

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH

ĐẠI HỌC KHOA HỌC TỰ NHIÊN

KHOA CÔNG NGHỆ THÔNG TIN



MÃ HÓA THÔNG TIN VÀ ỨNG DỤNG - CQ2016/2

2018 – 2019

ĐỒ ÁN THỰC HÀNH (LẬP TRÌNH) CUỐI KỲ

GVHD: TRẦN MINH TRIẾT, LƯƠNG VĨ MINH
1612406

TP. Hồ Chí Minh, 20/06/2019

MỤC LỤC

MỤC LỤC.....	1
1. Thông tin nhóm.....	2
2. Các chức năng.....	2
2.1. Đăng ký tài khoản và phát sinh cặp khóa (bất đối xứng)	2
2.2. Đăng nhập	4
2.3. Cập nhật thông tin và passphrase.....	6
2.4. Export và import thông tin về cặp khóa	9
2.4.1. Export Account	9
2.4.2. Import Account	10
2.5. Mã hóa và giải mã tập tin	13
2.5.1. Mã hóa tập tin	13
2.5.2. Giải mã tập tin	15
2.6. Ký và xác nhận chữ ký cho tập tin	18
2.6.1. Ký lên tập tin	18
2.6.2. Xác nhận chữ ký cho tập tin.....	19
3. Vấn đề và giải pháp	21
3.1. Private key của user.....	21
3.2. Chọn padding scheme và mode of operation	21
3.3. Khóa bí mật (K_s)	22
4. Bảng tổng hợp chức năng.....	22

1. Thông tin nhóm

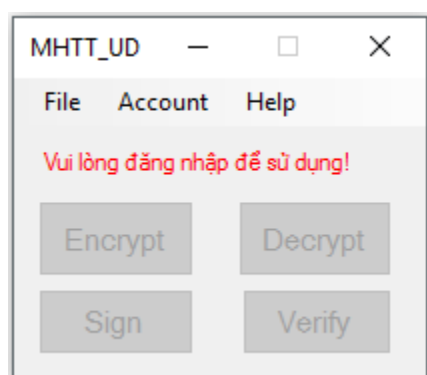
MSSV	Họ và tên	Điện thoại	Email
1612406	Đặng Phương Nam	0832117049	phuongnam.vl1997@gmail.com

Link Demo: https://youtu.be/q_lGSQgvaRA

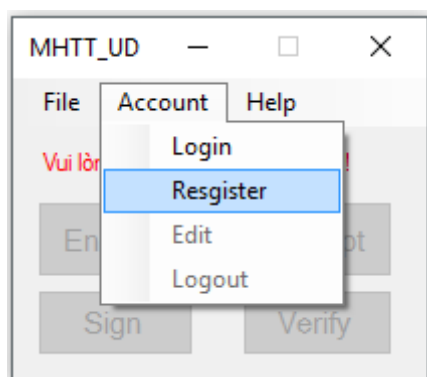
2. Các chức năng

2.1. Đăng ký tài khoản và phát sinh cặp khóa (bất đối xứng)

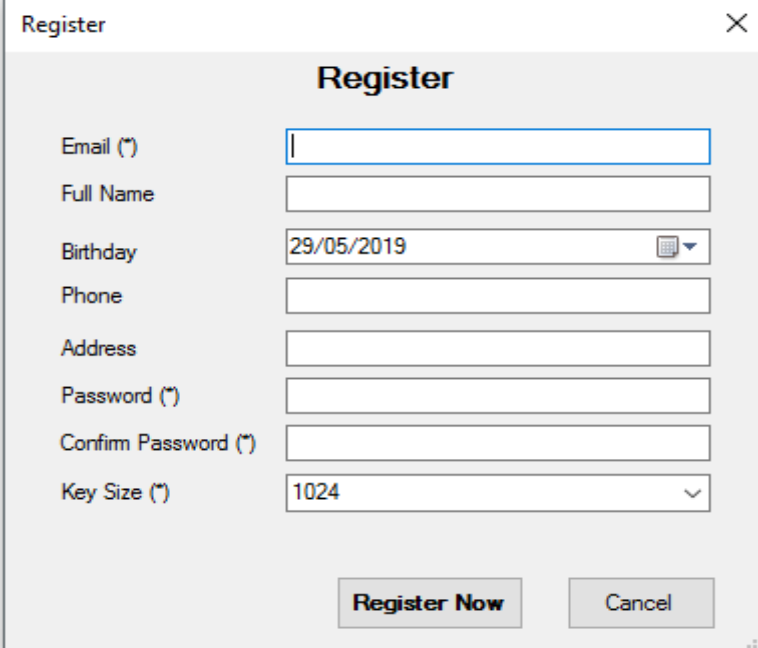
- Ban đầu chương trình chưa có user nào đăng nhập vào, nên tất cả các chức năng của chương trình đều bị khóa lại không cho sử dụng:



- Để đăng ký tài khoản mới, user chọn Account → Register:

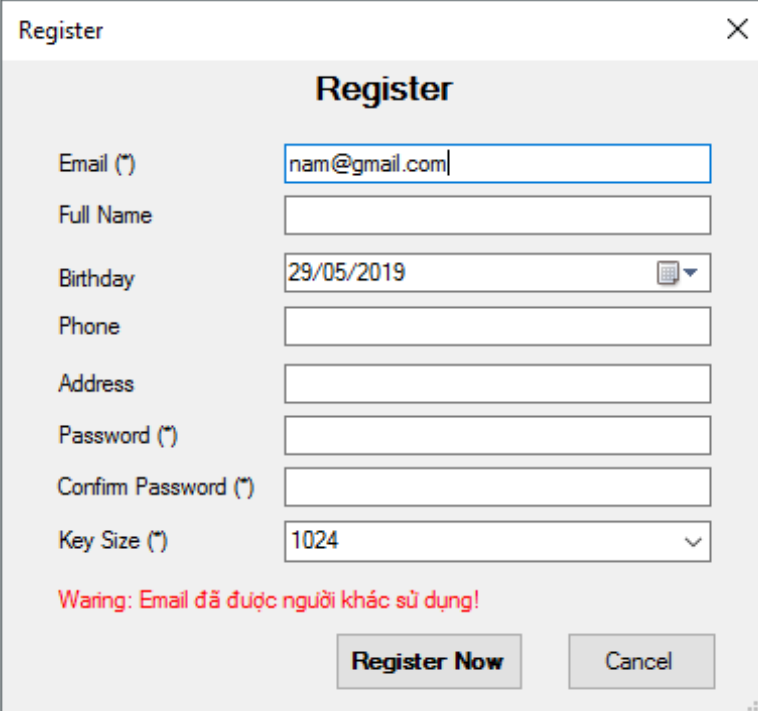


- Sau đó tiến hành điền các thông tin cần thiết vào khung bên dưới:



The image shows a 'Register' dialog box with a title bar containing a close button. The dialog has a title 'Register' and several input fields: 'Email (*)', 'Full Name', 'Birthday' (with a date picker showing 29/05/2019), 'Phone', 'Address', 'Password (*)', 'Confirm Password (*)', and 'Key Size (*)' (a dropdown menu showing 1024). At the bottom, there are two buttons: 'Register Now' and 'Cancel'.

