|  |
| --- |
|  |
| **BỘ CÔNG THƯƠNG**  **TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**  **---------------------------------------** |
| **BÀI TẬP LỚN**  **Môn: An toàn và bảo mật thông tin** |
|  |
| **TÌM HIỂU VỀ CHỮ KÝ ĐIỆN TỬ ELGAMAL VÀ VIẾT ỨNG DỤNG MINH HỌA** |
| **CBHD: *ThS. Trần Phương Nhung***  **Nhóm: 12** |
| **Thành viên nhóm:**   1. **Chu Phương Nam – 2018601946** 2. **Hoàng Văn Mạnh – 2019607142** |
|  |
|  |
|  |
| Hà Nội – 2021 |
|  |

# **Chương 1 : Tổng quan**

## **1.1 Bảo mật thông tin**

### **1.1.1 An toàn thông tin**

Với sự phát triển mạnh mẽ của công nghệ thông tin việc, ứng dụng các công nghệ mạng máy tính trở nên vô cùng phổ cập và cần thiết. Công nghệ mạng máy tính đã mang lại những lợi ích to lớn cho con người. Internet cho phép mọi người có thể truy cập, chia sẻ và khai thác thông tin một cách dễ dàng, hiệu quả và nhanh chóng. Sự phát triển mạnh mẽ của Internet về bản chất chính là việc đáp ứng lại sự gia tăng không ngừng của nhu cầu hoạt động trực tuyến trên hệ thống mạng toàn cầu của con người. Các hoạt động, các giao dịch trực tuyến trên Internet phát triển từ những hình thức sơ khai như trao đổi thông tin (email, messenger, …), quảng bá, ... đến những giao dịch phức tạp thể hiện qua các hệ thống chính phủ điện tử, thương mại điện tử ngày cá phát triển mạnh mẽ trên toàn cầu.

Bên cạnh việc phát triển mạnh mẽ của mạng Internet, vấn đề an toàn bảo mật thông tin trên không gian mạng là một vấn đề thách thức và khó giải quyết. Internet có những kỹ thuật cho phép mọi người truy cập, khai thác và chia sẻ thông tin với nhau. Nhưng chính việc đó cũng làm tăng nguy cơ thông tin của chúng ta bị người khác chính dẫn đến bị hư hỏng hay bị phá hủy hoàn toàn. Nguyên nhân của vấn đề này là việc truyền thông tin qua mạng Internet hiện nay chủ yếu sử dụng giao thức TCP/IP. TCP/IP cho phép các thông tin được từ máy tính này tới máy tính khác bằng cách đi qua một loạt các máy tính trung gian hoặc các mạng riêng biệt trước khi nó tới được đích. Chính vì vậy, nhờ vào giao thức TCP/IP các bên thứ ba có cơ hội để thực hiện các hành động gây mất an toàn thông tin khi chúng ta hoạt động trên không gian mạng.

Việc bảo vệ an toàn thông tin (dữ liệu) gồm có:

- Bảo mật: Bảo đảm tính bí mật cho tài liệu (cố định, đang di chuyển)

- Bảo toàn: Bảo đảm tính toàn vẹn của dữ liệu, bảo đảm tài liệu không bị thay đổi trong bộ nhớ hay trong quá trình truyền tin.

- Xác thực: Xác thực nguồn gốc của tài liệu, nhận dạng nguồn gốc của thông tin, cung cấp sự bảo đảm thông tin là đúng sự thực.

- Tính sẵn sàng: thông tin luôn sẵn sàng cho thực thể được phép sử dụng.

Để vừa đảm bảo tính bảo mật của thông tin lại không làm giảm sự phát triển của việc trao đổi thông tin trên toàn cầu thì chúng ta phải có các giải pháp phù hợp. Hiện có rất nhiều giải pháp cho vấn đề an toàn thông tin trên mạng như mã hóa thông tin, chữ ký điện tử, chứng chỉ điện tử (chứng chỉ khóa công khai), …

### **1.1.2 Mã hóa tài liệu**

**1.1.2.1 Hệ mã hóa**

Hệ mã hóa gồm 5 thành phần (**P, C, K, E, D**) thoả mãn các tính chất:

**P** (Plaintext) là tập hợp hữu hạn các bản rõ có thể, còn được gọi là không gian bản rõ.

**C** (Ciphertext) là tập hợp hữu hạn các bản mã có thể, còn được gọi là không gian bản mã. Mỗi phần tử của C có thể nhận được bằng cách áp dụng phép mã hoá Ek lên một phần tử của P, với k ∈ K.

**K** (Key) là tập hợp các khóa có thể còn gọi là không gian khóa (Khóa lập mã hay khóa giải mã).

**E** (Encryption) là tập hợp các quy tắc mã hóa có thể.

**D** (Decryption) là tập hợp các quy tắc giải mã có thể.

Một thông tin thường ở dạng bản rõ. Người gửi thực hiện mã hóa bản rõ bằng các khóa dùng để tạo mã (**Ke)**, kết quả thu được gọi là bản mã. Người nhận được bản mã, họ giải mã bằng khóa giải mã (**Kd)**, để thu được bản rõ.

**EKe(P) = C** và **DKd(C) = P**

Có một số cách phân loại mã hóa. Nếu phân loại mã hóa theo đặc trưng của khóa lập mã và khóa giải mã, thì có hai loại mã hóa:

* Mã hóa khóa đối xứng (Mã hóa khóa bí mật)
* Mã hóa khóa phi đối xứng (Mã hóa khóa công khai).

**1.1.2.2 Hệ mã hóa khóa bí mật**

* Hệ mã hóa khóa bí mật (secret key encryption) được đặc trưng bởi việc sử dụng một khóa duy nhất cho cả quá trình mã hóa và giải mã thông tin.
* Hệ mã hóa này yêu cầu người gửi và người nhận phải thỏa thuận một khóa trước khi thông báo được gửi đi, và khóa này phải được giữ bí mật giữa bên gửi và bên nhận (bên mã hoá và bên giải mã), đồng thời được giữ bí mật trong suốt thời gian sử dụng.
* Việc bảo mật thông tin phụ thuộc vào việc bảo mật khóa.

Kỹ thuật mã hóa dùng khóa bí mật còn được gọi là mật mã quy ước (conventional encryption) hoặc mật mã đối xứng(symmetric encryption)

Ví dụ về hệ mã hóa khóa bí mật: DES, IDEA, AES, …

EK(P) = C và DK(C) = P



*Hình 1.1. Hệ mã hóa khóa bí mật*

* Ưu điểm :
  + Mô hình khá đơn giản.
  + Dễ dàng tạo ra thuật toán mã hóa đối xứng cho cá nhân.
  + Dễ cài đặt và hoạt động hiệu quả
  + Hoạt động nhanh và hiệu quả do tốc độ mã hoá và giải mã cao.
* Nhược điểm :
  + Dùng chung khóa nên nhiều nguy cơ mất an toàn.
  + Khóa dùng chung rất dễ bị “bẻ khóa”, đánh cắp, ... do cũng phải truyền trên kênh truyền tin đến bên nhận.
  + Việc gửi thông tin cùng khóa cho số lượng người nhận lớn là khó khăn
  + Nếu số lượng người nhận tin lớn thì số khóa cần trao đổi cũng phải lớn dẫn đến tính an toàn và bảo mật giảm.

**1.1.2.3 Hệ mã hóa khóa công khai**

* Đặc trưng của kỹ thuật mật mã bất đối xứng là dùng hai khóa riêng biệt cho hai quá trình mã hóa và giải mã, trong đó có một khóa có thể được phổ biến công khai (public key) và khóa còn lại được giữ bí mật (private key).
* Cả hai khóa đều có thể được dùng để mã hóa hoặc giải mã và không có khoá nào có thể suy được từ khoá kia.
* Trong mọi trường hợp, khóa lập mã và khóa giải mã là khác nhau.
* Hệ mã hóa khóa công khai (public key encryption) còn được gọi là hệ

mã hóa bất đối xứng (asymmetric encryption).

* Hệ mã hóa này không yêu cầu người gửi và người nhận phải thỏa thuận một khóa bí mật. Khóa công khai (public key) cho mọi người biết để lập mã, khóa mật (private key) chỉ thuộc về một người, dùng để giải mã.
* Ví dụ về hệ mã hóa khóa công khai: RSA, Elgamal, …



*Hình 1.2. Hệ mã hóa khóa công khai*

**1.1.2.4 Hệ mã hóa bảo vệ tài liệu**

Hệ mã hóa có thể thực hiện được cả ba chức năng bảo vệ tài liệu: bảo mật, bảo toàn, xác thực.

* Bảo mật: Khi mã hóa tài liệu, kẻ gian sẽ không hiểu được thông tin
* Bảo toàn: Đảm bảo tài liệu không bị sửa đổi trong quá trình truyền. Khi mã hóa tài liệu theo cách này, kẻ gian sẽ không hiểu được thông tin, do đó không thể sửa đổi được tài liệu theo ý mình. Biện pháp này ngăn chặn kẻ gian ngay từ đầu. Khi dùng mã xác thực tài liệu, nếu kẻ gian sửa đổi tài liệu, thì mã xác thực của tài liệu bị sửa đổi sẽ khác với mã xác thực của tài liệu gốc. Do đó, người ta sẽ nhận ra có sự thay đổi trong tài liệu gốc. Như vậy mã xác thực dùng để kiểm tra tính toàn vẹn của tài liệu.
* Xác thực: Khi dùng mã xác thực với một tài liệu, mã xác thực dùng để minh chứng nguồn gốc của tài liệu đó, kẻ gian khó thể tạo ra mã xác thực giống như mã xác thực ban đầu.

