Shape

Description automatically generated

TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI

KHOA CÔNG NGHỆ THÔNG TIN

......ooꞶoo......



**BÀI TẬP LỚN**

**Môn: An toàn và bảo mật thông tin**

**Đề tài: Tìm hiểu về chữ ký điện tử Elgamal và viết ứng dụng minh họa**

Giảng viên hướng dẫn: ***ThS. Trần Phương Nhung***

Lớp: **20214IT6001001**

Nhóm 4 Ngô Quang Đồng - 2019603167

Hoàng Trần Minh Đức - 2019606723

Trần Văn Đức - 2019606889

Phạm Văn Dung - 2019601870

Nguyễn Mạnh Dũng - 2020606903

**Hà Nội – 2022**

**MỤC LỤC**

[CHƯƠNG 1. TỔNG QUAN 2](#_Toc113544913)

[1.1 Tóm lược ý tưởng và đề tài nghiên cứu 2](#_Toc113544914)

[1.2 Chữ ký điện tử Elgamal 5](#_Toc113544915)

[1.3 Phương pháp mã hoá bất đối xứng 8](#_Toc113544916)

[1.3.1 Mã hoá bất đối xứng là gì? 8](#_Toc113544917)

[1.3.2 Cách hoạt động của mã hoá bất đối xứng 8](#_Toc113544918)

[1.3.3 Ứng dụng của mã hoá bất đối xứng 9](#_Toc113544919)

[1.3.4 So sánh mã hóa bất đối xứng và mã hóa đối xứng 9](#_Toc113544920)

[1.4 Hàm băm SHA 10](#_Toc113544921)

[1.4.1 Định nghĩa 10](#_Toc113544922)

[1.4.2 Ứng dụng của hàm băm 13](#_Toc113544923)

[CHƯƠNG 2. KẾT QUẢ NGHIÊN CỨU 15](#_Toc113544924)

[2.1 Giới thiệu 15](#_Toc113544925)

[2.2 Nội dung thuật toán 16](#_Toc113544926)

[2.3 Thiết kế cài đặt chương trình demo thuật toán 16](#_Toc113544927)

[2.3.1. Giao diện chương trình đề mô 17](#_Toc113544928)

[2.4 Cài đặt và triển khai 19](#_Toc113544929)

[2.5 Thực hiện bài toán 20](#_Toc113544930)

[2.5.1 Phân công công việc 20](#_Toc113544931)

[2.5.2 Ngô Quang Đồng – Tạo khóa (Đã trình bày ở trên) 20](#_Toc113544932)

[2.5.3 Trần Văn Đức – Ký văn bản 20](#_Toc113544933)

[2.5.4 Hoàng Trần Minh Đức– Xác nhận văn bản 22](#_Toc113544934)

[2.5.5 Phạm Văn Dung- Kiểm tra sự toàn vẹn của tài liệu/văn bản 23](#_Toc113544935)

[2.5.6 Nguyễn Mạnh Dũng- Thuật toán 23](#_Toc113544936)

[CHƯƠNG 3. KIẾN THỨC LĨNH HỘI VÀ BÀI HỌC KINH NGHIỆM 24](#_Toc113544937)

[3.1 Nội dung đã thực hiện 24](#_Toc113544938)

[3.1.1 Nội dung học được thông qua thực hiện bài tập lớn 24](#_Toc113544939)

[3.1.2 Bài học kinh nghiệm được rút ra sau khi kết thúc bài tập lớn 25](#_Toc113544940)

[3.2 Hướng phát triển 26](#_Toc113544941)

[3.2.1 Tính khả thi của chủ đề nghiên cứu 26](#_Toc113544942)

[3.2.2 Những thuận lợi, khó khăn trong quá trình nghiên cứu 27](#_Toc113544943)

[3.2.2 Hướng phát triển và mở rộng của đề tài 27](#_Toc113544944)

**Lời nói đầu**

Ngày nay với sự xuất hiện của máy tính, các tài liệu văn bản giấy tờ và các thông tin quan trọng đều được số hóa và xử lý trên máy tính, được truyền đi trong một môi trường mà mặc định là không an toàn. Do đó yêu cầu về việc có một cơ chế, giải pháp để bảo vệ sự an toàn và bí mật của các thông tin nhạy cảm, quan trọng ngày càng trở nên cấp thiết.

