

|  |
| --- |
| **BỘ CÔNG THƯƠNG**  **TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**  Description: http://1.bp.blogspot.com/-oDrDn6oV3I0/TlfpS866QKI/AAAAAAAAAFU/CGNG7JWUeuw/s1600/LOGO+TRUONG.JPG |

**SỔ ĐIỂM DANH KÌ 6**

GIÁO VIÊN : TRẦN MAI LINH

LỚP : HTTT2

KHÓA: K16

HÀ NỘI 2024

MỤC LỤC

[DANH MỤC HÌNH ẢNH 4](#_Toc159823529)

[LỜI CẢM ƠN 6](#_Toc159823530)

[LỜI MỞ ĐẦU 7](#_Toc159823531)

[CHƯƠNG 1. TỔNG QUAN VỀ ĐỀ TÀI NGHIÊN CỨU 9](#_Toc159823532)

[1.1. Tổng quát về đề tài 9](#_Toc159823533)

[1.2. Tầm quan trọng của việc xây dựng sản phẩm tạo chữ ký số và giải mã chữ ký số cho các hợp đồng kinh tế. 9](#_Toc159823534)

[1.3. Mục tiêu nghiên cứu 11](#_Toc159823535)

[1.4. Phương pháp và công cụ nghiên cứu: 12](#_Toc159823536)

[CHƯƠNG 2. PHÂN TÍCH VÀ THIẾT KẾ 15](#_Toc159823537)

[2.1 Giới thiệu 15](#_Toc159823538)

[2.2 Nội dung nghiên cứu 15](#_Toc159823539)

[2.2.1 Hệ mã hóa bất đối xứng 16](#_Toc159823540)

[2.2.2 Chữ ký điện tử 18](#_Toc159823541)

[2.2.3 Chữ ký số 19](#_Toc159823542)

[2.2.4 Hàm băm 24](#_Toc159823543)

[2.2.5 Hệ mã hóa RSA 27](#_Toc159823544)

[2.2.6 Xây dựng tạo chữ ký số và giải mã chữ ký số cho các hợp đồng kinh tế 30](#_Toc159823545)

[CHƯƠNG 3. KẾT QUẢ THỰC HIỆN 35](#_Toc159823546)

[3.1. Tìm hiểu yêu cầu bài toán 35](#_Toc159823547)

[3.2. Xây dựng bài toàn 35](#_Toc159823548)

[3.2.1 Phân tích yêu cầu người dùng 35](#_Toc159823549)

[3.2.2 Thiết kế hệ thống 36](#_Toc159823550)

[3.3 Thực hiện bài toán 37](#_Toc159823551)

[3.3.1 Tạo khóa 37](#_Toc159823552)

[3.3.2 Đăng ký khóa 39](#_Toc159823553)

[3.3.3 Tìm thông tin khóa 41](#_Toc159823554)

[3.3.4 Tạo chữ ký 42](#_Toc159823555)

[3.3.5 Xác thực chữ ký 44](#_Toc159823556)

[CHƯƠNG 4: KẾT LUẬN VÀ BÀI HỌC KINH NGHIỆM 47](#_Toc159823557)

[4.1. Kiến thức kỹ năng đã học được trong quá trình thực hiện đề tài 47](#_Toc159823558)

[4.2. Tổng kết nội dung báo cáo 48](#_Toc159823559)

[TÀI LIỆU THAM KHẢO 50](#_Toc159823560)

DANH MỤC HÌNH ẢNH

[Hình ảnh 2-1: Khóa mã hóa và giải mã 13](#_Toc159433494)

[Hình ảnh 2-2: Chữ ký số 16](#_Toc159433495)

[Hình ảnh 2-3: Sơ đồ giải thuật 23](#_Toc159433496)

[Hình ảnh 2-4: Quy trình tạo chữ ký số 26](#_Toc159433497)

[Hình ảnh 2-5: Quy trình xác nhận chữ ký số 27](#_Toc159433498)

[Hình ảnh 3-1: Biểu đồ use case 29](#_Toc159433499)

[Hình ảnh 3-2: Hình ảnh thiết kế cơ sở dữ liệu 31](#_Toc159433500)

[Hình ảnh 3-3: Chức năng tạo khóa 32](#_Toc159433501)

[Hình ảnh 3-4: Sau khi bấm nút “Tạo khóa” 32](#_Toc159433502)

[Hình ảnh 3-5: 2 file được tải xuống sau khi bấm tải khóa 33](#_Toc159433503)

[Hình ảnh 3-6: Controller xử lý yêu cầu GET “/generate-key” 33](#_Toc159433504)

[Hình ảnh 3-7: Phần code tạo khóa 33](#_Toc159433505)

[Hình ảnh 3-8: Phần code cho chức năng tải khóa 34](#_Toc159433506)

[Hình ảnh 3-9: Chức năng đăng kí khóa chủ sở hữu khóa 34](#_Toc159433507)

[Hình ảnh 3-10: Sau khi đăng kí khóa thành công 35](#_Toc159433508)

[Hình ảnh 3-11: Controller cho yêu cầu GET “/register-key” 35](#_Toc159433509)

[Hình ảnh 3-12: Xử lý gửi yêu cầu đăng ký key 35](#_Toc159433510)

[Hình ảnh 3-13: Controller xử lý yêu cầu POST “/register” 36](#_Toc159433511)

[Hình ảnh 3-14: Service xử lý lưu thông tin khóa 36](#_Toc159433512)

[Hình ảnh 3-15: Chức năng tìm thông tin khóa 37](#_Toc159433513)

[Hình ảnh 3-16: Sau khi tìm kiếm thông tin của 1 khóa 38](#_Toc159433514)

[Hình ảnh 3-17: Controller cho yêu cầu GET “/thông tin khóa” 38](#_Toc159433515)

[Hình ảnh 3-18: Phần xử lý gửi yêu cầu tìm thông tin khóa 39](#_Toc159433516)

[Hình ảnh 3-19: Controller cho yêu cầu POST “/upload” 39](#_Toc159433517)

[Hình ảnh 3-20: Service xử lý tìm thông tin của khóa 39](#_Toc159433518)

[Hình ảnh 3-21: Chức năng kí file 40](#_Toc159433519)

[Hình ảnh 3-22: Sau khi thực hiện chức năng kí file 41](#_Toc159433520)

[Hình ảnh 3-23: File chữ kí được tải xuống 41](#_Toc159433521)

[Hình ảnh 3-24: Controller cho yêu cầu GET “/sign-file” 41](#_Toc159433522)

[Hình ảnh 3-25: Phần xử lý tạo chữ kí 42](#_Toc159433523)

[Hình ảnh 3-26: Phần xử lý tải chữ kí 42](#_Toc159433524)

[Hình ảnh 3-27: Chức năng xác thực chữ kí 43](#_Toc159433525)

[Hình ảnh 3-28: Sau khi xác thực chữ kí 44](#_Toc159433526)

[Hình ảnh 3-29: Controller xử lý yêu cầu GET “/verify-file” 44](#_Toc159433527)

[Hình ảnh 3-30: Phần xử lý xác thực chữ ký 45](#_Toc159433528)

# 

LỜI CẢM ƠN

Trước tiên, chúng em xin gửi lời cảm ơn chân thành tới giảng viên hướng dẫn TS. Lê Thị Anh, người đã giảng dạy chúng em trong thời gian học tập vừa qua, thầy đã cung cấp cho chúng em những kiến thức quý báu làm nền tảng để ứng dụng vào dự án nghiên cứu của mình.

Nhờ đó bài báo cáo này của chúng em đã được hoàn thiện một cách tốt nhất, đồng thời trong thời gian thực hiện dự án nghiên cứu, chúng em đã có thêm cho mình nhiều kiến thức bổ ích, tinh thần học tập hiệu quả, nghiêm túc và cả kĩ năng làm việc nhóm hiệu quả. Đây chắc chắn sẽ là những kiến thức mà chúng em có thể vận dụng vào học tập và công việc sau này.

Bài báo cáo thực hiện trong quá trình chúng em học tập môn học. Bước đầu đi vào thực tế của chúng em còn hạn chế và còn nhiều bỡ ngỡ nên không tránh khỏi những thiếu sót, chúng em rất mong nhận được những ý kiến đóng góp quý báu của Cô để bài báo cáo của chúng em được hoàn thiện hơn đồng thời có điều kiện bổ sung, nâng cao kiến thức của mình.

*Chúng em xin chân thành cảm ơn!*

LỜI MỞ ĐẦU

Ngày nay trong mọi hoạt động của con người thông tin đóng một vai trò quan trọng không thể thiếu. Xã hội càng phát triển nhu cầu trao đổi thông tin giữa các thành phần trong xã hội ngày càng lớn. Mạng máy tính ra đời đã mang lại cho con người rất nhiều lợi ích trong việc trao đổi và xử lý thông tin một cách nhanh chóng và chính xác. Chính từ những thuận lợi này đã đặt ra cho chúng ta một câu hỏi, liệu thông tin đi từ nơi gửi đến nơi nhận có đảm bảo tuyệt đối an toàn, ai có thể đảm bảo thông tin của ta không bị truy cập bất hợp pháp. Thông tin được lưu giữ, truyền dẫn, cùng sử dụng trên mạng lưới thông tin công cộng có thể bị nghe trộm, chiếm đoạt, xuyên tạc hoặc phá huỷ dẫn đến sự tổn thất không thể lường được. Đặc biệt là đối với những số liệu của hệ thống ngân hàng, hệ thống thương mại, cơ quan quản lý của chính phủ hoặc thuộc lĩnh vực quân sự được lưu giữ và truyền dẫn trên mạng. Nếu như vì nhân tố an toàn mà thông tin không dám đưa lên mạng thì hiệu suất làm việc cũng như hiệu suất lợi dụng nguồn dữ liệu đều sẽ bị ảnh hưởng. Trước các yêu cầu cần thiết đó, việc mã hoá thông tin sẽ đảm bảo an toàn cho thông tin tại nơi lưu trữ cũng như khi thông tin được truyền trên mạng.

Các phương thức tấn công thông qua mạng ngày càng tinh vi, phức tạp có thể dẫn đến mất mát thông tin, thậm chí có thể làm sụp đổ hoàn toàn hệ thống thông tin của tổ chức. Vì vậy an toàn thông tin là nhiệm vụ quan trọng, nặng nề và khó đoán trước đối với các hệ thống thông tin.

Một trong những ứng dụng của an toàn thông tin là chữ ký số. Với đặc điểm là đơn giản cho người sử dụng mà vẫn đảm bảo được tính bảo mật, kỹ thuật sử dụng chữ ký số là một trong những kỹ thuật được sử dụng phổ biến, đa dạng trong hầu hết các lĩnh vực, nhất là Tài chính, Ngân hàng, Kế toán…

Để ứng dụng các phương pháp trên vào thực tiễn, cùng với sự hướng dẫn của GV TS. Lê Thị Anh , chúng em lựa chọn đề tài “**Xây dựng sản phẩm tạo chữ ký số và giải mã chữ ký số cho các hợp đồng kinh tế** ”. Sau quá trình tìm hiểu và cùng nhau đưa ra ý kiến nhóm chúng em đã chia bài báo cáo của mình thành 4 nội dung chính được trình bày như sau:

Chương 1: Tổng quan về đề tài nghiên cứu

Chương 2: Phân tích và thiết kế

Chương 3: Kết quả thực hiện

Chương 4: Kết luận và bài học kinh nghiệm

# 

CHƯƠNG 1. TỔNG QUAN VỀ ĐỀ TÀI NGHIÊN CỨU

1.1. Tổng quát về đề tài

Chữ ký số điện tử đóng vai trò quan trọng trong việc bảo mật thông tin trực tuyến, và một trong những phương pháp phổ biến được sử dụng để tạo chữ ký số là hệ thống RSA. RSA, viết tắt của ba nhà toán học tên là Rivest, Shamir và Adleman, là một thuật toán mã hóa và giải mã dựa trên việc sử dụng khóa công khai và khóa riêng tư.

Ứng dụng của RSA trong chữ ký số điện tử giúp xác nhận tính toàn vẹn và nguồn gốc của thông tin truyền tải qua mạng. Không giống như chữ ký truyền thống, chữ ký số không chỉ đơn giản là một hình chữ ký ảo mà còn chứa thông tin về quá trình tạo chữ ký và khóa công khai của người tạo chữ ký.

