**BỘ TÀI NGUYÊN VÀ MÔI TRƯỜNG**

**TRƯỜNG ĐẠI HỌC TÀI NGUYÊN VÀ MÔI TRƯỜNG**

**KHOA HỆ THỐNG THÔNG TIN VÀ VIỄN THÁM**



**BÁO CÁO ĐỒ ÁN MÔN HỌC: AN TOÀN BẢO MẬT MÁY TÍNH & HỆ THỐNG**

**NGHIÊN CỨU PHƯƠNG PHÁP KÝ SỐ DSS VÀ XÂY DỰNG ỨNG DỤNG KÝ SỐ**

Lớp**: 08\_ĐH\_CNPM**

Giảng viên hướng dẫn : **ThS. Phạm Trọng Huynh**

Sinh viên thực hiện**: Nguyễn Thanh Ý MSSV: 0850080056**

**Trần Lê Tiến Hoà MSSV: 0850080019**

**Nguyễn Xuân Diệu MSSV: 0850080010**

***TP. Hồ Chí Minh, tháng 5 năm 2023***

**BỘ TÀI NGUYÊN VÀ MÔI TRƯỜNG**

**TRƯỜNG ĐẠI HỌC TÀI NGUYÊN VÀ MÔI TRƯỜNG**

**KHOA HỆ THỐNG THÔNG TIN VÀ VIỄN THÁM**



**BÁO CÁO ĐỒ ÁN MÔN HỌC: AN TOÀN BẢO MẬT MÁY TÍNH & HỆ THỐNG**

**NGHIÊN CỨU PHƯƠNG PHÁP KÝ SỐ DSS VÀ XÂY DỰNG ỨNG DỤNG KÝ SỐ**

Lớp**: 08\_ĐH\_CNPM**

Giảng viên hướng dẫn : **ThS. Phạm Trọng Huynh**

Sinh viên thực hiện**: Nguyễn Thanh Ý MSSV: 0850080056**

**Trần Lê Tiến Hoà MSSV: 0850080019**

**Nguyễn Xuân Diệu MSSV: 0850080010**

***TP. Hồ Chí Minh, tháng 5 năm 2023***

**MỞ ĐẦU**

Chữ ký số là một công nghệ quan trọng trong thế giới kỹ thuật số hiện nay. Nó giúp đảm bảo tính toàn vẹn và xác thực thông tin trên mạng internet, đặc biệt là trong các giao dịch trực tuyến. Chữ ký số được tạo ra từ việc sử dụng một cặp khóa, bao gồm khóa công khai và khóa riêng tư, để tạo ra một mã số đặc biệt. Khóa công khai được chia sẻ công khai với tất cả mọi người, trong khi khóa riêng tư chỉ được sử dụng bởi chủ sở hữu của nó.

Khi một tài liệu được ký bằng chữ ký số, mã số đó sẽ được gắn vào tài liệu đó và được chứng thực bởi khóa công khai của người ký. Sau đó, khi người nhận tài liệu muốn xác thực tính toàn vẹn và nguồn gốc của tài liệu đó, họ có thể sử dụng khóa công khai của người ký để kiểm tra tính hợp lệ của chữ ký số.

Chữ ký số không chỉ giúp đảm bảo tính toàn vẹn của thông tin mà còn giúp xác thực danh tính của người ký. Điều này rất quan trọng trong các giao dịch trực tuyến, nơi mà việc xác thực danh tính của người tham gia giao dịch là rất cần thiết. Ngoài ra, chữ ký số còn được sử dụng trong các lĩnh vực như chứng nhận số, bảo vệ dữ liệu và truyền tải thông tin an toàn.

Trong đồ án này, chúng ta sẽ tìm hiểu về chữ ký số, cách thức hoạt động của nó, cũng như các ứng dụng thực tế của công nghệ này trong đời sống và kinh doanh. Chúng ta cũng sẽ xem xét các thách thức và vấn đề liên quan đến việc triển khai chữ ký số, cùng với các giải pháp để giải quyết những thách thức đó. Với sự phát triển không ngừng của công nghệ thông tin, việc hiểu rõ về chữ ký số và các ứng dụng của nó sẽ rất quan trọng để đảm bảo tính an toàn và tin cậy trong thế giới kỹ thuật số ngày nay.

**LỜI CẢM ƠN**

Để hoàn thành tiểu luận này, em xin gửi lời cảm ơn chân thành đến:

Ban giám hiệu Trường đại học Tài nguyên và Môi trường TP.HCM vì đã tạo điều kiện về cơ sở vật chất với hệ thống thư viện hiện đại, đa dạng các loại sách, tài liệu thuận lợi cho việc tìm kiếm, nghiên cứu thông tin.

Xin cảm ơn giảng viên bộ môn - thầy Phạm Trọng Huynh đã giảng dạy tận tình, chi tiết để em có đủ kiến thức và vận dụng chúng vào bài tiểu luận này.

Do chưa có nhiều kinh nghiệm làm để tài cũng như những hạn chế về kiến thức, trong bài tiểu luận chắc chắn sẽ không tránh khỏi những thiếu sót. Rất mong nhận được sự nhận xét, ý kiến đóng góp, phê bình từ phía thầy để bài tiểu luận được hoàn thiện hơn.

Lời cuối cùng, em xin kính chúc thầy Phạm Trọng Huynh nhiều sức khỏe, thành công và hạnh phúc.

**NHẬN XÉT**

**………………………………………………………………………………………**

**………………………………………………………………………………………**

**………………………………………………………………………………………**

**………………………………………………………………………………………**

**………………………………………………………………………………………**

**………………………………………………………………………………………**

**………………………………………………………………………………………**

**………………………………………………………………………………………**

**………………………………………………………………………………………**

**………………………………………………………………………………………**

**………………………………………………………………………………………**

**………………………………………………………………………………………**

**………………………………………………………………………………………**

**………………………………………………………………………………………**

**………………………………………………………………………………………**

**Điểm**

**PHIẾU THEO DÕI TIẾN ĐỘ**

**THỰC HIỆN BÁO CÁO ĐỒ ÁN NHÓM**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Họ và tên** | **MSSV:** | **Lớp:** | **Mức độ đóng góp (%)** | **Ghi chú** |
| Nguyễn Thanh Ý | 0850080056 | 08\_ĐH\_CNPM | 35% | * Nghiên cứu tài liệu về ký số DSS * Tìm hiểu thuật toán ký số với ngôn ngữ Python * Xây dựng thuật toán ứng dụng ký số DSS * Xây dựng giao diện ứng dụng ký số DSS |
| Trần Lê Tiến Hòa | 0850080019 | 08\_ĐH\_CNPM | 30% | * Nghiên cứu tài liệu về ký số DSS * Tìm hiểu thuật toán ký số DSS với ngôn ngữ C# * Xây dựng các mô hình, luồng hoạt động của ký số DSS |
| Nguyễn Xuân Diệu | 0850080010 | 08\_ĐH\_CNPM | 35% | * Tìm hiểu thuật toán ký số DSS với ngôn ngữ Java * Xây dựng các thao tác trong ứng dụng DSS |

**MỤC LỤC**

[**I. GIỚI THIỆU ĐỒ ÁN 1**](#_Toc134599087)

[**1.1. Định nghĩa vấn đề 1**](#_Toc134599088)

[**1.2. Phạm vi của đồ án 1**](#_Toc134599089)

[**1.3. Mục tiêu, sự cần thiết của đề tài, tại sao lại chọn đề tài này? 2**](#_Toc134599090)

[**II. PHÂN TÍCH ĐỀ TÀI 4**](#_Toc134599091)

[**2.1. Tìm hiểu các phương pháp ký số 4**](#_Toc134599092)

[**2.2. Tìm hiểu phương pháp ký số DSS 5**](#_Toc134599093)

[**2.2.1. Ký số DSS là gì? 5**](#_Toc134599094)

[**2.2.2. Nguồn gốc ký số DSS 6**](#_Toc134599095)

[**2.2.3. Quá trình phát triển chuẩn DSS 6**](#_Toc134599096)

[**2.2.4. Tiêu chuẩn ký số DSS 6**](#_Toc134599097)

[**2.2.5. Nguyên tắc hoạt động phương pháp ký số DSS 7**](#_Toc134599098)

