|  |  |
| --- | --- |
| **ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH**  **TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN**  **KHOA CÔNG NGHỆ THÔNG TIN** | |
| A blue and white logo  Description automatically generated | |
| **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](#_Toc202610733)

[II. Kiến Trúc Hệ Thống 4](#_Toc202610734)

[1. Sơ đồ modules 4](#_Toc202610735)

[2. Sơ đồ lưu trữ 4](#_Toc202610736)

[3. Sơ đồ UI 5](#_Toc202610737)

[III. Chức Năng 5](#_Toc202610738)

[1. Đăng ký tài khoản người dùng 5](#_Toc202610739)

[2. Đăng nhập & xác thực đa yếu tố (MFA) 6](#_Toc202610740)

[3. Quản lý khóa RSA cá nhân 7](#_Toc202610741)

[4. QR code public key 7](#_Toc202610742)

[5. Cập nhật thông tin tài khoản 8](#_Toc202610743)

[6. Mã hóa tập tin gửi người khác 8](#_Toc202610744)

[7. Giải mã tập tin 10](#_Toc202610745)

[8. Ký số tập tin 10](#_Toc202610746)

[9. Xác minh chữ ký 11](#_Toc202610747)

[10. Phân quyền tài khoản 11](#_Toc202610748)

[11. Ghi Log bảo mật 12](#_Toc202610749)

[12. Chia nhỏ tập tin 12](#_Toc202610750)

[13. Kiểm tra trạng thái khóa 13](#_Toc202610751)

[14. Tìm kiếm public key 13](#_Toc202610752)

[15. Giới hạn đăng nhập 14](#_Toc202610753)

[16. Tùy chọn lưu định dạng lưu file 14](#_Toc202610754)

[17. Khôi phục tài khoản 15](#_Toc202610755)

# **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% |

# **Kiến Trúc Hệ Thống**

### **Sơ đồ modules**

|  |
| --- |
| Secure-Simulation/  ├── data/  │ ├── logs/ # ghi file log  │ ├── test/  │ │ ├── file/ # file test  │ │ └── qrcode/ # qrcode test  │ └── tmp/ # lưu trư tạm file, .png trong code  ├── gui/ # giao diện (PySide6)  ├── modules/  │ ├── account/ # trung gian mã hõa giữa UI trước khi lưu xuống database  │ ├── auth/ # chứng thực tài khoản  │ ├── config/ # cấu hình cơ bản  │ ├── crypto/ # thuật toán mã hóa  │ ├── database/ # cơ sở dữ liệu của chương trình  │ ├── types/ # định nghĩa kiểu dữ liệu  │ └── utils/ # tiện ích chung  ├── main.py  ├── requirement.txt  ├── app.db  └── readme.md |

### **Sơ đồ lưu trữ**

A diagram of a computer

AI-generated content may be incorrect.

### **Sơ đồ UI**

A white rectangular object with black text

AI-generated content may be incorrect.

A diagram of a person

AI-generated content may be incorrect.

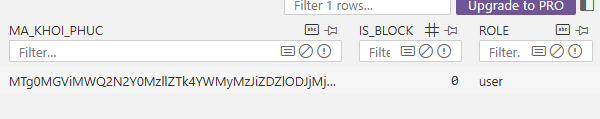
# **Chức Năng**

## **Đăng ký tài khoản người dùng**

|  |  |
| --- | --- |
| **Giao diện** | **File log** |
|  | * Log hành vi:      * Log security: |

* Bảng users trong database:

A group of text boxes

AI-generated content may be incorrect.

* 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

## **Đăng nhập & xác thực đa yếu tố (MFA)**

|  |  |  |
| --- | --- | --- |
|  | **Giao diện** | **Log xác thực** |
| Đăng nhập |  |  |
| OTP |  | * Quá trình gửi OTP:      * Nội dung sau khi gửi OTP: |
| TOTP |  |  |

## **Quản lý khóa RSA cá nhân**

|  |  |
| --- | --- |
| **Giao diện** | **File Log** |
|  | * **Log hành vi người dùng**      * **Log security** |

* 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

## **QR code public key**

|  |  |  |
| --- | --- | --- |
|  | **Giao diện** | **File log** |
| **Tạo QR** |  |  |
| **Đọc QR** |  |  |

## **Cập nhật thông tin tài khoản**

|  |  |
| --- | --- |
| **Giao diện** | **Log file** |
|  | * **Log hành vi**      * **Log security** |

* Kĩ 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

## **Mã hóa tập tin gửi người khác**

|  |  |
| --- | --- |
| **Giao diện** | **Log file** |
|  | * **Log hành vi:**      * **Log security:** |

* Định dạng metadata
  + Gộp file .enc

**A screenshot of a computer

AI-generated content may be incorrect.**

* + Tách file .key
    - File enc

**A screenshot of a computer code

AI-generated content may be incorrect.**

* + - File key

**A screenshot of a computer

AI-generated content may be incorrect.**

* 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

## **Giải mã tập tin**

|  |  |
| --- | --- |
| **Giao diện** | **Log file** |
|  | * **Log security**      * **Log hành vi** |

* 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 chữa bytes rõ của 1 file
  + Nhưng sau mã hóa file mã hóa lớn hơn file gốc vì có chữa thêm AES key và những nội dung được thêm vào nhằm giúp dễ đọc dễ nhận diện file.

## **Ký số tập tin**

|  |  |
| --- | --- |
| **Giao diện** | **Log file** |
|  | * **Log hành vi:**      * **Log security:** |

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

## **Xác minh chữ ký**

|  |  |
| --- | --- |
| **Giao diện** | **Log file** |
|  |  |
|  |  |

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

## **Phân quyền tài khoản**

|  |  |
| --- | --- |
| **Giao diện** | **Log file** |
| **A screenshot of a computer  AI-generated content may be incorrect.** | **A screenshot of a computer screen  AI-generated content may be incorrect.** |

## **Ghi Log bảo mật**

A close up of a text

AI-generated content may be incorrect.

## **Chia nhỏ tập tin**

* **Log tiến trình**

**A screen shot of a computer

AI-generated content may be incorrect.**

* So sánh dung lượng, block đã mã hóa:
  + Dung lương 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.

## **Kiểm tra trạng thái khóa**

**A screenshot of a computer

AI-generated content may be incorrect.**

## **Tìm kiếm public key**

|  |  |
| --- | --- |
| **Giao diện** | **Log file** |
|  |  |
|  |

## **Giới hạn đăng nhập**

|  |  |
| --- | --- |
| **Giao diện** | **Log file** |
|  |  |

## **Tùy chọn lưu định dạng lưu file**

* **Mã hóa**

|  |  |
| --- | --- |
| **Giao diện** | **Log file** |
| **A screenshot of a computer  AI-generated content may be incorrect.** |  |

* **Giải mã**

|  |  |  |
| --- | --- | --- |
|  | **Giao diện** | **Log file** |
| **.enc** |  |  |
| **.enc vs .key** |  |  |

## **Khôi phục tài khoản**

|  |  |
| --- | --- |
| Security.log |  |
| Login.log |  |