Hệ thống RSA sử dụng một cặp khóa: khóa công khai dùng để mã hóa và kiểm tra chữ ký, trong khi khóa riêng tư được giữ bí mật để giải mã và tạo chữ ký. Điều này đảm bảo rằng chỉ người có khóa riêng tư mới có thể tạo ra chữ ký phù hợp với khóa công khai được công bố.

Việc ứng dụng RSA trong chữ ký số điện tử giúp ngăn chặn việc giả mạo thông tin và tăng cường bảo mật trong giao tiếp trực tuyến. Công nghệ này đóng vai trò quan trọng trong các lĩnh vực như giao dịch tài chính trực tuyến, chính trị điện tử và bảo vệ thông tin cá nhân trên Internet.

1.2. Tầm quan trọng của việc xây dựng sản phẩm tạo chữ ký số và giải mã chữ ký số cho các hợp đồng kinh tế.

Trong thời đại ngày nay, nền kinh tế thế giới ngày càng chuyển hướng vào môi trường kinh doanh trực tuyến, làm tăng nhu cầu về sự an toàn, bảo mật và chứng thực trong các giao dịch điện tử. Việc xây dựng sản phẩm tạo chữ ký số và giải mã chữ ký số trở thành một yếu tố cực kỳ quan trọng để đảm bảo tính toàn vẹn, uy tín và hiệu quả của các hoạt động kinh doanh đặc biệt là trong quá trình giao dịch hợp đồng và chứng thực thông tin trực tuyến.Trong quá trình tìm hiểu và nghiên cứu nhóm chúng em có rút ra được một số thông tin về tầm quan trọng của việc triển khai sản phẩm như vậy:

+ Bảo mật thông tin và Chứng thực danh tính:

*Bảo mật thông tin:*

Chữ ký số đảm bảo an toàn cho dữ liệu trong quá trình truyền tải và lưu trữ, sử dụng các thuật toán mã hóa mạnh mẽ. Ngăn chặn bất kỳ thay đổi nào của thông tin trực tuyến mà không được sự cho phép.

*Chứng thực danh tính:*

Chữ ký số là công cụ quan trọng để chứng minh nguồn gốc và danh tính của người ký. Xác thực điện tử này tạo ra một lớp bảo vệ cao, đặc biệt quan trọng trong các giao dịch tài chính và pháp lý.

+ Pháp lý và Tuân thủ:

Sản phẩm tạo chữ ký số giúp tổ chức và cá nhân tuân thủ các quy định và luật lệ pháp lý liên quan đến việc sử dụng chữ ký và xác thực điện tử. Cung cấp một phương tiện hợp lệ để chứng minh độ chắc chắn của giao dịch trong trường hợp tranh chấp.

+ Hiệu quả và Tiết kiệm thời gian:

Sản phẩm này giảm bớt sự phụ thuộc vào giấy tờ và quy trình thủ tục truyền thống, từ đó giúp tối ưu hóa thời gian và giảm chi phí. Quá trình xử lý hợp đồng và giao dịch trở nên nhanh chóng và hiệu quả hơn.

+ Thuận tiện và Linh hoạt:

Người dùng có thể ký và xác thực từ mọi nơi có kết nối internet, giảm bớt sự ràng buộc về vị trí địa lý. Doanh nghiệp có thể linh hoạt hơn trong việc hợp tác với đối tác ở xa và quốc tế.

+ Chống giả mạo và Niềm tin từ đối tác:

Chữ ký số cung cấp một cấp độ bảo mật cao, khó bị giả mạo hơn so với chữ ký giấy thông thường. Điều này giúp xây dựng niềm tin từ đối tác và khách hàng, làm tăng giá trị của thương hiệu.

+ Đồng bộ với xu hướng số hóa:

*Hỗ trợ chuyển đổi số:*

Sản phẩm này không chỉ đáp ứng nhu cầu hiện tại mà còn hỗ trợ doanh nghiệp và tổ chức thích ứng với xu hướng số hóa và cách mạng công nghiệp 4.0.

Như vậy việc xây dựng sản phẩm tạo chữ ký số và giải mã chữ ký số không chỉ là một bước quan trọng trong việc bảo vệ thông tin mà còn là yếu tố quyết định trong việc nâng cao hiệu quả và niềm tin trong môi trường kinh doanh hiện đại. Sự tích hợp này không chỉ đáp ứng nhu cầu ngày càng cao về an toàn và chứng thực mà còn đồng hành cùng các doanh nghiệp trong hành trình số hóa và đổi mới.

1.3. Mục tiêu nghiên cứu

+ Xây dựng sản phẩm chữ ký số:

Mô tả chi tiết về quá trình phát triển sản phẩm, bao gồm các công nghệ và thuật toán được sử dụng để tạo ra chữ ký số. Đồng thời, tập trung vào tính năng và giao diện người dùng của sản phẩm để làm cho quá trình tạo chữ ký trở nên dễ dàng và hiệu quả.

+ Giải mã chữ ký số cho các hợp đồng kinh tế:

Trình bày cách sản phẩm của nhóm chúng em cách giải mã chữ ký số, đảm bảo tính xác thực và không thay đổi của thông tin trong hợp đồng. Mô tả các phương pháp và thuật toán được sử dụng để đảm bảo tính an toàn và chính xác.

+ Tích hợp an toàn và bảo mật:

Thảo luận về các biện pháp an toàn và bảo mật được tích hợp trong sản phẩm để bảo vệ chữ ký số khỏi các cuộc tấn công. Mô tả cụ thể về quản lý khóa, bảo vệ trước tấn công từ chối dịch vụ (DDoS), và các phương tiện khác để đảm bảo tính bảo mật của hệ thống.

+ Tương thích và dễ tích hợp:

Đề cập đến các sản phẩm của bạn có khả năng tương thích với các hệ thống và nền tảng khác nhau. Mô tả cách tích hợp sản phẩm vào quy trình làm việc hiện tại của các tổ chức và doanh nghiệp một cách thuận lợi.

+ Tối ưu hóa hiệu suất:

Chỉ ra các biện pháp đã được thực hiện để tối ưu hóa hiệu suất của sản phẩm, bao gồm tăng tốc độ xử lý chữ ký số và giảm thời gian giải mã. Đồng thời, trình bày kết quả và so sánh với các giải pháp tương tự khác.

1.4. Phương pháp và công cụ nghiên cứu:

• Phương pháp nghiên cứu tài liệu:

Thu thập, nghiên cứu thông tin về đề tài nghiên cứu từ các giáo trình, tài liệu, các chuẩn mực cơ bản trong việc xây dựng các đề tài có liên quan, tìm kiếm và tham khảo các đề tài tương tự trên các trang internet… Qua đó, chọn lọc những tài liệu cần thiết cho mục đích nghiên cứu và đối chiếu với thực tế nghiên cứu.

• Phương pháp thu thập số liệu:

Phương pháp thu thập số liệu thứ cấp: Dữ liệu thứ cấp được thu thập thông qua việc tìm hiểu trên sách báo, giáo trình, các tài liệu trên internet, thư viện và tham khảo các bài viết có liên quan.

• Sử dụng ngôn ngữ lập trình Java:

Java là một ngôn ngữ lập trình đa mục đích, nó được thiết kế để làm cho ứng dụng có thể chạy trên nhiều nền tảng khác nhau mà không cần sửa đổi mã nguồn. Điều này giúp đảm bảo tính tương thích và linh hoạt khi triển khai hệ thống chữ ký số trên nhiều môi trường hệ thống.

**Bảo mật cao( High Security)**

+ Java có tính bảo mật cao có cơ sở hạ tầng bảo mật mạnh mẽ, bao gồm các tính năng như sandboxing và kiểm soát quyền truy cập.

+ Các thư viện mã nguồn mở của Java như Bouncy Castle cung cấp các công cụ mạnh mẽ để xây dựng và xử lý chữ ký số.

**Thư viện mã nguồn mở (Open Source Libraries):**

+ Java có nhiều thư viện mã nguồn mở mạnh mẽ như Bouncy Castle, Apache Commons Codec, và OpenJDK Security, giúp phát triển ứng dụng chữ ký số hiệu quả và bảo mật.

+ Các thư viện này cung cấp các công cụ cho việc tạo chữ ký, xác thực, và giải mã chữ ký.

**Tích hợp dễ dàng ( Easy integration)**

+ Java hỗ trợ giao tiếp linh hoạt thông qua API và giao diện, giúp tích hợp ứng dụng chữ ký số vào các hệ thống và ứng dụng khác một cách dễ dàng.

+ Java có khả năng liên kết với các dịch vụ web, cơ sở dữ liệu, và các phương tiện truyền thông khác, tăng khả năng tích hợp của hệ thống chữ ký số.

**Hiệu suất và Linh hoạt (Performance and Flexibility):**

+ Java có hiệu suất cao và linh hoạt, cho phép xử lý một lượng lớn dữ liệu mà không làm giảm hiệu suất.

+ Java Virtual Machine (JVM) giúp ứng dụng chữ ký số chạy trên nhiều nền tảng mà không mất đi hiệu suất.

**Cộng đồng hỗ trợ (Strong Community Support):**

+ Java có một cộng đồng lớn, đa dạng, và chủ động. Điều này có nghĩa là có sẵn nhiều tài nguyên, tư duy, và hỗ trợ từ cộng đồng để giải quyết vấn đề và tối ưu hóa ứng dụng chữ ký số.

Từ đó cho ta thấy rằng việc sử dụng ngôn ngữ Java để tạo và giải mã chữ ký số mang lại sự linh hoạt, bảo mật cao, và tính toàn vẹn, giúp tăng cường an toàn trong các giao dịch kinh tế và bảo vệ thông tin quan trọng.

CHƯƠNG 2. PHÂN TÍCH VÀ THIẾT KẾ

2.1 Giới thiệu

- Chữ ký điện tử là một phương thức xác thực và xác nhận tính toàn vẹn của thông tin điện tử. Nó được sử dụng để xác định nguồn gốc và xác thực tính xác thực của một tài liệu, tệp tin hoặc thông điệp điện tử.

- Thay vì sử dụng chữ ký bằng mực truyền thống trên giấy, chữ ký điện tử được tạo ra và gắn kết với thông tin điện tử bằng cách sử dụng các thuật toán mã hóa và công nghệ mật mã. Chữ ký điện tử bao gồm một tập hợp các dữ liệu số, thường được gọi là "băm" (hash), được tạo ra từ thông tin cần ký và một khóa riêng (private key). Khi chữ ký điện tử được gắn kết với thông tin, nó có thể được xác minh bằng cách sử dụng khóa công khai (public key) tương ứng với khóa riêng đã được sử dụng để tạo chữ ký.

- Khi thông tin điện tử được ký bằng chữ ký điện tử, bất kỳ thay đổi nào trong thông tin sẽ làm thay đổi băm (hash) và chữ ký điện tử sẽ không còn hợp lệ. Do đó, chữ ký điện tử giúp xác định tính toàn vẹn của thông tin và bảo vệ khỏi việc sửa đổi trái phép.

- Chữ ký điện tử được áp dụng rộng rãi trong các lĩnh vực như giao dịch tài chính trực tuyến, chứng thực người dùng, ký hợp đồng điện tử và trao đổi thông tin an toàn trên mạng.

2.2 Nội dung nghiên cứu

● Hệ mã hóa bất đối xứng

● Chữ ký số

● Hệ mã hóa RSA

● Ứng dụng RSA vào bài toán chữ ký số

Các bước thực hiện triển khai đề tài bao gồm:

● Nghiên cứu nội dung thuật toán mã hóa RSA

● Tìm hiểu và nghiên cứu chữ ký số

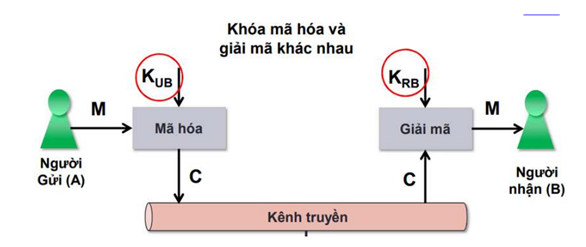
● Thiết kế và cài đặt chương trình demo thuật toán

Hình thức sản phẩm: sản phẩm bản mẫu

Kết quả đạt được: Nghiên cứu thuật toán, cài đặt chương trình và demo sản phẩm

2.2.1 Hệ mã hóa bất đối xứng

Ở hệ mật này thay vì người dùng dùng chung 1 khóa như ở hệ mật mã khóa đối xứng thì ở đây sẽ dùng 1 cặp khóa có tên là public key và private key.



