

Trường Đại học Khoa học Tự Nhiên - VNUHCM

Khoa Công nghệ Thông tin

---o0o---



Báo cáo đồ án

Bộ môn : An ninh máy tính
GVHD : Phan Quốc Kỳ
Lê Hà Minh
Lê Giang Thanh
Lớp : 22MMT
Sinh viên : Nguyễn Tấn Hoàng – 22127129
Lê Nguyễn Minh Châu – 22127042
Võ Minh Khôi - 22127213

Tp. Hồ Chí Minh, Tháng 7 năm 2025

Mục lục

Mục lục	2
Giới thiệu	Error! Bookmark not defined.
Danh sách thành viên.....	3
Chi tiết các tính năng.....	3
1. Đăng ký tài khoản người dùng	6
2. Đăng nhập & xác thực đa yếu tố (MFA):.....	9
3. Quản lý khóa RSA cá nhân:	12
4. QR Code Public Key	14
5. Cập nhật thông tin tài khoản:.....	15
6. Mã hoá tập tin gửi người khác	18
7. Giải mã tập tin.....	20
8. Ký số tập tin:	20
9. Xác minh chữ ký.....	23
10. Phân quyền tài khoản:.....	25
11. Ghi log bảo mật:.....	27
12. Chia nhỏ tập tin lớn:	28
13. Hiển thị trạng thái khóa:	29
14. Tìm kiếm public key	30
15. Giới hạn đăng nhập:.....	32
16. Tùy chọn định dạng lưu file:.....	33
17. Khôi phục tài khoản:	35
Bảng phân công công việc:	Error! Bookmark not defined.

1. Thông tin

1. Giới thiệu đề án

- Đề án này nhằm xây dựng một ứng dụng mô phỏng hệ thống bảo mật dựa trên các mô hình thực tế, cho phép người dùng thực hiện các thao tác bảo mật phổ biến như: đăng ký tài khoản, tạo và quản lý khóa RSA, mã hóa và ký số tập tin, xác thực đa yếu tố, phân quyền tài khoản và một số tính năng khác.
- Sản phẩm cuối cùng là một ứng dụng có khả năng mô phỏng đầy đủ quy trình bảo mật người dùng trong môi trường thực tế, cùng với báo cáo tổng kết và demo vận hành.

2. Danh sách thành viên

STT	Thành Viên	MSSV	Email
1	Võ Minh Khôi	22127213	Vmkhoe22@clc.fitus.edu.vn
2	Nguyễn Tấn Hoàng	22127129	Nthoang22@clc.fitus.edu.vn
3	Lê Nguyễn Minh Châu	22127042	Lnmchau22@clc.fitus.edu.vn

- Video demo:

3. Bảng phân công công việc

STT	Hạng mục	Nội dung & tiêu chí đánh giá chi tiết	Phân công	Hoàn thành	Điểm
1	Đăng ký tài khoản người dùng	Nhập thông tin, lưu passphrase SHA-256 + salt, lưu bằng CSDL hoặc file	Võ Minh Khôi	100%	0.5
2	Đăng nhập & xác thực đa yếu tố	OTP sinh đúng, giới hạn thời gian, xác thực mới truy cập	Võ Minh Khôi	100%	0.5
3	Quản lý khóa RSA	Tạo cặp khóa, mã hóa private key bằng AES, lưu khóa, kiểm tra hạn sử dụng	Lê Nguyễn Minh Châu	100%	0.5
4	QR code	Tạo QR đúng format (email, ngày, public key), quét được từ ảnh	Lê Nguyễn Minh Châu	100%	0.5
5	Mã hóa & giải mã tập tin	Mã hóa file bằng AES, mã hóa khóa phiên bằng RSA, metadata. Giải mã chính xác	Nguyễn Tấn Hoàng	100%	1.0

6	Ký số & xác minh chữ ký số	Ký bằng private key, xác minh bằng public key, thông báo người ký chính xác	Nguyễn Tấn Hoàng	100%	1.0
7	Cập nhật tài khoản & đổi passphrase	Sửa thông tin, đổi passphrase đảm bảo private key vẫn dùng được	Võ Minh Khôi	100%	0.5
8	Phân quyền tài khoản	Phân quyền đúng chức năng User/Admin, Admin xem DS tài khoản, khóa tài khoản	Võ Minh Khôi	100%	0.5
9	Ghi log hoạt động bảo mật	Ghi các sự kiện quan trọng: login, mã hóa, ký số, sửa thông tin	Lê Nguyễn Minh Châu	100%	0.5
10	Chia nhỏ file lớn (>5MB) khi mã hóa	Chia block, mã hóa riêng từng block (AES-GCM hoặc CBC + kiểm tra toàn vẹn)	Nguyễn Tấn Hoàng	100%	0.5
11	Kiểm tra và gia hạn khóa	Hiển thị trạng thái khóa, cho phép gia hạn hoặc tạo lại	Võ Minh Khôi	100%	0.5
12	Tìm kiếm public key	Tìm kiếm theo email, hiển thị ngày tạo và QR nếu có	Lê Nguyễn Minh Châu	100%	0.5
13	Giới hạn đăng nhập sai	Khoá tài khoản 5 phút sau 5 lần sai, log lỗi, cảnh báo người dùng	Võ Minh Khôi	100%	0.5
14	Tuỳ chọn định dạng lưu file	Cho phép lưu gộp hoặc tách file enc và key, giải mã nhận diện đúng	Nguyễn Tấn Hoàng	100%	0.5
15	Khôi phục tài khoản	Tạo và dùng Recovery Key đúng quy trình, đảm bảo tính bảo mật	Võ Minh Khôi	100%	0.5
16	Báo cáo, README, phân công	Rõ ràng, đủ mục, minh hoạ, hướng dẫn chạy	Cả nhóm	100%	0.75

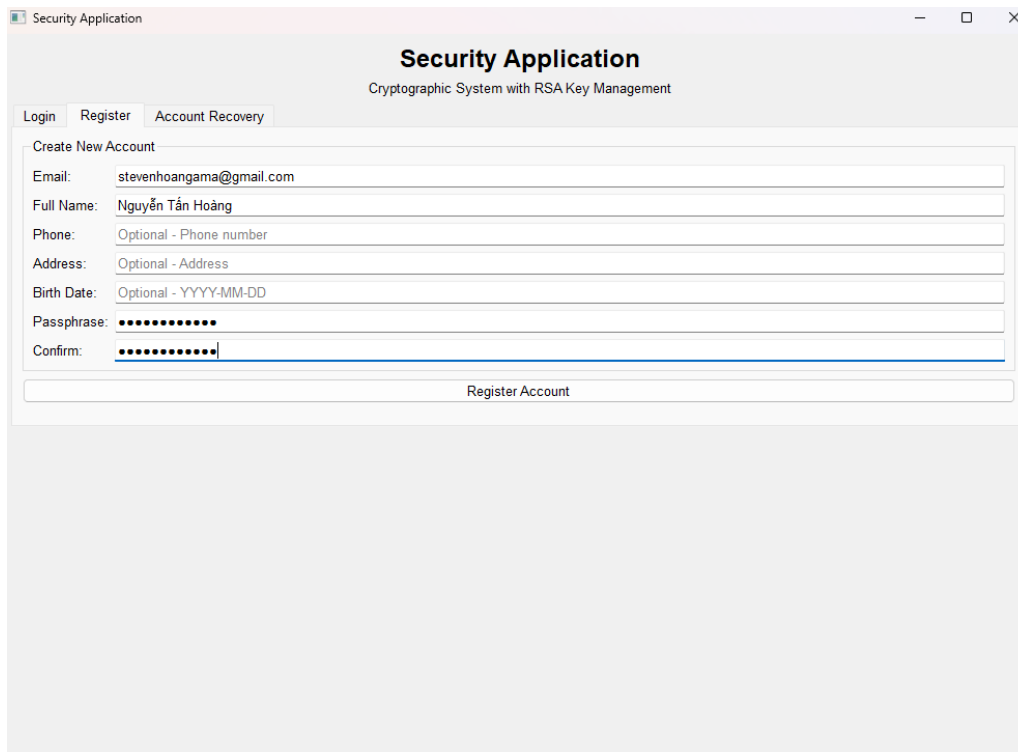
17	Demo sản phẩm + vấn đáp	Demo rõ ràng, trả lời đúng vai trò và phần mình làm	Cả nhóm		0.75
	Tổng cộng				9.25

2. Chi tiết các tính năng

1. Đăng ký tài khoản người dùng

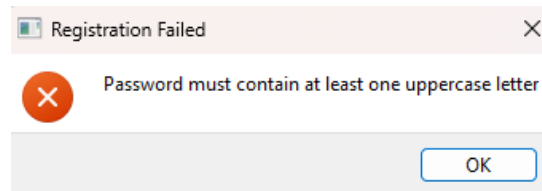
- Người dùng cần cung cấp thông tin cá nhân thông qua biểu mẫu đăng ký. Hệ thống phân loại các trường thông tin thành bắt buộc và không bắt buộc như sau:
 - Thông tin bắt buộc
 - Email: được sử dụng làm định danh duy nhất cho người dùng, phải hợp lệ theo định dạng chuẩn email. Hệ thống sẽ kiểm tra xem email đã được đăng ký trước đó chưa.
 - Họ tên: nhập đầy đủ họ và tên người dùng, dùng để hiển thị và quản lý tài khoản trong hệ thống.
 - Passphrase: mật khẩu cho tài khoản của người dùng. Passphrase phải tuân thủ các tiêu chí an toàn: ít nhất 8 ký tự, có cả chữ hoa và chữ thường, có cả số và ký hiệu.
Passphrase sẽ được kết hợp với salt ngẫu nhiên, sau đó được băm bằng SHA-256 và lưu vào CSDL.
 - Thông tin không bắt buộc
 - Ngày sinh: cho phép lưu trữ thông tin tuổi của người dùng (có thể phục vụ phân tích, thống kê hoặc cá nhân hóa trong tương lai).
 - Số điện thoại: Có thể được dùng trong các tính năng xác thực hai bước hoặc khôi phục tài khoản sau này.
 - Địa chỉ: Cung cấp thêm thông tin định vị người dùng, phục vụ cho một số chức năng mô phỏng trong hệ thống.

