TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI

KHOA CÔNG NGHỆ THÔNG TIN

------🙙🕮🙛-------



**BÁO CÁO THỰC NGHIỆM**

Học phần: An toàn & Bảo mật thông tin

**Chủ đề**: Tìm hiểu về chữ ký điện tử RSA và viết ứng dụng minh họa (Sử dụng ngôn ngữ C++, C#)

Giáo viên hướng dẫn : TS. Phạm Văn Hiệp

Nhóm sinh viên thực hiện :

1. Hoàng Minh Ánh Mã SV: 2022607872

2. Phạm Văn Đại Mã SV: 2021605488

3. Phan Đặng Thông Mã SV: 2021606302

4. Hoàng Thị Thúy Mã SV: 2021601086

5. Trần Thị Thu Trang Mã SV: 2021603154

Mã lớp học phần: 20232IT6001011

Nhóm: 5

Hà Nội - Năm 2024

**MỤC LỤC**

[LỜI MỞ ĐẦU 4](#_Toc170338258)

[CHƯƠNG 1. TỔNG QUAN VỀ ĐỀ TÀI 5](#_Toc170338259)

[1.1 Tổng quát về đề tài 5](#_Toc170338260)

[1.2 Lý do chọn đề tài 5](#_Toc170338261)

[1.3 Nội dung nghiên cứu 6](#_Toc170338262)

[*1.3.1 Hệ mã hóa bất đối xứng* 6](#_Toc170338263)

[*1.3.2 Chữ ký điện tử, Chữ ký số* 6](#_Toc170338264)

[*1.3.3 Hệ mã hóa RSA và hàm băm* 7](#_Toc170338265)

[*1.3.4 Ứng dụng của RSA trong chữ ký số điện tử* 7](#_Toc170338266)

[1.4 Các kiến thức cần có 8](#_Toc170338267)

[CHƯƠNG 2. PHÂN TÍCH VÀ THIẾT KẾ 10](#_Toc170338268)

[2.1 Giới thiệu 10](#_Toc170338269)

[2.2 Nội dung nghiên cứu 10](#_Toc170338270)

[**2.2.1 Hệ mã hóa bất đối xứng** 10](#_Toc170338271)

[**2.2.2 Chữ ký điện tử** 13](#_Toc170338272)

[**2.2.3 Chữ ký số** 13](#_Toc170338273)

[2.2.3.1 Khái niệm chữ ký số 13](#_Toc170338274)

[2.2.3.2 Đặc điểm chữ ký số 14](#_Toc170338275)

[2.2.3.3 Đối tượng sử dụng chữ ký số 14](#_Toc170338276)

[2.2.3.4 Mục đích sử dụng chữ ký số 14](#_Toc170338277)

[**2.2.4 Hàm băm** 15](#_Toc170338278)

[**2.2.5 Hệ mã hóa RSA** 16](#_Toc170338279)

[**2.2.6 Bài toán ứng dụng của RSA trong chữ ký số điện tử** 21](#_Toc170338280)

[2.2.6.1 Giới thiệu 21](#_Toc170338281)

[2.2.6.2 Nguyên lý hoạt động 21](#_Toc170338282)

[2.3 Thiết kế, cài đặt chương trình demo thuật toán 26](#_Toc170338283)

[**2.3.1 Chương trình C#** 26](#_Toc170338284)

[**2.3.2 Chương trình C++** 32](#_Toc170338285)

[CHƯƠNG 3. KẾT QUẢ THỰC HIỆN 35](#_Toc170338286)

[3.1 Nội dung đã thực hiện 35](#_Toc170338287)

[3.2 Thuận lợi và khó khăn trong quá trình nghiên cứu 35](#_Toc170338288)

[3.3 Hướng phát triển. 36](#_Toc170338289)

[TÀI LIỆU THAM KHẢO 38](#_Toc170338290)

DANH MỤC HÌNH ẢNH

[Hình 1: Phần tạo khóa C# 26](#_Toc170303145)

[Hình 2: Phần ký văn bản C# 27](#_Toc170303146)

[Hình 3: Phần xác nhận chữ ký C# 28](#_Toc170303147)

[Hình 4: Hướng dẫn tạo khóa và tạo chữ ký C# 28](#_Toc170303148)

[Hình 5: Hàm kiểm tra số nguyên tố C# 29](#_Toc170303149)

[Hình 6: Hàm tính modular multiplicative inverse của a modulo b sử dụng thuật toán Euclid C# 29](#_Toc170303150)

[Hình 7: Hàm tính x^n mod m bằng phương pháp đệ quy C#. 30](#_Toc170303151)

[Hình 8: Thuật toán sinh khóa C# 30](#_Toc170303152)

[Hình 9: Mã hóa sử dụng khóa bí mật C# 31](#_Toc170303153)

[Hình 10: Giải mã sử dụng khóa công khai C# 31](#_Toc170303154)

Hình 11: Giao diện chương trình C++ ................................................32

Hình 12: Sinh khóa..............................................................................33

Hình 13: Sinh chữ ký...........................................................................34

Hình 14: Kiểm tra chữ ký.....................................................................34

# LỜI MỞ ĐẦU

Trong thời đại công nghệ số phát triển mạnh mẽ, các giao dịch điện tử ngày càng trở nên phổ biến. Để đảm bảo tính xác thực và toàn vẹn của các giao dịch này, chữ ký số là một công cụ không thể thiếu. Chữ ký số sử dụng các thuật toán mã hóa để tạo ra một chuỗi ký tự có thể được sử dụng để xác định nguồn gốc và tính toàn vẹn của một thông điệp hoặc tài liệu. Ở đề tài này nhóm em đề cập tới thuật toán mã hóa RSA. Đây là một hệ mã hóa bất đối xứng, được phát triển bởi Ron Rivest, Adi Shamir và Leonard Adleman vào năm 1978. RSA dựa trên một bài toán khó giải trong lý thuyết số, đó là bài toán phân tích số nguyên tố.

Để ứng dụng phương pháp trên vào thực tiễn, được sự hướng dẫn của thầy Phạm Văn Hiệp, chúng em lựa chọn đề tài “Ứng dụng của RSA trong chữ ký số điện tử” với mong muốn áp dụng kiến thức đã học, giải quyết bài toán mã hóa chữ ký điện tử.