Hình ảnh 2-1: Khóa mã hóa và giải mã

Hệ mật sẽ bao gồm:

● Bản rõ (plaintext-M): bản tin được sinh ra bởi bên gửi

● Bản mật (ciphertext-C): bản tin che giấu thông tin của bản rõ, được gửi tới bên nhận qua một kênh không bí mật

● Khóa: Bên nhận có 1 cặp khóa:

○ Khóa công khai (Kub) : công bố cho tất cả mọi người biết (kể cả hacker)

○ Khóa riêng (Krb) : bên nhận giữ bí mật, không chia sẻ cho bất kỳ ai

● Mã hóa (encrypt-E): C = E(Kub, M)

● Giải mã (decrypt): M = D(Krb, C) = D(Krb, E(Kub, M))

Yêu cầu đối với cặp khóa (Kub, Krb) là:

● **Sử dụng các thuật toán sinh khóa để tạo ra khóa:** đối với việc này, sự ngẫu nhiên thường được đảm bảo thông qua sự kết hợp của các yếu tố như dữ liệu đầu vào từ người dùng, nguyên tắc ngẫu nhiên của quá trình sinh khóa

● **Có quan hệ về mặt toán học 1-1:** Mỗi khóa công khai (Kub) nên có một khóa riêng (Krb) tương ứng và ngược lại. Điều này đảm bảo tính duy nhất và không mâu thuẫn của cặp khóa.

● **Không thể tính ngược:** Khóa công khai không nên có khả năng dễ dàng tính ngược để tìm ra khóa riêng. Điều này làm tăng tính an toàn của hệ thống mã hóa.

● **Krb phải được giữ mật hoàn toàn:** Khóa riêng phải được giữ mật hoàn toàn và chỉ người nhận biết được nó. Nếu khóa riêng bị rò rỉ hoặc bị truy cập bởi bên thứ ba, tính bảo mật của hệ thống sẽ bị đe dọa.

Cơ chế hoạt động:

1. Người gửi(A) gửi thông tin đã được mã hóa bằng khóa công khai (Kub) của người nhận(B) thông qua kênh truyền tin không bí mật

2. Người nhận(B) nhận được thông tin đó sẽ giải mã bằng khóa riêng (Krb) của mình.

3. Hacker cũng sẽ biết khóa công khai (Kub) của B tuy nhiên do không có khóa riêng (Krb) nên Hacker không thể xem được thông tin gửi

Ưu điểm:

● **Dễ triển khai trong hệ thống mở:** khóa công khai có thể được công bố một cách rộng rãi.

● **An toàn và bảo mật:** Tính an toàn của hệ thống dựa vào sự khó khăn của việc tính toán ngược, tức là việc tính khóa riêng từ khóa công khai. Điều này là rất khó.

● **Quản lý khóa dễ dàng:** Vì khóa công khai có thể được công bố, quản lý khóa trở nên dễ dàng hơn so với mã hóa đối xứng, nơi mà cả hai bên cần phải giữ một khóa chung bí mật.

Nhược điểm:

● **Tính chậm trễ:** Quá trình mã hóa và giải mã trong hệ mã hóa bất đối xứng thường chậm hơn, đặc biệt là khi so sánh với mã hóa đối xứng. Điều này có thể làm giảm hiệu suất trong các ứng dụng yêu cầu xử lý nhanh.

● **Dung lượng khóa lớn:** Khóa bất đối xứng thường có kích thước lớn hơn so với khóa đối xứng, làm tăng dung lượng bộ nhớ và yêu cầu lưu trữ.

2.2.2 Chữ ký điện tử

Chữ ký điện tử (Electronic signature) là thông tin đi kèm theo dữ liệu (văn bản, hình ảnh, âm thanh, …) nhằm mục đích xác định người chủ của dữ liệu đó.

Chữ ký điện tử được tạo lập dưới dạng từ, chữ, số, ký hiệu, âm thanh hoặc các hình thức khác bằng phương tiện điện tử, gắn liền hoặc kết hợp một cách lôgic với thông điệp điện tử, có khả năng xác nhận người ký thông điệp dữ liệu và xác nhận sự chấp thuận của người đó đối với nội dung thông điệp dữ liệu đã ký.

Chữ ký điện tử cũng giống như chữ viết tay, tức là chữ ký điện tử được dùng để xác nhận lời hứa hay cam kết của người nào đó và sau đó không thể chối bỏ được. Chữ ký điện tử không đòi hỏi phải sử dụng giấy mực mà nó gắn đặc điểm nhận dạng của người ký vào một bản cam kết nào đó. Như vậy, chữ ký điện tử sẽ chứng thực định danh người gửi và bảo vệ sự toàn vẹn dữ liệu.

Chữ ký điện tử được sử dụng trong các giao dịch điện tử. Xuất phát từ thực tế, chữ ký điện tử cũng cần đảm bảo các chức năng: Xác định được người chủ của một dữ liệu nào đó: văn bản, hình ảnh, video, … của dữ liệu đó có bị thay đổi hay không.

2.2.3 Chữ ký số

#### 2.2.3.1 Khái niệm chữ ký số

Chữ ký số (Digital signature) là một dạng chữ ký điện tử (tập con của chữ ký điện tử) được tạo ra bằng sự biến đổi một thông điệp dữ liệu sử dụng hệ thống mật mã công khai, theo đó người có thông điệp dữ liệu ban đầu và khóa công khai của người ký có thể xác định được chính xác: [1]

● Việc biến đổi nêu trên được tạo ra bằng đúng khóa bí mật tương ứng với khóa công khai trong cùng một cặp khóa.

● Sự toàn vẹn nội dung của thông điệp dữ liệu từ khi thực hiện biến đổi

Căn cứ theo Khoản 12, Điều 3, Luật giao dịch điện tử 2023 định nghĩa về chữ ký số như sau: “*Chữ ký số là chữ ký điện tử sử dụng thuật toán khóa không đối xứng, gồm khóa bí mật và khóa công khai, trong đó khóa bí mật được dùng để ký số và khóa công khai được dùng để kiểm tra chữ ký số. Chữ ký số bảo đảm tính xác thực, tính toàn vẹn và tính chống chối bỏ nhưng không bảo đảm tính bí mật của thông điệp dữ liệu*”.

Chữ ký điện số là chuỗi thông tin cho phép xác định nguồn gốc, xuất xứ, thực thể đã tạo ra 1 thông điệp.

Chữ ký số khóa công khai là mô hình sử dụng các kỹ thuật mật mã để gắn với mỗi người sử dụng một cặp khóa công khai - bí mật, qua đó có thể ký các văn bản điện tử cũng như trao đổi các thông tin mật.



Hình ảnh 2-2: Chữ ký số

#### 2.2.3.2 Đặc điểm chữ ký số

Có 4 đặc điểm nổi bật khi sử dụng chữ ký số:

**- Tính xác thực**: Thông qua chứng thư số của cá nhân, tổ chức, doanh nghiệp, chữ ký số có thể giúp xác thực danh tính chủ nhân của chữ ký số.

**- Tính bảo mật:** Chữ ký số có tính bảo mật gần như tuyệt đối và thông tin không dễ bị đánh cắp bởi các hacker. Vì chữ ký số có tới 2 lớp mã khóa bảo mật đó là khóa bí mật và khóa công khai.

**- Tính toàn vẹn:** Văn bản/tài liệu có chữ ký số chỉ có thể được mở bởi duy nhất một người đó là người nhận văn bản/tài liệu đó. Vì vậy, trong môi trường giao dịch điện tử, mọi thông tin của tài liệu/văn bản đều được đảm bảo toàn vẹn một cách tuyệt đối.

**- Tính chống chối bỏ:** Khi các văn bản/tài liệu/hợp đồng đã có chữ ký số thì chữ ký số này không thể thay thế cũng không thể xóa bỏ.

Với những đặc điểm này, chữ ký số phù hợp sử dụng cho nhiều đối tượng khác nhau.

#### 2.2.3.3 Đối tượng sử dụng chữ ký số

Đối tượng sử dụng chữ ký số hiện nay bao gồm tất cả mọi cá nhân và tổ chức. Theo đó, các cá nhân và tổ chức sẽ sử dụng chữ ký số cho những mục đích cụ thể như sau:

**- Chữ ký số cho cá nhân/cá nhân thuộc tổ chức/doanh nghiệp:** Được sử dụng với mục đích khai nộp thuế thu nhập cá nhân, khai báo trên trang đăng ký kinh doanh hay ký hợp đồng lao động với đơn vị sử dụng lao động,....

**- Chữ ký số cho doanh nghiệp, tổ chức:** Được sử dụng với mục đích kê khai thuế, nộp thuế, đăng ký BHXH, khai nộp thuế hải quan,....Bên cạnh đó, doanh nghiệp, tổ chức còn sử dụng chữ ký số trong việc ký văn bản nội bộ, ký giao dịch đối soát, ký giao dịch chuyển khoản ngân hàng,....và nhiều mục đích khác.

#### 2.2.3.4 Mục đích sử dụng chữ ký số

Mục đích chính của việc sử dụng chữ ký số là đảm bảo tính toàn vẹn, xác thực và không thể chối bỏ của thông tin điện tử. Dưới đây là một số mục đích chính khi sử dụng chữ ký số:

1. Xác thực nguồn gốc: Chữ ký số giúp xác định rằng một tài liệu hoặc thông điệp điện tử đã được tạo ra bởi người gửi xác định. Nó cho phép người nhận xác minh rằng thông tin đến từ nguồn tin cậy và không bị giả mạo.

2. Tính toàn vẹn: Chữ ký số đảm bảo tính toàn vẹn của thông tin. Nếu bất kỳ sửa đổi nào được thực hiện trên tài liệu sau khi chữ ký số được tạo ra, quá trình xác minh sẽ thất bại, cho thấy thông tin đã bị thay đổi.

3. Không thể chối bỏ: Chữ ký số cung cấp tính năng không thể chối bỏ. Khi một tài liệu hoặc giao dịch được ký bằng chữ ký số, người gửi không thể từ chối việc ký kết hoặc từ chối tài liệu đó sau này.

4. Bảo mật: Chữ ký số sử dụng các thuật toán mã hóa và công nghệ mật mã để bảo vệ thông tin. Khóa riêng chỉ được biết đến bởi người sở hữu và không thể bị xâm phạm, đảm bảo tính bảo mật của chữ ký số.

5. Giao dịch điện tử an toàn: Chữ ký số được sử dụng rộng rãi trong giao dịch điện tử, bao gồm giao dịch tài chính trực tuyến và ký hợp đồng điện tử. Chúng đảm bảo tính toàn vẹn và xác thực của các giao dịch, giúp ngăn chặn gian lận và xác định trách nhiệm của các bên tham gia.

Tóm lại, chữ ký số đóng vai trò quan trọng trong việc xác thực thông tin, đảm bảo tính toàn vẹn và không thể chối bỏ, đồng thời cung cấp một cơ chế bảo mật cho các hoạt động điện tử.