- Giao diện đăng ký tài khoản:



The screenshot shows a web application window titled "Security Application" with the subtitle "Cryptographic System with RSA Key Management". It features three tabs: "Login", "Register", and "Account Recovery". The "Register" tab is active, displaying a "Create New Account" form. The form includes fields for Email (filled with "stevenhoangama@gmail.com"), Full Name (filled with "Nguyễn Tấn Hoàng"), Phone (placeholder "Optional - Phone number"), Address (placeholder "Optional - Address"), Birth Date (placeholder "Optional - YYYY-MM-DD"), Passphrase (masked with dots), and Confirm (masked with dots). A "Register Account" button is at the bottom of the form.

- Khi nhập mật khẩu không tuân thủ tiêu chí an toàn, người dùng nhận được thông báo sau:



- Khi nhập các thông tin bắt buộc đúng định dạng, người dùng nhận được thông báo sau:

Registration Successful ? X

✓ Account created successfully!

⚠ IMPORTANT: Save this recovery code securely.
You'll need it to recover your account if you forget your passphrase.

Recovery Code:

8UYU3XZ8BV3LZIEE

Copy Code

🔑 RSA keys generated and ready for use.

OK

Người dùng cần lưu mã khôi phục để có thể khôi phục tài khoản nếu người dùng mất mật khẩu (sẽ mô phỏng tính năng khôi phục tài khoản ở các phần tiếp theo).

- Log ghi lại hành động đăng ký của tài khoản trên (dòng 3 đến dòng 7):

3	3	NULL	rsa_keypair_generation	success	Generated 2048-bit RSA key pair	127.0.0.1	stevenhoangama@gmail.com	2025-07-14 07:19:34
4	4	NULL	private_key_encryption	success	Private key encrypted with AES-256-GCM	127.0.0.1	stevenhoangama@gmail.com	2025-07-14 07:19:35
5	5	1	user_keys_created	success	RSA key pair created, expires: 2025-10-12	127.0.0.1	stevenhoangama@gmail.com	2025-07-14 07:19:35
6	6	NULL	KEY_MANAGEMENT	success	RSA keys generated for new user: stevenhoangama@g...	127.0.0.1	stevenhoangama@gmail.com	2025-07-14 07:19:35
7	7	NULL	user_registration	success	New user registered successfully with keys	127.0.0.1	stevenhoangama@gmail.com	2025-07-14 07:19:35

- Cơ sở dữ liệu lưu thông tin tài khoản trên:

users / 1

id	email	name	phone
1	stevenhoangama@gmail.com	Nguyễn Tấn Hoàng	NULL
READONLY	READONLY	READONLY	READONLY
address	birth_date	password_hash	salt
NULL	NULL	ef4a1652bc01ffb7e7eca50c4b01f80f4396930ca31dd9e94afb68b3d45bfff19	58371179709f7e1446becc04aed724967fb543e98ef4388d90fcd3fbf67ab04
READONLY	READONLY	READONLY	READONLY
role	created_at	is_locked	failed_attempts
user	2025-07-14 07:19:34	0	0
READONLY	READONLY	READONLY	READONLY
locked_until	recovery_code_hash		
NULL	402cd1d9235b2f44fb55b321e857f860f0ec1aaf6e44b20fcbeca0d3c5e51a99		
READONLY	READONLY		

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

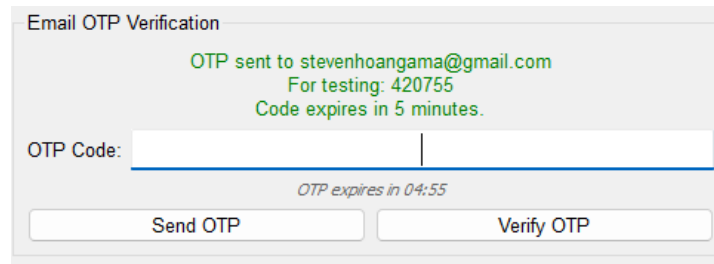
- Nhập thông tin xác thực
 - Nhập email để xác định danh tính người dùng, phải khớp với thông tin đã đăng ký trước đó.
 - Nhập passphrase tương ứng với email đã tạo. Hệ thống sẽ kiểm tra bằng cách kiểm tra hash của passphrase với salt tương ứng.
 - Giao diện nhập thông tin xác thực:
 - Log ghi lại hành động đăng nhập:

8	8	NULL	LOGIN_ATTEMPT	success	Successful login: stevenhoangama@gmail.com	127.0.0.1	stevenhoangama@gmail.com	2025-07-14 07:31:23
9	9	NULL	LOGIN_FLOW	success	Credentials verified for stevenhoangama@gmail.com, M...	127.0.0.1	stevenhoangama@gmail.com	2025-07-14 07:31:23

- Xác thực đa yếu tố:
 - Giao diện xác thực đa yếu tố:

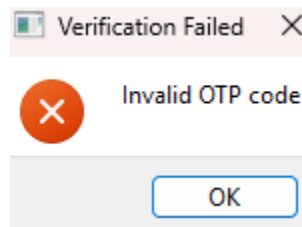
- Xác thực bằng OTP:
 - Người dùng chọn “Send OTP” để hệ thống sinh ra một mã OTP ngẫu nhiên 6 chữ số. Mã OTP này không gửi trực tiếp qua email mà là giả lập, hiển thị trực tiếp cho người dùng trong giao diện ứng dụng (mô phỏng hành vi gửi OTP qua email).

- Mã OTP có thời gian hiệu lực là 5 phút.
- Giao diện ứng dụng khi người dùng chọn gửi mã OTP:



The interface shows a form titled "Email OTP Verification". It displays a green message: "OTP sent to stevenhoangama@gmail.com", "For testing: 420755", and "Code expires in 5 minutes.". Below this is an "OTP Code:" label followed by a text input field. A timer below the input field says "OTP expires in 04:55". At the bottom are two buttons: "Send OTP" and "Verify OTP".

Người dùng nhận được thông báo lỗi nếu nhập sai mã OTP:



Hình chụp log khi tài khoản trên xác minh OTP thất bại:

12	12	1	otp_verification	failure	Invalid OTP code provided: 420751	127.0.0.1	stevenhoangama@gmail.com	2025-07-14 07:36:08
----	----	---	------------------	---------	-----------------------------------	-----------	--------------------------	---------------------

- Nếu người dùng nhập đúng mã OTP, người dùng sẽ được chuyển tới giao diện chính.

Hình chụp log khi tài khoản trên xác minh OTP thành công:

13	13	1	otp_verification	success	OTP verified successfully	127.0.0.1	stevenhoangama@gmail.com	2025-07-14 07:37:04
14	14	NULL	LOGIN_COMPLETE	success	Login completed with MFA: stevenhoangama@gmail.com	127.0.0.1	stevenhoangama@gmail.com	2025-07-14 07:37:04

○ Xác thực bằng TOTP:

- Người dùng chọn “Setup TOTP” trên giao diện hiển thị sau khi nhập email và passphrase để hệ thống sinh ra một mã QR.
- Người dùng sử dụng ứng dụng Google Authenticator trên thiết bị di động để quét mã QR này và sinh ra mã TOTP 6 chữ số để xác minh tài khoản.
- Giao diện ứng dụng khi người dùng chọn “Setup TOTP”:

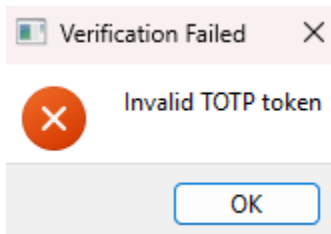
TOTP (Google Authenticator)

Scan QR code with Google Authenticator, then enter the 6-digit code.

