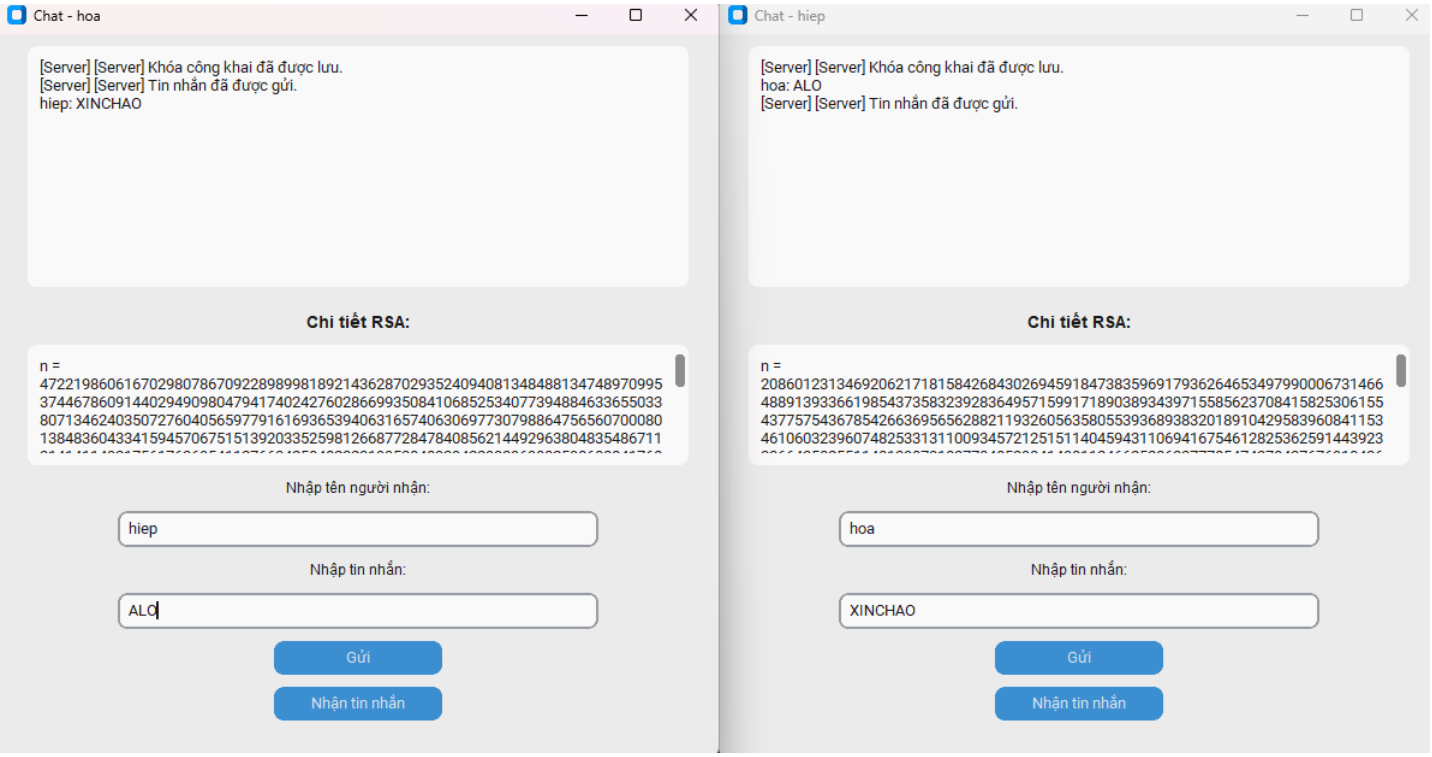
Mô Tả Chi Tiết Ứng Dụng Chat Sử Dụng Hệ Mật RSA

Ứng dụng chat này cho phép người dùng **gửi và nhận tin nhắn bảo mật** thông qua thuật toán **RSA**. Dữ liệu tin nhắn được mã hóa trước khi gửi đi và chỉ có người nhận mới có thể giải mã để đọc tin nhắn.



---

1. Tổng Quan Chức Năng

Ứng dụng được chia thành **client** (giao diện người dùng) và **server** (quản lý tin nhắn và khóa công khai). Chức năng cụ thể bao gồm:

1. **Đăng ký khóa công khai**: Người dùng gửi khóa công khai của mình lên server.
2. **Gửi tin nhắn**:
   - Tin nhắn được mã hóa bằng khóa công khai của người nhận.
   - Server chuyển tin nhắn đã mã hóa đến người nhận.
3. **Nhận tin nhắn**:
   - Người nhận lấy tin nhắn từ server và giải mã nó bằng khóa bí mật của mình.
4. **Quản lý khóa và tin nhắn**: Server lưu trữ khóa công khai và danh sách tin nhắn.

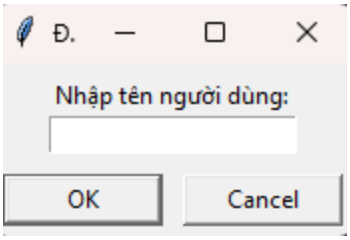
---

2. Thành Phần Chính Của Ứng Dụng

a. Client (File client_gui.py)

Chức năng: Cung cấp giao diện người dùng để gửi và nhận tin nhắn.