#### 2.2.3.5: Ưu điểm và nhược điểm của chữ ký số trong các hợp đồng kinh tế

Ưu điểm:

* Chữ ký số có khả năng xác định nguồn gốc chuẩn xác: Hệ thống mật mã hóa công khai cho phép mật mã hóa văn bản với khóa kí bí mật chỉ có chủ sở hữu của khóa mới biết. Để sử dụng chữ ký số thì văn bản phải mã hóa hàm băm. Sau khi sử dụng khóa bí mật của chủ khóa để mã hóa để có được chữ ký số. Để kiểm tra, bên nhận giải mã với khóa công khai để lấy lại hàm băm và rà soát với hàm băm của văn bản nhận được. Nếu hai giá trị này đảm bảo khớp nhau thì văn bản đó chính xác là của người sở hữu khóa bí mật.
* Chữ ký số có tính chắc chắn: Trong giao dịch, bên gửi có thể từ chối rằng văn bản đó không phải do mình gửi. Vậy nên, để phòng ngừa trường hợp này xảy ra, bên nhận có thể đề xuất bên gửi phải kèm thêm chữ ký số với văn bản. Điều này nhằm đảm bảo khi có tranh chấp, chữ ký số sẽ là một chứng cứ thuyết phục, chắc chắn để bên thứ ba giải quyết.
* Tính toàn vẹn thông tin: Doanh nghiệp sẽ không phải lo sợ vì tình trạng văn bản bị sửa đổi trong truyền đi bởi bất kỳ 1 tác nhân hay yếu tố nào đều dễ dàng bị phát hiện ngay lập tức. Quy trình mã hóa sẽ giúp ẩn nội dung thông tin với bên thứ ba.
* Tính bảo mật: Đây là ưu điểm nổi bật và tuyệt vời nhất của chữ ký số mang đến cho người dùng. Về kỹ thuật công nghệ, chữ ký số được làm dựa trên hạ tầng mã hóa công khai (PKI), trong đó phần quan trọng nhất là thuật toán mã hóa công khai RSA. Nhờ vậy, chữ ký số được tạo ra tương ứng, duy nhất với một người dùng cụ thể. Nghĩa là người khác sẽ không thể giải mạo được, chỉ có chủ sở hữu khoá bí mật mới có thể tạo ra và biết thông tin lưu trữ. Có thể khẳng định rằng, chữ ký số giúp bảo mật thông tin một cách an toàn tuyệt đối.
* Chữ ký số giúp tiết kiệm thời gian, chi phí và công sức: Vận hành doanh nghiệp, việc sử dụng chữ ký số trở thành nhu cầu thiết yếu và cần thiết. Điều này giúp doanh nghiệp dễ dàng, tiện lợi hơn trong giao dịch với ngân hàng hoặc các cơ quan hành chính khác mà không cần phải di chuyển cồng kềnh giấy tờ, hồ sơ phức tạp. Ở tại văn phòng, doanh nghiệp chỉ cần ký chữ ký số trên máy tính và gửi văn bản điện tử đến người nhận một cách gọn nhẹ, nhanh chóng.
* Sử dụng mọi lúc mọi nơi, luôn linh hoạt: Doanh nghiệp có thể sử dụng để ký kết văn bản, hợp đồng, chứng từ,… **mọi lúc mọi nơi**, kể cả trong giờ hành chính hay khi không ở trên công ty. Đây là ưu điểm của chữ ký số thể hiện sự linh hoạt, thuận tiện, giản lược được nhiều bước trong quá trình làm việc.
* Nâng cao trải nghiệm khách hàng: Theo khảo sát, hiện có khoảng **66%** sự tăng trưởng kỹ thuật số đến từ người dùng điện thoại thông minh. Điều này cho thấy, các doanh nghiệp đã thực hiện thủ tục trực tuyến thông qua điện thoại cá nhân nhiều hơn. Các khách hàng cũng hài lòng về việc sử dụng chữ ký số vì thủ tục đơn giản, không mất nhiều thời gian, công sức.
* Nâng cao hiệu quả hoạt động của doanh nghiệp: Chữ ký số **dùng được mọi lúc mọi nơi** một cách linh hoạt với những thủ tục đơn giản, nhanh chóng. Giúp thời gian **quay vòng hợp đồng nhanh hơn, công việc cần xử lý ít hơn**, giúp tăng hiệu quả hoạt động cho doanh nghiệp.
* Nâng cao danh tiếng của doanh nghiệp: Sử dụng chữ ký điện tử giúp **tăng hiệu quả làm việc** của doanh nghiệp sẽ tăng lên đáng kể. Giúp thúc đẩy danh tiếng, thể hiện được sự **nhanh nhẹn, linh động trong thời đại công nghệ**. Khách hàng, đối tác cũng sẽ thích hợp tác và có cảm tình tốt với doanh nghiệp, tiến tới giúp các giao dịch trở nên nhanh chóng và dễ dàng. [2]

Nhược điểm:

* Phức tạp trong quá trình chứng minh nếu xảy ra sai sót và giả mạo: Dù trường hợp sai sót, giả mạo chữ ký số rất hiếm khi xảy ra, tuy nhiên bạn nên dự liệu trước. Khi chữ ký số gặp trục trặc, cản trở việc xác minh người sử dụng không chính xác thì việc kiểm chứng lại chữ ký số đó sẽ khá khó khăn, tốn kém thời gian. Đây cũng là hạn chế khó tránh trong phương thức xác nhận bằng công nghệ cao. Tuy nhiên, biện pháp hiệu quả để khắc phục, hạn chế tình trạng này là cần cải thiện tính bảo mật, chắc chắn chữ ký số để giảm thiểu rủi ro cho người dùng.
* Chi phí : Để thực hiện thuật toán RSA phần lớn tốn chi phí thực hiện các phép tính cơ bản như : Tạo khóa, mã hóa, giải mã. Quá trình mã hóa, giải mã tương được với chi phí thực hiện các phép tính lũy thừa modulo n. Để đảm bảo cho khóa bí mật được an toàn thì thường chọn mũ công khai e nhỏ hơn nhiều so với số mũ bí mật d, do đó chi phí thời gian để thực hiện mã hóa dữ liệu nhỏ hơn nhiều so với thời gian giải mã. [2]

2.2.4 Hàm băm

* Lý thuyết

*Hàm băm (Hash Function)* là hàm toán học chuyển đổi thông điệp (message) có độ dài bất kỳ (hữu hạn) thành một dãy bit có độ dài cố định (tùy thuộc vào thuật toán băm). Dãy bít này được gọi là thông điệp rút gọn (message digest) hay giá trị băm (hash value), đại diện cho thông điệp ban đầu. [3]

* Tính chất cơ bản của hàm băm

Tính chất cơ bản của hàm băm mật mã là tính một chiều. Nghĩa là, một hàm mà trên thực tế không thể có ngược. Nếu bạn có một giá trị băm đầu ra, bạn sẽ không thể suy ngược lại được giá trị đầu vào là gì để có thể băm ra một thông điệp băm như vậy, hoặc ít nhất là rất khó suy luận được ra, trừ khi bạn vét cạn hết toàn bộ các khả năng có thể của thông điệp đầu vào. Đây là tính chất vô cùng quan trọng của hàm băm mật mã biến nó thành một công cụ cơ bản của mật mã hiện đại.

* Hàm băm SHA-1: Thuật toán SHA-1 nhận thông điệp ở đầu vào có chiều dài k<264 bit, thực hiện xử lý và đưa ra thông điệp thu gọn (message digest) có chiều dài cố định 160 bits. Quá trình tính toán cũng thực hiện theo từng khối 512bits, nhưng bộ đệm xử lý dùng 5 thanh ghi 32-bits. Thuật toán này chạy tốt với các bộ vi xử lý có cấu trúc 32 bits.
* Hàm băm SHA-2 thực chất bao gồm hai thuật toán băm: SHA-256 và SHA-512. SHA-224 là một biến thể của SHA-256 với các giá trị khởi tạo và đầu ra bị cắt bỏ khác nhau. SHA-384 và SHA-512/224 và SHA-512/256 ít được biết đến là tất cả các biến thể của SHA-512. SHA-512 an toàn hơn SHA-256 và thường nhanh hơn SHA-256 trên các máy 64 bit như AMD64. Do có nhiều phiên bản thuật toán khác nhau do đó kích thước đầu ra của họ SHA-2 cũng khác nhau tùy theo thuật toán. Phần mở rộng của tên phía sau tiền tố “SHA” chính là độ dài của thông điệp băm đầu ra. Ví dụ với SHA-224 thì kích thước đầu ra là 224 bit (28 byte), SHA-256 tạo ra 32 byte, SHA-384 tạo ra 48 byte và cuối cùng là SHA- 512 tạo ra 64 byte. Và chúng ta có thể đã biết rằng Bitcoin sử dụng hàm băm SHA-256 là một phiên bản trong họ SHA-2 này.
* SHA-3 được NIST phát hành vào ngày 5 tháng 8 năm 2015. Đây có lẽ là tiêu chuẩn hàm băm mới nhất cho đến hiện nay. SHA-3 là một tập con của họ nguyên thủy mật mã rộng hơn là Keccak. Thuật toán Keccak được đưa ra bởi Guido Bertoni, Joan Daemen, Michael Peeters và Gilles Van Assche. Keccak dựa trên cấu trúc bọt biển (sponge). Cấu trúc này cũng có thể được sử dụng để xây dựng các nguyên thủy mã hóa khác như các hệ mật mã dòng. SHA-3 cũng có các kích cỡ đầu ra tương tự như SHA-2 bao gồm: 224, 256, 384 và 512 bit.
* MD5: Trong mật mã học, MD5 (viết tắt của tiếng Anh Message-Digest algorithm 5, Thuật toán Tiêu hóa-tin nhắn 5) là một hàm băm mật mã học được sử dụng phổ biến với giá trị băm (hash) dài 128-bit. Là một chuẩn Internet (RFC 1321), MD5 đã được dùng trong nhiều ứng dụng bảo mật, và cũng được dùng phổ biến để kiểm tra tính toàn vẹn của tập tin. Một bảng băm MD5 thường được diễn tả bằng một số hệ thập lục phân 32 ký tự.

Ví dụ: Ta có thể mô phỏng trực quan một hệ mật mã khóa công khai như sau: Bob muốn gửi cho Alice một thông tin mật mà Bob muốn duy nhất Alice có thể đọc được. Để làm được điều này, Alice gửi cho Bob một chiếc hộp có khóa đã mở sẵn (Khóa công khai) và giữ lại chìa khóa. Bob nhận chiếc hộp, cho vào đó một tờ giấy viết thư bình thường và khóa lại (như loại khóa thông thường chỉ cần sập chốt lại, sau khi sập chốt khóa ngay cả Bob cũng không thể mở lại được-không đọc lại hay sửa thông tin trong thư được nữa). Sau đó Bob gửi chiếc hộp lại cho Alice. Alice mở hộp với chìa khóa của mình và đọc thông tin trong thư. Trong ví dụ này, chiếc hộp với khóa mở đóng vai trò khóa công khai, chiếc chìa khóa chính là khóa bí mật.

+ Một số ứng dụng của hàm băm mật mã trong việc tạo chữ ký số cho các hợp đồng kinh tế.

*Đảm bảo tính toàn vẹn và xác thực*: hàm băm được sử dụng để tạo một “ bản tóm tắt” (hash value) từ nội dung của hợp đồng kinh tế. Chữ ký số được tạo ra từ giá trị băm này, giúp đảm bảo tính toàn vẹn của dữ liệu. Nếu bất kỳ thay đổi nào trong hợp đồng, giá trị băm sẽ thay đổi và chữ ký số không còn hợp lệ.

*Xác thực nguồn gốc:* Chữ ký số được tạo ra từ giá trị băm của hợp đồng giúp xác định nguồn gốc của tài liệu. Người nhận hợp đồng có thể sử dụng khóa công khai của người ký để kiểm tra chữ ký số và so sánh với giá trị băm để đảm bảo tính xác thực.

*Bảo mật chống giả tạo*: Giá trị băm không thể dễ dàng đảo ngược, làm tăng khả năng chống lại các cuộc tấn công giả mạo thông tin. Hàm băm được thiết kế để làm cho việc tính toán giá trị băm từ dữ liệu gốc trở nên dễ dàng, nhưng ngược lại, việc phục hồi dữ liệu gốc từ giá trị băm là khó khăn, thậm chí là không thể (nếu hàm băm là không thể đảo ngược). Điều này làm cho chữ ký số dựa trên giá trị băm trở nên an toàn, vì người ta không thể dễ dàng tìm ra dữ liệu gốc từ chữ ký số.

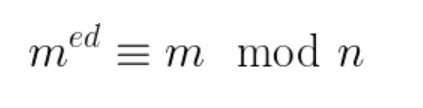
2.2.5 Hệ mã hóa RSA

Hệ mã hóa RSA là một hệ thống mã hóa khóa công khai (asymmetric encryption) được phát triển bởi ba nhà toán học Ronald Rivest, Adi Shamir và Leonard Adleman vào năm 1977. Tên của hệ thống này được lấy từ chữ cái đầu tiên của họ.

RSA dựa trên sự khó khăn trong việc phân tích số nguyên lớn thành các thừa số nguyên tố (Prime Factorization Problem). Nó sử dụng một cặp khóa, một khóa công khai (public key) và một khóa bí mật (private key). Mỗi khóa là những số cố định sử dụng trong quá trình mã hóa và giải mã. Khóa công khai được công bố rộng rãi cho mọi người và được dùng để [mã hóa](https://vi.wikipedia.org/wiki/M%C3%A3_h%C3%B3a). Những thông tin được mã hóa bằng khóa công khai chỉ có thể được giải mã bằng khóa bí mật tương ứng. Nói cách khác, mọi người đều có thể mã hóa nhưng chỉ có người biết khóa cá nhân (bí mật) mới có thể giải mã được. [4]

Hoạt động của RSA dựa trên 3 bước chính: Sinh khóa, mã hóa và giải mã.