### **1.1.3 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 chủ nhân của dữ liệu và xác nhận sự chấp thuận của người đó đối với nội dung 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 số. Xuất phát từ thực tế, chữ ký điện tử cần đảm bảo chức năng xác định được người chủ của một dữ liệu nào đó: văn bản, âm thanh, hình ảnh,… của dữ liệu đó có bị thay đổi hay không.
* Thông thường chữ ký của một người trên tài liệu thường đặt ở cuối bản tin để xác nhận nguồn gốc hay trách nhiệm của người ký với tài liệu đó. Với tài liệu đã được “số hóa” nếu chữ ký đặt ở cuối bản tin thì việc sao chép “chữ ký số” là dễ dàng và tính toàn vẹn dữ liệu sẽ không được đảm bảo. Vậy một “chữ ký số” đặt cuối tài liệu “số hóa” không thể chịu trách nhiệm đối với toàn bộ nội dung văn bản. “Chữ ký số” thể hiện trách nhiệm đối với toàn bộ tài liệu phải là chữ ký được ký trên từng bit của tài liệu đó. Tuy nhiên, chữ ký số cũng không thể ký trên bất kỳ tài liệu nào với độ dài tùy ý, vì như vậy chữ ký số sẽ có độ dài rất lớn. Với tài liệu dài người ta ký trên đại diện của nó mà đại diện này được tạo ra từ hàm băm.
* Chữ ký thông thường người ta kiểm tra bằng cách so sánh với chữ ký xác thực khác. Đây không phải phương pháp an toàn vì nó có thể giả mạo. Với chữ ký số, người ta có thể kiểm tra thông qua thuật toán kiểm tra công khai.Bất kỳ ai cũng có thể kiểm tra được chữ ký số. Việc dùng một lược đồ chữ ký an toàn sẽ ngăn chặn được khả năng giả mạo bởi nó sẽ đảm bảo ba yêu cầu:
  + Xác thực
  + Toàn vẹn dữ liệu
  + Không thể thoái thác trách nhiệm
* Bản thân bức điện, văn bản gửi đi cần chứa thông tin thay đổi liên tục (chẳng hạn như ngày tháng) để đảm bảo văn bản không bị dùng lại vì bản sao tài liệu được ký bằng chữ ký số đồng nhất với bản gốc
* **Lợi ích của việc sử dụng chữ ký điện tử :** 
  + Giảm thời gian
  + Giảm chi phí
  + Bảo mật thông tin

## **1.2 Tính pháp lý của chữ ký điện tử**

Để xác định tính pháp lý của 3 loại chữ ký điện tử gồm: Chữ ký số, chữ ký scan và chữ ký hình ảnh, doanh nghiệp có thể căn cứ vào các văn bản pháp luật sau đây:

* Luật Giao dịch điện tử năm 2005.
* Nghị định 130/2018/NĐ-CP ngày 27/9/2018 của Chính Phủ quy định chi tiết thi hành Luật Giao dịch điện tử năm 2005.
* Nghị định số 52/2013/NĐ-CP ngày 16/5/2013 của Chính phủ về thương mại điện tử.
* BLDS 2015 điều chỉnh tất cả các loại giao dịch và hợp đồng, bao gồm cả các giao dịch và hợp đồng được ký kết bằng chữ ký sống và các giao dịch và hợp đồng được ký kết thông qua phương tiện điện tử.

Theo Luật Giao dịch điện tử 2005, chữ ký điện tử có giá trị pháp lý nếu:

* Phương pháp tạo chữ ký điện tử cho phép xác minh người ký và chứng tỏ sự chấp thuận của người ký đối với nội dung hợp đồng.
* Phương pháp tạo chữ ký điện tử là đủ tin cậy, phù hợp với mục đích mà hợp đồng được khởi tạo và gửi đi.

Như vậy, theo các quy định của pháp luật hiện hành, pháp luật Việt Nam mới có quy định về chữ ký số, chưa có nhiều văn bản hướng dẫn cụ thể về hiệu lực của hợp đồng được ký kết bằng hình thức scan hay chữ ký hình ảnh. Do đó, khi tìm hiểu về khung pháp lý cho chữ ký điện tử sử dụng trên hợp đồng điện tử, doanh nghiệp có thể căn cứ vào các văn bản pháp luật quy định về chữ ký số để áp dụng.

## **1.3 Lược đồ chữ ký Elgamal**

Lược đồ Elgamal được đề xuất năm 1985 . Sau đó, Viện tiêu chuẩn và Công nghệ quốc gia Mỹ sửa đổi thành chuẩn chữ ký số (Digital Signature Standard – DSS). Lược đồ Elgamal không tất định cũng giống như hệ thống mã khóa công khai Elgamal. Điều này có nghĩa là, có nhiều chữ ký hợp lệ cho một thông điệp bất kỳ. Thuật toán kiểm thử phải có khả năng chấp nhận bất kỳ chữ ký hợp lệ nào khi xác minh.

Phương pháp Elgamal được xây dựng chỉ nhằm giải quyết bài toán chữ ký số.

**Tóm tắt lược đồ chữ ký Elgamal**

Cho p là số nguyên tố sao cho bài toán logarit rời rạc trên Zp là khó và cho ∈ Z\*p là phần tử nguyên thủy.

Cho p = Z\*p , A = Z\*p x Zp-1 và định nghĩa:

K = {(p,, a, ): = a (mod p)}

Giá trị p, , là công khai còn a là bí mật

Với K = {(p,, a, )} và một số ngẫu nhiên (bí mật) k ∈ Z\*p-1

Định nghĩa: Sigk (x, k) = (,), trong đó :

= k mod p và = (x – ay) k-1 mod (p-1)

Với x, y ∈ Z\*p và ∈ Zp-1 ta định nghĩa :

Ver(x, , ) = true ⬄ ^\* ^ x  (mod p)

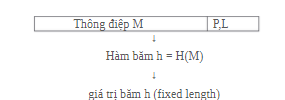
**1.4 Hàm băm SHA**

**Giới thiệu sơ lược về hàm băm mật mã:**

Hiểu theo nghĩa đơn giản, hàm băm là hàn cho tương ứng một mảng dữ liệu lớn với một mảng dữ liệu nhỏ hơn mà được dùng rộng rãi trong nhiều ứng dụng tin học, không chỉ phạm vi mật mã.

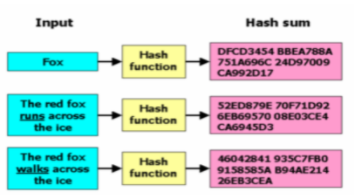
Trong mã hóa hàm băm được xem như là ảnh đại diện thu gọn của một dãy bit có độ dài hữu hạn tùy ý và được sử dụng để nhận diện cho chuỗi bit đó, kế hợp công cụ để tạo chữ ký số, cá hàm băm được dùng cho việc đảm bảo tính toàn vẹn của dữ liệu .

**Định nghĩa:**

****

* 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 quy định(tùy thuộc vào thuật toán hàm băm). Dãy bit này được gọi là thông điệp rút gọn, hay giá trị băm, đại diện cho thông điệp ban đầu
* Hàm băm là hàm một chiều mà neesy đưa một lượng dữ liệu bất kì qua hàm này sẽ cho ra một chuỗi số có độ dài cố định ở đầu ra
* hàm h(X) được gọi là hàm băm khi nó thỏa mãn 2 điều kiện sau:
* nén gọn: hàm h(x) tương ứng có chiều dài cố định n>0
* Dễ tính toán : với mọi điều kiện chuỗi vit đầu vào x có chiều dài hữu hạn tùy ý,h(X) được tính toán dễ dàng.

**Hoạt động của hàm băm:**

****

**Một hàm băm lý tưởng có các tính chất sau:**

* Tính kháng tiền ảnh: với mọi đầu ra y cho trước không thể tìm được bất kỳ giá trị đầu vào x sao cho h(x) = y
* Tính kháng tiền ảnh thứ 2: Với mọi điều kiện vào x cho trước y=h(X), không thể tính toán để tìm ra được x’≠ sao cho h(x’) = h(x)
* Tính kháng xung đột: Không thể tính toán để tìm được 2 giá trị đầu vào x’ và x phân biệt sao cho h(x) = h(x’)

**Phân loại hàm băm mật mã**

Dựa trên tham biến đầu vào của các hàm băm, các hàm băm mật mã được phân thành 2 lớp

* Lớp các hàm băm sử dụng khóa, chẳng hạn như Mac: nhận hai giá trị đầu vào
* Thông điệp cần tính giá trị hàm băm
* Khóa bí mật để băm văn bản theo đúng chuẩn quy định
* Lớp các hàm băm không sử dụng khóa :chỉ nhận vào một giá trị duy nhất là thông điệp

Trong lớp các hàm băm không sử dụng khóa thì MDCs. Lớp này lại chia thành các lớp nhỏ hơn

* Hàm băm một chiều: các hàm trong lớp này đều thảo mã tính chất là với mọi mã băm biết trước không thể tính toán được chuỗi bit đầu vào có mã băm bằng với mã băm đã cho
* Hàm băm kháng xung đột: các hàm trong lớp này thỏa mãn tính chất không thể tính toán để tìm ra hai chuỗi có cùng giá trị băm

**Cấu trúc của thuật toán hàm băm**

Khối dữ liệu đầu vào X có chiều dài tuỳ ý sẽ được phân thành các khối Con liên tiếp X1 , X2 , Xm ( với xi có chiều dài cố định là r ) . Tuy nhiên do chiều dài khối ban đầu là tùy ý nên ta cần thêm vào dữ liệu ban đầu một số bit phụ sao cho tổng số bit của khối dữ liệu x sau khi thêm vào sẽ là bội số của r . Ngoài ra số bit phụ thêm vào thường chứa một khối bit xác định chiều dài thực sự của khối dữ liệu khi chưa thêm các bit phụ . Sau đó ta lần lượt cắt từng khối con r bit từ khối x . Mỗi khối con r bit x ta thực hiện một hàm nén của hàm băm h ( x ) được ký hiệu là f . Tại bước thứ i , hàm nến f nhận dữ liệu đầu vào là xi và kết quả trung gian của bước trước đó để tạo đầu ra là kết quả trung gian bước thứ , ký hiệu là H. Kết quả trung gian tại mỗi bước H là một chuỗi bit có độ dài cố định bằng n > 0 . Nếu ký hiệu IV ( init value ) là giá trị khởi tạo ban đầu cho Ho , thì quá trình lặp xử lý dãy các khối con được mô tả như sau :