[**2.2.6. Ứng dụng ký số DSS 8**](#_Toc134599099)

[**2.3. Độ an toàn của chữ ký số DSS 8**](#_Toc134599100)

[**2.3.1. SHA-2 9**](#_Toc134599101)

[**2.3.2. SHA-3 10**](#_Toc134599102)

[**2.4. Các ứng dụng của chữ ký số DSS 11**](#_Toc134599103)

[**2.5. Hiện thực sản phẩm với chữ ký số DSS 11**](#_Toc134599104)

[**2.5.1. Tạo khoá chữ ký số 11**](#_Toc134599105)

[**2.5.2. Ký số lên file 12**](#_Toc134599106)

[**2.5.3. Gửi file ký số. 12**](#_Toc134599107)

[**2.5.4. Xác thực chữ ký của người gửi 12**](#_Toc134599108)

[**III. THIẾT KẾ & HIỆN THỰC 14**](#_Toc134599109)

[**3.1. Thiết kế mô hình thực hiện 14**](#_Toc134599110)

[**3.2. Sản phẩm với chữ ký số DSS 17**](#_Toc134599111)

[**3.2.1. Tạo khoá chữ ký số 17**](#_Toc134599112)

[**3.2.2. Ký số lên file 18**](#_Toc134599113)

[**3.2.3. Gửi file ký số 19**](#_Toc134599114)

[**3.2.4. Xác thực chữ ký của người gửi 19**](#_Toc134599115)

[**3.3. Một số giao diện của hệ thống 20**](#_Toc134599116)

[**IV. KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN 24**](#_Toc134599117)

[**4.1. Kết quả đạt được 24**](#_Toc134599118)

[**4.2. Đánh giá kết quả đạt được 24**](#_Toc134599119)

[**4.2.1. Ưu điểm 24**](#_Toc134599120)

[**4.2.2. Nhược điểm 25**](#_Toc134599121)

[**4.3. Hướng phát triển 26**](#_Toc134599122)

**DANH MỤC HÌNH**

[Hình 3. 1: Tạo và xác thực chữ ký 14](#_Toc134598400)

[Hình 3. 2: Sử dụng chữ ký số 14](#_Toc134598401)

[Hình 3. 3: Code tạo khoá chữ ký số 17](#_Toc134598402)

[Hình 3. 4: Code ký số lên file 17](#_Toc134598403)

[Hình 3. 5: Code xác thực chữ ký người gửi 18](#_Toc134598404)

[Hình 3. 6: Giao diện khởi tạo và xác thực chữ ký số 18](#_Toc134598405)

[Hình 3. 7: Kết quả sau khi khởi tạo chữ ký số 19](#_Toc134598406)

[Hình 3. 8: Kiểm tra file hợp lệ trước khi thực hiện 19](#_Toc134598407)

[Hình 3. 9: Tạo file ký số 20](#_Toc134598408)

[Hình 3. 10: Xác thực ký số thành công 20](#_Toc134598409)

[Hình 3. 11: Xác thực ký số thất bại 21](#_Toc134598410)

# GIỚI THIỆU ĐỒ ÁN

## **Định nghĩa vấn đề**

Trong đề tài của chúng ta, vấn đề được định nghĩa là một thách thức hoặc khó khăn trong việc triển khai công nghệ chữ ký số. Vấn đề có thể liên quan đến tính toàn vẹn và bảo mật dữ liệu, xác thực danh tính, hiệu quả và tiện ích trong sử dụng chữ ký số, hay các khó khăn về tính khả thi và chi phí khi triển khai công nghệ này.

Để giải quyết các vấn đề này, có thể cần đưa ra các giải pháp kỹ thuật, quy trình và chính sách phù hợp, hoặc sự thay đổi trong cách thức sử dụng chữ ký số. Nghiên cứu và tìm hiểu về các vấn đề liên quan đến chữ ký số sẽ giúp chúng ta hiểu rõ hơn về các thách thức và cơ hội trong việc triển khai công nghệ này, từ đó đưa ra các giải pháp phù hợp để giải quyết các vấn đề và tăng cường tính tin cậy và an toàn của việc sử dụng chữ ký số trong thế giới kỹ thuật số ngày nay.

Ngoài các vấn đề kỹ thuật và bảo mật, đề tài cũng có thể đề cập đến các vấn đề về chính sách và pháp luật liên quan đến chữ ký số. Việc đảm bảo tính hợp pháp và tuân thủ các quy định pháp lý là một trong những yếu tố quan trọng trong việc triển khai chữ ký số. Đồng thời, việc phát triển các chuẩn mực và quy trình đối với chữ ký số cũng là một vấn đề quan trọng trong việc đảm bảo tính tương thích và đồng nhất trong việc sử dụng chữ ký số giữa các tổ chức, cá nhân và các quốc gia.

Vì vậy, nghiên cứu và giải quyết các vấn đề liên quan đến chữ ký số là một yếu tố quan trọng trong việc đảm bảo tính toàn vẹn và an toàn của thông tin kỹ thuật số trong môi trường kinh doanh và xã hội ngày nay.

## **Phạm vi của đồ án**

Mục tiêu của đề tài xoay quanh việc nghiên cứu về chữ ký số và tập trung vào phương pháp ký số DSS, bao gồm các mục tiêu cụ thể sau:

1. Tìm hiểu các phương pháp ký số: Nghiên cứu và phân tích các phương pháp ký số, bao gồm cơ sở lý thuyết và cách thức thực hiện.
2. Tìm hiểu phương pháp ký số DSS: Tập trung nghiên cứu về phương pháp ký số DSS, đánh giá độ hiệu quả và tính khả dụng của nó trong các ứng dụng thực tế.
3. Độ an toàn của chữ ký số DSS: Nghiên cứu và đánh giá tính an toàn của chữ ký số DSS, phân tích các vấn đề về bảo mật và đề xuất các giải pháp để giải quyết các vấn đề đó.
4. Các ứng dụng của chữ ký số DSS: Nghiên cứu và phân tích các ứng dụng của chữ ký số DSS trong thực tiễn, bao gồm cả ứng dụng trong lĩnh vực kinh doanh và xã hội.
5. Hiện thực sản phẩm với chữ ký số DSS: Thực hiện việc hiện thực một sản phẩm sử dụng chữ ký số DSS để đánh giá tính khả dụng và hiệu quả của phương pháp này trong thực tế.

Ngoài ra, trong quá trình thực hiện đồ án, sẽ có các nội dung khác như:

1. Tìm hiểu các công cụ hỗ trợ phát triển chữ ký số: Tìm hiểu và sử dụng các công cụ hỗ trợ phát triển chữ ký số, bao gồm các thư viện mã nguồn mở.
2. Thực hiện thử nghiệm và đánh giá: Thực hiện các thử nghiệm để đánh giá tính chính xác và hiệu quả của chữ ký số DSS, đồng thời đánh giá hiệu quả của sản phẩm sử dụng chữ ký số DSS.
3. Tìm hiểu về quy định pháp luật liên quan đến chữ ký số: Tìm hiểu về các quy định pháp luật liên quan đến chữ ký số, bao gồm cả quy định về chứng thực chữ ký số và quản lý chữ ký số.

Tất cả các nội dung này sẽ giúp đưa ra được một cái nhìn toàn diện về chữ ký số DSS, từ đó đưa ra các giải pháp và đề xuất để nâng cao tính an toàn và hiệu quả trong việc sử dụng chữ ký số DSS trong thực tế.

## **Mục tiêu, sự cần thiết của đề tài, tại sao lại chọn đề tài này?**

Mục tiêu của đề tài là nghiên cứu về chữ ký số, phân tích các vấn đề liên quan đến tính toàn vẹn, bảo mật và xác thực danh tính trong việc sử dụng chữ ký số, đề xuất và phát triển các giải pháp để giải quyết các vấn đề đó và đánh giá hiệu quả của các giải pháp được đề xuất. Đồng thời, đề tài cũng nhằm mục đích nghiên cứu các vấn đề chính sách và pháp luật liên quan đến chữ ký số và đề xuất các giải pháp phù hợp để đảm bảo tính toàn vẹn và an toàn của thông tin kỹ thuật số.

