ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC

XÂY DỰNG ỨNG DỤNG CHAT AN TOÀN

Nhóm:

- Lý Văn Chản
- Nguyễn Ngọc Khánh

Giáo viên hướng dẫn: Trung tá, GV, TS. Cao Văn Lợi

Mục Lục

(3/36) Bảng phân công nghiệm vụ

Phân công	Công việc
Làm chung	• Thảo luận tìm hiểu lý thuyết tổng quan về các loại mã hóa. • Tìm hiểu tổng quan về mã hóa RSA • Thảo luận xây dựng hệ thống chat an toàn.
Lý Văn Chản	• Phụ trách backend
Nguyễn Ngọc Khánh	• Phụ trách frontend

(4/36) Lý do chọn đề tài

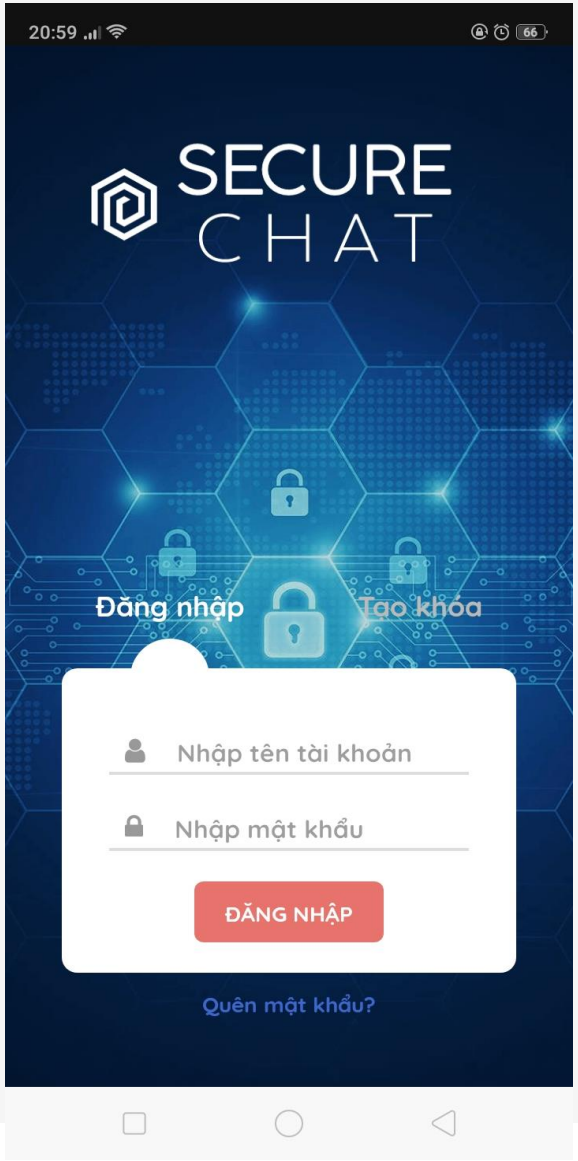
Tầm quan trọng của bảo mật thông tin ngày nay.

Nhu cầu trao đổi thông tin qua mạng internet ngày càng tăng

Thông tin trên internet rất dễ bị các hacker đánh cắp.

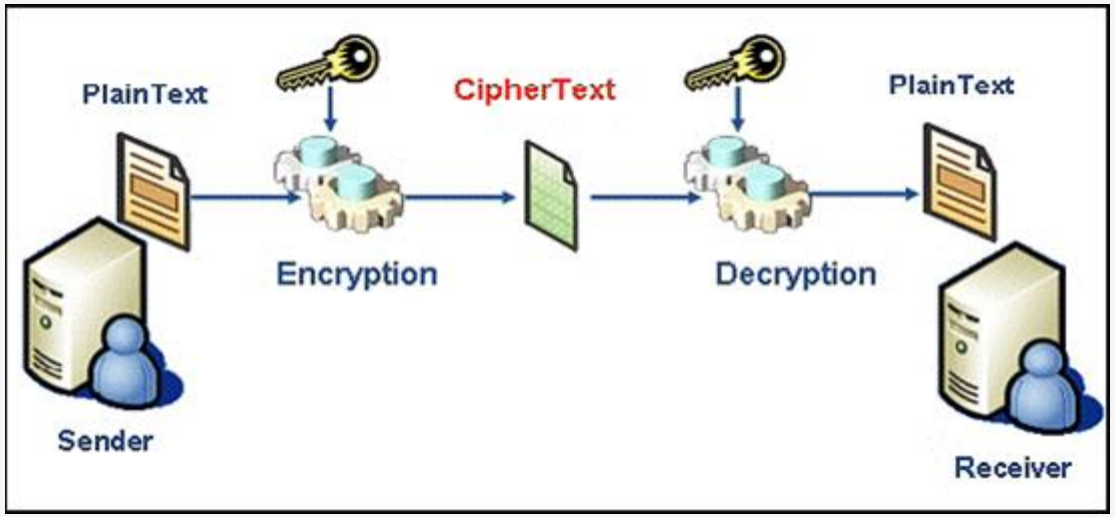
(5/36) Mục tiêu đề tài

Xây dựng một app chat bảo mật hoàn chỉnh



(6/36) Tổng quan về mã hoá bảo mật thông tin

Mã hóa là một thuật toán nhằm biến đổi thông tin từ dạng rõ sang dạng mờ



(7/36) Phân loại các phương pháp mã hóa

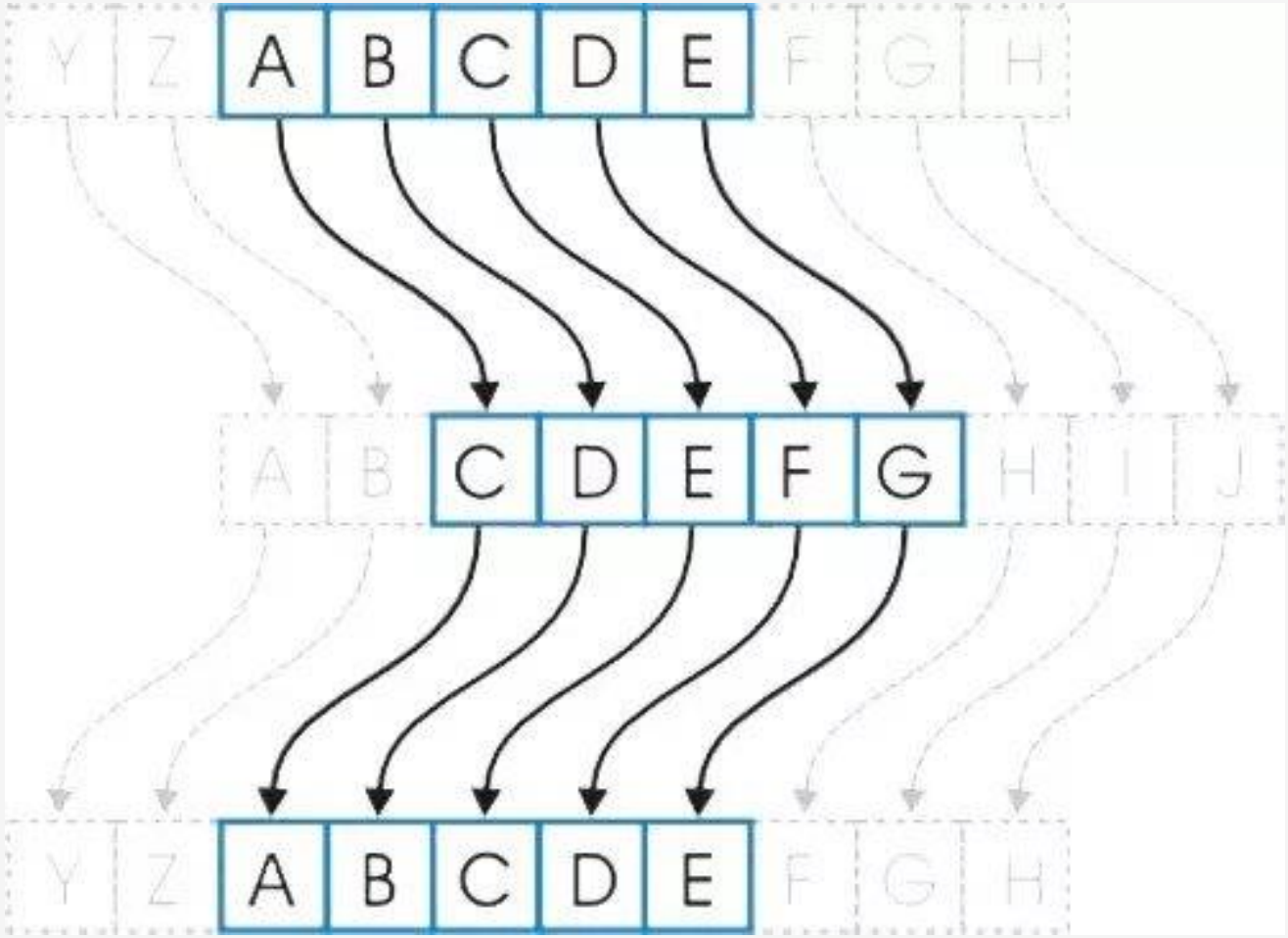
- Mã hóa cổ điển
- Mã hóa một chiều
- Mã hóa đối xứng
- Mã hóa bất đối xứng

(8/36) Mã hóa cổ điển

A mã hóa thông tin bằng thuật toán, và bên B giải mã thông tin, dựa vào thuật toán của bên A.

Độ an toàn của mã hoá sẽ chỉ dựa vào độ bí mật của thuật toán

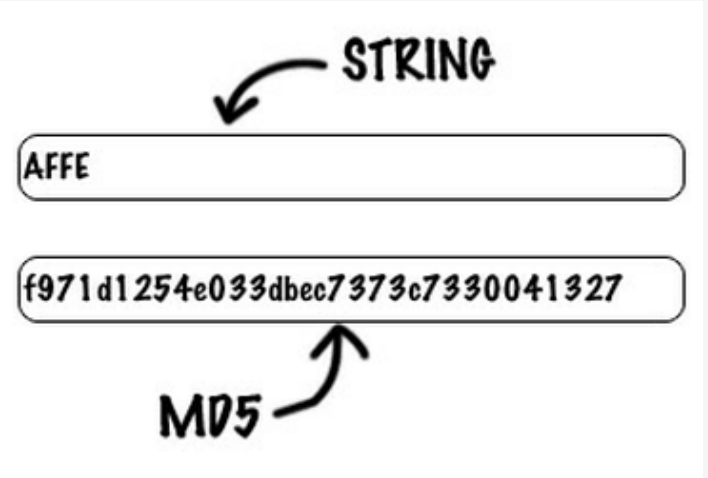
Một ví dụ về phương pháp mã hóa cổ điển: Giả sử ta mã hóa bằng cách thay đổi một kí tự trong chuỗi cần mã hóa thành kí tự liền kề (“Di hoc ve” thành “Ek ipd xg”). Thì bất cứ người nào, chỉ cần biết cách ta mã hóa, đều có thể giải mã được.