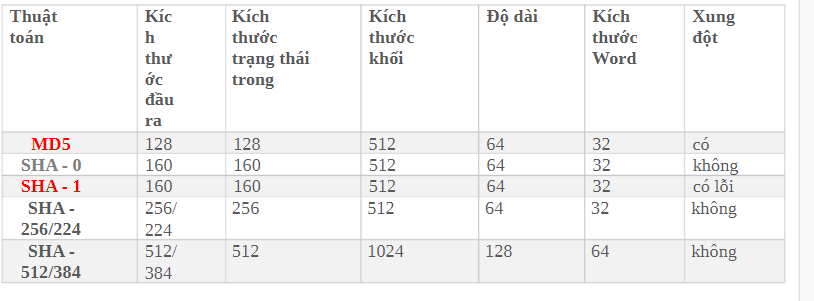
Ho = IV

Hı = f ( H : i-1 , x ) , ( i = 1 , ... , m )

h ( x ) = g ( H m )

H là kết quả trung gian sau bước thứ , là các biến dây chuyền . Hàm g ( x ) ánh xạ biến dây chuyền cuối cùng để tạo ra mã băm kết quả . Và thông thường g(x) được chọn là ánh xạ đồng nhất g(Hm)0Hm. Khâu then chốt trong xây dựng hàm băm là thiết kế nén f

**Các hàm băm mật mã sử dụng phổ biến hiện nay**

****

**SHA**

SHA hay thuật toán băm bảo mật là một họ những thuật toán băm mật mã do viện tiêu chuẩn và công nghệ Quốc gia (NIST) công bố thuộc tiêu chuẩn xử lý thông tin Liên Bang Hoa Kỳ (FIPS)[6,8,9]. Hiện tại có ba thuật toán SHA1, SHA2, SHA3 được định nghĩa.

Dưới đây các thuật toán băm SHA

- SHA 1

- SHA 2 ( SHA - 224; SHA - 256; SHA - 384; SHA - 512)

- SHA 3 ( SHA3 – 224; SHA3 – 256; SHA3 – 384; SHA3 – 512)

\* SHA1 & SHA2

Đối với SHA 1 và SHA – 256, thông điệp mở rộng được phân tích thành N khối 512 bits M(1), M(2), …, M(N) . Do đó 512 bits của khối dữ liệu đầu vào có thể được thể hiện bằng 16 từ 32 – bits, M0 (i) chứa 32 bits đầu của khối thông điệp i, M1 (i) chứa 32 bits kế tiếp…

Đối với SHA 384, SHA – 512 thông điệp mở rộng được phân tích thành N khối 1024 bits M(1), M(2),.., M(N). Do đó 1024 bits của khối dữ liệu ban đầu vào có thể được thể hiện bằng 16 từ 64 bits, M0 (i) chứa 64 bit đầu của khối thông điệp i, M1 (i) chứa 64 bits kế tiếp… M16 (i) chứa 64 bits cuối cùng.

Trước khi thực hiện băm, với mỗi thuật toán băm an toàn, giá trị băm ban đầu H (0) phải được thiết lập. Kích thước và số lượng từ trong H (0) tùy thuộc vào kích thước thông điệp rút gọn.

Các cặp thuật toán SHA – 224 và SHA – 256; SHA – 384 và SHA – 512 có các thao tác thực hiện giống nhau, chỉ khác nhau về số lượng bits kết quả của thông điệp rút gọn. Nói cách khác, SHA -224 sử dụng 224 bits đầu tiên trong kết quả thông điệp rút gọn sau khi áp dụng thuật toán SHA – 256. Tương tự SHA – 384 và SHA – 512 sử dụng 384 bits/512 bits đầu tiên trong kết quả thông điệp rút gọn.

\*Hàm băm SHA3

Trong tháng 11 năm 2007 Viện Tiêu Chuẩn và Công nghệ Quốc gia Mỹ (NIST) đã mở một cuộc thi để phát triển thuât toán hàm “băm” mới thay cho SHA2. Các thuật toán băm mới sẽ được gọi là Secure Hash Alorithm – 3 (SHA3) [10,11,12,13]. Có 56 trong đó 64 mẫu thiết kế đã tham gia cuộc thi SHA3, 51 mẫu đệ trình đã lọt qua vòng 1 và vào ngày 01 tháng 11 năm 2008, 14 mẫu đã lọt vào vòng 2. Chung kết thiết kế SHA -3 đã được công bố vào ngày 09 tháng 12 năm 2010. Các thuật toán cuối cùng được coi như một ứng cử viên thay thế cho SHA -3 lad BLAKE, Grostl, JH, Keccak và Skein. Các tiêu chí lựa chọn bao gồm việc thực thi trong cả phần mềm và phần cứng, dung lượng thực hiện phần cứng, phản ứng với những nguy cơ tấn công đã biết tốt nhất và đủ khác biệt với các ứng viên khác.

Trong tháng 10 năm 2012, Viện Tiêu Chuẩn và công nghệ (NIST) đã chọn các thuật toán Keccack như là tiêu chuẩn mới SHA – 3. Hàm băm được thiết kế bởi Guido Bertoni, Joan Daemen, Michael Peeters và Gilles van Assche. Các hoán vị cơ bản Keccak tạo điều kiện cho việc mở rộng các chức năng mã hóa hoán vị dựa trên hoán vị bổ sung.

Thuật toán SHA -3 bao gồm:

Bốn dạng hàm băm mật mã là: SHA 3 -224, SHA3 – 256, SHA3 – 384, SHA3 – 512.

Hai dạng hàm băm mở rộng là: SHAKE-128, SHAKE- 256.

1. Trạng thái Keccak Trong phần này, các hoán vị Keccak – p được xác định với hai tham số: - Độ dài cố định của chuỗi hoán vị được gọi là chiều rộng của hoán vị - Số lần lặp lại của một chuyển đổi được gọi là một vòng. SHA3 là tổ hợp các hàm sponge được đặc trưng bởi hai tham số, tốc độ r bits và cường độ an toàn c. Tổng, r+c xác định độ rộng của hàm băm SHA3. Phép hoán vị được sử dụng trong việc xây dựng Sponge và giới hạn giá tị cực đại là 1600.

Chiều rộng được biểu thị bởi b và số vòng được biểu thị bởi nr. Các Keccak – p hoán vị với số vòng là nr và chiều rộng b được ký hiệu Keccak – p[b nr].

Mỗi hàm nén Keccak là duy nhất bao gồm 24 dạng viên đạn và mỗi vòng được chia thành năm bước là: 𝜽(𝑨), Rho (ρ) và Pi (π), Chi(Χ), Iota(i) (sẽ tương ứng với 5 thuật toán sẽ trình bày bên dưới)

a. Thành phần của mảng trạng thái hàm băm SHA3

b. Chuyển dạng chuỗi thành dạng mảng các trạng thái

c. Chuyển mảng trạng thái thành dạng chuỗi

2. Đặc tả thuật toán chuyển trạng thái của Keccak –p[b,nr]

a) Đặc tả thuật toán theta 𝜃(𝐴)

b) Đặc tả thuật toán 2 Rho ρ(A)

c) Đặc tả thuật toán pi (π) d) Thuật toán 4 Chi(X);

e) Thuật toán 5 (Iota): j(A,ir)

3. Xây dựng Sponge.

Xây dựng sponge là một khuân khổ để xác định các hàm dạng nhị phân với độ dài đầu ra tùy ý. Việc xây dựng sử dụng ba thành phần sau:

- Hàm cơ bản về chuỗi có chiều dài cố định, kí hiệu là f.

- Một tham biến tốc độ, kí hiệu là r.

- Một quy tắc chêm/thêm, kí hiệu là pad.

Xây dựng sponge

**1.5 Kết luận chương**

Với chủ đề nghiên cứu thuộc lĩnh vực hoạt động “An toàn bảo mật”, trong chương 1 chúng ta đã nghiên cứu về hệ mã hóa khóa bí mật và hệ mã hóa khóa công khai. Hai loại mã hóa này khác nhau ở số lượng khóa, cách thức mã hóa và giải mã bằng các loại khóa. Mã hóa khóa bí mật sử dụng một khóa duy nhất cho cả quá trình mã hóa và giải mã thông tin. Trong khi đó, mã hóa khóa công khai sử dụng hai khóa khác nhau để mã hóa và giải mã thông tin. Mỗi hệ thống mã hóa có ưu nhược điểm riêng.

Đối với hệ mã hóa khóa bí mật, mô hình đơn giản, dễ thao tác, cài đặt, tốc độ xử lý nhanh nhưng độ an toàn không cao. Cả bên nhận và bên gửi đều đã biết về khóa bí mật, cho phép trao đổi thông tin từ A đến B hoặc từ B đến A, không phân được A và B trong quá trình trao đổi thông tin, vì thế kênh truyền phải được bảo vệ từ hai phía. Nếu khóa lập mã bị lộ thì người khác dễ dàng tìm ra khóa giải mã vì vậy vấn đề bảo mật thông tin khi sử dụng kỹ thuật mã hóa khóa bí mật là việc bảo mật khóa. Với n người sử dụng cần trao đổi thông tin với nhau dùng mã hóa khóa bí mật thì mỗi cá thể cần biết n1 khóa bí mật. Thế thì với n cá thể đòi hỏi phải có số khóa ít nhất là n\*(n-1)/2 khóa. Khi tăng số người sử dụng thì số khóa sẽ tăng rất nhanh, gây nên hậu quả kém an toàn.