Manual entry key: 3F4O7TYDGQQM6DCZ7HDDR3AD4EMLESE6

TOTP Code:

- Khi người dùng nhập sai mã xác thực, họ nhận được thông báo lỗi sau:



Hình chụp log sau khi nhập TOTP thất bại:

19	19	NULL	totp_verification	failure	Invalid TOTP token: 090321	127.0.0.1	NULL	2025-07-14 07:45:51
----	----	------	-------------------	---------	----------------------------	-----------	------	---------------------

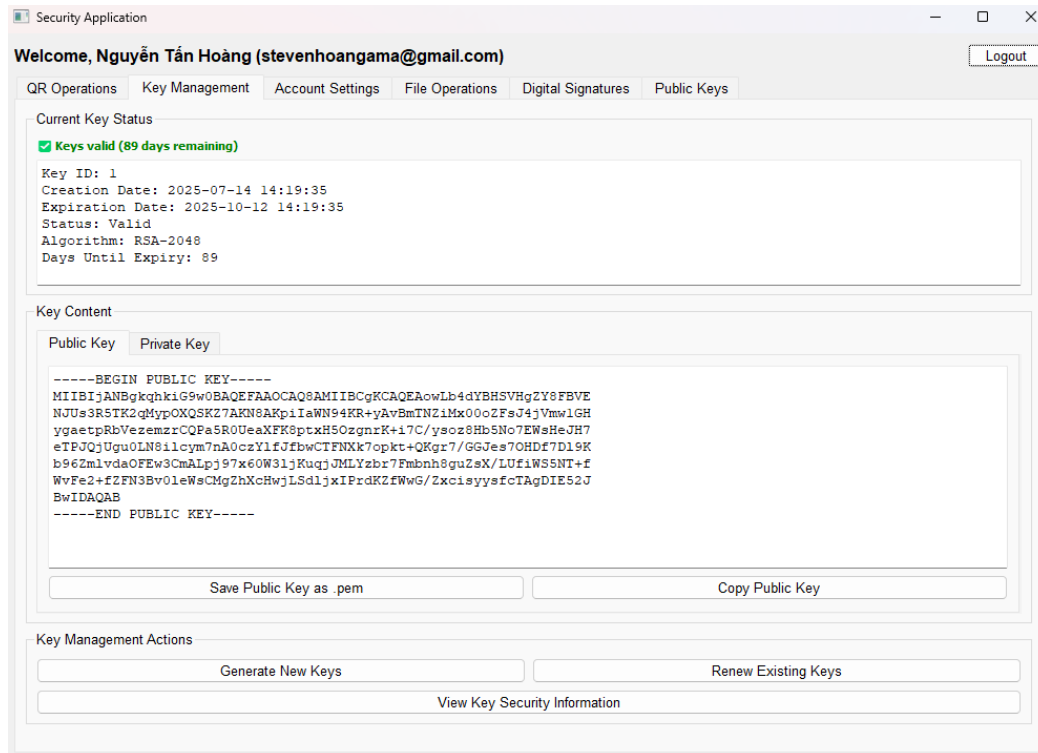
- Sau khi nhập đúng mã TOTP, người dùng được chuyển đến giao diện chính.

Hình chụp log sau khi nhập mã TOTP thành công:

21	21	NULL	totp_verification	success	TOTP token verified	127.0.0.1	NULL	2025-07-14 07:46:19
22	22	NULL	LOGIN_COMPLETE	success	Login completed with MFA: stevenhoangama@gmail.com	127.0.0.1	stevenhoangama@gmail.com	2025-07-14 07:46:19

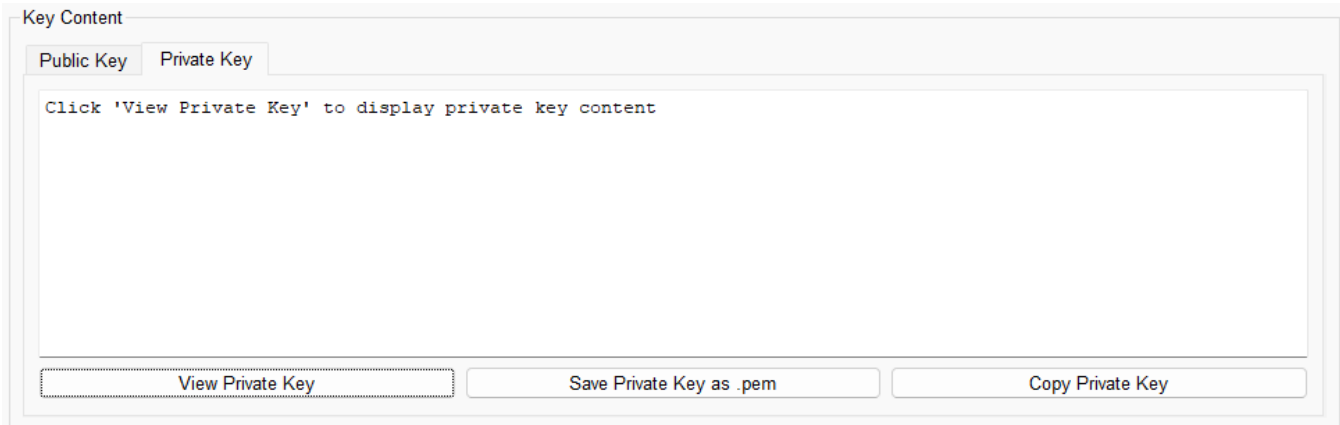
3. Quản lý khóa RSA cá nhân:

- Sau khi người dùng đăng ký tài khoản thành công, hệ thống tạo khóa RSA với độ dài khóa 2048 bit. Người dùng còn có thể làm mới khóa RSA. Khóa RSA của người dùng bao gồm:
 - Public Key: khóa công khai được lưu trong hệ thống gắn với email và ngày tạo khóa.
 - Private Key: khóa này được mã hóa bằng thuật toán AES được sinh ra từ passphrase gắn với tài khoản.
 - Ngày hết hạn của khóa sẽ là 90 ngày sau khi được tạo.
- Giao diện ứng dụng ở mục quản lý khóa RSA (mục “key management” trong ứng dụng):



- Mục “Current Key Status”: hiển thị thông tin trạng thái khóa, bao gồm những thông tin:
 - Key ID.
 - Ngày tạo khóa.
 - Ngày khóa hết hạn.
 - Trạng thái (valid hay invalid).
 - Số ngày còn lại trước khi khóa hết hạn.

- Mục “Key content”: mặc định hiển thị public key ứng với tài khoản. Người dùng có thể chọn vào “Private Key” → “View Private Key” để hệ thống hiển thị khóa này trực tiếp trên giao diện. Người dùng phải nhập passphrase để xem private key.
- Giao diện của khung “Key Content” khi chọn “Private Key”:



- Người dùng có thể lưu khóa (public và private) vào file .pem bằng cách nhấn chọn vào “Save Public Key as .pem” (hoặc “Save Private Key as .pem”). Người dùng sau đó chọn đường dẫn để lưu file này.

Nội dung file .pem của public key trên:

```

public_key_1.pem X
public_key_1.pem
1  |-----BEGIN PUBLIC KEY-----
2  |MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAowlb4dYBHSVHgZY8FBVE
3  |NJUs3R5TK2qMypOXQSKZ7AKN8AKpiIaWN94KR+yAvBmTNZiMx00oZFsj4jVmw1GH
4  |ygaetpRbVezemzrCQPa5R0UeaXFK8ptxH50zgnrK+i7C/ysoz8Hb5No7EWsHeJH7
5  |eTPJQjUgu0LN8ilcym7nA0czY1fJfbwCTFNXk7opkt+QKgr7/GGJes70HDF7D19K
6  |b96Zmlvda0FEw3CmALpj97x60W3ljKuqjJMLYzbr7Fmbnh8guZsX/LUfiwS5NT+f
7  |WvFe2+fZFN3Bv0leWsCMgZhXcHwjLSdljxIPrdKZfWwG/ZxcisyysfcTAgDIE52J
8  |BwIDAQAB
9  |-----END PUBLIC KEY-----
10

```

4. QR Code Public Key

- Sau khi người dùng đã tạo khóa RSA thành công, hệ thống cung cấp chức năng tạo mã QR chứa thông tin sau:
 - o Email: định danh người dùng.
 - o Ngày tạo khóa.
 - o Public Key: mã hóa base 64.
- Giao diện ứng dụng ở mục quản lý mã QR:

The screenshot shows a web application window titled "Security Application". The user is logged in as "Nguyễn Tấn Hoàng (stevenhoangama@gmail.com)". The interface has a navigation bar with tabs: "QR Operations", "Key Management", "Account Settings", "File Operations", "Digital Signatures", and "Public Keys". The "Public Keys" tab is selected.

Under the "Public Keys" tab, there are three main sections:

- Generate QR Code:** A section with the text "Generate a QR code containing your public key for easy sharing." and a button labeled "Generate QR Code for My Public Key".
- Import Public Key from QR Code:** A section with the text "Import someone else's public key by scanning their QR code image." and a button labeled "Import Public Key from QR Code".
- Search Public Keys:** A section with a search input field labeled "Email: Enter email to search" and a "Search" button.

Below these sections is a table titled "Imported Public Keys". The table has four columns: "Owner Email", "Creation Date", "Import Date", and "Status". The table is currently empty. A "Refresh" button is located at the bottom left of the table area.

