# I. Cài đặt các phần mềm và môi trường

Các phần mềm, thư viện được sử dụng sau đây là dành cho việc phát triển trên hệ điều hành Windows 11 Version 24H2.

## 1. OpenSSL

Download và cài đặt OpenSSL Light tại <https://slproweb.com/download/Win32OpenSSL_Light-3_5_0.exe>

## 2. IDE và Môi trường phát triển Java

* Download và cài đặt VS Code tại: <https://code.visualstudio.com/download>
* Hướng dẫn setup môi trường cho Java trong VS Code tại: <https://code.visualstudio.com/docs/languages/java>
* Download và cài đặt JDK 24 tại [Java Downloads | Oracle](https://www.oracle.com/java/technologies/downloads/#jdk24-windows)
* Download **mysql/mysql-connector-java/8.0.33** tại [Central Repository: mysql/mysql-connector-java/8.0.33](https://repo1.maven.org/maven2/mysql/mysql-connector-java/8.0.33/)
* Download và cài đặt MySQL Community tại [MySQL :: MySQL Community Downloads](https://dev.mysql.com/downloads/)

# II. Quá trình thực hiện

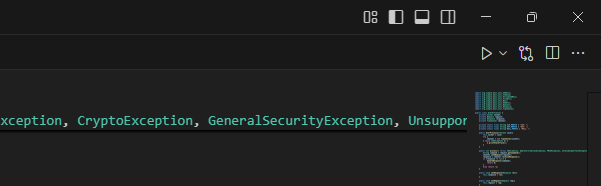
## 1. Sinh cặp khóa RSA cho các người dùng

Tạo file *./keys/generate\_keys.cmd* chứa các command để tạo các cặp khóa RSA cho Alice, Bob và Charlie.

Sử dụng công cụ OPENSSL

## 2. Khởi chạy ứng dụng

Trong VS Code, chạy Server app rồi chạy Client app bằng cách nhấn vào icon run ở góc trên bên phải IDE.