(9/36) Mã hóa một chiều

Chỉ có thể mã hóa chứ không thể giải mã

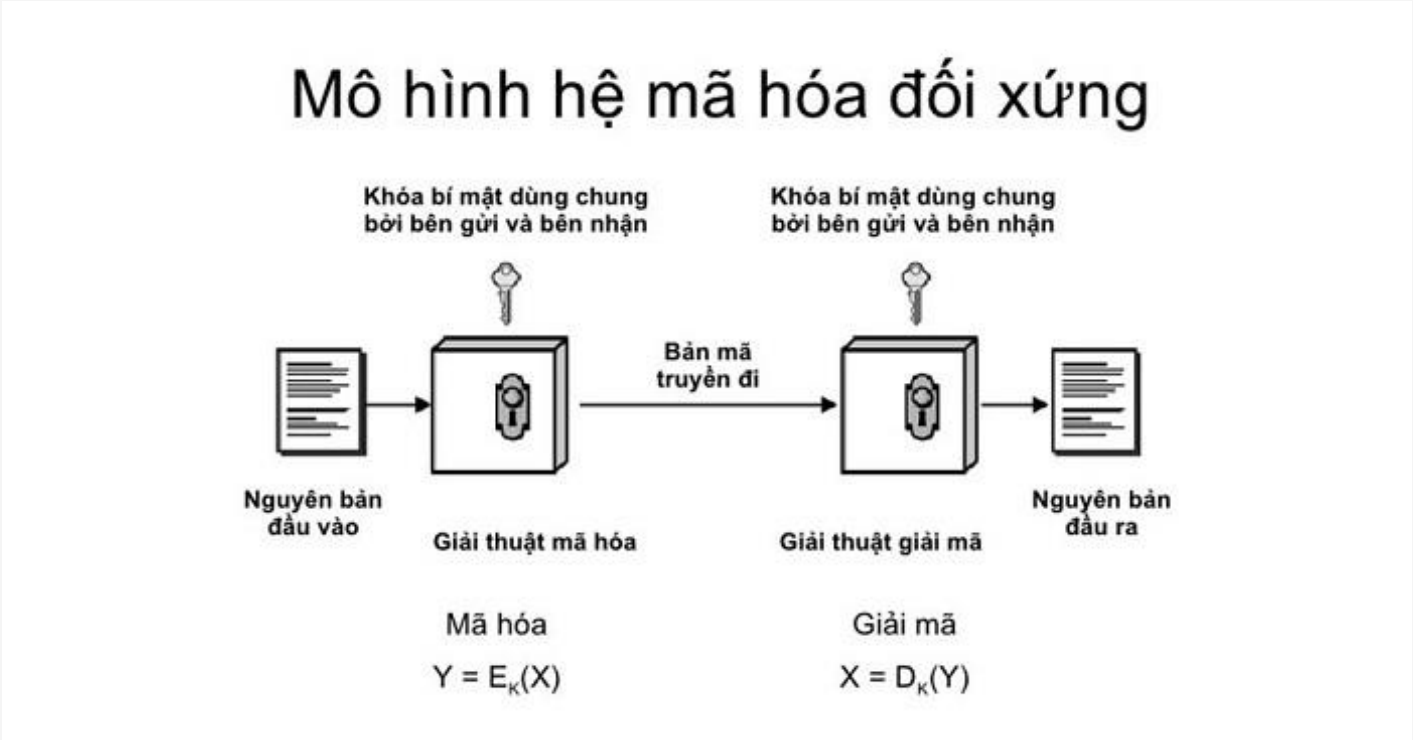
Sử dụng một hàm băm (hash function) để biến một chuỗi thông tin thành một chuỗi hash có độ dài nhất định.



(10/36) Mã hóa đối xứng

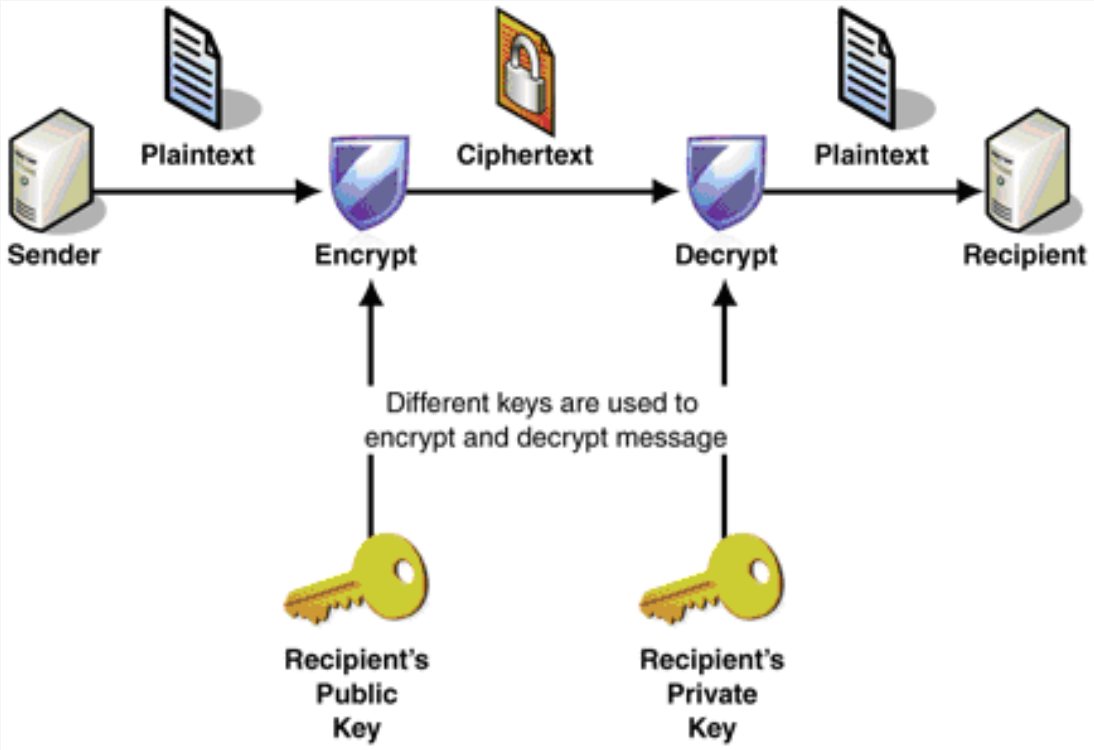
Mã hóa đối xứng (Hay còn gọi là mã hóa khóa bí mật)

Sử dụng cùng một secret key để mã hóa và giải mã



(11/36) Mã hóa bất đối xứng

Mã hóa bất đối xứng (Hay còn gọi là mã hóa khóa công khai) là phương pháp mã hóa mà key mã hóa và key giải khác nhau.



(12/36) Tổng quan về hệ mã hoá RSA

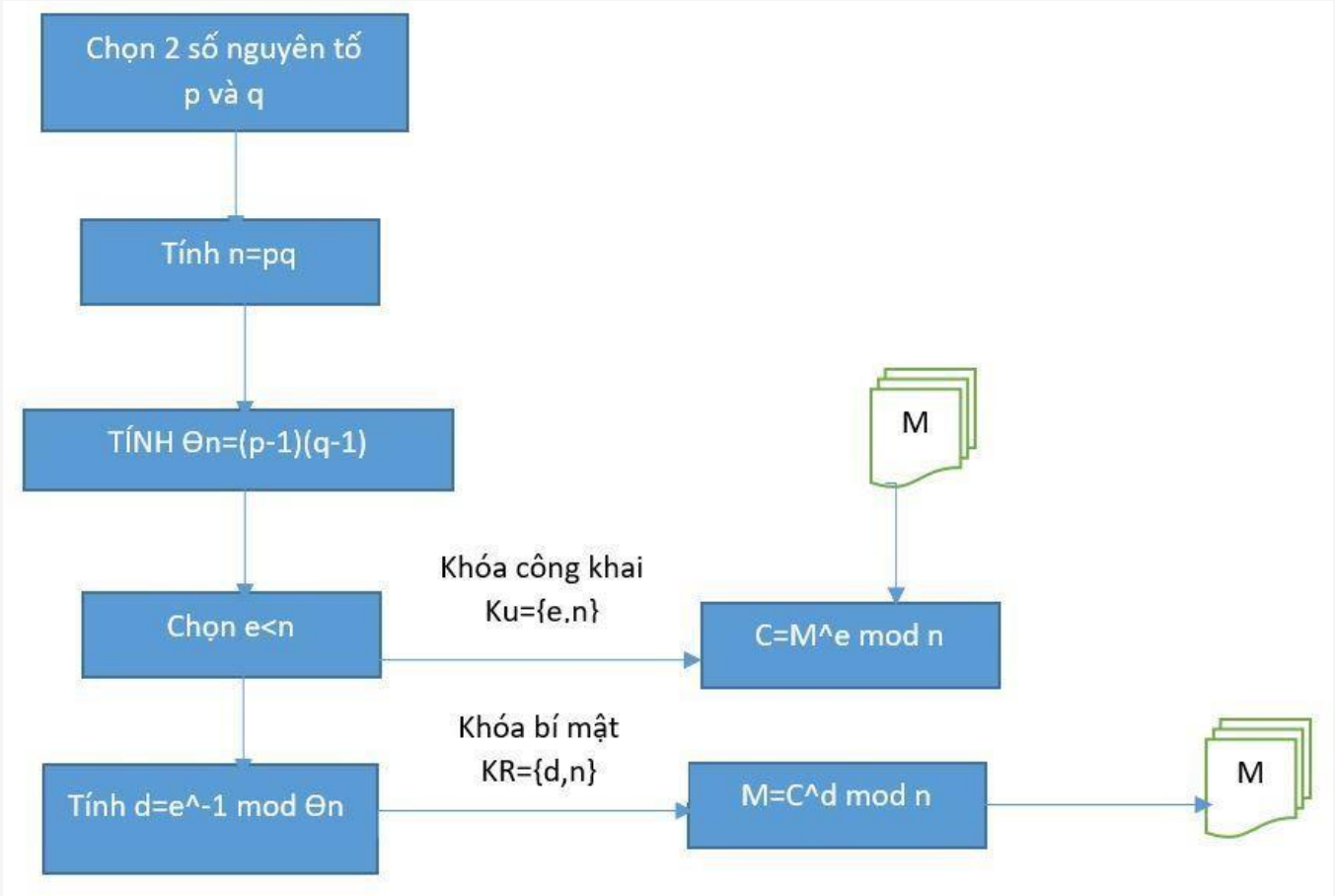
Thuật toán được Ron Rivest, Adi Shamir và Len Adleman mô tả lần đầu tiên vào năm 1977 tại Học viện Công nghệ Massachusetts (MIT). Tên của thuật toán lấy từ 3 chữ cái đầu của tên 3 tác giả.

Thuật toán RSA được MIT đăng ký bằng sáng chế tại Hoa Kỳ vào năm 1983 (Số đăng ký 4.405.829). Bằng sáng chế này hết hạn vào ngày 21 tháng 9 năm 2000.

Thuộc loại mã hoá bất đối xứng.