Mật mã học chính là ngành khoa học đảm bảo cho mục đích này. Khó có thể thấy một ứng dụng Tin học có ích nào lại không sử dụng các thuật toán mã hóa thông tin. Chính vì nhu cầu cần thiết của mã hóa thông tin, nên nhóm em cùng với sự hướng dẫn của cô Trần Phương Nhung đã tìm hiểu về “Nghiên cứu hệ mật Elgamal và ứng dụng trong chữ ký số”. Chính vì vậy độ an toàn và khả năng ứng dụng của hệ Elgamal trong mã hóa thông tin cũng rất cao và ổn định.

Mặc dù đã cố gắng để hoàn thiện đề tài tốt nhất có thể, nhưng chắc chắn không thể tránh khỏi những thiếu sót. Nhóm em rất mong nhận được sự góp ý của thầy cô và các bạn để đồ án tốt nghiệp của em được hoàn thiện hơn.

*Xin chân thành cảm ơn!*

# 

# CHƯƠNG 1. TỔNG QUAN

## 1.1 Tóm lược ý tưởng và đề tài nghiên cứu

Kể từ khi con người phát minh ra chữ viết, các chữ ký thường luôn được sử dụng hàng ngày, chẳng hạn như ký một biên nhận trên một bức thư nhận tiền từ ngân hàng, ký hợp đồng hay một văn bản bất kỳ nào đó. Chữ ký viết tay thông thường trên tài liệu thường được dùng để xác định người ký nó.

Sơ đồ chữ ký điện tử là một phương pháp ký một văn bản hay lưu bức điện dưới dạng điện tử. Chẳng hạn một bức điện có chữ ký được lưu hành trên mạng máy tính. Chữ ký điện tử từ khi ra đời đã có nhiều ứng dụng rộng rãi trong các giao dịch thương mại, từ việc xác minh chữ ký cho đến các thẻ tín dụng, các sơ đồ định danh và các sơ đồ chia sẻ bí mật… Sau đây, chúng ta sẽ tìm hiểu một số sơ đồ chữ ký quan trọng. Song trước hết, chúng ta sẽ thảo luận một vài điểm khác biệt cơ bản giữa chữ ký thông thường và chữ ký điện tử.

Đầu tiên là vấn đề ký một tài liệu. Với chữ ký thông thường nó là một phần vật lý của tài liệu. Tuy nhiên, một chữ ký điện tử không gắn theo kiểu vật lý vào bức điện nên thuật toán được dùng phải là “không nhìn thấy” theo cách nào đó trên bức điện.

Thứ hai là vấn đề kiểm tra. Chữ ký thông thường được kiểm tra bằng cách so sánh nó với chữ ký xác thực khác. Ví dụ, ai đó ký một tấm séc để mua hàng, người bán sẽ so sánh chữ ký trên mảnh giấy đó với chữ ký nằm ở mặt sau thẻ tín dụng để kiểm tra. Mặt khác, chữ ký số có thể kiểm tra bằng một thuật toán kiểm tra một cách công khai. Như vậy, bất kỳ ai cũng cũng có thể kiểm tra được chữ ký điện tử. Việc sử dụng một sơ đồ ký an toàn có thể ngăn chặn được khả năng giả mạo. Sự khác biệt cơ bản giữa chữ ký điện tử và chữ ký thông thường là ở chỗ: một bản copy tài liệu có chữ ký được đồng nhất với bản gốc. Nói cách khác, tài liệu có chữ ký trên giấy thường có thể khác biệt với bản gốc điều này để ngăn chặn một bức điện được ký khỏi bị dùng lại. Ví dụ, nếu B ký một bức điện xác minh cho A rút 100$ từ tài khoản của mình, anh ta chỉ muốn A có khả năng làm điều đó một lần. Vì thế, bản thân bức điện phải chứa thông tin để khỏi dùng lại, chẳng hạn như dùng dịch vụ gán nhãn thời gian (Time Stamping Service).