- Lưu ý các trường Email, Password, Confirm Password và Key Size không được rỗng, đồng thời Email sử dụng để đăng ký không được trùng với Email của các Account đã có trong database (nếu vi phạm sẽ hiện lên dòng **màu đỏ** thông báo):



The image shows the same 'Register' dialog box as above, but with the 'Email (*)' field filled with 'nam@gmail.com'. Below the input fields, a red error message is displayed: 'Warning: Email đã được người khác sử dụng!'. The 'Register Now' and 'Cancel' buttons are still at the bottom.

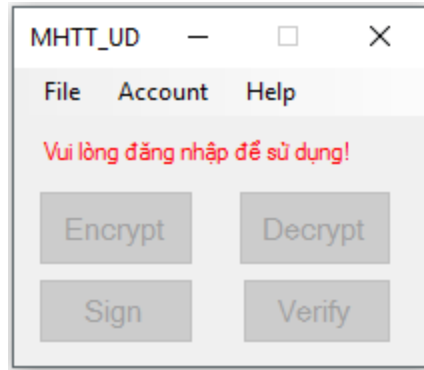
- Khi điền đầy đủ các thông tin mà không có dòng chữ đỏ hiển thị, lúc này user tiếp tục bấm **Register Now** để đăng ký tài khoản:

- Khi đăng ký thành công, tài khoản tự login vào chương trình, xuất hiện **dòng màu đỏ** hiển thị user đang dùng, các chức năng trong chương trình lúc này đã cho phép user sử dụng:

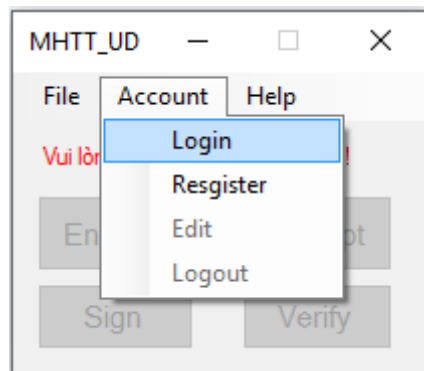


2.2. Đăng nhập

- Ban đầu chương trình chưa có user nào đăng nhập vào, nên tất cả các chức năng của chương trình đều bị khóa lại không cho sử dụng:

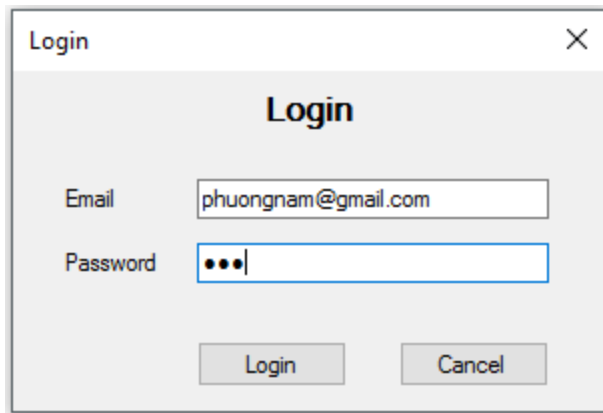


- Để đăng nhập, user chọn Account → Login:

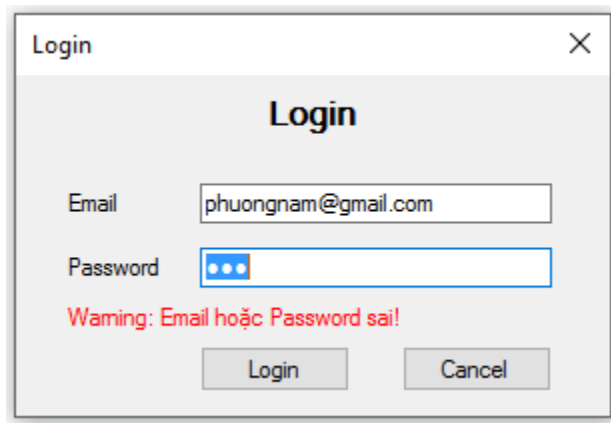


- User điền thông tin Email và Password vào khung bên dưới:

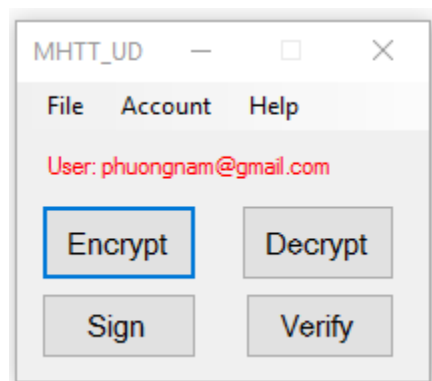
- Sau khi điền đầy đủ thông tin, user bấm **Login** để đăng nhập:



- Nếu đăng nhập không thành công thì có **dòng chữ đỏ** hiển thị thông báo và user vui lòng nhập lại thông tin chính xác:

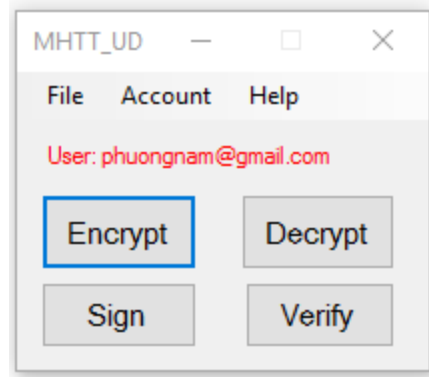


- Nếu đăng nhập thành công thì bảng **Login** biến mất và xuất hiện **dòng màu đỏ** hiển thị user đang dùng, các chức năng trong chương trình lúc này đã cho phép user sử dụng:

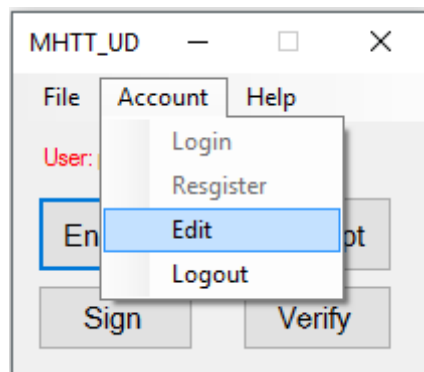


2.3. Cập nhật thông tin và passphrase

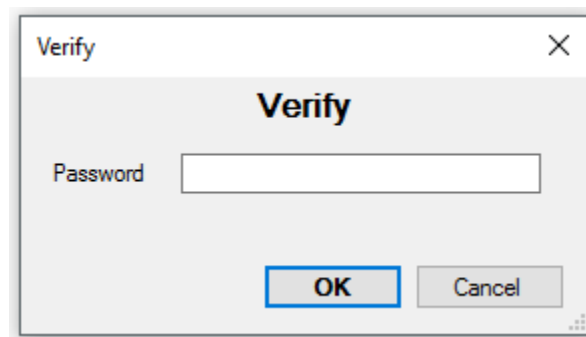
- Ban đầu user đã login thành công vào chương trình:



- Để cập nhật thông tin, user chọn user chọn Account → Edit::



- Xuất hiện yêu cầu user nhập Password để xác nhận:



- Khi user xác nhận thành công sẽ hiển thị bảng **Edit Information** để user cập nhật thông tin:

Edit Information

Full Name:

Birthday:

Phone:

Address:

☐ Change password

Old Password (*):

New Password (*):

Confirm Password (*):

Save **Cancel**

- Nếu user muốn thay đổi Password thì tích chọn vào ô Change password, sau đó điền đúng Password cũ rồi mới điền Password mới và Confirm của Password mới:

Edit Information

Full Name:

Birthday:

Phone:

Address:

☒ Change password

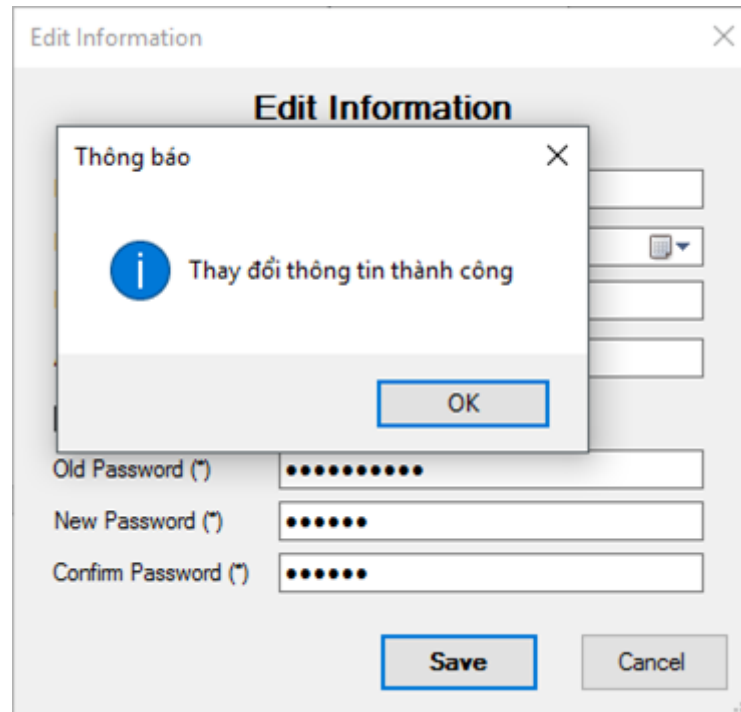
Old Password (*):

New Password (*):

Confirm Password (*):

Save **Cancel**

- Sau khi cập nhật thông tin xong, user bấm **Save** để lưu lại toàn bộ thông tin, chương trình sẽ xuất hiện thông báo thành công:



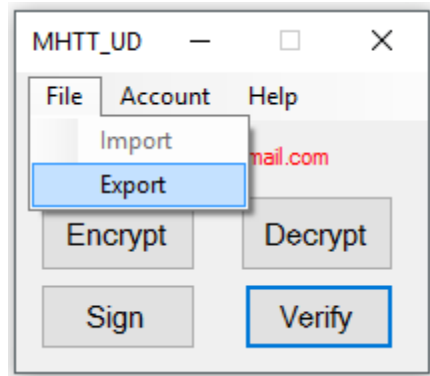
2.4. Export và import thông tin về cặp khóa

2.4.1. Export Account

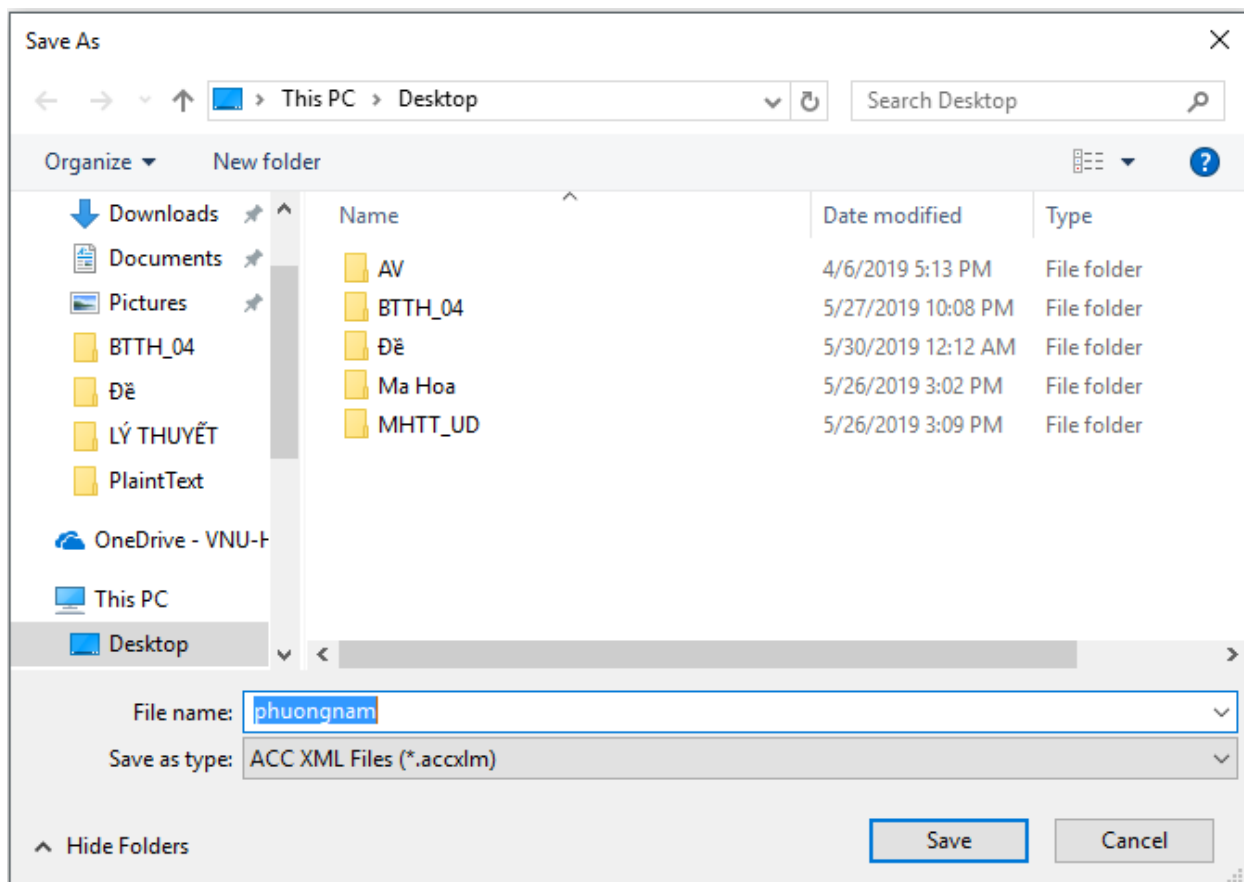
- Ban đầu user đã login thành công vào chương trình:



- Để Export Account, user chọn File → Export:

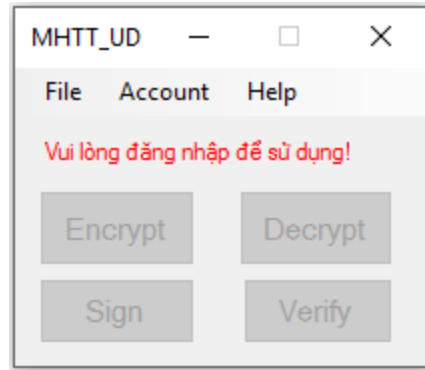


- Sau đó, chương trình hiện lên Browser Save As, user cần chọn nơi lưu trữ thích hợp và điền tên cho file export (mặc định file có đuôi accxlm), cuối cùng bấm **Save**:

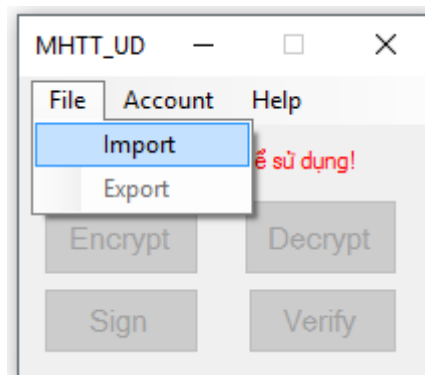


2.4.2. Import Account

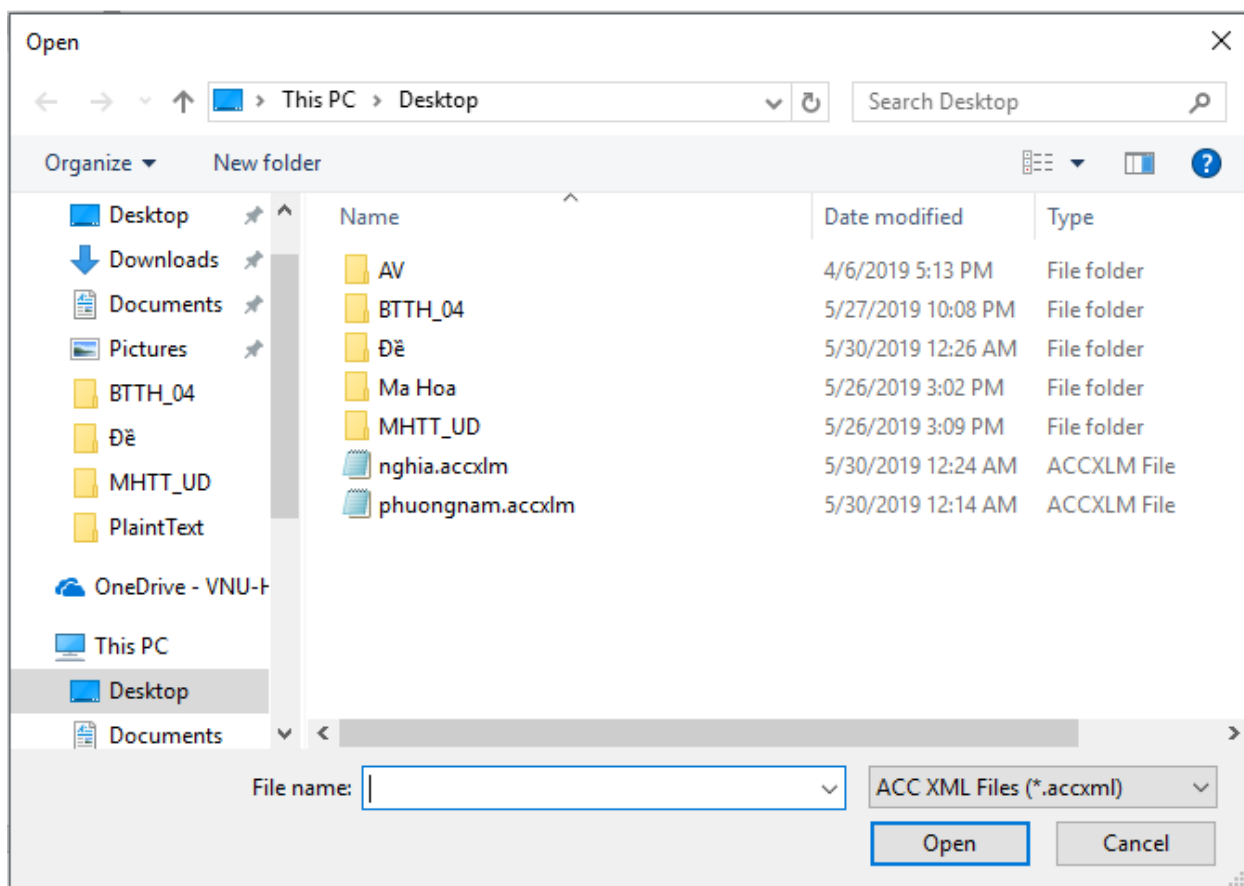
- Ban đầu chương trình chưa có user nào đăng nhập vào, nên tất cả các chức năng của chương trình đều bị khóa lại không cho sử dụng:



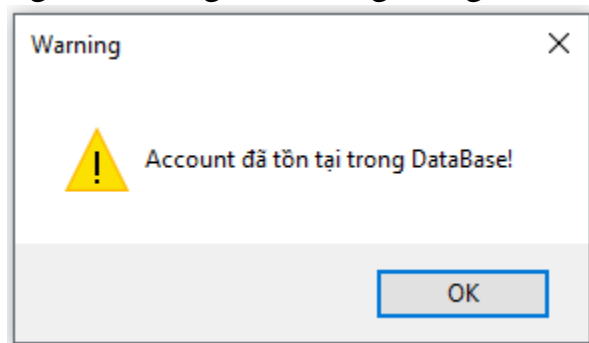
- Để Import Account, user chọn File → Import:



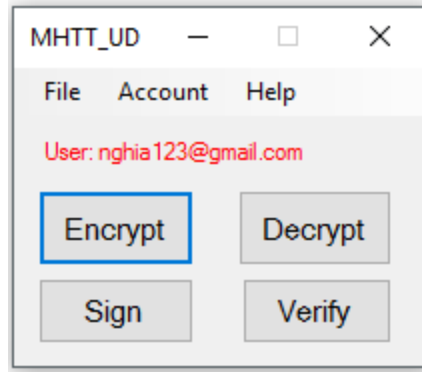
- Sau đó, chương trình hiện lên Browser Open, user cần chọn file (có đuôi .accxlm) để import vào chương trình:



- Nếu import không thành công sẽ có bảng thông báo xuất hiện:



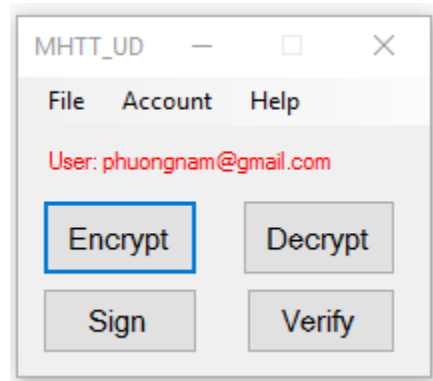
- Nếu import thành công thì chương trình tự động lấy thông tin user trong file import để login vào và giao diện chương trình sẽ như thế này:



2.5. Mã hóa và giải mã tập tin

2.5.1. Mã hóa tập tin

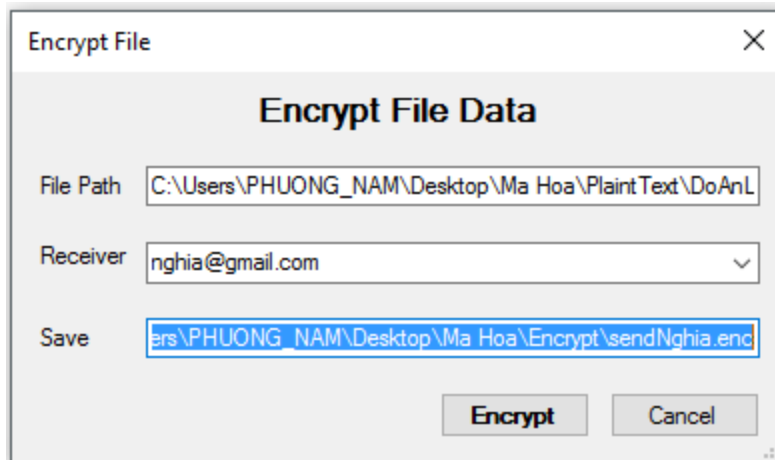
- Ban đầu user đã login thành công vào chương trình:



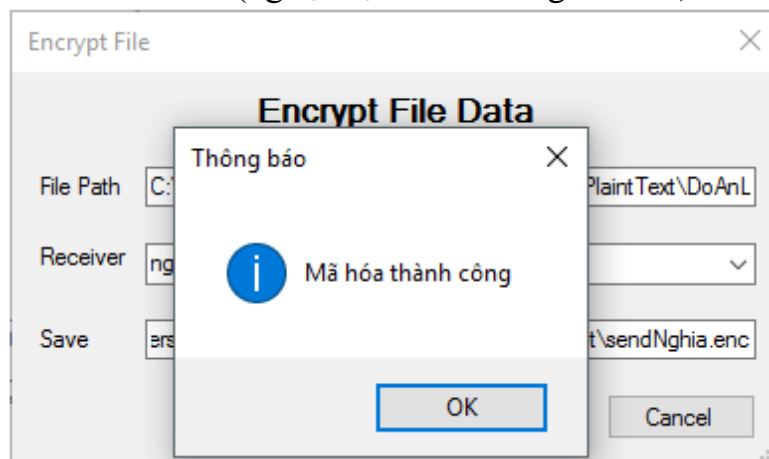
- Tiếp theo, user click vào nút **Encrypt** thì xuất hiện bảng bên dưới:

The image shows a dialog box titled 'Encrypt File' with a close button (X) in the top right corner. The main title inside the dialog is 'Encrypt File Data'. There are three input fields: 'File Path' (a text box), 'Receiver' (a dropdown menu showing 'thinh@gmail.com'), and 'Save' (a text box). At the bottom right, there are two buttons: 'Encrypt' (highlighted with a blue border) and 'Cancel'.

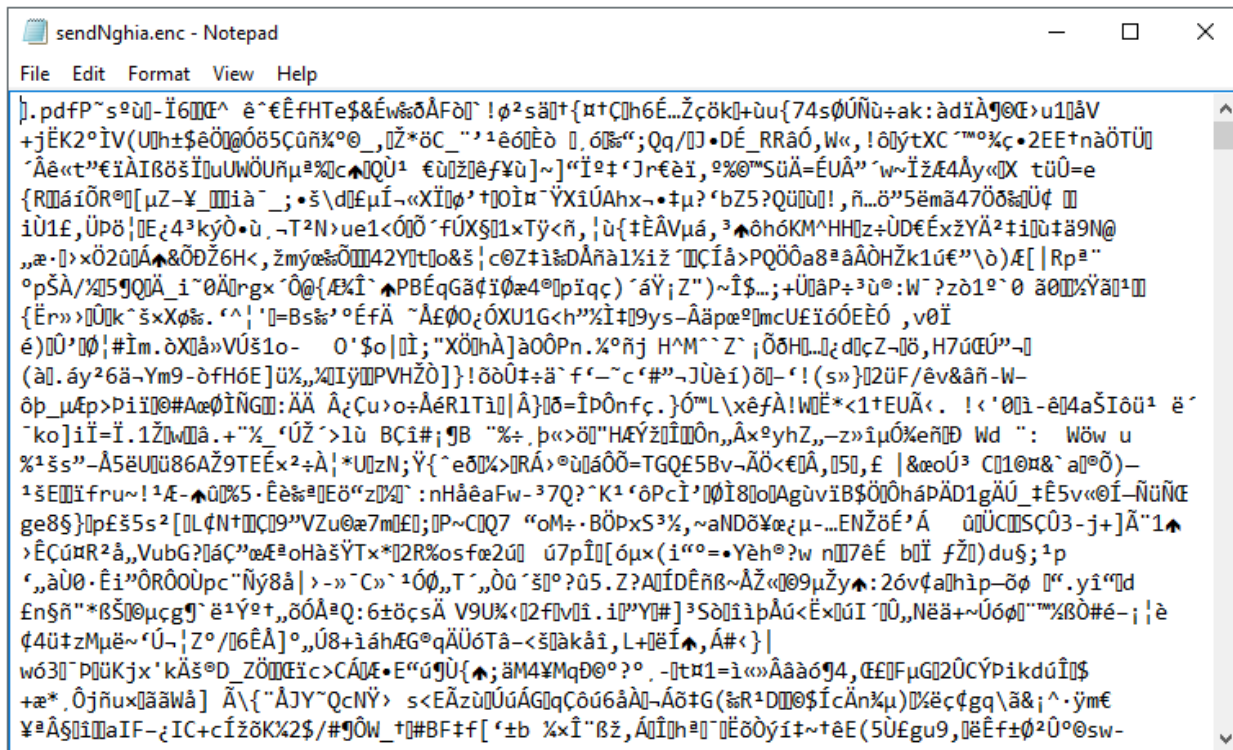
- User cần chọn tập tin cần mã hóa ở File Path, chọn người nhận ở Reciever và chọn nơi lưu tập tin mã hóa (có đuôi .enc) ở Save:



- Cuối cùng, user bấm **Encrypt** để mã hóa tập tin, nếu thành công sẽ xuất hiện thông báo như bên dưới (ngược lại sẽ có thông báo lỗi):



- Hình ảnh tập tin mã hóa thành công:

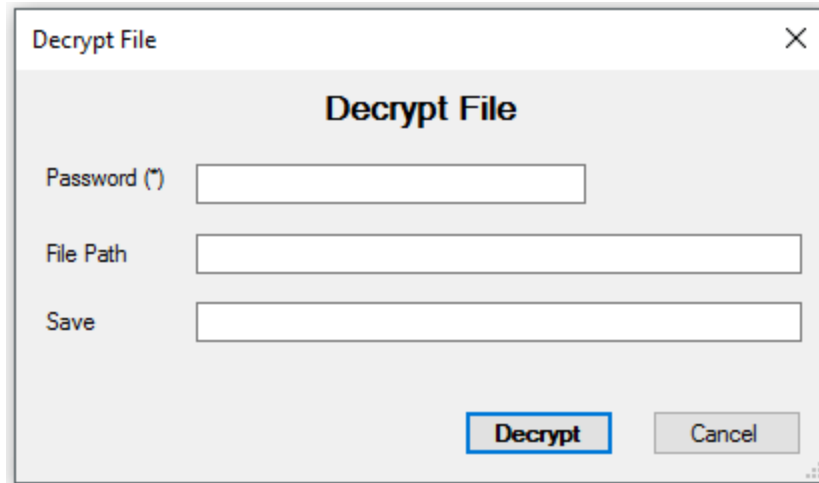


2.5.2. Giải mã tập tin

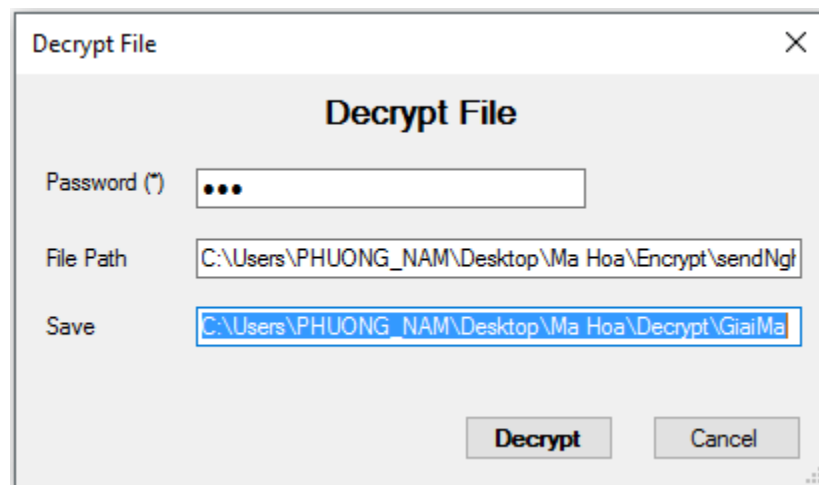
- Ban đầu user đã login thành công vào chương trình:



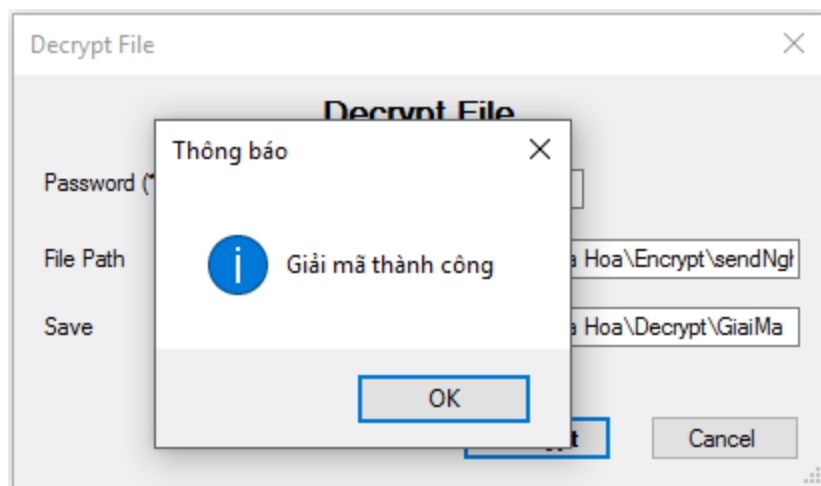
- Tiếp theo, user click vào nút **Decrypt** thì xuất hiện bảng bên dưới:



- Tiếp theo, User phải nhập chính xác Password, sau đó chọn tập tin đã mã hóa tại File Path và nơi lưu lại tập tin giải mã tại Save:



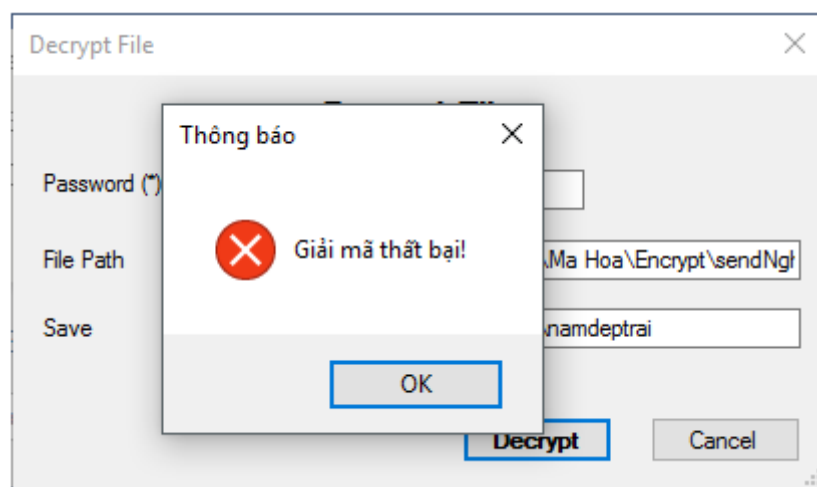
- Cuối cùng, user bấm **Decrypt** để giải mã tập tin, nếu thành công sẽ xuất hiện bảng thông báo như bên dưới:



- Tập tin giải mã thu được:



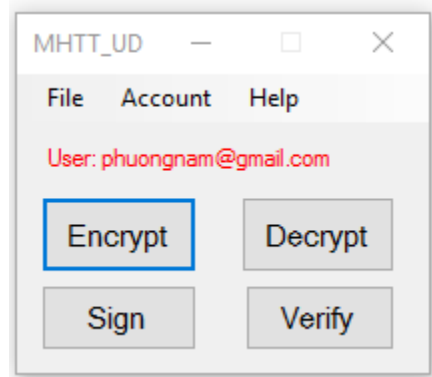
Trường hợp user không phải chủ nhân tập tin mã hóa:



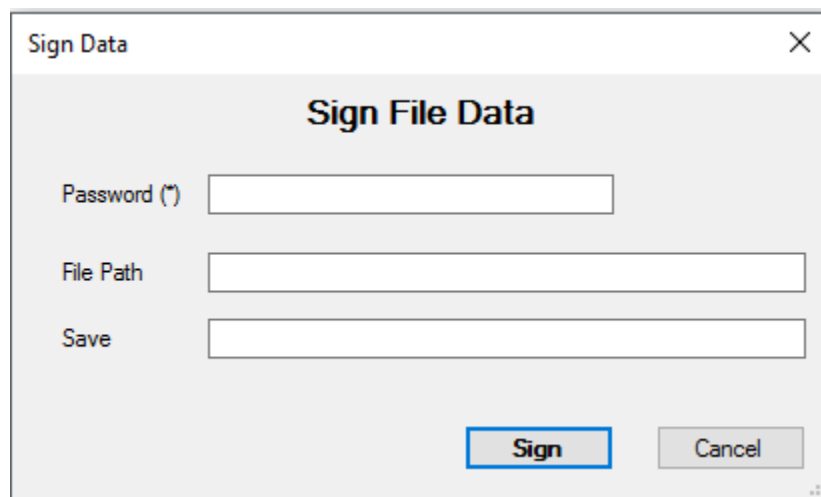
2.6. Ký và xác nhận chữ ký cho tập tin

2.6.1. Ký lên tập tin

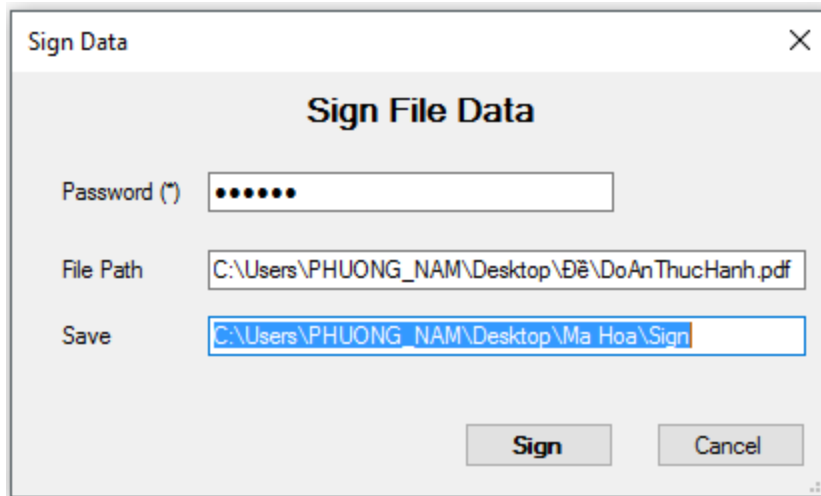
- Ban đầu user đã login thành công vào chương trình:



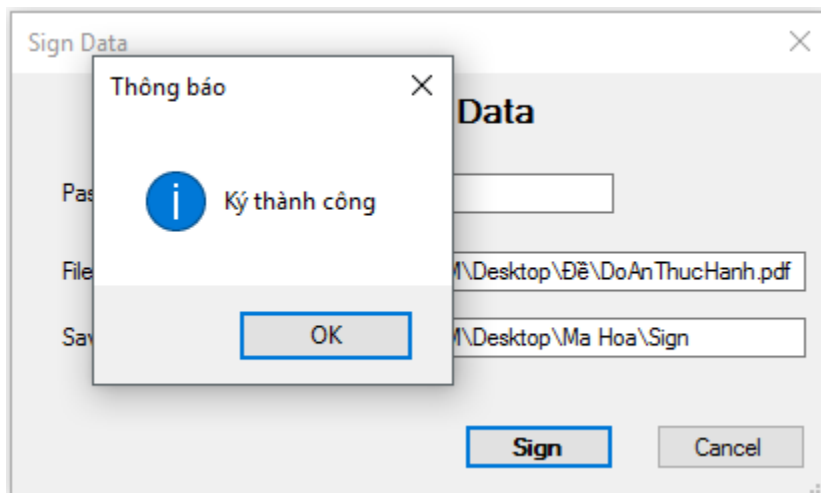
- Tiếp theo, user click vào nút **Sign** thì xuất hiện bảng bên dưới:



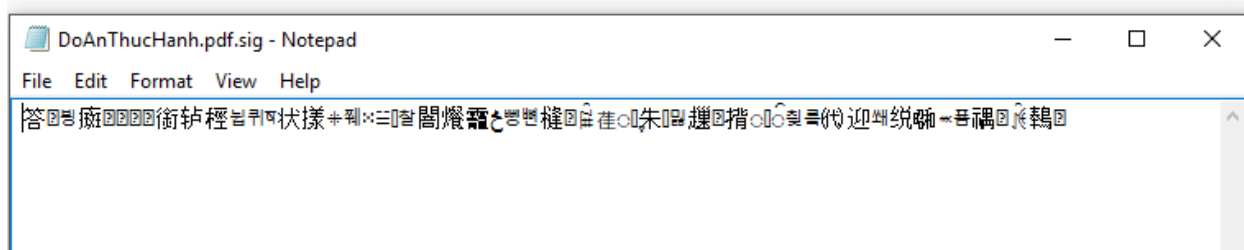
- User cần nhập đúng Password, chọn tập tin cần ký ở File Path và chọn nơi lưu tập tin ký (chữ ký) ở Save:



- Cuối cùng, user bấm **Sign** để ký lên tập tin sẽ xuất hiện thông báo như bên dưới:



- Hình ảnh chữ ký thu được:

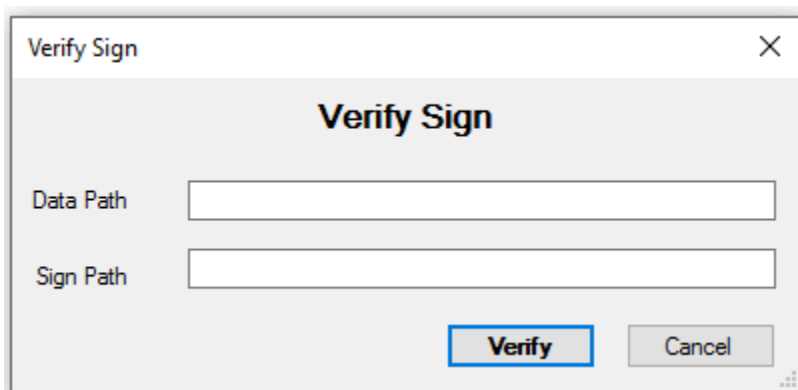


2.6.2. Xác nhận chữ ký cho tập tin

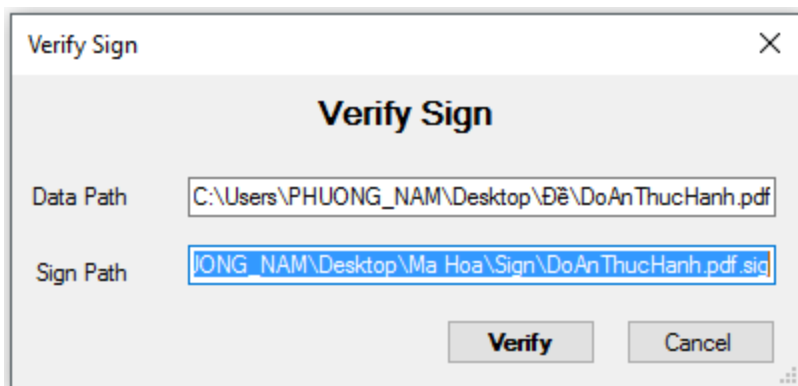
- Ban đầu user đã login thành công vào chương trình:



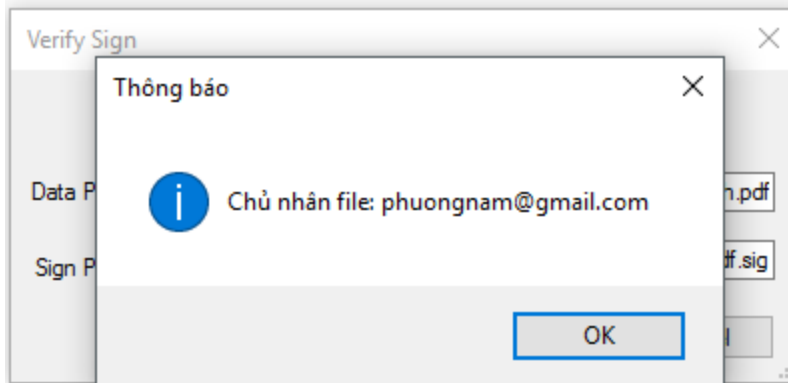
- Tiếp theo, user click vào nút **Verify** thì xuất hiện bảng bên dưới:



- User tiến hành chọn tập tin data cần xác thực ở Data Path và chữ ký cần xác thực ở Sign Path:



- Cuối cùng, user bấm Verify để xác thực nếu xác thực thành công sẽ xuất hiện thông báo bên dưới (ngược lại thông báo không thành công):



3. Vấn đề và giải pháp

3.1. Private key của user

Nhóm sinh viên tự quyết định nên sử dụng passphrase để mã hóa private key hay chỉ dùng passphrase để kiểm tra xem NSD có phải là người chủ của cặp khóa hay không. Nên được, nên có giải thích lý do phương án mình chọn trong báo cáo.