(13/36) Tạo Khoá

Quy trình tạo khoá, mã hoá và giải mã RSA



(14/36) Nhược điểm

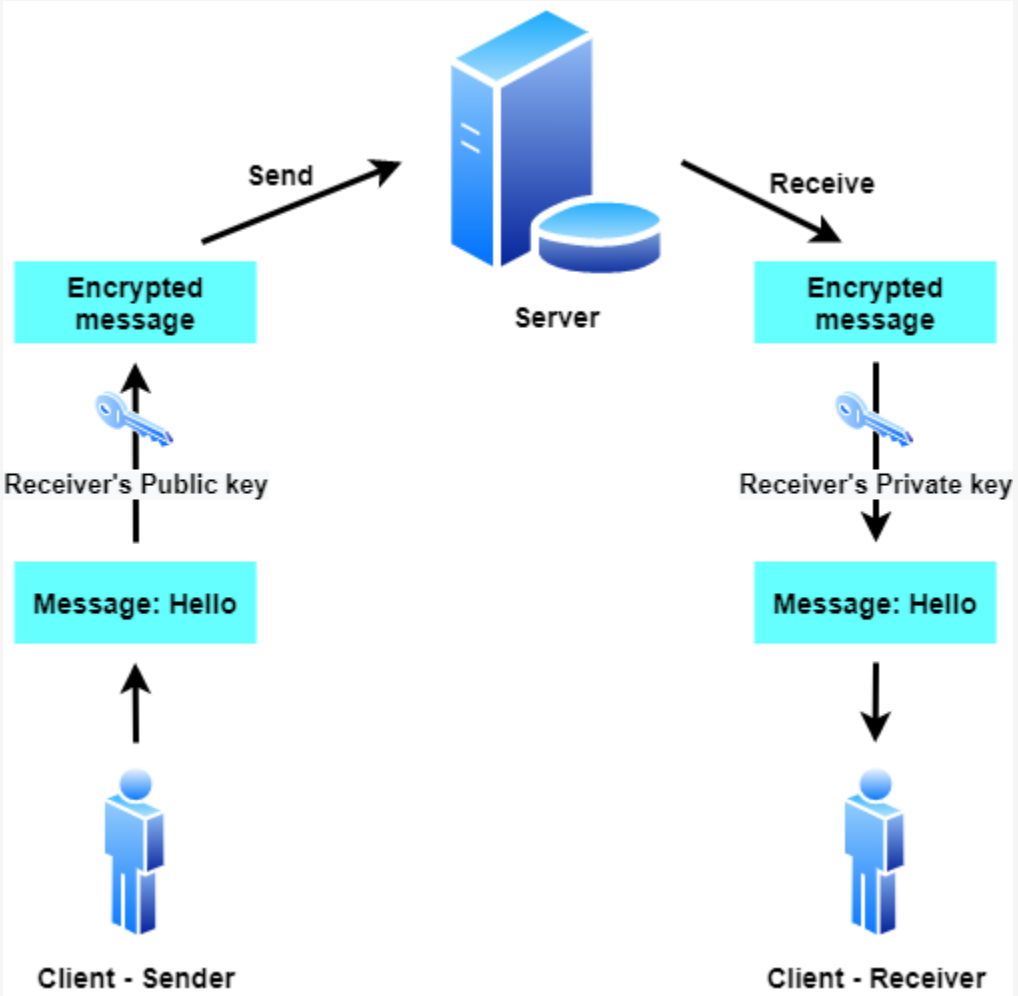
Năm 2010, các nhà khoa học thuộc Đại học Michigan đã công bố phát hiện một kẽ hở trong hệ thống mật mã hoá RSA. Cách phá vỡ hệ thống, lấy khoá bí mật RSA 1024 bit chỉ trong vài ngày thay vì vài năm nếu tấn công theo cách thông thường - tấn công bằng brute force (dò tìm lần lượt). Các nhà khoa học tạo một điện thế lớn để gây lỗi hệ thống, từ đó giúp tìm ra khoá bí mật. Việc tấn công được thực hiện trên một FPGA. Báo cáo được trình bày tại hội nghị DATE 2010 diễn ra tại Dresden, Đức tháng 3 năm 2010.

(15/36) Các cách khắc phục nhược điểm trên:

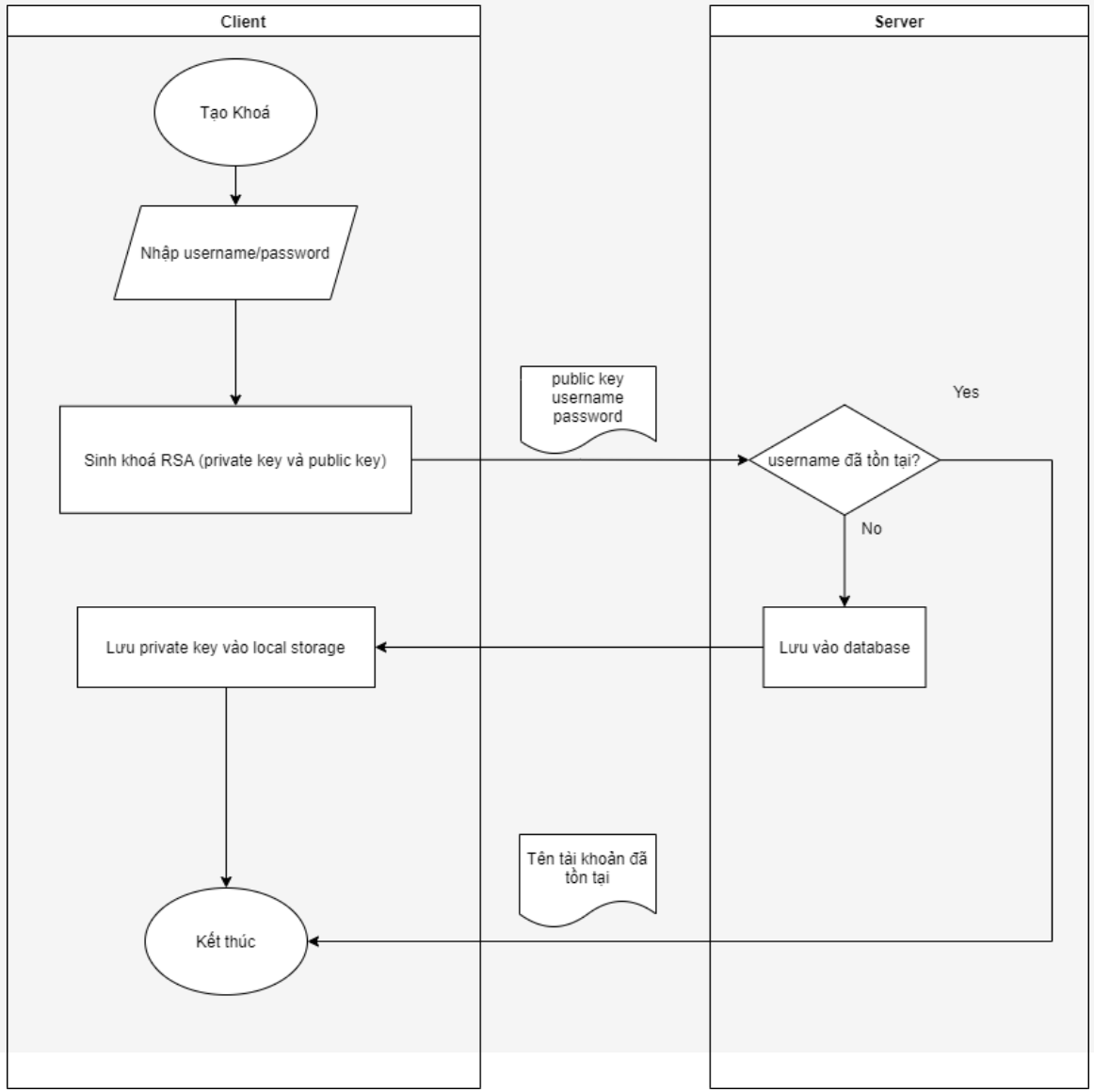
Gợi ý người dùng reset cặp khoá định kỳ, đương nhiên các tin nhắn cũ sẽ không thể giải mã được nữa, tuy nhiên người dùng có thể chọn phương án backup dữ liệu về local hoặc người dùng có thể mã hoá toàn bộ tin nhắn cũ với cặp key mới và chuyển về cho server, quá trình này sẽ khá mất thời gian.

(16/36) Tổng quan về hệ thống chat an toàn

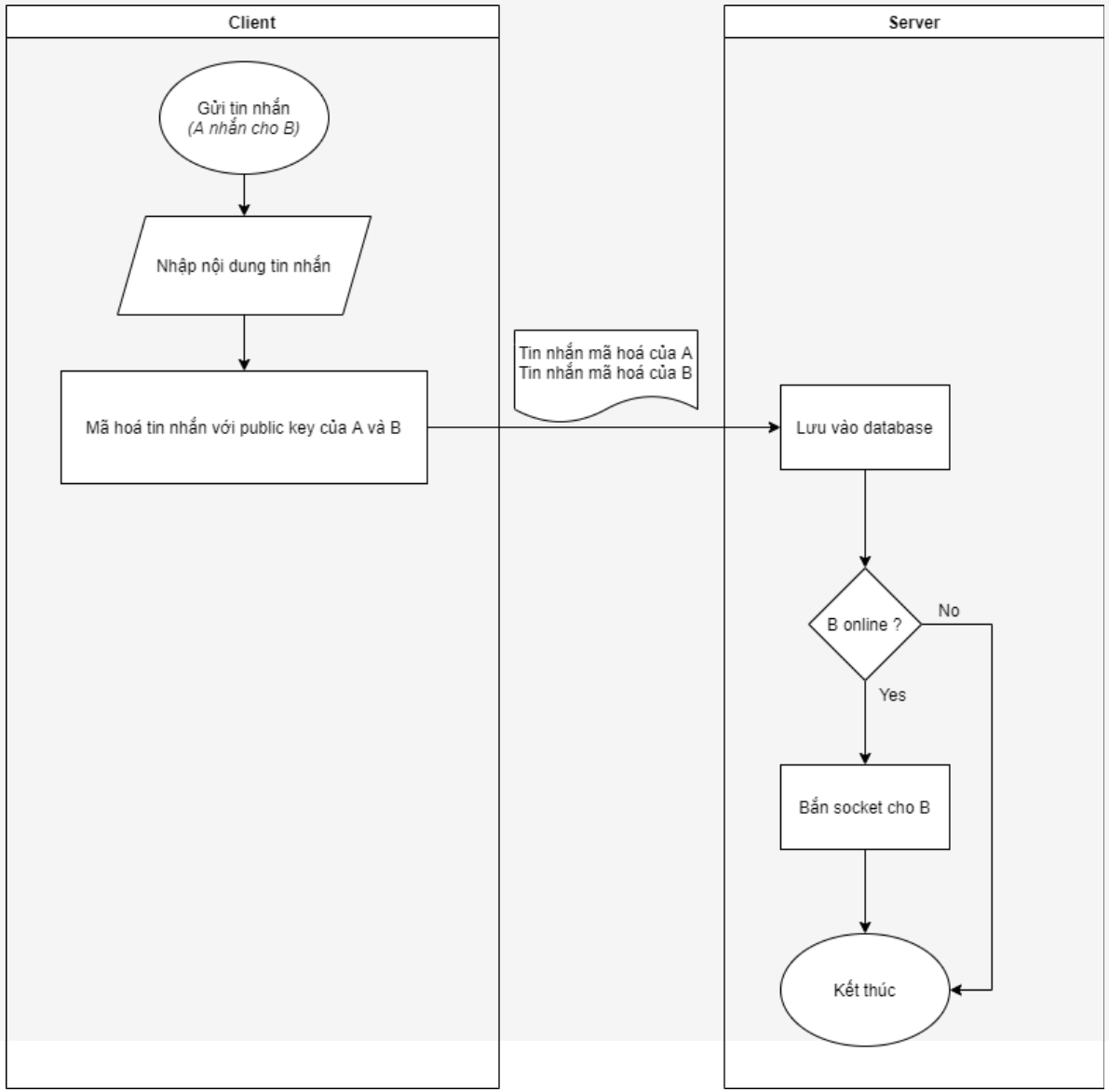
Trong hệ thống, mỗi user sẽ là một client, giao tiếp với nhau bằng websocket thông qua server. Mỗi khi gửi tin nhắn, tin nhắn phải được mã hoá bằng public key rồi mới được gửi đi thông qua server. Khi đến người nhận muốn tin nhắn về dạng đọc được thì cần phải sử dụng private key để giải mã mới có thể đọc được