Đề tài nhóm gồm 3 phần:

Chương 1: Tổng quan về đề tài

Chương 2: Phân tích và thiết kế

Chương 3: Kết quả thực hiện

Đề tài được hoàn thành bằng sự cộng tác của các thành viên nhóm cùng sự hướng dẫn của thầy Phạm Văn Hiệp. Nội dung đề tài được hoàn thành dựa trên những lý thuyết đã học về Chuẩn dữ liệu RSA cùng nhiều tài liệu tham khảo khác tuy nhiên không tránh khỏi thiếu sót mong nhận thêm phản ánh và góp ý từ phía giảng viên và quý bạn đọc.

***Chúng em xin trân thành cảm ơn!***

# CHƯƠNG 1. TỔNG QUAN VỀ ĐỀ TÀI

## 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 Lý do chọn đề tài

Từ thời xa xưa, ông cha chúng ta thường sử dụng con dấu của cá nhân hoặc những chữ ký tay để sử dụng cho các loại văn bản giấy tờ thực, thánh chỉ, các hiệp ước, hiệp định hoặc các bản cam kết. Những chữ ký tay này mang vai trò quyết định giá trị của văn bản và đại diện cho trách nhiệm của các bên tham gia ký kết văn bản. Nhưng vào thời đại phát triển hiện nay, các công ty doanh nghiệp sử dụng dịch vụ kinh doanh giao dịch điện tử ngày càng nhiều, dẫn đến thanh toán, xác thực online trở nên cực kỳ quan trọng . Việc các công ty di chuyển hợp đồng lẫn nhân sự đến gặp tận nơi để ký kết theo cách thủ công thời xưa khá là bất tiện, tốn khá nhiều thời gian, công sức, nhân lực. Đặc biệt dưới sự bùng phát của dịch bệnh COVID-19 vừa qua càng khiến việc này trở nên khó khăn và nguy hiểm.

Chính vì những bất cập trên, chữ ký điện tử ra đời, mở ra một kỷ nguyên mới về thời đại công nghệ chữ ký số. Cho nên nhóm 6 chúng em chọn đề tài nghiên cứu về chữ ký điện tử trong bảo mật thông tin kết hợp với hệ mã hóa RSA và ứng dụng chữ ký điện tử RSA trong bài báo cáo môn An toàn bảo mật thông tin này.

Đề tài này chúng ta cần nắm vững được cách mã hóa thông tin bằng hệ mã hóa RSA và cách áp dụng chữ ký điện tử trong an toàn và bảo mật thông tin.

## 1.3 Nội dung nghiên cứu

Với đề tài ứng dụng của RSA trong chữ ký số điện tử, nhóm 6 sẽ tiến hành nghiên cứu tập trung vào các nội dung sau:

### *1.3.1 Hệ mã hóa bất đối xứng*

Hệ mã hoá bất đối xứng (asymmetric encryption) là một phương pháp mã hoá thông tin sử dụng một cặp khóa chia thành hai phần: khóa công khai (public key) và khóa riêng tư (private key). Cặp khóa này được tạo ra sao cho dữ liệu được mã hóa bằng khóa công khai chỉ có thể được giải mã bằng khóa riêng tư tương ứng và ngược lại. Trong giai đoạn này, chúng ta sẽ tìm hiểu mô hình mã hoá bất đối xứng, khoá công khai (public key), khoá riêng tư (private key), cơ chế hoạt động, ưu điểm, nhược điểm của hệ mã hoá bất đối xứng.

### *1.3.2 Chữ ký điện tử, Chữ ký số*

Chữ ký điện tử là một khái niệm rộng, bao gồm mọi hình thức ký kết được thực hiện bằng phương tiện điện tử, nhằm xác định danh tính của người ký và thể hiện sự chấp thuận của họ đối với nội dung thông tin được ký.

Chữ ký số (digital signature) là một cách để xác thực tính toàn vẹn và nguồn gốc của một thông điệp hoặc tài liệu điện tử. Chữ ký số thường được tạo ra bằng cách sử dụng hệ mã hoá bất đối xứng, như RSA hoặc DSA.Trong giai đoạn này, chúng ta sẽ tìm hiểu quá trình hoạt động của chữ ký số, các bước thực hiện.

### *1.3.3 Hệ mã hóa RSA và hàm băm*

RSA là một thuật toán mã hóa khóa công khai. Đây là thuật toán đầu tiên phù hợp với việc tạo ra chữ ký điện tử đồng thời với việc mã hóa. RSA đang được sử dụng phổ biến trong thương mại điện tử và được cho là đảm bảo an toàn với điều kiện độ dài khóa đủ lớn. RSA được Ron Rivest, Adi Shamir và Len Adleman giới thiệu năm 1977 tại Học viện Công nghệ Massachusetts (MIT). Trong giai đoạn này, chúng ta sẽ tìm hiểu quy trình hoạt động của hệ mã hoá RSA(thuật toán RSA), ý tưởng(Motivation) và hiện thực ý tưởng .

Hàm băm là một hàm toán học lấy một đầu vào dữ liệu và tạo ra một đầu ra có độ dài cố định. Đầu ra của hàm băm được gọi là giá trị băm hoặc tóm tắt.

Hệ thống RSA và hàm băm có thể được sử dụng cùng nhau để cải thiện bảo mật. Ví dụ: hàm băm thường được sử dụng để tạo một tóm tắt (digest) của thông điệp hoặc dữ liệu gốc, và sau đó chữ ký số được tạo dựa trên tóm tắt này. Mục đích của việc này là đảm bảo tính toàn vẹn của thông điệp và xác nhận rằng thông điệp không bị thay đổi trong quá trình truyền tải.

### *1.3.4 Ứng dụng của RSA trong chữ ký số điện tử*

Chữ ký số RSA là một ứng dụng quan trọng của hệ mã hoá RSA, được sử dụng để xác thực người gửi thông điệp và đảm bảo tính toàn vẹn của thông điệp trong quá trình truyền tải. Chữ ký số RSA là một công cụ quan trọng trong việc đảm bảo an toàn thông tin và xác thực trong các giao dịch điện tử và truyền thông trực tuyến. Chúng ta sẽ triển khai cụ thể phương pháp này bằng các ngôn ngữ lập trình để thực hiện xử lý chữ ký số điện tử bằng phương pháp hệ mã RSA và tìm hiểu thêm một số lợi ích khi sử dụng RSA trong chữ ký số.