Một sơ đồ chữ ký điện tử thường chứa hai thành phần: thuật toán ký sig () và thuật toán xác minh ver (). B có thẻ ký một bức điện x dùng thuật toán ký an toàn (bí mật). Kết quả chữ ký y = sig(x) nhận được có thể được kiểm tra bằng thuật toán xác minh công khai ver(y). Khi cho trước cặp (x, y), thuật toán xác minh cho giá trị TRUE hay FALSE tùy thuộc vào việc chữ ký được xác định như thế nào.

Vậy thế nào là chữ ký điện tử? Chúng ta có một số định nghĩa như sau:

* Là một định danh điện tử được tạo ra bởi máy tính được các tổ chức sử dụng nhằm đạt được tính hiệu quả và có hiệu lực như là các chữ ký tay.
* Là một cơ chế xác thực hóa cho phép người tạo ra thông điệp đính kèm một mã số vào thông điệp giống như là việc ký một chữ ký lên văn bản bình thường.

Các chữ ký điện tử được sinh và sử dụng bởi các hệ chữ ký (sơ đồ) điện tử, dưới đây là định nghĩa một hệ chữ ký điện tử.

**Định nghĩa:**

Một sơ đồ chữ ký điện tử là 5 bộ (P, A, K, S, V) thỏa mãn các điều kiện dưới đây:

1. P là tập hữu hạn các bức điện (thông điệp, bản rõ) có thể.
2. A là tập hữu hạn các chữ ký có thể.
3. K là tập không gian khóa (tập hữu hạn các khóa có thể).
4. Với mỗi khóa K ∈ k tồn tại một thuật toán sigk ∈ s và một thuật toán xác minh verk ∈ v. Mỗi sigk: P -> A {TRUE, FALSE} là những hàm sao cho mỗi bức điện x ∈ P và mỗi chữ ký y ∈ A thỏa mãn phương trình dưới đây.

Ver (x, y) = { TRUE nếu y = sig(x) FALSE nếu y # sig(x)

Với mỗi K ∈ k, hàm sigk và verk là các hàm đa thức thời gian. Hàm verk sẽ là hàm công khai còn hàm sigk là bí mật. Không thể dễ dàng tính toán để giả mạo chữ ký của B trên bức điện x, nghĩa là với x cho trước chỉ có B mới có thể tính được y để ver (x, y) = TRUE. Một sơ đồ chữ ký không thể an toàn vô điều kiện vì một người C nào đó có thể kiểm tra tất cả chữ số y trên bức điện x nhờ dùng thuật toán ver () công khai cho tới khi anh ta tìm thấy chữ ký đúng. Vì thế nếu có đủ thời gian, C luôn có thể giả mạo chữ ký của B. Như vậy mục đích của chúng ta là tìm các sơ đồ chữ ký điện tử an toàn về mặt tính toán.

Chú ý rằng ai đó có thể giả mạo chữ ký của B trên một bức điện “ngẫu nhiên” x bằng cách tính x = ek(y) với y nào đó. Khi đó y = sigk(x). Một biện pháp xung quanh vấn đề khó khăn này là yêu cầu các bức điện chứa đủ phần dư để chữ ký giả mạo kiểu này không phù hợp với toàn bộ nội dung của bức điện x trừ một xác suất rất nhỏ. Có thể dùng hàm Băm (hash function) như MD4, MD5 trong việc tính kết nối các sơ đồ chữ ký điện tử sẽ loại phương pháp giả mạo này.

Điều thứ ba là vấn đề sai lầm của người ký khi sử dụng cùng một giá trị k trong việc ký hai bức điện khác nhau. Cho (γ, δ1) là chữ ký trên bức điện x1 và (γ, δ2) là chữ ký trên bức điện x2. Việc kiểm tra sẽ thực hiện:

βγγδ1 ≡ αx1 (mod p) βγγδ2 ≡ αx2 (mod p)

Do đó: αx1-x2 ≡ γ δ1 -δ2 (mod p).