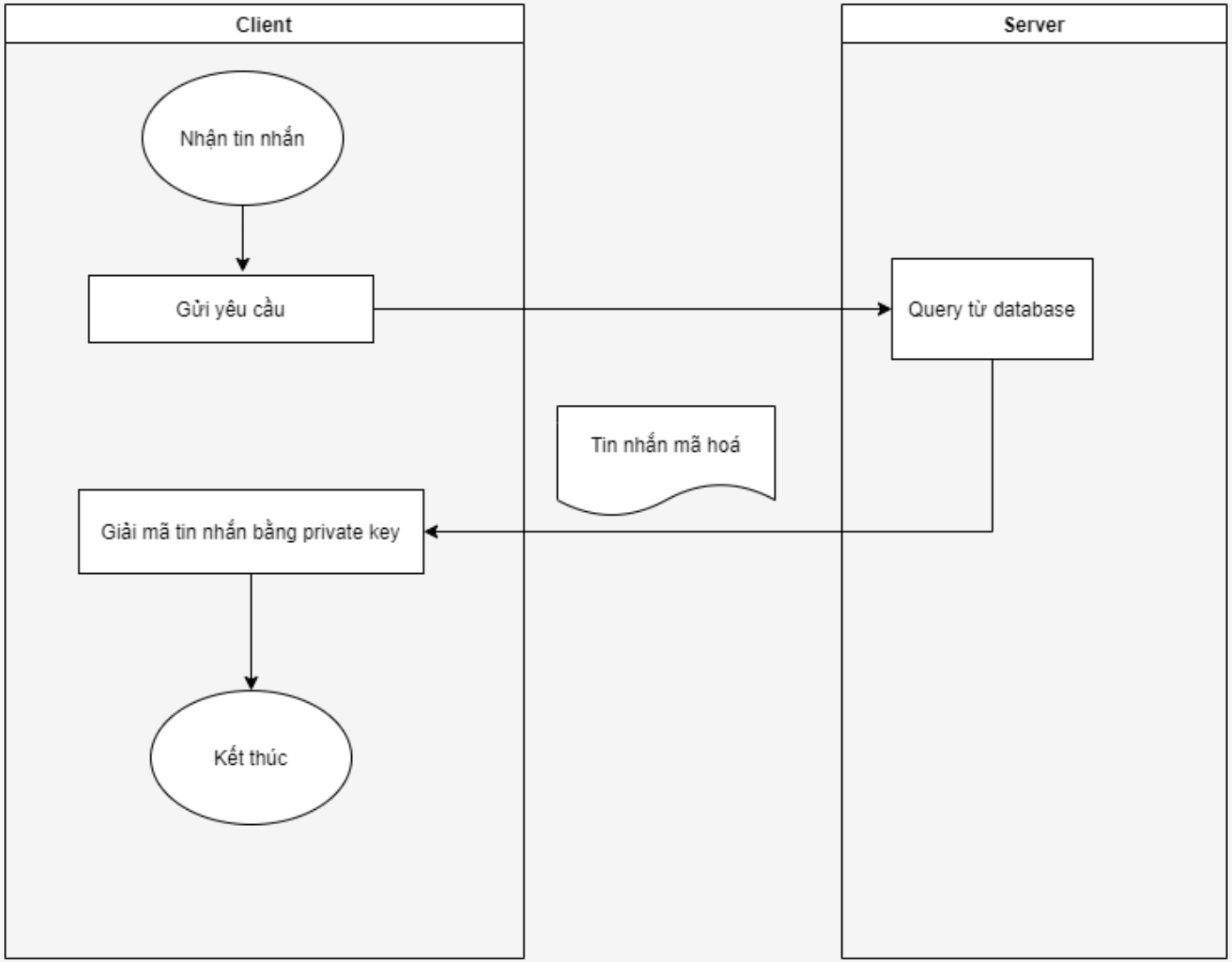
(17/36) Quy trình tạo khoá



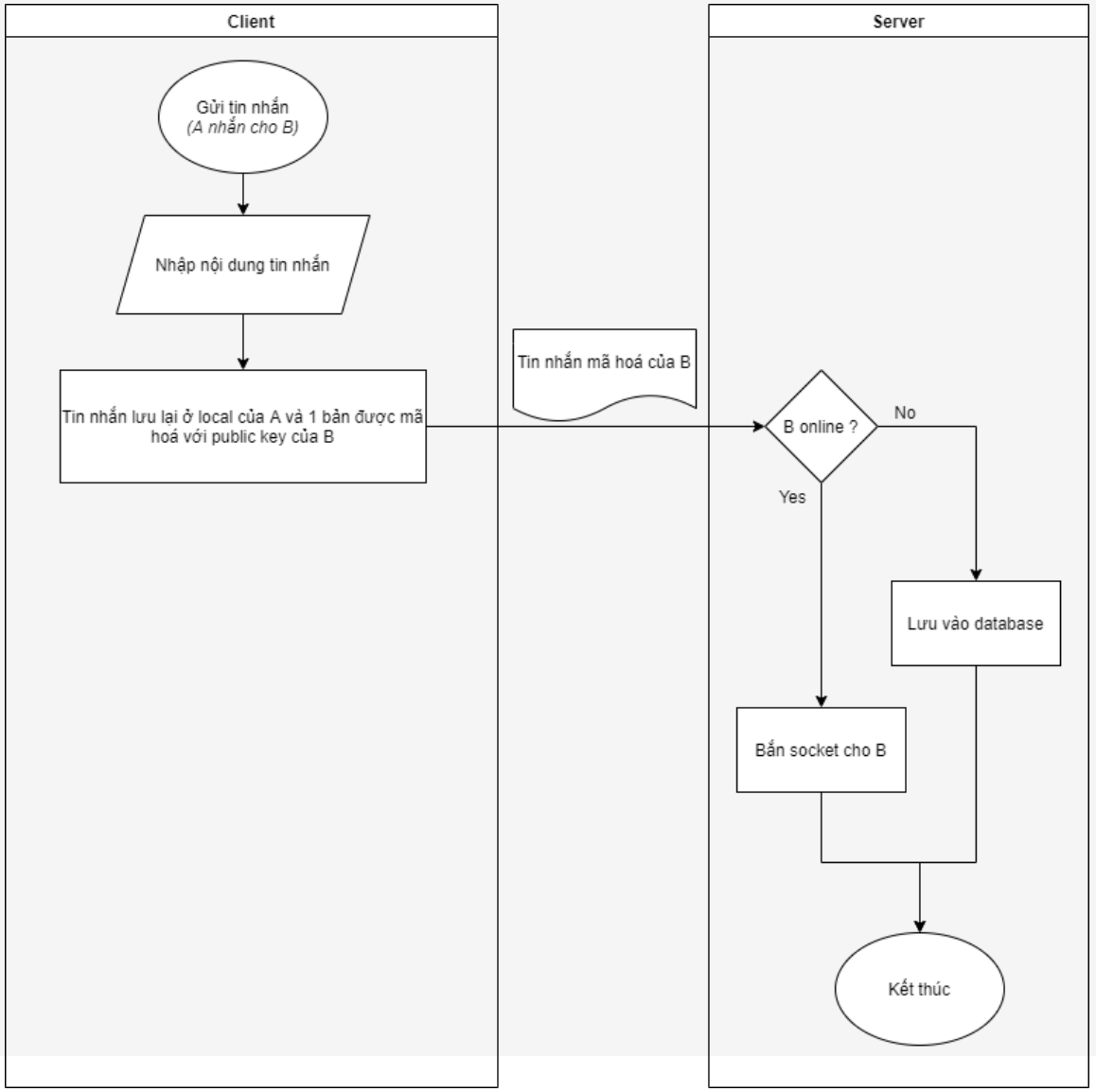
(18/36) Quy trình gửi tin nhắn lưu ở server



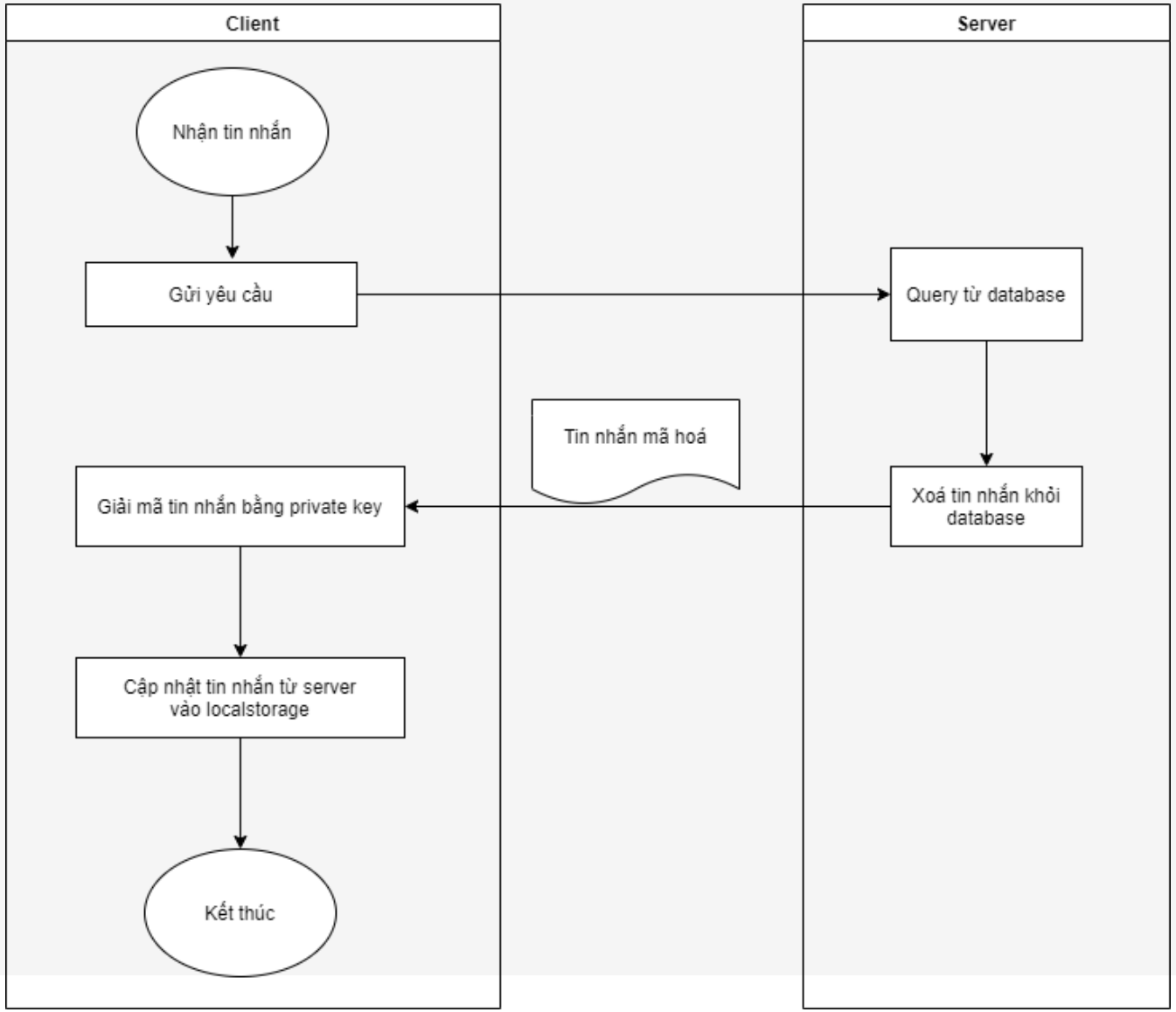
(19/36) Quy trình nhận tin nhắn lưu ở server



