

**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN
KHOA CÔNG NGHỆ THÔNG TIN**



**BÁI CÁO ĐỒ ÁN THỰC HÀNH 1
HỌC PHẦN: AN NINH MÁY TÍNH**

Nhóm: 22127233 – Trần Hoàng Linh

Lớp: 22MMT

Thành Phố Hồ Chí Minh, Ngày 07 Tháng 04 Năm 2025

Mục Lục

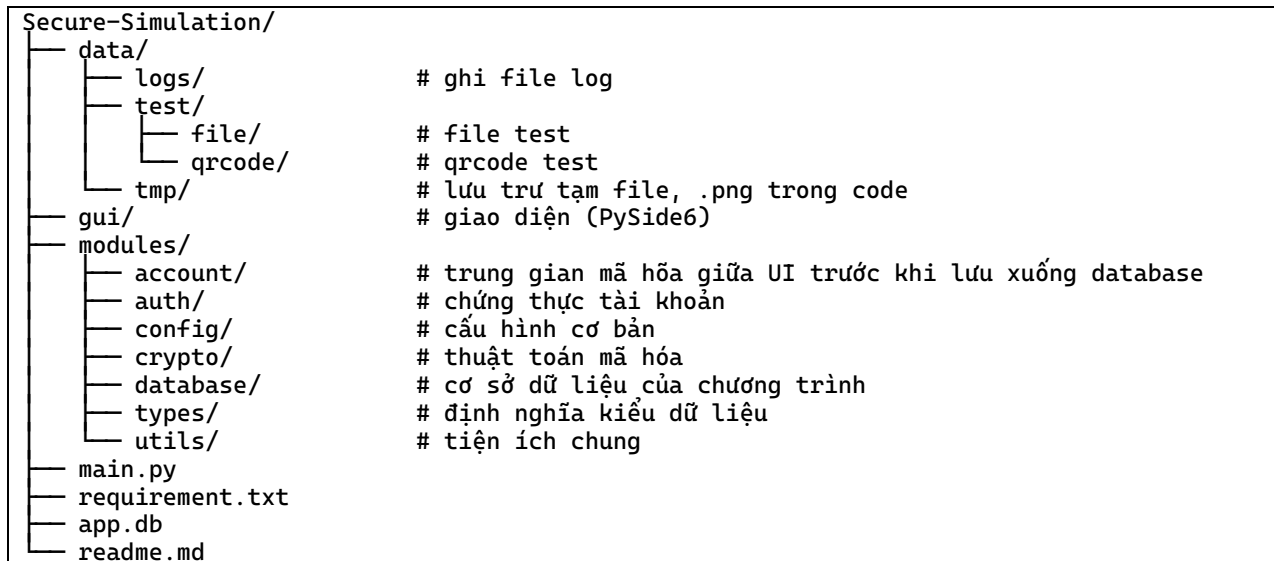
I.	Nội Dung.....	3
II.	Kiến Trúc Hệ Thống.....	4
1.	Sơ đồ modules	4
2.	Sơ đồ lưu trữ.....	4
3.	Sơ đồ UI	5
III.	Chức Năng	5
1.	Đăng ký tài khoản người dùng	5
2.	Đăng nhập & xác thực đa yếu tố (MFA).....	6
3.	Quản lý khóa RSA cá nhân.....	7
4.	QR code public key	7
5.	Cập nhật thông tin tài khoản.....	8
6.	Mã hóa tập tin gửi người khác.....	8
7.	Giải mã tập tin	10
8.	Ký số tập tin.....	10
9.	Xác minh chữ ký.....	11
10.	Phân quyền tài khoản	11
11.	Ghi Log bảo mật.....	12
12.	Chia nhỏ tập tin	12
13.	Kiểm tra trạng thái khóa.....	13
14.	Tìm kiếm public key	13
15.	Giới hạn đăng nhập	14
16.	Tùy chọn lưu định dạng lưu file.....	14
17.	Khôi phục tài khoản	15

I. Nội Dung

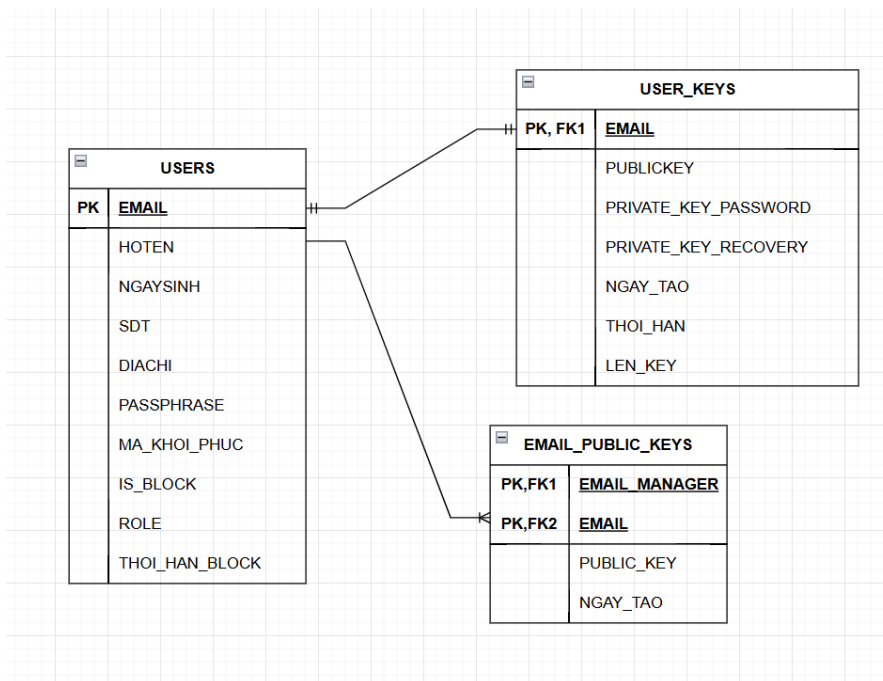
STT	Hạng Mục	Trạng Thái	Tỷ Lệ
1	Đăng ký tài khoản người dùng	Hoàn thành	100%
2	Đăng nhập & xác thực đa yếu tố (MFA)	Hoàn thành	100%
3	Quản lý khóa RSA cá nhân	Hoàn thành	100%
4	QR Code Public Key	Hoàn thành	100%
5	Cập nhật thông tin tài khoản	Hoàn thành	100%
6	Mã hóa tập tin gửi người khác	Hoàn thành	100%
7	Giải mã tập tin	Hoàn thành	100%
8	Ký số tập tin	Hoàn thành	100%
9	Xác nhận chữ ký	Hoàn thành	100%
10	Phân quyền tài khoản	Hoàn thành	100%
11	Ghi log bảo mật	Hoàn thành	100%
12	Chia nhỏ tập tin lớn	Hoàn thành	100%
13	Kiểm tra trạng thái khóa	Hoàn thành	100%
14	Tìm kiếm public key	Hoàn thành	100%
15	Giới hạn đăng nhập	Hoàn thành	100%
16	Tùy chọn định dạng lưu file	Hoàn thành	100%
17	Khôi phục tài khoản	Hoàn thành	100%

