

**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 chữ ký điện tử Elgamal và viết ứng dụng minh họa**.

Giáo viên hướng dẫn : TS. Phạm Văn Hiệp

Nhóm sinh viên thực hiện :

1. Vũ Thị Hường Mã SV: 2021601944

2. Trịnh Thu Phương Mã SV: 2021600948

3. Trịnh Bá Nguyên Mã SV: 2021602345

4. Nguyễn Thị Hồng Nhung Mã SV: 2021602687

5. Võ Anh Dũng Mã SV: 2022606587

Mã lớp học phần: 20232IT6001005

Nhóm: 6

Hà Nội - Năm 2024

**MỤC LỤC**

[DANH MỤC HÌNH ẢNH 4](#_heading=h.1fob9te)

[LỜI NÓI ĐẦU 5](#_heading=h.3znysh7)

[CHƯƠNG 1: TỔNG QUAN 6](#_heading=h.2et92p0)

[1.1. Lý do chọn đề tài 6](#_heading=h.tyjcwt)

[1.2. Tổng quan về An toàn bảo mật thông tin 6](#_heading=h.3dy6vkm)

[1.2.1. Lý do phải bảo vệ thông tin 6](#_heading=h.1t3h5sf)

[1.2.2. Khái niệm hệ thống và tài sản hệ thống 7](#_heading=h.4d34og8)

[1.2.3. Các mối đe doạ đối với một hệ thống và các biện pháp ngăn chặn 7](#_heading=h.2s8eyo1)

[1.2.4. Mục tiêu chung của an toàn bảo mật thông tin 8](#_heading=h.17dp8vu)

[1.3. Các kiến thức cơ sở 8](#_heading=h.3rdcrjn)

[1.4. Nội dung nghiên cứu 9](#_heading=h.26in1rg)

[CHƯƠNG 2: KẾT QUẢ NGHIÊN CỨU 11](#_heading=h.lnxbz9)

[2.1. Tìm hiểu về chữ ký điện tử 11](#_heading=h.35nkun2)

[2.2.1. Khái niệm 11](#_heading=h.1ksv4uv)

[2.2.2. Lĩnh vực hoạt động 11](#_heading=h.44sinio)

[2.2.3. Ưu và nhược điểm 13](#_heading=h.2jxsxqh)

[2.2.4. Nguyên lý hoạt động 15](#_heading=h.z337ya)

[2.2. Chữ ký điện tử Elgamal 18](#_heading=h.4i7ojhp)

[2.2.1. Lược đồ chữ ký điện tử Elgamal 18](#_heading=h.2xcytpi)

[2.2.2. Ví dụ 18](#_heading=h.1ci93xb)

[2.2.3. Độ an toàn 24](#_heading=h.3whwml4)

[2.3. Hàm băm 25](#_heading=h.2bn6wsx)

[2.3.1. Giới thiệu hàm băm Hash 25](#_heading=h.qsh70q)

[2.3.2. Tính chất cơ bản của hàm băm Hash 26](#_heading=h.1pxezwc)

[2.3.3. Một số hàm băm thông dụng 26](#_heading=h.49x2ik5)

[2.3.4. Ứng dụng của hàm băm Hash 27](#_heading=h.2p2csry)

[2.3.5. Thuật toán hàm băm SHA-1 29](#_heading=h.23ckvvd)

[2.3.5.1. Giới thiệu hàm băm SHA-1 29](#_heading=h.ihv636)

[2.3.5.2. Thuật toán SHA-1 29](#_heading=h.32hioqz)

[2.4. Mã hóa bất đối xứng 32](#_heading=h.41mghml)

[2.4.1. Giới thiệu 32](#_heading=h.2grqrue)

[2.4.2. Nguyên lý hoạt động 32](#_heading=h.vx1227)

[2.4.3. Ưu Điểm và Ứng Dụng 33](#_heading=h.3fwokq0)

[2.5. Thiết kế, cài đặt chương trình 34](#_heading=h.1v1yuxt)

[2.5.1. Chương trình C# 34](#_heading=h.4f1mdlm)

[2.5.2. Chương trình C++ 38](#_heading=h.19c6y18)

[CHƯƠNG 3: KẾT LUẬN VÀ BÀI HỌC KINH NGHIỆM 47](#_heading=h.28h4qwu)

[3.1. Kiến thức kỹ năng đã học được trong quá trình thực hiện đề tài 47](#_heading=h.nmf14n)

[3.2. Bài học kinh nghiệm 47](#_heading=h.37m2jsg)

[3.3. Đề xuất về tính khả thi của chủ đề nghiên cứu, những thuận lợi, khó khăn 47](#_heading=h.1mrcu09)

[TÀI LIỆU THAM KHẢO 49](#_heading=h.46r0co2)

# DANH MỤC HÌNH ẢNH

[Hình 1. Quá trình tạo chữ ký 16](#_heading=h.3j2qqm3)

[Hình 2. Quá trình kiểm tra chữ ký 17](#_heading=h.1y810tw)

[Hình 3. Ví dụ hàm băm hash 25](#_heading=h.3as4poj)

[Hình 4. Mã hóa thông điệp bằng khóa bí mật của người ký 28](#_heading=h.147n2zr)

[Hình 5. Chứng thực chữ ký số 28](#_heading=h.3o7alnk)

[Hình 6. Sơ đồ thuật toán SHA-1 30](#_heading=h.1hmsyys)

[Hình 7. Giao diện chương trình C# 34](#_heading=h.2u6wntf)

[Hình 8. Giao diện chương trình C++ 38](#_heading=h.3tbugp1)

# LỜI NÓI ĐẦU

Bài tập lớn của chúng em có thể được thực hiện một cách suôn sẻ, thành công, không thể không kể đến công lao to lớn trong việc dạy dỗ, truyền đạt kiến thức của giảng viên hướng dẫn TS. Phạm Văn Hiệp, Khoa Công nghệ thông tin, trường Đại học Công nghiệp Hà Nội. Những chia sẻ, hướng dẫn của thầy thực sự là vốn quý, là nguyên liệu giúp chúng em hoàn thành bài tập lớn một cách tốt nhất!

Đề tài của chúng em được triển khai và gói gọn trong 3 chương, cụ thể như sau:

* Chương 1: Tổng quan: Mô tả tổng quát đề tài nghiên cứu
* Chương 2: Kết quả nghiên cứu: Trình bày những nhiệm vụ, công việc chính khi thực hiện đề tài và kết quả đạt được
* Chương 3: Kết luận và bài học kinh nghiệm

# CHƯƠNG 1: TỔNG QUAN

## **1.1. Lý do chọn đề tài**

**Bảo mật thông tin** luôn là vấn đề quan trọng hàng đầu trong các lĩnh vực tình báo, quân sự, ngoại giao, và đây cũng là một vấn đề đã được nghiên cứu hàng nghìn năm nay. Bảo mật thông tin là duy trì tính bảo mật, tính toàn vẹn và tính sẵn sàng của thông tin. Bảo mật nghĩa là đảm bảo thông tin chỉ được tiếp cận bởi những người được cấp quyền tương ứng. Tính toàn vẹn là bảo vệ sự chính xác, hoàn chỉnh của thông tin và thông tin chỉ được thay đổi bởi những người được cấp quyền. Tính sẵn sàng của thông tin là những người được quyền sử dụng có thể truy xuất thông tin khi họ cần. Vấn đề bảo mật đang được nhiều người tập trung nghiên cứu và tìm mọi giải pháp để đảm bảo an toàn, an ninh cho hệ thống phần mềm, đặc biệt là các hệ thống thông tin trên mạng Internet cho phép mọi người truy cập, khai thác và chia sẻ thông tin. Mặt khác nó cũng là nguy cơ chính dẫn đến thông tin bị rò rỉ hoặc bị phá hoại. Lúc này việc bảo mật an toàn dữ liệu là vấn đề thời sự, là một chủ đề rộng có liên quan đến nhiều lĩnh vực và trong thực tế có nhiều phương pháp được thực hiện để đảm bảo dữ liệu.

Sự ra đời của văn bản điện tử đã kéo theo sự xuất hiện của giao dịch điện tử, từ đó phát sinh nhu cầu ký trên văn bản điện tử để thực hiện được các giao dịch ấy, và đó cũng là lúc mà chữ ký điện tử được hình thànhnhằm chứng thực tác giả của văn bản đó và giúp người nhận kiểm tra tính toàn vẹn của nội dung văn bản gốc.

Nhằm tìm hiểu một trong những phương pháp bảo vệ an toàn thông tin có tính an toàn cao hiện nay là dùng ***Chữ ký điện tử*** .Nhóm em đã chọn đề tài: “***Tìm hiểu về chữ ký điện tử ElGamal và viết ứng dụng minh họa***.” cho báo cáo thực nghiệm học phần An toàn và bảo mật thông tin

## **1.2. Tổng quan về An toàn bảo mật thông tin**

### 1.2.1. Lý do phải bảo vệ thông tin

* Thông tin là một bộ phận quan trọng và là tài sản thuộc quyền sở hữu của các tổ chức
* Sự thiệt hại và lạm dụng thông tin không chỉ ảnh hưởng đến người sử dụng hoặc các ứng dụng mà nó còn gây ra các hậu quả tai hại cho toàn bộ tổ chức đó
* Thêm vào đó sự ra đời của Internet đã giúp cho việc truy cập thông tin ngày càng trở nên dễ dàng hơn

### 1.2.2. Khái niệm hệ thống và tài sản hệ thống

* **Khái niệm hệ thống**: Hệ thống là một tập hợp các máy tính bao gồm các thành phần, phần cứng, phần mềm và dữ liệu làm việc được tích luỹ qua thời gian.
* **Tài sản của hệ thống bao gồm:**
* Phần cứng
* Phần mềm
* Dữ liệu
* Các truyền thông giữa các máy tính của hệ thống
* Môi trường làm việc
* Con người

### 1.2.3. Các mối đe doạ đối với một hệ thống và các biện pháp ngăn chặn

**Có 3 hình thức chủ yếu đe dọa đối với hệ thống:**

* Phá hoại: kẻ thù phá hỏng thiết bị phần cứng hoặc phần mềm hoạt động trên hệ thống.
* Sửa đổi: Tài sản của hệ thống bị sửa đổi trái phép. Điều này thường làm cho hệ thống không làm đúng chức năng của nó. Chẳng hạn như thay đổi mật khẩu, quyền người dùng trong hệ thống làm họ không thể truy cập vào hệ thống để làm việc.
* Can thiệp: Tài sản bị truy cập bởi những người không có thẩm quyền. Các truyền thông thực hiện trên hệ thống bị ngăn chặn, sửa đổi.

**Các đe dọa đối với một hệ thống thông tin có thể đến từ ba loại đối tượng như sau:**

* Các đối tượng từ ngay bên trong hệ thống (insider), đây là những người có quyền truy cập hợp pháp đối với hệ thống.
* Những đối tượng bên ngoài hệ thống (hacker, cracker), thường các đối tượng này tấn công qua những đường kết nối với hệ thống như Internet chẳng hạn.
* Các phần mềm (spyware, adware …) chạy trên hệ thống.

**Các biện pháp ngăn chặn:**

* **Điều khiển thông qua phần mềm:** dựa vào các cơ chế an toàn bảo mật của hệ thống nền (hệ điều hành), các thuật toán mật mã học.
* **Điều khiển thông qua phần cứng:** các cơ chế bảo mật, các thuật toán mật mã học được cứng hóa để sử dụng.
* **Điều khiển thông qua các chính sách của tổ chức:** ban hành các qui định của tổ chức nhằm đảm bảo tính an toàn bảo mật của hệ thống.

### 1.2.4. Mục tiêu chung của an toàn bảo mật thông tin

* **Tính bí mật (Confidentiality):** Đảm bảo rằng thông tin không bị truy cập bất hợp pháp.
* **Tính toàn vẹn (Integrity):** Đảm bảo rằng thông tin không bị sử dụng bất hợp pháp.
* **Tính sẵn sàng (Availability):** Tài sản luôn sẵn sàng được sử dụng với những người có thẩm quyền.
* **Tính xác thực (Authentication):** Đảm bảo rằng dữ liệu nhận được chắc chắn là dữ liệu gốc ban đầu.

## **1.3. Các kiến thức cơ sở**

**Thuật toán và định lý:**

* Nắm rõ các kiến thức cơ bản về Chữ ký điện tử (Định nghĩa, ưu, nhược điểm, vai trò,...)
* Kiến thức về chữ ký điện tử Elgamal (Lược đồ chữ ký điện tử Elgamal, cách tạo chữ ký, cách xác minh chữ ký,…)
* Kiến thức về các thuật toán sinh khóa, mã hóa, giải mã cùng với các thuật toán liên quan như thuật toán kiểm tra số nguyên tố, phép toán Modulo, Euclid mở rộng, phần tử sinh,...
* Phương pháp mã hóa bất đối xứng, và ứng dụng của nó 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 ký điện tử

**Ngôn ngữ lập trình:**

* Ngôn ngữ C++: hiểu về cú pháp và cách sử dụng các cấu trúc dữ liệu cơ bản, lớp và đối tượng, thư viện chuẩn C++, và quy trình biên dịch và chạy chương trình.
* Ngôn ngữ C#: hiểu về cú pháp của C# và các khái niệm như lớp, đối tượng, và thuộc tính. Nắm vững các thư viện chuẩn của .NET Framework hoặc .NET Core và cách sử dụng chúng để phát triển ứng dụng.

**Kiến thức về sử dụng các công cụ lập trình**

* Đối với C++ : Visual studio 2019/ DevC++
* Đối với C# : Visual studio 2019

## **1.4. Nội dung nghiên cứu**

* **Tìm hiểu về chữ ký điện tử**

● Khái niệm thế nào là chữ ký điện tử ?

● Lĩnh vực hoạt động

● Một số ưu nhược điểm của chữ ký điện tử.

* **Chữ ký điện tử ElGamal**

● Lược đồ chữ ký điện tử ElGamal.

● Ví dụ minh hoạ.

● Độ an toàn của chữ ký điện tử ElGamal

* **Tìm hiểu phương pháp mã hóa bất đối xứng ứng dụng trong chữ ký điện tử**

● Mã hóa bất đối xứng là gì?

● Đặc điểm

▪ Ưu điểm

▪ Hạn chế

● Ứng dụng trong chữ ký số

▪ Chữ ký số

▪ Chữ ký số sử dụng hệ mật mã Elgamal

▪ Ưu điểm

▪ Ý nghĩa

* **Tìm hiểu về hàm băm SHA**

● Giới thiệu hàm băm Hash

● Tính chất cơ bản của hàm băm Hash

● Danh sách các hàm băm mật mã học

● Ứng dụng hàm băm Hash

● Thuật toán hàm băm SHA-1

▪ Giới thiệu hàm băm SHA-1

▪ Thuật toán băm SHA-1

● Thuật toán hàm băm SHA-256

▪ Mã hoá SHA-256 là gì ?