Bên cạnh đó, trong thời đại của cuộc cách mạng công nghiệp 4.0, việc sử dụng thông tin kỹ thuật số ngày càng phổ biến và đóng vai trò quan trọng trong đời sống kinh doanh và xã hội. Tuy nhiên, sự phát triển của các công nghệ thông tin và truyền thông cũng đặt ra nhiều thách thức về tính toàn vẹn, bảo mật và xác thực danh tính của thông tin.

Trong lĩnh vực này, chữ ký số được coi là một trong những giải pháp quan trọng để đảm bảo tính toàn vẹn, bảo mật và xác thực danh tính của thông tin kỹ thuật số. Tuy nhiên, việc triển khai chữ ký số còn gặp nhiều vấn đề liên quan đến tính khả thi, tính tương thích và tính khả dụng trong thực tế. Do đó, nghiên cứu và giải quyết các vấn đề liên quan đến chữ ký số là rất cần thiết và có ý nghĩa quan trọng trong việc đảm bảo tính toàn vẹn và an toàn của thông tin kỹ thuật số trong môi trường kinh doanh và xã hội hiện nay.

Nhóm chúng em chọn đề tài này vì quan tâm đến các vấn đề liên quan đến tính toàn vẹn, bảo mật và xác thực danh tính của thông tin kỹ thuật số, đặc biệt là trong bối cảnh của cuộc cách mạng công nghiệp 4.0. Chữ ký

# PHÂN TÍCH ĐỀ TÀI

## **Tìm hiểu các phương pháp ký số**

* + 1. **Chữ ký số là gì?**

Ký số (Digital Signature) là một phương pháp sử dụng công nghệ mã hóa để đảm bảo tính toàn vẹn, xác thực, và không chối bỏ của thông tin điện tử. Ký số giúp đảm bảo rằng thông tin không bị thay đổi trong quá trình truyền tải và được gửi từ người gửi đến người nhận đúng chính xác.

* + 1. **Phương pháp ký số**

Phương pháp ký số thường sử dụng các thuật toán mật mã học như RSA, DSA, ECDSA, EdDSA,... để tạo ra một chữ ký số (digital signature) được gắn vào thông tin. Chữ ký số này được tạo ra bằng cách sử dụng một khóa riêng tư (private key), chỉ có người gửi thông tin biết và một khóa công khai (public key) được cung cấp cho người nhận thông tin để xác thực chữ ký số.

Khi người nhận thông tin nhận được chữ ký số, họ sẽ sử dụng khóa công khai để xác minh tính toàn vẹn và xác thực của thông tin. Nếu chữ ký số hợp lệ, tức là thông tin không bị thay đổi và được gửi từ người gửi chính xác, thì người nhận sẽ tin tưởng vào tính chính xác và tin cậy của thông tin đó.

Các phương pháp ký số được sử dụng rộng rãi trong các ứng dụng liên quan đến giao dịch điện tử, bảo mật thông tin, chứng thực người dùng, chứng thực tài khoản ngân hàng, thẻ thanh toán, v.v.

Các phương pháp ký số là các phương thức được sử dụng để tạo chữ ký số và đảm bảo tính toàn vẹn của thông tin. Dưới đây là một số phương pháp ký số phổ biến:

* Digital Signature Standard (DSS): Là một thuật toán ký số được sử dụng rộng rãi trong các ứng dụng liên quan đến chữ ký số, bao gồm cả các giao dịch tài chính trực tuyến và các giao dịch điện tử khác. DSS sử dụng các phương thức toán học như RSA và DSA để tạo chữ ký số.
* RSA: Là một phương pháp ký số khóa công khai, dựa trên việc sử dụng một cặp khóa bao gồm khóa riêng và khóa công khai. Khóa riêng được sử dụng để tạo chữ ký số, trong khi khóa công khai được sử dụng để xác minh chữ ký số.
* Elliptic Curve Digital Signature Algorithm (ECDSA): Là một thuật toán ký số dựa trên đường cong elip, được sử dụng để tạo chữ ký số. ECDSA sử dụng các phương thức toán học như RSA và DSA để tạo chữ ký số.
* EdDSA: Là một phương pháp ký số dựa trên đường cong elip, tương tự như ECDSA. Tuy nhiên, EdDSA được coi là nhanh hơn và an toàn hơn ECDSA.
* GPG (GNU Privacy Guard): Là một phần mềm mã nguồn mở được sử dụng để tạo chữ ký số và mã hóa dữ liệu. GPG sử dụng thuật toán RSA hoặc DSA để tạo chữ ký số.
* Hash-based Signatures: Là một phương pháp ký số sử dụng các hàm băm để tạo chữ ký số. Các phương pháp này bao gồm Lamport One-Time Signature Scheme (LOST) và Merkle Signature Scheme (MSS).

Mỗi phương pháp ký số có những ưu điểm và nhược điểm riêng, tùy thuộc vào nhu cầu và yêu cầu cụ thể của ứng dụng. *Ví dụ RSA và DSA là các phương pháp được sử dụng rộng rãi trong các ứng dụng ký số truyền thống, trong khi ECDSA và EdDSA thường được sử dụng trong các ứng dụng di động hoặc Internet of Things (IoT)*. Các phương pháp ký số khác nhau cũng có thể được sử dụng để đảm bảo tính toàn vẹn và xác thực của thông tin tùy thuộc vào nhu cầu của người sử dụng.

## **Tìm hiểu phương pháp ký số DSS**

### **Ký số DSS là gì?**

Phương pháp ký số DSS: (Digital Signature Standard) là một chuẩn ký số được sử dụng rộng rãi trong các ứng dụng liên quan đến bảo mật thông tin và giao dịch điện tử. Chuẩn DSS được phát triển bởi Cơ quan Tiêu chuẩn Quốc gia Hoa Kỳ (National Institute of Standards and Technology - NIST) vào năm 1991.

### **Nguồn gốc ký số DSS**

Digital Signature Standard (DSS) là một chuẩn được phát triển bởi Cục Tiêu chuẩn và Công nghệ Quốc gia (NIST) của Hoa Kỳ vào năm 1994. Chuẩn DSS được thiết kế để xác minh tính toàn vẹn của tài liệu bằng cách sử dụng chữ ký số.

DSS được phát triển để thay thế hệ thống chữ ký số đầu tiên được phát triển bởi Rivest, Shamir và Adleman (RSA) vào những năm 1970. DSS sử dụng thuật toán ký số Digital Signature Algorithm (DSA), là một phương pháp ký số đối xứng dựa trên việc sử dụng khóa bí mật và khóa công khai.

Sau khi DSS được phát triển, nó đã trở thành một chuẩn được chấp nhận rộng rãi trong lĩnh vực bảo mật và được sử dụng trong nhiều ứng dụng, bao gồm xác thực tài liệu điện tử, chuyển tiền điện tử và chữ ký số cho các tài khoản ngân hàng trực tuyến.

### **Quá trình phát triển chuẩn DSS**

Quá trình phát triển ký số DSS bắt đầu từ những năm 1990 khi một số chuyên gia bảo mật đầu tiên nhận ra rằng các hệ thống ký số hiện tại như RSA và DSA không đáp ứng được các yêu cầu bảo mật của tương lai. Một số vấn đề đó bao gồm khả năng phá mã mật mã học, sự gia tăng của các cuộc tấn công mạng và khả năng tấn công vào cấu trúc khóa công khai. Với sự phát triển của kỹ thuật và sự cần thiết về tính bảo mật cao, DSS được phát triển bởi Cơ quan Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ (NIST) dưới sự hướng dẫn của Chính phủ Hoa Kỳ vào giữa những năm 1990. Tiêu chuẩn DSS đã được công bố vào năm 1994. Sau đó, DSS đã được sử dụng rộng rãi trong nhiều ứng dụng bảo mật, bao gồm các chuyển tiền điện tử, thư điện tử, lưu trữ dữ liệu và phân phối phần mềm. Nó cũng đã được tích hợp vào các chuẩn bảo mật khác như SSL/TLS, S/MIME và IPsec.

Tuy nhiên, vào năm 2013, DSS đã bị đánh giá là không còn đủ bảo mật do các phát hiện liên quan đến khả năng tấn công bằng thuật toán bí mật. NIST đã rút lại DSS và phát triển các chuẩn bảo mật mới như SHA-3 và các thuật toán ký số Elliptic Curve.