II. Kiến Trúc Hệ Thống

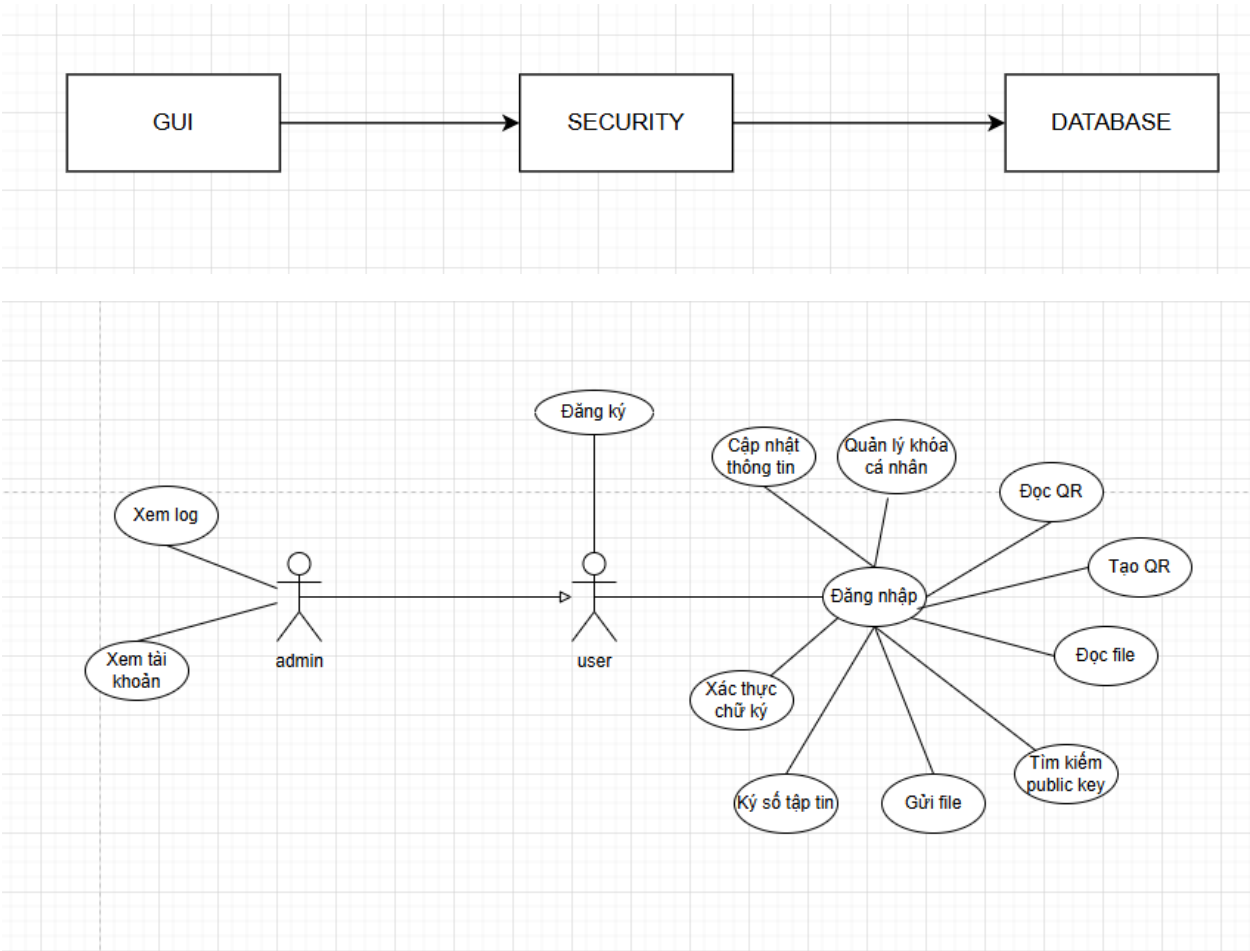
1. Sơ đồ modules



2. Sơ đồ lưu trữ



3. Sơ đồ UI



III. Chức Năng

1. Đăng ký tài khoản người dùng

Giao diện	File log
	<div>- Log hành vi:</div> <pre>data > logs > loginlog 1 2025-07-03 21:48:28,086 [INFO] - [login]: vietnamsonglai005@gmail.com - Bắt đầu đăng ký tài khoản 2 2025-07-03 21:48:28,086 [INFO] - [login]: vietnamsonglai005@gmail.com - Nguyen Van An - 3/6/2004 - 987987897 - Địa chỉ số 1 3 2025-07-03 21:48:40,531 [INFO] - [login]: vietnamsonglai005@gmail.com - Đăng ký tài khoản thành công 4</pre> <div>- Log security:</div> <pre>data > logs > securitylog 1 2025-07-03 21:48:28,086 [INFO] - [security]: vietnamsonglai005@gmail.com - Mã hóa mật khẩu bằng SHA_256 2 2025-07-03 21:48:28,087 [INFO] - [security]: vietnamsonglai005@gmail.com - Mã hóa mã khôi phục bằng SHA_256 3 2025-07-03 21:48:29,365 [INFO] - [security]: vietnamsonglai005@gmail.com - AES Mã hóa private key bằng password - thành công 4 2025-07-03 21:48:29,365 [INFO] - [security]: vietnamsonglai005@gmail.com - AES Mã hóa private key bằng mã khôi phục - thành công 5</pre>

- Bảng users trong database:

app.db

Filter 3 tables...

Rows: 1

TABLES

EMAIL_PUBLIC_KEYS

USERS

USER_KEYS

EMAIL

Filter...

HOTEN

Filter...

