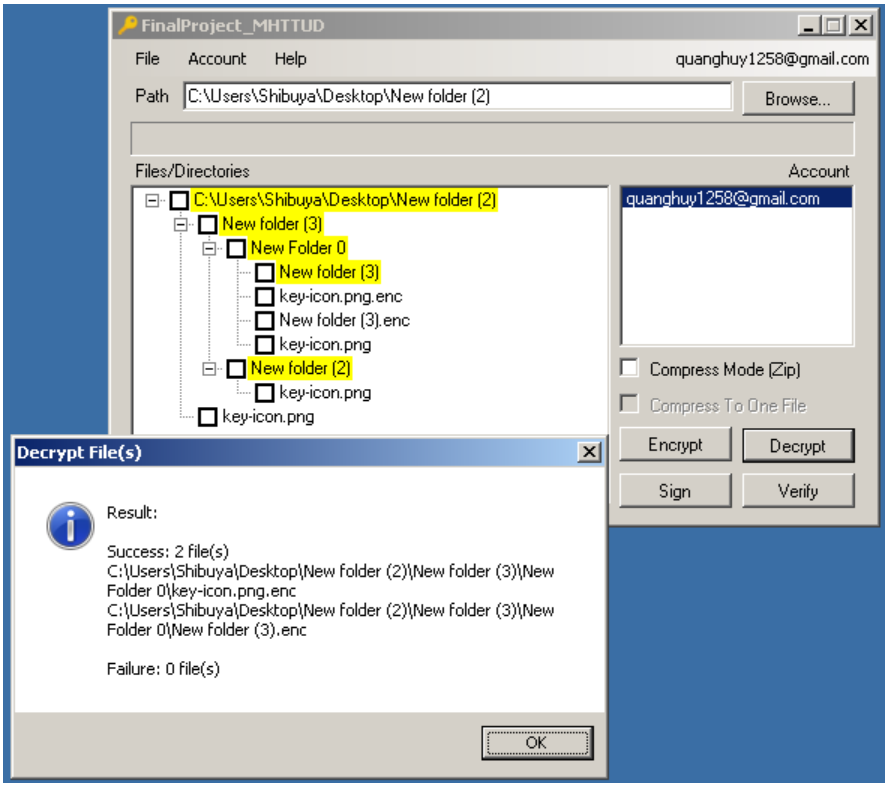
- Thuật toán nén sử dụng thư viện System.IO.Compression của C#. Chuẩn nén sử dụng là Zip.

2.2.2. Giải mã

- Chỉ có chủ sở hữu của khoá dùng để mã hoá file mới có thể giải mã được file. Chức năng giải mã chỉ dùng cho file có phần mở rộng .enc, không dùng cho các trường hợp khác. Để giải mã file thì người dùng phải đăng nhập vào tài khoản của mình, đồng thời mỗi lần dùng chức năng này đều phải nhập lại password để xác nhận. Đây là màn hình giao diện khi thực hiện giải mã.



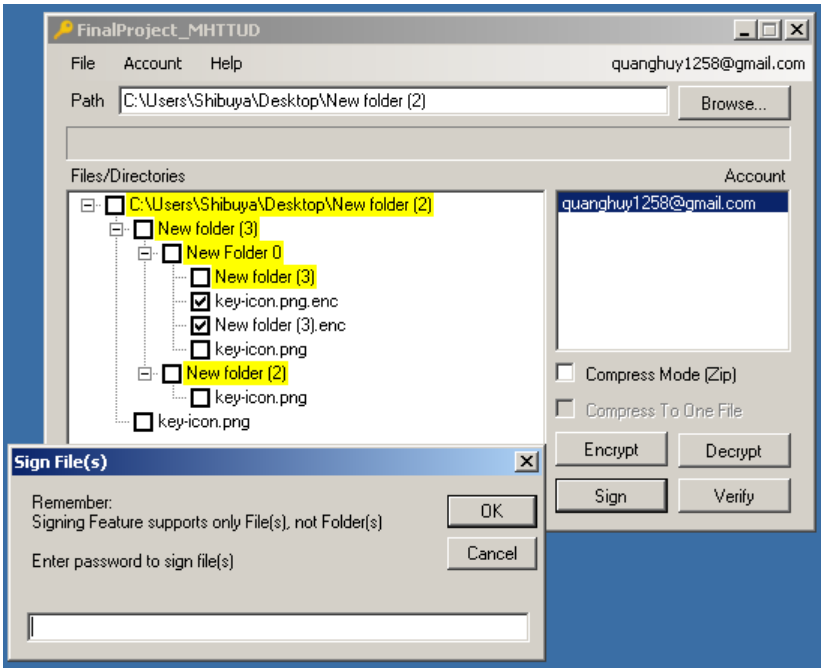
- Đối với file mã hoá không nén thì khi giải mã sẽ giải mã ra file. Đối với file mã hoá có nén thì khi giải mã sẽ giải mã ra thư mục. Đây là màn hình giao diện sau khi giải mã thành công.