Giải pháp:

Private key là thông tin bí mật chỉ có chủ nhân của nó mới có thể xem được, kể cả admin hay bất kỳ ai cũng không xem được. Phòng khi database của chương trình bị mất đi mà không làm mất private key của các users, ta nên mã hóa private key user bằng passphrase trước khi lưu xuống database, lúc này cả passphrase cũng được bảo mật bằng cách thêm salt và hash nên lúc này có thể đảm bảo rằng việc mã hóa private key của user là đủ an toàn.

3.2. Chọn padding scheme và mode of operation

Chương trình cho phép NSD chọn padding scheme và mode of operation, hay quy định sẵn (cố định) 1 padding scheme và 1 mode of operation? Nếu cho phép NSD chọn thì làm cách nào để khi giải mã, hệ thống tự động xác định được tập tin đã được mã hóa với padding scheme và mode of operation nào?

Giải pháp:

Không, chương trình sẽ chọn 1 padding scheme và 1 mode of operation cố định. Do nếu NSD không có kiến thức về mã hóa thì 2 thông tin này có thể gây ra rắc rối cho NSD, vì thế họ thường chọn một cách ngẫu hứng mà không biết rõ chúng hoạt động như thế nào từ đó dẫn đến nguy cơ mất an toàn thông tin mã hóa.

3.3. Khóa bí mật (K_s)

Khóa bí mật (K_s) sau khi được mã hóa bằng public key của người nhận, nên được đưa vào phần nào trong tập tin dữ liệu mã hóa? Làm sao để hệ thống tự động lấy ra được thông tin này khi giải mã?

Giải pháp:

- Cấu trúc tập tin mã hóa
 - + 1 byte đầu tiên: chiều dài chuỗi chứa đuôi mở rộng của tập tin data được mã hóa (ví dụ: .pdf, .mp4, .doc, ...).
 - + Các bytes tiếp theo: nội dung chuỗi chứa đuôi mở rộng của tập tin data được mã hóa.
 - + 1 byte tiếp theo: chiều dài của khóa bí mật (K_s) đã được mã hóa bằng public key người nhận.
 - + Các bytes tiếp theo: nội dung khóa bí mật (K_s) đã được mã hóa bằng public key người nhận.
 - + Tất cả các bytes còn lại: lưu trữ nội dung tập tin đã mã hóa bằng khóa bí mật (K_s).
- Dựa vào cấu trúc tập tin mã hóa, chương trình có thể tiến hành đọc theo thứ tự trên để rút ra 3 thông tin quan trọng là: đuôi mở rộng của tập tin data, khóa bí mật (K_s) đã mã hóa và nội dung tập tin đã mã hóa. Từ đó, chương trình phía người nhận có thể dùng private key của mình giải mã lấy K_s , rồi sau đó dùng K_s để giải mã toàn bộ nội dung mã hóa (bằng một thuật toán quy ước sẵn) và cuối cùng thêm đuôi mở rộng vào tập tin giải mã.

4. Bảng tổng hợp chức năng

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

2.4	Lưu lại thông tin cập nhật	<input checked="" type="checkbox"/>	
3. Export và Import thông tin về cặp khóa			
3.1	Export cặp khóa và thông tin liên quan	<input checked="" type="checkbox"/>	
3.2	Import cặp khóa và thông tin liên quan	<input checked="" type="checkbox"/>	
4. Mã hóa tập tin			
4.1	Cho NSD chọn tập tin cần mã hóa	<input checked="" type="checkbox"/>	
4.2	Cho NSD chọn thuật toán mã hóa đối xứng	<input type="checkbox"/>	
4.3	Cho NSD chọn người nhận	<input checked="" type="checkbox"/>	
4.4	Hệ thống phát sinh khóa bí mật (K_s)	<input checked="" type="checkbox"/>	
4.5	Mã hóa nội dung tập tin (mã hóa đối xứng)	<input checked="" type="checkbox"/>	
4.6	Mã hóa khóa bí mật K_s bằng public key của người nhận	<input checked="" type="checkbox"/>	
4.7	Đưa thông tin khóa bí mật đã được mã hóa vào tập tin	<input checked="" type="checkbox"/>	
4.8	Cho NSD chọn padding mode	<input type="checkbox"/>	Không bắt buộc
4.9	Cho NSD chọn mode of operation	<input type="checkbox"/>	Không bắt buộc
4.10	Nén tập tin trước khi mã hóa	<input type="checkbox"/>	Không bắt buộc
4.11	Cho phép chọn nhiều tập tin để xử lý cùng lúc	<input type="checkbox"/>	Không bắt buộc
5. Giải mã tập tin			
5.1	Kiểm tra passphrase trước khi giải mã tập tin	<input checked="" type="checkbox"/>	
5.2	Giải mã khóa bí mật K_s bằng private key của người nhận	<input checked="" type="checkbox"/>	
5.3	Giải mã nội dung tập tin	<input checked="" type="checkbox"/>	
5.4	Giải nén tập tin (nếu đã nén khi mã hóa)	<input type="checkbox"/>	Không bắt buộc
6. Ký trên tập tin			
6.1	Kiểm tra passphrase trước khi ký	<input checked="" type="checkbox"/>	
6.2	Hash tập tin cần ký	<input checked="" type="checkbox"/>	
6.3	Tạo tập tin chữ ký	<input checked="" type="checkbox"/>	
7. Xác nhận chữ ký cho tập tin			
7.1	Hệ thống tự động duyệt qua từng public key có trong dữ liệu	<input checked="" type="checkbox"/>	Sinh viên có thể làm ở mức độ đơn giản hơn là cho NSD chọn muốn kiểm tra bằng public key của ai.
7.2	Kiểm tra chữ ký hợp lệ	<input checked="" type="checkbox"/>	
8. Các chức năng khác			
Nhóm sinh viên có thể bổ sung các chức năng đặc biệt khác chưa được liệt kê trong phần dưới đây			
	Giao diện quản lý hệ thống tập tin, thư mục	<input type="checkbox"/>	
	Plug-in vào Microsoft Word	<input type="checkbox"/>	
	Plug-in vào Microsoft Outlook	<input type="checkbox"/>	

	<i>Tự cài đặt thêm thuật toán mã hóa mới</i>	<input type="checkbox"/>	
	<i>Sử dụng thêm thư viện các thuật toán mã hóa mới</i>	<input type="checkbox"/>	
	<i>Xử lý digital certificate</i>	<input type="checkbox"/>	
	<i>Có demo</i>	<input checked="" type="checkbox"/>	
	<i>Hướng dẫn sử dụng</i>	<input checked="" type="checkbox"/>	
...		<input type="checkbox"/>	