NGAYSINH

Filter...

SĐT

Filter...

DIACHI

Filter...

PASSPHRASE

Filter...

1

2

vietnamsonglai005@gmail.com

Nguyen Van An

3/6/2004

987987897

Dia chi so 1

NGE0MzcwOTBiZjZlZGY1NTNHNzExNjcxOGZjODVlZjVlY...

Filter 1 rows...

Upgrade to PRO

MA_KHOI_PHUC

Filter...

IS_BLOCK

Filter...

ROLE

Filter...


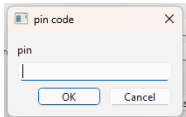
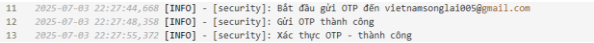

MTg0MGViMWQ2N2Y0MzllZTk4YWMyMzJlZDZlODJjMjM...

0

user

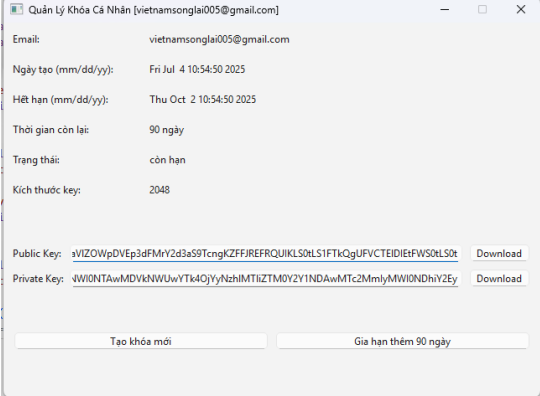
- Kỹ thuật bảo mật:
 - Passphrase có độ mạnh tối thiểu (ít nhất 8 ký tự, có chữ hoa, số, ký hiệu).
 - Dùng SHA-256 kết hợp thêm salt ngẫu nhiên để mã hóa passphrase rồi lưu xuống database
 - Xác thực passphrase bằng cách lấy salt ngẫu nhiên từ CSDL khi đăng ký lúc ban đầu, kết hợp với passphrase hiện tại và thực hiện SHA-256 lại lần nữa rồi so với hash được lưu trong CSDL

2. Đăng nhập & xác thực đa yếu tố (MFA)

	Giao diện	Log xác thực
Đăng nhập		
OTP		<p>- Quá trình gửi OTP:</p>  <p>- Nội dung sau khi gửi OTP:</p> <p>(không có chủ đề) Hộp thư đến x</p> <p> thlinh22@clc.fitus.edu.vn 22:31 Th 5, 3 thg 7 (2 ngày trước) đến ▾</p> <p>code: 1mcCE6 date: Thu Jul 3 22:31:20 2025 expired: Thu Jul 3 22:31:50 2025</p>

TOTP		<pre> 14 2025-07-03 22:28:05,314 [INFO] - [security]: Bắt đầu tạo TOTP ... 15 2025-07-03 22:28:05,467 [INFO] - [security]: Tạo QR TOTP thành công 16 2025-07-03 22:28:20,407 [INFO] - [security]: Xác thực TOTP - thành công </pre>
------	---	---

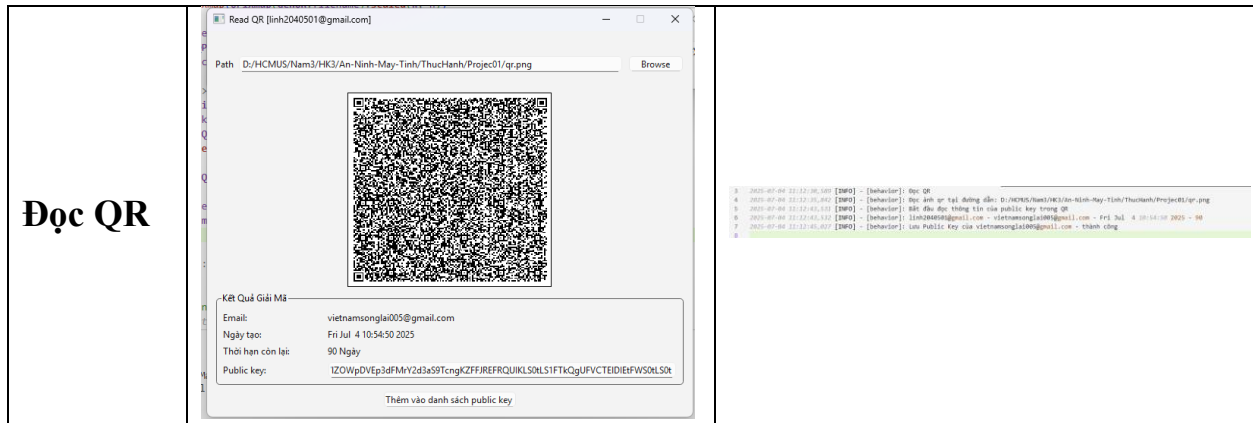
3. Quản lý khóa RSA cá nhân

Giao diện	File Log
	<p>- Log hành vi người dùng</p> <pre> data > logs > vietnamsonglai005@gmail.com > behavior.log 1 2025-07-04 10:54:36,841 [INFO] - [behavior]: xem quản lý khóa 2 2025-07-04 10:54:42,809 [INFO] - [behavior]: Gia hạn khóa thêm 90 3 2025-07-04 10:54:47,799 [INFO] - [behavior]: Nhập password 4 2025-07-04 10:54:47,799 [INFO] - [behavior]: Nhập mã khôi phục 5 2025-07-04 10:54:50,811 [INFO] - [behavior]: Tạo khóa mới thành công 6 </pre> <p>- Log security</p> <pre> 4 2025-07-04 10:54:50,774 [INFO] - [security]: vietnamsonglai005@gmail.com - RSA sinh private key vs public key - thành công 5 2025-07-04 10:54:50,790 [INFO] - [security]: vietnamsonglai005@gmail.com - AES mã hóa private key bằng password - thành công 6 2025-07-04 10:54:50,797 [INFO] - [security]: vietnamsonglai005@gmail.com - AES mã hóa private key bằng mã khôi phục - thành công 7 2025-07-04 10:54:50,811 [INFO] - [security]: vietnamsonglai005@gmail.com - Thay đổi khóa private key vs public key - thành công 8 </pre>

