BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC NGOẠI NGỮ - TIN HỌC

THÀNH PHỐ HỒ CHÍ MINH

ĐỒ ÁN MÔN HỌC

LẬP TRÌNH MẠNG NÂNG CAO

Nguyễn Công Khang - 21DH110770

Phạm Đức Thiên Phúc - 21DH112813

Nguyễn Minh Đức – 21DH113591

GVGD: Th.S Phan Gia Lượng

MỤC LỤC

Danh Mục Hình Ảnh

LỜI NÓI ĐẦU

Trong thời đại công nghệ thông tin bùng nổ, lập trình mạng đã trở thành một lĩnh vực then chốt và không thể thiếu trong việc phát triển các hệ thống và ứng dụng kết nối toàn cầu. Với sự phát triển không ngừng của Internet và các công nghệ mạng, việc hiểu và nắm vững các kiến thức về lập trình mạng đã trở thành một yêu cầu cấp thiết đối với các lập trình viên và kỹ sư phần mềm.

Đồ án "Lập Trình Mạng Nâng Cao" được thực hiện nhằm mục đích nghiên cứu, phân tích và triển khai các kỹ thuật lập trình mạng cơ bản và nâng cao. Nội dung của đồ án không chỉ tập trung vào các lý thuyết nền tảng mà còn chú trọng đến việc ứng dụng thực tiễn qua các dự án và bài tập cụ thể. Qua đó, sinh viên sẽ được trang bị các kỹ năng cần thiết để thiết kế, triển khai và quản lý các ứng dụng mạng một cách hiệu quả.

Trong quá trình thực hiện đồ án, chúng em đã gặp không ít khó khăn và thử thách. Tuy nhiên, với sự hỗ trợ nhiệt tình từ giảng viên hướng dẫn **Th.S Phan Gia Lượng** và sự nỗ lực không ngừng của bản thân, chúng em đã hoàn thành đồ án này đúng thời hạn. Chúng em hy vọng rằng đồ án này sẽ là nguồn tài liệu hữu ích cho các bạn sinh viên và những ai quan tâm đến lĩnh vực lập trình mạng.

Chúng em xin chân thành cảm ơn.

Chương 1: Giới thiệu đề tài

Giả sử bạn muốn nói với bạn mình một bí mật. Nếu bạn ở ngay bên cạnh họ, bạn chỉ cần thì thầm điều gì đó. Nếu bạn ở hai phía đối nhau của đất nước, điều đó sẽ không an toàn. Bạn có thể viết nó ra và gửi cho họ qua đường bưu điện hoặc sử dụng điện thoại. Nhưng cách này sẽ không an toàn và bất kỳ ai có động cơ đủ mạnh đều có thể chặn được tin nhắn.

Nếu bí mật đó đủ quan trọng, bạn không nên mạo hiểm viết nó ra. Gián điệp hoặc một nhân viên bưu điện lừa đảo có thể xem nó qua thư của bạn. Tương tự như vậy, ai đó có thể nghe trộm điện thoại của bạn mà bạn không biết và họ sẽ ghi lại mọi cuộc gọi mà bạn thực hiện.

Một giải pháp để ngăn chặn kẻ nghe trộm và truy cập nội dung tin nhắn là mã hóa nó. Về cơ bản, điều này có nghĩa là thêm một mã vào tin nhắn, nó sẽ làm cho tin nhắn thành một mớ hỗn độn. Nếu mã của bạn đủ phức tạp, thì những người duy nhất có thể truy cập vào thư gốc là những người có quyền truy cập vào mã.

Nếu bạn có cơ hội chia sẻ mã với bạn mình trước đó, thì một trong hai người có thể gửi tin nhắn được mã hóa bất cứ lúc nào. Nhưng nếu bạn không có cơ hội chia sẻ mã đó thì sao?

Đây là một trong những vấn đề cơ bản của mật mã, đã được giải quyết bằng các sơ đồ mã hóa public-key (còn được gọi là mã hóa bất đối xứng) như RSA.

Theo mã hóa RSA, các tin nhắn được mã hóa bằng một mã gọi là public key, mã này có thể được chia sẻ công khai. Do một số đặc thù tính toán khoa học khác biệt của thuật toán RSA, một khi một thông điệp đã được mã hóa bằng public key, nó chỉ có thể được giải mã bằng một key được gọi là private key. Mỗi người dùng RSA có cặp key bao gồm public key và private key của riêng họ. Private key cần được giữ bí mật.

Các lược đồ public key khác với key symmetric, trong khi đó cả quá trình mã hóa và giải mã đều phải sử dụng private key. Những khác biệt này làm cho mã hóa public key như RSA hữu ích để giao tiếp trong các tình huống mà trước đó không có cơ hội để phân phối key một cách an toàn.

Các thuật toán key đối xứng có các ứng dụng riêng của chúng. Chẳng hạn như mã hóa dữ liệu cho mục đích sử dụng các nhân hoặc khi có các kênh bảo mật mà private có thể được chia sẻ.