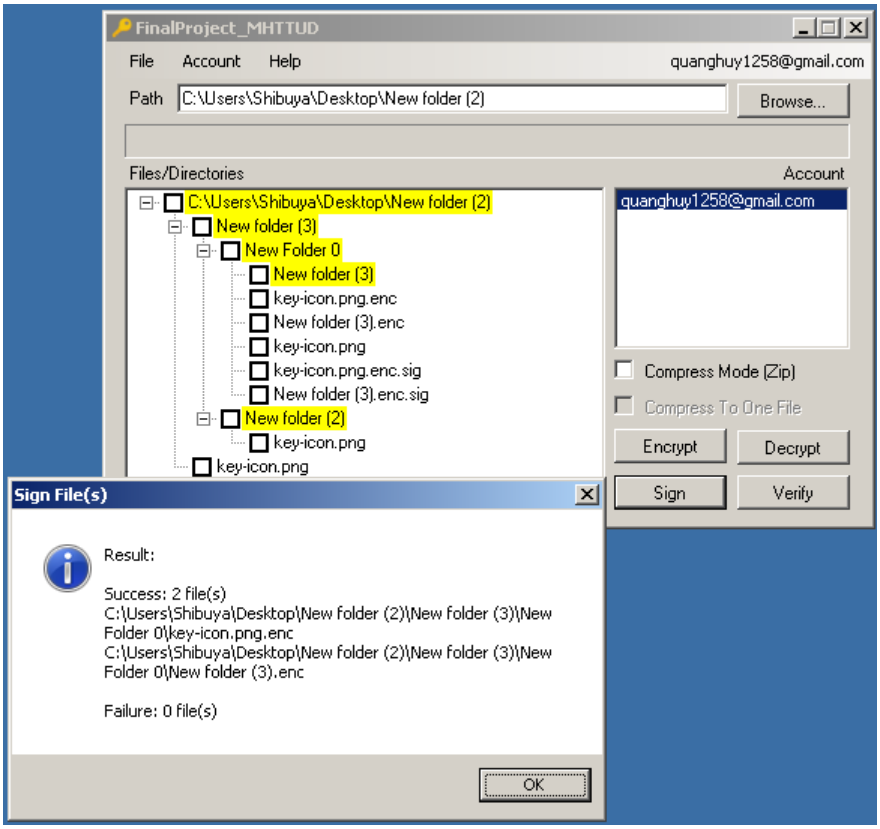
2.3. Ký và xác nhận chữ ký

2.3.1. Ký file

- Chức năng ký chỉ dùng cho file, không dùng cho thư mục. Người dùng cần đăng nhập để có thể sử dụng chức năng này. Ngoài ra, mỗi lần dùng chức năng này, người dùng cần phải nhập lại password để xác nhận. Chương trình có thể cho phép người dùng ký cùng lúc nhiều file. Đây là màn hình giao diện khi thực hiện chức năng ký.