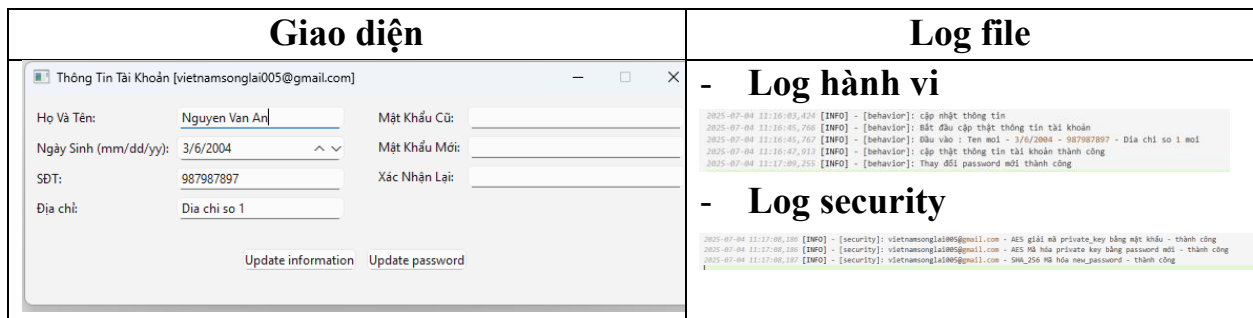
- Kỹ thuật bảo mật:
 - Tạo cặp khóa RSA (2048 bit)
 - Private Key mã hóa bằng AES sinh từ passphrase
 - Public key lưu công khai gắn với email, ngày tạo

4. QR code public key

	Giao diện	File log
Tạo QR		<pre> 2025-07-04 11:11:48,679 [INFO] - [behavior]: Tạo QR 2025-07-04 11:11:48,703 [INFO] - [behavior]: Bắt đầu tạo QR 2025-07-04 11:11:48,930 [INFO] - [behavior]: Tạo QR - thành công </pre>

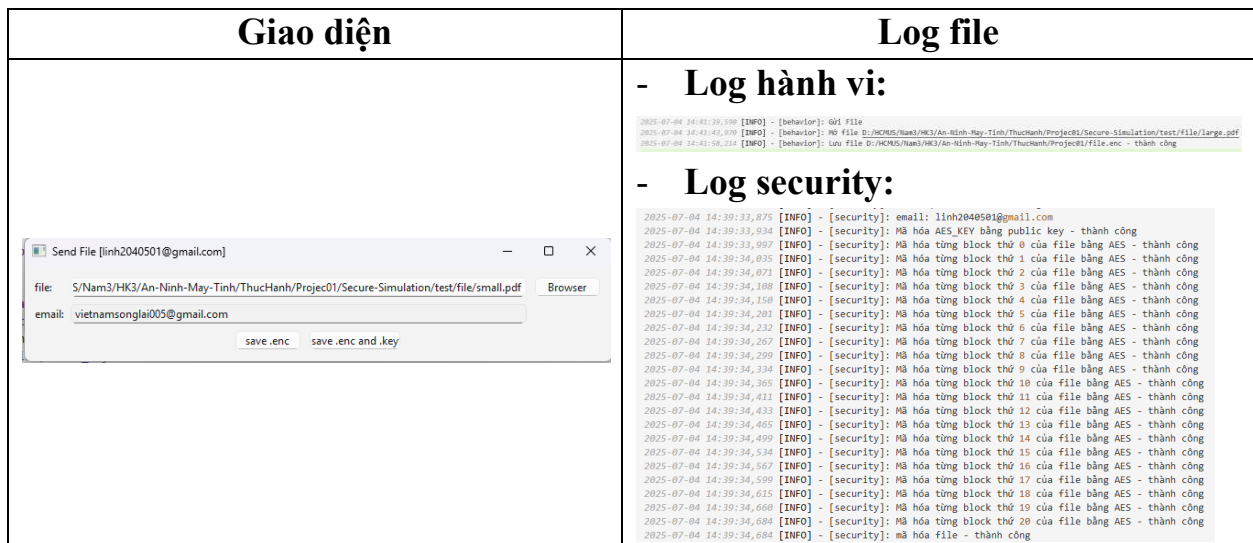


5. Cập nhật thông tin tài khoản



- Kỹ thuật bảo mật:
 - Giải mã private key bằng password cũ sau đó mã hóa private key lại bằng password mới và mã hóa password mới bằng AES rồi lưu xuống CSDL

6. Mã hóa tập tin gửi người khác



- Định dạng metadata

- Gộp file .enc

```
D: > HCMUS > Nam3 > HK3 > An-Ninh-May-Tinh > ThucHanh > Projec01 > file.enc
1 {
2   "file_enc": [
3     "1H0Z2H0RfHm5j1z2m2j53m1A5H2m1T212N29K121m2Q01W21Wj530K4m1m2W0K120QXm1T42j21m2m1jvH
4     Q0ZGE2ZTuxYjlmOWU3NTU1ND00MTE0NmRmMjYyMTA3ZTAyNWESZGIzNDU0MDNiOWQ5YzozYWRhZTYwYTI0ZTA",
5   ],
6   "key_enc": "cEnRatNKum8+lwCYPtThDBKYHK5NjNWy1YH1rRpBPuUGiNRpInum50X1CQ7LZuZmYRxBxrq10zDT5
7   R4xqecbkRukhwNmEYMY4pBguTgnf7vdtQrp5ATj+P1wjj0H06WCalmgwM4NwbFhpAxtGqwoRfvzmkXV0SG7pw1cg;
8   +DU0eUuZn2XrQb2GXdgA==",
9   "nguoai_gui": "linh2040501@gmail.com",
10  "ten_file": "small.pdf",
11  "timestamp": "2025-07-04T04:34:16.297650Z"
12 }
```

- Tách file .key

- File enc

```
D: > HCMUS > Nam3 > HK3 > An-Ninh-May-Tinh > ThucHanh > Projec0
1 {
2   "file_enc": [
3     "MzNzU4Mzc3YTU5ZDRiODJjZDozM0NlYzh0OTZhMG
4   ],
5   "nguoai_gui": "linh2040501@gmail.com",
6   "ten_file": "small.pdf",
7   "timestamp": "2025-07-04T04:37:15.765462Z"
8 }
```