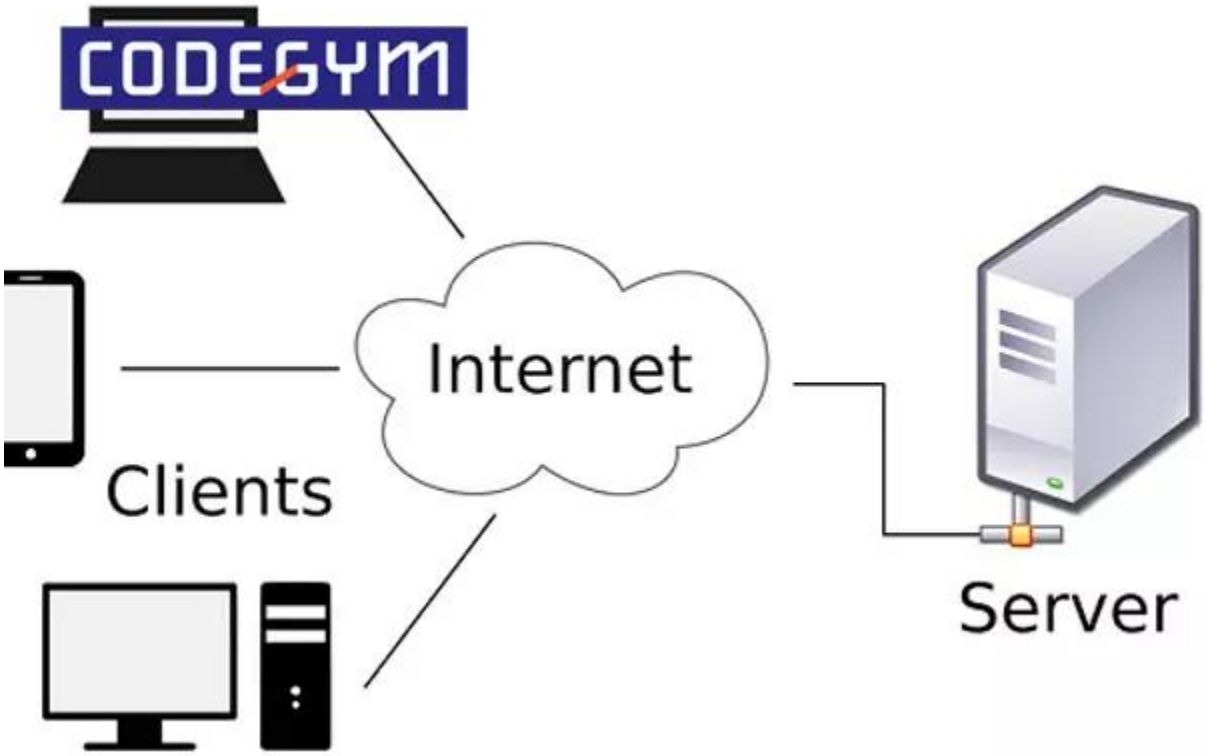
Chương 2: Cơ sở lí thuyết

I. Mạng máy tính

1. Khái niệm

Với mục đích phân tích và nghiên cứu quá trình giao tiếp, Mạng máy tính đã được tạo ra như một bước tiến mới trong lịch sử. Bởi nó liên kết toàn bộ các hệ thống máy tính khác nhau để trao đổi thông tin cần thiết.

Do đó, việc kết nối mạng chỉ thực hiện được khi có mạng riêng của nó. Có 4 loại mạng cơ bản là: LAN, MAN, WAN và PAN. Người dùng cần chú ý cơ chế hoạt động của các mạng để lựa chọn phát triển chương trình mạng được tốt nhất.



Hình 1 Mô hình mạng máy tính

2. Phân loại

- **Mạng LAN (Local Area Network)**

Mạng LAN là mạng cục bộ nên có đường truyền ngắn. Với giao thức TCP/IP, mạng LAN chủ yếu được sử dụng tại nơi diện tích nhỏ như: văn phòng, tòa nhà, trường học.

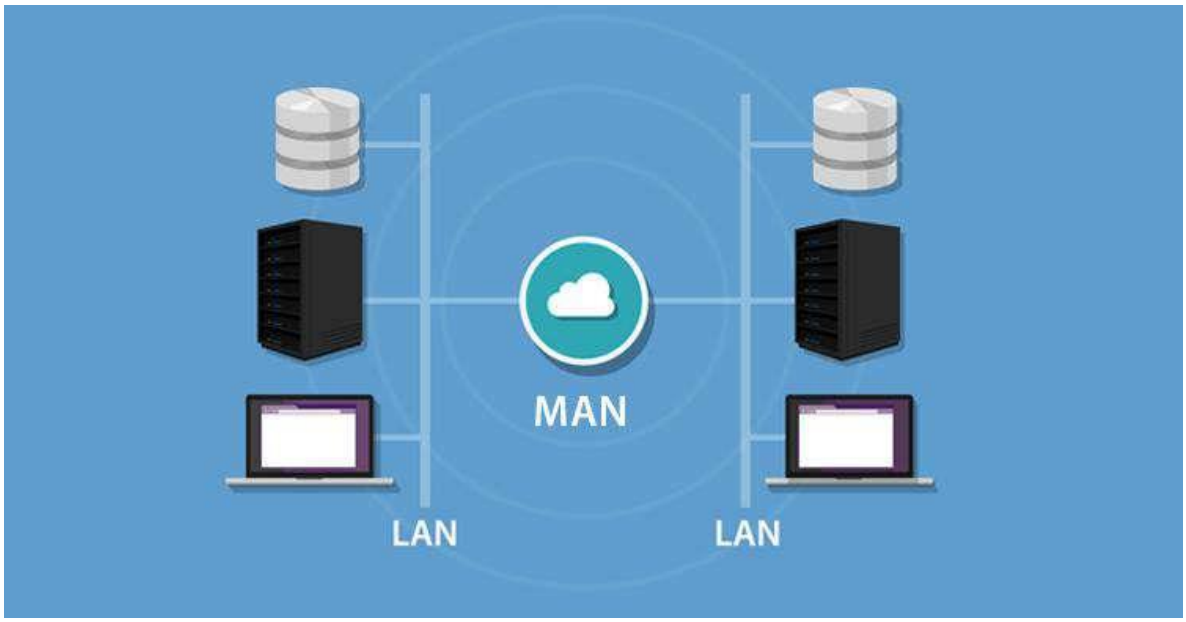
Tất cả máy tính kết nối mạng LAN đều được sử dụng để kết nối vào máy chủ sau đó chờ quyền truy cập để thực hiện lệnh in trên máy in.

Hình 2 Ảnh mô tả mạng LAN

- **Mạng MAN (Metropolitan Area Network)**

Khác với mạng LAN, mạng đô thị MAN có phạm vị kết nối rộng hơn, hình thành nhờ sự kết nối nhiều mạng LAN với nhau.

Đây là mô hình rộng cung cấp dịch vụ giá trị gia tăng; trên một đường truyền tốc độ nhanh để kết nối và mở rộng triển khai các doanh nghiệp với nhau.