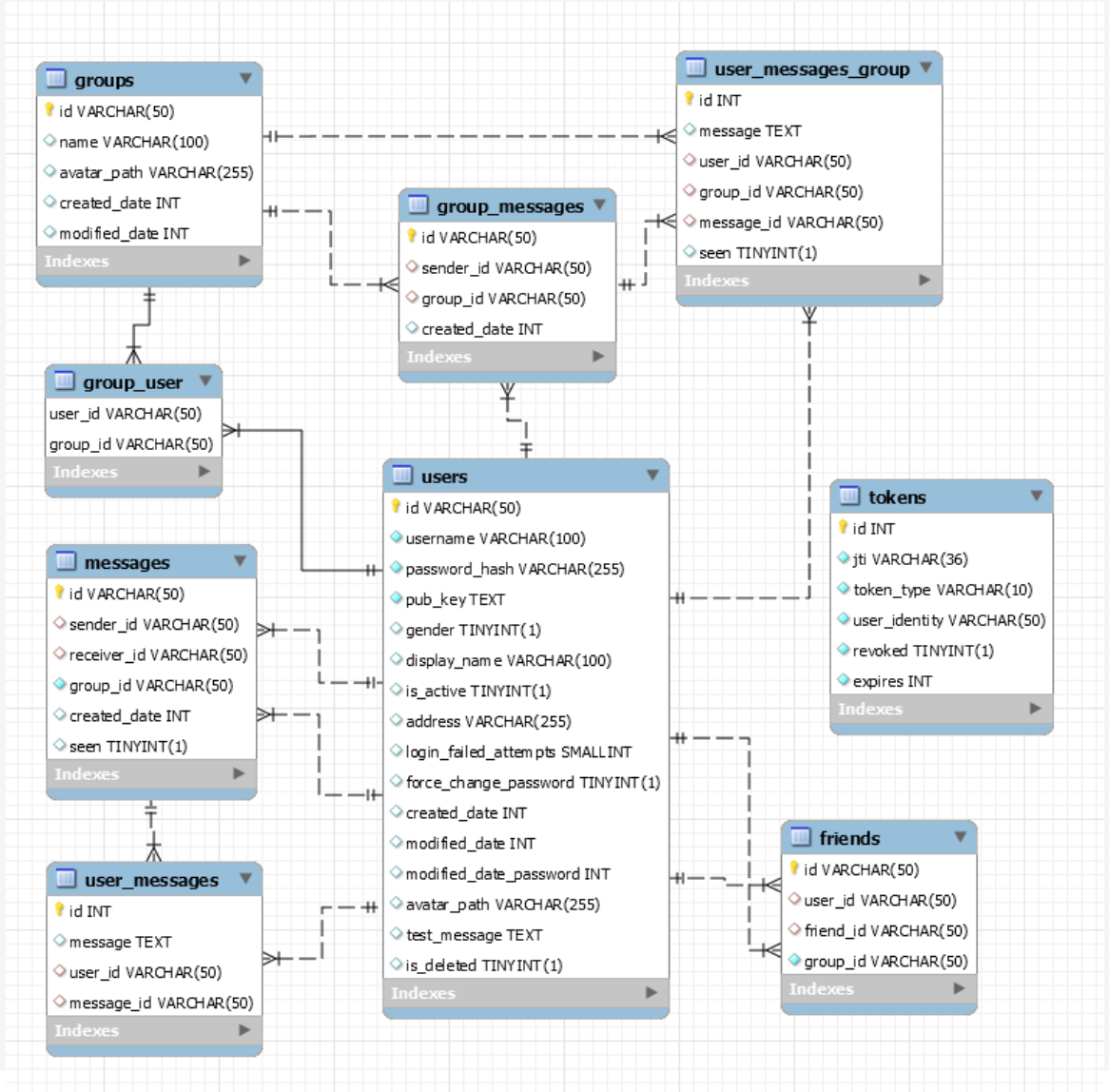
(20/36) Quy trình gửi tin nhắn lưu ở client



(21/36) Quy trình nhận tin nhắn lưu ở client



(22/36) Mô hình Quan hệ



(23/36) Tổng quan về Backend

Link repo github: https://github.com/mountain-chan/secure-chat-backend

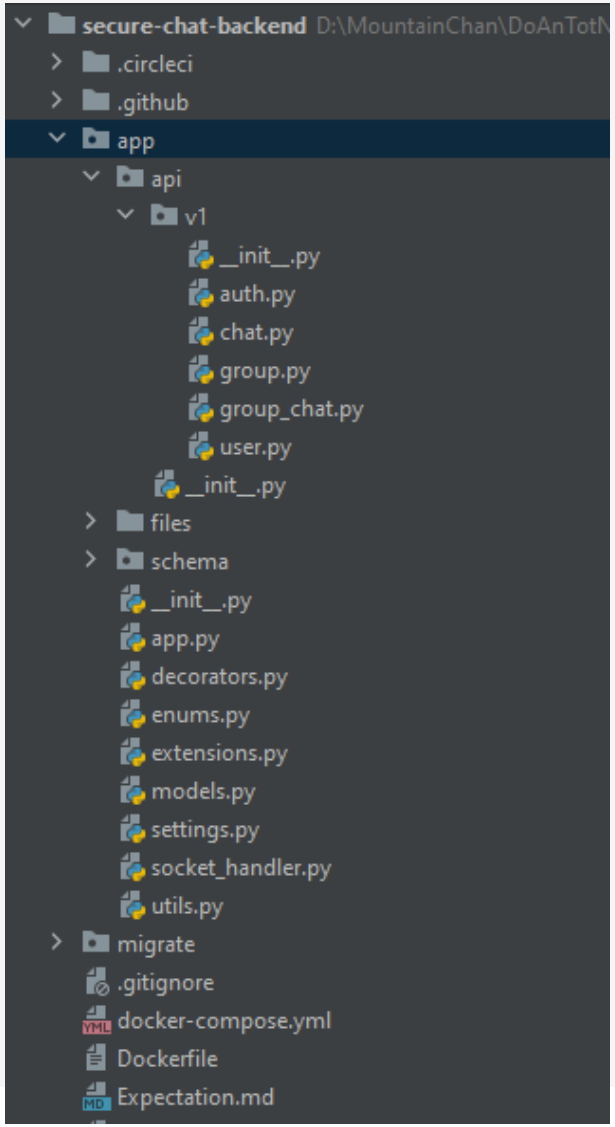
Sử dụng Python 3.7

Database server: Mysql 8.0

Các thư viện chính sử dụng:

- Flask
- Flask-sqlalchemy
- Flask-SocketIO

Hỗ trợ build bằng docker



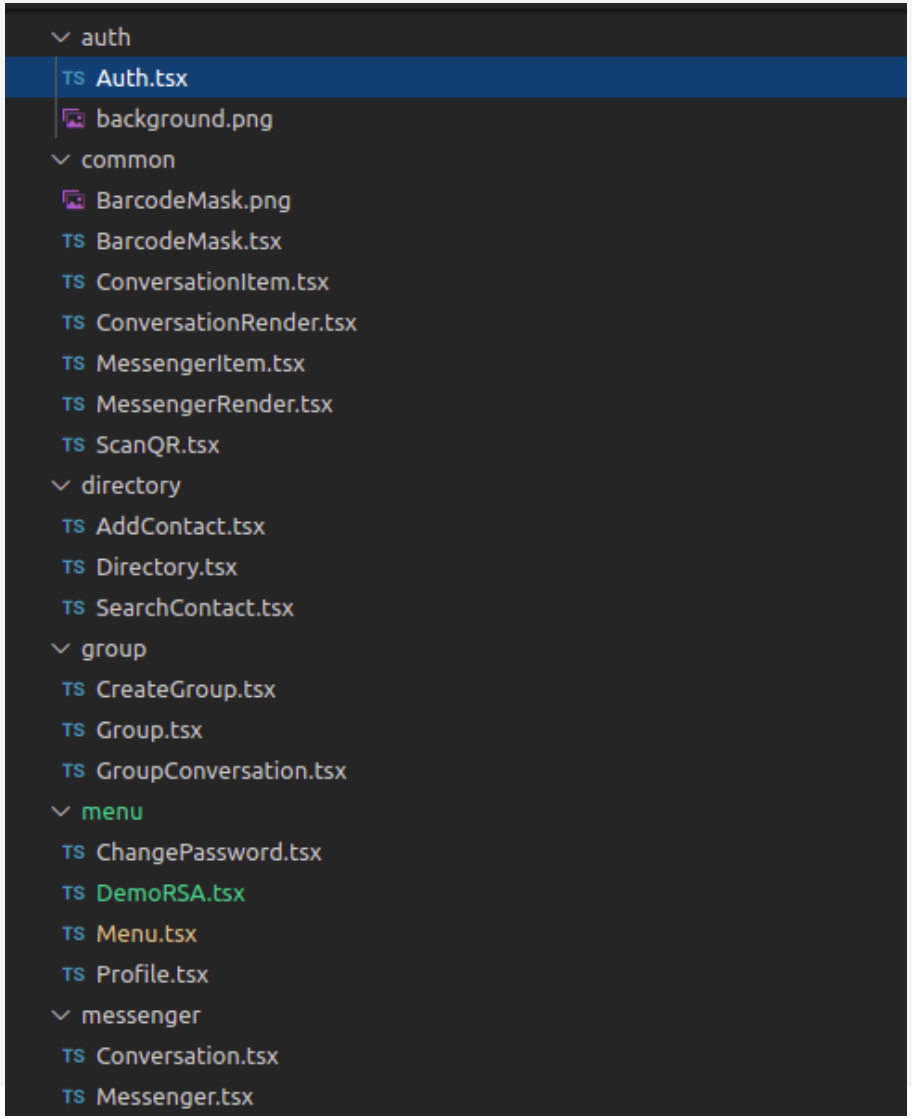
(24/36) Tổng quan về frontend

Link repo github: https://github.com/WHKnightZ/RN-Secure-Chat

Sử dụng React Native - expo

Các thư viện chính sử dụng:

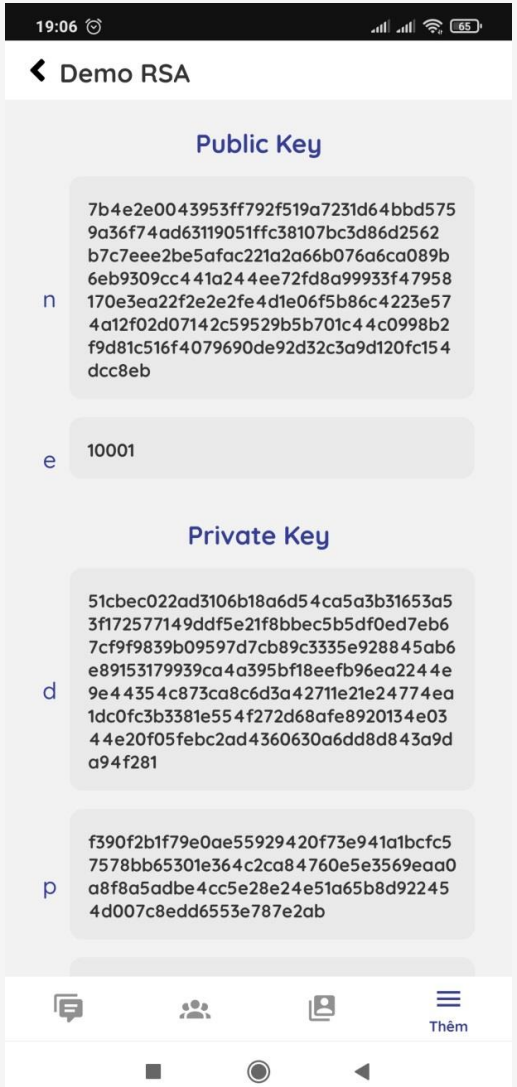
- expo
- socket.io-client

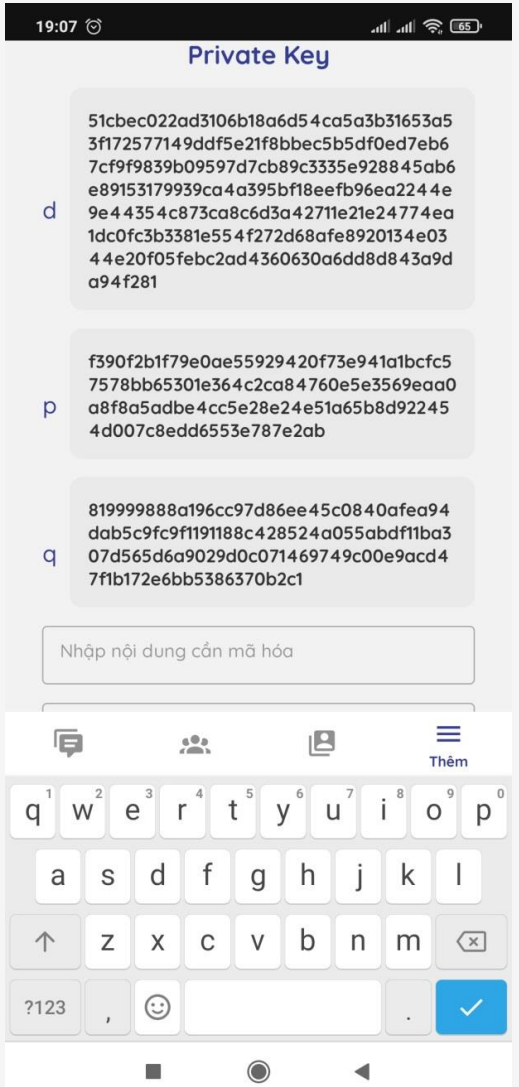


(25/36) Hàm sinh khoá công khai và khoá bí mật

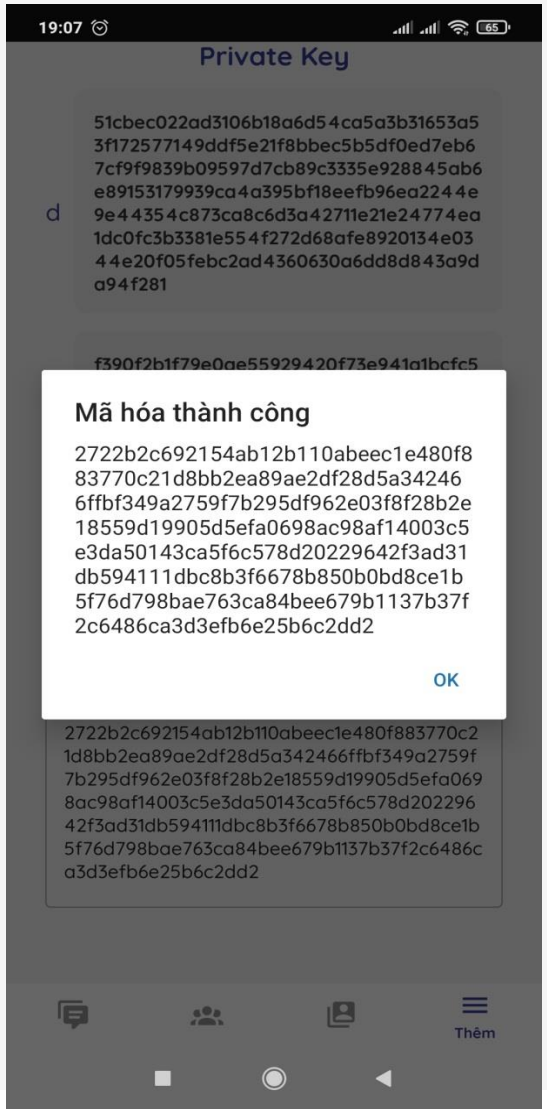
```
export const registerAction = async (dispatch: any, payload: any) => {
  const { username, password } = payload;

  const bits = 1024;
  // 65537 is commonly used as a public exponent in the RSA cryptosystem.
  // Because it is the Fermat number Fn = 2^(2^n) + 1 with n = 4
  const exponent = '10001'; // 0x10001 => 65537
  rsa.generate(bits, exponent);
  const { publicKey, privateKey } = getKey();
  const testMessage = rsa.encrypt('SC');

  const response: any = await callApi({
    api: rest.register(),
    method: 'post',
    body: { username, password, pub_key: publicKey, test_message: testMessage },
  });
  const { status } = response;
  if (status) {
    await AsyncStorage.setItem(`${username}-private`, privateKey);
    await loginAction(dispatch, { username, password });
```