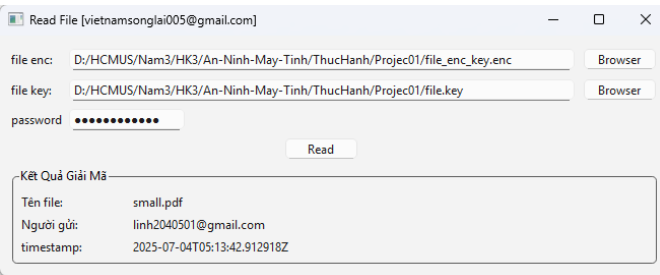
- File key

```
D: > HCMUS > Nam3 > HK3 > An-Ninh-May-Tinh > ThucHanh > Projec01 > file.key
1 {
2   "key_enc": "fINNVi3gwvw6N7GmUrFgIKP5UomjeTZJ8m2TYbIdtOwI
3 }
```

- Kỹ thuật bảo mật

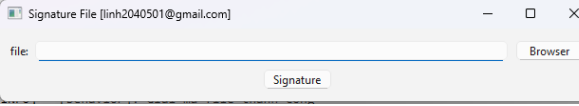
- Sinh khóa AES ngẫu nhiên
 - Mã hóa file bằng AES – GCM
 - Mã hóa khóa AES bằng RSA public key người nhận

7. Giải mã tập tin

Giao diện	Log file
	<p>- Log security</p> <pre> 2025-07-04 14:42:53,772 [INFO] - [security]: Email: vietnamsonglai005@gmail.com 2025-07-04 14:42:53,785 [INFO] - [security]: AES giải mã private key bằng password - thành công 2025-07-04 14:42:53,835 [INFO] - [security]: giải mã AES_KEY bằng private key - thành công 2025-07-04 14:42:53,902 [INFO] - [security]: giải mã block thứ 0 của file bằng AES - thành công 2025-07-04 14:42:53,967 [INFO] - [security]: giải mã block thứ 1 của file bằng AES - thành công 2025-07-04 14:42:54,019 [INFO] - [security]: giải mã block thứ 2 của file bằng AES - thành công 2025-07-04 14:42:54,085 [INFO] - [security]: giải mã block thứ 3 của file bằng AES - thành công 2025-07-04 14:42:54,135 [INFO] - [security]: giải mã block thứ 4 của file bằng AES - thành công 2025-07-04 14:42:54,205 [INFO] - [security]: giải mã block thứ 5 của file bằng AES - thành công 2025-07-04 14:42:54,252 [INFO] - [security]: giải mã block thứ 6 của file bằng AES - thành công 2025-07-04 14:42:54,330 [INFO] - [security]: giải mã block thứ 7 của file bằng AES - thành công 2025-07-04 14:42:54,385 [INFO] - [security]: giải mã block thứ 8 của file bằng AES - thành công 2025-07-04 14:42:54,452 [INFO] - [security]: giải mã block thứ 9 của file bằng AES - thành công 2025-07-04 14:42:54,518 [INFO] - [security]: giải mã block thứ 10 của file bằng AES - thành công 2025-07-04 14:42:54,594 [INFO] - [security]: giải mã block thứ 11 của file bằng AES - thành công 2025-07-04 14:42:54,669 [INFO] - [security]: giải mã block thứ 12 của file bằng AES - thành công 2025-07-04 14:42:54,740 [INFO] - [security]: giải mã block thứ 13 của file bằng AES - thành công 2025-07-04 14:42:54,806 [INFO] - [security]: giải mã block thứ 14 của file bằng AES - thành công 2025-07-04 14:42:54,873 [INFO] - [security]: giải mã block thứ 15 của file bằng AES - thành công 2025-07-04 14:42:54,934 [INFO] - [security]: giải mã block thứ 16 của file bằng AES - thành công 2025-07-04 14:42:54,985 [INFO] - [security]: giải mã block thứ 17 của file bằng AES - thành công 2025-07-04 14:42:55,051 [INFO] - [security]: giải mã block thứ 18 của file bằng AES - thành công 2025-07-04 14:42:55,118 [INFO] - [security]: giải mã block thứ 19 của file bằng AES - thành công 2025-07-04 14:42:55,184 [INFO] - [security]: giải mã block thứ 20 của file bằng AES - thành công 2025-07-04 14:42:55,250 [INFO] - [behavior]: Giải mã file thành công </pre> <p>- Log hành vi</p> <pre> 2025-07-04 14:42:01,100 [INFO] - [behavior]: Đọc file được gửi 2025-07-04 14:42:46,990 [INFO] - [behavior]: Mã file enc: D:\HCMUS\Nam3\HK3\An-Ninh-May-Tinh\ThucHanh\Projec01\file_enc 2025-07-04 14:42:51,230 [INFO] - [behavior]: tên file: large.pdf 2025-07-04 14:42:55,250 [INFO] - [behavior]: Người gửi: linh2040501@gmail.com 2025-07-04 14:42:55,250 [INFO] - [behavior]: timestamp: 2025-07-04T05:13:42.912918Z </pre>

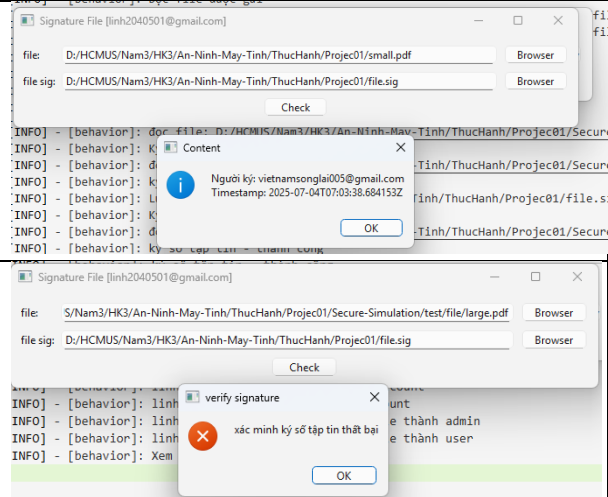
- Kỹ thuật bảo mật
 - Giải mã private key bằng password
 - Dùng private key giải mã được để giải mã khóa AES
 - Dùng khóa AES giải mã file
- So sánh nội dung trước/ sau mã hóa:
 - Trước mã hóa file chứa bytes rõ của 1 file
 - Nhưng sau mã hóa file mã hóa lớn hơn file gốc vì có chứa thêm AES key và những nội dung được thêm vào nhằm giúp dễ đọc dễ nhận diện file.