▪ Ứng dụng của SHA-256

Áp dụng thực hiện xây dựng chương trình với các ngôn ngữ C++,Java, C#, JavaScript, Python

# CHƯƠNG 2: KẾT QUẢ NGHIÊN CỨU

## **2.1. Tìm hiểu về chữ ký điện tử**

### 2.2.1. Khái niệm

* Chữ ký điện tử là một dạng thông tin được gắn liền hoặc kết hợp với dữ liệu điện tử. Loại chữ ký này nhằm giúp xác định danh tính chủ thể của dữ liệu và thể hiện sự chấp thuận của chủ thể đối với nội dung hợp đồng. Dữ liệu điện tử có thể được trình bày dưới hình thức văn bản, hình ảnh, video… Chữ ký được sử dụng trong giao dịch điện tử của các chủ thể dữ liệu có các đặc điểm sau:
* Tính toàn vẹn: Đảm bảo dữ liệu không bị thay đổi sau khi được ký.
* Tính xác thực: Xác định chính xác người ký.
* Tính không thể chối cãi: Người ký không thể chối bỏ việc đã ký.
* Tính bảo mật: Đảm bảo thông tin ký được bảo mật.
* Chữ ký điện tử được sử dụng rộng rãi trong nhiều lĩnh vực như hợp đồng, giao dịch điện tử và thủ tục hành chính. Chữ ký có giá trị pháp lý tương đương với chữ ký viết tay nếu chữ ký đó tuân thủ đúng các quy định của pháp luật.
* 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, ảnh, video, … dữ liệu đó có bị thay đổi hay không

### 2.2.2. Lĩnh vực hoạt động

Phạm vi ứng dụng của chữ ký số rất rộng, gồm nhiều lĩnh vực, như: Ký số trong thư điện tử cho phép khách hàng xác định chính xác người gửi; Sử dụng chữ ký số thực hiện việc ký các văn bản xác nhận khi đầu tư chứng khoán trực tuyến, bán hàng trực tuyến, thanh toán trực tuyến, chuyển tiền trực tuyến; Ký số trong hợp đồng kinh tế mà không cần gặp mặt trực tiếp; Ký số trong kê khai, nộp thuế trực tuyến, khai báo hải quan và thông quan trực tuyến… Trong các cơ quan Nhà nước, ứng dụng chữ ký số là một yếu tố không thể thiếu để xây dựng Chính phủ điện tử và cải cách thủ tục hành chính. Trong các doanh nghiệp, chữ ký số là công cụ hữu hiệu trong giao dịch với các cơ quan nhà nước thông qua các dịch vụ công trực tuyến, giao dịch với các đối tác và khách hàng của mình. Việc ứng dụng chữ ký số giúp tiết kiệm chi phí (chi phí mua giấy in, mực in, chi phí và thời gian gửi văn bản); giảm thiểu sức lao động trong công tác quản lý, bảo mật dữ liệu cá nhân và dữ liệu chuyên môn; giảm thời gian, tiết kiệm chi phí đi lại của người dân và doanh nghiệp; quan trọng nhất là minh bạch hóa thông tin, làm thay đổi phương pháp, tác phong công tác, phương thức làm việc...

**Ứng dụng chữ ký số:**

* **Trong chính phủ điện tử**

● Khai báo hải quan điện tử, thuế điện tử

● Khai sinh, khai tử

● Cấp các loại giấy tờ và chứng chỉ

● Hệ thống nộp hồ sơ xin phép: xuất bản, xây dựng, y tế, giáo dục...

* **Trong thương mại điện tử**

● Chứng thực danh tính người tham gia giao dịch, xác thực tính an toàn của giao dịch điện tử qua mạng Internet.

● Chứng thực tính nguyên vẹn của hợp đồng, tài liệu...

● Ứng dụng xác thực trong Internet banking

● Ứng dụng xác thực trong giao dịch chứng khoán

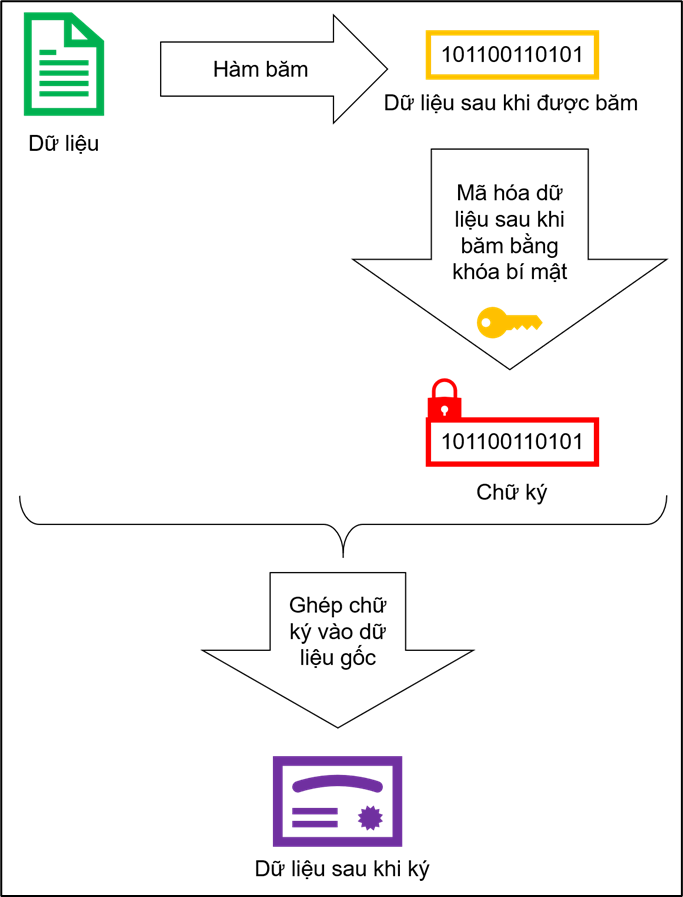
● Ứng dụng xác thực trong mua bán, đấu thầu qua mạng

### 2.2.3. Ưu và nhược điểm

* **Ưu điểm**
* **Đảm bảo tính toàn vẹn dữ liệu:** Việc sử dụng chữ ký điện tử giúp xác minh dữ liệu có bị thay đổi hay không.
* **Giúp xác thực người ký dễ dàng:** Có thể xác minh thông tin của người ký dữ liệu điện tử một các dễ dàng thông qua khóa công khai của hệ mã.
* **Chống thoái thác:** Khi chữ ký điện tử được tạo ra, người ký sẽ không thể phủ nhận việc đã ký chữ ký đó.
* **Tiết kiệm thời gian:** Sử dụng chữ ký điện tử giúp cho việc thực hiện ký kết các giao dịch, hợp đồng, phát hành hóa đơn, báo cáo, … một cách nhanh chóng thay vì phải chuyển văn bản giấy và ký tay. Việc dùng chữ ký điện tử trong trường hợp này sẽ tiết kiệm được tối đa thời gian ký. Bên cạnh đó có thể tiết kiệm được thời gian đi lại, gặp gỡ đối tác để ký tay; không phải mất thời gian in giấy tờ.
* **Tiết kiệm chi phí:** Các tổ chức không cần sử dụng đến giấy tở cho các văn bản. Họ sẽ tiết kiệm được chi phí cho các nguồn lực vật chất, thời gian, nhân sự và không gian văn phòng. Tác động tích cực đến môi trường. Giảm thiểu sử dụng giấy cũng cắt giảm chất thải vật lý do giấy tạo ra.
* **Giúp truy xuất nguồn gốc dễ dàng:** Chữ ký điện tử tạo ra một dấu vết kiểm tra giúp lưu trữ hồ sơ nội bộ dễ dàng hơn cho doanh nghiệp. Với việc tất cả mọi thông tin được ghi lại và lưu trữ bằng kỹ thuật số, thì cơ hội mắc lỗi trong hồ sơ hoặc làm thất lạc dữ liệu sẽ giảm đáng kể.
* **Chính xác và bảo mật thông tin:** Việc sử dụng chữ ký số sẽ đảm bảo việc không tẩy xóa, thay đổi các thông tin như thực hiện ký giấy, đảm bảo tính toàn vẹn của dữ liệu, là bằng chứng cho các giao dịch điện tử, nội dùng điện tử được ký kết. Chữ ký số được tạo ra bởi những thông tin dữ liệu phức tạp thông qua mã hóa và khó bị giả mạo nên sẽ giúp bảo mật thông tin một cách an toàn.
* **Có thể sử dụng chữ ký điện tử mọi lúc, mọi nơi:** Chữ ký điện tử có thể được sử dụng mọi lúc và mọi nơi không phải phụ thuộc vào giờ làm việc hành chính, thời tiết hay địa lý. Việc ký kết các hợp đồng, văn bản điện tử trở nên dễ dàng và nhanh chóng.
* **Giúp hạn chế tối đa việc làm giả chữ ký, gian lận thủ tục:** Để sử dụng chữ ký điện tử để ký văn bản điện tử, cần phải có khóa bí mật của hệ mã hóa sử dụng cho việc ký. Vì vậy, khi sử dụng chữ ký điện tử sẽ hạn chế việc làm giả chữ ký; đem lại sự minh bạch trong việc xác nhận quyền và nghĩa vụ của các bên trong nội dung văn bản ký.
* **Tăng cường bảo mật cho các hệ thống truyền thông Internet:** Ứng dụng chữ ký số vào việc ký kết các văn bản, hợp đồng, truyền dữ liệu trực tuyến trở lên an toàn hơn, người dùng có thể xác minh tính toàn vẹn của dữ liệu cũng như xác thực danh tính người thực hiện ký dữ liệu.
* **Hỗ trợ bảo mật các hệ thống BlockChain:** Chữ ký số đảm bảo rằng chỉ những chủ sở hữu hợp pháp của tiền điện tử mới có thể ký một giao dịch để chuyển tiền.
* **Nhược điểm**
* **Sự an toàn và tính bảo mật cử chữ ký điện tử phụ thuộc vào thuật toán được sử dụng:** Chữ ký điện tử được tạo ra bởi việc sử dụng các hàm băm và các hệ thống mã hóa. Bởi vậy mức độ an toàn và tính bảo mật của chữ ký điện tử sẽ phụ thuộc vào việc lựa chọn các hàm băm đàng tin cậy và các hệ thống mã hóa có tính bảo mật cao.
* **Có thể bị giả mạo chữ ký nếu xảy ra sai sót:** Nếu các khóa bí mật của hệ mã hóa bị rò rỉ hoặc bằng cách nào đó bị xâm phạm, các thuộc tính xác thực và chống thoái thác sẽ bị vô hiệu; từ đó dẫn đến khả năng giả mạo chữ ký, giả mạo danh tính để thực hiện các hoạt động phi pháp.
* **Khó chứng minh, xác thực chữ ký nếu để xảy ra sai sót:** Chữ ký điện tử được tạo nên bởi những thông tin, dữ liệu phức tạp nên trường hợp chứng minh, kiểm chứng lại chữ ký sẽ gây ra khó khăn cho người sử dụng. Người sử dụng cần cải thiện tối đa tính bảo mật của chữ ký điện tử để tránh trường hợp sai sót không mong muốn xảy ra.
* **Khó khăn khi thực hiện các thủ tục:** Khi tiến hành ký, xác thực chữ ký điện tử có thể gặp các lỗi như: hệ thống máy tính chưa tương thích, khả năng truy cập mạng, …

### 2.2.4. Nguyên lý hoạt động

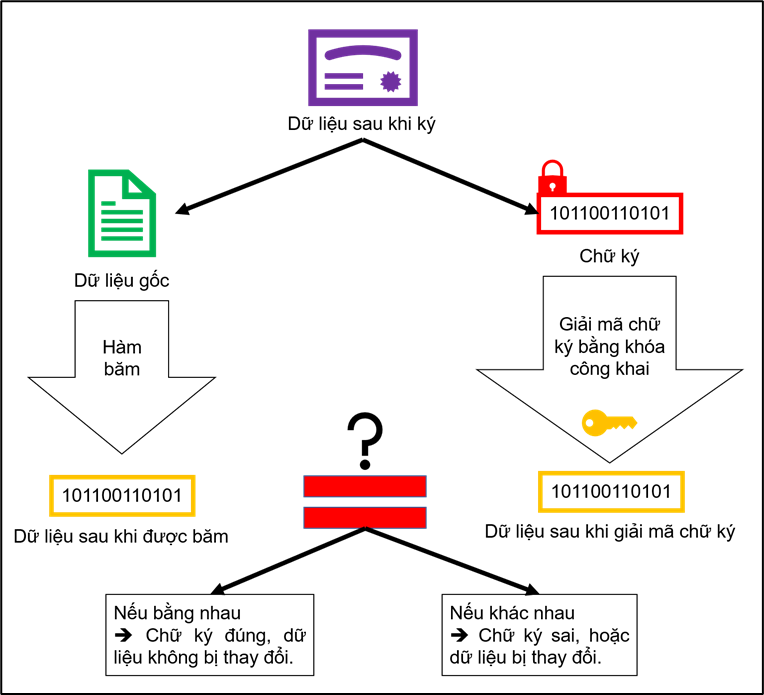
* **Quá trình ký**
* **B1:** Tạo khóa bằng hệ mã hóa gồm khóa bí mật và khóa công khai. Sử dụng khóa bí mật để tạo chữ ký.
* **B2:** Sử dụng thuật toán băm (MD5 hoặc SHA), để băm dữ liệu cần ký thành một chuỗi ký tự duy nhất với độ dài cố định. Có thể gọi là chuỗi H1.
* Lưu ý thuật toán băm dữ liệu phải 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 ngay 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 1. 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 (MD5 hoặc SHA) 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 (dữ liệu) 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 2. Quá trình kiểm tra chữ ký*

## **2.2. Chữ ký điện tử Elgamal**

### 2.2.1. Lược đồ chữ ký điện tử Elgamal

⮚ **Tạo tham số và khóa :**

+ Chọn số nguyên tố **p** đủ lớn

+ Chọn phần tử nguyên thủy **g**: **g ϵ Zp\***.

+ Chọn ngẫu nhiên khóa bí mật x sao cho: 1 < **x** < **p**

Tính khóa công khai **y = gx mod p**.