Hệ mã hóa khóa công khai ra đời đã khắc phục được nhược điểm của hệ mã hóa khóa bí mật, điển hình của hệ mật này có thể kể đến như RSA, Elgamal, … Mã hóa khóa công khai có độ an toàn và tính thuận tiện trong quản lý khóa cao mặc dù xử lý chậm hơn. Trong các ứng dụng mã hóa hiện đại, người ta thường kết hợp các ưu điểm của hai loại mã hóa này.

Từ lược đồ chữ ký Elgamal nhóm đã triển khai cụ thể hóa bài toán bằng 2 ngôn ngữ: CSharp và Python.

Bên cạnh đó, chúng ta đã nghiên cứu về chữ ký điện tử là một dạng thông tin đi kèm theo dữ liệu (có thể là văn bản, hình ảnh, video,...) được sử dụng với mục đích xác định chủ sở hữu dữ liệu đó. Chữ ký điện tử được sử dụng trong các giao dịch điện tử và cần đảm bảo xác định tính cố định trong dữ liệu của chủ sở hữu.

**Những kiến thức cần để hoàn thành đề tài đó là hiểu được cái khái niệm của hệ mã hóa, chữ ký điện từ, lược đồ chữ ký Elgamal, mã hóa bất đối xứng và hàm băm.**

**Chương 2 : Kết quả nghiên cứu**

## **2.1 Giới thiệu**

**a. Tên đề tài nghiên cứu** : Tìm hiểu về chữ ký điện tử ElGamal và viết ứng dụng minh họa.

**b. Nhiệm vụ của đề tài :**

* Tìm hiểu về chữ ký điện tử, chữ ký điện tử Elgamal.
* Tìm hiểu phương pháp mã hóa bất đối xứng ứng dụng trong chữ ký điện tử.
* Tìm hiểu về hàm băm SHA
* Ứng dụng xây dựng chương trình
* Demo chương trình

**c. Các bước thực hiện triển khai đề tài :**

1. Nghiên cứu tìm hiểu phân biệt rõ về hệ mã hóa công khai, hệ mã hóa bí mật
2. Nghiên cứu tìm hiểu về chữ ký điện tử, (thế nào là chữ ký điện tử, lợi ích tính ứng dụng của chữ ký điện tử, ...), chữ ký điện tử Elgamal
3. Nghiên cứu tìm hiểu phương pháp mã hóa bất đối xứng
   * Thế nào là hệ mã hóa bất đối xứng
   * Phân biệt hệ mã hóa bất đối xứng với hệ mã hóa đối xứng
   * Ưu điểm khi sử dụng hệ mã hóa bất đối xứng
4. Nghiên cứu tìm hiểu phương pháp hàm băm SHA
   * Định nghĩa thế nào là hàm băm
   * Hàm băm dùng để làm gì
5. Thiết kế và cài đặt chương trình theo lược đồ chữ ký Elgamal

**d. Hình thức sản phẩm:** Sản phẩm ứng dụng

**e. Kết quả đạt được :**

* Hiểu và nắm các vấn đề đã nêu ở trên
* Từ việc hiểu hoàn thành việc triển khai cài đặt phần mềm minh họa

## **2.2 Nội dung thuật toán**

**2.2.1 Thuật toán sinh khóa**

Mỗi cá thể trong hệ thống tạo một khóa công khai và một khóa riêng tương ứng. Mỗi cá thể thực hiện các bước sau :

1. Tạo số nguyên tố lớn p và chọn ∈ Zp
2. Chọn số nguyên a: 1 a p-2
3. Tính y = a mod p

***Lúc này:*** Khóa công khai là (p, , y), khóa bí mật là a.

**2.2.2 Thuật toán sinh chữ ký**

Để ký lên thông điệp m ta thực hiện lần lượt các bước

1. Chọn số nguyên k, 1 k p-2 , với GCD(k, p-1) = 1
2. Tính r = ak mod p
3. Tính k-1 mod (p-1)
4. Tính s = k-1 \* (h(m) – a \* r) mod (p-1)

*Chú thích: h(m) tức kết quả sau khi sử dụng hàm Hash lên văn bản m*

1. Chữ ký của A lên thông điệp m là (r, s)

**2.2.3 Thuật toán chứng thực chữ ký**

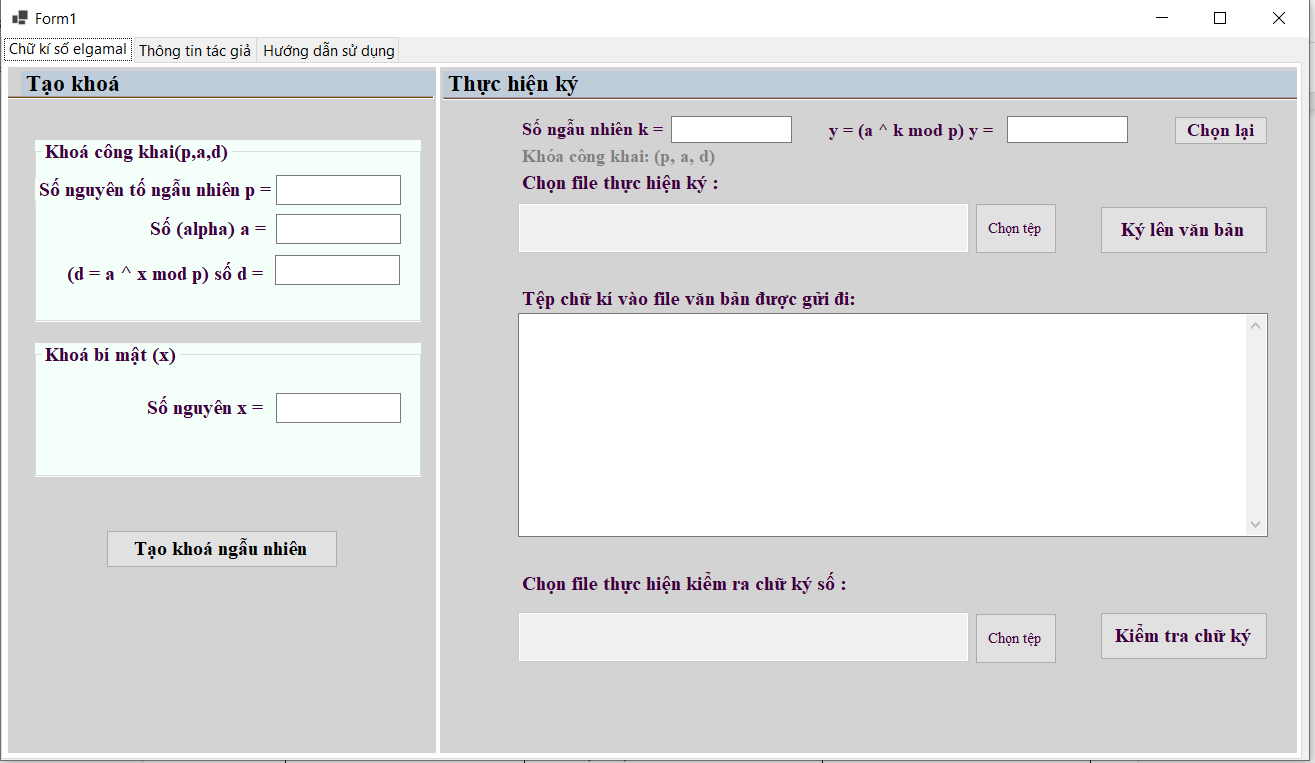
Thực hiện các bước sau để chứng thực chữ ký (r, s) lên m

1. Xác nhận khóa công khai của bên gửi là (p, , β)
2. Kiểm tra r, 1 r p - 1, nếu không đúng thì từ chối chữ ký của bên gửi
3. Tính v1 = yr \* rs mod p
4. Tính h(m) và v2 = h(m) mod p
5. Nếu v1 = v2 thì chấp nhận chữ ký của A

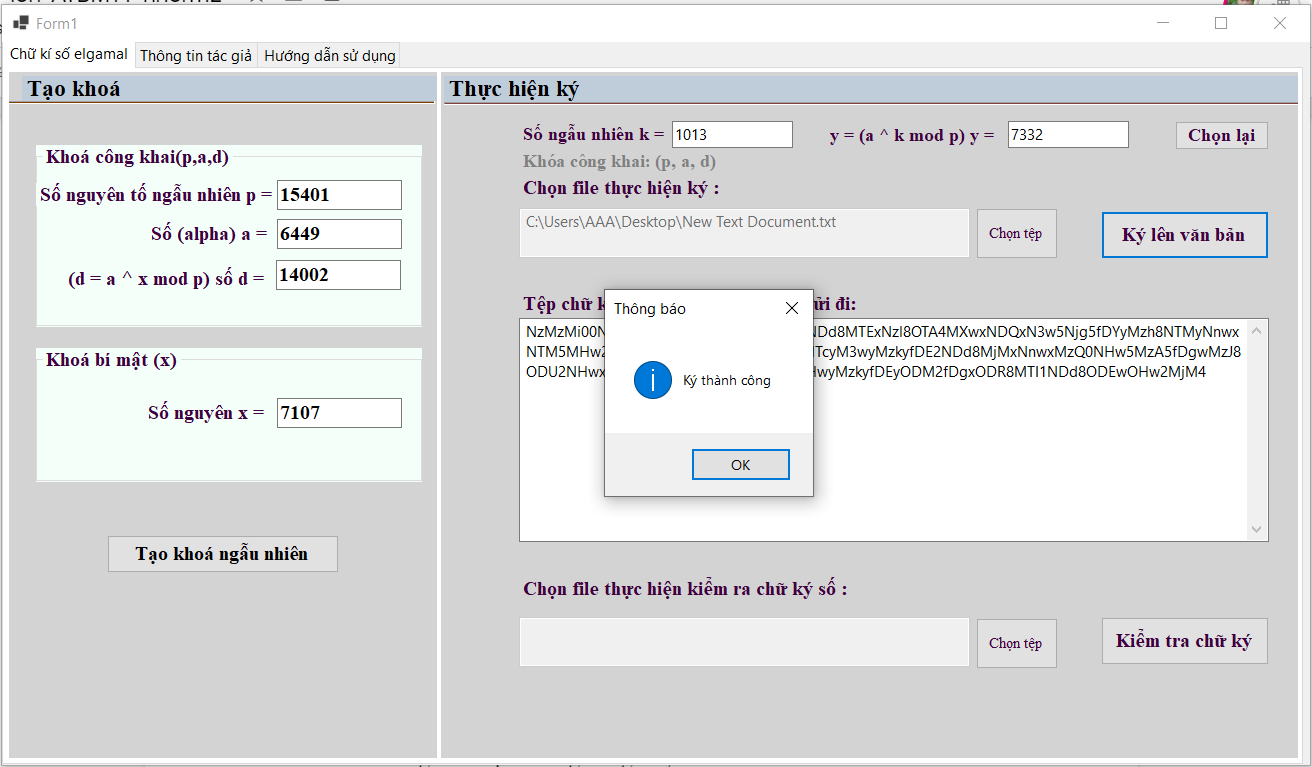
## **2.3 Thiết kế, cài đặt chương trình demo thuật toán**