**1.3.5 Đánh giá tính khả thi và hiệu quả**

Sau khi đã triển khai và đánh giá tính khả thi và hiệu quả của phương pháp, chúng ta sẽ đánh giá độ tin cậy và tính bảo mật của phương pháp, đồng thời đề xuất các cải tiến và phát triển cho phương pháp trong tương lai. Một số phát triển có thể bao gồm việc phát triển các phương pháp tối ưu hóa để cải thiện hiệu suất của RSA, đặc biệt là trong môi trường có tải cao hoặc phát triển cách quản lý khóa hiệu quả hơn và an toàn hơn, đặc biệt là trong các hệ thống phức tạp.

## 1.4 Các kiến thức cần có

**1.4.1 Kiến thức về mật mã học và an ninh thông tin**

Để hiểu được cơ chế hoạt động của thuật toán RSA trong chữ ký số điện tử, cần có các kiến thức cơ bản về mật mã học và an ninh thông tin, bao gồm các khái niệm và thuật ngữ cơ bản, các phương pháp tấn công và bảo vệ thông tin, các thuật toán mã hóa đối xứng và bất đối xứng, …

**1.4.2 Kiến thức về lập trình**

* Để ứng dụng RSA trong chữ ký số điện tử, cần nắm vững các kiến thức về lập trình, bao gồm các ngôn ngữ lập trình, các cấu trúc dữ liệu và thuật toán cơ bản, các thư viện mã hóa và phân tích rủi ro thông tin,...
* Các kiến thức ngôn ngữ lập trình: C++, C# và lập trình giao diện
* Kiến thức về sử dụng các công cụ lập trình: Apache Netbeans

**1.4.3 Kiến thức về toán học**

Để hiểu được phương pháp bảo mật thông tin-Ứng dụng của RSA trong chữ ký số điện tử, sinh viên cần nắm vững các kiến thức về thuật toán như thuật toán Euclid, định lý Fermat, hàm số Euler, thuật toán Miller-Rabin....Phương pháp mã hóa bất đối xứng và ứng dụng của phương pháp mã hóa bất đối xứng vào trong quá trình tạo và xác minh chữ ký điện tử. Kiến thức về hàm Băm (Hash) và ứng dụng của nó trong quá trình tạo chữ điện tử.

**1.4.4 Kiến thức về quản lý dữ liệu**

Để triển khai các phương pháp bảo mật thông tin trong chữ ký số, sinh viên cần nắm vững các kiến thức về quản lý dữ liệu, bao gồm các khái niệm cơ bản về cơ sở dữ liệu, các phương pháp truy vấn dữ liệu và xử lý dữ liệu, …

# CHƯƠNG 2. PHÂN TÍCH VÀ THIẾT KẾ

## 2.1 Giới thiệu

Chữ ký điện tử được ứng dụng và thừa kế từ các thành tựu khoa học về mã hoá khoá công khai. Trong chương này ở các mục sau chúng ta sẽ tìm hiểu kỹ hơn về các thức tạo và xác thực chữ ký số.

Các 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

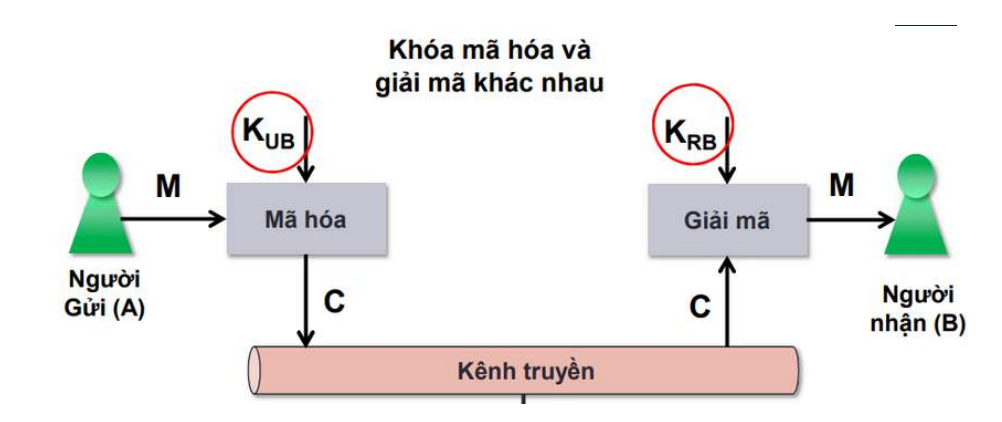
Hình thức sản phẩm: sản phẩm bản mẫu

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

## 2.2 Nội dung nghiên cứu

### **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.

  
 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:

* 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 kể từ khi thực hiện biến đổi

#### 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

Chữ ký số bao gồm 3 mục đích chính, quan trọng sau đây:

- Dùng để kê khai, nộp tờ khai, nộp các nghĩa vụ tài chính trong lĩnh vực thuế, hải quan và giao dịch chứng khoán,....

- Dùng khi doanh nghiệp cần thực hiện các thủ tục về đăng ký doanh nghiệp như: đăng ký địa điểm kinh doanh, thành lập chi nhánh, văn phòng đại diện hay thay đổi đăng ký kinh doanh,....

- Sử dụng khi doanh nghiệp và đối tác/khách hàng của doanh nghiệp ký kết hợp đồng thông qua hình thức trực tuyến.

Như vậy, mục đích cuối cùng khi sử dụng chữ ký số đó là giúp cho quá trình trao đổi thông tin, dữ liệu giữa các bên liên quan trở nên nhanh chóng và thuận lợi hơn. Đồng thời dễ dàng thao tác các thủ tục trực tuyến, rút ngắn thời gian trao đổi mà vẫn đảm bảo tính bảo mật cao và an toàn về mặt pháp lý.

### **2.2.4 Hàm băm**

- Hàm băm mật mã là hàm toán học chuyển đổi một 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 bit này được gọi là thông điệp rút gọn (message digest) hay giá trị băm (hash value), đại diện cho thông điệp ban đầu.

- Hàm băm giúp xác định được tính toàn vẹn dữ liệu của thông tin: mọi thay đổi, dù là rất nhỏ, trên thông điệp cho trước, ví dụ chỉ thay đổi giá trị 1 bit, đều làm thay đổi thông điệp rút gọn tương ứng. Tính chất này hữu ích trong việc phát sinh, kiểm tra chữ ký điện tử, các đoạn mã chứng nhận thông điệp, phát sinh số ngẫu nhiên, tạo ra khóa cho quá trình mã hóa, ….