Đặt γ = αk, khi đó: x1 – x2 = k (δ1 -δ2) (mod p – 1).

Bây giờ đặt d = UCLN (δ1 -δ2, p - 1). Vì d | (δ1 -δ2) và d | (p-1) nên nó cũng chia hết cho (x1 – x2). Ta đặt tiếp:

x’ = (x1 – x2)/d

δ’ = (δ1 -δ2)/d

p’ = (p-1)/d

Cuối cùng, ta được: x’ ≡ k δ’ (mod p’). Vì UCLN (δ’, p’) = 1 nên ta có: ɛ = (δ’)-1 mod p’

Như vậy, giá trị k sẽ được xác định như sau:

k = x’ɛ(mod p’) = x’ɛ + ip’ (mod p)

Với 0 <= I <= d – 1, ta có thể tìm được giá trị k duy nhất bằng hàm kiểm tra: γ ≡ αk mod p.

## 1.2 Chữ ký điện tử Elgamal

Hệ chữ ký Elgamal được đưa ra vào năm 1985. Một phiên bản sửa đổi hệ này được Học viện Quốc gia tiêu chuẩn và kỹ thuật (NIST) đưa ra như một chuẩn của chữ ký điện tử. Hệ chữ ký Elgamal được thiết kế riêng biệt cho mục đích chữ ký, trái ngược với RSA thường được sử dụng cho cả mục đích mã hóa công khai và chữ ký. Hệ chữ ký Elgamal là không xác định, nghĩa là có rất nhiều giá trị chữ ký cho cùng một bức điện cho trước. Thuật toán xác minh phải có khả năng nhận bất kỳ giá trị chữ ký nào như là việc xác thực. Sơ đồ chữ ký Elgamal được miêu tả như sau:

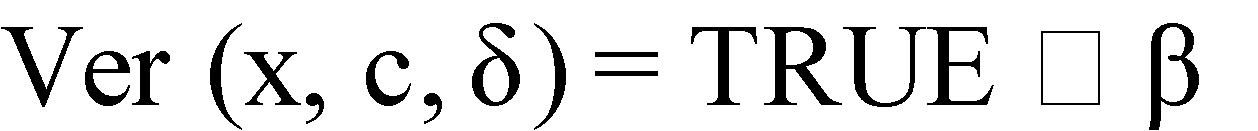
Cho p là một số nguyên tố như là bài toán logarit rời rạc trong Zp, α ∈ Zp\* là một phần tử nguyên và P = Zp\*, A = (Zp\*) \*Zp-1, và định nghĩa:

K = {(p, α, a, β) : β ≡ αa (mod p)} trong đó giá trị p, α và β là công khai, còn a là bí mật.

Với K={p, α, a, β } và chọn ngẫu nhiên k ∈ Zp-1 \* ,định nghĩa: sigk(x,k)=(γ,δ) trong đó: γ= αk mod

δ = (x – a\* γ) k-1 mod (p - 1).

Với x, γ ∈ Zp\* và δ ∈ Zp-1, định nghĩa:

γ γδ ≡ αx (mod p).

Nếu chữ ký là đúng thì việc xác nhận thành công khi:

βγ γδ ≡ αaγ αkδ (mod p)

≡ αx (mod p).

Trong đó: aγ + kδ ≡ x (mod p-1).

B sẽ tính toán chữ ký bằng việc sử dụng cả giá trị bí mật a (một phần của khóa) và số bí mật ngẫu nhiên k (giá trị để ký bức điện). Việc xác minh có thể thực hiện được chỉ với các thông tin được công khai:

Ví dụ:

Chúng ta chọn p = 467, α = 2, a = 127. Ta tính: β = αa mod p = 2127 mod 467 = 132. Bây giờ B muốn ký lên bức điện x = 100 và anh ta chọn một giá trị ngẫu nhiên k= 213 (chú ý là UCLN (213, 466) = 1 và 213-1 = mod 466 = 431). Sau đó tính:

γ = 2213 mod 467 = 29

δ = (100 – 127\*29)431 mod 466 = 51.