**Sinh khóa**

Vấn đề cốt lõi của sinh khóa trong RSA là tìm được bộ 3 số tự nhiên e, d, và n sao cho:

Ở đây: m – là số tự nhiên được chuyển hóa từ bản rõ M

(d,n) – là khóa bí mật

(e,n) – là khóa công khai

Cần phải bảo mật d sao cho dù biết e và n hay thậm chí cả “m” cũng không thể tìm ra được “d”

Giả sử An và Bình cần trao đổi thông tin bí mật thông qua một kênh không an toàn (ví dụ như [Internet](https://vi.wikipedia.org/wiki/Internet)). Với thuật toán RSA, An đầu tiên cần tạo ra cho mình cặp khóa gồm khóa công khai và khóa bí mật theo các bước sau:

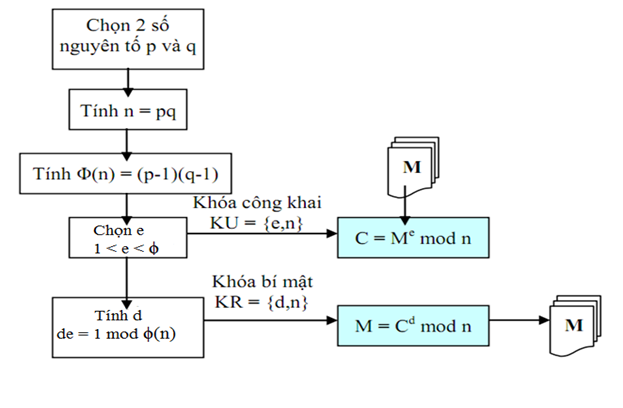
Bước 1: Chọn 2 số nguyên tố lớn p và q với p # q, lựa chọn ngẫu nhiên độc lập.

Bước 2: Tính n = p\*q và φ(*n*) = (p-1)(q-1)

Bước 3: Chọn một số ngẫu nhiên e (1< e <φ(*n*) )) sao cho gcd( e, φ(*n*) )) = 1

Bước 4: Sử dụng thuật toán Euclide mở rộng để tính số d, 1< d < φ(*n*). Sao cho e.d ≡ 1 (mod φ(*n*))

Bước 5: Khóa công khai là (n,e), khóa bí mật là (n,d).



Hình ảnh 2-3: Sơ đồ giải thuật

Ví dụ cụ thể:

1. Chọn hai số nguyên tố *p* = 23, *q* = 41

2. Tính: *n* = *p*\**q* = 23\*41 = 943 và φ(*n*) = 22\*40 = 880

3. Chọn *e* = 7, 1< *e* < 880. Tính *d*: Từ *e*\**d* = 1 mod 880, tìm được *d* = 503.

5. Khóa công khai là (*e*, *n*) = (7, 943);

Khóa bí mật (*d, n*) = (503, 943).

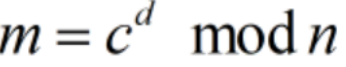
**Mã hóa và giải mã**

Trong phần này, chúng ta sẽ tìm hiểu cách mã hóa với public key(n, e) và giải mã với Private key (n, d).

**Thực hiện mã hóa RSA** như sau:

Nếu chúng ta có bản rõ M, chúng ta cần chuyển nó thành một số tự nhiên m trong khoảng (0, n) sao cho m, n nguyên tố cùng nhau.

* Mã hóa m thành d như sau:
* Sau đó c sẽ được chuyển tới người nhận

**Thực hiện giải mã RSA** tại người nhận bằng Private key (n, d):

Kết quả:

Ví dụ:

1: A nhận khóa công khai n = 943 và e = 7

2: Thông tin cần gửi m = 35

3: c = 357 mod 943

4: c = 545

5: Giải mã

m = 545503 mod 943 => m =35

2.2.6 Xây dựng tạo chữ ký số và giải mã chữ ký số cho các hợp đồng kinh tế

Khi công nghệ ngày càng phát triển, chuyển đổi số là một trong những yêu cầu bắt buộc để doanh nghiệp có thể theo kịp đối thủ và bứt phá tạo lợi thế cạnh tranh cũng như tối ưu nguồn lực. Doanh nghiệp sẽ đầu tư vào các công nghệ phù hợp, đào tạo nhân viên để sử dụng công nghệ số hiệu quả và thay đổi mô hình kinh doanh để thích nghi với nền kinh tế số. Thực hiện chuyển đổi số mang đến cho doanh nghiệp nhiều lợi ích lớn: Nâng cao hiệu quả hoạt động; Tăng cường khả năng cạnh tranh; Tăng trưởng doanh thu; Tạo ra giá trị mới. Trong quá trình chuyển đổi số, chữ ký số được doanh nghiệp đặc biệt quan tâm. Đối với các cá nhân, chữ ký số có giá trị pháp lý tương đương chữ ký tay, còn đối với các tổ chức, doanh nghiệp, chữ ký số có giá trị tương đương con dấu và chữ ký của người đại diện pháp luật. Chữ ký số cũng dùng để xác nhận cam kết của tổ chức, cá nhân đối với dữ liệu số và được pháp luật thừa nhận. Khi doanh nghiệp hoặc cá nhân thực hiện giao kết hợp đồng kinh tế điện tử để hợp đồng có giá trị pháp lý bắt buộc phải sử dụng chữ ký số theo Luật giao dịch điện tử. Trường hợp các hợp đồng kinh tế điện tử không sử dụng chữ ký số sẽ không đảm bảo tính pháp lý và dễ xảy ra tranh chấp.

Với chữ ký số, doanh nghiệp có thể thực hiện các giao dịch thương mại hoàn toàn trực tuyến. Thay vì hai bên phải di chuyển và trực tiếp gặp mặt tại trụ sở/ chi nhánh công ty, thì các tài liệu như thư ngỏ hợp tác, hợp đồng, thỏa thuận sẽ được gửi đi bằng email đến phía đối tác và được ký kết nhanh chóng bằng thiết bị máy tính hoặc điện thoại thông minh… Quy trình này làm giảm các đầu việc thủ công khác như đóng gói thư từ, dán tem, chờ đợi nhân viên bưu điện… đặc biệt tiết kiệm thời gian và tiền bạc trong trường hợp hai bên doanh nghiệp có khoảng cách xa về mặt địa lý như doanh nghiệp ở ngoại tỉnh hoặc công ty nước ngoài, cắt giảm được các khoản tiền xăng xe, ăn uống, chi phí vé máy bay, khách sạn… Chưa kể, trong trường hợp có sai sót, cần chỉnh sửa hợp đồng thì khoản phí trên có thể càng dôi lên gấp bội.

Như vậy, ta đã hiểu được chữ ký số đóng vai trò quan trọng như thế nào đối với các doanh nghiệp ngày nay. Vậy làm thế nào để xây dựng tạo ra được sản phẩm chữ ký số và giải mã chúng trong các hợp đồng kinh tế?

#### 2.2.6.1 Quy trình tạo và xác nhận chữ ký số

Quy trình tạo ra chữ ký số cho mỗi phiên làm việc như sau: Khóa bí mật được tạo ra khi một người đăng ký sử dụng dịch vụ và được lưu trữ trong một thiết bị phần cứng đặc biệt an toàn như: Token, SmartCard. Thiết bị này có hình dạng giống như USB hay một chiếc móc chìa khóa, rất nhỏ gọn, dễ mang theo. Vì được lưu trữ an toàn trong thiết bị, khóa bí mật không thể bị sao chép. Thiết bị này không có cơ chế ghi đè dữ liệu nên cũng loại trừ trường hợp bị virus phá hoại.

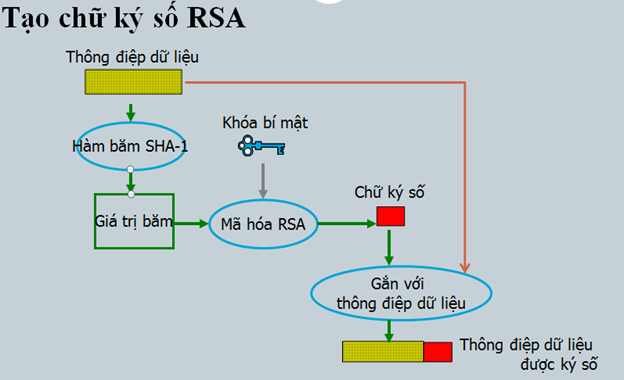
Quá trình sử dụng chữ ký số bao gồm 2 bước: [5]

Bước 1: Tạo chữ ký số ( sử dụng khóa bí mật để ký số).

Bước 2: Kiểm tra chữ ký (kiểm tra khóa công khai có hợp lệ hay không), trong đó sử dụng 3 thuật toán: tạo khóa, tạo chữ ký số, kiểm tra tính xác thực của chữ ký số. Khóa công khai thường được công khai thông qua việc chứng thực khóa công khai. Hình dưới đây là quy trình tạo và xác nhận chữ ký số.

*Khóa bí mật (Private Key)*: Là khóa không được công bố trong cặp khóa dùng để tạo chữ ký số và thuộc hệ mật mã bất đối xứng.

*Khóa công khai (Public Key)*: Là khóa được phân phối công khai trong cặp khóa dùng để kiểm tra chữ ký số, khóa công khai được tạo bởi khóa bí mật tương ứng trong cặp khóa và thuộc hệ mật mã bất đối xứng. Nếu chỉ biết khóa công khai, không thể dễ dàng tìm ra khóa bí mật dẫn tới việc giả mạo chữ ký số.



Hình ảnh 2-4: Quy trình tạo chữ ký số

Quy trình tạo chữ ký số:

**B1:** Tạo khóa bằng hệ mã hóa gồm khóa bí mật và khóa công khai. Sử dụng khóa bí mật để tạo chữ ký.

**B2:** Sử dụng thuật toán băm, để băm dữ liệu cần ký thành một chuỗi ký tự duy nhất với độ dài cố định. Có thể gọi là chuỗi H1.

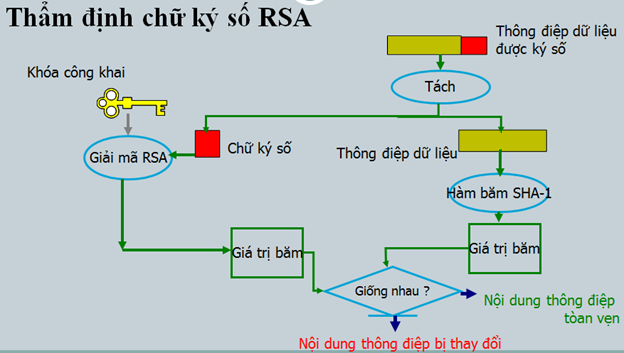
○ Lưu ý thuật toán băm dữ liệu phải được thống nhất giữa người ký và người xác nhận để có được kết quả chính xác giống nhau khi kiểm tra chữ ký.

○ Lý do mã hóa dữ liệu sau khi được băm thay vì toàn bộ dữ liệu là vì dữ liệu sau khi được băm sẽ trở thành một chuỗi có độ dài cố định. Điều này giúp tiết kiệm thời gian và giảm kích thước lưu trữ của chữ ký.

○ Giá trị sau khi băm là duy nhất. Bất kỳ thay đổi nào trong dữ liệu ngày cả thay đổi một ký tự cũng sẽ dẫn đến giá trị khác. Thuộc tính này cho phép người sử dụng có thể xác định được tính toàn vẹn của dữ liệu.

**B3:** Sử dụng khóa bí mật để mã hóa chuỗi được băm từ dữ liệu ban đầu theo hệ mã hóa được chọn. Bản mã của quá trình mã hóa chính là chữ ký số được tạo ra.

**B4:** Gửi dữ liệu cần xác thực và chữ ký cho người nhận. Có thể thực hiện theo 2 cách:  
 + Gửi riêng chữ ký và dữ liệu gốc cho người nhận.  
 + Ghép chữ ký vào nội dung của dữ liệu cần ký và gửi dữ liệu sau khi ghép cho người nhận. Người nhận sau khi nhận được sẽ cần tách chữ ký ra khỏi dữ liệu gốc để có thể xác thực chữ ký.



Hình ảnh 2-5: Quy trình xác nhận chữ ký số

Trong hình ta thấy:

Quy trình kiểm tra chữ ký

**B1:** Nhận dữ liệu gốc và chữ ký của người ký. Nếu chữ ký được ghép vào dữ liệu gốc thì cần tách riêng nội dung và chữ ký để có thể xử lý độc lập.