**2.3.1 Giao diện chương trình demo**

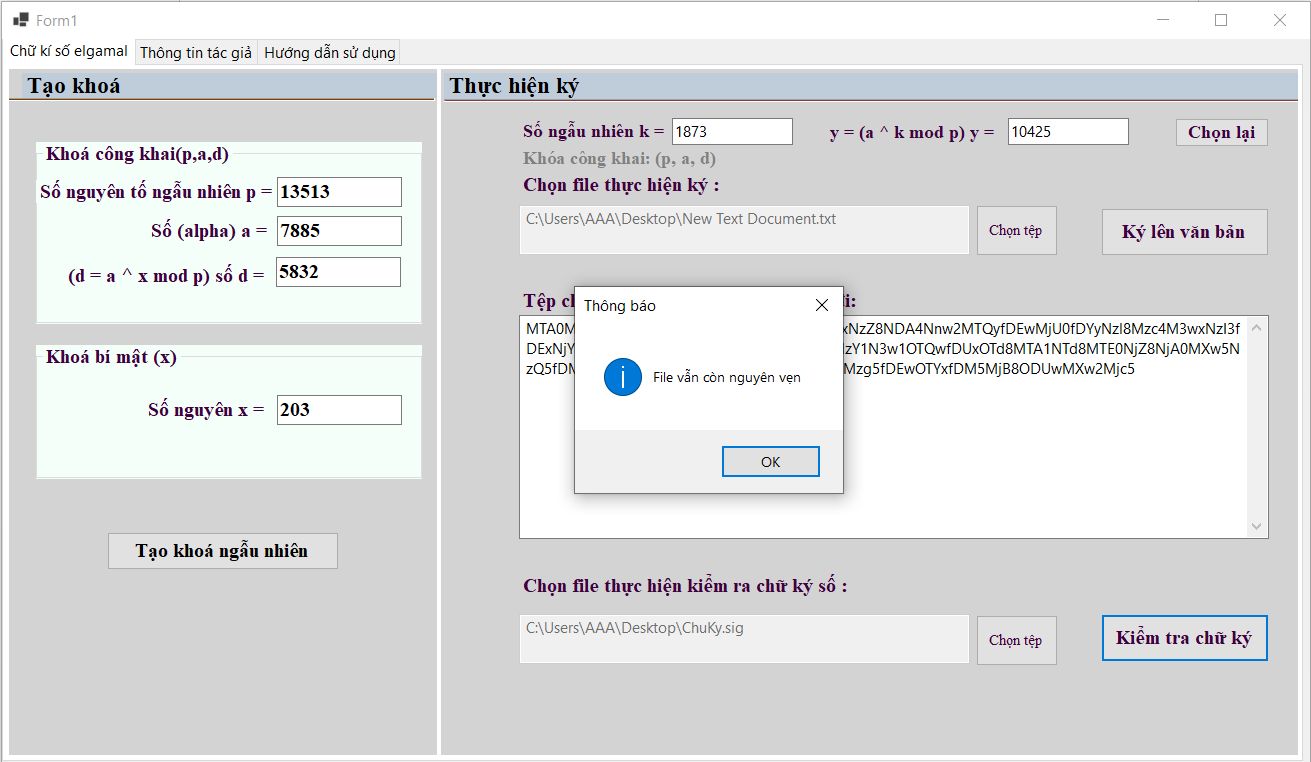
* Chương trình tạo bởi ngôn ngữ Csharp
  + Giao diện chính



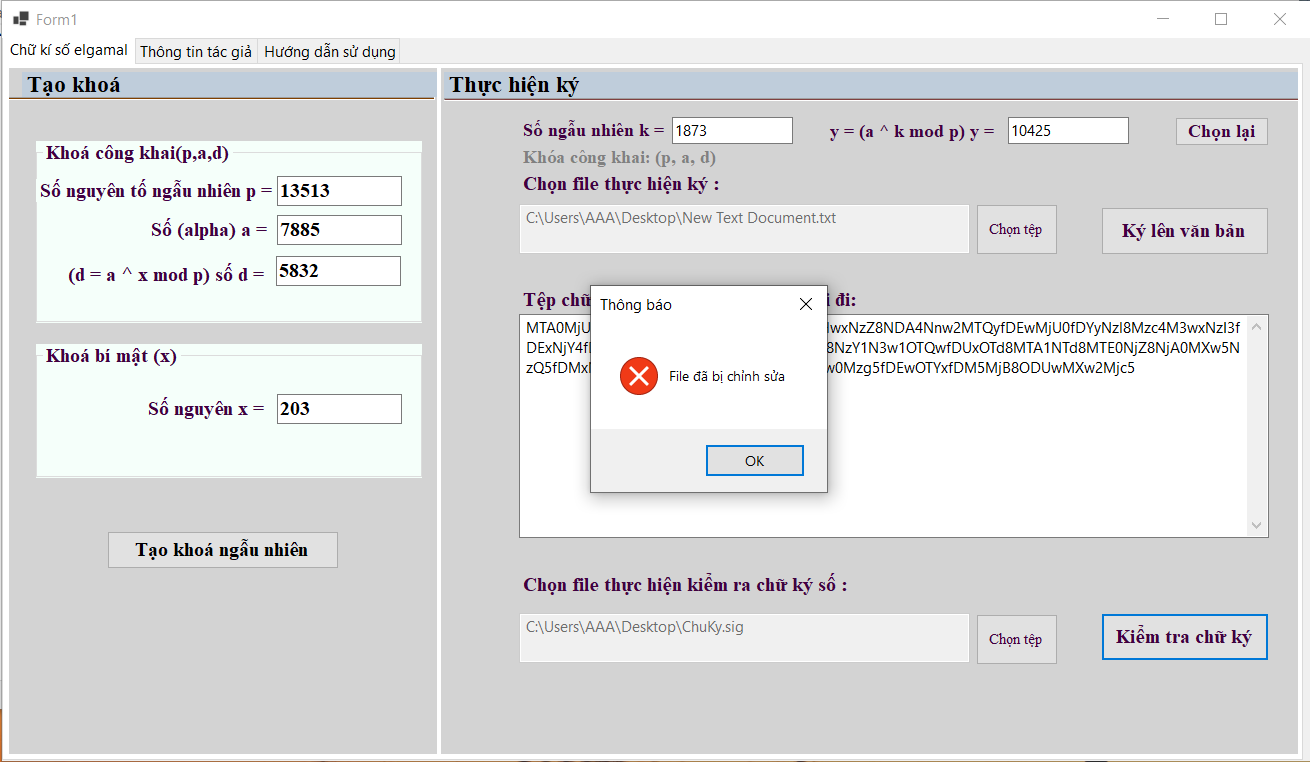
* + Giao diện sau khi ký thành công văn bản



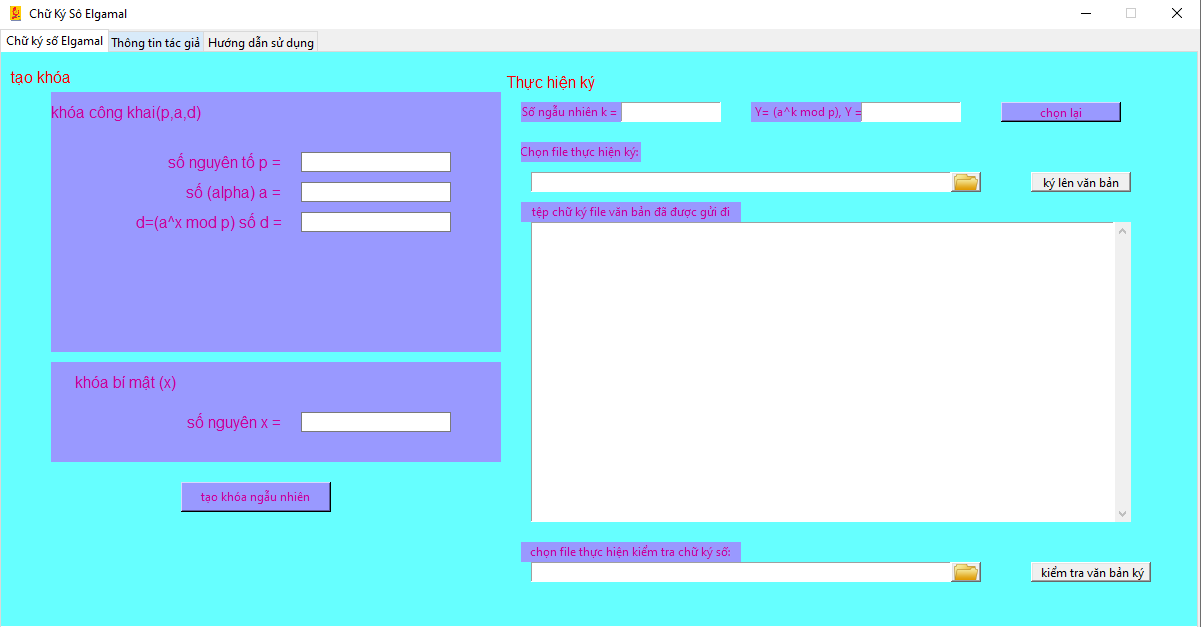
* + Giao diện sau khi văn bản được kiểm tra vẫn nguyên vẹn chưa bị chỉnh sửa