+ Định nghĩa tập khoá: **={(p, g, x, y) : y = gx mod p}.**

+ Các giá trị **p, g, y** được công khai, phải giữ bí mật **x.**

⮚ **Tạo chữ ký**

+ Thông điệp ban đầu **M**

+ Chọn ngẫu nhiên số **k** thỏa mãn điều kiện: 1 < k < p - 1 và gcd(k, p - 1) = 1

+ Tính thành phần thứ nhất: **r = gk mod p**

+ Tính thành phần thứ hai: **s = k-1 \* (H(M) - x \* r) mod (p - 1)**

Trong đó: H(.) là hàm băm

⮚ **Kiểm tra chữ ký**

+ Tính thành phần thứ nhất: u = gH(M) mod p

+ Tính thành phần thứ hai: yr \* rs mod p

+ Kiểm tra: Nếu (u = v) thì chữ ký (r, s) là hợp lệ, ngược lại là giả mạo.

### 2.2.2. Ví dụ

Chữ ký ElGamal trên dữ liệu **H(M) = 112**

**a, Tạo các tham số và khóa**

o Chọn số nguyên tố p = 463

o Chọn phần tử nguyên thủy **g = 2 ϵ Zp\*.**

o Chọn khoá bí mật là **x** = 211 **ϵ Zp\***.

o Tính khóa công khai **y = gx mod p =** 2211 mod 463

Áp dụng thuật toán bình phương và nhân ta có:

+ a = 2, b= 211, n= 463

+ Đổi b=211 sang số nhị phân ta được b = 211= b7b6b5b4b3b2b1b0=11010011(2)

+ Khởi tạo f = 1;

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| i | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| bi | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 |
| f | 2 | 8 | 64 | 321 | 255 | 205 | 247 | 249 |

**+ Với i = 7 : Có b7 = 1:**

● f = f \* f = 1 \* 1 = 1; f = f mod 463 = 1 mod 463 = 1

● f = f \* a =1 \* 2 = 2; f = f mod 463 = 2 mod 463 =2

**+ Với i = 6 : Có b6 = 1:**

● f = f \* f = 2\*2 = 4; f = f mod 463 = 4 mod 463 = 4

● f = f \* a = 4 \*2 = 8; f = f mod 463 = 8 mod 463 = 8

**+ Với i = 5 : Có b5 = 0:**

● f = f \* f = 8 \* 8 = 64; f = f mod 463 = 64 mod 463 = 64

**+ Với i = 4 : Có b4 = 1:**

● f = f \* f = 64\*64 = 4096; f = f mod 463 = 4096 mod 463 = 392

● f = f \* a =392\*2 = 784; f =f mod 463 = 784 mod 463 = 321

**+ Với i = 3 : Có b3 = 0:**

● f = f \* f = 321\*321 = 103041; f = f mod 463 = 103041 mod 463 = 255

**+ Với i = 2 : Có b2 = 0:**

● f = f \* f = 255\*255 = 65025; f = f mod 463 = 65025 mod 463 = 205

**+ Với i = 1 : Có b1 = 1:**

● f = f \* f = 205\*205 = 42025; f = f mod 463 = 42025 mod 463 = 355

● f = f \* a =355\*2 = 710; f =f mod 463 = 710 mod 463 = 247

**+ Với i = 0 : Có b0 = 1:**

● f = f \* f = 355\*355 = 126025; f = f mod 463 = 126025 mod 463 = 356

● f = f \* a = 356 \* 2 = 712; f = f mod 463 = 712 mod 463 = 249

**Vậy y = 2211 mod 463 = 249**

o Định nghĩa tập khoá: **={(p, g, x, y) : y = gx mod p}.**

o Các giá trị **p**, **g, y** được công khai, phải giữ bí mật **x.**

**b, Tạo chữ ký:**

+ Chọn **k** = 235 **ϵ Zp-1\*** và gcd**( k, p-1) =** gcd(235, 462) **=** 1

+ **Tính thành phần thứ nhất:** r = gk mod p = 2235 mod 463

Áp dụng thuật toán bình phương và nhân ta có:

+ a = 2, b = 235, n = 463

+ Đổi b = 235 sang số nhị phân ta được b = 235 = b7b6b5b4b3b2b1b0=11101011(2)

+ Khởi tạo f = 1

Ta lập bảng để tính các bước theo giá trị các bit nhị phân của 235

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| i | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| b | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 |
| f | 2 | 8 | 128 | 179 | 188 | 156 | 57 | 16 |

**+ Với i = 7 : Có b7 = 1:**

● f = f \* f = 1\*1 = 1; f = f mod 463 = 1 mod 463 = 1

● f = f \* a =1 \*2 = 2; f =f mod 463 = 2 mod 463 =2

**+ Với i = 6 : Có b6 = 1:**

● f = f \* f = 2\*2 = 4; f = f mod 463 = 4 mod 463 = 4

● f = f \* a =4 \*2 = 8; f =f mod 463 = 8 mod 463 = 8

**+ Với i = 5 : Có b5 = 1:**

● f = f \* f = 8\*8 = 64; f = f mod 463 = 64 mod 463 = 64

● f = f \* a =64 \*2= 128; f = f mod 463 = 128 mod 463 = 128

**+ Với i = 4 : Có b4 = 0:**

● f = f\*f = 128\*128 = 16384; f = f mod 463 = 16384 mod 463 = 179

**+ Với i = 3 : Có b3 = 1:**

● f = f \* f = 179\*179 = 32041; f = f mod 463 = 32041 mod 463 = 94

● f = f \* a =94 \*2= 188; f =f mod 463 = 188 mod 463 = 188

**+ Với i = 2 : Có b2 = 0:**

● f = f \* f = 188\*188 = 35344; f = f mod 463 = 35344 mod 463 = 156

**+ Với i = 1 : Có b1 = 1:**

● f = f \* f = 156\*156 = 24336; f = f mod 463 = 24336 mod 463 = 260

● f = f \* a =260\*2 = 520; f = f mod 463 = 520 mod 463 = 57

**+ Với i = 0 : Có b0 = 1:**

● f = f \* f = 57\*57 = 3249; f = f mod 463 = 3249 mod 463 = 8

● f = f \* a =8\*2 = 16; f = f mod 463 = 16 mod 463 = 16

**Vậy r = 2235 mod 463 = 16**

**+ Tính thành phần thứ hai:** s = k-1 \* (H(M) - x \* r) mod (p - 1)

Tìm k-1 mod (p-1) = 235-1 mod 462

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Dòng | r0 | r1 | r2 | q | t0 | t1 |
| 0 | 462 | 235 | 227 | 1 | 0 | 1 |
| 1 | 235 | 227 | 8 | 1 | 1 | 461 |
| 2 | 227 | 8 | 3 | 28 | 461 | 2 |
| 3 | 8 | 3 | 2 | 2 | 2 | 405 |
| 4 | 3 | 2 | 1 | 1 | 405 | 116 |
| 5 | 2 | 1 | 0 | 2 | 116 | 289 |

**Dòng 0:**

+ r0 = 462, r1 = 235

+ r2  = r0  % r1 = 462 % 235 = 227

+ q = r0 / r1 = 462 / 235 = 1

+ t0 = 0, t1 = 1

**Dòng 1:**

+ r0 = 235, r1 = 227

+ r2  = r0  % r1 = 235 % 227 = 8

+ q = r0 / r1 = 235 / 227 = 1

+ t0 = 1

+ t1 = t0  - q \* t1 mod n = 0 - 1 \* 1 mod 462 = 461 (Lấy các giá trí q, t0, t1 ở dòng i - 1 để tính)

**Bước i = 2:**

+ r0 = 227, r1 = 8

+ r2  = r0  % r1 = 227 % 8 = 3

+ q = r0 / r1 = 227 / 8 = 28

+ t0 = 461

+ t1 = t0  - q \* t1 mod n = 1 - 1 \* 461 mod 462 = 2 (Lấy các giá trí q, t0, t1 ở dòng i - 1 để tính)

**Bước i = 3:**

+ r0 = 8, r1 = 3

+ r2  = r0  % r1 = 8 % 3 = 2

+ q = r0 / r1 = 8 / 3 = 2

+ t0 = 2

+ t1 = t0  - q \* t1 mod n = 461 - 28 \* 2mod 462 = 405 (Lấy các giá trí q, t0, t1 ở dòng i - 1 để tính)

**Bước i = 4:**

+ r0 = 3, r1 = 2

+ r2  = r0  % r1 = 3 % 2 = 1

+ q = r0 / r1 = 3 / 2 = 1

+ t0 = 405

+ t1 = t0  - q \* t1 mod n = 2 - 2 \* 405 mod 462 = 116 (Lấy các giá trí q, t0, t1 ở dòng i - 1 để tính)

**Bước i = 5:**

+ r0 = 2, r1 = 1

+ r2  = r0  % r1 = 2 % 1 = 0

+ q = r0 / r1 = 2 / 1 = 2

+ t0 = 116

+ t1 = t0  - q \* t1 mod n = 405 - 1 \* 116 mod 462 = 289 (Lấy các giá trí q, t0, t1 ở dòng i - 1 để tính)

Vậy 235-1 mod 462 = 289

**s** = k-1 \* (H(M) - x \* r) mod (p-1) **=** 289 **\*** (112 - 211 \* 16) mod 462 =108

**c, Kiểm tra chữ ký:**

**u** = gH(M) mod p **=** 2112 mod 463 =132

**v** = **yr \* rs =** 24916 \*16108 mod 463 = 132

**u = v =>** chữ ký là đúng.

### 2.2.3. Độ an toàn

Độ an toàn của chữ ký điện tử Elgamal dựa vào độ an toàn của hệ mật Elgamal.

Độ an toàn của hệ mật Elgamal: dựa vào tính khó giải của các bài toán logarit rời rạc.

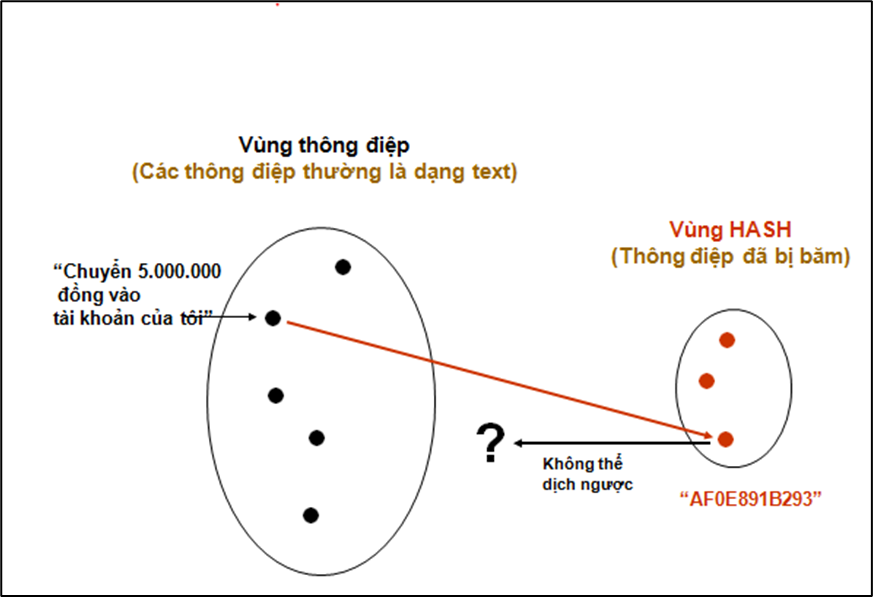
• Bài toán logarit rời rạc: để tính được X, hoặc k, kẻ tấn công cần phải giải một trong hai bài toán logarit rời rạc: YA = ax mod q hoặc C1 = ak mod q. Trong lý thuyết mã hóa, bài toán logarit rời rạc là bài toán khó, đây là bài toán không giải được trong thời gian đa thức.

## **2.3. Hàm băm**

### 2.3.1. Giới thiệu hàm băm Hash

Hàm băm (Hash function) là một hàm toán học chuyển đổi một thông điệp đầu vào có độ dài bất kỳ 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 (hash function) là hàm một chiều mà nếu đưa một lượng dữ liệu bất kì qua hàm này sẽ cho ra một chuỗi có độ dài cố định ở đầu ra.



*Hình 3. Ví dụ hàm băm hash*

**Mã hóa SHA là gì?**

Mã hóa SHA có tên đầy đủ là Secure Hash Algorithm hay còn gọi là thuật giải băm an toàn. Đây là tổ hợp 5 thuật giải băm mật được phát triển bởi NSA (National Security Agency) – Cục An ninh Quốc gia Mỹ và được xuất bản thành chuẩn của chính phủ Mỹ bởi NIST (National Institute of Standards and Technology) – Viện Công nghệ và chuẩn quốc gia Mỹ.

Thuật giải SHA đã được chấp nhận bởi FIPS (Federal Information Processing Standards) – Tiêu chuẩn Xử lý Thông tin Liên bang. Mã hóa SHA được dùng để chuyển đổi từ một đoạn dữ liệu nhất định thành một đoạn dữ liệu có chiều dài không đổi nhưng với xác suất khác biệt cao.

Năm thuật giải SHA chuẩn bao gồm:

SHA-1: Trả lại kết quả dài 160 bit

SHA-224: Trả lại kết quả dài 224 bit

SHA-256: Trả lại kết quả dài 256 bit

SHA-384: Trả lại kết quả dài 384 bit

SHA-512: Trả lại kết quả dài 512 bit

### 2.3.2. Tính chất cơ bản của hàm băm Hash

✔ **Tính một chiều:** không thể suy ra dữ liệu ban đầu từ kết quả, điều này tương tự như việc bạn không thể chỉ dựa vào một dấu vân tay lạ mà suy ra ai là chủ của nó được.

✔ **Tính duy nhất**: xác suất để có một vụ va chạm (hash collision), tức là hai thông điệp khác nhau có cùng một kết quả hash là cực kỳ nhỏ.

### 2.3.3. Một số hàm băm thông dụng

MD5 (Message Digest 5 - 128 bit)

SHA-1 (Secure Hash Algorithm 1 - 160 bit)

SHA-256 (Secure Hash Algorithm 256 bit)

SHA-512 (Secure Hash Algorithm 512 bit)

RIPEMD-160 (RACE Integrity primitives Evaluation Message Digest 160 bit)

Trong đó hàm SHA-1 là một trong những hàm được sử dụng rộng rãi nhất ở Việt Nam.

### 2.3.4. Ứng dụng của hàm băm Hash

⮚ **Xác thực mật khẩu**

Mật khẩu thường không được lưu dưới dạng văn bản rõ (clear text), mà ở dạng tóm tắt. Để xác thực một người dùng, mật khẩu do người đó nhập vào được băm ra bằng hàm Hash và so sánh với kết quả băm được lưu trữ.