- Khung “Generate QR Code”: sinh ra mã QR (lưu bằng file ảnh .png) bằng cách chọn “Generate QR Code for My Public Key”.
 - QR Code chứa public key của tài khoản trên:



Quét mã QR trên trả về thông tin sau, bao gồm email, ngày tạo và public key đã mã hóa bằng base 64:

```

stevenhoangama@gmail.com|2025-07-
14|LS0tLS1CRUdJTiBQVUJMSUMgS0VZLS0tLS0KTU1JQklqQU5CZ2txaGtpRz13MEJBUUVGQUFPQ
0FR0EFNSU1CQ2dLQ0FRRUFvd0xiNGRZQkhTVkhnWlk4RkJWRQpOS1VzM1I1VEsycU15cE9YUVNLW
jdBS044QUtwaUlhV045NEtSK3lBdkJtVE5aaU14MdBvWkZzSjRqVm13MUdICnlnYWV0cFJiVmV6Z
W16ckNRUGE1UjBVZWYRks4cHR4SDVPemducksraTdDL3lzb3o4SGI1Tm83RVdzSGVKSDcKZVRQS
lFqVWd1MEx0OGlsY3ltN25BMGN6WwXmSmZid0NURk5YazdvcGt0K1FLZ3I3L0dHSmVzN09IRGY3R
Gw5SwpiOTZabWx2ZGFPRkV3M0NtQUxwajk3eDYwVzNsakt1cWpKTUxZemJyN0ZtYm5oOGd1WnNYL
0xVZm1XUzVOVCTmCld2RmUyK2ZaRk4zQnYwbGVXc0NNZ1poWGNId2pMU2RsanhJUHJkS1pmV3dHL
1p4Y2lzeXlzMmNUQWdESUU1MkoKQndJREFRQUIKLS0tLS1FTkQgUFVCTE1DIETfWS0tLS0tCg==
  
```

- Khung “Import Public Key from QR Code”: đọc QR từ file .png để hiển thị thông tin và lưu.
 - Sau khi import ảnh mã QR thành công, thông tin public key được lưu ở mục “Imported Public Keys” ở khung dưới cùng trong giao diện:

	Owner Email	Creation Date	Import Date	Status
1	nthoang22@clc.fitus.edu.vn	2025-07-14	2025-07-14 08:43:53	Active

Refresh

- Khung “Search Public Keys”: tìm public key bằng cách nhập email của người dùng khác.

5. Cập nhật thông tin tài khoản:

- Người dùng được phép chỉnh sửa các trường sau:
 - o Họ tên
 - o Ngày sinh
 - o Địa chỉ
 - o Số điện thoại

Các trường này không ảnh hưởng đến hệ thống xác thực, nên có thể thay đổi linh hoạt theo nhu cầu người dùng.

- Người dùng có thể thay đổi passphrase trong trường hợp cần tăng cường bảo mật. Người dùng được yêu cầu nhập passphrase cũ đúng mới được đổi passphrase.
- Giao diện của mục quản lý tài khoản:

The screenshot shows a web application window titled "Security Application". The user is logged in as "Nguyễn Tấn Hoàng (stevenhoangama@gmail.com)". The interface has a top navigation bar with tabs: "QR Operations", "Key Management", "Account Settings", "File Operations", "Digital Signatures", and "Public Keys". The "Account Settings" tab is active.

Profile Information

Full Name:

Email:

Phone:

Address:

Birth Date:

Change Passphrase

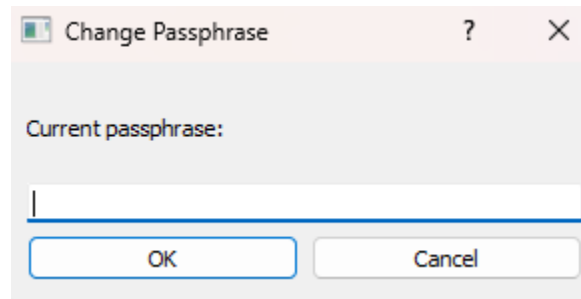
Change your account passphrase. This will re-encrypt your private keys.

Recent Activity

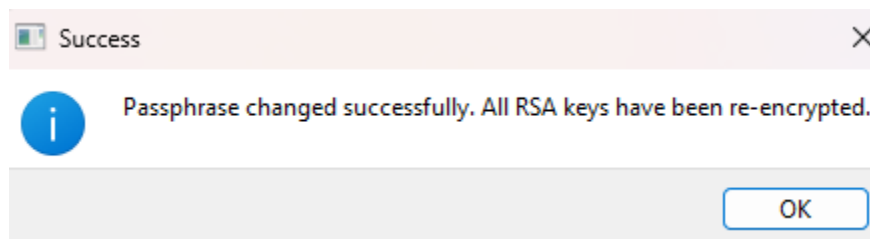
	Date/Time	Action	Status	Details
1	2025-07-14 08:43:47	otp_verification	success	OTP verified successfully
2	2025-07-14 08:43:43	otp_generated	success	OTP expires at 2025-07-14 15:48:43.677996
3	2025-07-14 08:31:49	public_key_qr_generated	success	Generated QR code for own public key
4	2025-07-14 07:42:21	totp_user_setup	success	TOTP setup and stored for user stevenhoangama@gmail.com

- o Khung "Profile Information": cho phép chỉnh sửa các trường: họ tên, số điện thoại, địa chỉ, ngày sinh. Sau khi chỉnh sửa, người dùng phải nhấn "Update Profile" để hệ thống lưu thông tin mới lại.

- Khung “Change Passphrase”: cho phép người dùng thay đổi passphrase:
 - Khi nhấn vào nút “Change Passphrase”, người dùng được yêu cầu nhập passphrase cũ trước:



- Sau đó người dùng được yêu cầu nhập Passphrase mới (nhập 2 lần để xác minh Passphrase mới nhập là đúng). Người dùng sẽ nhận được thông báo passphrase và RSA được tạo mới thành công:



- Hình chụp log sau khi thay đổi passphrase cho tài khoản trên:

55	55	NULL	private_key_decryption	success	Private key decrypted successfully	127.0.0.1	stevenhoangama@gmail.com	2025-07-14 08:56:51
56	56	NULL	private_key_encryption	success	Private key encrypted with AES-256-GCM	127.0.0.1	NULL	2025-07-14 08:56:51
57	57	NULL	PASSPHRASE_CHANGE	success	Passphrase changed for user: stevenhoangama@gmail.c...	127.0.0.1	stevenhoangama@gmail.com	2025-07-14 08:56:51

- Hệ thống sẽ không lưu lại passphrase cũ, và passphrase mới sẽ được mã hóa như cách nhập passphrase ở bước tạo tài khoản.

6. Mã hoá tập tin gửi người khác

- Tính năng này cho phép người dùng mã hóa tập tin trước khi gửi cho người nhận, đảm bảo chỉ người nhận có private key tương ứng mới có thể giải mã và truy cập nội dung.
- Giao diện mục mã hóa tập tin để gửi người khác (mục “File Operations”):

Security Application

Welcome, Nguyễn Tấn Hoàng (stevenhoangama@gmail.com) Logout

QR Operations | Key Management | Account Settings | **File Operations** | Digital Signatures | Public Keys

Encrypt File

File: Browse

Recipient: Refresh Recipients

Output Format: Encrypt File

Decrypt File

Encrypted File: Browse

Key File (optional): Browse

Decrypt File

File Operation Information

File Encryption Information:

- Files are encrypted using AES-256-GCM for security
- RSA public keys encrypt the AES session keys
- Large files (>3MB) are processed in chunks for efficiency
- Encrypted files can be saved in combined (.enc) or separate (.enc + .key) format
- Only the recipient's private key can decrypt the file

- Giao diện khung:

Encrypt File

File: Browse

Recipient: Refresh Recipients

Output Format: Encrypt File

- Việc gửi file đến người khác hoạt động như sau:
 - Chọn file cần gửi (chọn nút “Browse” bên phải dòng “File”).
 - Chọn email người nhận: Email này phải tồn tại trong hệ thống và có public key hợp lệ.
 - Nếu không có public key, hệ thống sẽ hiển thị thông báo lỗi, không cho phép tiếp tục.
 - Chọn “Encrypt File” để mã hóa file đã chọn.
 - Hệ thống sẽ mã hóa file như sau:

- Bước 1: Sinh khóa phiên (Ksession): Sinh ngẫu nhiên một khóa AES (ví dụ 256 bit) gọi là Ksession, dùng làm khóa tạm thời cho việc mã hóa nội dung file.
- Bước 2: Mã hóa nội dung tập tin: Sử dụng thuật toán AES bằng GCM để mã hóa nội dung file với Ksession. IV (vector khởi tạo) cũng được sinh ngẫu nhiên và lưu kèm dữ liệu.
- Bước 3: Mã hóa Ksession bằng RSA: Lấy public key của người nhận (đã lưu từ trước) rồi mã hóa bằng RSA 2048-bit. Người nhận sẽ dùng private key tương ứng để giải mã sau này.
- Bước 4: Gắn metadata đã mã hóa: tạo gói thông tin bao gồm: email, tên tập tin gốc, thời điểm gửi, thông tin của file, ...
- Bước 5: Tùy chọn định dạng lưu trữ: Người dùng được chọn giữa 2 chế độ lưu kết quả:
 - Gộp 1 file .enc: gồm dữ liệu đã mã hóa, Ksession đã mã hóa, metadata, IV.
 - Tách thành 2 file (.enc và .key):
 - File .enc: chứa nội dung file đã mã hóa bằng AES.
 - File .key: chứa Ksession đã mã hóa và metadata.