### **Tiêu chuẩn ký số DSS**

Được thiết kế để sử dụng trong các ứng dụng chuyển tiền điện tử, phân phối phần mềm, thư điện tử, lưu trữ dữ liệu và các ứng dụng yêu cầu tính toàn vẹn dữ liệu cao. DSS có thể triển khai trên phần mềm, phần cứng hoặc phần sụn. Thuật toán chữ ký số được sử dụng trong DSS sử dụng hai số lớn được tính toán dựa trên một thuật toán duy nhất và xác định tính xác thực của chữ ký. Chữ ký số chỉ có thể được tạo bởi người có thẩm quyền sử dụng khóa riêng của họ và người dùng hoặc công chúng có thể xác minh chữ ký với sự trợ giúp của các khóa công khai được cung cấp cho họ. Một điểm khác biệt chính giữa mã hóa và hoạt động chữ ký trong DSS là mã hóa có thể đảo ngược, trong khi hoạt động chữ ký số thì không. Nó cũng không cung cấp khả năng liên quan đến phân phối khóa hoặc trao đổi khóa. Tiêu chuẩn Chữ ký số đảm bảo tính toàn vẹn của dữ liệu và các tài liệu điện tử được bảo mật. Nó cũng đảm bảo không thoái thác liên quan đến chữ ký và cung cấp tất cả các biện pháp bảo vệ để ngăn chặn mạo danh.

### **Nguyên tắc hoạt động phương pháp ký số DSS**

Nguyên tắc hoạt động của phương pháp ký số DSS: Được dựa trên thuật toán Digital Signature Algorithm (DSA), một thuật toán mã hóa đối xứng sử dụng hàm băm (hash function) để tạo ra một chữ ký số. Thuật toán DSA sử dụng một khóa riêng tư để tạo ra chữ ký số và một khóa công khai để xác minh tính toàn vẹn của chữ ký số. Quá trình tạo chữ ký số DSS bao gồm ba bước chính sau:

Bước 1: Tạo ra giá trị băm (hash value) của thông tin cần ký

*Trước khi tạo chữ ký số, thông tin cần ký sẽ được đưa qua hàm băm (hash function) để tạo ra một giá trị băm duy nhất đại diện cho thông tin đó. Giá trị băm này thường có kích thước cố định và không thể khôi phục lại được thông tin gốc ban đầu.*

Bước 2: Tạo chữ ký số sử dụng khóa riêng tư

*Sau khi có giá trị băm của thông tin cần ký, người ký sử dụng khóa riêng tư của mình để tạo ra chữ ký số. Quá trình này bao gồm việc tạo ra một số ngẫu nhiên và tính toán dựa trên giá trị băm và khóa riêng tư. Kết quả của quá trình này là một chữ ký số duy nhất liên kết với thông tin cần ký và được tạo ra bằng khóa riêng tư của người ký.*

Bước 3: Xác minh tính toàn vẹn của chữ ký số sử dụng khóa công khai

*Sau khi có chữ ký số, người nhận sẽ sử dụng khóa công khai của người ký để xác minh tính toàn vẹn của chữ ký số. Quá trình này bao gồm việc sử dụng giá trị băm của thông tin cần ký và chữ ký số để tính toán một giá trị số mới. Nếu giá trị số mới này giống với giá trị số được tính toán bởi người ký trước đó, chữ ký số được xác minh là hợp lệ và thông tin cần ký được xác nhận là không bị sửa đổi.*

Bước 4: Gửi chữ ký số: Gửi thông điệp đã được ký và chữ ký số đến người nhận.

Bước 5: Xác minh chữ ký số

*Người nhận sử dụng khóa công khai tương ứng để xác minh chữ ký số. Họ sẽ băm thông điệp và so sánh giá trị băm này với giá trị băm được ký bởi người ký. Nếu giá trị băm khớp với giá trị băm được ký, chữ ký số được coi là hợp lệ.*

Tổng quan về quá trình hoạt động của phương pháp ký số DSS là sử dụng khóa riêng tư để tạo ra chữ ký số liên kết với thông tin cần ký và sau đó sử dụng khóa công khai để xác minh tính toàn vẹn của chữ ký số này. Quá trình này đảm bảo tính bảo mật và xác thực của thông tin ký.

### **Ứng dụng ký số DSS**

Đến từ khả năng của nó trong việc tạo ra chữ ký số có tính toàn vẹn cao và khả năng xác minh nhanh chóng. Chữ ký số được tạo ra bởi DSS là một mã số ngẫu nhiên được tính toán dựa trên thông tin cần ký và khóa riêng tư của người ký. Sau khi tạo ra chữ ký số, người nhận có thể sử dụng khóa công khai của người ký để xác minh tính toàn vẹn của chữ ký số đó. Quá trình xác minh này rất nhanh chóng và không yêu cầu phải tiết lộ khóa riêng tư của người ký.

Phương pháp ký số DSS có nhiều ưu điểm, bao gồm tính bảo mật cao, độ tin cậy cao, khả năng xác thực nhanh chóng, và khả năng ứng dụng trong nhiều lĩnh vực khác nhau. Chuẩn DSS được sử dụng trong nhiều ứng dụng, bao gồm các hệ thống quản lý chứng khoán, các hệ thống thanh toán điện tử, các ứng dụng liên quan đến chứng thực người dùng và chứng thực tài khoản ngân hàng. Tuy nhiên, DSS cũng có một số hạn chế, bao gồm sự phụ thuộc vào hàm băm để tạo ra chữ ký số và việc yêu cầu sử dụng khóa riêng tư để tạo ra chữ ký số. Do đó, các ứng dụng sử dụng DSS cần phải đảm bảo tính bảo mật của khóa riêng tư và sử dụng các hàm băm đủ mạnh để tránh bị tấn công từ các kẻ tấn công.

## **Độ an toàn của chữ ký số DSS**

Chữ ký số DSS được coi là một trong những chuẩn chữ ký số an toàn và đáng tin cậy. Tuy nhiên, độ an toàn của nó phụ thuộc vào việc sử dụng các thủ tục và thuật toán được áp dụng để tạo và xác thực chữ ký số.

Hiện nay, chuẩn chữ ký số DSS sử dụng các thuật toán mã hóa khóa công khai được coi là an toàn như SHA-2 hoặc SHA-3 để tạo chữ ký số. Các khóa được sử dụng trong quá trình tạo chữ ký số cũng được đảm bảo là không thể bị đoán trước và khó khăn để phá vỡ. Tuy nhiên, cũng có những ưu điểm và hạn chế của chuẩn chữ ký số DSS, ví dụ như kích thước khóa bí mật và công khai phải đủ lớn để đảm bảo tính an toàn của nó, việc tạo chữ ký số có thể tốn nhiều thời gian và tài nguyên máy tính, và nó không thể đảm bảo tính riêng tư của dữ liệu. Tóm lại, việc đảm bảo tính an toàn của chữ ký số DSS phụ thuộc vào việc sử dụng các thuật toán và thủ tục phù hợp để tạo và xác thực chữ ký số, cũng như sự cập nhật và tuân thủ các tiêu chuẩn và quy định liên quan đến chữ ký số.

SHA-2 (Secure Hash Algorithm 2) và SHA-3 (Secure Hash Algorithm 3) là hai trong số các thuật toán mã hóa khóa công khai được sử dụng để tạo chữ ký số. Cả hai đều được phát triển bởi Cơ quan Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ (NIST), và được sử dụng rộng rãi trong các ứng dụng an ninh mạng và bảo mật thông tin.

Các thuật toán mã hóa khóa công khai như SHA-2 và SHA-3 sử dụng một hàm băm (hash function) để biến đổi dữ liệu đầu vào thành một chuỗi nhị phân cố định độ dài, gọi là giá trị băm (hash value). Hàm băm có tính chất không thể đoán trước, nghĩa là nó không thể dự đoán được giá trị băm của một dữ liệu mới nếu không biết dữ liệu đầu vào ban đầu.