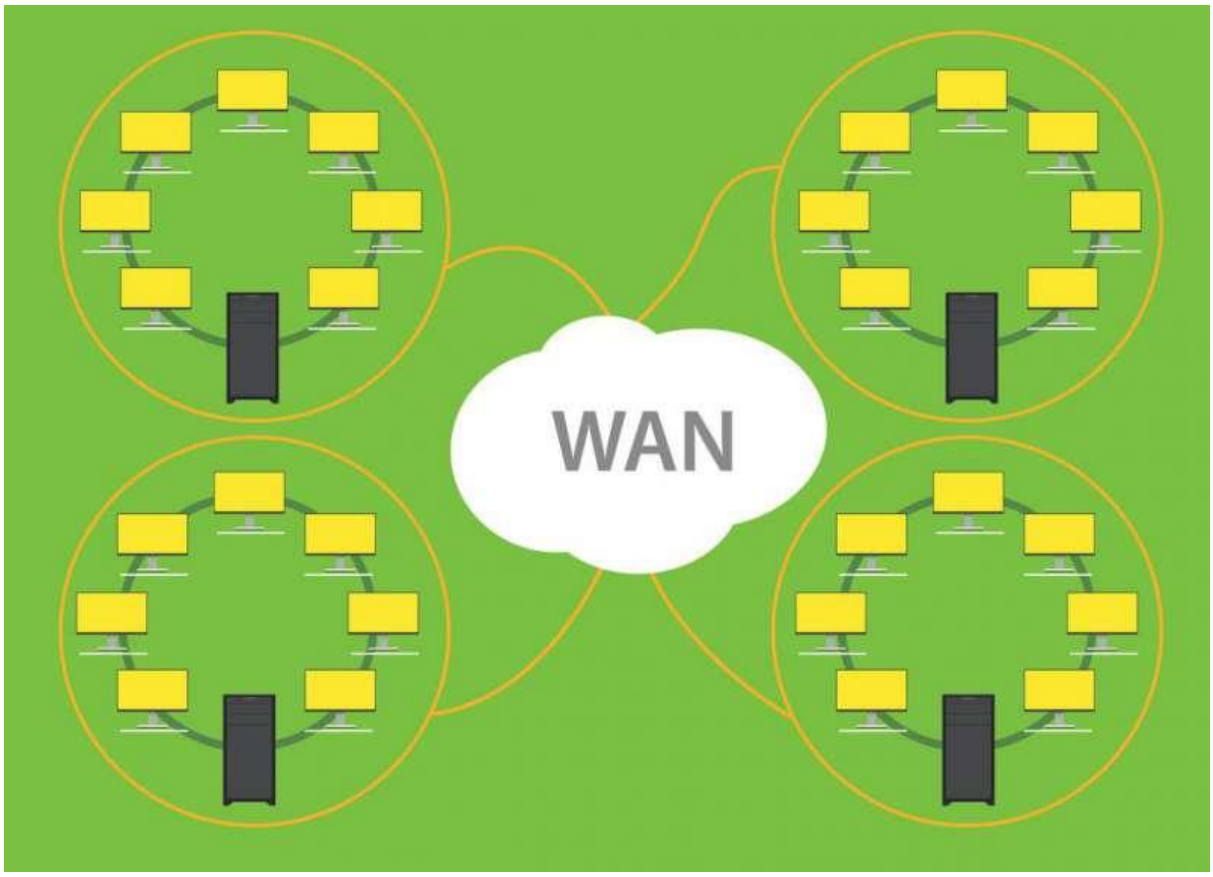


Hình 3 Ảnh mô tả mạng MAN

- **Mạng WAN (Wide Area Network)**

Mạng diện rộng WAN là sự kết hợp giữa mạng LAN và mạng MAN với việc sử dụng đường dây cáp quang hay thuê bao hoặc thông qua đường truyền vệ tinh.

Phạm vi hoạt động của mạng rộng lớn hơn, bao gồm cả một quốc gia, khu vực địa lý hay thậm chí ở toàn cầu.



Hình 4 Ảnh mô tả mạng WAN

- **Mạng PAN (Personal Area Network)**

Mạng PAN có khả năng phát tín hiệu kết nối trong một diện tích nhỏ để truyền dữ liệu thông qua mạng trực tuyến.

Cá nhân có thể sử dụng mạng PAN giữa các thiết bị với nhau như di động. máy tính. để liên lạc thuận lợi hơn hoặc kết nối với các mạng cao cấp hơn.

Hình 5 Ảnh mô tả mạng PAN

II. Lập trình mạng

Lập trình mạng nói một cách dễ hiểu là công việc của người sẽ phát triển ứng dụng tại hệ thống doanh nghiệp từ việc lập sổ sách nhân sự, quản lý tiền cho đến việc sáng tạo các trò chơi, điều khiển để thêm sức hấp dẫn thu hút hơn.

Công thức để xây dựng lập trình mạng như sau:

Lập trình mạng = Kiến thức mạng + Mô hình lập trình mạng + Ngôn ngữ lập trình mạng

Theo công thức này thì sẽ rất dễ nhận thấy ba vấn đề chính cần quan tâm là kiến thức mạng truyền thông, mô hình lập trình và ngôn ngữ lập trình.

Về kiến thức mạng truyền thông thì đây là kiến thức chung về mạng di động: mạng Bluetooth, hệ thống GPS, mạng Sensor… mà người làm quản trị cần nắm vững cách sử dụng để khai thác.

Mô hình lập trình là kiến thức về tất cả các cách xây dựng hệ thống mạng, kiến thức về cơ sở dữ liệu, mô hình xây dựng các chương trình ứng dụng mạng.

III. Client

1. Khái niệm

"Client" là thuật ngữ chỉ 1 thiết bị hoặc phần mềm kết nối đến mạng hoặc dịch vụ để truy cập các tài nguyên. Client có vai trò gửi yêu cầu và nhận kết quả từ 1 máy chủ (server)

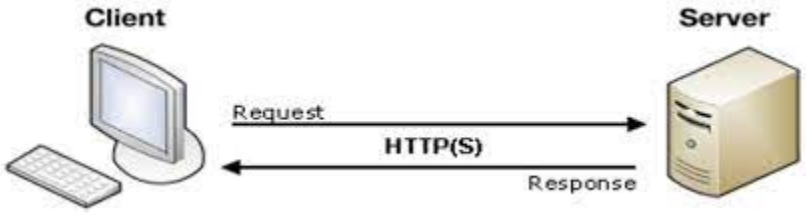
2. Ví dụ

- Web browser (trình duyệt web): Được sử dụng để truy cập các trang web thông qua internet
- Email client (client email): Dùng để gửi và nhận email từ 1 máy chủ email
- FTP client: Để truy cập và quản lý các tệp trên 1 máy chủ FTP (File Tranfer Protocol)
- Game client: Cho phép người dung kết nối đến máy chủ game để tham gia các trò chơi trực tuyến

IV. Server

1. Khái niệm

"Server" (máy chủ) là 1 thiết bị hoặc phần mềm cung cấp các dịch vụ, tài nguyên, hoặc chứng năng cho các thiết bị khác, gọi là các client, thông qua mạng hoặc internet. Máy chủ thường được cấu hình để xử lý các yêu cầu từ các client và phản hồi bằng cách cung cấp dữ liệu, tài nguyên, hoặc các dịch vụ khác theo yêu cầu



Hình 6 Mô hình Client - Server

2. Ví dụ

- Web server: Cung cấp các trang web và nội dung trực tuyến cho các trình duyệt web (clients) thông qua giao thưc HTTP hoặc HTTPS
- Email server: Quản lí và phân phối email giữa các người dùng thông qua giao thức email như POP3, IMAP, SMTP
- File server: Lưu trữ và quản lý các tệp tin và thư mục trên mạng cho phép các client truy cập và chia sẻ dữ liệu
- Database server: Lưu trữ và quản lý cơ sở dữ liệu, cho phép các client truy vấn và cập nhật dữ liệu
- Game server: Được sử dụng trong các trò chơi trực tuyến để quản lý và điều phối các trận đấu, người chơi và dữ liệu game

V. Chữ ký số

1. Khái niệm

"Chữ ký số" là một dạng chữ ký điện tử được tạo ra dựa trên các thông điệp dữ liệu sử dụng hệ thống mật mã không đối xứng.