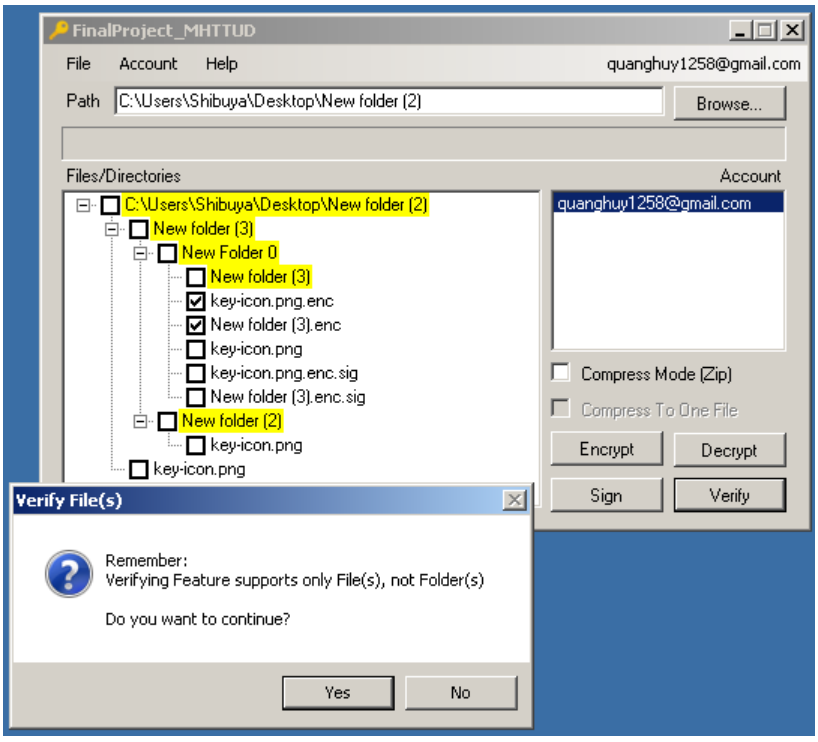


- Đây là màn hình giao diện sau khi ký thành công. Sau khi ký, các file lưu chữ ký sẽ có phần mở rộng .sig

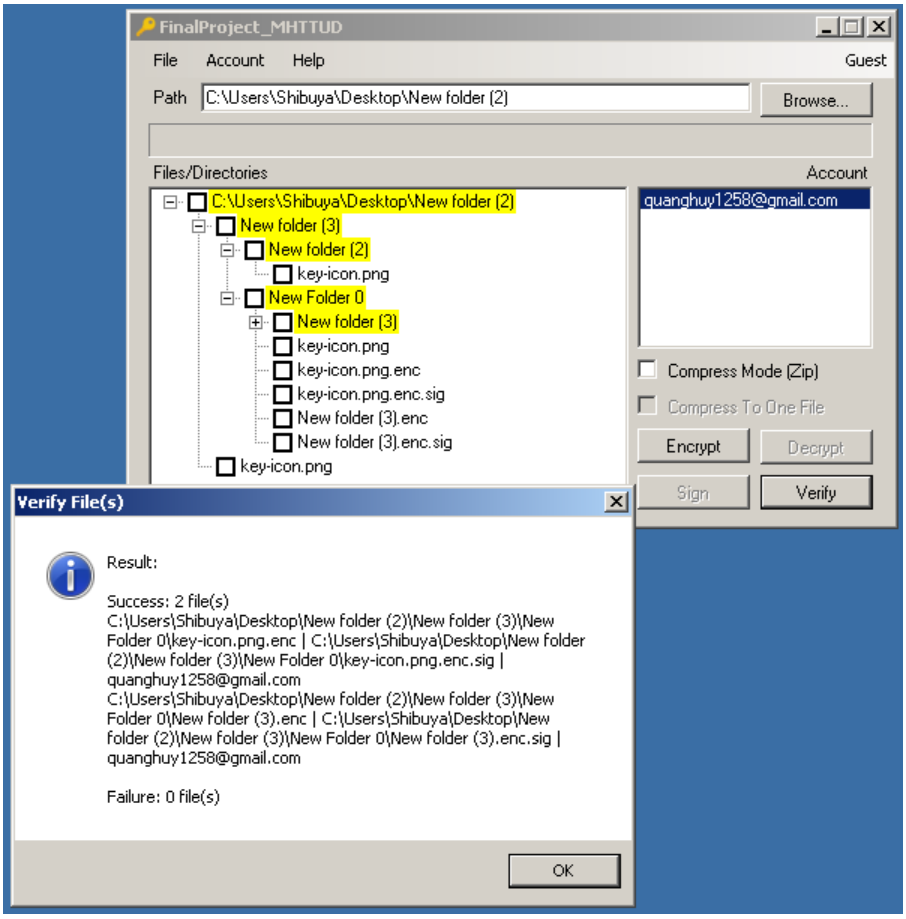


2.3.2. Xác nhận chữ ký file

- Bất kỳ người dùng nào (kể cả Khách) cũng có thể sử dụng chức năng xác nhận chữ ký. Chương trình cho phép người dùng có thể xác nhận cùng lúc nhiều file. Tuy nhiên, mỗi file người dùng cần phải chọn file chữ ký tương ứng. Chương trình chỉ chấp nhận những file chữ ký có phần mở rộng là .sig . Đây là màn hình giao diện khi thực hiện xác nhận chữ ký.