- Các tính chất cơ bản của hàm băm:

* Là hàm một chiều, không thể thực hiện phép biến đổi ngược như trong quá trình mã hóa và giải mã, nghĩa là với một message\_digest cho trước, khó có thể tìm được một message nào mà có hàm băm bằng message\_digest này.
* Khó có thể tìm được hai message mà có cùng một message\_digest.
* Hàm một chiều: Hàm f(x) được gọi là hàm một chiều, nếu tính y = f(x) là dễ, nhưng việc tính ngược x = f -1 (y) là rất khó (dễ nghĩa là tính được trong thời gian đa thức,(khó là không tính được trong thời gian đa thức).

**Ví dụ:** Hàm f(x) = p\*q = n là hàm một chiều vì biết p và q tính n là dễ nhưng ngược lại biết n tìm p và q là khó.

Hàm băm là nền tảng cho nhiều ứng dụng mã hóa. Có nhiều thuật toán để thực hiện hàm băm, trong số đó, phương pháp SHA-1 và MD5 thường được sử dụng khá phổ biến từ thập niên 1990 đến nay.

### **2.2.5 Hệ mã hóa RSA**

* Mục đích: **RSA** là một thuật toán mật mã hóa khóa công khai. Đây là thuật toán đầu tiên phù hợp với việc tạo ra chữ ký điện tử đồng thời với việc mã hóa. Nó đánh dấu một sự tiến bộ vượt bậc của lĩnh vực mật mã học trong việc sử dụng khóa công cộng. RSA đang được sử dụng phổ biến trong [thương mại điện tử](https://vi.wikipedia.org/wiki/Th%C6%B0%C6%A1ng_m%E1%BA%A1i_%C4%91i%E1%BB%87n_t%E1%BB%AD) và được cho là đảm bảo an toàn với điều kiện độ dài khóa đủ lớn.
* Mô tả sơ lược:
* Thuật toán RSA có hai [khóa](https://vi.wikipedia.org/wiki/Kh%C3%B3a_(m%E1%BA%ADt_m%C3%A3)): [khóa công khai](https://vi.wikipedia.org/wiki/M%E1%BA%ADt_m%C3%A3_h%C3%B3a_kh%C3%B3a_c%C3%B4ng_khai) (hay khóa công cộng) và [khóa bí mật](https://vi.wikipedia.org/w/index.php?title=Kh%C3%B3a_b%C3%AD_m%E1%BA%ADt&action=edit&redlink=1) (hay khóa cá nhân). 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.

Ví dụ: Ta có thể mô phỏng trực quan một hệ mật mã khóa công khai như sau: Bình muốn gửi một thông tin mật muốn duy nhất An có thể đọc được. An gửi cho Bình một chiếc hộp có khóa đã mở sẵn và giữ lại chìa khóa. Bình nhận chiếc hộp, cho vào đó một tờ giấy viết thư bình thường và khóa lại (như loại khoá thông thường chỉ cần sập chốt lại, sau khi sập chốt khóa ngay cả Bình cũng không thể mở lại được-không đọc lại hay sửa thông tin trong thư được nữa). Sau đó Bình gửi chiếc hộp lại cho An. An 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.

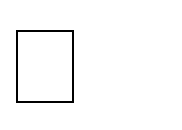
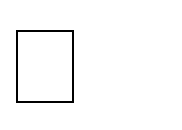
* Ý tưởng và ví dụ
* Ý tưởng về một hệ mật khóa công khai đã được Diffie và Hellman đưa ra vào 1976. Còn việc hiện thực hóa hệ mật khóa công khai thì do Rivest, Shamir và Adleman đưa ra đầu tiên vào 1977, họ đã tạo nên hệ mật RSA nổi tiếng.
* Hệ mật này sử dụng các tính toán trong Zn, trong đó n là tích của 2 số nguyên tố phân biệt p và q. Ta có thể mô tả hệ mật RSA như sau:

Cho n = p.q trong đó p và q là các số nguyên tố.

Đặt P=C=Zn và định nghĩa:

* K=(n,p,q,a,b);
* n=p.q ;
* p, q là các số nguyên tố, ab=1(mod∅(n))

Với K =(n,p,q,a,b) ta xác định:

* ek(x)=xb mod n
* dk(y)=ya mod n các giá trị n và b được công khai và các giá trị p, q, a được giữ kín,
* ∅(n)=(p-1)(q-1)
* Quá trình thực hiện hệ mật RSA: (người gửi: Alice; người nhận: Bob):
  + Bob tạo hai số nguyên tố lớn p và q
  + Bob tính n = pq và ∅(n) = (p-1)(q-1)
  + Bob chọn một số ngẫu nhiên e (0<e<∅(n)) sao cho gcd(e,∅(n))=1
  + Bob tính de = 1 mod ∅(n) bằng cách dùng thuật toán Euclide
  + Bob công bố n và e trong một danh bạ và dùng chúng làm khoá công khai.
* Mô tả cách hoạt động của RSA:
  + Tạo khóa:
    - Bước này bao gồm quá trình tạo ra cặp khóa gồm khóa công khai (public key) và khóa bí mật (private key).
    - Đầu tiên, chọn hai số nguyên tố lớn p và q.
    - Tính toán modulus (n) bằng cách nhân p và q: n = p \* q.
    - Tính toán hàm Euler (phi) của n: phi = (p – 1) \* (q – 1).
    - Chọn một số nguyên e sao cho 1 < e < phi(n) và e là số nguyên tố cùng nhau với phi.
    - Tính toán khóa bí mật d bằng cách tìm nghịch đảo modulo của e theo modulo phi: d = e^(-1) mod phi.
    - Khóa công khai là cặp (n, e) và khóa bí mật là cặp (n, d).
  + Mã hóa
    - Để mã hóa một thông điệp (plaintext), chia nó thành các khối nhỏ hơn.
    - Mỗi khối được biểu diễn bằng một số nguyên m (nhỏ hơn n).
    - Áp dụng công thức mã hóa: ciphertext = m^e mod n.
    - Kết quả là ciphertext (văn bản mã hóa
  + Giải mã
    - Khi nhận được ciphertext, để giải mã chúng ta sử dụng khóa bí mật (n, d).
    - Áp dụng công thức giải mã: plaintext = ciphertext^d mod n.
    - Kết quả là plaintext (văn bản gốc).