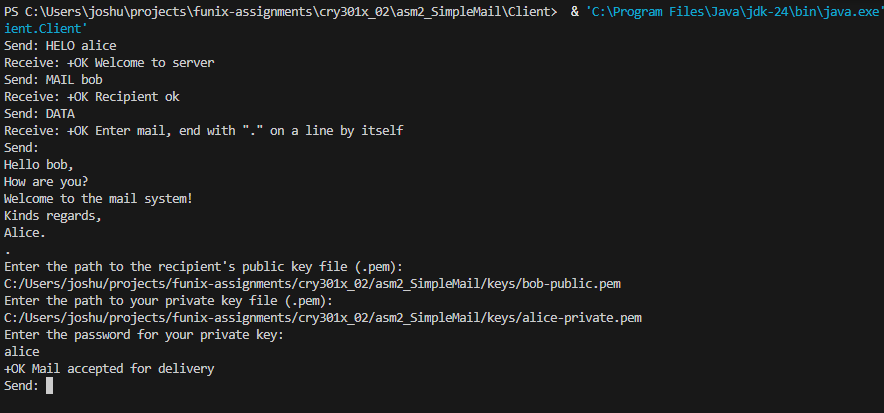
# III. Thực thi và kiểm thử kết quả

## 1. UC\_DATA - Gửi nội dung email

### 1.1. Luồng chính

**Các bước thực thi:**

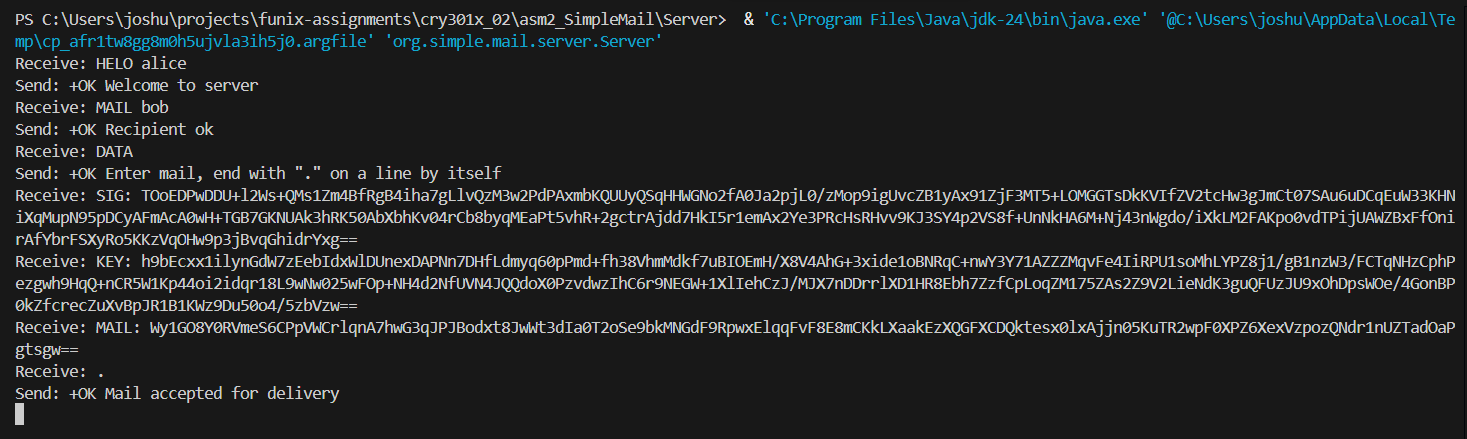
1. Người dùng gửi lệnh DATA
2. MailClient hiển thị thông báo thành công từ MailServer “+OK Enter mail, end with "." on a line by itself”
3. Người dùng nhập nội dung email cho tới khi kết thúc bằng “**.**”
4. MailClient yêu cầu người dùng nhập đường dẫn file .pem chứa khóa công khai của người nhận
5. Người dùng nhập đường dẫn file chứa khóa công khai của người nhận
6. MailClient yêu cầu người dùng nhập đường dẫn file .pem chứa khóa riêng của người dùng
7. Người dùng nhập đường dẫn file chứa khóa riêng của mình
8. MailClient yêu cầu người dùng nhập mật khẩu bảo vệ khóa riêng
9. Người dùng nhập mật khẩu bảo vệ khóa riêng
10. MailClient thông báo kết quả gửi email thành công từ MailServer “+OK Mail accepted for delivery”



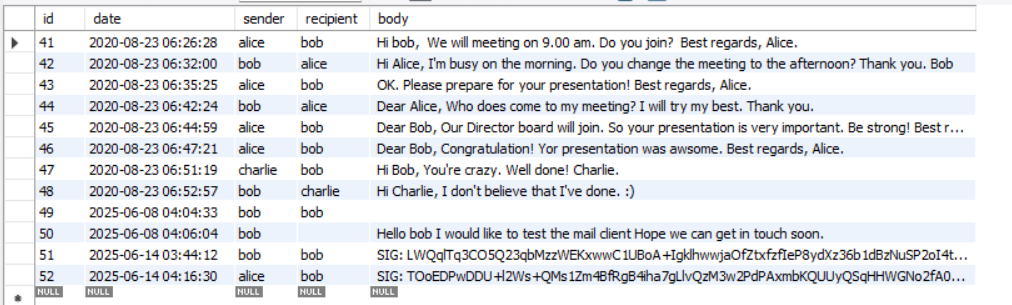
**Kết quả:**

Server log như sau:

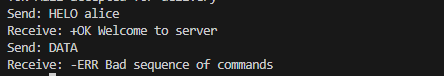
* Dữ liệu đã được mã hóa.
* Có đầy đủ 3 thành phần:
  + SIG – signature
  + KEY – AES key đã được mã hóa
  + MAIL – nội dung mail đã được mã hóa



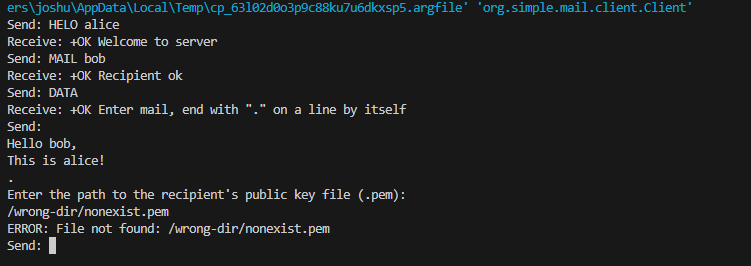
Trong database, record có ID = 52 là email đã được gửi và lưu thành công vào database.