8. Ký số tập tin

Giao diện	Log file
	<p>- Log hành vi:</p> <pre> 2025-07-04 13:56:50,383 [INFO] - [behavior]: Ký file 2025-07-04 13:57:03,120 [INFO] - [behavior]: Đọc file: D:\HCMUS\Nam3\HK3\An-Ninh-May-Tinh\ThucHanh\Projec01\Secure-Simulation\test\file\small.pdf 2025-07-04 13:57:36,134 [INFO] - [behavior]: ký số tập tin - thành công </pre> <p>- Log security:</p> <pre> 2025-07-04 14:03:34,350 [INFO] - [security]: vietnamsonglai005@gmail.com - AES giải mã private key bằng password - thành công </pre>

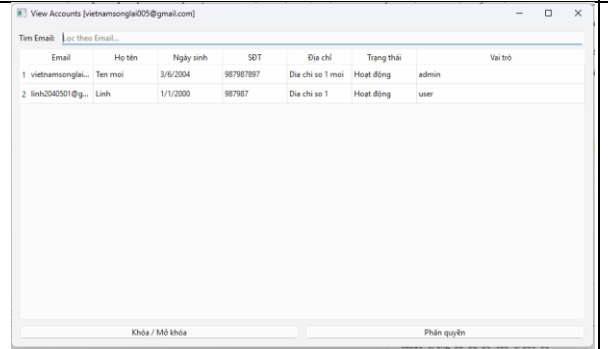
- Kỹ thuật bảo mật:
 - Băm file bằng SHA-256
 - Ký file bằng private key được giải mã bằng password

9. Xác minh chữ ký

Giao diện	Log file
	<pre>2025-07-04 14:04:26,800 [INFO] - [behavior]: xác thực chữ ký 2025-07-04 14:04:27,800 [INFO] - [behavior]: NO file D:\HCMUS\Nam3\HK3\An-Ninh-May-Tinh\ThucHanh\Projec01\file.sig 2025-07-04 14:04:27,800 [INFO] - [behavior]: NO file D:\HCMUS\Nam3\HK3\An-Ninh-May-Tinh\ThucHanh\Projec01\small.pdf 2025-07-04 14:04:29,800 [INFO] - [behavior]: Người ký: vietnamsonglai005@gmail.com - Thời gian: 2025-07-04T07:03:38.684153Z - Xác minh chữ ký thành công 2025-07-04 14:19:12,800 [INFO] - [behavior]: xác thực chữ ký 2025-07-04 14:19:17,800 [INFO] - [behavior]: NO file D:\HCMUS\Nam3\HK3\An-Ninh-May-Tinh\ThucHanh\Projec01\Secure-Simulation\test\file\large.pdf 2025-07-04 14:19:23,800 [INFO] - [behavior]: NO file D:\HCMUS\Nam3\HK3\An-Ninh-May-Tinh\ThucHanh\Projec01\file.sig 2025-07-04 14:19:56,990 [INFO] - [behavior]: Xác minh chữ ký thất bại</pre>

- Kỹ thuật bảo mật:
 - Xác thực chữ ký bằng public key đã lưu

10. Phân quyền tài khoản

Giao diện	Log file
	<pre>2025-07-04 14:15:48,536 [INFO] - [behavior]: Xem các tài khoản trong hệ thống 2025-07-04 14:15:54,024 [INFO] - [behavior]: linh2040501@gmail.com - Unblock account 2025-07-04 14:15:54,439 [INFO] - [behavior]: linh2040501@gmail.com - block account 2025-07-04 14:15:55,729 [INFO] - [behavior]: linh2040501@gmail.com thay đổi role thành admin 2025-07-04 14:15:56,099 [INFO] - [behavior]: linh2040501@gmail.com thay đổi role thành user 2025-07-04 14:17:23,355 [INFO] - [behavior]: Xem các tài khoản trong hệ thống 2025-07-04 14:24:24,767 [INFO] - [behavior]: Xem log hệ thống 2025-07-04 14:24:26,310 [INFO] - [behavior]: Xem log: login.log 2025-07-04 14:24:29,021 [INFO] - [behavior]: Xem log: security.log 2025-07-04 14:24:32,974 [INFO] - [behavior]: Xem log: linh2040501@gmail.com\behavior.log 2025-07-04 14:24:35,314 [INFO] - [behavior]: Xem log: vietnamsonglai005@gmail.com\behavior.log 2025-07-04 14:24:40,777 [INFO] - [behavior]: Xem log: linh2040501@gmail.com\behavior.log 2025-07-04 14:24:45,236 [INFO] - [behavior]: Xem log: vietnamsonglai005@gmail.com\behavior.log</pre>

11. Ghi Log bảo mật

```
2025-07-05 21:43:15,707 [INFO] - [security]: vietnamsonglai005@gmail.com - Mã hóa mật khẩu bằng SHA_256
2025-07-05 21:43:15,707 [INFO] - [security]: vietnamsonglai005@gmail.com - Mã hóa mã khôi phục bằng SHA_256
2025-07-05 21:43:15,884 [INFO] - [security]: vietnamsonglai005@gmail.com - RSA sinh private key vs public key - thành công
2025-07-05 21:43:15,901 [INFO] - [security]: vietnamsonglai005@gmail.com - AES Mã hóa private key bằng password - thành công
2025-07-05 21:43:15,902 [INFO] - [security]: vietnamsonglai005@gmail.com - AES Mã hóa private key bằng mã khôi phục - thành công
2025-07-05 21:43:24,320 [INFO] - [security]: Bắt đầu tạo TOTP ...
2025-07-05 21:43:24,455 [INFO] - [security]: Tạo QR TOTP thành công
2025-07-05 21:43:27,972 [INFO] - [security]: Xác thực TOTP - thành công
2025-07-05 21:43:53,507 [INFO] - [security]: vietnamsonglai005@gmail.com - AES giải mã private_key bằng mật khẩu - thành công
2025-07-05 21:43:53,507 [INFO] - [security]: vietnamsonglai005@gmail.com - AES Mã hóa private key bằng password mới - thành công
2025-07-05 21:43:53,509 [INFO] - [security]: vietnamsonglai005@gmail.com - SHA_256 Mã hóa new_password - thành công
2025-07-05 21:44:19,907 [INFO] - [security]: vietnamsonglai005@gmail.com - AES giải mã private_key bằng mật khẩu - thành công
2025-07-05 21:44:19,907 [INFO] - [security]: vietnamsonglai005@gmail.com - AES Mã hóa private key bằng password mới - thành công
2025-07-05 21:44:19,908 [INFO] - [security]: vietnamsonglai005@gmail.com - SHA_256 Mã hóa new_password - thành công
2025-07-05 21:44:51,693 [INFO] - [security]: vietnamsonglai005@gmail.com - RSA sinh private key vs public key - thành công
2025-07-05 21:44:51,694 [INFO] - [security]: vietnamsonglai005@gmail.com - AES Mã hóa private key bằng password - thành công
2025-07-05 21:44:51,694 [INFO] - [security]: vietnamsonglai005@gmail.com - AES Mã hóa private key bằng mã khôi phục - thành công
2025-07-05 21:44:51,699 [INFO] - [security]: vietnamsonglai005@gmail.com - Thay đổi khóa private key vs public key - thành công
```