Khi tạo chữ ký số, người ký sẽ sử dụng hàm băm SHA-2 hoặc SHA-3 để tạo giá trị băm của tài liệu cần ký. Sau đó, người ký sử dụng khóa bí mật của mình để mã hóa giá trị băm đó, tạo ra chữ ký số. Chữ ký số này được gửi cùng với tài liệu gốc, và người nhận sẽ sử dụng khóa công khai của người ký để giải mã chữ ký số và xác thực tính toàn vẹn của tài liệu. Các thuật toán mã hóa khóa công khai như SHA-2 và SHA-3 được đánh giá là an toàn và đáng tin cậy trong việc tạo chữ ký số, bởi vì tính chất không thể đoán trước của hàm băm đảm bảo rằng người tấn công không thể thay đổi tài liệu mà không phá vỡ tính toàn vẹn của chữ ký số. Ngoài ra, các thuật toán này cũng được sử dụng trong việc mã hóa dữ liệu nhạy cảm để đảm bảo tính bảo mật của thông tin.

### **SHA-2**

SHA-2 là một họ hàm băm được sử dụng rộng rãi trong các ứng dụng mã hóa và bảo mật thông tin. SHA-2 là viết tắt của "Secure Hash Algorithm 2" và được phát triển bởi Cục An ninh Quốc gia Hoa Kỳ (National Security Agency - NSA) vào năm 2001, nhằm thay thế cho SHA-1 đã bị xác định có nhiều lỗ hổng bảo mật.

SHA-2 bao gồm một số hàm băm với độ dài khác nhau, bao gồm SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 và SHA-512/256. Các hàm băm này được thiết kế để đảm bảo tính toàn vẹn và bảo mật của dữ liệu thông qua việc tạo ra một giá trị băm duy nhất cho dữ liệu đầu vào.

Các hàm băm SHA-2 có thể sử dụng để thực hiện các chức năng bảo mật như chứng thực dữ liệu, xác minh nguồn gốc dữ liệu và mã hóa thông tin. Các hàm băm SHA-2 được sử dụng trong các ứng dụng bảo mật như TLS/SSL, SSH, S/MIME, IPsec và các giao thức bảo mật khác.

Tuy nhiên, cũng cần lưu ý rằng các hàm băm SHA-2 không phải là giải pháp hoàn hảo và vẫn có thể bị tấn công bởi các kỹ thuật tấn công hiện đại. Do đó, các chuyên gia bảo mật khuyến khích việc sử dụng các hàm băm có độ dài khóa lớn hơn như SHA-3 hoặc BLAKE để tăng cường tính an toàn và bảo mật cho hệ thống bảo mật của mình.

### **SHA-3**

SHA-3 là một tiêu chuẩn băm mã hóa an toàn mới nhất do Viện Công nghệ Massachusetts (Massachusetts Institute of Technology - MIT) phát triển. Nó được phát triển nhằm nâng cao độ an toàn và tính bảo mật của các tiêu chuẩn băm trước đó như SHA-1 và SHA-2. SHA-3 được chấp nhận bởi Tổ chức Tiêu chuẩn Hóa Quốc tế (International Organization for Standardization - ISO) và Cục An ninh Quốc gia Hoa Kỳ (National Security Agency - NSA).

SHA-3 sử dụng thuật toán băm Keccak, được lựa chọn thông qua một cuộc thi toàn cầu được tổ chức bởi NIST. Cuộc thi này là một phần của quá trình tìm kiếm một hàm băm mới và an toàn hơn cho tiêu chuẩn băm mã hóa của Mỹ. Keccak được thiết kế để chống lại các cuộc tấn công như tấn công bằng cách tìm kiếm, tấn công bằng lực brute force và tấn công bằng cách sử dụng các kỹ thuật đường giả.

SHA-3 cho phép tạo ra các giá trị băm với độ dài khác nhau, tối đa là 512 bit, và có độ an toàn cao. Nó được sử dụng trong nhiều ứng dụng bảo mật như TLS/SSL, SSH, S/MIME, IPsec và các giao thức bảo mật khác. Tuy nhiên, vì SHA-3 là một tiêu chuẩn mới, nó có thể không được hỗ trợ bởi tất cả các ứng dụng bảo mật, vì vậy người dùng cần phải kiểm tra trước khi sử dụng.

Với tính linh hoạt và tính bảo mật cao, SHA-3 được xem là một tiêu chuẩn băm mã hóa an toàn và được sử dụng rộng rãi trong các ứng dụng bảo mật hiện đại.

## **Các ứng dụng của chữ ký số DSS**

Chữ ký số DSS (Digital Signature Standard) được sử dụng rộng rãi trong các lĩnh vực liên quan đến bảo mật thông tin và giao dịch điện tử, bao gồm:

* Giao dịch tài chính: Chữ ký số DSS được sử dụng để xác thực các giao dịch tài chính trực tuyến, bao gồm các giao dịch chuyển tiền và giao dịch chứng khoán.
* Đăng ký trang web và thương hiệu: Chữ ký số DSS được sử dụng để xác thực các chứng chỉ SSL/TLS cho các trang web, giúp đảm bảo tính bảo mật và xác thực cho người dùng khi truy cập các trang web đó.
* Bảo vệ thông tin cá nhân: Chữ ký số DSS được sử dụng để bảo vệ thông tin cá nhân của người dùng trên Internet, bao gồm việc đăng ký và xác thực tài khoản trực tuyến, chữ ký số cũng được sử dụng để ký và mã hóa email.
* Chứng thực phần mềm: Chữ ký số DSS được sử dụng để đảm bảo tính xác thực và an toàn cho các phần mềm và ứng dụng, đặc biệt là các ứng dụng liên quan đến bảo mật và quản lý hệ thống.

Bảo vệ quyền sở hữu trí tuệ: Chữ ký số DSS được sử dụng để xác thực và bảo vệ quyền sở hữu trí tuệ, bao gồm việc ký và mã hóa các tài liệu bản quyền và tài liệu thương mại.

Tóm lại, chữ ký số DSS có rất nhiều ứng dụng khác nhau trong nhiều lĩnh vực, đóng vai trò quan trọng trong việc bảo vệ thông tin và đảm bảo tính toàn vẹn của các giao dịch điện tử.

## **Hiện thực sản phẩm với chữ ký số DSS**

* + 1. **Tạo khoá chữ ký số**

Để tạo chữ ký số, ta cần sử dụng một thuật toán mã hóa để biến đổi dữ liệu thành một giá trị số học có độ dài cố định và duy nhất. Sau đó, ta sử dụng khóa riêng tư của mình để ký vào giá trị này và tạo ra chữ ký số.

Các bước để tạo chữ ký số:

1. Chọn một thuật toán mã hóa, ví dụ như SHA-256.
2. Chuẩn bị dữ liệu cần ký, ví dụ như một tập tin văn bản.
3. Áp dụng thuật toán mã hóa lên dữ liệu, tạo ra một giá trị số học duy nhất.
4. Sử dụng khóa riêng tư của người ký để ký vào giá trị số học này.
5. Kết quả chính là chữ ký số, được lưu trữ dưới dạng một tệp tin đính kèm với dữ liệu gốc.

Tùy thuộc vào thuật toán và phương pháp ký khác nhau, các bước có thể có thêm hoặc bớt đi một vài thao tác. Tuy nhiên, quá trình tạo chữ ký số luôn bao gồm các bước chính như trên.

* + 1. **Ký số lên file**

Để ký số lên file, ta cần thực hiện các bước sau:

1. Sau khi tạo một đối tượng ký số DSS từ private key.
2. Đọc dữ liệu từ file cần ký số.
3. Sử dụng đối tượng ký số DSS để ký số dữ liệu.
4. Lưu chữ ký và dữ liệu ký số vào file.
   * 1. **Gửi file ký số.**

Sau khi ký số lên file, file đã được mã hóa và bảo vệ bằng chữ ký số. Người gửi có thể gửi file ký số đến người nhận thông qua các kênh truyền thông khác nhau như email, đường truyền internet, USB, v.v.

Việc gửi file ký số giúp đảm bảo tính toàn vẹn và bảo mật của file khi truyền tải. Bên cạnh đó, người nhận cũng có thể xác thực tính hợp pháp của file bằng cách sử dụng chữ ký số được đính kèm trong file ký số.