Chữ ký số có tác dụng tương đương với chữ ký tay cá nhân. Thường được sử dụng để xác thực danh tính cá nhân thông qua các trường hợp:

Ký các văn bản hoặc tài liệu điện tử như hợp đồng, hóa đơn… Sử dụng trong các giao dịch trực tuyến như kê khai giao dịch cá nhân, giao dịch qua mobile banking hoặc giao dịch chứng khoán…

Hình 7 Ảnh minh họa chữ ký số

Chữ ký số cá nhân được biết tới là một loại chữ ký điện tử và có giá trị ngang với chữ ký tay. Thường được dùng để xác minh danh tính của cá nhân ký các văn bản, giao dịch trực tuyến… Ngoài ra, chữ ký số cũng có tác dụng giúp bạn kê khai nộp thuế theo hình thức trực tuyến.

Một chữ ký số cá nhân thể hiện các thông tin:

Tên của cá nhân là chủ thể của chứng thư số đã đăng ký Tên của công ty cung cấp dịch vụ chữ ký số.

2. Đặc điểm

Chữ ký số giúp xác thực danh tính của chủ nhân chữ ký thông qua chứng thư số của cá nhân, doanh nghiệp, tổ chức Hai lớp mã khóa bảo mật thông tin, ngăn chặn tình trạng thông tin bị đánh cắp bởi hacker Chỉ cá nhân đã thực hiện chữ ký số mới có thể nhận, mở văn bản có chữ ký số. Bảo đảm sự an toàn trong việc sử dụng thông tin điện tử Chữ ký số một khi đã thực hiện thì bạn không thể xóa bỏ và không thể thay thế.

Ngoài ra, đối tượng sở hữu chữ ký số cá nhân cũng có khác biệt:

Các cá nhân nằm trong doanh nghiệp, tổ chức sử dụng chữ ký số cá nhân để ký các văn bản nằm trong quyền hạn, chức vụ Các cá nhân có nhu cầu sử dụng chữ kỹ số cá nhân để ký các văn bản, nội dung điện tử.

3. Thành phần

Chữ ký số được tạo nên từ thuật toán RSA - thuật toán tạo ra mật mã mã khóa công khai. Bao gồm hệ thống một cặp khóa không đối xứng: một khóa công khai (Public Key) và một khóa bí mật (Private Key). Trong đó có 5 thành phần chính:

- **Khóa bí mật:** được sử dụng để tạo ra chữ ký số
- **Khóa công khai:** có chức năng thẩm định chữ ký và xác thực người dùng. Thường được tạo nên từ các cặp khóa bí mật tương ứng.
- **Người ký:** cá nhân sử dụng khóa bí mật để ký một số thông điệp dữ liệu dưới danh nghĩa của mình.
- **Người nhận:** tổ chức hoặc cá nhân nhận được chữ ký số, sau đó tiến hành sử dụng chứng thư số để kiểm tra chữ ký và cuối cùng là tiến hành các hợp đồng, giao dịch liên quan.
- **Ký số:** đưa khóa bí mật vào một phần mềm tự động để tạo nên chữ ký số và gắn vào một thông điệp dữ liệu mà bạn muốn.

4. Các loại phổ biến hiện nay

- **Chữ ký số USB Token:** Là loại chữ ký số truyền thống và được sử dụng phổ biến trên thị trường ngày nay. USB Token là thiết bị cần dùng tới phần cứng kết hợp để lưu trữ dữ liệu mã hóa của cá nhân, tổ chức, doanh nghiệp.
- **Chữ ký số Smartcard:** Là loại chữ ký được thiết lập sẵn trên SIM giúp người dùng sử dụng thiết bị di động nhanh chóng. Tuy nhiên loại hình chữ ký này lại có một nhược điểm to lớn. Nó phụ thuộc vào sự cung cấp của các nhà mạng và không thể thực hiện ký số khi ở nước ngoài.
- **Chữ ký số HSM:** Là loại hình chữ ký số sử dụng giao thức mạng để xử lý việc ký các văn bản. Trong đó HSM được sử dụng như một thiết bị vật lý giúp bảo vệ các mã khóa của chứng thư số.
- **Chữ ký số từ xa:** Được biết đến là chữ ký số không sử dụng USB Token, được đánh giá là chữ ký số có tính năng ứng dụng mạnh nhất. Chữ ký số từ xa sử dụng công nghệ đám mây để tiến hành tạo chữ ký và không cần thêm bất kỳ phần cứng nào hỗ trợ.

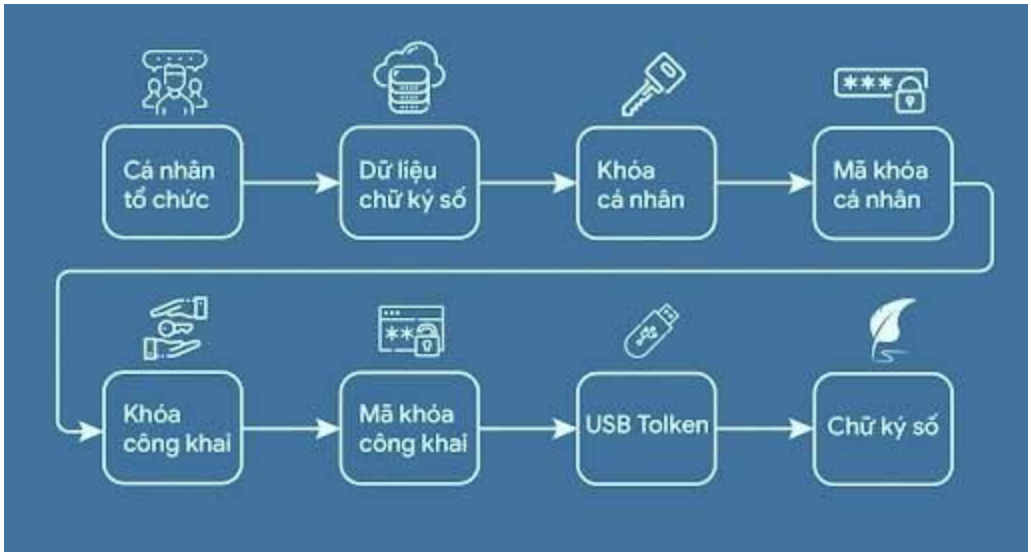
5. Quy trình tạo chữ ký

- **Bước 1:** Chọn một cơ quan cấp chứng chỉ số

Bạn cần chọn một trong các cơ quan cấp chứng chỉ số uy tín và được công nhận để đảm bảo rằng chữ ký số của bạn có giá trị pháp lý. (Ví dụ: ViettelCA, BKAVCA, VNPT-CA, FPT-CA,...)