**Các ví dụ về khóa**

**Ví dụ 1:** Chọn hai số nguyên tố: p = 101, q = 113.

- Tính n = p \* q = 101 \* 113 = 11413.

φ(n) = (p-1)\* (q -1)

= (101- 1)\* (113 - 1) = 100\*112 = 11200.

- Chọn e = 3533 vì gcd(e, φ(n)) = gcd(3533, 11200) = 1.

- Tính d = e-1 mod 11200 = 6597 (Dùng giải thuật Euclid mở rộng).

- Vậy khóa công khai là (e, n) = (3533, 11413); khóa bí mật là (d, n) = (6597, 11413).

**Ví dụ 2:**

Chọn hai số nguyên tố p = 43, q = 59.

Tính n = 43 \* 59 = 2537, φ(n) = 42 \* 58 = 2436

Chọn e = 13 vì gcd(e, φ(n)) = gcd(13, 2436) = 1

Tính d = e-1 mod 2436 = 937. (Dùng giải thuật Euclide mở rộng)

Khóa công khai là (e, n) = (13, 2537).

Khóa bí mật là (d, n) = (937, 2537).

Tiếp theo để mã hóa thông điệp M: “DAI HOC” ta thực hiện như sau:

A white square with black letters and numbers

Description automatically generated

***Bảng 1.3 Bảng quy ước mã hóa thông điệp***

Đầu tiên ta chuyển thông điệp M trên về dạng số và nhóm lại thành từng khối có 4 chữ số ta được bản rõ:

0300 0807 1402

Sau đó mã hóa mỗi khối của bản rõ thực hiện như sau:

C = *m*13 (mod 2537)

Với *m* = 0300 Ta có C = 030013 mod 2537 = 1031.

*m* = 0807 Ta có C = 080713 mod 2537 = 1123.

*m* = 1402 Ta có C = 140213 mod 2537 = 0331.

Để giải mã khối thông điệp C ta thực hiện:

*m* = C937 (mod 2537)

Với C = 1031 ta có: *m* = 1031937 mod 2537 = 0300.

C = 1123 ta có: *m* = 1123937 mod 2537 = 0807.

C = 0331 ta có: m = 0331937 mod 2537 = 1402.

Ta đã tìm được bản rõ dưới dạng số, kết hợp với bảng quy ước trên ta khôi

phục lại nội dung thông điệp M là “DAI HOC”.

### **2.2.6 Bài toán ứng dụng của RSA trong chữ ký số điện tử**

#### 2.2.6.1 Giới thiệu

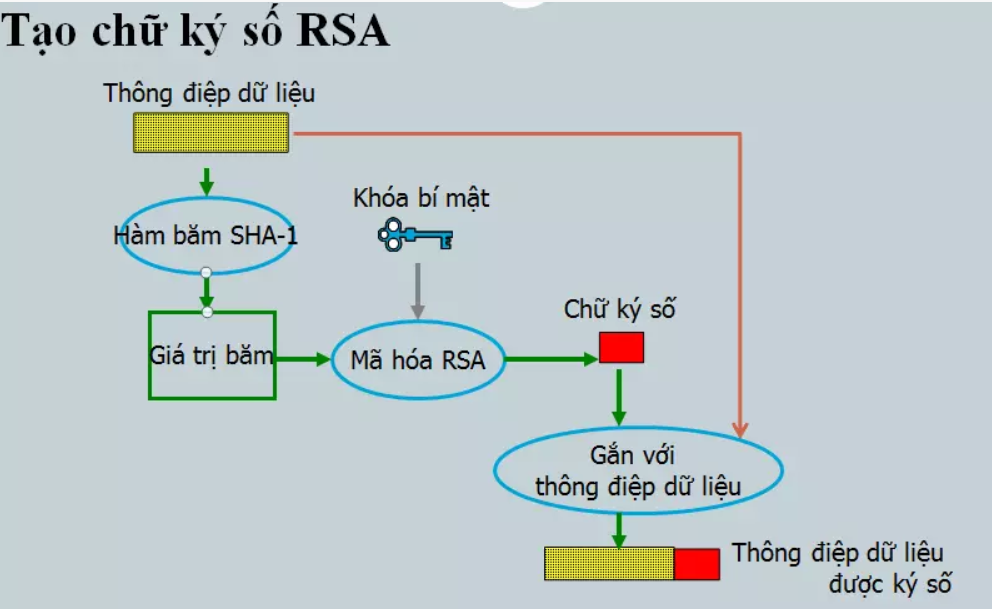
Bài toán ứng dụng của RSA trong chữ ký số điện tử là một trong những ví dụ tiêu biểu về cách giải quyết vấn đề xác thực và bảo mật trong môi trường truyền thông điện tử. RSA là một hệ mật mã công khai, sử dụng cặp khóa công khai và khóa bí mật, nơi khóa công khai được chia sẻ cho mọi người và khóa bí mật chỉ được giữ bởi người tạo chữ ký.

* *Giải thuật tạo ra chữ ký số* (Digital Signature generation algorithm) là một phương pháp sinh chữ ký số.
* *Giải thuật kiểm tra chữ ký số*(Digital Signature verification algorithm) là một phương pháp xác minh tính xác thực của chữ ký số, có nghĩa là nó thực sự được tạo ra bởi 1 bên chỉ định.
* *Một hệ chữ ký số* (Digital Signature Scheme) bao gồm giải thuật tạo chữ số và giải thuật kiểm tra chữ kỹ số.
* *Quá trình tạo chữ ký số* (Digital Signature signing process):
  + Giải thuật tạo chữ ký số.
  + Phương pháp chuyển dữ liệu thông điệp thành dạng có thể ký được.
* ***Quá trình kiểm tra chữ ký số***(Digital signature verification process):
  + Giải thuật kiểm tra chữ ký số.
  + Phương pháp khôi phục dữ liệu từ thông điệp.