- Log hành vi của hành động mã hóa file ở hình trên:

69 69 1 file_encrypted success Regular File send_to.txt encrypted for nthoang22@clc.fit... 127.0.0.1 stevenhoangama@gmail.com 2025-07-14 09:10:35

- Nội dung file mã hóa (gồm metadata, Ksession và một phần dữ liệu file đã mã hóa):

```
{
  "metadata": {
    "sender_email": "stevenhoangama@gmail.com",
    "recipient_email": "nthoang22@clc.fitus.edu.vn",
    "original_filename": "cat.jpg",
    "file_size": 41006,
    "timestamp": "2025-07-14T16:08:46.078131",
    "algorithm": "AES-256-GCM",
    "format_version": "1.0",
    "is_large_file": false
  },
  "nonce": "8f68de48c34301e1efdd87",
  "encrypted_session_key":
    "4a0796a8a3bf7ad639627a11d7b088413707a27600af494883e7a4f52b8f560b99bcae64b7cbe620bdd081a17badcac06cc31efa53ff48fc89f9ae9b8476ee7661de3553b41141d9a034f56dbe6902c820bcc323
    9e7b1f08f40eba8795f5a8d3e1d30d965d95d972f585c0ec8bfff336f52b45974f6190c726500ffaebf8cc0990e1bfe8f0888543f7c5cdcb31bf1598c86292631a3373aa57534905fc268ab3245c21f7159e23db17
    a6875af5ac105f35d560a3142601e84fb8c339e2ea9ec368e7d0a128fbab2aaac607c9825841d7c584d3f3d3d5dfb5500f9403eb763f6ff1f0acee7165ec164593383eb5ded9a41808519333debc61dcb3a532b1
    936e9d",
  "ciphertext":
    "4b965f5a751f8cd86074bf192c3d506f588dbc9f87faf61b73925acedb82b4047d106687b7553611523b71902c2cadb6de839f64572889cdfa58df7c103585b11651f4721dc7b3dc9391f87ef85596708294055a
    885c3ded86c4c4423cb651fb4fa88ea52a30c451a9c0d3f87929a35927b182f464521915fbf4ad556a2b146264788e2d9a2871db731a94ba873c62a9d78c53a869d49944046300d4eaea19ff2dd873338def38e1
    20e1a1af9168f54b3ee27d4d1efb597dbd13392b4f70ad7f54bdce497c6372ecd06fb903d56c988b616bda6f5595046db23eebd9dfea890d7652611a2e01de2f246f428ca06dd5b0633f40a5cc3de9187d604070e4
    49f7fb62fc1b65cfd5332e4017c494d3e5fe6f44509d8f72101223f5bd9f94037028035393a2ff82e4e3070c8bb1d0820b264e290693baac33742c0e66b042ce8f5550fe1f6880d644f62f2cd355ecd5f334366
    ec964beea351cb65bdd3524d5ca5cfc6c19d2cdd7ac36976ec10a9e3ab31e5b5f6007f174d27b7d2dca54190e2b3a36bf977c510b3f4bd28e571fda1be6b64e39726ef5d98a910f24f246d15bf96dccc58ca0c56"
```

7. Giải mã tập tin

- Giao diện khung (trong mục “File Operations”):

- Để mã hóa file được gửi đến, người dùng thực hiện những bước sau:
 - o Chọn file cần decrypt (chọn nút “Browse” bên phải dòng “File”).
 - o Chọn Decrypt file. Hệ thống sẽ yêu cầu người dùng nhập passphrase mới có thể decrypt.
 - o File sau khi Decrypt sẽ được lưu vào thư mục /data/decrypted.
- Log hành vi của hành động mã hóa file trên:

79	79	NULL	private_key_decryption	success	Private key decrypted successfully	127.0.0.1	nthoang22@clc.fitus.edu.vn	2025-07-14 09:15:56
80	80	2	file_decrypted	success	Regular File cat.jpg decrypted from stevenhoangama@g...	127.0.0.1	nthoang22@clc.fitus.edu.vn	2025-07-14 09:15:56

8. Ký số tập tin:

- Tính năng "Ký số tập tin" cho phép người dùng tạo chữ ký số để đảm bảo tính toàn vẹn và xác thực nguồn gốc của tập tin. Khi tập tin được ký, người nhận có thể kiểm tra xem nội dung có bị thay đổi hay không và xác minh người gửi dựa trên public key của họ.
- Giao diện của mục ký số tập tin (Digital Signatures):

- Để ký tập tin, người dùng thực hiện các bước sau:
 - Trong khung “Sign File”, người dùng chọn file cần ký.
 - Sau đó người dùng chọn “Create Digital Signature” để lưu file `.sig` tương ứng.
- Hệ thống thực hiện các bước sau để ký file:
 - Bước 1: Băm nội dung tập tin: Đọc toàn bộ nội dung file, tính toán giá trị băm SHA-256.
 - Bước 2: Ký số bằng khóa riêng (private key): Dùng private key RSA của người dùng (giải mã từ bản lưu mã hóa bằng AES). Chữ ký này có thể xác minh lại bằng public key tương ứng.
 - Bước 3: Tạo file chữ ký `.sig`: Lưu chữ ký số kèm metadata dưới dạng file riêng biệt có định dạng `.sig`.

- Nội dung file .sig của file trên hình sau khi ký:

```

1  {
2    "signer_email": "stevenhoangama@gmail.com",
3    "original_filename": "cat.jpg",
4    "timestamp": "2025-07-14T10:29:24.871661+00:00",
5    "file_hash": "5a5d2bfff5e03b6cc88cadbaac9d27a20ec4ef308e77ad460847e101ea13dccc6",
6    "algorithm": "SHA-256",
7    "padding": "PSS",
8    "mgf": "MGF1(SHA256)",
9    "salt_length": "max",
10   "format_version": "1.0"
11 }
12 ---SIGNATURE---
13 eSUBk_DC4 7-\sI~y400&xDC4/Q1xN(DLE) ><,D L}V
14 W|z>STXx^HF SI gHc0"qqSUB|bPm
15 xC7;i"X
16 }[vfBS nI P/W`Owx-y:

```

- Log hành vi khi ký tập tin:

```

153      153      NULL  file_signed      success      File: cat.jpg, Hash: 5a5d2bfff5e03b6cc...      127.0.0.1      stevenhoangama@gmail.com      2025-07-14 10:29:24

```

9. Xác minh chữ ký

- Tính năng "Xác minh chữ ký số" cho phép người dùng kiểm tra tính toàn vẹn và xác thực của một tập tin đã được ký số.
- Thao tác người dùng:
 - o Người dùng chọn một file bất kỳ.
 - o Sau đó người dùng chọn file chữ ký .sig tương ứng.
 - o Hệ thống sau đó trả về kết quả, cho biết file với chữ ký có tương ứng với nhau không.
- Sau khi nhận được hai tệp đầu vào, hệ thống thực hiện:
 - o Bước 1: Tính lại giá trị băm SHA-256: Đọc nội dung tập tin gốc. Và tính toán lại giá trị băm SHA-256.
 - o Bước 2: Duyệt qua các public key đã lưu. Hệ thống kiểm tra chữ ký .sig bằng cách:
 - Duyệt từng public key trong danh sách (gắn với email, ngày tạo). Dùng public key để giải mã chữ ký, thu được giá trị băm gốc đã ký.
 - So sánh với giá trị băm vừa tính ở bước 1.
 - Nếu trùng khớp thì chữ ký hợp lệ, xác định được người ký.
- Sau khi nhập 2 file (file gốc và file chữ ký), hệ thống trả về kết quả sau khi kiểm tra:
 - o Giao diện khi chữ ký hợp lệ:

Verify Signature

Original File: D:/study/comsec/project1/cat.jpg

Browse

Signature File (.sig): D:/study/comsec/project1/data/signatures/cat_20250714_172924.sig

Browse

Verify Signature

Verification Results

✓ VERIFICATION SUCCESSFUL

Signature verified! Signed by: stevenhoangama@gmail.com on 2025-07-14T10:29:24.871661+00:00

Signature Details:

- Signer: stevenhoangama@gmail.com
- Date: 2025-07-14T10:29:24.871661+00:00
- File: cat.jpg
- Hash: 5a5d2bff5e03b6cc88cadbaac9d27a20ec4ef308e77ad460847e101ea13dccc6

- o Log hành vi trong trường hợp này:

154	154	NULL	signature_verification	success	Verified signature for cat.jpg by stevenhoangama@gmail...	127.0.0.1	stevenhoangama@gmail.com	2025-07-14 10:30:27
-----	-----	------	------------------------	---------	---	-----------	--------------------------	---------------------

- Giao diện khi chữ ký không hợp lệ:

Verify Signature

Original File: D:/study/comsec/project1/send_to.txt

Browse

Signature File (.sig): D:/study/comsec/project1/data/signatures/cat_20250714_172924.sig

Browse

Verify Signature

Verification Results

✗ VERIFICATION ERROR

Signature verification failed: File hash does not match signature.