- **Bước 2:** Đăng ký và xác thực thông tin

Sau khi chọn cơ quan cấp chứng chỉ số, bạn cần đăng ký tài khoản trên trang web của cơ quan đó và xác thực thông tin của mình bằng các giấy tờ như CMND/CCCD/Hộ chiếu, giấy phép kinh doanh,..



Hình 8 Quy trình tạo chữ ký số

- **Bước 3:** Thực hiện xác thực danh tính

Bạn cần đến trực tiếp cơ quan cấp chứng chỉ số để cung cấp các giấy tờ liên quan và đăng ký cho việc xác thực bằng chữ ký.

- **Bước 4:** Tạo chữ ký số

Sau khi hoàn thành các bước đăng ký và xác thực, bạn có thể tạo chữ ký số bằng cách sử dụng phần mềm cung cấp bởi cơ quan cấp chứng chỉ số. Bạn cần cài đặt phần mềm này trên máy tính của mình và thực hiện tạo chữ ký theo hướng dẫn.

- **Bước 5:** Lưu trữ chữ ký số

Sau khi tạo ra chữ ký số, bạn cần lưu trữ nó một cách an toàn và bảo mật. Bạn có thể lưu trữ chữ ký số trên ổ đĩa USB hoặc trên máy tính của mình và đảm bảo rằng không có ai có thể truy cập vào nó.

Lưu ý: Chữ ký số là một giấy tờ quan trọng và có giá trị pháp lý nên bạn cần bảo mật nó và không chia sẻ với bất kỳ ai nếu không cần thiết.

VI. RSA

1. Khái niệm

RSA là 1 trong những thuật toán mã hóa khóa công khai (public-key cryptography) quan trọng và được sử dụng rộng rãi trong bảo mật thông tin. Thuật toán này được đặt tên theo ba nhà khoa học máy tinh Ronald Rivest, Adi Shamir và Leonard Adleman, người đã phát triển nó vào năm 1977

RSA được sử dụng rộng rãi trong các ứng dụng bảo mật như mã hóa dữ liệu trong giao tiếp an toàn mạng (SSL/TLS), chữ ký số để xác minh tính xác thực của thông tin, và trong các hệ thống xác thực người dùng. Tuy nhiên, việc sử dụng RSA đòi hỏi tính toán năng lượng lớn hơn so với các thuật toán mã hóa đối xứng khác như AES, vì vậy trong thực tế, thường kết hợp sử dụng RSA với các thuật toán khác để cân bằng hiệu suất và bảo mật

2. Đặc điểm

- Mã hóa và giải mã khóa công khai: RSA sử dụng cặp khóa bao gồm khóa công khai (public key) và khóa bí mật (private key). Khóa công khai dùng để mã hóa dữ liệu, trong khóa bí mật dùng để giải mã, Điều này cho phép người dùng có thể chia sẽ khóa công khai mà không cần phải chia sẽ khóa bí mật, đảm bảo tính bảo mật cao
- Mã hóa RSA: Để mã hóa dữ liệu sử dụng RSA, dữ liệu ban đầu sẽ được chia thành các khối nhỏ hơn và mỗi khối này sẽ được mã hóa bằng khóa công khai
- Giải mã RSA: Sau khi được mã hóa, dữ liệu sẽ được giải mã bằng khóa bí mật tương ứng. Chỉ có người nắm giữ khóa bí mật mới có thể giải mã được dữ liệu đã được mã hóa
- An toàn và bảo mật: RSA dựa trên sự khó khăn của việc phân tích thừa số nguyên lớn (integer factorization problem), một vấn đề toán học khó. Kích thước cảu các khóa RSA được sử dụng phụ thuộc vào mức dộ an toàn mà người triển khai mong muốn đạt được

3. Thường được sử dụng ở đâu?

Mã hóa RSA thường được sử dụng kết hợp với các sơ đồ mã hóa khác. Và cho các chữ ký kỹ thuật số có thể chứng minh tính xác thực và tính toàn vẹn của

một thông điệp. Nó thường không được sử dụng để mã hóa toàn bộ thư và file vì nó kém hiệu quả và tốn tài nguyên hơn so với mã hóa key đối xứng.

Để làm cho mọi thứ hiệu quả hơn, một file thường sẽ được mã hóa bằng thuật toán key đối xứng. Sau đó key đối xứng sẽ được mã hóa bằng mã hóa RSA. Theo quy trình này, chỉ người có quyền được truy cập vào RSA private key mới có thể giải mã key đối xứng.

Nếu không thể truy cập key đối xứng, thì không thể giải mã file gốc. Phương pháp này có thể được sử dụng để bảo mật các thư và file mà không mất nhiều thời gian và tài nguyên.

Mã hóa RSA có thể được sử dụng trong một số hệ thống khác nhau. Nó có thể vận hành trong OpenSSL, wolfCrypt, cryptlib và một số thư viện mật mã khác.

Theo truyền thống, nó được sử dụng trong TLS và cũng là thuận toán ban đầu được sử dụng trong mã hóa PGP. RSA vẫn được nhìn thấy trong một loạt các trình duyệt web, email, VPN, chat và các kênh giao tiếp khác.

RSA cũng thường được sử dụng để tạo kết nối an toàn giữa VPN client và VPN server. Theo các giao thức như OpenVPN, TLS có thể sử dụng thuật toán RSA để trao đổi key và thiết lập một kênh an toàn.

Mã hóa RSA đóng vai trò quan trọng trong việc thiết lập kết nối an toàn SSL/TLS và bảo vệ dữ liệu truyền tải trên mạng.