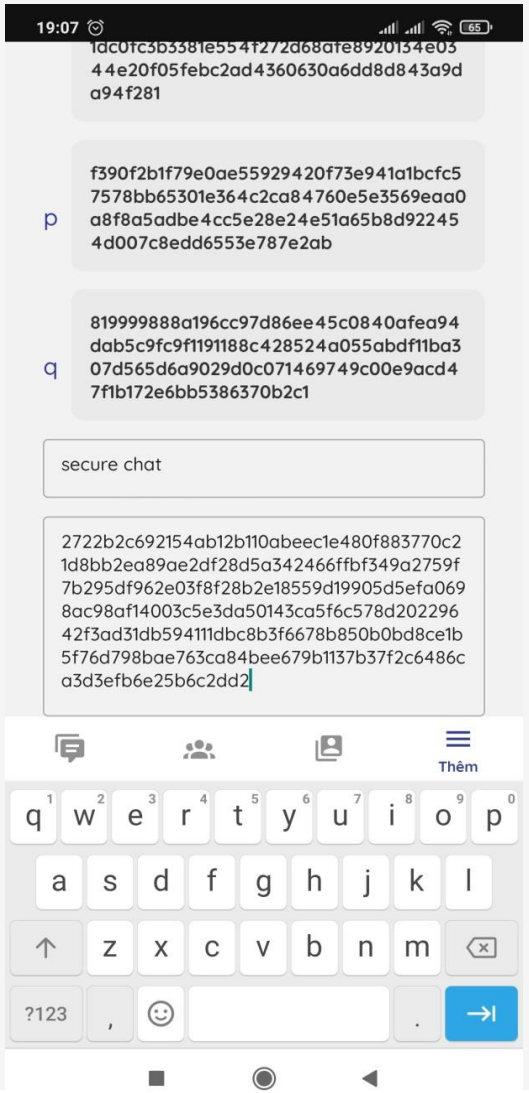
(26/36) Demo mã hoá và giải mã RSA



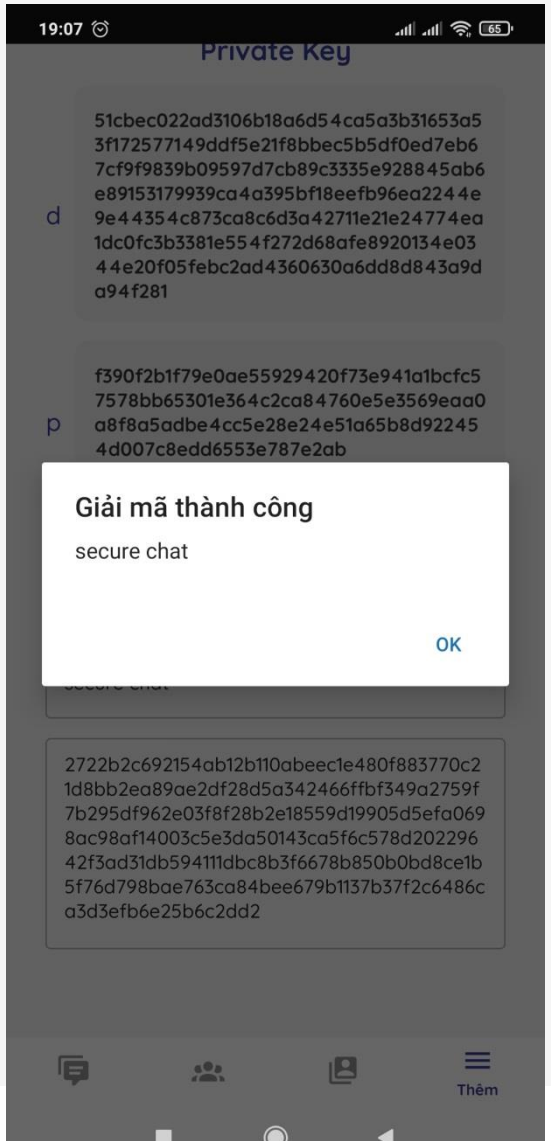


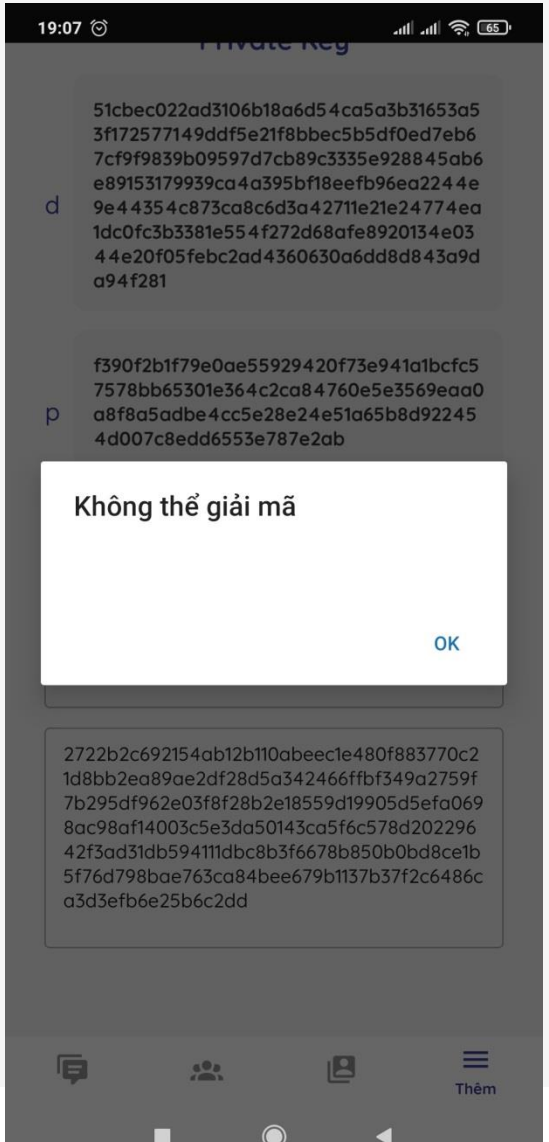
(27/36) Hiển thị chuỗi sau khi đã mã hoá