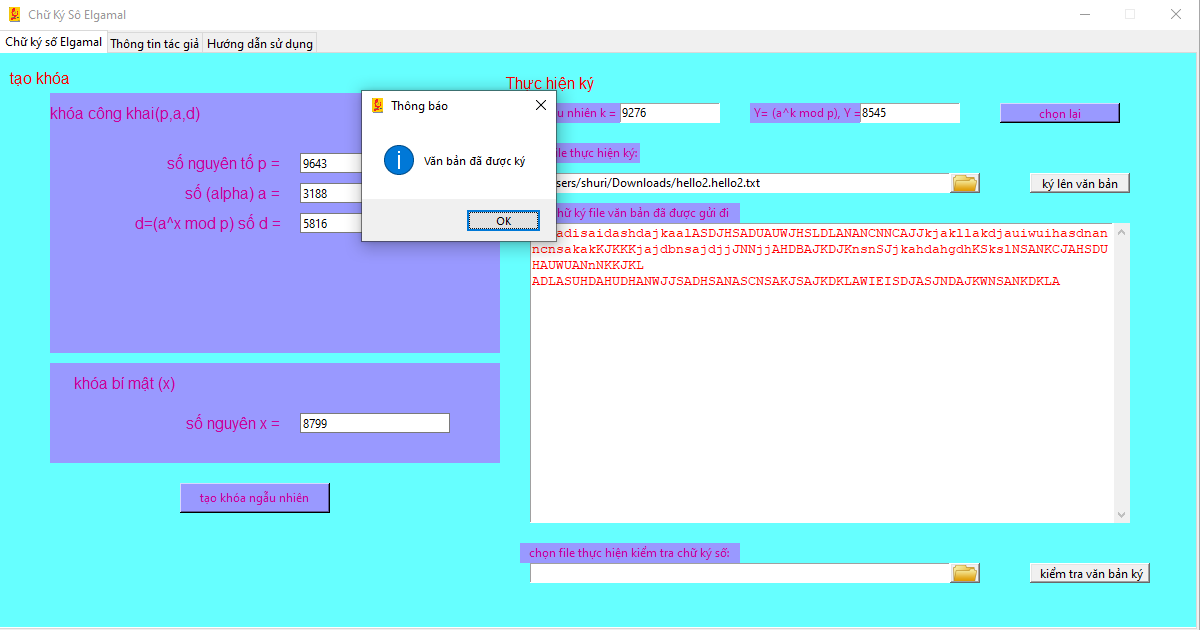
* + Giao diện sau khi văn bản được kiểm tra đã bị chỉnh sửa



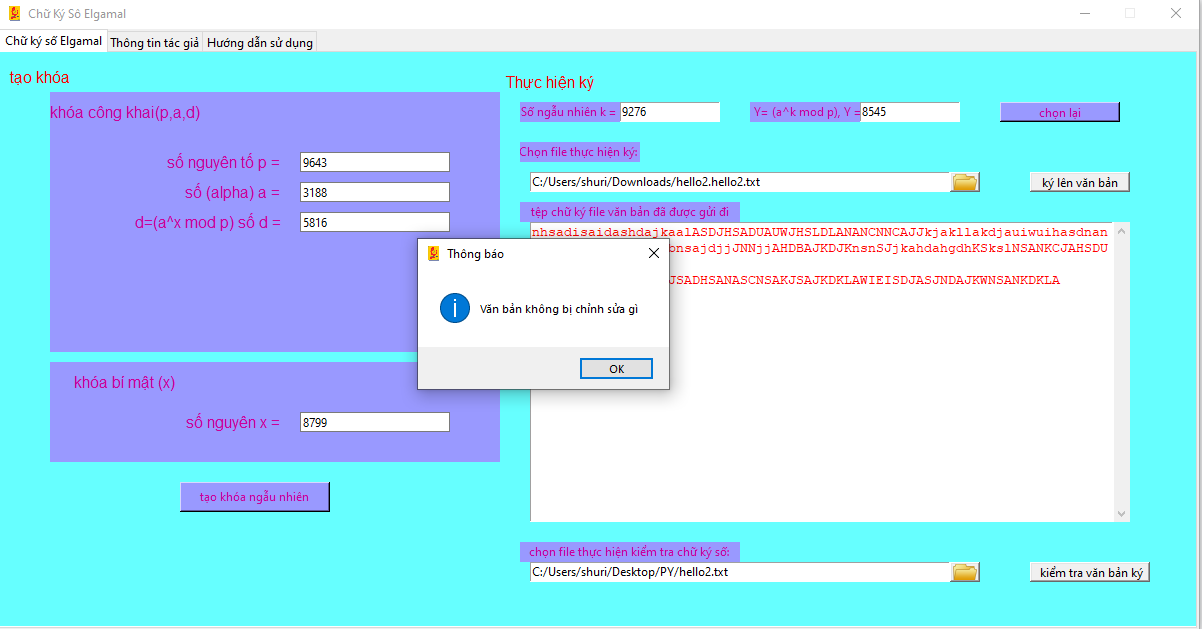
* Chương trình tạo bởi ngôn ngữ Python
  + Giao diện chính



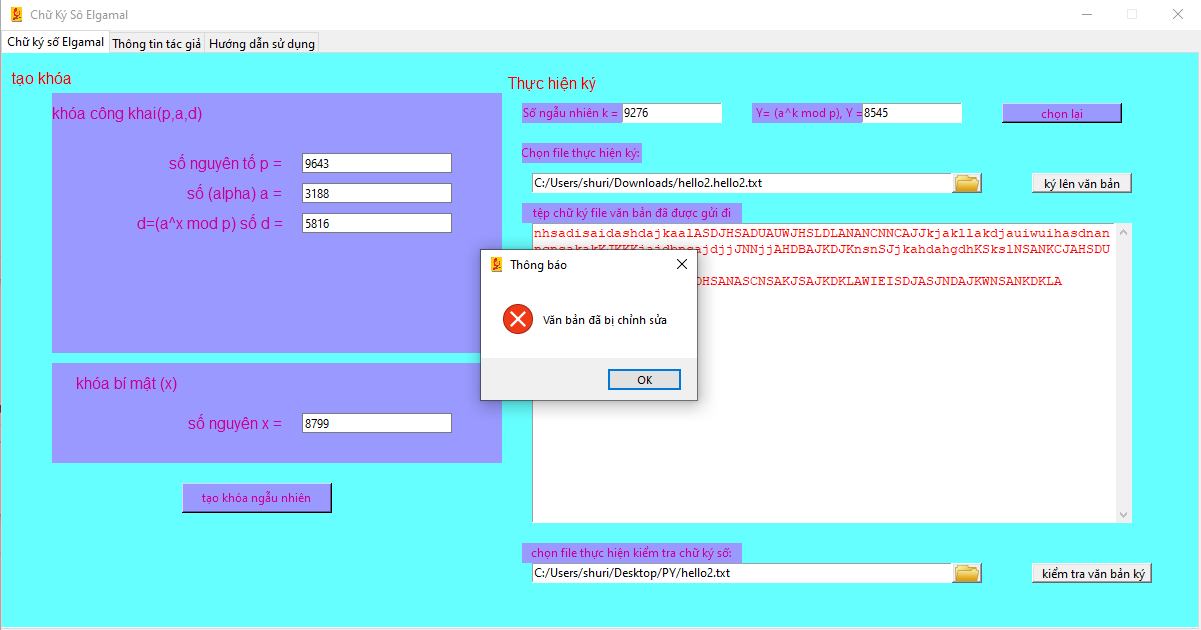
* + Giao diện sau khi ký thành công văn bản



* + Giao diện sau khi văn bản được kiểm tra vẫn nguyên vẹn chưa bị chỉnh sửa



* + Giao diện sau khi văn bản được kiểm tra đã bị chỉnh sửa



## **2.4 Cài đặt và phát triển**

**2.4.1 Phần chương trình viết bằng ngôn ngữ Csharp**

**2.4.1.1 Trình bày tóm tắt công cụ triển khai chương trình đề mô sử dụng trong để tài**

Visual Studio là một trong những công cụ hỗ trợ lập trình nổi tiếng và phổ biến nhất hiện nay của Microsoft, chưa có một phần mềm nào có thể thay thế được nó. Visual Studio được viết bằng 2 ngôn ngữ đó chính là C# và VB+

Visual Studio là một phần mềm lập trình hệ thống được sản xuất trực tiếp từ Microsoft. Từ khi ra đời đến nay, Visual Studio đã có rất nhiều các phiên bản sử dụng khác nhau. Điều đó, giúp cho người dùng có thể lựa chọn được phiên bản tương thích với dòng máy của mình cũng như cấu hình sử dụng phù hợp nhất.