* + 1. **Xác thực chữ ký của người gửi**

Sau khi nhận được file ký số từ người gửi, người nhận có thể xác thực tính hợp pháp của file bằng cách xác minh chữ ký số được đính kèm trong file. Quá trình xác thực chữ ký số bao gồm các bước sau:

1. Lấy chữ ký số được đính kèm trong file ký số.
2. Tính toán lại giá trị băm của file gốc bằng cách sử dụng hàm băm được sử dụng để tạo chữ ký số.
3. So sánh giá trị băm được tính toán ở bước 2 với giá trị băm được lưu trữ trong chữ ký số. Nếu hai giá trị băm giống nhau, chữ ký số được xác thực là hợp pháp và file được coi là chính thức.

Việc xác thực chữ ký số giúp đảm bảo tính toàn vẹn, bảo mật và chính xác của file và giúp người nhận có thể đánh giá tính hợp pháp của nội dung trong file.

# THIẾT KẾ & HIỆN THỰC

## **Thiết kế mô hình thực hiện**

A picture containing screenshot, design

Description automatically generated

Hình 3. 1: Tạo và xác thực chữ ký

Graphical user interface

Description automatically generated

Hình 3. 2: Sử dụng chữ ký số

* ***Mã hóa chữ ký***

Chữ ký số (hay chữ ký điện tử) là giải pháp được quốc tế và Việt Nam công nhận về tính pháp lý, có thể giải quyết triệt để các nguy cơ an ninh trong giao dịch trực tuyến đặc biệt là giao dịch ngân hàng điện tử.

Chữ ký số tương đương chữ ký tay, có các thuộc tính định danh, xác thực đúng nguồn gốc, đảm bảo được tính toàn vẹn của dữ liệu nhận được và chống từ chối. Chữ ký số sử dụng một cặp khóa: Khóa bí mật (private key) và khóa công khai (public key).

Khóa bí mật là một khóa trong cặp khóa thuộc hệ thống mã không đối xứng được dùng để tạo chữ ký số. Khóa công khai là một khóa trong cặp khóa thuộc hệ thống mã không đối xứng, được sử dụng để xác thực chữ ký số. Không thể sử dụng khóa công khai để tìm ra khóa bí mật.

Chữ ký số được tạo ra bằng cách áp dụng thuật toán Băm (hash) một chiều trên văn bản cần ký điện tử để tạo ra văn bản phân tích, sau đó sử dụng khóa bí mật để mã hóa tạo ra chữ ký số đính kèm với văn bản gốc để gửi đi. Khi nhận, văn bản được tách ra làm 2 phần, phần văn bản gốc được sử dụng thuật toán Băm tạo ra văn bản phân tích để so sánh với bản Băm từ người gửi được phục hồi từ việc sử dụng khóa công khai để giải mã.

* ***Làm căn cứ pháp lý***

Chữ ký số được xem như một phương tiện hữu hiệu để các ngân hàng tăng cường tính cạnh tranh trong thời đại công nghệ điện tử. Khác với văn bản giấy có chữ ký bằng tay, những văn bản điện tử có thể chuyển theo đường truyền Internet và qua nhiều đơn vị xử lý trong một thời gian rất ngắn.

Như vậy, việc sử dụng chữ ký số và thực hiện những giao dịch điện tử cho phép tiết kiệm thời gian, sức lực và tăng hiệu quả lao động nhưng vẫn đảm bảo tính pháp lý và tính toàn vẹn của dữ liệu cần bảo vệ.

Đối với khách hàng chữ ký số làm giảm khả năng giả mạo chữ ký; ngăn chặn khả năng làm giả tài liệu; cho phép xác định tác giả văn bản và tính nguyên gốc của văn bản.

Đối với ngân hàng: Chữ ký số giúp các ngân hàng giảm thiểu chi phí đầu tư trong triển khai và mở rộng dịch vụ, tăng cường khả năng quản lý rủi ro hiệu quả. Bên cạnh đó, ứng dụng phương thức bảo mật này giúp xây dựng hình ảnh ngân hàng hiện đại, tin cậy và an toàn hơn.

Chia sẻ về tính ứng dụng của chữ ký số trong ngân hàng, ông Phạm Hồng Tuấn - Trưởng Phòng An ninh và Quản lý Rủi ro CNTT VietinBank cho biết: Tại VietinBank chữ ký số đang được dùng lưu chuyển các văn bản điện tử có mẫu cố định như: Các biểu mẫu đăng ký, thay đổi dịch vụ nội bộ; yêu cầu đổi mật khẩu, thay đổi thông tin người dùng và là giải pháp bảo mật quan trọng trong các kênh thanh toán giữa ngân hàng với bên thứ ba...

Hiện nay việc sử dụng chữ ký số cũng còn có những hạn chế nhất định trong giao dịch điện tử bởi: Sự lệ thuộc vào máy tính và chương trình phần mềm; bản gốc, bản chính hay vấn đề có thời hạn của chữ ký số và không hiệu quả nếu người dùng là nạn nhân của lừa đảo.

Như vậy, sự ra đời của chữ ký số là cơ sở khẳng định giá trị pháp lý của văn bản điện tử và cho phép thực hiện những giao dịch điện tử. Tuy nhiên, để chữ ký số thực sự trở nên phổ biến, thông dụng trong các hoạt động ngân hàng đồng thời phát huy những tính năng vượt trội và có thể thay thế tài liệu giấy thì vẫn cần nghiên cứu và khắc phục những hạn chế của chữ ký số; cần có thêm hành lang pháp lý hay những công cụ khác để khẳng định giá trị pháp lý của tài liệu điện tử. Điều này cần sự đầu tư nghiên cứu của các nhà khoa học, các chuyên gia và sự hỗ trợ của các nhà quản lý.

|  |
| --- |
| ***Các nghị định, thông tư liên quan đến chữ ký số:***  *- Điều 14 Nghị định số 27/2007/NĐ-CP của Chính phủ quy định các cơ quan tài chính và tổ chức, cá nhân có tham gia giao dịch điện tử trong hoạt động tài chính với cơ quan tài chính phải sử dụng chữ ký số và chứng thư số do Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng cung cấp.*  *- Điều 5 Nghị định số 35/2007/NĐ-CP của Chính phủ quy định cơ quan, tổ chức, cá nhân sử dụng giao dịch điện tử trong hoạt động ngân hàng phải đáp ứng điều kiện “Có chữ ký điện tử theo quy định của pháp luật”.*  *- Điều 12 Thông tư số 31/2015/TT-NHNN của Ngân hàng Nhà nước quy định: Đối với các giao dịch giá trị cao phải xác thực bằng các phương pháp xác thực mạnh như sinh trắc học hoặc chữ ký số.* |

## **Sản phẩm với chữ ký số DSS**

* + 1. **Tạo khoá chữ ký số**

**A screen shot of a computer code

Description automatically generated with low confidence**

Hình 3. 3: Code tạo khoá chữ ký số

Đây là một đoạn mã Java để tạo cặp khóa RSA. Cụ thể, chương trình sử dụng lớp **SecureRandom** để tạo một số ngẫu nhiên, sau đó sử dụng **KeyPairGenerator** để tạo ra cặp khóa RSA có độ dài 2048 bit. Sau đó, chương trình lấy khóa công khai và khóa bí mật của cặp khóa này, mã hóa chúng dưới dạng mảng byte và trả về dưới dạng danh sách **List<byte[]>** gồm hai phần tử, phần tử đầu tiên là khóa công khai và phần tử thứ hai là khóa bí mật.

Cụ thể, đoạn mã này có các bước thực hiện như sau:

* Tạo đối tượng **SecureRandom** để tạo một số ngẫu nhiên.
* Tạo đối tượng **KeyPairGenerator** với thuật toán RSA và độ dài khóa là 2048 bit.
* Khởi tạo cặp khóa RSA bằng phương thức **generateKeyPair()** của đối tượng **KeyPairGenerator**.
* Lấy khóa công khai và khóa bí mật từ cặp khóa RSA bằng phương thức **getPublic()** và **getPrivate()**.
* Mã hóa khóa công khai và khóa bí mật dưới dạng mảng byte bằng phương thức **getEncoded()**.
* Thêm khóa công khai và khóa bí mật vào danh sách **List<byte[]>** và trả về.
  + 1. **Ký số lên file**

**A picture containing text, screenshot, font

Description automatically generated**

Hình 3. 4: Code ký số lên file

Mã nguồn trên là một phương thức được viết bằng ngôn ngữ lập trình Java, có chức năng tạo chữ ký số cho một đoạn dữ liệu (biểu diễn dưới dạng mảng byte).