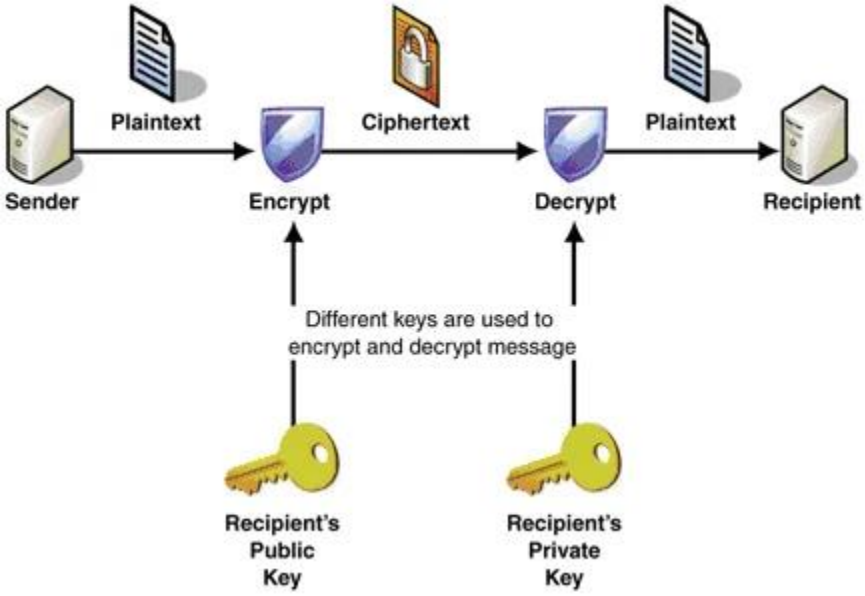
4. Phương thức hoạt động trên thực tế

Đầu tiên, mỗi người cần thiết lập cặp key của riêng mình và chia sẻ public key với nhau. Hai người cần giữ bí mật về private key của họ để thông tin liên lạc của họ được bảo mật.

Khi người gửi có public key của người nhận, họ có thể sử dụng key đó để mã hóa dữ liệu mà họ muốn bảo mật. Khi nó đã được mã hóa bằng public key, nó chỉ có thể được giả mã bằng private key từ cùng một cặp key. Ngay cả cùng một public key cũng không thể được sử dụng để giải mã dữ liệu. Điều này là do các thuộc tính của chức năng hàm trapdoor mà đã được đề cập.

Khi người nhận nhận được tin nhắn được mã hóa, họ sử dụng private key của mình để truy cập dữ liệu. Nếu người nhân muốn gửi lại thông tin liên lạc theo cách an toàn, thì họ có thể mã hóa tin nhắn của mình bằng public key. Một lần nữa, khi nó đã được mã hóa bằng public key, cách duy nhất để thông tin có thể được truy cập là thông qua private key.

Theo cách này, mã hóa RSA có thể được sử dụng bởi các bên chưa biết trước đây để gửi dữ liệu một cách an toàn.



Hình 9 Phương thức hoạt động của RSA

VII. Mã hóa Base64

1. Khái niệm

Trong lập trình, Base64 là nhóm lược đồ mã hóa nhị phân thành văn bản đại diện cho dữ liệu nhị phân (cụ thể hơn là chuỗi byte 8 bit) ở định dạng chuỗi ASCII bằng việc dịch dữ liệu sang biểu diễn cơ số 64. Thuật ngữ Base64 bắt nguồn từ một mã hóa truyền nội dung MIME. Mỗi chữ số Base64 không phải là đại diện cuối cùng cho chính xác 6 bit dữ liệu. Do đó, ba byte 8 bit (24 bit) có thể được biểu diễn bằng bốn chữ số Base64 6 bit.

Thông thường tất cả các lược đồ mã hóa nhị phân thành văn bản, Base64 được thiết kế để mang dữ liệu được lưu trữ ở định dạng nhị phân qua các kênh chỉ hỗ trợ nội dung văn bản một cách đáng tin cậy. Base64 đặc biệt phổ biến trên World Wide Web, trong đó các công dụng của nó bao gồm khả năng đính các tệp hình ảnh hoặc các nội dung nhị phân khác vào bên trong các nội dung văn bản như tệp HTML và CSS.

Base64 cũng được sử dụng rộng rãi để gửi các tệp đính kèm email. Điều này bắt buộc vì SMTP chỉ được thiết kế để vận chuyển các ký tự ASCII 7-bit. Chi phí phải trả cho mã hóa này là 33–36% (33% bởi chính mã hóa; thêm tối đa 3% do ngắt dòng được chèn).

2. Đặc điểm

Bộ 64 ký tự cụ thể được chọn để đại diện cho các giá trị 64 chữ số cho cơ sở khác nhau giữa các lần triển khai. Chiến lược chung là chọn 64 ký tự phổ biến cho hầu hết các bảng mã và cũng có thể in được. Sự kết hợp này khiến dữ liệu khó có thể bị sửa đổi khi truyền qua các hệ thống thông tin, chẳng hạn như email, theo truyền thống không phải là 8-bit clean. Ví dụ, triển khai Base64 của MIME, ta sử dụng A-Z, a-z, và 0-9 cho 62 giá trị đầu tiên. Các biến thể khác chia sẻ thuộc tính này nhưng khác nhau về các ký hiệu được chọn cho hai giá trị cuối cùng; một ví dụ là UTF-7.

Các trường hợp sớm nhất của kiểu mã hóa này được tạo ra để liên lạc quay số giữa các hệ thống chạy cùng một hệ điều hành. Ví dụ: uuencode cho UNIX và BinHex cho TRS-80 (sau này được điều chỉnh cho Macintosh), và do đó có thể đưa ra nhiều giả định hơn về những ký tự nào an toàn để sử dụng. Ví dụ: uuencode sử dụng chữ hoa, chữ số và nhiều ký tự dấu câu, nhưng không sử dụng chữ thường.

3. Bảng Base64

STT	Nhị phân	Đầu ra	STT	Nhị phân	Đầu ra	STT	Nhị phân	Đầu ra	STT	Nhị phân	Đầu ra
0	000000	A	16	010000	Q	32	100000	g	48	110000	w
1	000001	B	17	010001	R	33	100001	h	49	110001	x
2	000010	C	18	010010	S	34	100010	i	50	110010	y
3	000011	D	19	010011	T	35	100011	j	51	110011	z
4	000100	E	20	010100	U	36	100100	k	52	110100	0
5	000101	F	21	010101	V	37	100101	l	53	110101	1
6	000110	G	22	010110	W	38	100110	m	54	110110	2
7	000111	H	23	010111	X	39	100111	n	55	110111	3
8	001000	I	24	011000	Y	40	101000	o	56	111000	4
9	001001	J	25	011001	Z	41	101001	p	57	111001	5
10	001010	K	26	011010	a	42	101010	q	58	111010	6
11	001011	L	27	011011	b	43	101011	r	59	111011	7
12	001100	M	28	011100	c	44	101100	s	60	111100	8
13	001101	N	29	011101	d	45	101101	t	61	111101	9
14	001110	O	30	011110	e	46	101110	u	62	111110	+
15	001111	P	31	011111	f	47	101111	v	63	111111	/
Đệm		=									