- **Giao Diện**:



    - **Khu vực chat**: Hiển thị tin nhắn và thông báo từ server.
    - **Khu vực nhập tin nhắn**:
        - Ô nhập **tên người nhận**.
        - Ô nhập **nội dung tin nhắn**.
    - **Khu vực hiển thị khóa RSA**: Hiển thị thông tin chi tiết về khóa RSA của người dùng (n, e, d).
    - Nút chức năng:
        - **Gửi**: Gửi tin nhắn mã hóa đến người nhận.
        - **Nhận tin nhắn**: Kiểm tra và lấy các tin nhắn mới từ server.
- **Các Chức Năng Chính**:
    - **Sinh khóa RSA**:
        - Khi ứng dụng khởi động, hệ thống tự động tạo **khóa công khai** và **khóa bí mật**.
    - **Đăng ký khóa công khai**:
        - Gửi khóa công khai lên server để chia sẻ với các người dùng khác.
    - **Gửi tin nhắn**:
        - Lấy khóa công khai của người nhận từ server.
        - Mã hóa tin nhắn bằng khóa công khai của người nhận.
        - Gửi tin nhắn đã mã hóa đến server.
    - **Nhận tin nhắn**:
        - Lấy các tin nhắn đã mã hóa từ server.
        - Giải mã tin nhắn bằng khóa bí mật của người dùng.

---

b. Hệ Mật RSA (File He_mat_RSA.py)

Hệ mật RSA được sử dụng để **mã hóa** và **giải mã** tin nhắn.

- **Quy Trình Sinh Khóa**:
    1. Chọn hai số nguyên tố lớn p và q.
    2. Tính $n=p\times q$
    3. Tính $\phi(n)=(p-1)\times(q-1)$
    4. Chọn số e (là số nguyên tố cùng nhau với $\phi(n)$).
    5. Tính d là nghịch đảo modular của e với $\phi(n)$: $e\times d\equiv 1 \pmod{\phi(n)}$.
    6. Kết quả:
        - **Khóa công khai**: (n,e).
        - **Khóa bí mật**: (n,d).
- **Mã Hóa**:
    - Tin nhắn mmm được chuyển đổi thành dạng số thông qua hàm text_to_number.
    - Mã hóa ccc được tính như sau: c=m^e mod n.
- **Giải Mã**:
    - Tin nhắn được giải mã bằng khóa bí mật: m=c^d mod n.
    - Kết quả số được chuyển ngược về văn bản thông qua hàm number_to_text.

---

c. Server (File server_demo.py)

Server đóng vai trò trung tâm để:

- **Lưu trữ khóa công khai**: Khi người dùng đăng ký, server lưu khóa công khai tương ứng với tên người dùng.
- **Lưu trữ tin nhắn**: Tin nhắn được mã hóa và gửi lên server.
- **Quản lý các yêu cầu**:
    1. **REGISTER**: Đăng ký khóa công khai.
    2. **GET_KEY**: Trả về khóa công khai của người dùng khác.
    3. **SEND_MESSAGE**: Lưu tin nhắn đã mã hóa.
    4. **GET_MESSAGES**: Gửi danh sách tin nhắn đã mã hóa của người dùng.

Luồng Dữ Liệu:

- Server nhận các yêu cầu từ client thông qua **socket** và xử lý theo từng loại yêu cầu.
- Server hoạt động theo mô hình **đa luồng**, cho phép xử lý nhiều client cùng lúc.

---

3. Quy Trình Giao Tiếp Giữa Client và Server

Bước 1: Đăng Ký Khóa Công Khai

1. Khi client khởi động, khóa công khai được tạo và gửi lên server.
2. Server lưu khóa công khai của người dùng.

Bước 2: Gửi Tin Nhắn

1. Người gửi chọn tên người nhận và nhập nội dung tin nhắn.
2. Client gửi yêu cầu lấy khóa công khai của người nhận từ server.
3. Sau khi nhận được khóa công khai:
    - Tin nhắn được mã hóa bằng khóa công khai của người nhận.
4. Client gửi tin nhắn đã mã hóa lên server.
5. Server lưu tin nhắn trong danh sách tin nhắn của người nhận.

Bước 3: Nhận Tin Nhắn

1. Người nhận gửi yêu cầu lấy tin nhắn từ server.
2. Server gửi danh sách tin nhắn đã mã hóa đến client.
3. Client giải mã tin nhắn bằng khóa bí mật của mình và hiển thị nội dung tin nhắn.

---

4. Ví Dụ Minh Họa

Người dùng "hoa" gửi tin nhắn "ALO" cho "hiep":

1. **hoa** khởi động ứng dụng và gửi khóa công khai lên server.
2. **hoa** nhập tên người nhận là "hiep" và nội dung tin nhắn "ALO".
3. **hoa** yêu cầu khóa công khai của "hiep" từ server.
4. **hoa** mã hóa tin nhắn "ALO" thành dạng số và gửi tin nhắn đã mã hóa đến server.
5. Server lưu tin nhắn vào danh sách của "hiep".

6. Khi **hiep** nhận tin nhắn, tin nhắn được giải mã thành "ALO".

---

5. Kết Luận

Ứng dụng chat này đảm bảo **tính bảo mật** và **riêng tư** nhờ vào hệ mật RSA:

- **Tin nhắn được mã hóa**: Chỉ người nhận có khóa bí mật mới giải mã được tin nhắn.
- **Quản lý khóa công khai**: Server đóng vai trò trung gian để chia sẻ khóa công khai giữa các người dùng.
- **Giao diện thân thiện**: Người dùng dễ dàng gửi và nhận tin nhắn thông qua giao diện đồ họa.