⮚ **Xác thực thông điệp (Message authentication – Thông điệp tóm tắt - message digests)**

Giá trị đầu vào (tin nhắn, dữ liệu...) bị thay đổi tương ứng giá trị băm cũng bị thay đổi. Do vậy nếu một kẻ tấn công phá hoại, chỉnh sửa dữ liệu thì server có thể biết ngay lập tức.

⮚ **Bảo vệ tính toàn vẹn của tập tin, thông điệp được gửi qua mạng**

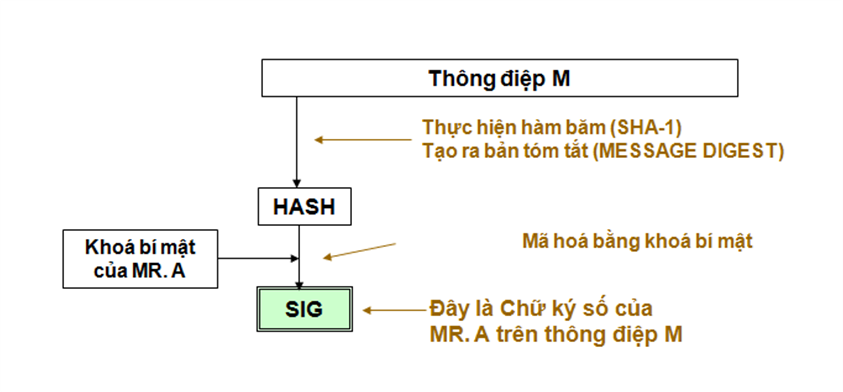
Hàm băm mật mã có tính chất là hàm 1 chiều. Từ khối dữ liệu hay giá trị đầu vào chỉ có thể đưa ra 1 giá trị băm duy nhất. Như chúng ta đã biết đối với tính chất của hàm 1 chiều. Một người nào đó dù bắt được giá trị băm họ cũng không thể suy ngược lại giá trị, đoạn tin nhắn băm khởi điểm.

Ví dụ: việc xác định xem một file hay một thông điệp có bị sửa đổi hay không có thể thực hiện bằng cách so sánh tóm tắt được tính trước và sau khi gửi (hoặc một sự kiện bất kỳ nào đó). Còn có thể dùng tóm tắt thông điệp làm một phương tiện đáng tin cậy cho việc nhận dạng file.

Hàm băm thường được dùng trong [bảng băm](http://vi.wikipedia.org/w/index.php?title=B%E1%BA%A3ng_b%C4%83m&action=edit&redlink=1) nhằm giảm chi phí tính toán khi tìm một khối dữ liệu trong một tập hợp. Giá trị băm đóng vai trò gần như một khóa để phân biệt các khối dữ liệu.

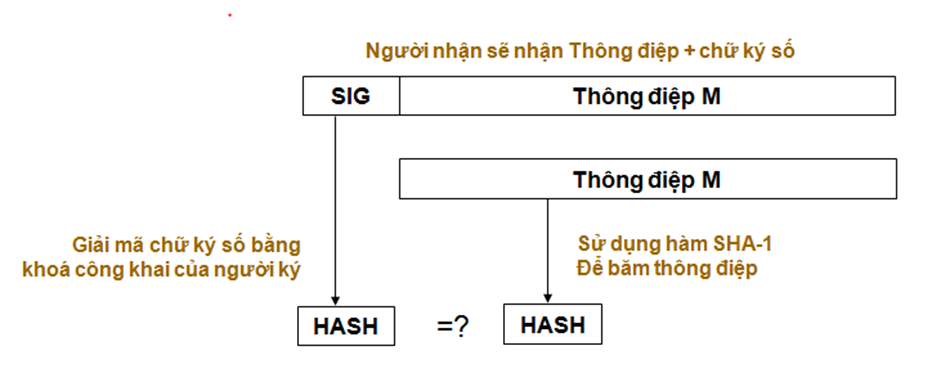
⮚ **Tạo chữ ký điện tử (Digital signatures)**

**Chữ ký số có được bằng cách đem mã hoá bản tóm tắt của thông điệp bằng khóa bí mật của người ký**

****

*Hình 4. Mã hóa thông điệp bằng khóa bí mật của người ký*

**Chứng thực bằng chữ ký số**

******

*Hình 5. Chứng thực chữ ký số*

Nếu kết quả băm giống nhau, Thông điệp được xác thực.

Tại sao? Vì nếu bất kỳ BIT nào của M hay SIG bị thay đổi, kết quả băm sẽ khác

⇨ **Đây là một ứng dụng cực kỳ quan trọng của hàm Hash, đặc biệt là trong thương mại điện tử.**

### 2.3.5. Thuật toán hàm băm SHA-1

#### **2.3.5.1.** **Giới thiệu hàm băm SHA-1**

Năm 1990, Ron Rivest đã sáng tạo ra hàm băm MD4. Sau đó năm 1992, ông cải tiến MD4 và phát triển một hàm băm khác: MD5. Năm 1993, Cơ quan An ninh Quốc gia Hoa Kỳ/Cục An ninh Trung ương (NSA) đã công bố,một hàm băm rất giống với MD5 được gọi là SHA. Vào năm 1995, sau việc khắc phục những lỗ hổng kỹ thuật, NSA đã thay đổi SHA trở thành một hàm băm mật mã khác gọi là SHA-1.

SHA-1 (Secure Hash Algorithm) là thuật toán cũng được xây dựng trên thuật toán MD4, đang được sử dụng rộng rãi. Thuật toán SHA-1 tạo ra chuỗi mã băm có chiều dài cố định 160 bit từ chuỗi bit dữ liệu đầu vào x có chiều dài tùy ý.

#### **2.3.5.2.** **Thuật toán SHA-1**

I**nput**: thông điệp với độ dài tối đa 2^64 bits

**Output**: thông điệp rút gọn (message digest) có độ dài 160 bits

Giải thuật gồm 5 bước trên khối 512 bits

***Bước 1: Nhồi dữ liệu***

* Thông điệp được nhồi thêm các bit sao cho độ dài L mod 512 luôn đồng dư là 448.
* Thông điệp luôn luôn được nhồi thêm các bit.
* Số bit nhồi thêm phải nằm trong khoảng 1-512.
* Phần thêm vào cuối dữ liệu gồm 1 bit 1 và theo sau là các bit 0.

***Bước 2: Thêm độ dài****:*

* Độ dài khối dữ liệu ban đầu sẽ được biểu diễn dưới dạng nhị phân 64 bit và được thêm cuối chuỗi nhị phân mà ta thu được ở bước 1.
* Độ dài được biểu diễn dưới dạng nhị phân 64 bit không dấu
* Kết quả thu được từ 2 bước là một khối dữ liệu có độ dài là bội số của 512. (Với cứ 512 bit là một khối dữ liệu)

***Bước 3: Khởi tạo bộ đệm MD (MD buffer)***

Một bộ đệm 160 bit được dùng để lưu trữ các giá trị băm trung gian và kết quả. Bộ đệm được biểu diễn bằng 5 thanh ghi 32-bit với các giá trị khởi tạo ở dạng big-endian (byte có trọng số lớn nhất trong từ nằm ở địa chỉ thấp nhất) và có 2 bộ đệm. 5 thanh ghi của bộ đệm đầu tiên được đánh đặt tên là A, B,C,D,E và tương tự cho bộ đệm thứ 2 là H0, H1, H2, H3, H4. Có giá trị như sau (Theo dạng Hex):

H0=67452301

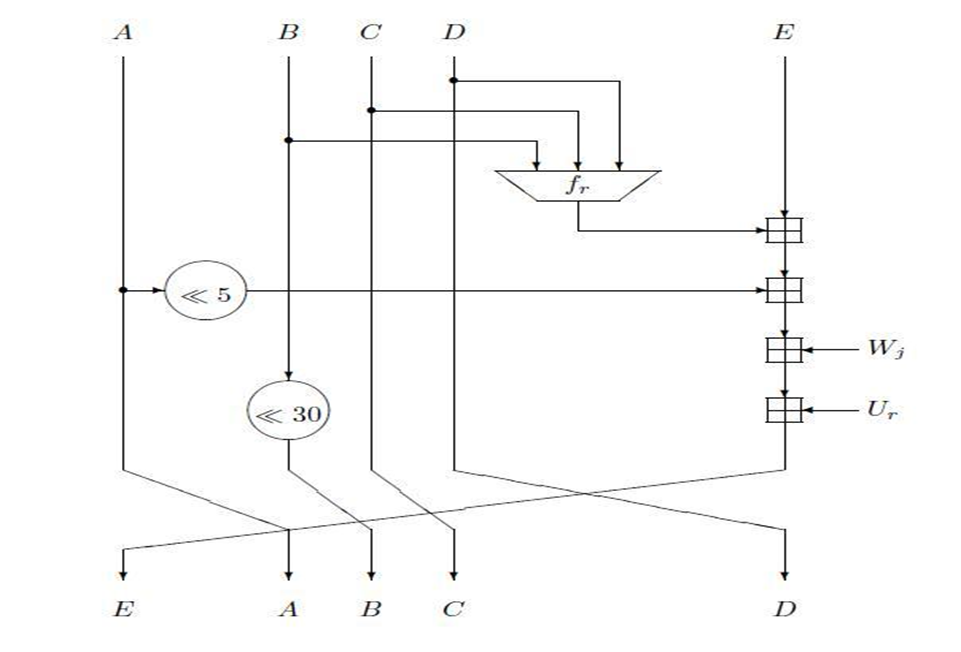
H1= EFCDAB89

H2= 98BADCFE

H3= 10325476

H4= C3D2E1F0

***Bước 4: Xử lý các khối dữ liệu 512 bit***

******

*Hình 6. Sơ đồ thuật toán SHA-1*

* Trọng tâm của giải thuật bao gồm 4 vòng lặp thực hiện tất cả 80 bước.
* 4 vòng lặp có cấu trúc như nhau, chỉ khác nhau ở hàm logic Ft.

|  |  |  |
| --- | --- | --- |
| **Bước** | **Hàm** | **Giá trị** |
| (0≤ t ≤ 19) | Ft=F(B, C,D) | (B AND C) OR ( (NOT B) AND D) |
| (20≤ t ≤ 39) | Ft=F(B, C,D) | B XOR C XOR D |
| (40≤ t ≤ 59) | Ft=F(B, C,D) | (B AND C) OR (B AND D) OR (C AND D) |
| (60≤ t ≤ 79) | Ft=F(B, C,D) | B XOR C XOR D |

* Mỗi vòng có đầu vào gồm khối 512-bit hiện thời và một bộ đệm 160 bit A, C, B, D, E. Các thao tác sẽ cập nhật giá trị bộ đệm.
* Chia khối dữ liệu đã nhồi thêm (cuối bước 2) thành 16 nhóm (mỗi nhóm gồm 32 bit) và đặt theo thứ tự là: W1,W0 ,....,W15
* Mở rộng từ 16 nhóm 32 bit lên đến 80 nhóm 32 bit bằng vòng lặp
* For 16 to 79 let
* Wt= S1(Wt-3 XOR Wt-8 XOR Wt-14 XOR Wt-16)
* Gán A=H0, B=H1, C=H2, D=H3, E=H4.
* Mỗi vòng lặp sử dụng theo công thức chung với 1 hằng số Kt = (0≤ t ≤ 79) như sau:

For t= 0 to 79 do

TEMP= S5(A)+Ft(B,C,D)+ E + Wt + Kt

E=D; D=C; C= S30(B); B=A; A= TEMP

Với:

Kt= 5A827999 (0≤ t ≤ 19)

Kt= 6ED9EBA1(20≤ t ≤ 39)

Kt= 8F1BBCDC(40≤ t ≤ 59)

Kt= CA62C1D6(60≤ t ≤ 79) .

* Đầu ra của 4 vòng (bước 80) được cộng với giá trị của bộ đệm để tạo ra 1 chuỗi kết quả dài 160 bit.

H0 =H0 + A

H1 =H1 + B

H2 =H2 + C

H3 =H3 + D

H4 =H4 + E

**Bước 5: Xuất kết quả**

Sau khi thao tác trên toàn bộ N khối dữ liệu (blocks). Kết quả của khối thứ N là chuỗi băm 160 bit.

H=H0H1H2H3H4

## **2.4. Mã hóa bất đối xứng**

### 2.4.1. Giới thiệu

Mã hóa bất đối xứng là một phương pháp mã hóa mà trong đó sử dụng hai khóa: một khóa dùng để mã hóa và một khóa khác dùng để giải mã. Sự khác biệt chính giữa hai khóa này là khóa dùng để mã hóa có thể công khai, tức là ai cũng có thể biết, trong khi khóa dùng để giải mã là bí mật và chỉ được người nhận thông điệp giữ.

### 2.4.2. Nguyên lý hoạt động

Thuật toán mã hóa bất đối xứng sử dụng một hàm toán học phức tạp mà khó có thể giải ngược nếu không biết khóa giải mã. Một trong những thuật toán mã hóa bất đối xứng phổ biến nhất là RSA, được tạo ra bởi Ronald Rivest, Adi Shamir và Leonard Adleman.

1. **Sinh khóa:**
   * Chọn hai số nguyên tố lớn p và q.
   * Tính n = p \* q, là phần tử của khóa công khai và khóa bí mật.
   * Tính hàm Euler của n: φ(n) = (p - 1) \* (q - 1).
   * Chọn một số nguyên e sao cho 1 < e < φ(n) và gcd(e, φ(n)) = 1. e là phần tử công khai.
   * Tính d sao cho (d \* e) mod φ(n) = 1. d là phần tử bí mật.
2. **Mã hóa:**
   * Mã hóa một thông điệp M thành một số nguyên c, với công thức: c = M^e mod n.
   * Số c chính là thông điệp đã được mã hóa.
3. **Giải mã:**
   * Giải mã số c thành thông điệp M, với công thức: M = c^d mod n.
   * Số M chính là thông điệp gốc.