Cụ thể, các dòng mã thực hiện những công việc sau:

* Nhận đầu vào là khóa riêng (PrivateKey) và đoạn dữ liệu cần ký số (DS) được biểu diễn dưới dạng mảng byte.
* Chuyển đổi khóa riêng từ định dạng PKCS#8 về đối tượng PrivateKey, sử dụng lớp KeyFactory và phương thức generatePrivate().
* Khởi tạo đối tượng Signature với thuật toán ký SHA256withRSA, sử dụng phương thức getInstance().
* Khởi tạo đối tượng Signature với khóa riêng, sử dụng phương thức initSign().
* Cập nhật đoạn dữ liệu cần ký số vào đối tượng Signature, sử dụng phương thức update().
* Tạo chữ ký số cho đoạn dữ liệu bằng cách gọi phương thức sign() của đối tượng Signature. Kết quả trả về là một mảng byte biểu diễn chữ ký số.

Tóm lại, phương thức CreateSign1() thực hiện việc tạo chữ ký số dựa trên thuật toán RSA và hàm băm SHA-256. Nó cũng yêu cầu đầu vào là khóa riêng để ký số dữ liệu.

* + 1. **Gửi file ký số**

Sau khi ký số lên file, file đã được mã hóa và bảo vệ bằng chữ ký số. Người gửi có thể gửi file ký số đến người nhận thông qua các kênh truyền thông khác nhau như email, đường truyền internet, USB, v.v.

Việc gửi file ký số giúp đảm bảo tính toàn vẹn và bảo mật của file khi truyền tải. Bên cạnh đó, người nhận cũng có thể xác thực tính hợp pháp của file bằng cách sử dụng chữ ký số được đính kèm trong file ký số.

* + 1. **Xác thực chữ ký của người gửi**

**A screen shot of a computer program

Description automatically generated with low confidence**

Hình 3. 5: Code xác thực chữ ký người gửi

Hàm **verifyy** được sử dụng để xác thực chữ ký số dựa trên khóa công khai và dữ liệu gốc (Input) và chữ ký số (Signature).

Các đối số đầu vào bao gồm:

* **PublicKey**: mảng byte chứa khóa công khai dùng để xác thực chữ ký số.
* **Input**: mảng byte chứa dữ liệu gốc (thông điệp) được ký số.
* **Signature**: mảng byte chứa chữ ký số được tạo ra từ dữ liệu gốc.

Đầu tiên, hàm này sử dụng **X509EncodedKeySpec** để chuyển đổi mảng byte **PublicKey** thành đối tượng khóa công khai. Sau đó, nó sử dụng **verifyDigitalSignature** để xác thực chữ ký số.

Hàm **verifyDigitalSignature** sử dụng đối tượng **Signature** để xác thực chữ ký số. Đầu tiên, nó khởi tạo **Signature** với thuật toán "SHA256withRSA" và khóa công khai được chuyển đổi từ mảng byte **PublicKey**. Sau đó, nó cập nhật dữ liệu đầu vào bằng cách sử dụng phương thức **update** với tham số là mảng byte **Input**. Cuối cùng, nó sử dụng phương thức **verify** của đối tượng **Signature** để xác thực chữ ký số **Signature**.

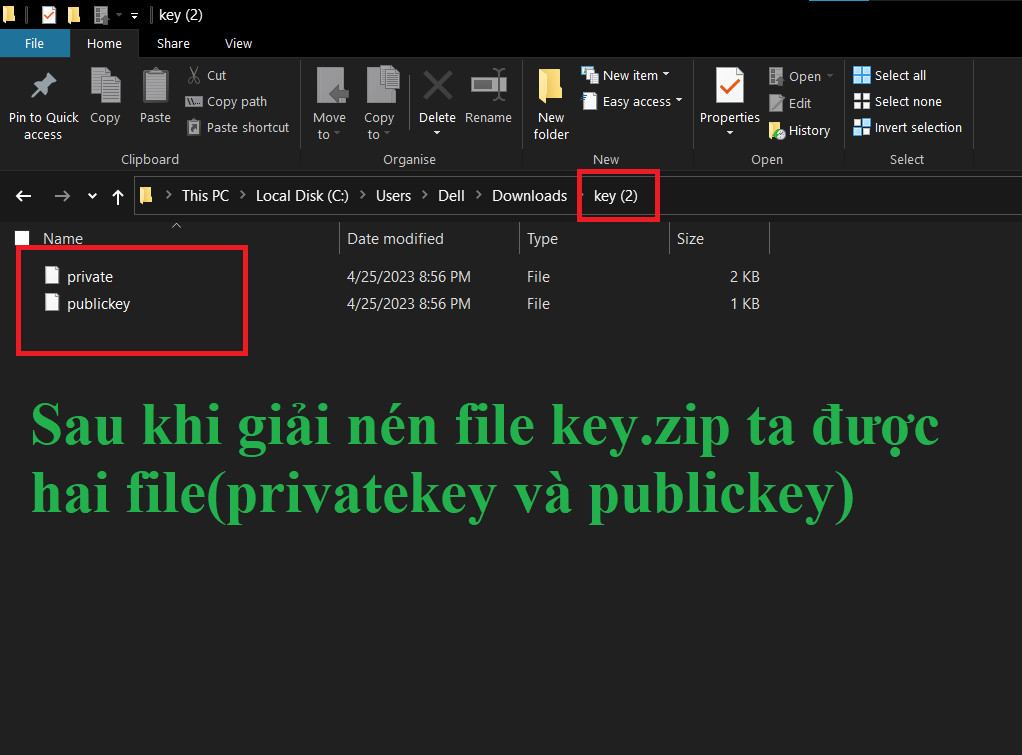
Kết quả trả về của hàm **verifyy** là **true** nếu chữ ký số **Signature** được xác thực bởi khóa công khai **PublicKey** và **Input**.

## **Một số giao diện của hệ thống**

A screenshot of a computer

Description automatically generated with medium confidence

Hình 3. 6: Giao diện khởi tạo và xác thực chữ ký số



Hình 3. 7: Kết quả sau khi khởi tạo chữ ký số

**A screenshot of a computer

Description automatically generated**

Hình 3. 8: Kiểm tra file hợp lệ trước khi thực hiện

**A screenshot of a computer

Description automatically generated with medium confidence**

Hình 3. 9: Tạo file ký số

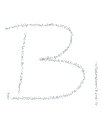
**A screenshot of a computer

Description automatically generated with medium confidence**

Hình 3. 10: Xác thực ký số thành công

****

Hình 3. 11: Xác thực ký số thất bại

**A screenshot of a computer

Description automatically generated with low confidence**



Hình 3. 12: File hợp đồng được xác thực thành công sau khi ký

# KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

## **Kết quả đạt được**

Kết quả đạt được của việc hiện thực sản phẩm với chữ ký số DSS trên 3 ngôn ngữ Java, C# và Python với yêu cầu xác thực chữ ký - thêm được chữ ký vào các file văn bản là:

1. Tạo khoá chữ ký số:

* Tạo cặp khóa (public key và private key) sử dụng thuật toán DSS.
* Tạo chữ ký số DSS bằng cách sử dụng private key và văn bản cần ký.

1. Ký số lên file:

* Đọc file văn bản cần ký.
* Ký số file bằng cách sử dụng chữ ký số DSS đã được tạo.

1. Gửi file ký số:

* Gửi file văn bản đã ký và chữ ký số DSS đi kèm đến người nhận.

1. Xác thực chữ ký của người gửi:

* Đọc file văn bản và chữ ký số DSS được gửi đến.
* Xác thực chữ ký số bằng cách sử dụng public key và văn bản đã được ký.
* Nếu chữ ký số hợp lệ, file văn bản đã ký được xác thực và được coi là đáng tin cậy.