Hình 10 Bảng mục lục ký tự của Base64

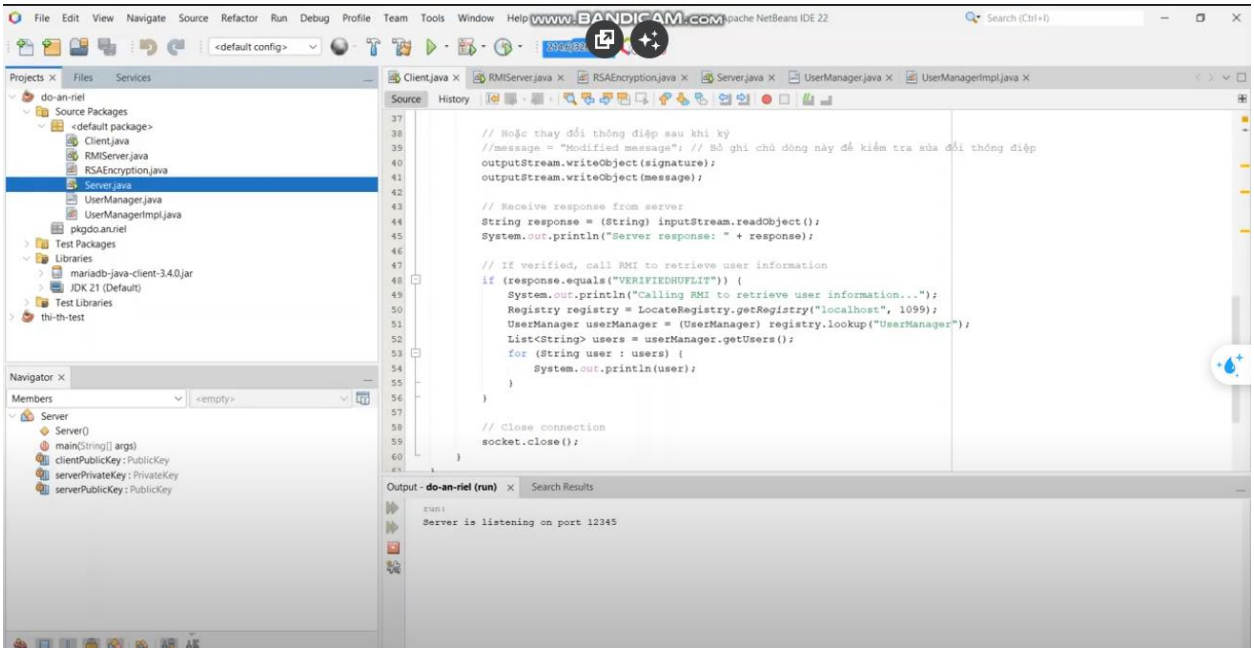
Chương 3: Thực hành

- **Trước khi dùng khóa Private Key**

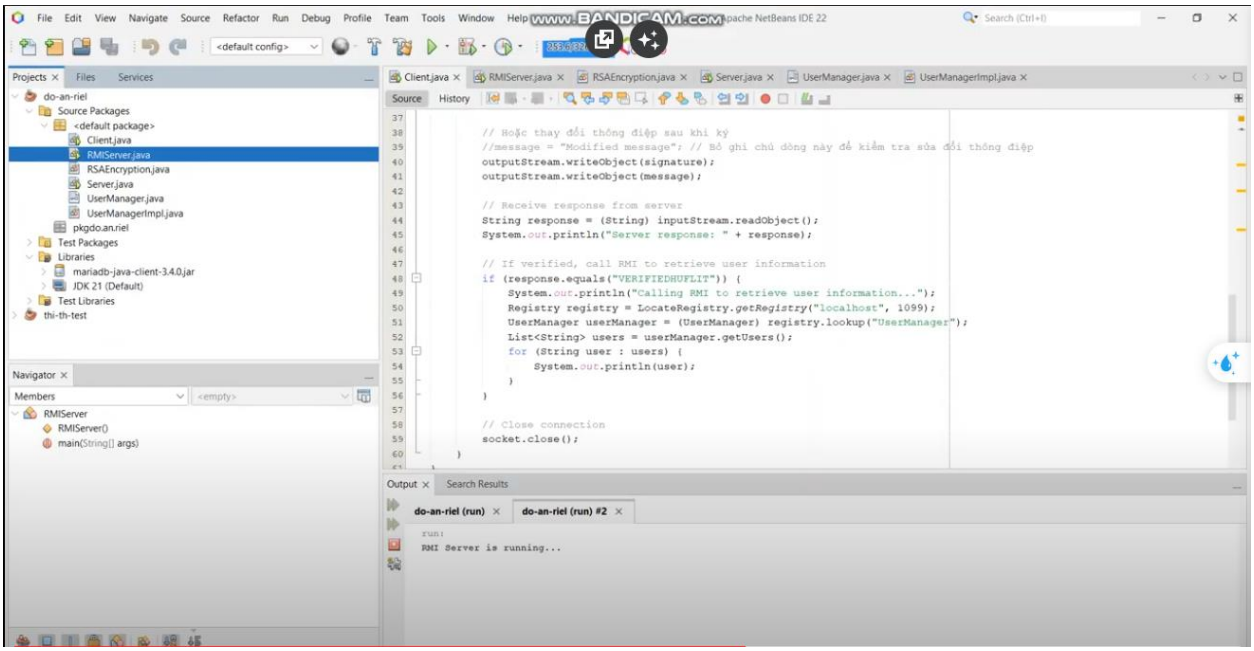
```
MariaDB [(none)]> use UserInfo;
Database changed
MariaDB [UserInfo]> show tables;
+--------------------+
| Tables_in_userinfo |
+--------------------+
| user               |
+--------------------+
1 row in set (0.001 sec)

MariaDB [UserInfo]> select * from user;
+----+---------+-------------+-----+
| id | name    | phonenumber | age |
+----+---------+-------------+-----+
|  1 | Alice   | 1234567890  |  30 |
|  2 | Bob     | 0987654321  |  25 |
|  3 | Charlie | 1231231234  |  35 |
|  4 | David   | 3213214321  |  28 |
|  5 | Eve     | 9879879870  |  22 |
+----+---------+-------------+-----+
5 rows in set (0.000 sec)
```