**B2:** Ở phần nội dung gốc, người nhận làm công việc giống như người ký đó là sử dụng chương trình thuật toán băm đã được thống nhất với người ký để băm dữ liệu gốc. Có thể gọi là chuối H2.

**B3:** Người nhận sử dụng khóa công khai do người ký cung cấp để giải mã chữ ký, từ đó thu được chỗi H1 là một chuỗi có độ dài cố định được sinh ra sau khi người ký băm dữ liệu gốc.

**B4:** Đối chiếu thông tin trùng khớp giữa chuỗi H1 và chuỗi H2. Nếu khớp nhau tức nội dung của dữ liệu chính xác không bị thay đổi, xác định được người tạo chính là người ký và hoàn tất quá trình kiểm tra chữ ký. Nếu thông tin chuỗi H1 và H2 không trùng khớp, tức là nội dung bị thay đổi hoặc chữ ký không chính xác.

**Lưu ý:** Bất kỳ thay đổi dù là nhỏ nhất vào nội dung thông điệp sau khi đã khởi tạo chữ ký điện tử cũng sẽ tạo ra kết quả hoàn toàn khác ở phía người nhận khi họ băm dữ liệu và thực hiện đối chiếu với chữ ký đã được mã hóa.

CHƯƠNG 3. KẾT QUẢ THỰC HIỆN

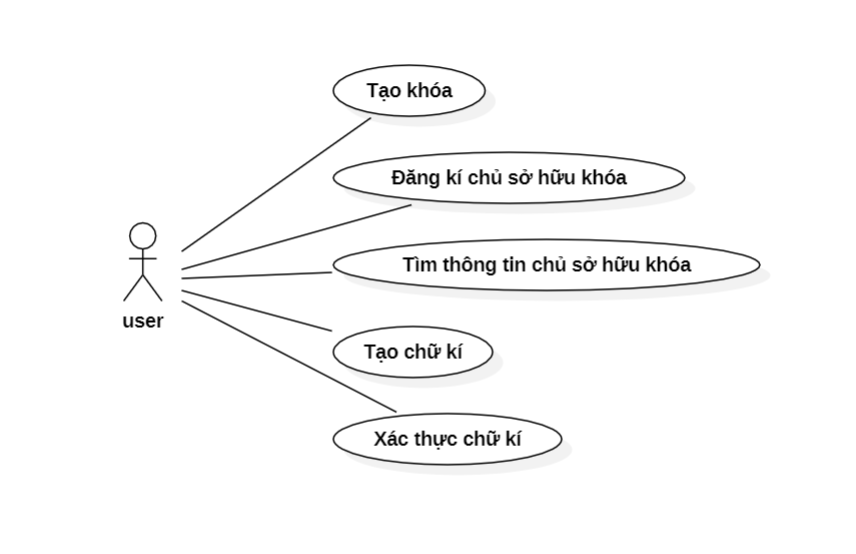
3.1. Tìm hiểu yêu cầu bài toán

* Xây dựng website về chữ ký số cho các hợp đồng kinh tế
* Chức năng:
* Tạo khóa:
* Đăng ký chủ sở hữu khóa:
* Tìm thông tin chủ sở hữu khóa
* Tạo chữ ký.
* Xác thực chữ ký.

3.2. Xây dựng bài toàn

3.2.1 Phân tích yêu cầu người dùng

#### 3.2.1.1 Biểu đồ use case



Hình ảnh 3-1: Biểu đồ use case

#### 3.2.1.2 Mô tả tóm tắt các usecase

* Tạo khóa: cho phép người dùng tạo 1 cặp khóa public key và private key của hệ mật RSA
* Đăng ký chủ sở hữu: cho phép người dùng đăng ký quyền sở hữu khóa của mình
* Tìm thông tin chủ sở hữu khóa: cho phép người dùng có thể tìm thông tin về chủ sở hữu của 1 public key
* Tạo chữ ký: cho phép người dùng tạo chữ ký cho file bằng private key của mình
* Xác thực chữ ký: cho phép người dùng xác thực chữ ký

3.2.2 Thiết kế hệ thống

#### 3.2.2.1 Kiến trúc hệ thống

Nhóm em quyết định sử dụng kiến trúc MVC (Model View Controller) với ngôn ngữ Java trên nền tảng Spring Boot để xây dựng hệ thống.

Model (Mô hình): Đại diện cho dữ liệu và logic xử lý dữ liệu. Nó quản lý trạng thái của ứng dụng và thực hiện các thao tác liên quan đến dữ liệu. Gồm 3 package:

- entity: Chứa các class đối tượng gồm các thuộc tính và các phương thức get, set.

- Dao: Chứa các class có những phương thức truy xuất đến cơ sở dữ liệu và trả về giá trị là các Object tương ứng.

View(Giao diện): Là phần hiển thị thông tin cho người dùng và tương tác với họ. Nó hiển thị dữ liệu từ Mô hình và chịu trách nhiệm về hiển thị đồ họa, giao diện người dùng và tương tác. Nhóm em sử dụng bootstrap để hiển thị giao diện và thymeleaf để hiển thị dữ liệu lên giao diện.

Controller (Bộ điều khiển): Làm trung gian giữa Mô hình và Giao diện. Nó xử lý các sự kiện và yêu cầu từ người dùng, sau đó cập nhật Mô hình hoặc Giao diện tùy thuộc vào thông tin nhận được. Mọi logic, thuật toán xử lý dữ liệu đều được thực hiện ở đây.

#### A screenshot of a computer Description automatically generated3.2.2.2. Thiết kế cơ sở dữ liệu

Hình ảnh 3-2: Hình ảnh thiết kế cơ sở dữ liệu

3.3 Thực hiện bài toán

3.3.1 Tạo khóa

#### 3.3.1.1 Mô tả chức năng

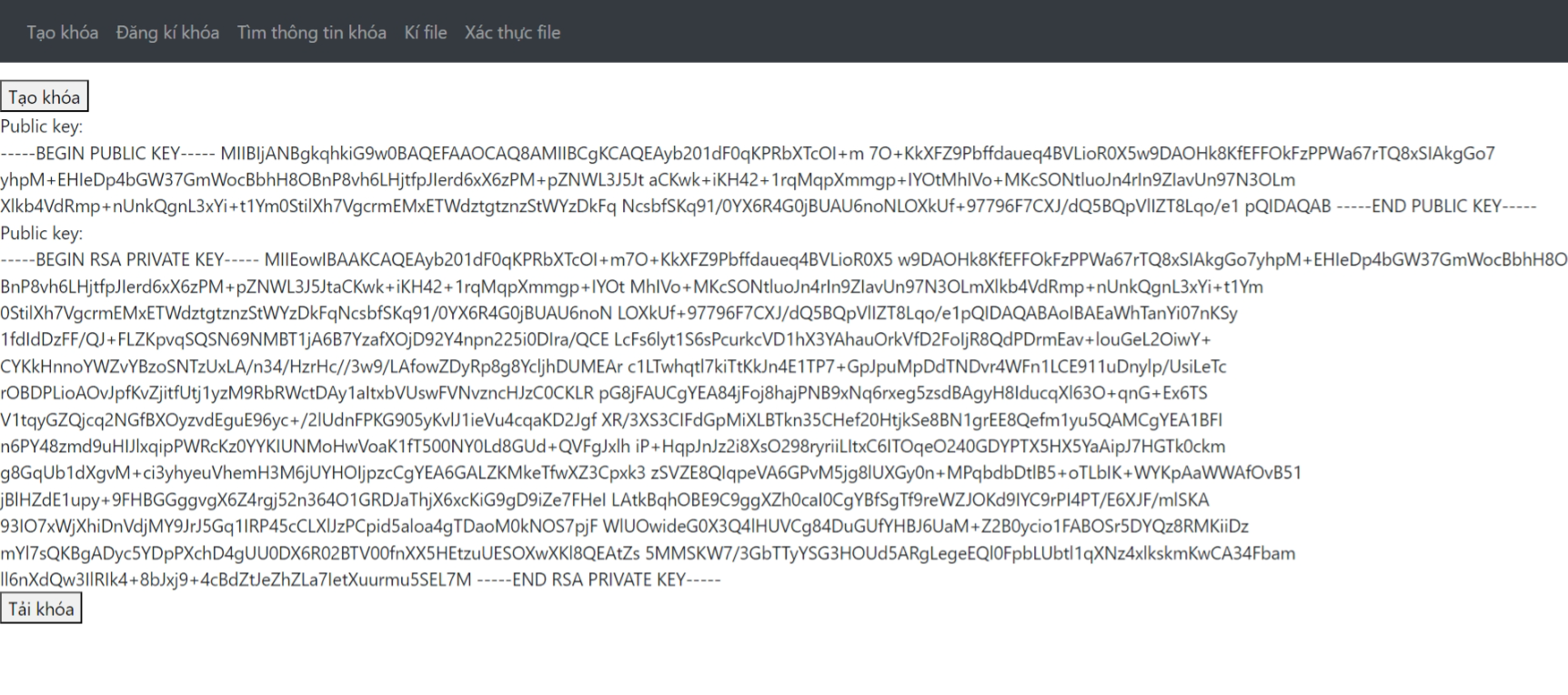
* Cho phép người dùng tạo 1 cặp khóa public key và private key hệ mật RSA
* Người dùng có thể tải key xuống
  + gồm 2 file là: public\_key.txt và private\_key.txt

#### 3.3.1.2 Thiết kế giao diện thực tế

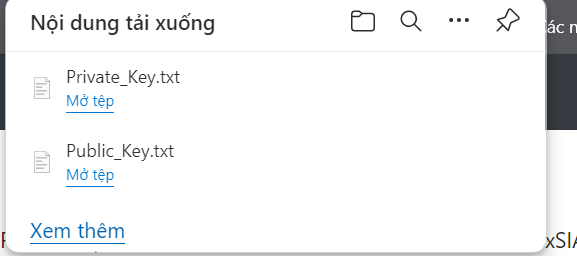
A black and white rectangular object

Description automatically generated

Hình ảnh 3-3: Chức năng tạo khóa



Hình ảnh 3-4: Sau khi bấm nút “Tạo khóa”



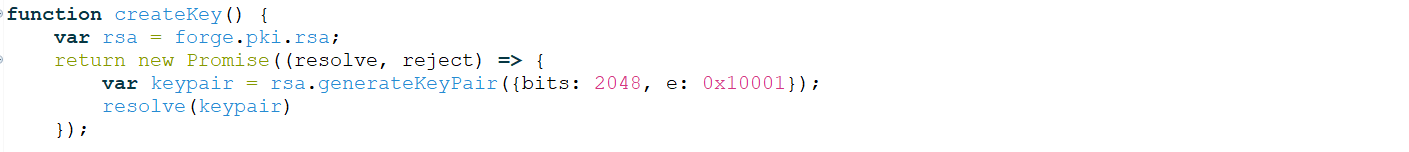
Hình ảnh 3-5: 2 file được tải xuống sau khi bấm tải khóa

#### 3.3.1.3 Logic xử lý

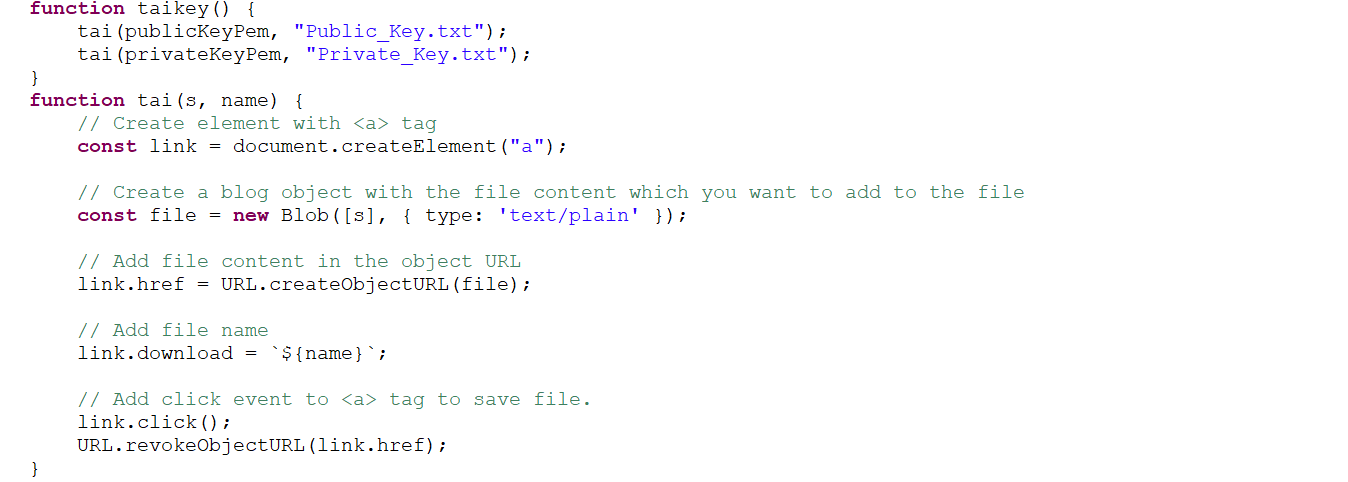
* người dùng truy cập vào đến /generate-key