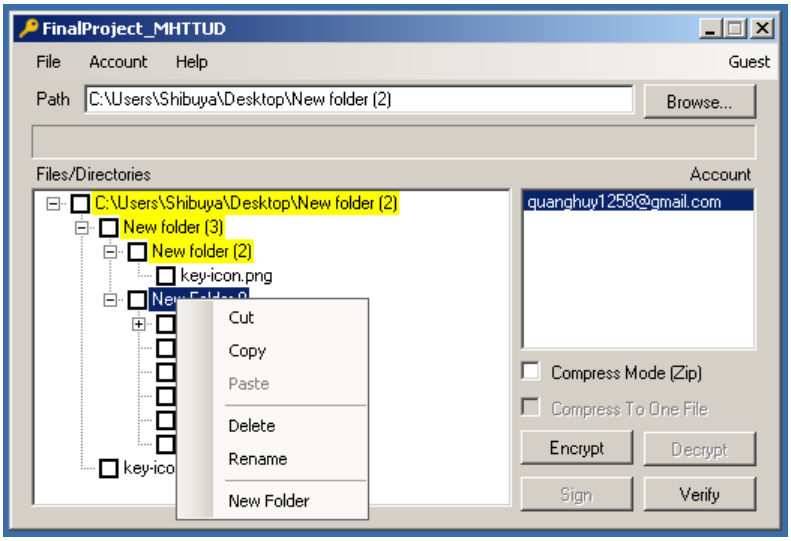


- Đây là màn hình giao diện sau khi xác nhận chữ ký. Nếu xác nhận chữ ký thành công thì chương trình sẽ hiển thị tên file chứa nội dung, tên file chứa chữ ký và email của người ký.



2.4. Các chức năng liên quan đến quản lý hệ thống tập tin, thư mục

- Đây là màn hình giao diện khi thực hiện chức năng quản lý hệ thống tập tin, thư mục. Chương trình cho phép người dùng chọn và mở thư mục hiện hành. Khi đó, chương trình sẽ hiển thị cây thư mục trong thư mục hiện hành. Chương trình cung cấp người dùng các chức năng Cut, Copy, Paste, Delete, Rename file và thư mục, tạo thư mục mới trong thư mục hiện hành. Các thư mục sẽ được tô màu vàng, còn các file không được tô màu.



3 Các vấn đề và giải pháp

3.1. Vấn đề lưu trữ tài khoản

- Vấn đề những thông tin nào của tài khoản cần được bảo mật và không cần được bảo mật?

→ Giải pháp: Chỉ có passphrase và private key cần được bảo mật. Những thông tin còn lại không được bảo mật để cung cấp các thông tin bổ sung về chủ cặp khoá nếu cần khi mã hoá file hay xác nhận chữ ký. Để bảo mật passphrase thì chương trình chỉ lưu salt và hash(passphrase+salt). Để bảo mật private key thì chương trình chỉ lưu bản mã của private key được mã bằng mã hoá đối xứng với key là hash của passphrase.

- Vấn đề tài khoản và cơ sở dữ liệu được lưu xuống nên lưu dạng text hay binary được mã lại bằng khoá được nhúng sẵn trong chương trình?

→ Giải pháp: Cho dù được mã lại bằng khoá được nhúng sẵn trong chương trình thì với kỹ thuật dịch ngược mã nguồn, sẽ có lúc khoá đó bị lộ ra. Vì vậy, lưu dạng nào cũng không đảm

bảo an toàn, nên chọn lưu dạng text để đơn giản hoá quá trình đọc ghi dữ liệu. Mục tiêu của chương trình là đảm bảo an toàn cho passphrase và private key của tài khoản.

3.2. Vấn đề mã hoá và giải mã

- Vấn đề cho phép người dùng chọn padding scheme và mode of operation hay quy định sẵn cố định 1 padding scheme và 1 mode of operation?