### 2.4.3. Ưu Điểm và Ứng Dụng

Mã hóa bất đối xứng có một số ưu điểm quan trọng:

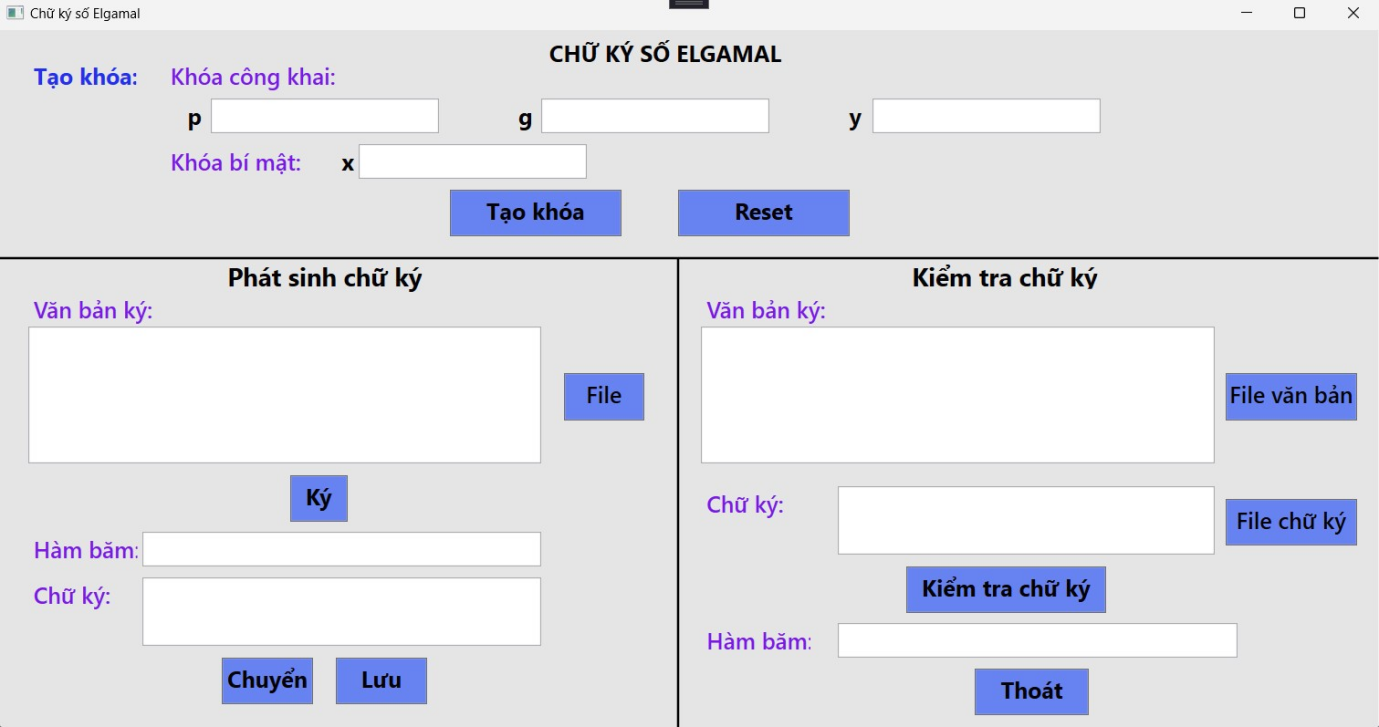
* **An Toàn:** Việc giải mã một thông điệp mà không có khóa bí mật là rất khó, dựa trên tính phức tạp của các hàm toán học được sử dụng.
* **Khóa Công Khai:** Khóa công khai có thể được chia sẻ một cách an toàn và dễ dàng với nhiều người.

Ứng dụng của mã hóa bất đối xứng bao gồm:

* **Bảo Mật Dữ Liệu:** Mã hóa bất đối xứng được sử dụng rộng rãi trong việc bảo vệ dữ liệu trên internet, bao gồm việc mã hóa thông tin cá nhân và thanh toán trực tuyến.
* **Ký Số Điện Tử:** Nó cũng được sử dụng để tạo chữ ký số điện tử, cho phép xác thực dữ liệu mà không cần tiết lộ khóa bí mật.

## **2.5. Thiết kế, cài đặt chương trình**

### 2.5.1. Chương trình C#



*Hình 7. Giao diện chương trình C#*

*Thực hiện tạo chữ ký :*

**Cách 1:** Tạo khóa tự động

**Bước 1:** Kích vào “Tạo Khóa”, chương trình sẽ tự động sinh ra số p ,g , x, y

**Cách 2**: Nhập từ bàn phím :

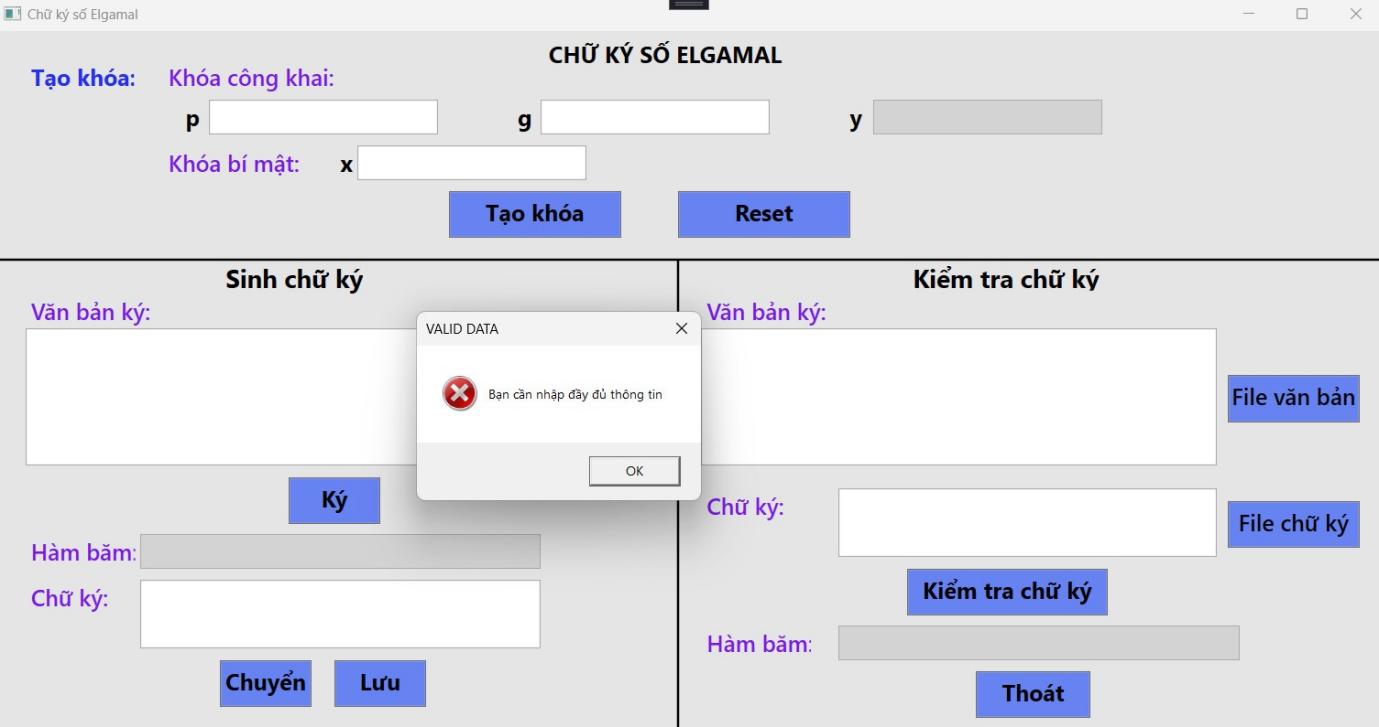
Nhập thông số nguyên tố p, số a, số alpha, và số k để thực hiện quá trình ký số.

Ở đây thực hiện bắt lỗi nhập liệu :

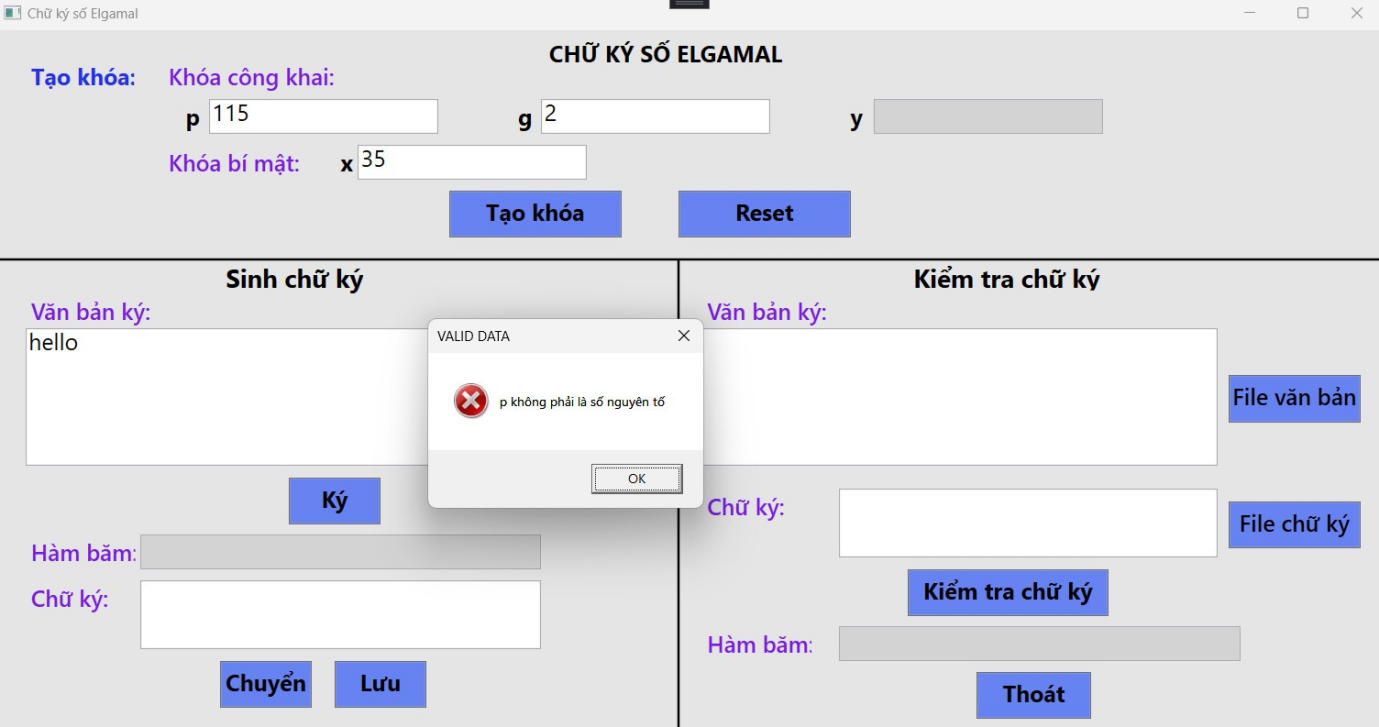
* Chưa nhập đủ thông tin
* Kiểm tra số p đã là số nguyên tố chưa. Hiển thị thông báo p không phải số nguyên tố.