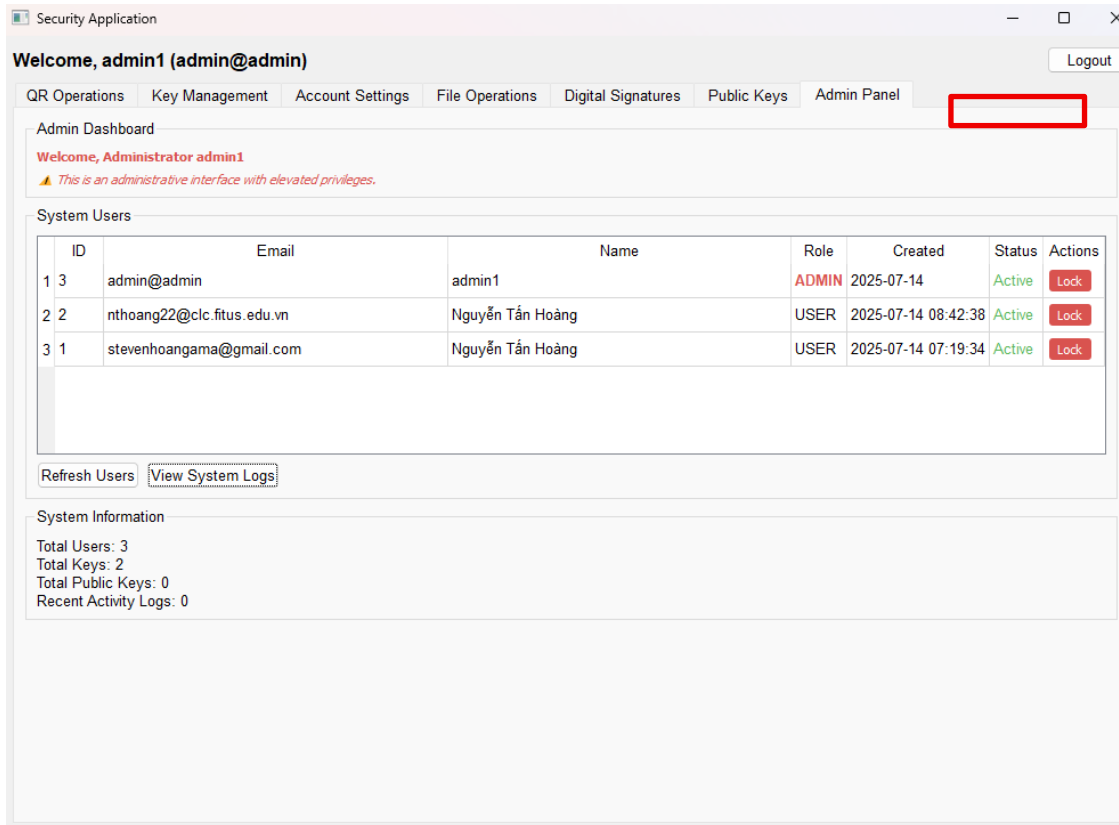
Log hành vi trong trường hợp này:

155	155	NULL	signature_verification	failure	Hash mismatch for send_to.txt	127.0.0.1	stevenhoangama@gmail.com	2025-07-14 10:41:17
-----	-----	------	------------------------	---------	-------------------------------	-----------	--------------------------	---------------------

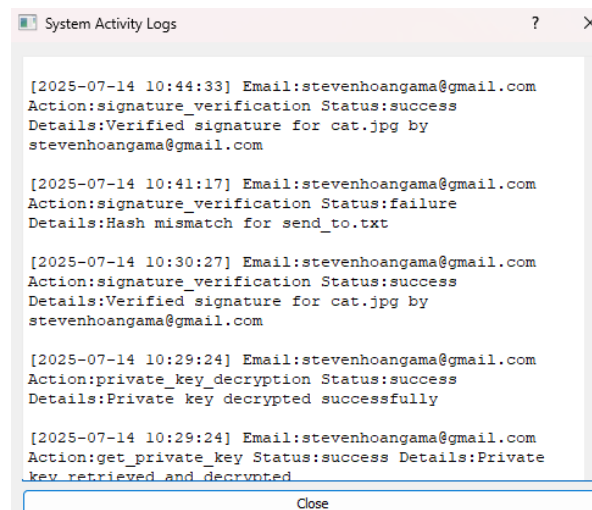
10. Phân quyền tài khoản:

- Tính năng "Phân quyền tài khoản" được thiết kế để quản lý quyền truy cập và vai trò của người dùng trong hệ thống. Bằng cách phân chia rõ vai trò admin và user, hệ thống đảm bảo rằng chỉ người quản trị mới có thể thực hiện các tác vụ nhạy cảm như xem danh sách tài khoản, quản lý trạng thái người dùng và theo dõi hoạt động hệ thống.
- Mỗi tài khoản trong hệ thống sẽ có một trường cờ (flag), với các giá trị:
 - Admin: tài khoản quản trị hệ thống.
 - User: tài khoản người dùng thông thường.
- Quyền của user: có thể thực hiện các tính năng cơ bản như:
 - Đăng ký, đăng nhập.
 - Tạo/gửi khóa RSA.
 - Gửi, nhận file đã mã hóa.
 - Tạo QR cho public key.
 - Mã hóa, ký số và xác minh tập tin.
 - Cập nhật thông tin cá nhân.
- Quyền của admin: gồm mọi quyền của user, thêm một số tính năng quản trị:
 - Xem danh sách tài khoản trong hệ thống. Thông tin hiển thị cho admin gồm: Thông tin hiển thị gồm: email, họ tên, vai trò, trạng thái (bình thường hoặc bị khóa), ngày tạo.
 - Khóa/Mở khóa tài khoản: Có thể chuyển trạng thái của tài khoản người dùng:
 - Khóa: người dùng không thể đăng nhập hoặc sử dụng các tính năng của hệ thống.
 - Mở khóa: khôi phục quyền truy cập cho tài khoản đã bị khóa.
 - Xem log hoạt động toàn hệ thống: Truy cập lịch sử thao tác của tất cả người dùng. Thông tin hiển thị bao gồm:
 - Thời gian đăng nhập.
 - Hành động thực hiện (ví dụ: tạo khóa RSA, mã hóa file, xác minh chữ ký...).

- Giao diện của admin: có thêm mục “Admin Panel” đối với tài khoản admin:



- Các thao tác của admin trên giao diện:
 - o Xem được role (admin hay user) của mọi tài khoản: hiển thị ở cột role.
 - o Khóa/mở khóa tài khoản bằng cách chọn “Lock”/”Unlock” đối với tài khoản tương ứng.
 - o Xem log thao tác của hệ thống: chọn nút “View System Logs” ở trong giao diện admin.
 - Hình chụp log hệ thống của admin:



11. Ghi log bảo mật:

- Tính năng này ghi lại toàn bộ hoạt động liên quan đến bảo mật trong hệ thống nhằm phục vụ kiểm tra, giám sát và truy vết khi cần thiết.
- Hoạt động được ghi lại vào file `security.log` ở thư mục hệ thống.
- Nội dung trong mỗi dòng bao gồm:
 - o Thời gian thực hiện hành động.
 - o Email (tài khoản) thực hiện hành động.
 - o Hành động được thực thi.
 - o Trạng thái: thành công hay thất bại.
 - o Chi tiết hành động: hành động cụ thể khi thực hiện thành công, hay lý do thất bại.
- Dưới đây là trích một đoạn của `security.log` sau khi thực thi một số hành động:

```

1 [2025-07-14 14:18:50,172] [INFO] Email:None Action:daily_lifecycle_check Status:succes Details:Processed lifecycle for 0 keys
2 [2025-07-14 14:18:50,647] [INFO] Email:None Action:app_start_gui Status:succes Details:GUI application started
3 [2025-07-14 14:19:35,058] [INFO] Email:stevenhoangama@gmail.com Action:rsa_keypair_generation Status:succes Details:Generated 2048-bit RSA key pair
4 [2025-07-14 14:19:35,298] [INFO] Email:stevenhoangama@gmail.com Action:private_key_encryption Status:succes Details:Private key encrypted with AES-256-GCM
5 [2025-07-14 14:19:35,529] [INFO] Email:stevenhoangama@gmail.com Action:user_keys_created Status:succes Details:RSA key pair created, expires: 2025-10-12
6 [2025-07-14 14:19:35,650] [INFO] Email:stevenhoangama@gmail.com Action:KEY_MANAGEMENT Status:succes Details:RSA keys generated for new user: stevenhoangama@gmail.com
7 [2025-07-14 14:19:35,759] [INFO] Email:stevenhoangama@gmail.com Action:user_registration Status:succes Details:New user registered successfully with keys
8 [2025-07-14 14:31:23,613] [INFO] Email:stevenhoangama@gmail.com Action:LOGIN_ATTEMPT Status:succes Details:Successful login: stevenhoangama@gmail.com
9 [2025-07-14 14:31:23,703] [INFO] Email:stevenhoangama@gmail.com Action:LOGIN_FLOW Status:succes Details:Credentials verified for stevenhoangama@gmail.com, MFA required
10 [2025-07-14 14:35:37,898] [INFO] Email:stevenhoangama@gmail.com Action:otp_generated Status:succes Details:OTP expires at 2025-07-14 14:40:37.708594
11 [2025-07-14 14:35:38,003] [INFO] Email:stevenhoangama@gmail.com Action:email_simulation Status:succes Details:OTP email simulated for stevenhoangama@gmail.com
12 [2025-07-14 14:36:08,638] [ERROR] Email:stevenhoangama@gmail.com Action:otp_verification Status:failure Details:Invalid OTP code provided: 420751
13 [2025-07-14 14:37:04,358] [INFO] Email:stevenhoangama@gmail.com Action:otp_verification Status:succes Details:OTP verified successfully
14 [2025-07-14 14:37:04,438] [INFO] Email:stevenhoangama@gmail.com Action:LOGIN_COMPLETE Status:succes Details>Login completed with MFA: stevenhoangama@gmail.com
15 [2025-07-14 14:42:20,398] [INFO] Email:stevenhoangama@gmail.com Action:LOGIN_ATTEMPT Status:succes Details:Successful login: stevenhoangama@gmail.com
16 [2025-07-14 14:42:20,496] [INFO] Email:stevenhoangama@gmail.com Action:LOGIN_FLOW Status:succes Details:Credentials verified for stevenhoangama@gmail.com, MFA required
17 [2025-07-14 14:42:21,487] [INFO] Email:stevenhoangama@gmail.com Action:totp_setup Status:succes Details:TOTP setup for stevenhoangama@gmail.com
18 [2025-07-14 14:42:21,648] [INFO] Email:stevenhoangama@gmail.com Action:totp_user_setup Status:succes Details:TOTP setup and stored for user stevenhoangama@gmail.com
19 [2025-07-14 14:45:51,128] [ERROR] Email:None Action:totp_verification Status:failure Details:Invalid TOTP token: 090321
20 [2025-07-14 14:46:01,502] [ERROR] Email:None Action:totp_verification Status:failure Details:Invalid TOTP token: 090322
21 [2025-07-14 14:46:19,233] [INFO] Email:None Action:totp_verification Status:succes Details:TOTP token verified
22 [2025-07-14 14:46:19,308] [INFO] Email:stevenhoangama@gmail.com Action:LOGIN_COMPLETE Status:succes Details>Login completed with MFA: stevenhoangama@gmail.com
23 [2025-07-14 15:11:10,079] [INFO] Email:stevenhoangama@gmail.com Action:private_key_decryption Status:succes Details:Private key decrypted successfully
24 [2025-07-14 15:13:24,748] [INFO] Email:stevenhoangama@gmail.com Action:private_key_decryption Status:succes Details:Private key decrypted successfully

```

12. Chia nhỏ tập tin lớn:

- Giúp xử lý và mã hóa hiệu quả các tập tin có dung lượng lớn bằng cách chia nhỏ thành các block, đảm bảo an toàn và toàn vẹn dữ liệu khi mã hóa.
- Trong quá trình mã hóa và gửi file cho người khác (mục 5), nếu tập tin > 5MB, hệ thống sẽ chia nhỏ ra thành các block 1MB và mã hóa chúng.
- Hình chụp log cho hành động mã hóa và gửi cho người khác:

197	197	1	file_encrypted	success	Large File book.pdf encrypted for nthoang22@clc.fitus.e...	127.0.0.1	stevenhoangama@gmail.com	2025-07-14 12:50:33
-----	-----	---	----------------	---------	--	-----------	--------------------------	---------------------

File được mã hóa có kích thước ~ 23MB và được chia thành 23 block kích thước 1MB.

13. Hiện thị trạng thái khóa:

- Giúp người dùng theo dõi tình trạng cặp khóa RSA đang sử dụng để đảm bảo luôn có khóa hợp lệ phục vụ mã hóa, giải mã và ký số.
- Khi truy cập giao diện kiểm tra (ở mục Key Management), hệ thống hiển thị:
 - Ngày tạo khóa
 - Hạn dùng (mặc định 90 ngày từ ngày tạo)
 - Trạng thái:
 - Còn hạn: còn hơn 7 ngày trước khi hết hạn.
 - Gần hết hạn: còn dưới 7 ngày trước khi hết hạn.
 - Hết hạn: khóa không còn sử dụng được.
- Giao diện kiểm tra trạng thái khóa:

Security Application

Welcome, Nguyễn Tấn Hoàng (stevenhoangama@gmail.com) Logout

QR Operations | **Key Management** | Account Settings | File Operations | Digital Signatures | Public Keys

Current Key Status

✓ **Keys valid (89 days remaining)**

Key ID: 1
 Creation Date: 2025-07-14 14:19:35
 Expiration Date: 2025-10-12 14:19:35
 Status: Valid
 Algorithm: RSA-2048
 Days Until Expiry: 89