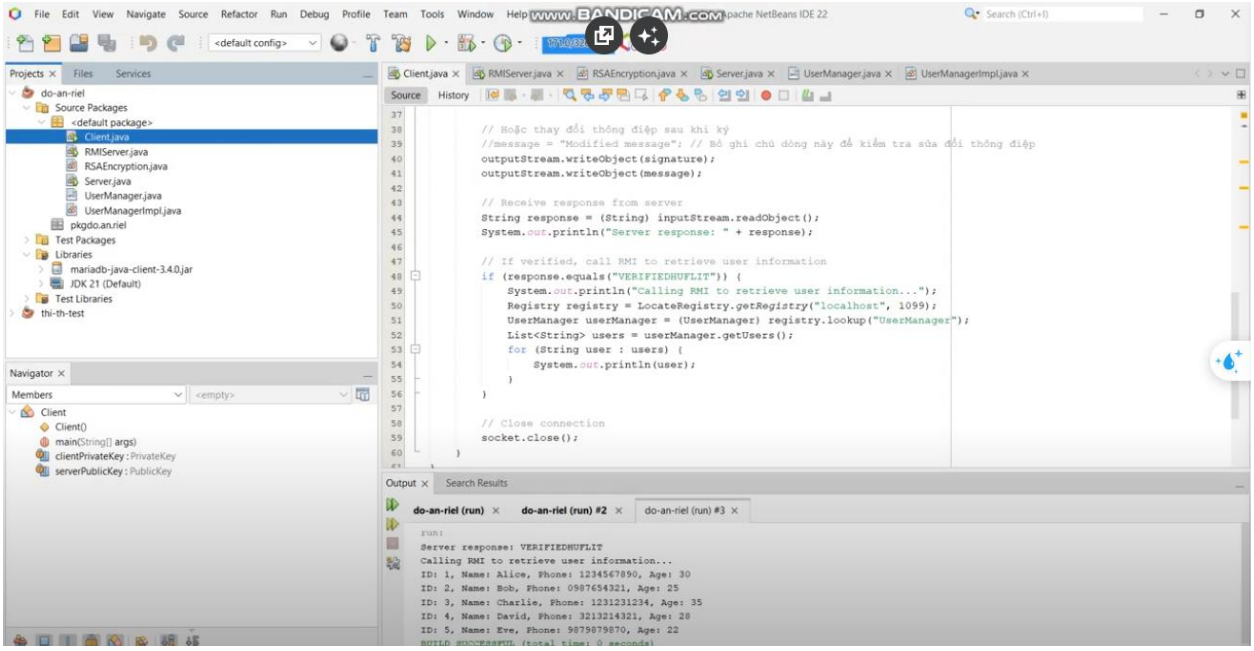
Hình 11 Database UserInfo



Hình 12 Run Server



Hình 13 Run RMI Server

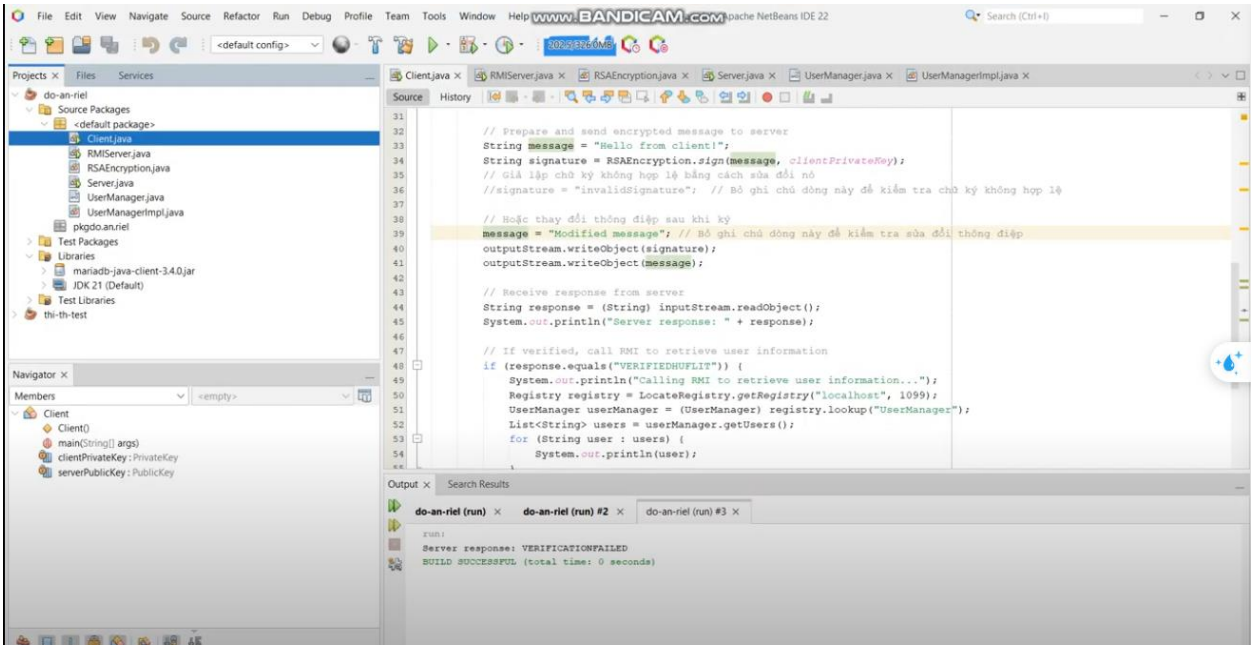


Hình 14 Run Client

- **Sau khi có khóa Private Key**

```
31
32      // Prepare and send encrypted message to server
33      String message = "Hello from client!";
34      String signature = RSAEncryption.sign(message, clientPrivateKey);
35      // Giả lập chữ ký không hợp lệ bằng cách sửa đổi nó
36      //signature = "invalidSignature";  // Bỏ ghi chú dòng này để kiểm tra chữ ký không hợp lệ
37
38      // Hoặc thay đổi thông điệp sau khi ký
39      //message = "Modified message"; // Bỏ ghi chú dòng này để kiểm tra sửa đổi thông điệp
40      outputStream.writeObject(signature);
41      outputStream.writeObject(message);
42
43      // Receive response from server
44      String response = (String) inputStream.readObject();
45      System.out.println("Server response: " + response);
46
47      // If verified, call RMI to retrieve user information
48      if (response.equals("VERIFIEDHUFLIT")) {
49          System.out.println("Calling RMI to retrieve user information...");
50          Registry registry = LocateRegistry.getRegistry("localhost", 1099);
51          UserManager userManager = (UserManager) registry.lookup("UserManager");
52          List<String> users = userManager.getUsers();
53          for (String user : users) {
54              System.out.println(user);
```

Hình 15 Bỏ ghi chú dòng 39 và Run lại



Hình 16 Kết quả

Chương 4: Kết luận

Tài liệu tham khảo

https://songoaivu.hatinh.gov.vn/chu-ky-so-la-gihuong-dan-cach-tao-chu-ky-so-ca-nhan-don-gian-1692928130.html#:~:text="Chữ%20ký%20số"%20là%20một,như%20hợp%20đồng%2C%20hóa%20đơn…

https://codegym.vn/blog/lap-trinh-mang-la-gi/

https://vietnix.vn/rsa/