→ Giải pháp: Với giả định rằng người dùng phổ thông không biết quá nhiều về các kỹ thuật bảo mật, nếu để người dùng chọn thì sẽ tiềm ẩn các nguy cơ mất an toàn bảo mật. Do vậy, chương trình sẽ quy định sẵn cố định 1 padding scheme và 1 mode of operation.

3.3. Vấn đề lựa chọn password

- Vấn đề: Khi tạo tài khoản hay chỉnh sửa thông tin cá nhân, người dùng có thể tạo ra 1 password yếu, có thể bị tấn công bằng cách brute force. Làm cách nào để hạn chế điều đó?

→ Giải pháp: Chương trình không ép buộc người dùng phải tạo password thoả mãn các điều kiện cho 1 password mạnh vì có thể khiến cho người dùng gặp khó khăn, gây ức chế khi đăng ký tài khoản, dẫn đến có thể bị mất khách hàng. Tuy nhiên, chương trình vẫn đưa ra đánh giá password của người dùng là mạnh hay yếu để người dùng nhận thức được mức độ rủi ro khi sử dụng password của mình.

4 Bảng tổng hợp chức năng

STT	Chức năng	Thực hiện	Ghi chú
1. Đăng ký tài khoản và phát sinh cặp khoá (bất đối xứng):			
1.1	Nhập đầy đủ thông tin về người sở hữu khoá	Có	
1.2	Cho NSD chọn độ dài cặp khoá (từ 512 đến 1024)	Có	
1.3	Phát sinh cặp khoá với độ dài được chọn	Có	
1.4	Passphrase được lưu dưới dạng Hash(Passphrase kết hợp với Salt) và Salt	Có	
1.5	Lưu trữ thông tin về người sở hữu và thông tin cặp khoá vào file hay CSDL	Có	
1.6	Mã hoá nội dung private key	Có	
2. Cập nhật thông tin tài khoản và passphrase			
2.1	Có kiểm tra passphrase trước khi cập nhật hay không?	Có	

2.2	Cho phép cập nhật thông tin cá nhân	Có	
2.3	Cho phép phát sinh passphrase	Có	
2.4	Lưu lại thông tin cập nhật	Có	
3. Export và Import thông tin về cặp khoá			
3.1	Export cặp khoá và thông tin liên quan	Có	
3.2	Import cặp khoá và thông tin liên quan	Có	
4. Mã hoá tập tin			
4.1	Cho NSD chọn tập tin cần mã hoá	Có	
4.2	Cho NSD chọn thuật toán mã hoá đối xứng	Không	
4.3	Cho NSD chọn người nhận	Có	
4.4	Hệ thống phát sinh khoá bí mật (K_s)	Có	
4.5	Mã hoá nội dung tập tin (mã hoá đối xứng)	Có	
4.6	Mã hoá khoá bí mật K_s bằng public key của người nhận	Có	
4.7	Đưa thông tin khoá bí mật đã được mã hoá vào tập tin	Có	
4.8	Cho NSD chọn padding mode	Không	
4.9	Cho NSD chọn mode of operation	Không	
4.10	Nén tập tin trước khi mã hoá	Có	Có 2 chế độ là có nén trước khi mã và không có nén trước khi mã. Ngoài tập tin ra, còn áp dụng cho cả thư mục.
4.11	Cho phép chọn nhiều tập tin để xử lý cùng lúc	Có	Có 2 chế độ là xử lý các file cùng lúc nhưng riêng biệt và xử lý các file cùng lúc nén chung vào 1 tập tin rồi mã
5. Giải mã tập tin			
5.1	Kiểm tra passphrase trước khi giải mã tập tin	Có	
5.2	Giải mã khoá bí mật K_s bằng private key của người nhận	Có	
5.3	Giải mã nội dung tập tin	Có	
5.4	Giải nén tập tin (nếu đã nén khi mã hoá)	Có	
6. Ký trên tập tin			
6.1	Kiểm tra passphrase trước khi ký	Có	
6.2	Hash tập tin cần ký	Có	
6.3	Tạo tập tin chữ ký	Có	
7. Xác nhận chữ ký trên tập tin			
7.1	Hệ thống tự động duyệt qua từng public key có trong dữ liệu	Có	
7.2	Kiểm tra chữ ký hợp lệ	Có	
8. Các chức năng khác			
8.1	Giao diện quản lý hệ thống tập tin, thư mục	Có	

8.2	Liên hệ với nhà phát triển	Có	