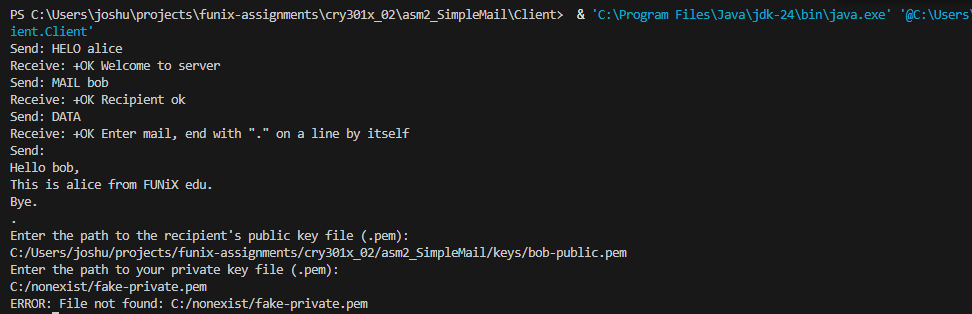
### 1.2. Luồng phụ 1 - MailClient hiển thị thông báo lỗi nhận được từ MailServer “-ERR Bad sequence of commands” nếu điều kiện không được đáp ứng.



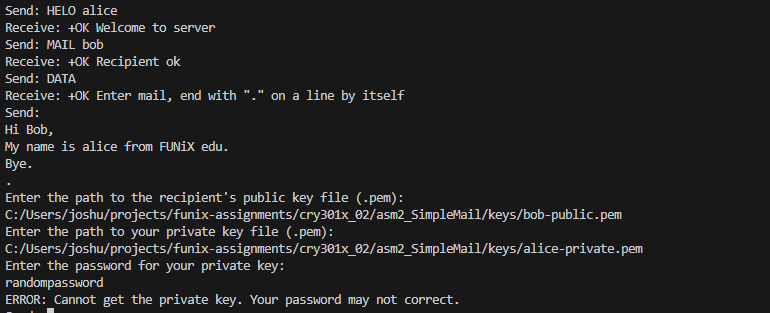
### 1.3. Luồng phụ 2 - MailClient thông báo lỗi vào ra file.



### 1.4. Luồng phụ 3 - MailClient thông báo lỗi vào ra file.



### 1.5. Luồng phụ 4 – MailClient thông báo lỗi không truy xuất được khóa riêng.



## 2. UC\_RETR – Nhận nội dung email

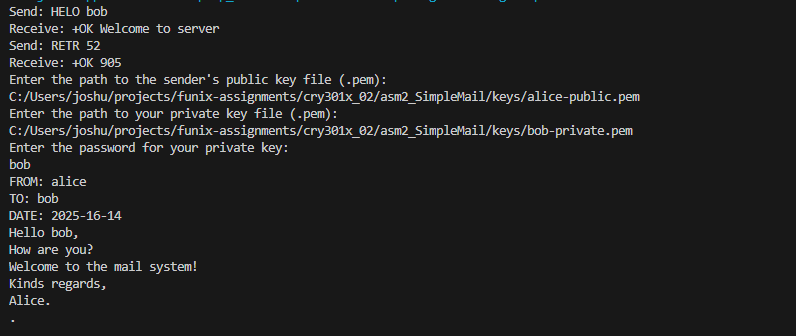
### 2.1. Luồng chính

**Các bước thực hiện**

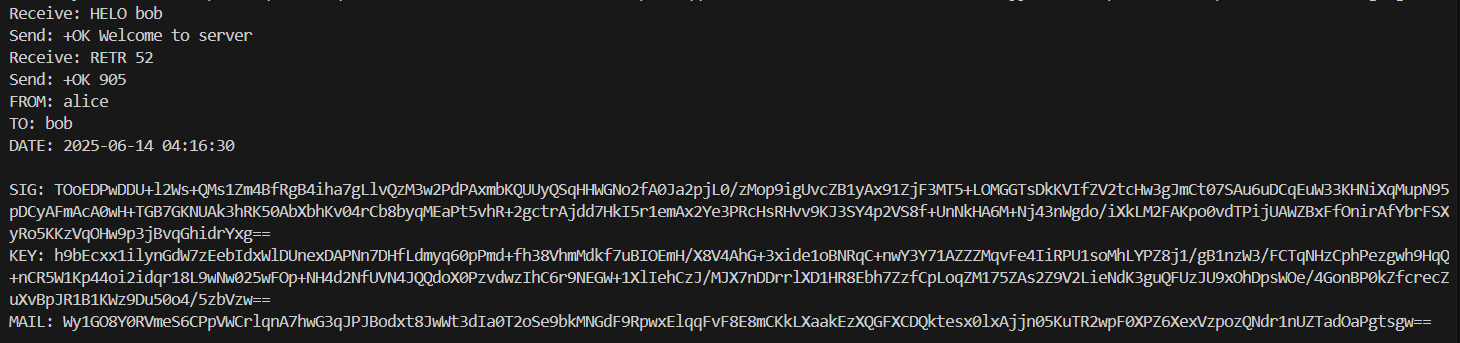
1. Người dùng gửi lệnh RETR *id*
2. MailClient yêu cầu nhập đường dẫn file .pem chứa khóa công khai của người gửi
3. Người dùng nhập đường dẫn file chứa khóa công khai của người gửi
4. MailClient hiển thị thông báo xác thực email thành công
5. MailClient yêu cầu nhập đường dẫn file .pem chứa khóa riêng của người dùng
6. Người dùng nhập đường dẫn file chứa khóa riêng của mình
7. MailClient yêu cầu người dùng nhập mật khẩu bảo vệ khóa riêng
8. Người dùng nhập mật khẩu bảo vệ khóa riêng
9. MailClient hiển thị nội dung email.

