**AN NINH MÁY TÍNH**

ĐỒ ÁN 1

C:\Users\tdqua_000\Dropbox\SS-Slides\DeCuong-CDIO\Template CDIO v4.2\Templates\Hinh anh\LogoTruong.png

Khoa Công nghệ thông tin

Đại học Khoa học tự nhiên TP HCM

# Thông tin nhóm:

Các thành viên trong nhóm:

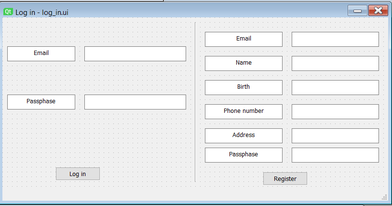
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **STT** | **MSSV** | **Họ và tên** | **Vai trò trong nhóm** | **Phân công** |
| 1 | 19127424 | Triệu Nguyễn Minh Huy | Nhóm trưởng | Làm UI phần log in , register , hash passphase có salt |
| 2 | 19127457 | Nguyễn Tuấn Kiệt |  | Làm hàm tạo session key cho aes , hàm kí chữ kí , hàm sinh khoá private và public |
| 3 | 19127509 | Trương Thế Phú |  | Làm UI phần giải mã và mã hoá file |

# Yêu cầu đồ án:

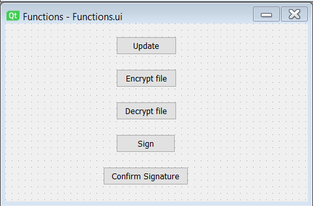
**1. Đăng ký tài khoản người dùng:**

-Ứng dụng cho phép người dùng đăng ký 1 tài khoản với các thông tin: email ,họ tên, ngày sinh, điện thoại, địa chỉ, mật khẩu (passphase). Mật khẩu cần được lưu trữ dưới dạng Hash (SHA 256) có kết hợp với Salt.

-Sử dụng JSON để lưu trữ thông tin người dùng



UI của màn hình log in

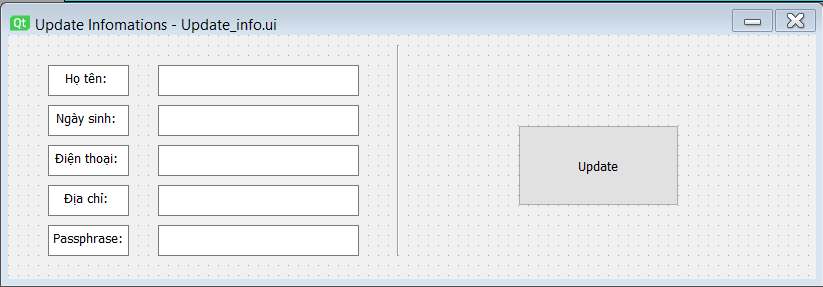


UI của màn hình để thao tác

**2.Phát sinh cặp khoá bất đối xứng:**

-Phát sinh được cặp khóa RSA rồi nhưng chưa mã khóa Kprivate bằng AES

**3. Cập nhật thông tin tài khoản**



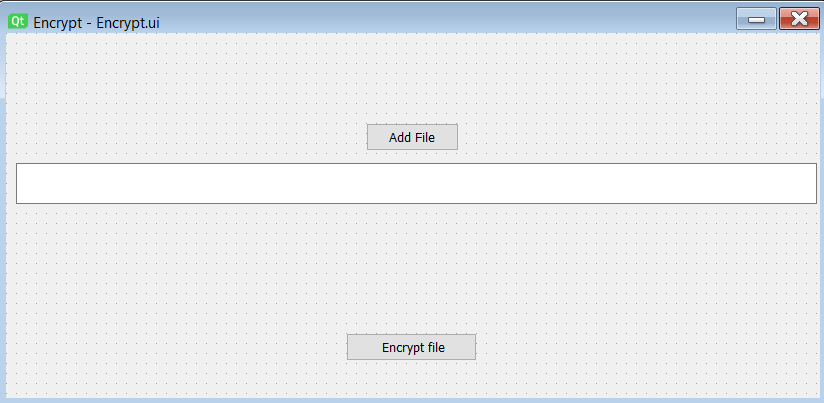
UI cập nhật thông tin tài khoản

-Cho phép cập nhật thông tin tài khoản (họ tên, ngày sinh, điện thoại, địa chỉ, passphase).

**4. Mã hoá tập tin (người gửi mã khoá tập tin và gửi cho người nhận)**

-Cho phép người dùng chọn tập tin cần mã hoá và chọn người nhận (giả sử người nhận là 1 người dùng khác của ứng dụng)

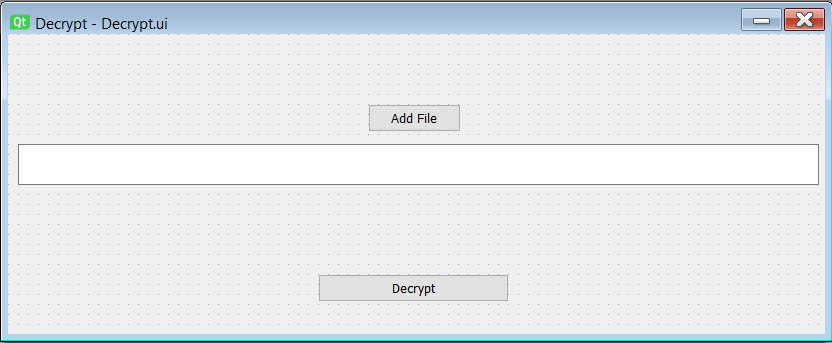
-Nhưng chưa mã hóa được KSession



UI để mã hóa file

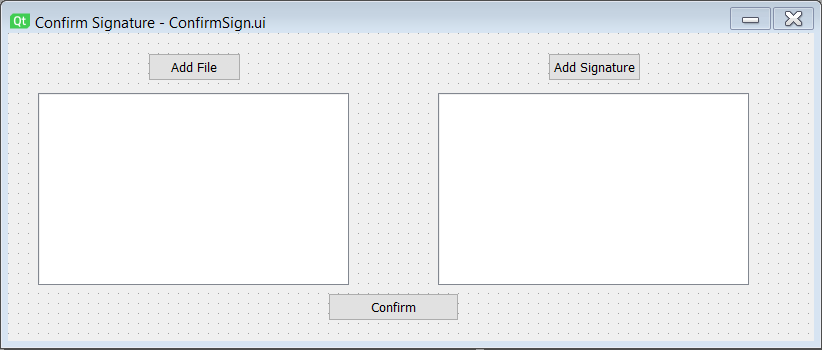
**5. Giải mã tập tin (người nhận nhận tập tin và giải mã)**

-Chưa giải mã ra được file giống với file ban đầu :

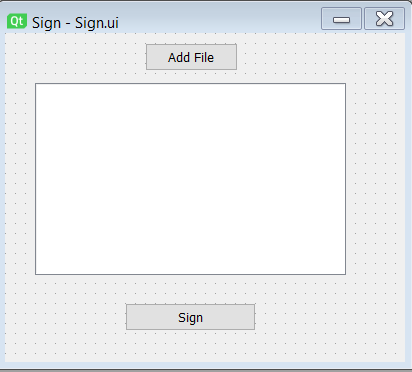


UI để giải mã file

**6. Ký trên tập tin:**



UI của signature

UI chữ ký