Key Content

Public Key | Private Key

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAowLb4dYBHSVHgZY8FBVE
NJUs3R5TK2qMyPOXSKZ7AKN8AKpiIaWN94KR+yAvBmTNZiMx00oZFsj4jVmw1GH
ygaetpRbVezemzrCQPa5R0UeaXFK8ptxH5OzgnrK+i7C/ysoz8Hb5No7EWsHeJH7
eTPJQjUgu0LN8ilcym7nA0czY1fJfbwCTFNXk7opkt+QKgr7/GGJes7OHDf7D19K
b96ZmlvdaOFFew3CmALpj97x60W31jKuqjJMLYzbr7Fmbnh8guZsX/LUfiWS5NT+f
WvFe2+fZFN3Bv01eWsCMgZhXcHwjLSdljxIPrdKZfWwG/ZxcisyysfcTAgDIE52J
BwIDAQAB
-----END PUBLIC KEY-----
```

Save Public Key as .pem Copy Public Key

Key Management Actions

Generate New Keys Renew Existing Keys

View Key Security Information

- Ở mục Key Management, tại khung “Current Key Status”, giao diện đang hiển thị rằng khóa vẫn còn hạn sử dụng 89 ngày.

14. Tìm kiếm public key

- Tính năng này giúp người dùng tra cứu khóa công khai (public key) của người khác trong hệ thống để phục vụ các tác vụ như mã hóa tập tin, xác minh chữ ký hoặc chia sẻ dữ liệu an toàn.
- Để tìm kiếm public key, người dùng thực hiện các bước sau:
 - o Ở mục Public Keys, nhập email của người dùng khác trong khung “Search Public Keys”.
 - o Sau khi tìm kiếm, nếu tìm thấy public key tương ứng với email thì kết quả được hiển thị ở mục “Available Public Keys” ngay bên dưới, với email, QR Code, ngày tạo khóa và thời hạn còn lại.
- Giao diện của mục “Public Keys”:

Security Application

Welcome, Nguyễn Tấn Hoàng (stevenhoangama@gmail.com) [Logout](#)

QR Operations | Key Management | Account Settings | File Operations | Digital Signatures | **Public Keys**

Search Public Keys

Email: [Search](#)

Available Public Keys

	Email	QR Code	Creation Date	Expire In
1	test@email.com	Show QR	2025-07-14	89 days
2	nthoang22@clc.fitus.edu.vn	Show QR	2025-07-14	89 days

[Refresh All Keys](#) [Show All Keys](#)

Public Key Management Information

Public Key Management:

- Public keys are used to encrypt files for specific recipients
- Import public keys via QR codes or direct sharing
- Search for keys by email address to find available recipients
- All imported keys are stored securely for future use
- Click QR Code button to view and share public keys

- Sau khi nhập email để tìm public key (trong ví dụ sẽ tìm test@email.com), hệ thống sẽ thông báo tìm khóa thành công và trong mục Available Public Keys sẽ chỉ hiển thị email tương ứng:

Search Public Keys

Email:

Available Public Keys

Email	QR Code	Creation Date	Expire In
1 test@email.com	<input type="button" value="Show QR"/>	2025-07-14	89 days

Search Results

Found 1 matching keys.

- Nếu không tìm thấy email tương ứng, hệ thống sẽ thông báo lỗi, và không có key nào xuất hiện trong mục “Available Public Keys”:

Search Public Keys

Email:

Available Public Keys

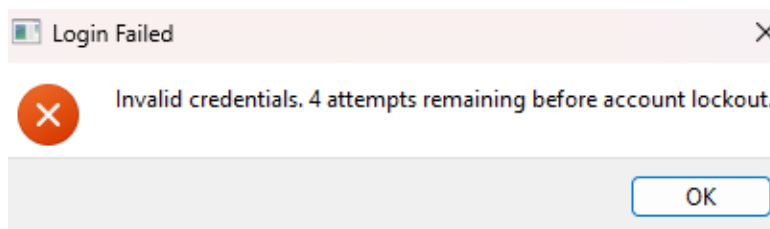
Email	QR Code	Creation Date	Expire In
-------	---------	---------------	-----------

Search Results

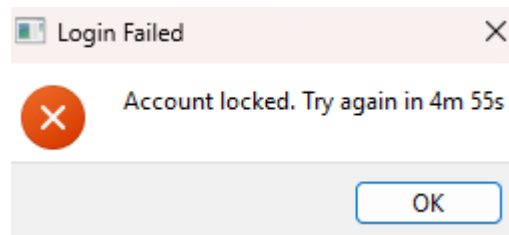
No keys found matching that email.

15. Giới hạn đăng nhập:

- Tính năng này giúp ngăn chặn tấn công dò mật khẩu (brute-force) bằng cách giới hạn số lần đăng nhập sai và tạm khóa tài khoản trong thời gian ngắn.
- Cơ chế hoạt động:
 - o Sau 5 lần nhập sai passphrase liên tiếp, tài khoản sẽ bị tự động khóa trong 5 phút.
 - o Trong thời gian bị khóa, người dùng không thể đăng nhập, giao diện sẽ hiển thị thời gian chờ còn lại.
 - o Sau 5 phút, tài khoản tự mở lại nếu không có hành vi đáng ngờ khác.
 - o Mỗi lần đăng nhập sai, hệ thống sẽ ghi chú vào security.log với các thông tin: email, thời gian, hành động đăng nhập và trạng thái (thất bại).
- Giao diện ở màn hình đăng nhập:
 - o Khi nhập sai mật khẩu, hệ thống hiển thị thông báo sau:



- o Nếu nhập sai 5 lần liên tiếp, hệ thống sẽ hiển thị thông báo sau vào lần đăng nhập tiếp theo:



- Hình chụp log khi đăng nhập sai mật khẩu 5 lần liên tiếp:

234	234	NULL	LOGIN_ATTEMPT	failure	Invalid password for user: test@email.com	127.0.0.1	test@email.com	2025-07-14 13:28:45
235	235	NULL	LOGIN_ATTEMPT	failure	Invalid password for user: test@email.com	127.0.0.1	test@email.com	2025-07-14 13:29:50
236	236	NULL	LOGIN_ATTEMPT	failure	Invalid password for user: test@email.com	127.0.0.1	test@email.com	2025-07-14 13:29:52
237	237	NULL	LOGIN_ATTEMPT	failure	Invalid password for user: test@email.com	127.0.0.1	test@email.com	2025-07-14 13:29:53
238	238	NULL	account_lockout	warning	Account locked for 5 minutes: test@email.com	127.0.0.1	test@email.com	2025-07-14 13:29:54

Những lần đăng nhập sau (mà thời gian 5 phút khóa tài khoản chưa hết), log ghi lại thông tin như sau:

240	240	NULL	LOGIN_ATTEMPT	warning	Locked account login attempt: test@email.com	127.0.0.1	test@email.com	2025-07-14 13:29:58
-----	-----	------	---------------	---------	--	-----------	----------------	---------------------

16. Tùy chọn định dạng lưu file:

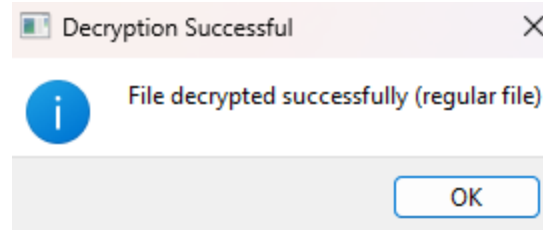
- Tính năng này cung cấp sự linh hoạt trong quá trình mã hóa và giải mã tập tin, cho phép người dùng lựa chọn cách lưu trữ phù hợp với mục đích sử dụng hoặc chia sẻ.
- Khi mã hóa file, người dùng có thể chọn:
 - o Gộp tất cả vào một file .enc duy nhất.
 - o Tách riêng thành file .enc (chứa nội dung file đã mã hóa) và file .key (chứa khóa AES đã mã hóa và metadata).
- Khi giải mã file, người dùng chọn định dạng đầu vào:
 - o File mã hóa chỉ có file .enc, gồm cả key và nội dung file đã mã hóa.
 - o Có cả 2 file .enc và .key.
- Giao diện cho tính năng chọn định dạng lưu file:

- o Người dùng chọn file cần mã hóa ở trường “File” (nhấn Browse để chọn File từ máy tính).
- o Người dùng chọn người nhận (email) hợp lệ ở trường “Recipient”.
- o Người dùng chọn ở trường “Output Format”:
 - Chọn “Combined (.enc)” để gộp cả key và nội dung file đã mã hóa.
 - Chọn “Separated (.enc + .key)” để tách ra 2 file .enc và .key.
- o Nếu chọn Separated như trên, hệ thống sẽ tách ra 2 file như sau:

cat_20250715_162128.enc	15-Jul-25 4:21 PM	ENC File	81 KB
cat_20250715_162128.key	15-Jul-25 4:21 PM	KEY File	1 KB

- Giao diện cho tính năng chọn định dạng khi giải mã file:

- o Người dùng bắt buộc phải chọn file .enc ở trường “Encrypted File”.
- o Nếu file mã hóa và file chứa khóa tách ra, người dùng chọn Key File ở trường “Key File (optional)”.
- o Sau khi mã hóa file thành công, hệ thống hiển thị thông báo thành công:



17. Khôi phục tài khoản:

- Tính năng cho phép người dùng khôi phục quyền truy cập vào tài khoản trong trường hợp quên passphrase.
- Cơ chế hoạt động:
 - Khi tạo tài khoản, hệ thống tạo ra một mã khôi phục duy nhất. Mã này chỉ hiển thị một lần và yêu cầu người dùng lưu lại mã an toàn; mã này không thể truy xuất lại sau khi thoát khỏi màn hình.
 - Quá trình khôi phục tài khoản:
 - Ở màn hình đăng nhập, người dùng chọn mục “Account Recovery”.
 - Người dùng nhập vào các mục:
 - Email: email tương ứng với tài khoản của người dùng.
 - Recovery Code: mã khôi phục người dùng đã lưu trước đó.
 - New Passphrase: passphrase mới của người dùng.
 - Confirm: xác minh passphrase mới.
 - Sau khi nhập vào các trường hợp lệ, người dùng nhấn “Recover Account” để xác nhận khôi phục tài khoản.
 - Hệ thống cho phép người dùng bảo lưu khóa RSA cũ nếu họ nhập đúng mật khẩu cũ. Nếu để trống ở trường này, khóa RSA cũ sẽ hết hiệu lực.
 - Mã này chỉ có hiệu lực 1 lần, tài khoản này không thể khôi phục nếu mất passphrase được nữa.
 - Giao diện của màn hình khôi phục tài khoản:

Login Register Account Recovery

Use your 16-character recovery code to reset your passphrase.
Warning: This will invalidate your existing RSA keys.

Account Recovery

Email: a@example.com

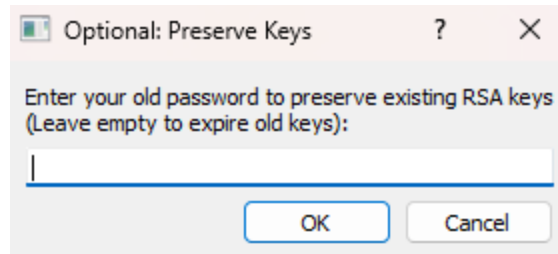
Recovery Code: QEQGTVCCKRU-DDC5-

New Passphrase:

Confirm:

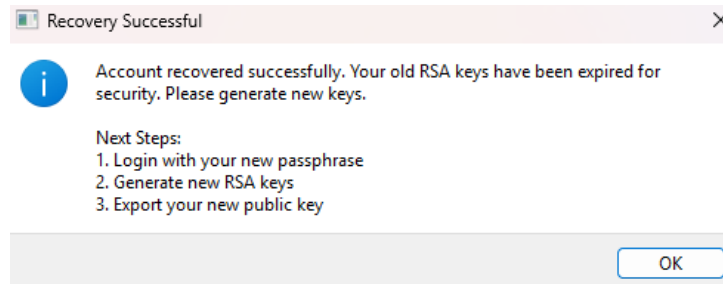
Recover Account

- Khi chọn Recover Account, hệ thống hiển thị thông báo sau:

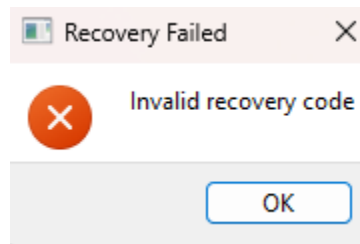


Người dùng nhập mật khẩu cũ để bảo lưu khóa RSA. Nếu không, khóa RSA cũ sẽ hết hiệu lực.

- Sau khi khôi phục tài khoản, hệ thống hiển thị thông báo khôi phục tài khoản thành công:



- Nếu nhập sai mã khôi phục, hệ thống hiển thị thông báo lỗi sau:



3. Tham khảo

- https://en.wikipedia.org/wiki/RSA_cryptosystem
- <https://www.geeksforgeeks.org/computer-networks/rsa-algorithm-cryptography/>
- <https://pypi.org/project/pyotp/>
- https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
- https://en.wikipedia.org/wiki/Galois/Counter_Mode
- <https://www.sqlite.org/docs.html>
- <https://pypi.org/project/qrcode/>
- <https://pypi.org/project/pyzbar/>
- <https://pypi.org/project/cryptography/>
- <https://docs.python.org/3/library/logging.html>
-