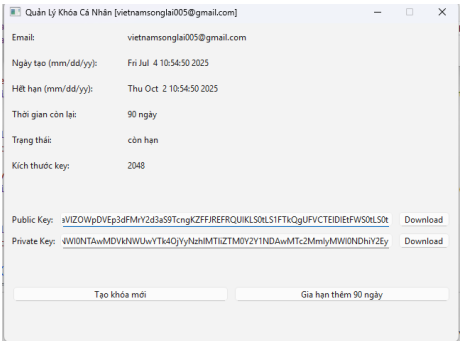
12. Chia nhỏ tập tin

- Log tiến trình

```
2025-07-04 14:41:50,097 [INFO] - [security]: email: linh2040501@gmail.com
2025-07-04 14:41:50,144 [INFO] - [security]: Mã hóa AES_KEY bằng public key - thành công
2025-07-04 14:41:50,204 [INFO] - [security]: Mã hóa từng block thứ 0 của file bằng AES - thành công
2025-07-04 14:41:50,249 [INFO] - [security]: Mã hóa từng block thứ 1 của file bằng AES - thành công
2025-07-04 14:41:50,287 [INFO] - [security]: Mã hóa từng block thứ 2 của file bằng AES - thành công
2025-07-04 14:41:50,333 [INFO] - [security]: Mã hóa từng block thứ 3 của file bằng AES - thành công
2025-07-04 14:41:50,370 [INFO] - [security]: Mã hóa từng block thứ 4 của file bằng AES - thành công
2025-07-04 14:41:50,416 [INFO] - [security]: Mã hóa từng block thứ 5 của file bằng AES - thành công
2025-07-04 14:41:50,452 [INFO] - [security]: Mã hóa từng block thứ 6 của file bằng AES - thành công
2025-07-04 14:41:50,482 [INFO] - [security]: Mã hóa từng block thứ 7 của file bằng AES - thành công
2025-07-04 14:41:50,516 [INFO] - [security]: Mã hóa từng block thứ 8 của file bằng AES - thành công
2025-07-04 14:41:50,549 [INFO] - [security]: Mã hóa từng block thứ 9 của file bằng AES - thành công
2025-07-04 14:41:50,583 [INFO] - [security]: Mã hóa từng block thứ 10 của file bằng AES - thành công
2025-07-04 14:41:50,599 [INFO] - [security]: Mã hóa từng block thứ 11 của file bằng AES - thành công
2025-07-04 14:41:50,642 [INFO] - [security]: Mã hóa từng block thứ 12 của file bằng AES - thành công
2025-07-04 14:41:50,666 [INFO] - [security]: Mã hóa từng block thứ 13 của file bằng AES - thành công
2025-07-04 14:41:50,699 [INFO] - [security]: Mã hóa từng block thứ 14 của file bằng AES - thành công
2025-07-04 14:41:50,733 [INFO] - [security]: Mã hóa từng block thứ 15 của file bằng AES - thành công
2025-07-04 14:41:50,765 [INFO] - [security]: Mã hóa từng block thứ 16 của file bằng AES - thành công
2025-07-04 14:41:50,782 [INFO] - [security]: Mã hóa từng block thứ 17 của file bằng AES - thành công
2025-07-04 14:41:50,823 [INFO] - [security]: Mã hóa từng block thứ 18 của file bằng AES - thành công
2025-07-04 14:41:50,849 [INFO] - [security]: Mã hóa từng block thứ 19 của file bằng AES - thành công
2025-07-04 14:41:50,882 [INFO] - [security]: Mã hóa từng block thứ 20 của file bằng AES - thành công
2025-07-04 14:41:50,882 [INFO] - [security]: mã hóa file - thành công
```

- So sánh dung lượng, block đã mã hóa:
 - Dung lượng sau mã hóa lớn hơn file gốc rất nhiều
 - Mỗi block được chia nhỏ ra từ file nên khi giải mã file liên tục được giải mã/mã hóa nhiều lần.

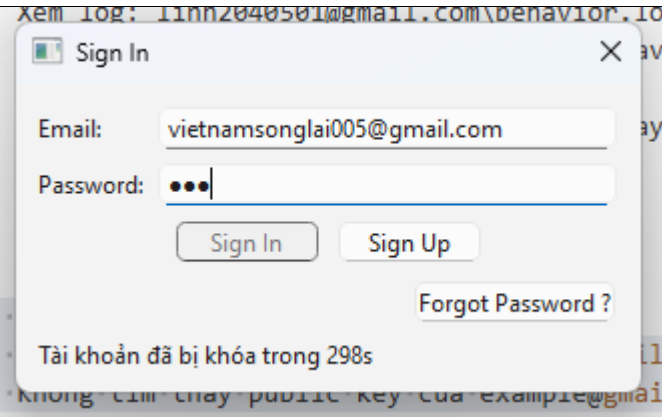
13. Kiểm tra trạng thái khóa



14. Tìm kiếm public key

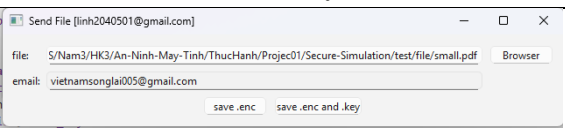
Giao diện	Log file
<p>Search Public Key [linh2040501@gmail.com]</p> <p>Email: <input type="text" value="vietnamsonglai005@gmail.com"/> Search</p> <p>Kết Quả</p> <p>Email: vietnamsonglai005@gmail.com</p> <p>Ngày tạo: Fri Jul 4 10:54:50 2025</p> <p>Thời hạn còn lại: 90 Ngày</p> <p>Public key: <code>IZOWpDVEp3dFMrY2d3aS9TcngKZFFJREFRQUIKLS0tLS1FTkQgUFVCTEIDIEtFWS0tLS0t</code></p>	<pre> 177 2025-07-04 14:59:15,937 [INFO] - [behavior]: Tìm kiếm Public Key 178 2025-07-04 14:59:21,171 [INFO] - [behavior]: Tìm Public key của vietnamsonglai005@gmail.com 179 2025-07-04 14:59:30,358 [INFO] - [behavior]: Không tìm thấy public key của example@gmail.com </pre>