**Kết quả**

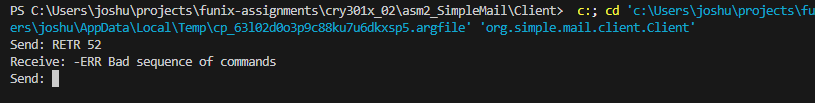
* Email đã được đọc thành công.



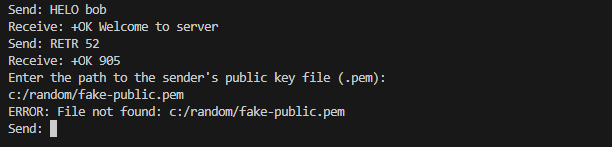
* Mail vẫn ở dạng được mã hóa ở phía server



### 2.2. Luồng phụ 1 – MailClient hiển thị thông báo lỗi nhận được từ MailServer “-ERR Bad sequence of commands” nếu điều kiện không được đáp ứng.

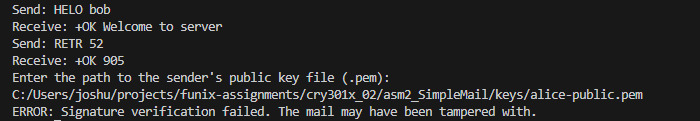


### 2.3. Luồng phụ 2 – MailClient thông báo lỗi vào ra file.

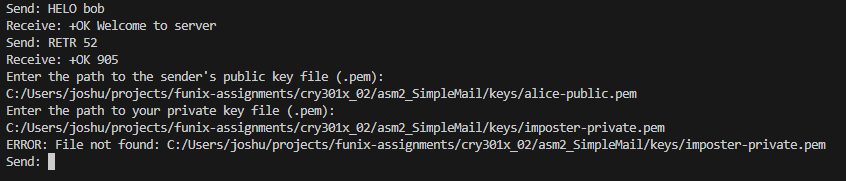


### 2.4. Luồng phụ 3 – MailClient thông báo xác thực email thất bại.

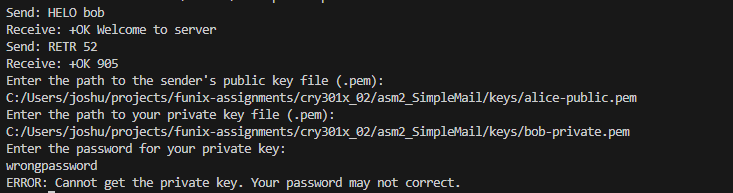
Trường hợp chữ ký không hợp lệ (chỉnh sửa nội dung trong database để làm sai chữ ký tạo trường hợp này).



### 2.5. Luồng phụ 4 – MailClient thông báo lỗi vào ra file.



### 2.6. Luồng phụ 5 – MailClient thông báo lỗi không truy xuất được khóa riêng do sai mật khẩu.



# IV. Đề xuất cải tiến

Trong kịch bản mã hóa mail ở trên, chúng ta đã:

* Dùng mã hóa đối xứng AES cho nội dung email;
* Dùng mã hóa bất đối xứng để mã hóa AES key để đảm bảo gửi key tới người dùng được an toàn.

Mặc dù giải pháp đã phần nào đảm bảo được tính bí mật. Tuy nhiên, giải pháp vẫn còn một số hạn chế:

* Chưa đảm bảo được nội dung email có bị chỉnh sửa hay không?
* Hiệu năng của RSA signature khá hạn chế.

Chúng ta có thể sử dụng thêm mã xác thực thông điệp HMAC.

* HMAC có thể đảm bảo nội dung thư được mã hóa không bị thay đổi và đến từ người gửi hợp pháp.
* HMAC nhanh hơn và ít tốn kém hơn về mặt tính toán so với chữ ký số dựa trên RSA, điều này có thể cải thiện hiệu suất cho các máy chủ thư quy mô lớn.