**Hình ảnh minh họa về một số lỗi nhập liệu:**

* Lỗi chưa nhập đủ thông tin



* Lỗi p không phải là số nguyên tố



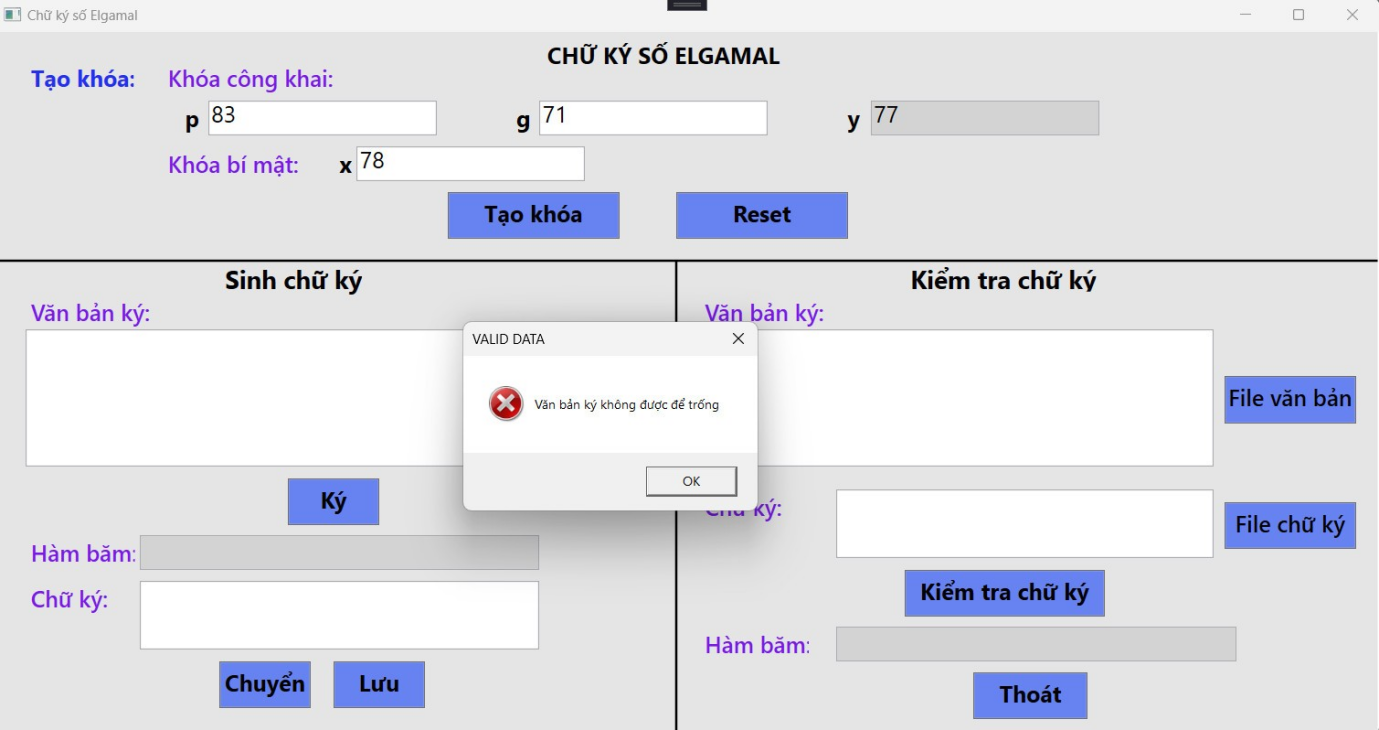
*Thực hiện ký:*

**Bước 2**:

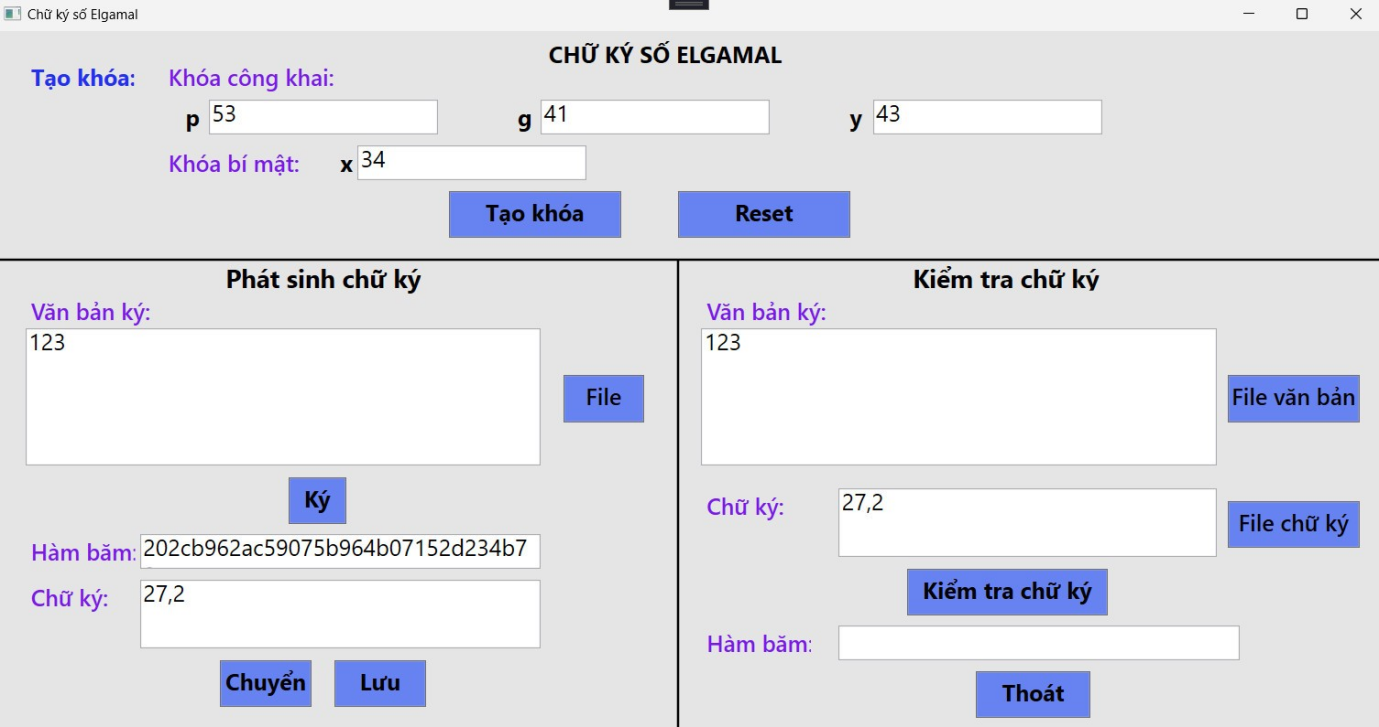
* Chọn file văn bản cần ký hoặc nhập vào ô “Văn bản ký”
* Kích nút “ Ký”
* Sau khi ký xong thì có thể lưu lại chữ ký.

Ở đây thực hiện bắt lỗi nhập liệu :

* Lỗi chưa chọn file



Khi thực hiện ký văn bản thành công, chương trình sẽ hiển thị nội dung của file thực hiện chữ ký, hàm băm, tệp chữ ký và file văn bản được gửi đi như sau:



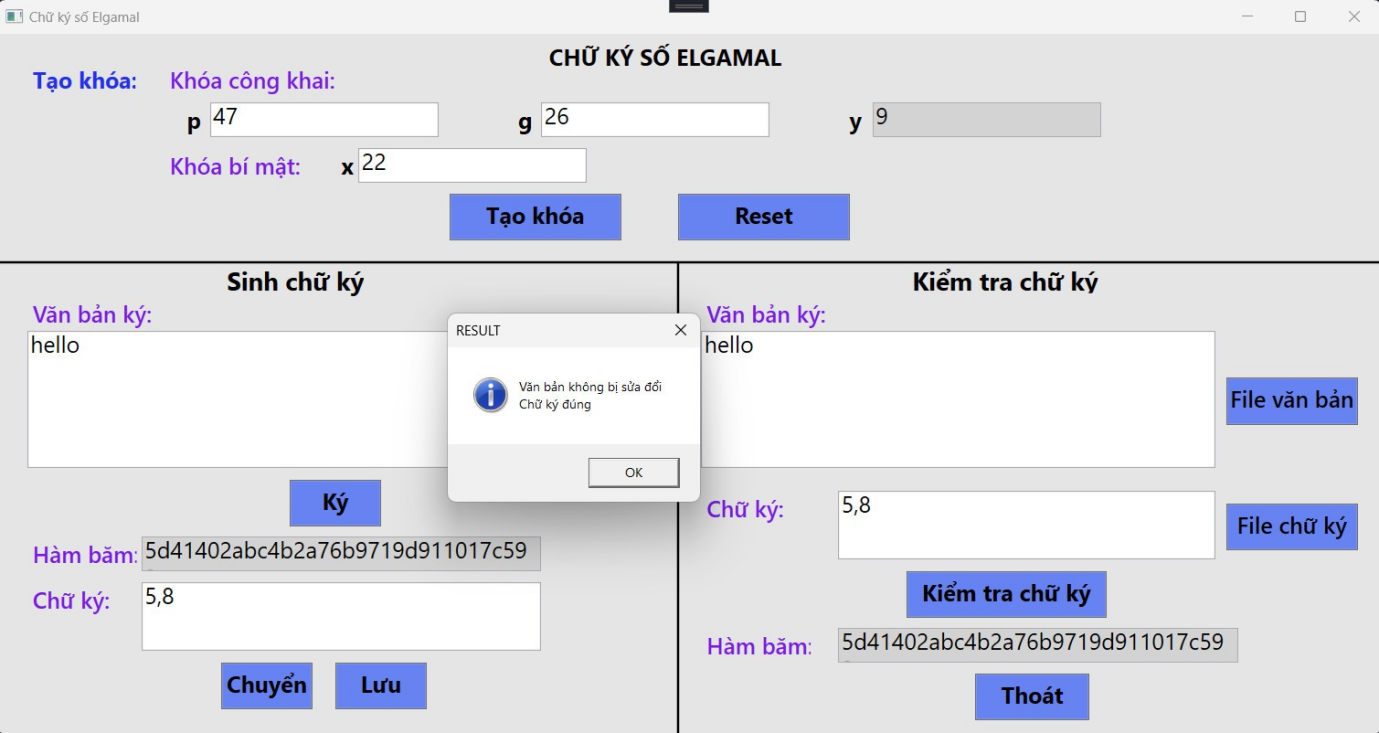
*Kiểm tra chữ ký :*

**Bước 3:**

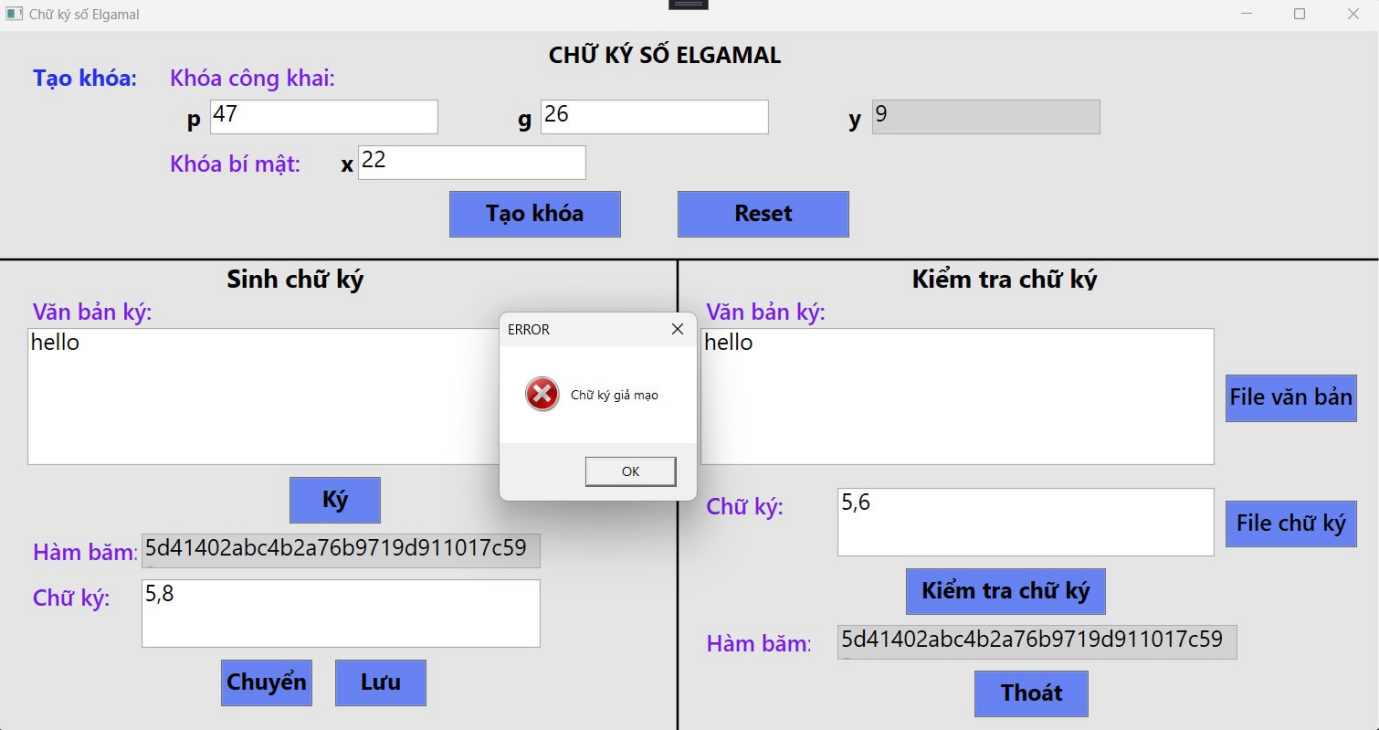
* Chọn file cần kiểm tra chữ ký
* Kích nút kiểm tra chữ ký