Một số tính năng của phần mềm Visual Studio:

* Biên tập mã: Giống như bất kỳ một IDE khác, Visual Studio gồm có một trình soạn thảo mã hỗ trợ tô sáng cú pháp và hoàn thiện mả bằng cách sử dụng IntelliSense không chỉ cho các hàm, biến và các phương pháp mà còn sử dụng cho các cấu trúc ngôn ngữ như: Truy vấn, vòng điều khiển, …
* Trình gỡ lỗi: Visual Studio có một trình gỡ lỗi có tính năng vừa lập trình gỡ lỗi cấp máy và gỡ lỗi cấp mã nguồn. Tính năng này hoạt động với cả hai mã quản lý giống như ngôn ngữ máy và có thể sử dụng để gỡ lỗi các ứng dụng được viết bằng các ngôn ngữ được hỗ trợ bởi Visual Studio.
* Thiết kế:
  + Windows Forms Designer: Được sử dụng với mục đích xây dựng GUI xây dựng Windows Forms, được bố trí dùng để xây dựng các nút điều khiển, các điều hướng các sự kiện. Có thể được liên kết với các nguồn dữ liệu, các loại cơ sở dữ liệu khác nhau như: SQL server, Mysql, Mongo , …
  + WPF Designer: Tính năng này cũng giống như Windows Forms Designer có công dụng hỗ trợ kéo và thả để tạo ra giao diện. Hỗ trợ mạnh mẽ thao tác của lập trình viên với máy tính, giữa người dùng IDE và máy tính.
  + Web designer/development: Visual Studio cũng có một trình soạn thảo và thiết kế website cho phép các trang web được thiết kế theo tính năng kéo và thả đối tượng. Mục đích là để hỗ trợ người dùng tạo trang web dễ dàng hơn, những yêu cầu đơn giản như thiết kế website du lịch hay các trang giới thiệu của công ty có thể sử dụng tính năng này vì nó vẫn đảm bảo cho bạn sở hữu được một website hoàn chỉnh.
* Điểm mạnh khi sử dụng Visual Studio:
  + Visual Studio hỗ trợ lập trình trên nhiều ngôn ngữ như: C/C++, C#, F#, Visual Basic, HTML, CSS, JavaScript, ....
  + Là một công cụ hỗ trợ việc Debug một cách dễ dàng và mạnh mẽ như: Breakpoint, xem giá trị của biến trong quá trình chạy, hỗ trợ debug từng câu lệnh.
  + Giao diện Visual Studio rất dễ sử dụng đối với người mới bắt đầu lập trình, có thể dễ dàng học được cách sử dụng Visual Studio
  + Visual Studio hỗ trợ phát triển các ứng dụng: Desktop MFC, Windows Form, Universal App, ứng dụng mobile Windows Phone 8/8.1, Windows 10, …
  + Visual Studio hỗ trợ xây dựng ứng dụng một cách chuyên nghiệp bằng các công cụ kéo thả.
  + Visual Studio được đông đảo lập trình viên trên thế giới sử dụng.
  + Nhờ có đông đảo người sử dụng nên khi gặp các lỗi liên quan có thể dễ dàng tìm được cách sửa chữa và tiếp tục làm việc

**2.4.1.2 Hướng dẫn cài đặt và chạy chương trình demo**

* Tải Visual Studio Community tại [<https://visualstudio.microsoft.com/>]
* Tiến hành cài đặt Visual Studio với các Plug in của C# (.NET desktop development)
* Sau khi hoàn tất, mở Visual Studio và chọn Open Project…
* Nhấn run (Local Windows Debugger)

**2.4.2 Phần chương trình viết bằng ngôn ngữ Python**

**2.4.2.1 Trình bày tóm tắt công cụ triển khai chương trình đề mô sử dụng**

**Visual Studio Code** là một trình biên tập mã được phát triển bởi [Microsoft](https://vi.wikipedia.org/wiki/Microsoft) dành cho [Windows](https://vi.wikipedia.org/wiki/Microsoft_Windows), [Linux](https://vi.wikipedia.org/wiki/Linux) và [macOS](https://vi.wikipedia.org/wiki/MacOS). Nó hỗ trợ chức năng debug, đi kèm với [Git](https://vi.wikipedia.org/wiki/Git_(ph%E1%BA%A7n_m%E1%BB%81m)), có syntax highlighting, tự hoàn thành mã thông minh, [snippets](https://vi.wikipedia.org/w/index.php?title=Snippets&action=edit&redlink=1), và [cải tiến mã nguồn](https://vi.wikipedia.org/wiki/C%E1%BA%A3i_ti%E1%BA%BFn_m%C3%A3_ngu%E1%BB%93n). Nó cũng cho phép tùy chỉnh, do đó, người dùng có thể thay đổi theme, phím tắt, và các tùy chọn khác. Nó miễn phí và là [phần mềm mã nguồn mở](https://vi.wikipedia.org/wiki/Ph%E1%BA%A7n_m%E1%BB%81m_t%E1%BB%B1_do_ngu%E1%BB%93n_m%E1%BB%9F), mặc dù gói tải xuống chính thì là [có giấy phép](https://vi.wikipedia.org/wiki/Ph%E1%BA%A7n_m%E1%BB%81m_s%E1%BB%9F_h%E1%BB%AFu_%C4%91%E1%BB%99c_quy%E1%BB%81n).

**Visual Studio Code** được dựa trên [Electron](https://vi.wikipedia.org/wiki/Electron), một nền tảng được sử dụng để triển khai các ứng dụng [Node.js](https://vi.wikipedia.org/wiki/Node.js) máy tính cá nhân chạy trên động cơ bố trí Blink. Mặc dù nó sử dụng nền tảng Electron nhưng phần mềm này không phải là một bản khác của [Atom](https://vi.wikipedia.org/wiki/Atom), nó thực ra được dựa trên trình biên tập của [Visual Studio Online](https://vi.wikipedia.org/wiki/Microsoft_Visual_Studio) (tên mã là "Monaco").

Trong cuộc khảo sát vào năm 2018 trên Stack Overflow, Visual Studio Code được xếp hạng là trình biên tập mã phổ biến nhất, với 34.9% của 75398 người trả lời tuyên bố sử dụng nó.

Một số tính năng của **Visual Studio Code**:

* Visual Studio Code là một trình biên tập mã. Nó hỗ trợ nhiều ngôn ngữ và chức năng tùy vào ngôn ngữ sử dụng theo như trong bảng sau. Nhiều chức năng của Visual Studio Code không hiển thị ra trong các menu tùy chọn hay giao diện người dùng. Thay vào đó, chúng được gọi thông qua khung nhập lệnh, hoặc qua một tập tin



Visual Studio Code có thể được mở rộng qua [plugin](https://vi.wikipedia.org/wiki/Plugin). Điều này giúp bổ sung thêm chức năng cho trình biên tập và hỗ trợ thêm ngôn ngữ. Một tính năng đáng chú ý là khả năng tạo phần mở rộng để phân tích mã, như là các linter và công cụ phân tích, sử dụng [Language Server Protocol](https://vi.wikipedia.org/w/index.php?title=Language_Server_Protocol&action=edit&redlink=1).

**2.4.2.2 Hướng dẫn cài đặt và chạy chương trình demo**

* Tải Visual studio code tại: <https://code.visualstudio.com/Download>
* Tiến hành cài đặt Visual studio code với các Extension cần thiết như Python và thiết lập môi trường Python
* Sau khi hoàn tất mở visual studio code và chọn open project hoặc có thể kéo thả thư mục chứa code cần thực thi vào biểu tượng của Visual studio code
* Nhấn Run => Start Debugging hoặc F5 để chạy chương trình

## **2.5 Thực hiện bài toán**

**2.5.1 Phân công công việc**

Các chức năng chính :

* Hàm sinh khóa random ra khóa công khai, khóa bí mật và số nguyên k
* Thêm file .txt cần ký và thực hiện ký
* Kiểm tra chữ ký cần thêm file cần kiểm tra và file chữ ký

|  |  |  |
| --- | --- | --- |
| **Tên sinh viên** | **Tên công việc** | |
| **Nội dung tìm hiểu** | **Ngôn ngữ demo** |
| Chu Phương Nam | Tìm hiểu phương pháp mã hóa bất đối xứng ứng dụng trong chữ ký điện tử | CSharp |
| Hoàng Văn Mạnh | Chữ ký điện tử và chữ ký điện tử Elgamal | Python |

# **Chương 3 : Phần kiến thức lĩnh hội và bài học kinh nghiệm**

## **3.1 Nội dung đã thực hiện**

Các kết quả chính đạt được của đề tài:

a. Về lý thuyết:

\* **Lĩnh hội được cơ sở lý thuyết của chữ ký điện tử về khái niệm, tính pháp lý ứng dụng thực tiễn của chữ ký điện tử từ đó có thể rút ra được ưu và nhược điểm:**

* Ưu điểm:
  + Sử dụng chữ ký điện tử bảo đảm tính pháp lý của các giao dịch điện tử, cho phép các giao dịch có thể thực hiện trong môi trường điện tử.
  + Chữ ký điện tử và thực hiện những giao dịch điện tử cho phép tiết kiệm thời gian, sức lực và tăng hiệu quả lao động.
  + Ngăn chặn khả năng giả mạo chữ ký
  + Ngăn chặn khả năng làm giả tài liệu. Sau khi tài liệu đã ký bằng chữ ký điện tử thì không thể thay đổi, Bất cứ sự thay đổi nào của văn bản dù nhỏ nhất cũng có thể bị phát hiện chữ ký điện tử được tạo ra bởi hệ cặp khóa bí mật và công khai, khi nội dung thay đổi khóa công khai sẽ không còn tương thích với khóa bí mật hay nói cách khác, người nhận sẽ không thể dùng khóa công khai để giải mã.
* Nhược điểm:
  + Tính bảo mật có thể bị đe dọa: Trở ngại lớn nhất khi sử dụng chữ ký số là khả năng tách biệt khỏi chủ nhân, hay chủ nhân của chữ ký không phải là duy nhất. Tồn tại một số đối tượng có thể có được mật mã, đó là bộ phận cung cấp phần mềm, bộ phận cài đặt phần mềm, ngoài ra với sự phát triển của máy tính tốc độ xử lý cao việc giải ngược các bài toán ký số là có thể và đó có thể đánh cắp được mật mã
  + Sự cố thời hạn của chữ ký điện tử: Chữ ký điện tử là chương trình phần mềm được cấp có thời hạn sử dụng. Về lý thuyết văn bản có hiệu lực pháp lý trong thời hạn của chữ ký. Tuy nhiên, thực tế hiệu lực pháp lý của văn bản hoàn toàn có thể bị nghi ngờ khi chữ ký hết hạn sử dụng

**\* Lĩnh hội về chữ ký số Elgamal, hiểu rõ nguyên tắc sinh khóa ký số và phương pháp để kiểm tra chữ ký, nắm bắt rõ những thuật toán có để xử lý như thuật toán sinh khóa từ đó rút ra những được ưu và nhược điểm:**

**\* Hiểu và ứng dụng hàm băm SHA trong việc ký và xác nhận chữ ký điện tử, thấy được vai trò ứng dụng của hàm băm:**

**Hàm băm (Hash function) là giải thuật nhằm sinh ra các giá trị** băm tương ứng với mỗi khối dữ liệu (có thể là một chuỗi ký tự, một đối tượng trong lập trình hướng đối tượng, v.v...)