Hình ảnh 3-6: Controller xử lý yêu cầu GET “/generate-key”



Hình ảnh 3-7: Phần code tạo khóa



Hình ảnh 3-8: Phần code cho chức năng tải khóa

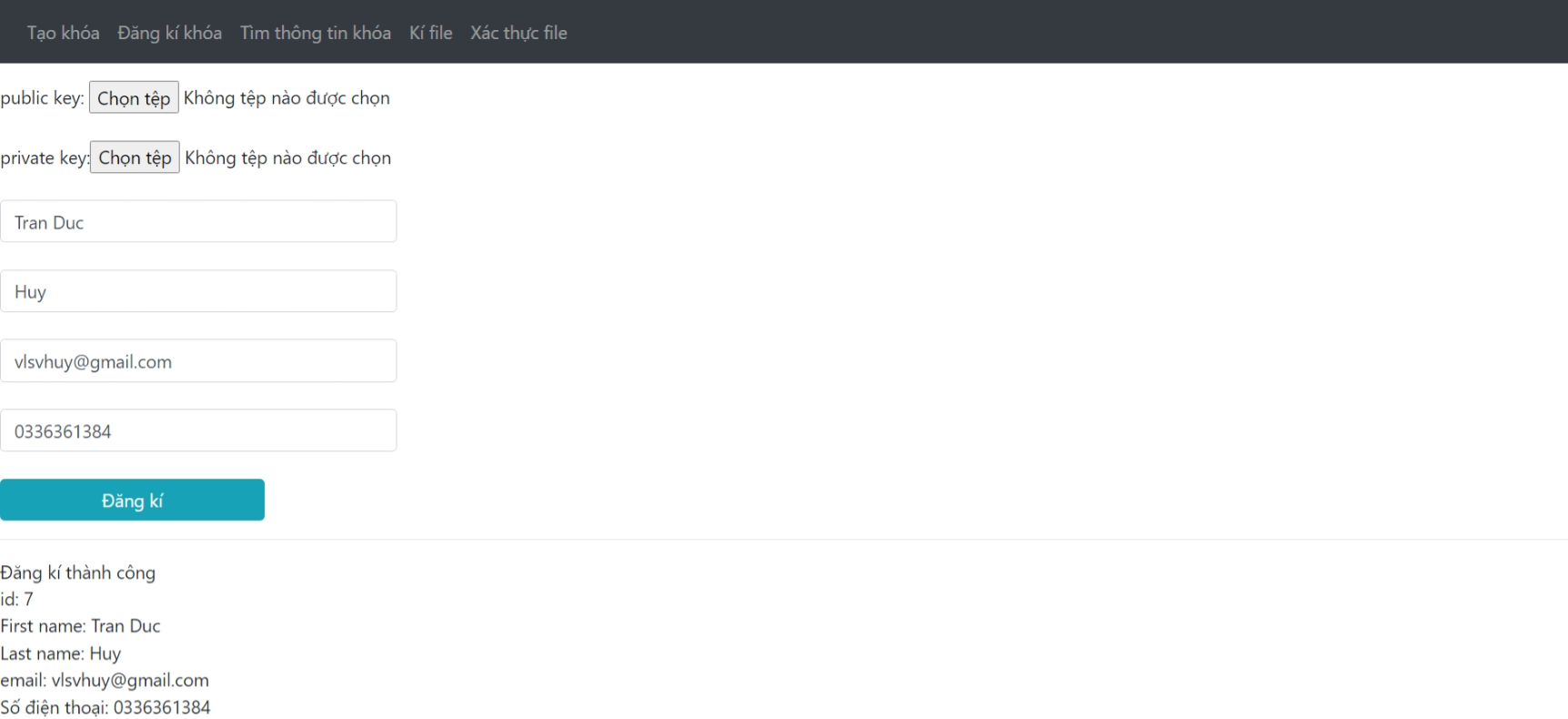
3.3.2 Đăng ký khóa

#### 3.3.2.1 Mô tả chức năng

* Chức năng cho phép người dùng đăng ký quyền sở hữu khóa.
* Người dùng tải 2 file private key và public key, điền thông tin cá nhân và bấm nút “Đăng ký”.

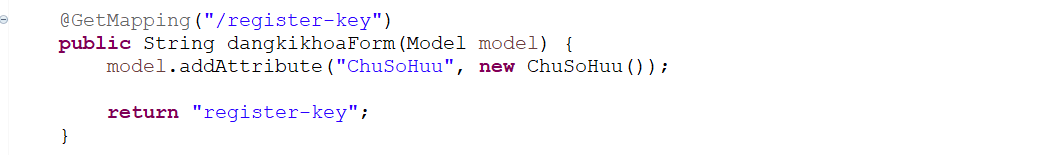
#### A screenshot of a computer Description automatically generated3.3.2.2 Thiết kế giao diện thực tế

Hình ảnh 3-9: Chức năng đăng kí khóa chủ sở hữu khóa

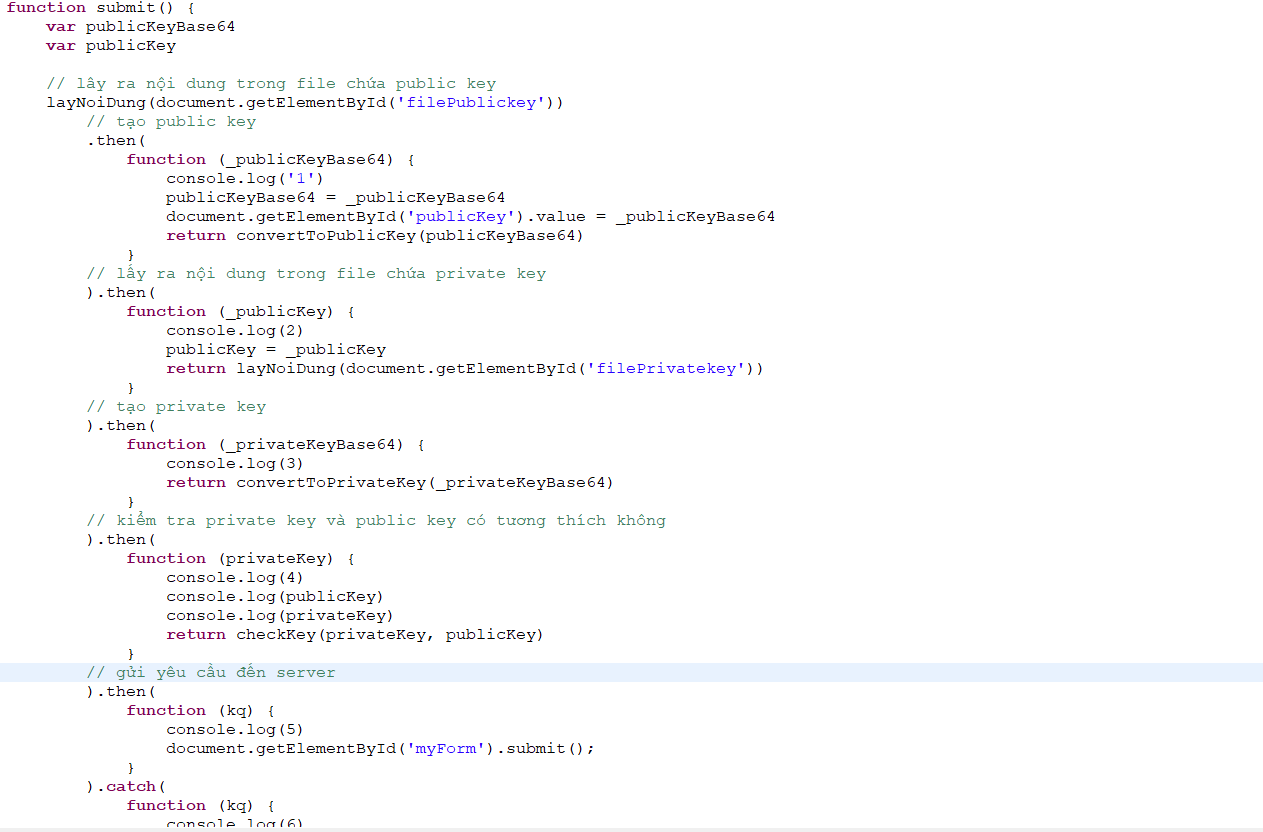


Hình ảnh 3-10: Sau khi đăng kí khóa thành công

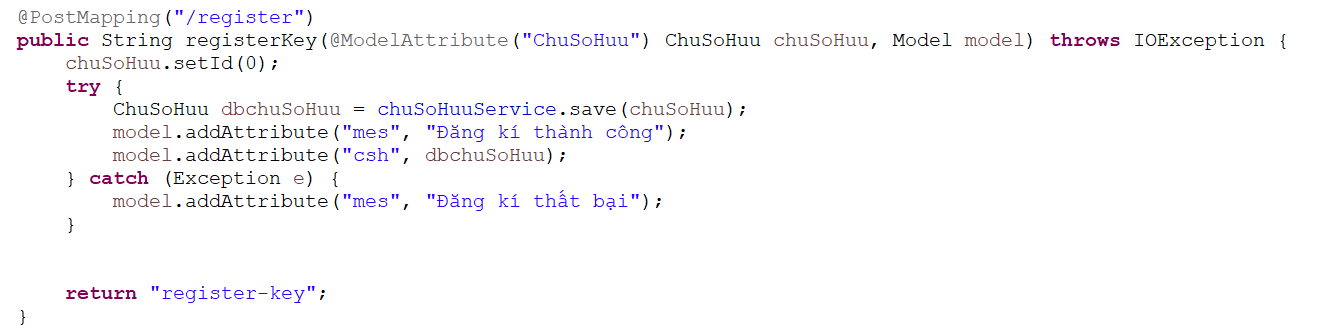
#### 3.3.2.3 Logic xử lý

****

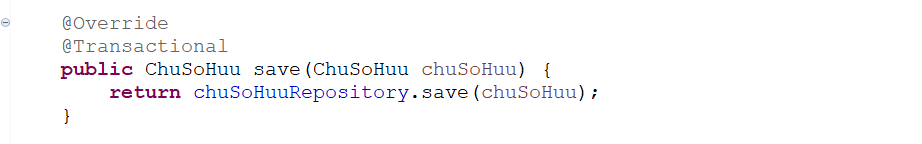
Hình ảnh 3-11: Controller cho yêu cầu GET “/register-key”



Hình ảnh 3-12: Xử lý gửi yêu cầu đăng ký key



Hình ảnh 3-13: Controller xử lý yêu cầu POST “/register”



Hình ảnh 3-14: Service xử lý lưu thông tin khóa

3.3.3 Tìm thông tin khóa

#### 3.3.3.1 Mô tả chức năng

* Chức năng cho phép người dùng tìm thông tin về chủ sở hữu của 1 khóa
* Người dùng upload file public key và bấm “upload file”
* Hệ thống sẽ hiển thị ra thông tin chủ sở hữu nếu có dữ liệu

3.3.3.2 Thiết kế giao diện thực tế

A screenshot of a computer

Description automatically generated

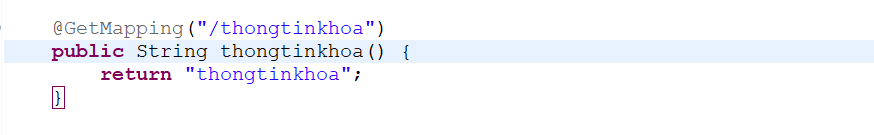
Hình ảnh 3-15: Chức năng tìm thông tin khóa