*Kết quả*

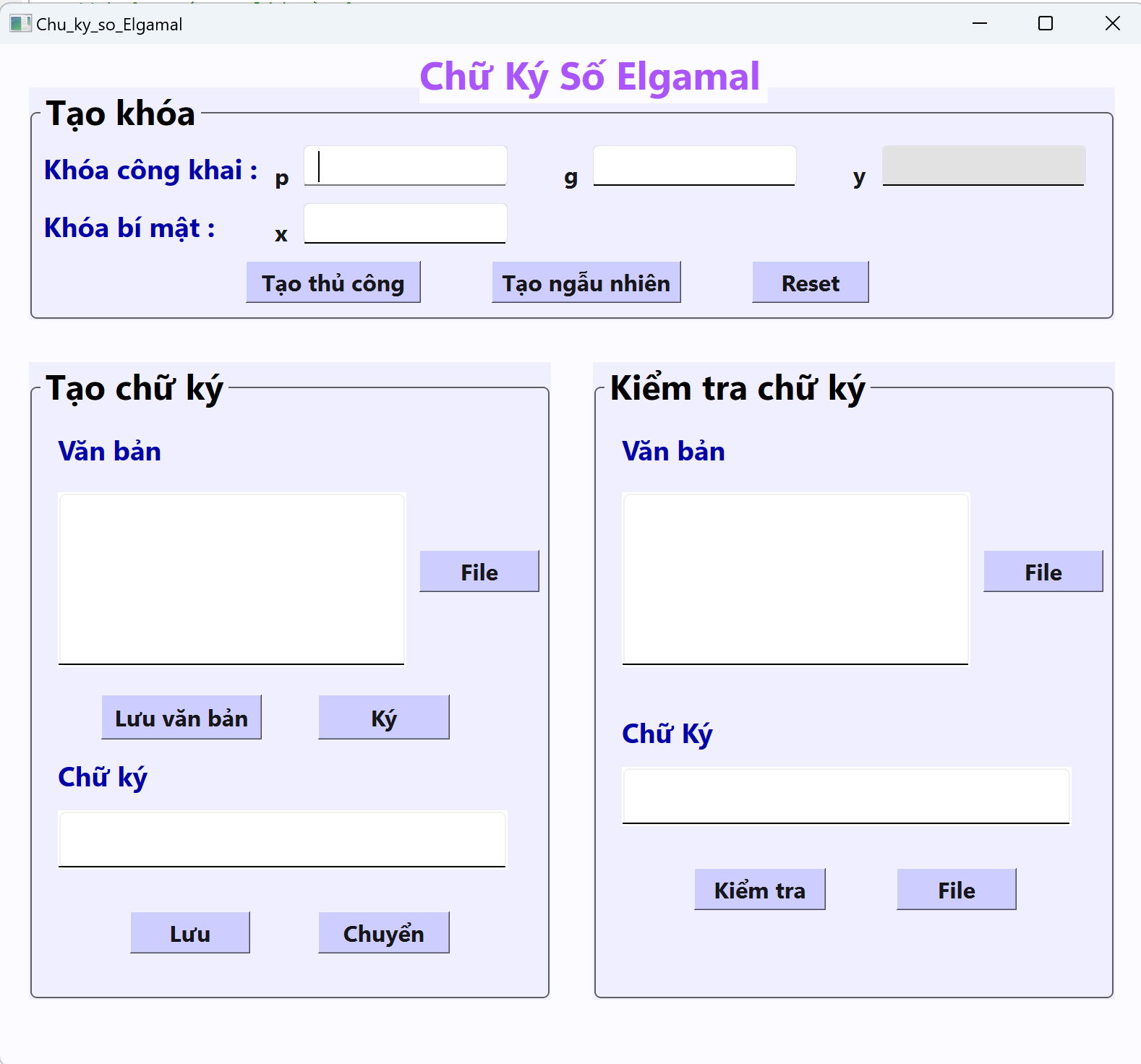
* Nếu tài liệu chưa bị chỉnh sửa



* Nếu tài liệu đã bị chỉnh sửa



### 2.5.2. Chương trình C++



*Hình 8. Giao diện chương trình C++*

*Thực hiện tạo chữ ký :*

**Cách 1:** Tạo khóa tự động

**Bước 1:**

Kích vào “Tạo ngẫu nhiên”, chương trình sẽ tự động sinh ra số p ,g , x, y

**Cách 2**: Nhập từ bàn phím :

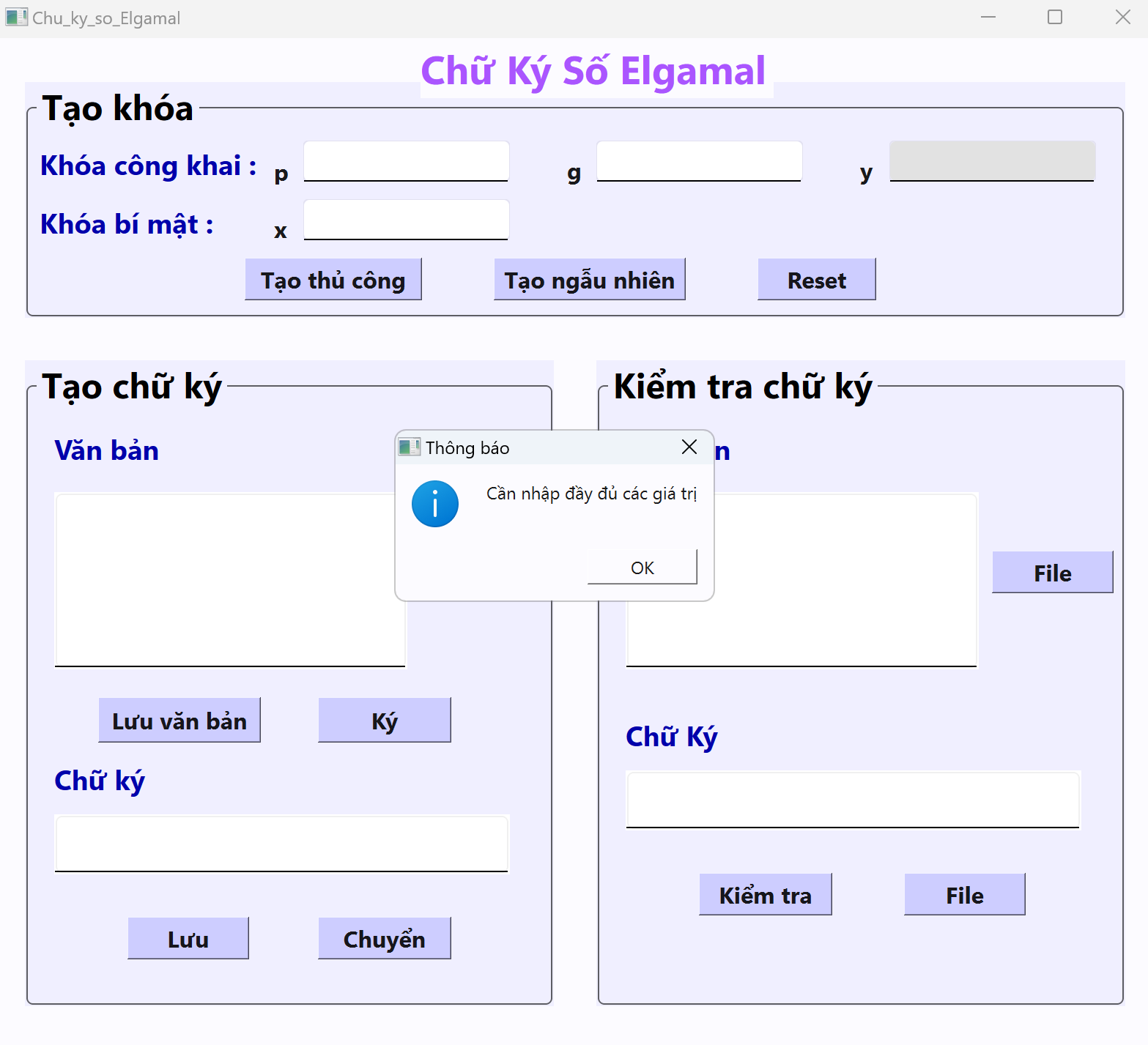
Nhập thông số nguyên tố p , số g , số x để thực hiện quá trình ký số.

Kích vào”Tạo thủ công”

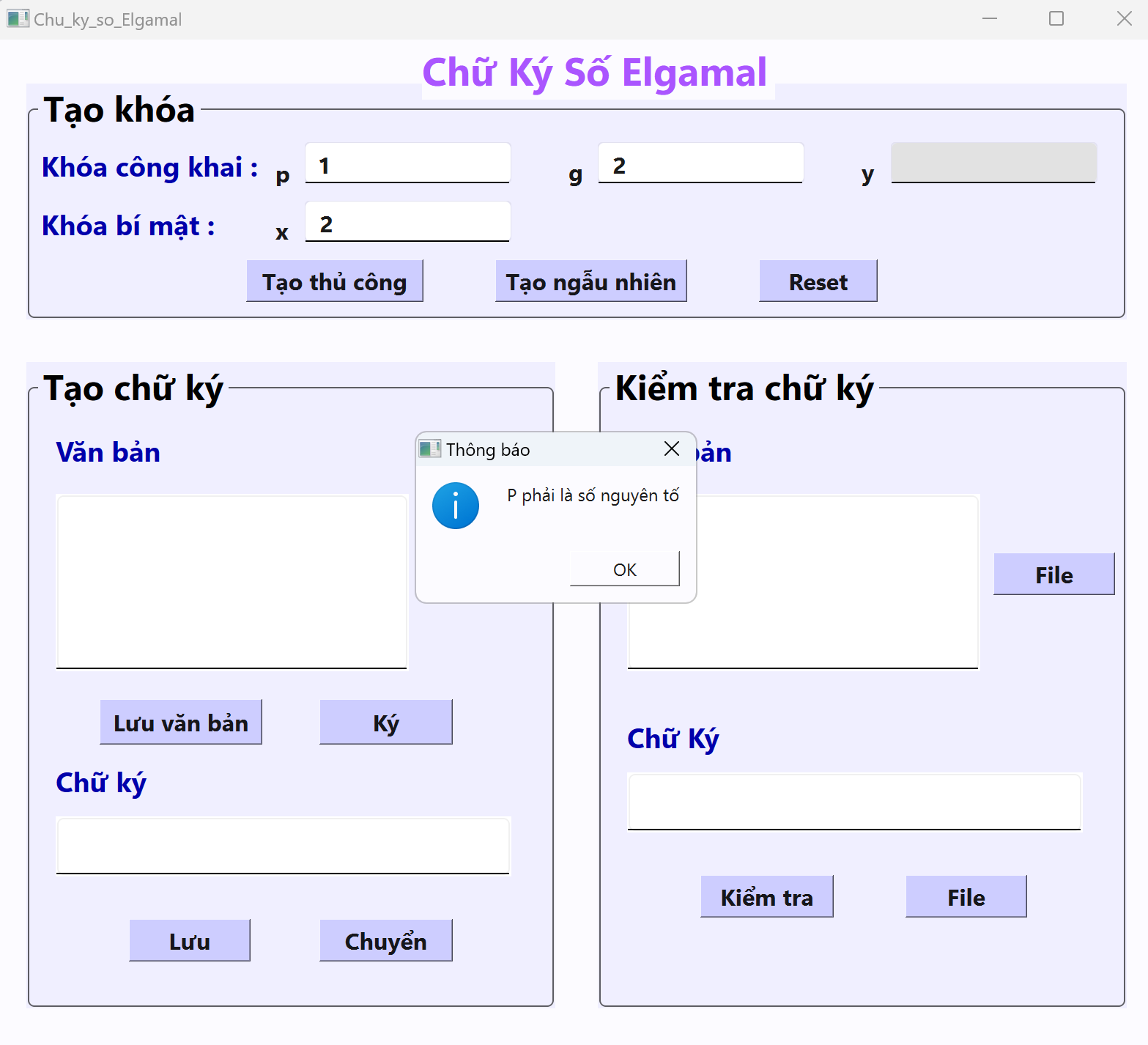
Ở đây thực hiện bắt lỗi nhập liệu :

* Chưa nhập đủ thông tin
* Kiểm tra số p đã là số nguyên tố chưa. Hiển thị thông báo p không phải số nguyên tố.

**Hình ảnh minh họa về một số lỗi nhập liệu:**



-Lỗi p không là số nguyên tố

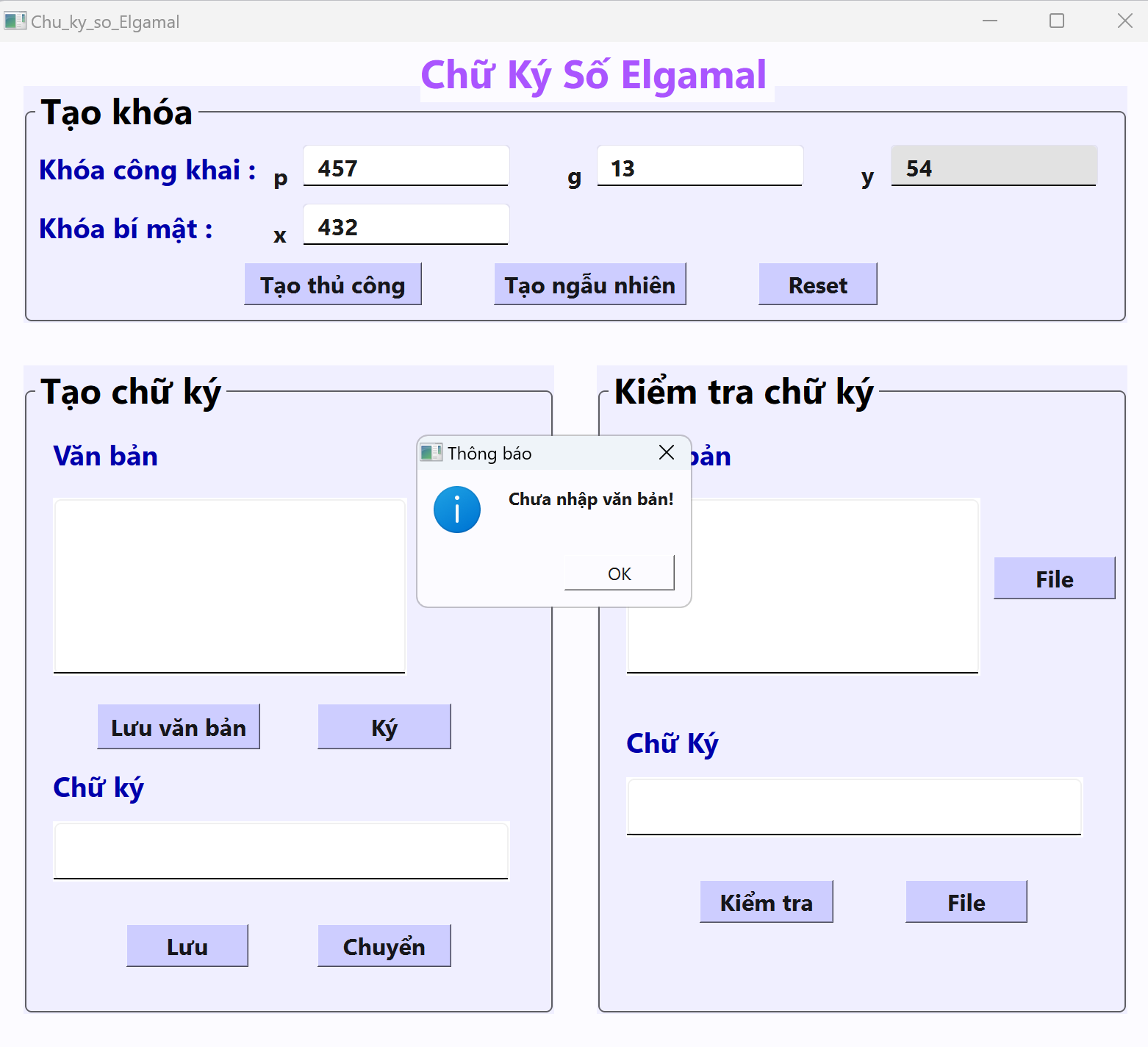


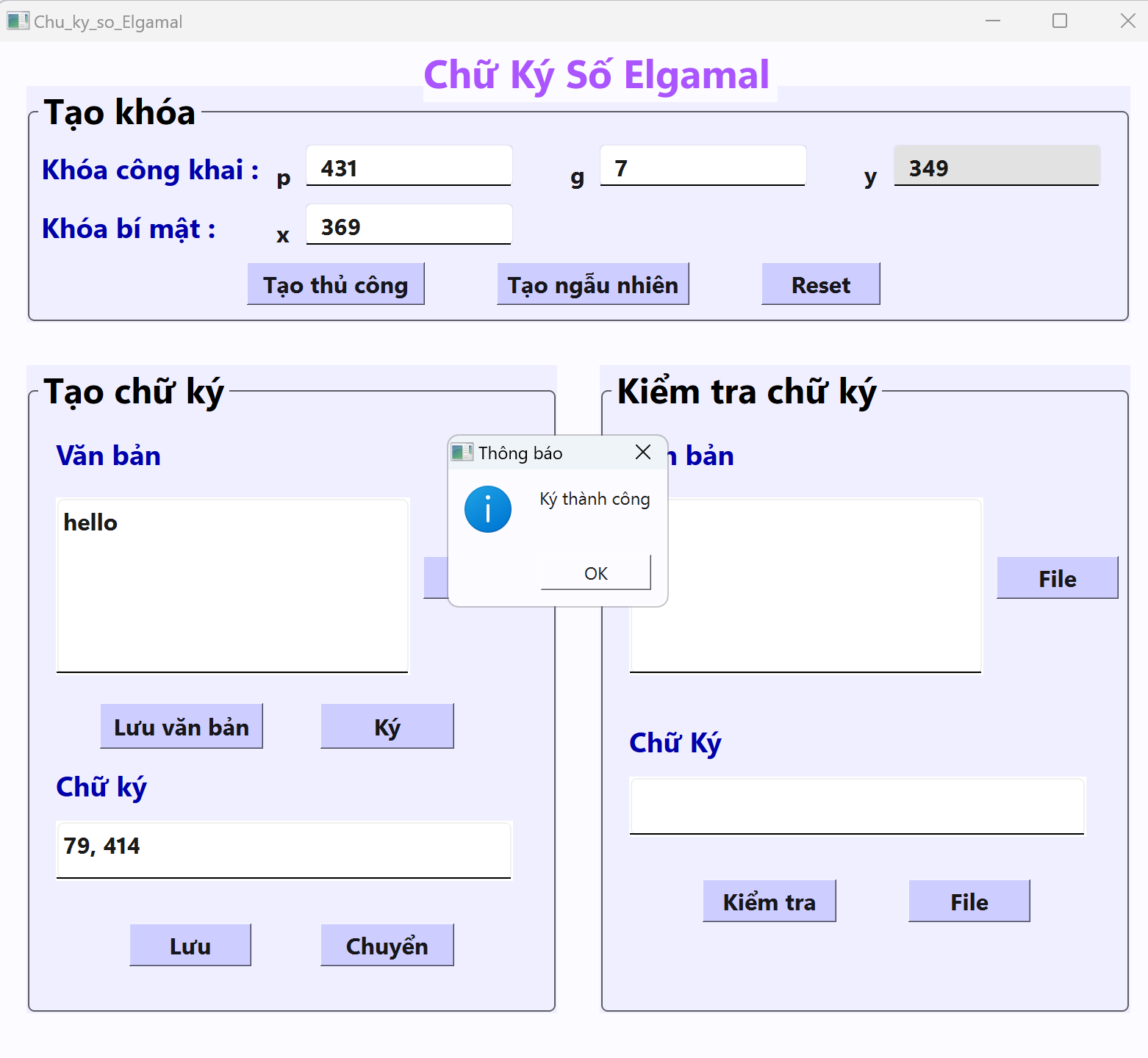
**Bước 2**:

* Chọn file văn bản cần ký hoặc nhập vào ô “Văn bản”
* Kích nút “ Ký”
* Sau khi ký xong thì có thể lưu lại chữ ký.