Giá trị băm đóng vai trò gần như một khóa để phân biệt các khối dữ liệu. Tuy nhiên vẫn có hiện tượng trùng khóa hay còn gọi làđụng đô và cố gắng cải thiện giải thuật để giảm thiểu sựđụng độ đó

SHA (Secure Hash Algorithm hay Thuật giải băm an toàn) là nămthuật giải được chấp nhận bởiFIFS (Tổ chức tiêu chuẩn xử lý thông tin liên bang) dùng để chuyển một đoạn dữ liệu nhất định thành một đoạn dữ liệu có chiều dài không đổi với xác suất khác biệt cao

***\*Ứng dụng hàm băm***

* Tạo khóa bí mật từ mật khẩu
* Kiểm tra tính toàn vẹn dữ liệu
* HMAC (mã chứng thực thông điệp sử dụng hàm băm)
* Chữ ký điện tử.
* Xác thực thông điệp :

Một ứng dụng điển hình của một hàm băm mật mã học như sau: Alice đưa cho Bob một câu đố khó và tuyên bố rằng cô ấy đã giải được rồi. Bob muốn tự giải, nhưng cũng muốn chắc chắn là Alice đúng là đã giải được. Do đó, Alice viết đáp án , gắn thêm một nonce ngẫu nhiên, tính giá trị băm của nó, và đưa kết quả băm cho Bob (trong khi vẫn giữ bí mật đáp án và nonce). Bằng cách này, khi Bob tự giải xong, Alice có thể chứng minh rằng cô đã có đáp án từ trước cách đưa nonce cho Bob. Trong thực tiễn, Alice và Bob thường là các chương trình máy tính, và bí mật thường là cái gì đó không dễ lừa bằng một lời giải cho câu đó. Ứng dụng trên được gọi là một hệ thống tin cậy (commitment scheme ) .

Một ứng dụng quan trọng khác của các hàm băm bảo mật là sự kiểm tra tính toàn vẹn của thông điệp . 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 . 6.2 . Chữ ký số Một ứng dụng có liên quan là kiểm tra 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 và so sánh với kết quả băm được lưu trữ . Do các lý do cả về bảo mật và hiệu năng chương trình , đa số các thuật toán chữ ký số nói rằng chỉ có tóm lược của thông điệp , chứ không phải toàn văn thông điệp , được ký " , Các hàm bẵm con có thể được dùng để tạo các bit giả ngẫu nhiên ( pseudorandom ) .

\* **Hiểu phương pháp mã hóa bất đối xứng ứng dụng trong chữ ký điện tử**

Mã hóa bất đối xứng là một loại mã hóa sử dụng hai khóa riêng biệt nhưng có liên quan đến toán học để mã hóa và giải mã dữ liệu.

Khóa công khai mã hóa dữ liệu trong khi khóa riêng tư tương ứng của nó giải mã nó. Đây là lý do tại sao nó còn được gọi là mã hóa khóa công khai, mật mã khóa công khai và mã hóa khóa bất đối xứng. Khóa công khai được mở cho tất cả mọi người.

Bất kỳ ai cũng có thể truy cập và mã hóa dữ liệu bằng nó. Tuy nhiên, sau khi được mã hóa, dữ liệu đó chỉ có thể được mở khóa bằng cách sử dụng khóa riêng tương ứng (khóa bí mật ).

Mã hóa bất đối xứng là một cách để bạn xác minh các bên thứ ba mà bạn chưa từng gặp qua các kênh công khai không an toàn. Không giống như các phương pháp mã hóa đối xứng dựa vào một khóa để mã hóa và giải mã dữ liệu, mã hóa khóa không đối xứng sử dụng hai khóa riêng biệt để thực hiện các chức năng này.

Đây là lý do tại sao mã hóa khóa công khai được coi là một yếu tố quan trọng trong nền tảng của bảo mật Internet. Cơ sở hạ tầng khóa công khai (PKI), một khuôn khổ các chính sách, quy trình và công nghệ giúp bảo mật thông tin liên lạc của bên thứ ba qua Internet. Để làm được điều này, nó dựa vào cả mã hóa bất đối xứng và đối xứng.

Dùng phương pháp mã hóa bất đối xứng khi:

* Cần xác thực các bên
* Cần xác minh tính toàn vẹn của dữ liệu và
* Bảo vệ bản thân, bảo vệ tính bảo mật toàn vẹn của các loại văn bản truyền đi trên không gian mạng Internet
* Trao đổi khóa đối xứng.
* Xử lý phần lớn mã hóa dữ liệu.

Có một số thuật toán phổ biến cho mã hóa bất đối xứng và trao đổi khóa là Diffie-Hellman, RSA, ECDSA, ElGamal và DSA.

Ưu điểm của phương pháp mã hóa bất đối xứng:

* Không cần phải chia sẻ khóa mã hóa mã (khóa bí mật) “một cách bí mật”. Vì vậy người dùng có thể dễ dàng sử dụng hệ thống
* Sử dụng ít khóa hơn hệ mã hóa đối xứng: n phần tử cần sử dụng chỉ cần n khóa thay vì n(n-1)/2 khóa
* An toàn hơn mã hóa đối xứng: Độ phức tạp của bài toán Logarit lớn nên độ an toàn cao. Bên cạnh đó như đã chia sẻ nhiều lần thì việc chia sẻ duy nhất một khóa cho nhiều người gây mất an toàn trong việc bảo mật thông tin của gói thông tin muốn, được chia sẻ
* Giúp việc phân phối tệp tin trở nên dễ dàng: không cần quan tâm đến tín bảo mật của khóa, có thể phân phối số lượng lớn khóa công khai
* Có thể áp dụng sử dụng phương pháp này trong việc tạo chữ ký điện tử

Nhược điểm của phương pháp mã hóa bất đối xứng:

* Tốc độ: Các khóa được tính khá dài, việc này khiến các máy chủ phải tính toán nhiều hơn nhằm đạt được tính bảo mật cao, vì vậy tốc độ chậm hơn so với hệ mã hóa đối xứng
* Dung lượng lưu trữ: yêu cầu dung lượng lưu trữ lớn

b. Về thực nghiệm:

* Xây dựng thư viện tính toán số nguyên lớn, thuật toán ký số dựa trên lược đồ Elgamal.
* Áp dụng hàm băm trong việc rút ngắn độ dài của đoạn văn bản cần ký
* Kỹ năng xử lý những bài toán modulo phức tạp
* Cài đặt chương trình ký số thử nghiệm. Tiến hành thực nghiệm và đánh giá kết quả.

c. Về bài học rút ra:

## **3.2 Hướng phát triển**

Đối với lĩnh vực nghiên cứu của bài tập lớn có thể mở rộng, phát triển theo hướng xây dựng mô hình kiểm soát tính toàn vẹn thông tin và các lược đồ mã hóa khóa công khai, đảm bảo độ an toàn cao và tiên tiến hơn.

Hướng phát triển của đề tài là xây dựng chương trình để có thể kết nối trực tiếp vào một số phần mềm gửi nhận email và phần mềm quản lý văn bản. Đồng thời xây dựng một hệ thống chứng thực khóa công khai cho các thành viên, nhằm tránh trường hợp bị người khác giả mạo khóa công khai của người nhận khi thực hiện trao đổi thông tin.

Tuy còn những hạn chế nhất định, nhưng trong quá trình nghiên cứu, hoàn thành bài tập lớn đã giúp tôi trang bị thêm nhiều kiến thức cơ bản về bảo mật thông tin. Từ đó có thể xây dựng các ứng dụng bảo mật hoàn chỉnh hơn, phục vụ cho việc tham mưu ứng dụng công nghệ thông tin vào công tác quản lý tại đơn vị mình đang công tác.

# 

# 

# 

# **TÀI LIỆU THAM KHẢO**

##### Địa chỉ trên internet

1. [<https://vi.wikipedia.org/>]
2. Tài liệu về mã hóa khóa công khai [<https://sal.vn/L6z3d3>]
3. Tài liệu liên quan hàm băm [<https://sal.vn/Dxnwt9>]
4. Tài liệu liên quan SHA256 [<https://en.bitcoinwiki.org/wiki/SHA-256>]
5. Tài liệu về mã hóa Elgamal [https://sal.vn/tYwJA3] [<https://en.wikipedia.org/wiki/ElGamal_encryption>]
6. Tìm hiểu về hàm băm SHA và các phiên bản SHA thường dùng  
   [ssl.vn/tim-hieu-ve-sha-va-cac-phien-ban-sha-thuong-dung.html]
7. Phân biệt hệ mật mã đối xứng và bât đối xứng [https://sal.vn/7JYCuD]