#### 2.2.6.2 Nguyên lý hoạt động

Quá trình ký

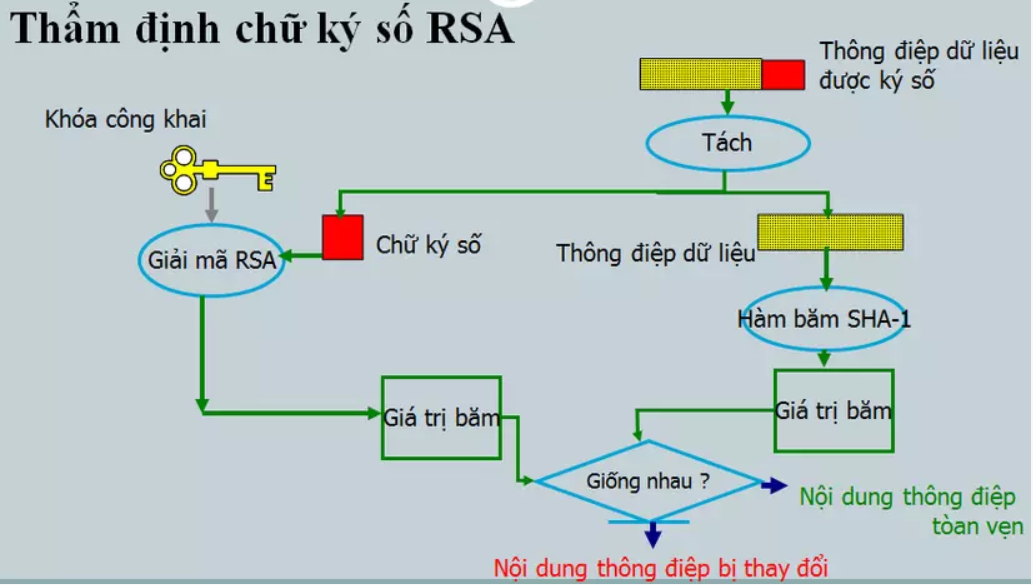
* **B1:** Tạo khóa bằng hệ mã hóa gồm khóa bí mật và khóa công khai. Sử dụng khóa bí mật để tạo chữ ký.
* **B2:** Sử dụng thuật toán băm, để băm dữ liệu cần ký thành một chuỗi ký tự duy nhất với độ dài cố định. Có thể gọi là chuỗi H1.
  + Lưu ý thuật toán băm dữ liệu phải được thống nhất giữa người ký 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 4. Quá trình tạo chữ ký*

Quá 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.



*Hình 5. Quá trình kiểm tra chữ ký*

Ví dụ: Giả sử A ký một chữ ký *s* lên thông điệp P = 31229978 sau đó gửi cho B. Cá thể B bất kỳ có thể chứng thực chữ ký có đúng là của A hay không và khôi phục lại thông điệp P từ chữ ký *s. (Quá trình này không sử dụng hàm băm)*

**Quá trình sinh khóa:**

Cá thể A thực hiện các bước sau:

1. Chọn hai số nguyên tố *p* = 7927, *q* = 6997.
2. Tính: *n* = *p*\**q* = 7927\*6997 = 55465219

φ(*n*) = 7926\*6996 = 55450296

1. Chọn *e* = 5, 1< *e* < 55450296.
2. Tính *d*: Từ *e*\**d* = 1 mod 55450296, tìm được *d* = 44360237.

Khóa công khai là (*e*, *n*) = (5, 55450296);

Khóa bí mật (*d, n*) = (44360237, 55450296).

**Quá trình sinh chữ ký:**

Giả sử M = Zn và hàm *R*: M -> Zn xác định *R*(P) = P với mọi P thuộc M.

P = 31229978 khi đó A thực hiện:

* 1. Số hóa thông điệp P: Tính *m* = *R*(P) = 31229978,
  2. Tính chữ ký

*s* = *m*d mod *n*

= 3122997844360237 mod 55465219 = 30729435.

* 1. Gửi *s* cho B.

**Quá trình chứng thực chữ ký:**

B thực hiện các bước sau:

1. Nhận khóa công khai của A là (5, 55465219)
2. Tính *m* = *s*e mod *n*

= 307294355 mod 55465219 = 31229978

1. Kiểm tra *m* = 31229978 thuộc [0, 55465219]. Xác nhận chữ ký *s* là của A.
2. Khôi phục P = *R-1*(*m*) = 31229978.

## 2.3 Thiết kế, cài đặt chương trình demo thuật toán

### **2.3.1 Chương trình C#**

**- Phần tạo khóa**

* Tại giao diện tạo khóa chúng ta nhấn vào phần tạo khóa để sinh khóa công khai và khóa bí mật  
  A screenshot of a computer

  Description automatically generated

Hình 1: Phần tạo khóa C#

**- Phần ký văn bản**

* Tại giao diện ký văn bản ta lần lượt thực hiện các bước sau:
  + Tải văn bản cần ký
  + Ký vào văn bản đó
  + Sau khi đã ký xong thì lưu lại chữ ký