Việc hiện thực sản phẩm này giúp người dùng có thể sử dụng chữ ký số DSS để ký và xác thực tài liệu trên các nền tảng khác nhau bằng 3 ngôn ngữ lập trình phổ biến là Java, C# và Python. Ngoài ra, sản phẩm còn đáp ứng yêu cầu xác thực chữ ký và thêm chữ ký vào các file văn bản, giúp người dùng có thể sử dụng sản phẩm một cách tiện lợi và hiệu quả.

## **Đánh giá kết quả đạt được**

* + 1. **Ưu điểm**

Các ưu điểm của sản phẩm hiện thực chữ ký số DSS trên 3 ngôn ngữ Java, C# và Python với yêu cầu xác thực chữ ký bao gồm:

* Đa nền tảng: Sản phẩm có thể hoạt động trên các hệ điều hành khác nhau như Windows, Linux, Mac OS, v.v. do sử dụng các ngôn ngữ lập trình đa nền tảng như Java, C# và Python.
* Độ an toàn cao: Sản phẩm sử dụng phương pháp ký số DSS có độ an toàn cao, giúp đảm bảo tính toàn vẹn và bảo mật của các file văn bản được ký số.
* Dễ sử dụng: Sản phẩm được thiết kế đơn giản và dễ sử dụng, giúp người dùng có thể tạo và xác thực chữ ký một cách nhanh chóng và thuận tiện.
* Khả năng tương thích cao: Sản phẩm có khả năng tương thích với các ứng dụng và công nghệ khác nhau, giúp người dùng có thể sử dụng sản phẩm một cách linh hoạt.
* Tiết kiệm thời gian và chi phí: Sản phẩm giúp tiết kiệm thời gian và chi phí cho người dùng bằng cách tự động tạo chữ ký số và xác thực chữ ký một cách nhanh chóng và chính xác.

Tổng quan, sản phẩm hiện thực chữ ký số DSS trên 3 ngôn ngữ Java, C# và Python với yêu cầu xác thực chữ ký đáp ứng được các yêu cầu cơ bản của một hệ thống chữ ký số và mang lại nhiều lợi ích cho người dùng.

* + 1. **Nhược điểm**

Một số nhược điểm của việc sử dụng chữ ký số DSS và cách hiện thực sản phẩm có thể bao gồm:

* Khó khăn trong việc triển khai: DSS là một thuật toán phức tạp và việc hiện thực sản phẩm với DSS đòi hỏi kỹ năng chuyên môn cao trong lĩnh vực mã hóa và bảo mật.
* Giới hạn đối với các hệ thống nhúng: Vì DSS sử dụng phép toán số học phức tạp, việc triển khai DSS trên các hệ thống nhúng có tài nguyên hạn chế có thể gặp khó khăn.
* Có thể bị tấn công bởi các kỹ thuật tấn công thời gian thực: Mặc dù DSS được coi là một thuật toán bảo mật, nó vẫn có thể bị tấn công bởi các kỹ thuật tấn công thời gian thực.
* Khó khăn trong việc quản lý chìa khóa: Việc quản lý chìa khóa DSS là rất quan trọng và có thể rất khó khăn, đặc biệt là khi số lượng người dùng là rất lớn.
* Khó khăn trong việc tích hợp với các hệ thống khác: Việc tích hợp DSS với các hệ thống khác có thể gặp khó khăn, đặc biệt là với các hệ thống có kiến trúc khác nhau.

## **Hướng phát triển**

Để phát triển đề tài ký số DSS, có thể thực hiện những bước sau:

* Nghiên cứu các phương pháp ký số mới: Hiện nay, có nhiều phương pháp ký số khác nhau và các phương pháp này đều có ưu điểm và hạn chế riêng. Nên nghiên cứu, so sánh và áp dụng những phương pháp mới nhất và tiên tiến nhất để cải thiện độ an toàn và hiệu suất của hệ thống ký số.
* Phát triển ứng dụng ký số trên các nền tảng khác nhau: Để phát triển ứng dụng ký số phù hợp với nhu cầu sử dụng của nhiều người dùng, có thể phát triển các ứng dụng trên nhiều nền tảng khác nhau như Android, iOS, Windows, Linux, v.v. Điều này sẽ giúp người dùng dễ dàng truy cập và sử dụng ứng dụng ký số trên các thiết bị khác nhau.
* Tích hợp tính năng xác thực bằng nhận diện giọng nói hoặc khuôn mặt: Để cải thiện tính bảo mật và độ chính xác của hệ thống ký số, có thể tích hợp tính năng xác thực bằng nhận diện giọng nói hoặc khuôn mặt. Điều này sẽ giúp người dùng dễ dàng xác thực chữ ký một cách chính xác và nhanh chóng hơn.
* Phát triển tính năng quản lý danh sách truy cập: Tính năng này sẽ giúp người dùng quản lý danh sách các người được phép truy cập vào tài liệu hoặc file ký số của mình. Người dùng có thể tùy chọn phân quyền cho từng người dùng và quản lý danh sách này một cách dễ dàng.
* Tích hợp tính năng lưu trữ đám mây: Tính năng này sẽ giúp người dùng lưu trữ và quản lý các file ký số của mình trên các nền tảng đám mây như Google Drive, OneDrive, Dropbox, v.v. Điều này sẽ giúp người dùng truy cập và chia sẻ file ký số một cách dễ dàng và thuận tiện hơn.

**TÀI LIỆU THAM KHẢO**

**Tiếng Việt**

1. "Chữ ký số và bảo mật thông tin" của Trần Văn Toàn - Nhà xuất bản Đại học Quốc gia Hà Nội, 2018.Quy chế đào tạo trình độ đại học https://thuvienphapluat.vn/van-ban/Giao-duc/Thong-tu-08-2021-TT-BGDDT-Quy-che-dao-tao-trinh-do-dai-hoc-470013.aspx
2. "Chữ ký số trong ứng dụng mã hóa" của Trần Công Án - Nhà xuất bản Công nghệ thông tin, 2017.
3. "Mật mã học và chữ ký số" của Vũ Thế Khương - Nhà xuất bản Đại học Khoa học Tự nhiên, 2014.
4. "Chữ ký số và ứng dụng" của Đỗ Ngọc Hải - Nhà xuất bản Đại học Khoa học Tự nhiên, 2013.
5. "Chữ ký số và ứng dụng trong công nghệ thông tin" của Lê Huy Hùng - Nhà xuất bản Giáo dục, 2010.
6. "Chữ ký số - Lý thuyết và ứng dụng" của Trần Đình Thái - Nhà xuất bản Khoa học và Kỹ thuật, 2010.
7. "Chữ ký số trong thương mại điện tử" của Nguyễn Hải Đăng - Nhà xuất bản Thông tin và Truyền thông, 2012.
8. "Chữ ký số và bảo mật trên Internet" của Nguyễn Đăng Dũng - Nhà xuất bản Đại học Quốc gia Hà Nội, 2007.
9. "Chữ ký số và ứng dụng trong công nghệ thông tin" của Nguyễn Văn Khánh - Nhà xuất bản Giáo dục, 2005.
10. "Bảo mật thông tin và chữ ký số" của Lê Đình Hiệp - Nhà xuất bản Bách Khoa, 2009.

**Tiếng Anh**

1. "Beginning Cryptography with Java" by David Hook - Publisher: Wiley, 2005.
2. "Java Security" by Scott Oaks and Tanuj Gulati - Publisher: O'Reilly Media, 2017.
3. "Applied Cryptography in Java" by Mark Stamp - Publisher: CRC Press, 2003.
4. "Java Security Handbook" by Jamie Jaworski - Publisher: Sams Publishing, 2001.
5. "Java Network Programming and Distributed Computing" by David Reilly and Michael Reilly - Publisher: Addison-Wesley Professional, 2002.
6. "Java Security Solutions" by Nicholas G. McDonald and Daniel Steinberg - Publisher: Wiley, 2002.
7. "Java Cryptography Extensions: Practical Guide for Programmers" by Jason Weiss - Publisher: Addison-Wesley Professional, 2004.
8. "Java 9 Security" by Pankaj Kumar - Publisher: Packt Publishing, 2017.
9. "Java Security: Web Services, Single Sign-On, and XML" by David Hook - Publisher: Wiley, 2008.
10. "Java Cryptography" by Jonathan Knudsen and Eric Young - Publisher: O'Reilly Media, 1998.