15. Giới hạn đăng nhập

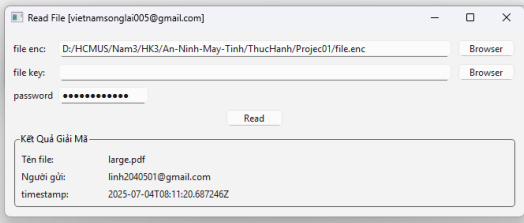
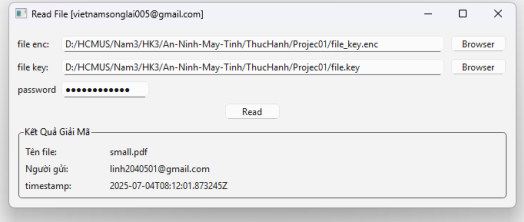
Giao diện	Log file
	<pre>2025-07-04 15:05:51,914 [WARNING] - [login]: vietnamsonglai005@gmail.com - 50 lần nhập sai mật khẩu: 1 2025-07-04 15:05:52,293 [WARNING] - [login]: vietnamsonglai005@gmail.com - 50 lần nhập sai mật khẩu: 2 2025-07-04 15:05:52,687 [WARNING] - [login]: vietnamsonglai005@gmail.com - 50 lần nhập sai mật khẩu: 3 2025-07-04 15:05:53,077 [WARNING] - [login]: vietnamsonglai005@gmail.com - 50 lần nhập sai mật khẩu: 4 2025-07-04 15:05:53,467 [WARNING] - [login]: vietnamsonglai005@gmail.com - 50 lần nhập sai mật khẩu: 5 2025-07-04 15:05:53,467 [INFO] - [login]: vietnamsonglai005@gmail.com - Lock tài khoản trong 5 phút</pre>

16. Tùy chọn lưu định dạng lưu file

- Mã hóa

Giao diện	Log file
	<pre>2025-07-04 15:10:40,458 [INFO] - [behavior]: Gõ file 2025-07-04 15:10:52,500 [INFO] - [behavior]: Hở file D:\HCMUS\Nam3\HK3\An-Ninh-May-Tinh\ThucHanh\Projec01\Secure-Simulation\test\file\small.pdf 2025-07-04 15:11:01,860 [INFO] - [behavior]: Hở file D:\HCMUS\Nam3\HK3\An-Ninh-May-Tinh\ThucHanh\Projec01\Secure-Simulation\test\file\large.pdf 2025-07-04 15:11:10,922 [INFO] - [behavior]: Lưu file D:\HCMUS\Nam3\HK3\An-Ninh-May-Tinh\ThucHanh\Projec01\file.enc - thành công 2025-07-04 15:11:20,780 [INFO] - [behavior]: Lưu file D:\HCMUS\Nam3\HK3\An-Ninh-May-Tinh\ThucHanh\Projec01\file.enc - thành công 2025-07-04 15:11:46,208 [INFO] - [behavior]: Gõ file 2025-07-04 15:11:51,490 [INFO] - [behavior]: Hở file D:\HCMUS\Nam3\HK3\An-Ninh-May-Tinh\ThucHanh\Projec01\small.pdf 2025-07-04 15:12:06,180 [INFO] - [behavior]: Lưu file D:\HCMUS\Nam3\HK3\An-Ninh-May-Tinh\ThucHanh\Projec01\file.key.enc - thành công 2025-07-04 15:12:16,858 [INFO] - [behavior]: Lưu file D:\HCMUS\Nam3\HK3\An-Ninh-May-Tinh\ThucHanh\Projec01\file.key - thành công</pre>

- Giải mã

	Giao diện	Log file
.enc		<pre>2025-07-04 15:13:17,290 [INFO] - [behavior]: Hở file enc: D:\HCMUS\Nam3\HK3\An-Ninh-May-Tinh\ThucHanh\Projec01\file.enc 2025-07-04 15:13:25,500 [INFO] - [behavior]: tên file: large.pdf 2025-07-04 15:13:25,500 [INFO] - [behavior]: Người gửi: linh2040501@gmail.com 2025-07-04 15:13:25,500 [INFO] - [behavior]: timestamp: 2025-07-04T08:11:20.687246Z</pre>
.enc vs .key		<pre>2025-07-04 15:14:00,430 [INFO] - [behavior]: Hở file enc: D:\HCMUS\Nam3\HK3\An-Ninh-May-Tinh\ThucHanh\Projec01\file.key.enc 2025-07-04 15:14:12,093 [INFO] - [behavior]: Hở file key: D:\HCMUS\Nam3\HK3\An-Ninh-May-Tinh\ThucHanh\Projec01\file.key 2025-07-04 15:14:14,193 [INFO] - [behavior]: tên file: small.pdf 2025-07-04 15:14:14,193 [INFO] - [behavior]: Người gửi: linh2040501@gmail.com 2025-07-04 15:14:14,193 [INFO] - [behavior]: timestamp: 2025-07-04T08:12:01.873245Z</pre>

17. Khôi phục tài khoản

Security.log	<div>2025-07-04 15:22:43,026 [INFO] - [security]: vietnamsonglai005@gmail.com - AES giải mã private_key bằng mã khôi phục - thành công</div> <div>2025-07-04 15:22:43,026 [INFO] - [security]: vietnamsonglai005@gmail.com - AES Mã hóa private key bằng password mới - thành công</div> <div>2025-07-04 15:22:43,026 [INFO] - [security]: vietnamsonglai005@gmail.com - SHA_256 Mã hóa new_password - thành công</div>
Login.log	<div>2025-07-04 15:22:43,033 [INFO] - [login]: vietnamsonglai005@gmail.com - Thay đổi password mới thành công</div>