A screenshot of a computer

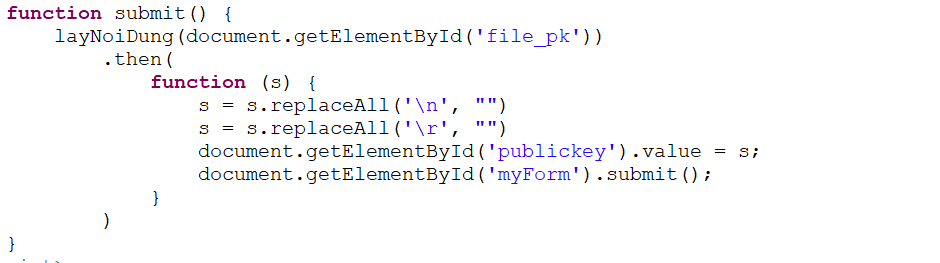
Description automatically generated

Hình ảnh 3-16: Sau khi tìm kiếm thông tin của 1 khóa

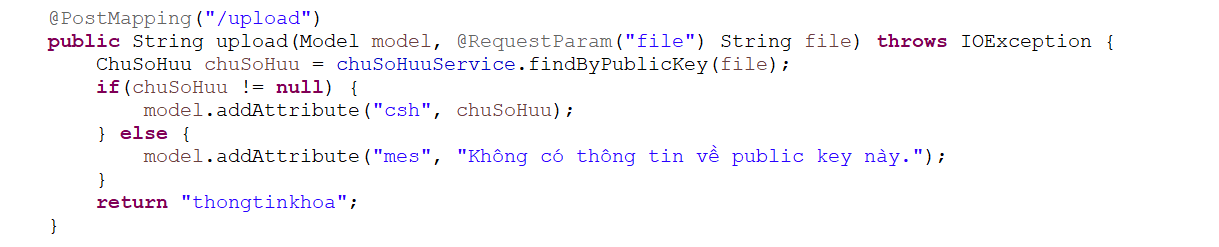
#### 3.3.3.3 Logic xử lý



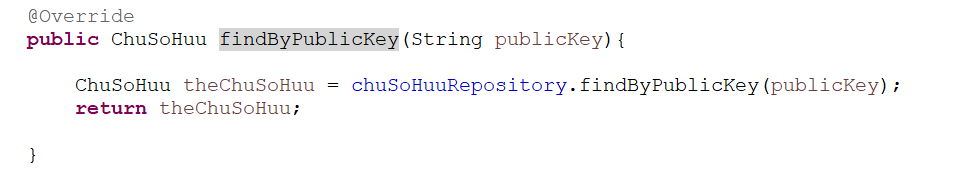
Hình ảnh 3-17: Controller cho yêu cầu GET “/thông tin khóa”



Hình ảnh 3-18: Phần xử lý gửi yêu cầu tìm thông tin khóa



Hình ảnh 3-19: Controller cho yêu cầu POST “/upload”



Hình ảnh 3-20: Service xử lý tìm thông tin của khóa

3.3.4 Tạo chữ ký

#### 3.3.4.1 Mô tả chức năng

* chức năng cho phép người dùng tạo 1 chữ kí bằng private key của mình
* người dùng upload file private key và file cần ký rồi bầng “ký file”
* hệ thống sẽ tạo chữ ký và cho phép người dùng tải chữ ký xuống.

*3.3.4.2 Thiết kế giao diện thực tế*

A screenshot of a computer

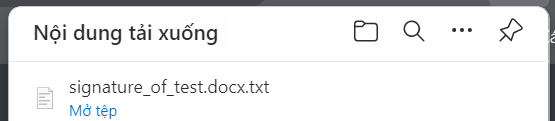
Description automatically generated

Hình ảnh 3-21: Chức năng kí file

A screenshot of a computer

Description automatically generated

Hình ảnh 3-22: Sau khi thực hiện chức năng kí file



Hình ảnh 3-23: File chữ kí được tải xuống

3.3.4.3 Logic xử lý

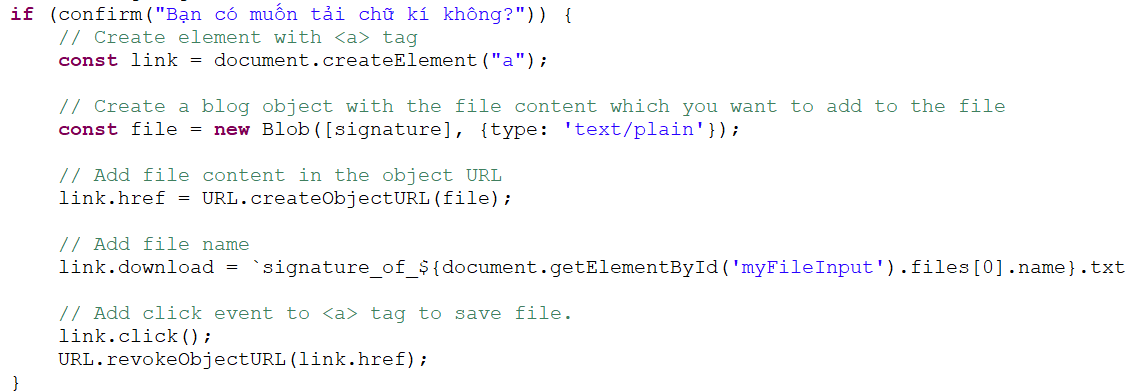
A close-up of a sign-up

Description automatically generated

Hình ảnh 3-24: Controller cho yêu cầu GET “/sign-file”



Hình ảnh 3-25: Phần xử lý tạo chữ kí



Hình ảnh 3-26: Phần xử lý tải chữ kí

3.3.5 Xác thực chữ ký

#### 3.3.5.1 Mô tả chức năng

* Chức năng cho phép người dùng có thể xác thực chữ ký bằng public key
* người dùng upload file cần xác thực, chữ kí, public key và bấm “Xác thực”
* Hệ thống sẽ kiểm tra và thông báo “Chữ kí đúng” hoặc “Chữ ký sai”

#### 3.3.5.2 Thiết kế giao diện thực tế

A screenshot of a computer

Description automatically generated

Hình ảnh 3-27: Chức năng xác thực chữ kí

A screenshot of a computer

Description automatically generated

Hình ảnh 3-28: Sau khi xác thực chữ kí

#### 3.3.5.3 Logic xử lý

Hình ảnh 3-29: Controller xử lý yêu cầu GET “/verify-file”



Hình ảnh 3-30: Phần xử lý xác thực chữ ký

CHƯƠNG 4: KẾT LUẬN VÀ BÀI HỌC KINH NGHIỆM

4.1. Kiến thức kỹ năng đã học được trong quá trình thực hiện đề tài

Sau quá trình nghiên cứu và phân tích đề tài nhóm chúng em đã nhận ra và có được những kiến thức và kĩ năng như sau:

**Về kiến thức:**

+ Hiểu về cơ bản của mã hóa và giải mã trong ngữ cảnh chữ ký số.

+ Nắm vững các thuật toán mã hóa như RSA, DSA, hàm băm, mã hóa bất đối xứng được sử dụng trong tạo chữ ký số

+ Làm quen với việc quản lý khóa công khai và khóa cá nhân

+ Hiểu cách quản lý chứng chỉ số và thực hiện kiểm tra tính hợp lệ của chúng

+ Học được cách áp dụng kiến thức lý thuyết vào thực tế và giải quyết các vấn đề thực tế.

+ Học được cách phân tích, thiết kế và triển khai một hệ thống bảo mật thông tin có tính ứng dụng cao.

**Về kỹ năng:**

+ Nắm vững ngôn ngữ lập trình Java để xây dựng chương trình ứng dụng demo cho chữ ký số

+ Rèn luyện kỹ năng phân tích và thiết kế hệ thống bảo mật.

+ Rèn luyện kỹ năng làm việc nhóm, giao tiếp và trao đổi thông tin.

+ Rèn luyện kỹ năng tự học và tìm kiếm thông tin.

+ Nâng cao kỹ năng viết báo cáo kỹ thuật và trình bày kết quả của dự án.

**Bài học kinh nghiệm:**

Các kỹ năng cần phải có như :

- Kỹ năng làm việc nhóm.

- Kỹ năng tóm tắt, phân tích và giải quyết vấn đề.

- Kỹ năng nghiên cứu, tìm tòi và học hỏi.

**Kiến thức bắt buộc:**

- Các môn toán học và lập trình.

- Cách thức hoạt động của chữ ký RSA, hệ mã hoá RSA.

**Kiến thức chuyên sâu :**

- Có kiến thức nền tảng về máy tính (phần cứng, phần mềm) và hệ thống mạng.

- Hiểu và nắm bắt về luật an toàn thông tin.

- Vận dụng tốt ngôn ngữ lập trình Java

- Hiểu và vận hành quy trình phát triển phần mềm.

- Phân tích lỗ hổng, virus, mã độc, phân tích đánh giá hệ thống.

- Có chuyên môn về mã hóa thông tin, an toàn cơ sở dữ liệu.

- Có ý thức nâng cao hiểu biết, nhận thức bản thân về an toàn thông tin. Tự trau dồi kinh nghiệm ứng phó sự cố bảo mật cũng như vận hành các quy trình bảo mật mới.

# **4.2. Tổng kết nội dung báo cáo**

Bằng những kiến thức cô Lê Thị Anh giảng dạy cùng với sự hiểu biết về ngôn ngữ java, nhóm chúng em đã hoàn thành đề tài” *Xây dựng sản phẩm tạo chữ ký số và giải mã chữ ký số cho các hợp đồng kinh kế*” một cách hoàn thiện nhất.

Nhóm 6 đã tạo ra một trang Web gồm 5 chức năng: tạo khóa, đăng ký khóa, tìm thông tin khóa, tạo chữ ký và xác thực chữ ký.

* **Tạo khóa**: chức năng này đảm bảo rằng mỗi người dùng có 1 tài khoản và 1 public key. Cho phép người tạo ra cặp public key và private key bằng hệ mật RSA, người dùng có thể tải xuống file chứa 2 key này.
* **Đăng ký khóa:** chức năng này cho phép người dùng đăng ký quyền sở hữu khóa, khi người dùng tải file public key và private key, sau đó điền thông tin cá nhân. Ấn nút đăng kí, khi hiển thị đăng kí thành công thì dữ liệu về chủ sở hữu và key được lưu trong CSDL.
* **Tìm thông tin khóa:** khi người dùng tải file public key ấn “upload file” thông tin chủ sở hữu sẽ hiện nếu có trong CSDL.
* **Tạo chữ ký:** chức năng cho phép tạo ra chữ ký bằng private key của chủ sở hữu. Cần upload file private key và file cần ký. Khi ký thành công người dùng cần tài file về để lưu trữ.
* **Xác thực chữ ký:** Cho phép người nhận được văn bản xác thực chữ ký. Hệ thống sẽ kiểm tra và thông báo “Chữ ký đúng” hoặc “Chữ ký sai”.

TÀI LIỆU THAM KHẢO

|  |  |
| --- | --- |
| [1] | T. Mai, "Chữ ký số là gì? Chức năng, ưu và nhược điểm của chữ ký số," 12 8 2020. [Online]. Available: https://wiki.tino.org/chu-ky-so-la-gi/. |
| [2] | Thu, "9 ƯU ĐIỂM CỦA CHỮ KÝ SỐ THÚC ĐẨY CÁ NHÂN, DOANH NGHIỆP LỰA CHỌN SỬ DỤNG," Tổng Công ty Dịch Vụ Viễn Thông. Trung Tâm Kinh Doanh VNPT Hà Nội, 17 11 2022. [Online]. Available: https://vinaphonehanoi.vnpt.vn/tin-tuc-chi-tiet/9-uu-diem-cua-chu-ky-so-thuc-day-ca-nhan-doanh-nghiep-lua-chon-su-dung-840. |
| [3] | Wikipedia®, "Hàm Băm," Wikimedia Foundation, Inc., 24 12 2023. [Online]. Available: https://vi.wikipedia.org/wiki/H%C3%A0m\_b%C4%83m. |
| [4] | Wikipedia®, "Hệ Mã Hóa RSA," Wikimedia Foundation, Inc., 9 24 2023. [Online]. Available: https://vi.wikipedia.org/wiki/RSA\_%28m%C3%A3\_h%C3%B3a%29. |
| [5] | K. C. Nghệ, "Giáo Trình An Toàn Bảo Mật Thông Tin," in *Giáo Trình An Toàn Bảo Mật Thông Tin*, Hà Nội, ĐH GTVT, 2007, p. 152. |