Ở đây thực hiện bắt lỗi nhập liệu :

* Lỗi chưa chọn file



Khi thực hiện ký văn bản thành công :

Sau đó chương trình sẽ hiển thị nội dung của file thực hiện chữ ký,tệp chữ ký và file văn bản được gửi đi như sau:



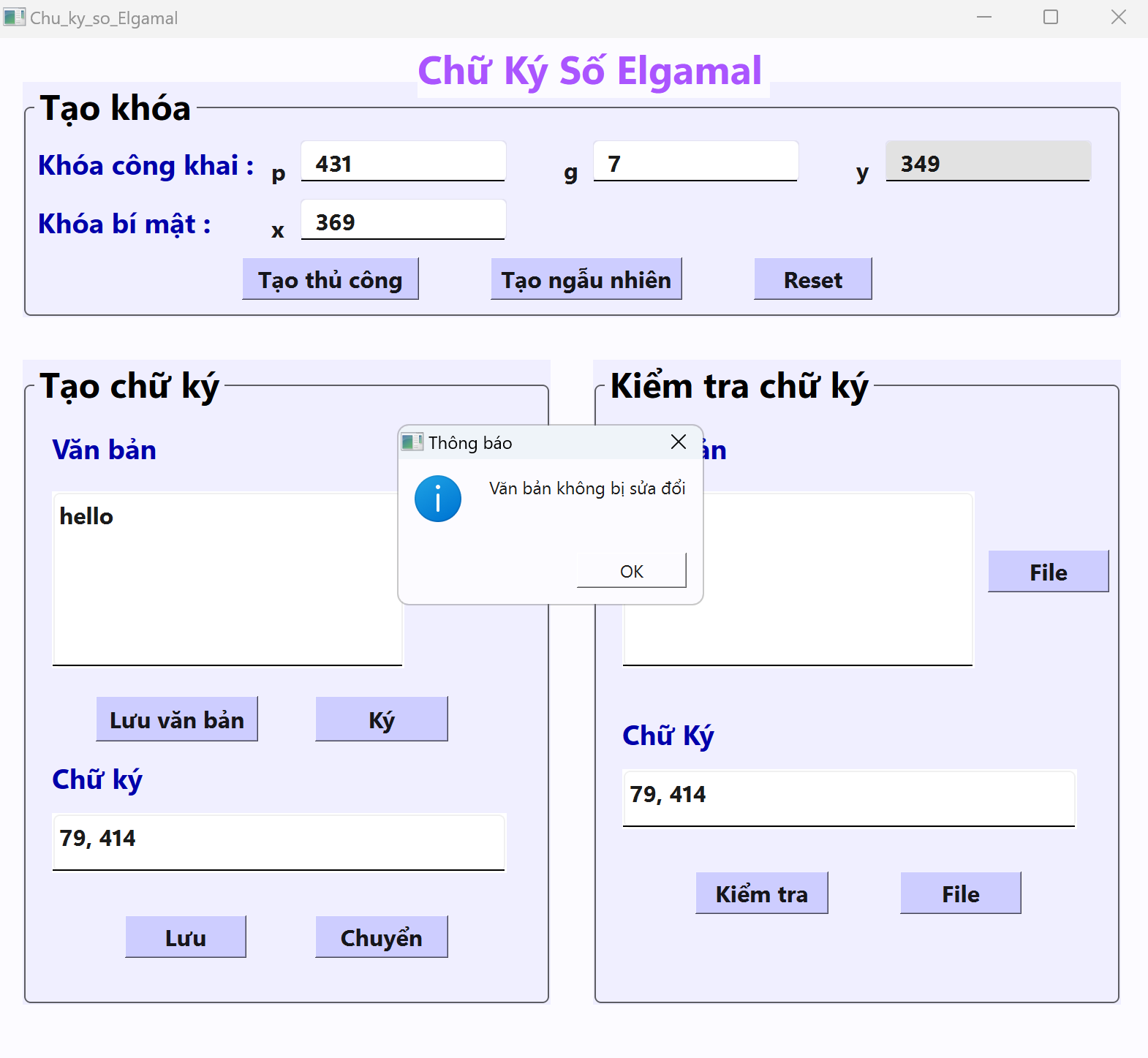
*Kiểm tra chữ ký :*

**Bước 3:**

* Chọn file cần kiểm tra chữ ký
* Kích nút kiểm tra chữ ký

*Kết quả*

* Nếu tài liệu chưa bị chỉnh sửa

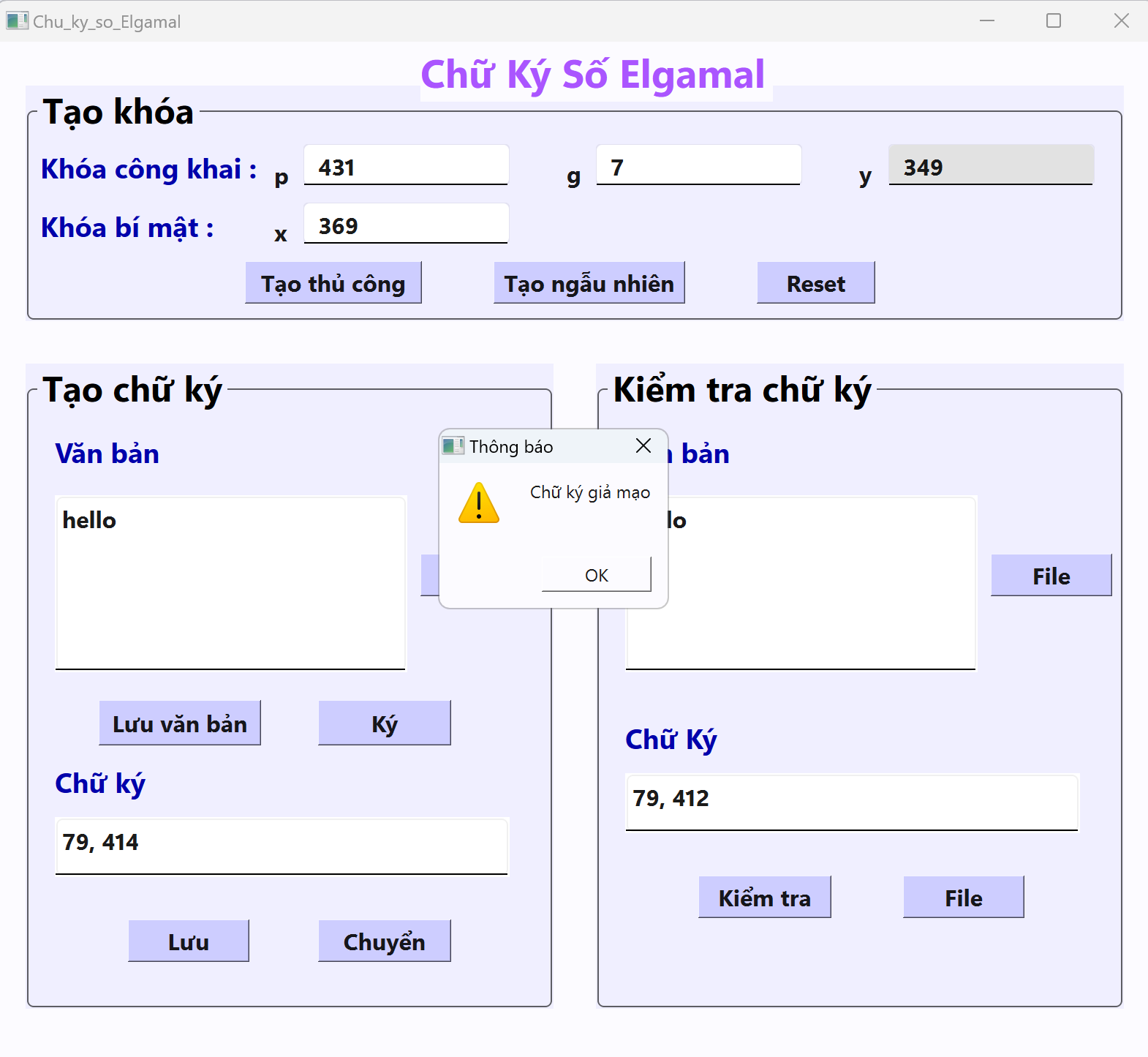


* Nếu tài liệu đã bị chỉnh sửa



Ở đây thực hiện bắt lỗi nhập liệu :

* Nhập sai chữ ký để kiểm tra



# CHƯƠNG 3: KẾT LUẬN VÀ BÀI HỌC KINH NGHIỆM

## **3.1. Kiến thức kỹ năng đã học được trong quá trình thực hiện đề tài**

* Qua quá trình nghiên cứu và thực hiện bài thực nghiệm, nhóm chúng em đã học được:
* Những kiến thức quan trọng trong môn An toàn và Bảo mật thông tin.
* Nhóm đã hiểu rõ về cách hoạt động và sử dụng của các hệ mã hóa
* Ngoài ra, kinh nghiệm của nhóm đã mở rộng đến việc thiết kế chương trình minh họa chữ ký điện tử Elgamal
* Nhóm cũng đã nắm bắt được cách mã hóa, giải mã, những kỹ năng quan trọng trong bảo mật thông tin.
* Qua dự án này, nhóm đã phát triển kỹ năng làm việc nhóm và khả năng phân chia công việc hiệu quả trong nhóm.

## **3.2. Bài học kinh nghiệm**

* Đảm bảo tính bảo mật cao khiến nó phù hợp cho các ứng dụng mật mã.
* Có thể mở rộng để hỗ trợ các tác vụ khác nhau như mã hóa và chữ ký. Điều này làm cho nó trở thành một lựa chọn linh hoạt cho các hệ thống mật mã.
* Được sử dụng trong các hệ thống giao tiếp bảo mật và cung cấp cơ chế xác thực như SSL/TLS trong việc bảo vệ thông tin trên Internet.
* Có thể chậm hơn so với một số phương pháp khác trong việc xác thực chữ ký điện tử lớn.
* Lựa chọn phổ biến cho việc bảo vệ thông tin và xác thực chữ ký điện tử trong các ứng dụng mật mã học.

## **3.3. Đề xuất về tính khả thi của chủ đề nghiên cứu, những thuận lợi, khó khăn**

Hiện nay, các giao dịch điện tử ngày càng trở nên phổ biến. Để bảo đảm an toàn cho các giao dịch này, cần phải sử dụng đến giải pháp chữ ký số. Chữ ký số được sử dụng để đảm bảo tính bảo mật, tính toàn vẹn, tính chống chối bỏ của các thông tin giao dịch trên mạng Internet. Chữ ký số tương đương với chữ ký tay nên có giá trị sử dụng trong các ứng dụng giao dịch điện tử với máy tính và mạng Internet cần tính pháp lý cao.

Hơn nữa, ngoài việc là một phương tiện điện tử được pháp luật thừa nhận về tính pháp lý, chữ ký số còn là một công nghệ mã hóa và xác thực rất mạnh. Nó có thể giúp bảo đảm an toàn, bảo mật cao cho các giao dịch trực tuyến, nhất là các giao dịch chứa các thông tin liên quan đến tài chính.

Hiện tại công nghệ chữ ký số tại Việt Nam có thể sử dụng trong các giao dịch để mua bán hàng trực tuyến, đầu tư chứng khoán trực tuyến, chuyển tiền ngân hàng, thanh toán trực tuyến. Ngoài ra, Bộ Tài chính cũng đã áp dụng chữ ký số vào kê khai, nộp thuế trực tuyến qua mạng Internet và các thủ tục hải quan điện tử như khai báo hải quan và thông quan trực tuyến mà không phải in các tờ khai, đóng dấu đỏ của công ty và chạy đến cơ quan thuế xếp hàng và ngồi đợi vài tiếng đồng hồ, có khi đến cả ngày để nộp tờ khai này.

Trong quá trình nghiên cứu để đạt được kết quả là tốt sẽ gặp rất nhiều quá khăn khi sử dụng chữ ký số cần phải cân nhắc trong việc lựa chọn đơn vị cung cấp đáng tin cậy. Nguồn nhân lực tạm ổn định vốn kiến thức, cơ cấu quản lý nhân vẫn còn đang trong quá trình phát triển, hoạt động nhóm giữa các thành viên chủ yếu là trực tuyến bởi quãng đường giữa các thành viên là xa.

Những nhóm, tổ chức cũng có những thế mạnh riêng là: Mọi người trong tổ chức hoạt động với nhau một cách tích cực, các thành viên có thái độ cầu tiến. trang thiết bị đầy đủ.

Trong tương lai tại Việt Nam chữ ký số có thể sử dụng với các ứng dụng chính phủ điện tử bởi các cơ quan nhà nước sắp tới sẽ làm việc với người dân hoàn toàn trực tuyến và một cửa. Khi cần làm thủ tục hành chính hay một sự xác nhận của cơ quan nhà nước, người dân chỉ cần ngồi ở nhà khai vào mẫu đơn và ký số để gửi là xong.

# TÀI LIỆU THAM KHẢO

[1] Bùi Doãn Khanh, Nguyễn Đình Thúc, Mã hóa thông tin – Lý thuyết và ứng dụng, NXB Lao động xã hội, 2011.

[2] Nguyễn Xuân Dũng, Bảo mật thông tin – Mô Hình và ứng dụng, NXB thống kê, 2009.

[3] TS. Phạm Văn Hiệp – Bài giảng, tài liệu môn An toàn bảo mật thông tin – Đại học Công nghiệp Hà Nội.

[4] Bùi Doãn Khanh, Nguyễn Đình Thúc, Mã hóa thông tin – Lý thuyết và ứng dụng, NXB Lao động xã hội, 2011.

[5] William Stallings, Cryptography and Network Security Principles and Practices, Fourth Edition, Prentice Hall, 2005.

[6]<https://efyca.vn/chu-ky-so-dien-tu-va-nhung-ung-dung-cua-chu-ky-so-dien-tu.html>

[7] <https://en.wikipedia.org/wiki/ElGamal_signature_scheme>

[8]<https://toplist.vn/top-list/ky-nang-quan-trong-nhat-de-dan-den-thanh-cong-4784.htm>