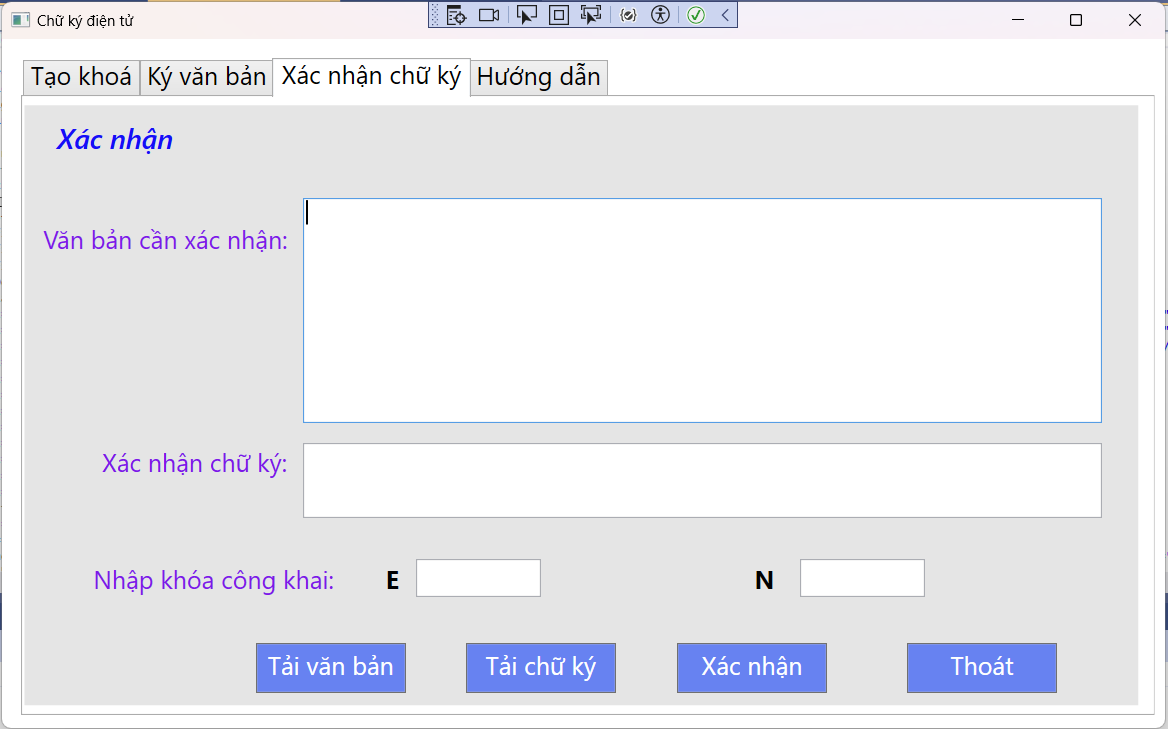
A screenshot of a computer

Description automatically generated

Hình 2: Phần ký văn bản C#

**- Phần xác nhận văn bản**

* Tại giao diện xác nhận văn bản ta thực hiện các bước:
  + Tải văn bản đã ký và cần xác nhận lên
  + Tải chữ ký kèm theo đã được ký ở văn bản
  + Xác nhận chữ ký
* Nếu văn bản đã được chỉnh sửa hoặc chữ ký kèm theo không chính xác sẽ xuất ra thông báo là văn bản đã được chỉnh sửa hoặc chữ ký không chính xác.
* Nếu văn bản và chữ ký đều chính xác thì chương trình sẽ thông báo chữ ký đã chính xác.



Hình 3: Phần xác nhận chữ ký C#

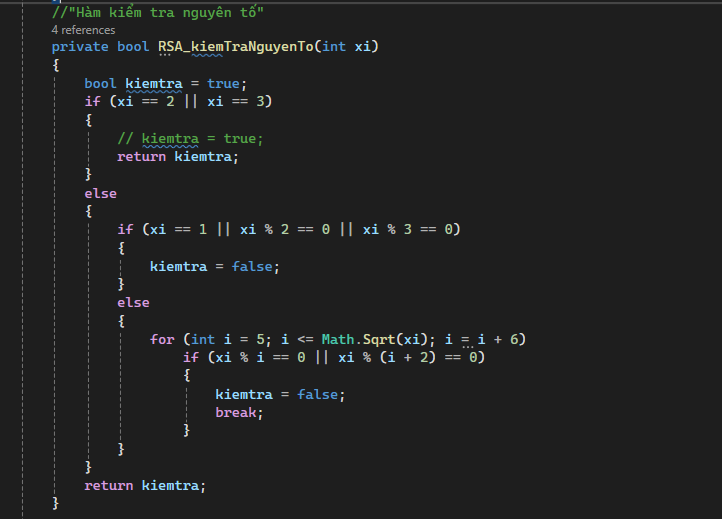
**- Hướng dẫn tạo khóa và tạo chữ ký**

A screenshot of a computer

Description automatically generated

Hình 4: Hướng dẫn tạo khóa và tạo chữ ký C#

**- Cài đặt chương trình:**



Hình 5: Hàm kiểm tra số nguyên tố

A computer screen with colorful text

Description automatically generated

Hình 6: Hàm tính modular multiplicative inverse của a modulo b sử dụng thuật toán Euclid C#

A computer screen with numbers and symbols

Description automatically generated

Hình 7: Hàm tính x^n mod m bằng phương pháp đệ quy.

A computer code on a black background

Description automatically generated

Hình 8: Thuật toán sinh khóa



Hình 9: Mã hóa sử dụng khóa bí mật C#

A computer screen with many colorful text

Description automatically generated with medium confidence

Hình 10: Giải mã sử dụng khóa công khai

### **2.3.2 Chương trình C++**

Ảnh có chứa ảnh chụp màn hình, văn bản, Phần mềm đa phương tiện, Phần mềm đồ họa

Mô tả được tạo tự động

Hình 11: Giao diện chương trình C++

**- Phần tạo khóa**

* Tại giao diện chúng ta nhấn vào phần sinh khóa hay sinh ngẫu nhiên để sinh khóa công khai và khóa bí mật

**- Phần ký văn bản**

* Tại phần ký văn bản ta lần lượt thực hiện các bước sau:
  + Tải văn bản cần ký
  + Ký vào văn bản đó

Sau khi đã ký xong thì lưu lại chữ ký  
**- Phần xác nhận văn bản**

* Tại phần xác nhận văn bản ta thực hiện các bước:
  + Tải văn bản đã ký và cần xác nhận lên
  + Tải chữ ký kèm theo đã được ký ở văn bản
  + Xác nhận chữ ký
* Nếu văn bản đã được chỉnh sửa hoặc chữ ký kèm theo không chính xác sẽ xuất ra thông báo là văn bản đã được chỉnh sửa hoặc chữ ký không chính xác.
* Nếu văn bản và chữ ký đều chính xác thì chương trình sẽ thông báo chữ ký đã chính xác.

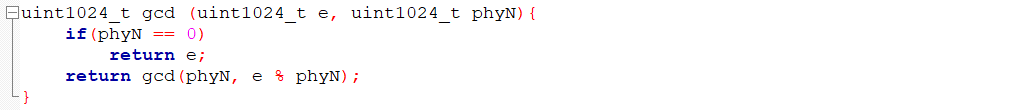
**- Cài đặt chương trình:**

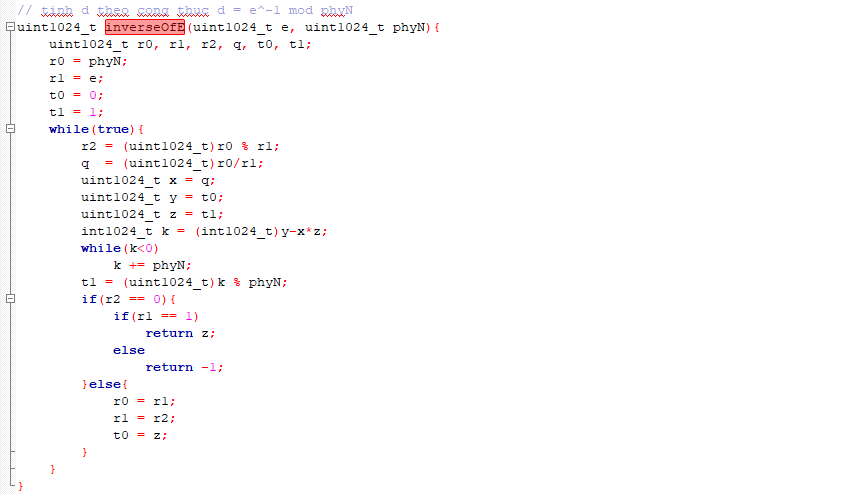
Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, hàng