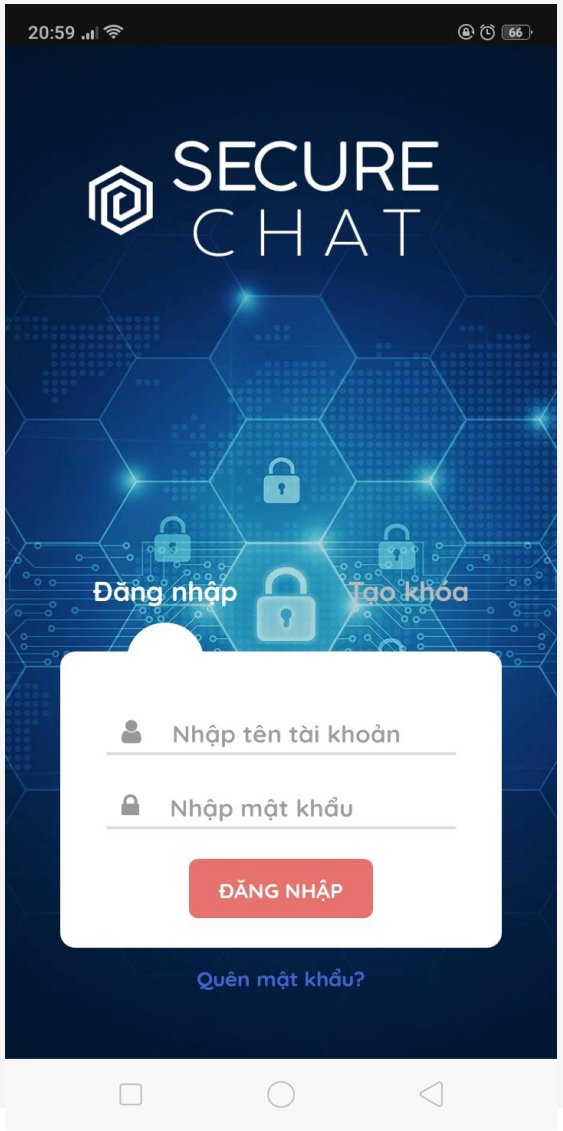


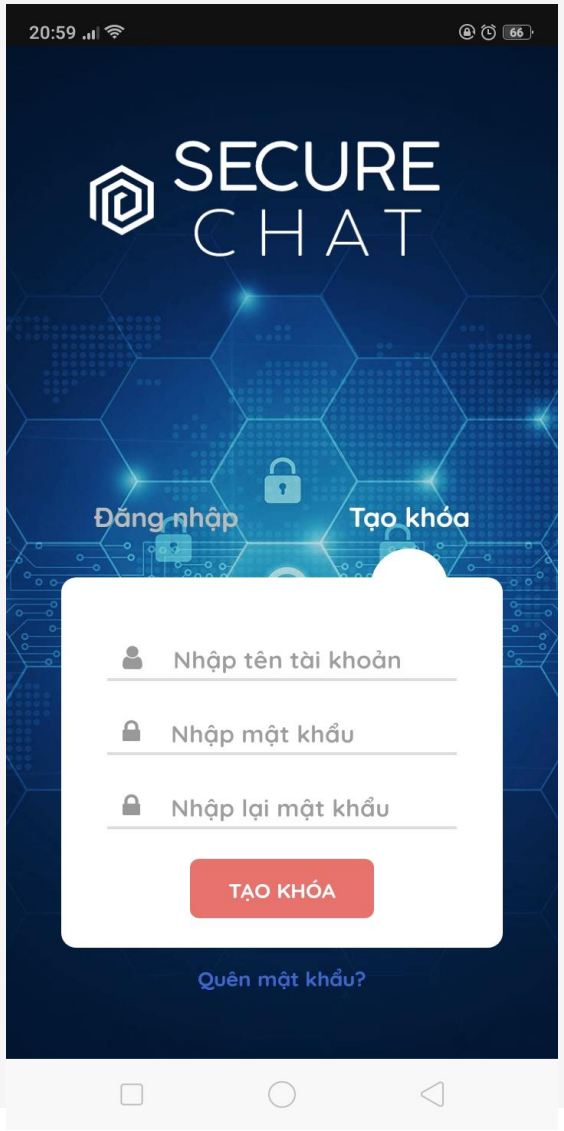
(28/36) Màn hiển thị kết quả giải mã



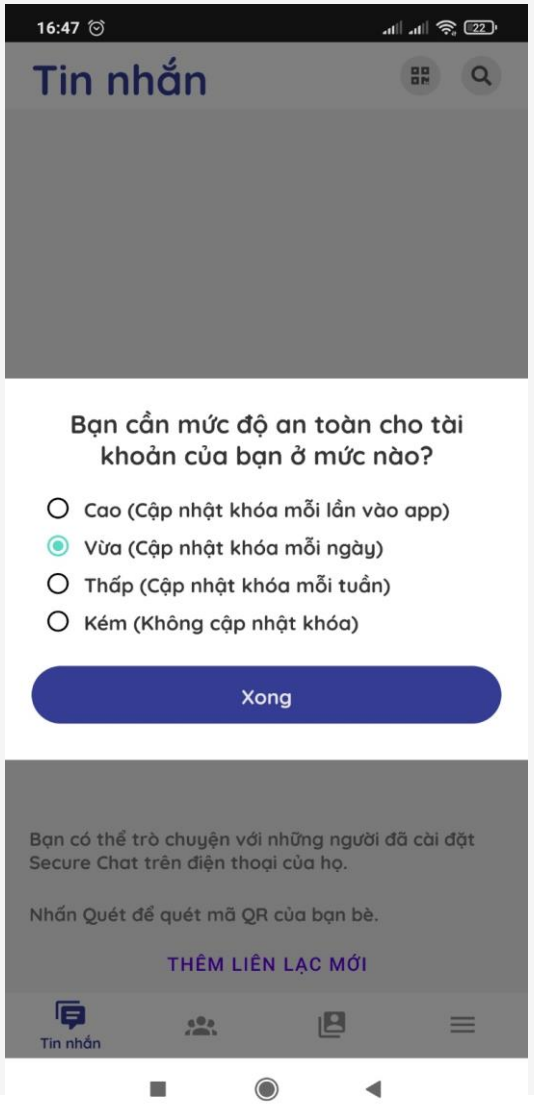


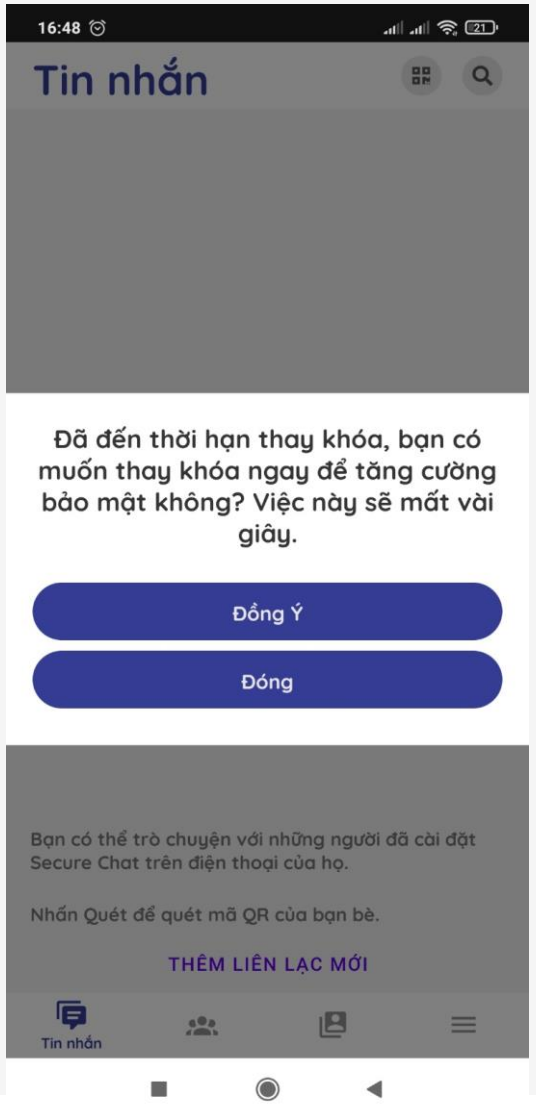
(29/36) Màn đăng nhập và màn tạo khoá



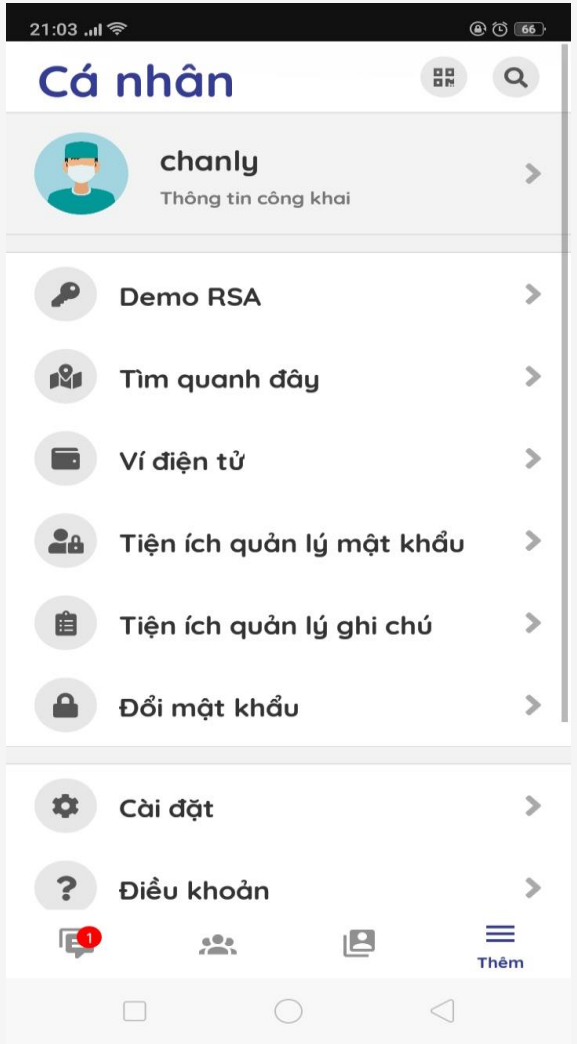


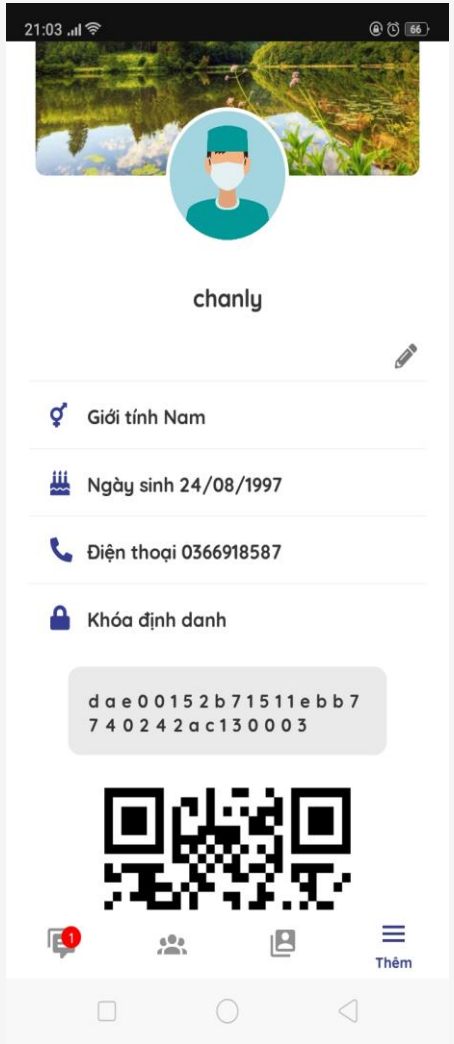
Thiết lập mức độ an toàn cho tài khoản



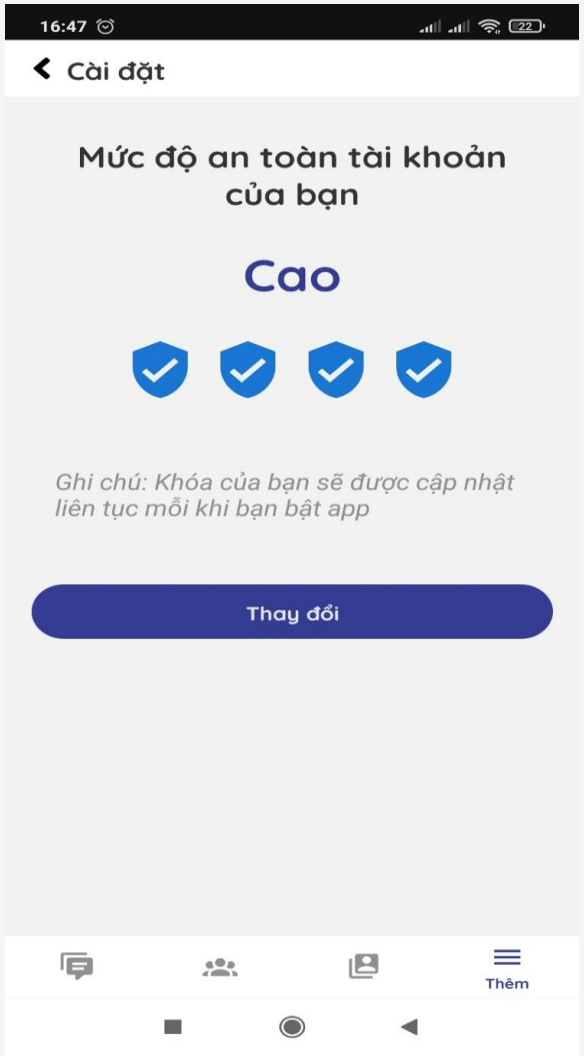


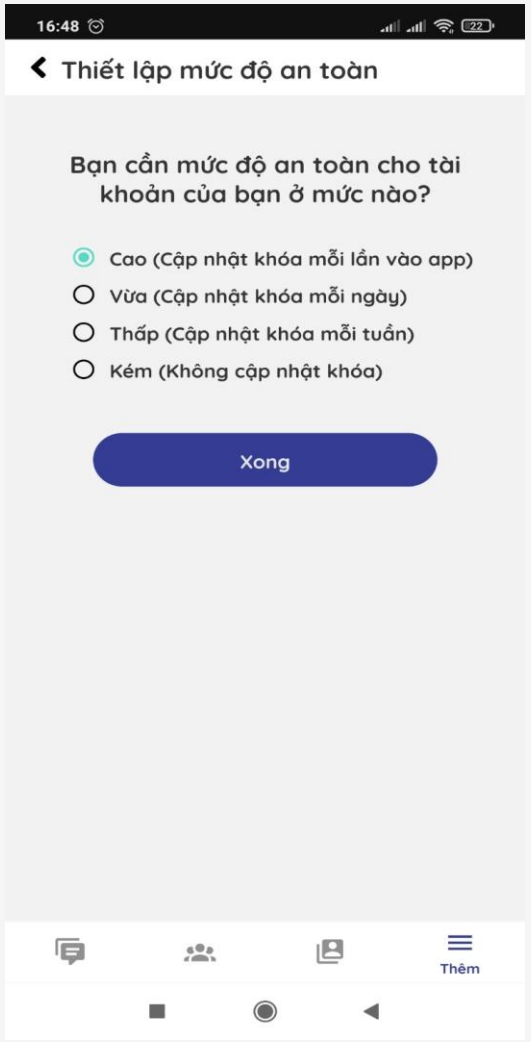
Màn menu và trang cá nhân



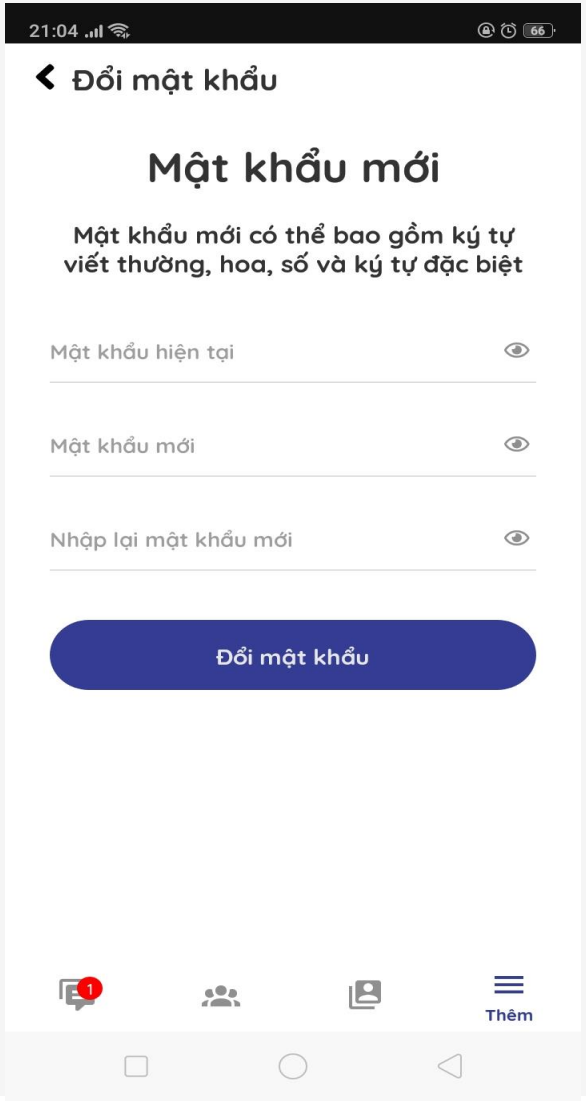


Màn cập nhật mức độ an toàn cho tài khoản



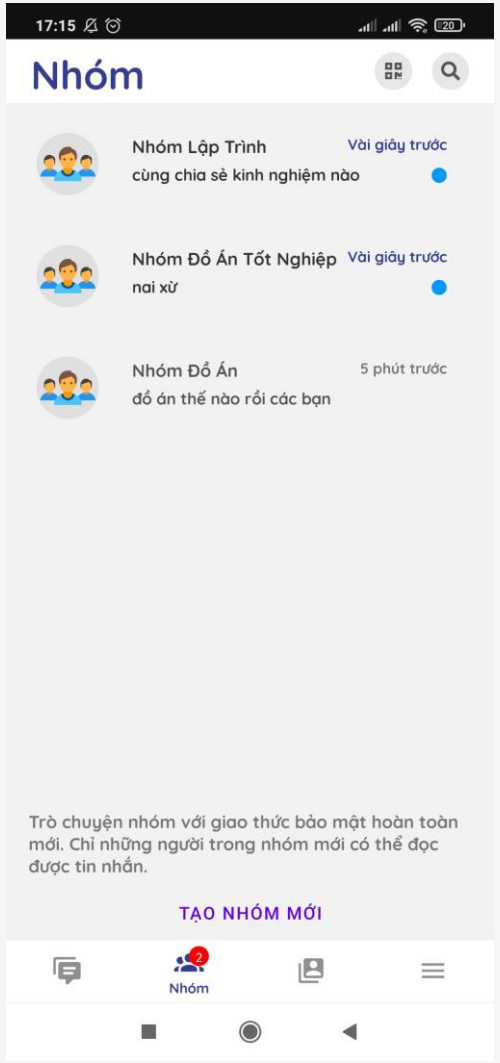


Màn đổi mật khẩu



Màn chat và danh sách các cuộc trò chuyện 2 người

Màn chat và danh sách các cuộc trò chuyện nhóm



Tài liệu tham khảo

[1] https://en.wikipedia.org/wiki/RSA_(cryptosystem)

[2] https://www.stdio.vn/cyber-security/co-ban-ve-ma-hoa-e35mL

[3] https://flask-socketio.readthedocs.io/en/latest/

[4] https://viblo.asia/p/he-ma-hoa-rsa-va-chu-ky-so-6J3ZgkgMZmB