Mô tả được tạo tự động

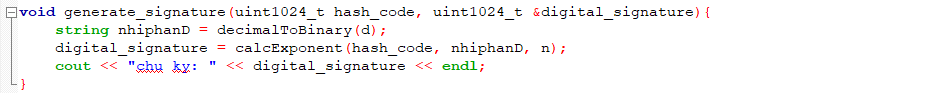
Ảnh có chứa văn bản, Phông chữ, hàng, ảnh chụp màn hình

Mô tả được tạo tự động





Hình 12: sinh khóa



Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, số

Mô tả được tạo tự động

Ảnh có chứa văn bản, hàng, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

Hình 13: Sinh chữ ký

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, số

Mô tả được tạo tự động

Hình 14: Kiểm tra chữ ký

# CHƯƠNG 3. KẾT QUẢ THỰC HIỆN

## 3.1 Nội dung đã thực hiện

Về kiến thức:

* Nắm vững các khái niệm về chữ ký điện tử, thuật toán RSA, hàm băm, mã hóa bất đối xứng.
* 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 C++, C# để xây dựng chương trình ứng dụng demo cho chữ ký điện tử.
* 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.

## 3.2 Thuận lợi và khó khăn trong quá trình nghiên cứu

* Thuận lợi
  + Thuật toán RSA là một trong những thuật toán chữ ký số và mã hóa khóa công khai phổ biến và được sử dụng rộng rãi trong hệ thống bảo mật thông tin.
  + Nghiên cứu về ứng dụng của RSA trong chữ ký số có thể mang lại nhiều kết quả có ứng dụng thực tế và sâu sắc.
  + Chữ ký số và hệ thống chữ ký số điện tử đóng vai trò quan trọng trong việc xác minh danh tính và chứng thực thông tin trong môi trường truyền thông điện tử.
  + Nghiên cứu về cách cải thiện hiệu suất và bảo mật của hệ thống RSA có thể đưa ra những tiến bộ đáng kể trong lĩnh vực này.
* Khó khăn
  + Việc tìm hiểu kiến thức về toán học đòi hỏi sự tư duy cao.
  + RSA sử dụng các phép toán số học lớn và đối mặt với thách thức về hiệu suất trong xử lý số lớn.

## 3.3 Hướng phát triển.

Chữ ký số RSA là một phương pháp mã hóa và xác nhận chữ ký quan trọng trong lĩnh vực bảo mật thông tin. Để phát triển và mở rộng chữ ký số RSA, có một số cải tiến nên được xem xét:

* Tăng kích thước khóa: Kích thước khóa lớn hơn sẽ làm cho việc tìm kiếm khóa riêng tư thông qua phân tích dựa trên sức mạnh tính toán trở nên khó khăn hơn.
* Tích hợp với công nghệ mới: Kết hợp RSA với các công nghệ mới như trí tuệ nhân tạo (AI) để phát hiện và ngăn chặn tấn công một cách hiệu quả hơn, hoặc tích hợp vào mô hình blockchain để cung cấp tính toàn vẹn và xác nhận trong hệ thống phi tập trung.
* Tăng cường hiệu suất: Cải thiện hiệu suất của quá trình tạo chữ ký và xác nhận, có thể thông qua việc tối ưu hóa mã nguồn, sử dụng phần cứng tăng tốc, hoặc các kỹ thuật khác để giảm thời gian xử lý.
* Chữ ký số đa yếu tố: Xem xét cách tích hợp chữ ký số RSA vào các hệ thống đa yếu tố, nơi nó có thể kết hợp với các phương tiện xác thực khác như mật khẩu để cung cấp lớp bảo mật mạnh mẽ hơn.

Trong tương lai, chữ ký số RSA sẽ tiếp tục đóng một vai trò quan trọng trong nhiều lĩnh vực, đặc biệt là trong bối cảnh sự phát triển nhanh chóng của thế giới số. Dưới đây là một số ứng dụng tiềm năng:

* Bảo mật Giao dịch Tài chính: Chữ ký số RSA có thể được sử dụng để đảm bảo tính toàn vẹn và xác thực trong các giao dịch tài chính trực tuyến, bảo vệ khỏi tấn công giả mạo và gian lận.
* Chữ ký trong Blockchain: Blockchain sử dụng chữ ký số để xác minh tính toàn vẹn của các khối dữ liệu. RSA có thể được tích hợp vào các hệ thống blockchain để đảm bảo an toàn và đáng tin cậy.
* Quản lý Điện tử và Chữ ký Điện tử: Chữ ký số RSA có thể được áp dụng rộng rãi trong quản lý điện tử, chẳng hạn như chứng nhận và xác thực các tài liệu trực tuyến, giúp tạo ra môi trường làm việc điện tử an toàn.
* Xác thực trong Y tế Điện tử: Trong lĩnh vực y tế điện tử, chữ ký số có thể đảm bảo an toàn thông tin bệnh nhân và xác thực các tài liệu y tế trực tuyến.
* Chữ ký trong Chính phủ Điện tử: Các hệ thống chữ ký số RSA có thể được tích hợp vào các dự án chính phủ điện tử để bảo vệ thông tin quan trọng và xác thực người dùng.

Những ứng dụng này chỉ là một số ví dụ và không giới hạn sự đa dạng của cách mà chữ ký số RSA có thể được tích hợp trong thế giới số ngày nay và tương lai.

# TÀI LIỆU THAM KHẢO

1. Nguyễn Bá Thái (2011), **“**Nghiên cứu lược đồ chia sẻ bí mật và ứng dụng của chúng vào việc thi tuyển sinh đại học”, Luận văn Thạc sĩ, Trường đại học Công nghệ, ĐHQG Hà Nội.

2. Khoa Công Nghệ (2007), Giáo trình An toàn và bảo mật thông tin, Đại học Giao Thông Vận Tải, Hà Nội.

3. Ethos (2018). What is key sharing? Shamir Secret Sharing Explained. Youtube: https://www.youtube.com/watch?v=nh8UV0SynQg