Bất cứ ai cũng có thể kiểm tra chữ ký này bằng cách tính: 132292951 ≡ 189 (mod 467) 2100 ≡ 189 (mod 467).

Giả sử kẻ thứ ba C muốn giả mạo chữ ký của B trên bức điện x mà không biết số bí mật a. Nếu C chọn một giá trị γ và cố gắng tìm δ, anh ta phải tính một hàm logarit rời rạc logγ αx β

γ. Mặt khác, nếu đầu tiên anh ta chọn δ để cố gắng tìm γ thì anh ta phải tính βγ γδ = αx (mod p). Cả hai việc này đều không thể thực hiện được.

Tuy nhiên có một lý thuyết mà C có thể ký tên lên một bức điện ngẫu nhiên bằng cách chọn đồng thời γ, δ và x. Cho i, j là số nguyên với 0 <=i, j <= p-2, và UCLN (j, p-1) = 1. Sau đó tính:

γ = αi βj mod p

δ = - γj-1 (mod p-1)

x = - γij-1 (mod p-1).

Như vậy, ta xem (γ, δ) là giá trị chữ ký cho bức điện x. Việc xác minh thực sẽ thực hiện như sau:

βγ γδ ≡ βα^i β^j (αi βj)- α^i.β^j.j^-1 (mod p)

≡ βα^i β^j α-ij α^i β^j β-α^i β^j (mod p)

≡ α-ij α^i β^j

≡ α-γij^-1 (mod p)

≡ αx (mod p).

Ví dụ:

Như ví dụ trên, ta chọn p = 467, α = 2, β = 132. Kẻ thứ ba C sẽ chọn i = 99 và j = 179. Anh ta sẽ tính:

γ = 299132179 mod 467 = 117 δ = -117\*151 mod 466 = 41 x = 99\*44 mod 466 = 331

Cặp giá trị (117, 41) là giá trị chữ ký cho bức điện 331. Việc xác minh được thực hiện như sau:

13211711741 ≡ 303 (mod 467)

2331 ≡ 303 (mod 467).

Một phương pháp thứ hai có thể giả mạo chữ ký là sử dụng lại chữ ký của bức điện trước đó, nghĩa là với cặp (γ, δ) là giá trị chữ ký của bức điện x, nó sẽ được C ký cho nhiều bức điện khác. Cho h, i, j là các số nguyên, trong đó 0 <= i, j, h <= p – 2 và UCLN (hγ – jδ, p – 1) = 1.

λ = γh αi βj mod p

µ = δλ(hγ – jδ)-1 mod (p – 1)

x’ = λ(hx + iδ)(hγ - jδ)-1 mod (p – 1).

Ta có thể kiểm tra βλ λµ = αx’mod p. và do đó, (λ, µ) là cặp giá trị chữ ký của bức điện x’.

## 1.3 Phương pháp mã hoá bất đối xứng

### 1.3.1 Mã hoá bất đối xứng là gì?

Hệ thống mã hóa bất đối xứng (Asymmetric cryptosystem) là hệ thống mã hóa sử dụng một khóa công khai (public key) và một khóa bí mật (private key) cho quá trình mã hóa và giải mã.

Hệ thống mã hóa bất đối xứng còn được gọi là hệ thống mã hóa khóa công khai (public-key cryptosystem)

### 1.3.2 Cách hoạt động của mã hoá bất đối xứng

Mã hóa không đối xứng sử dụng một cặp khóa liên quan đến toán học để mã hóa và giải mã: khóa công khai và khóa riêng tư. Nếu khóa công khai được sử dụng để mã hóa, thì khóa cá nhân liên quan được sử dụng để giải mã; nếu khóa riêng tư được sử dụng để mã hóa, thì khóa công khai liên quan được sử dụng để giải mã.

Hai người tham gia vào quy trình mã hóa bất đối xứng là người gửi và người nhận; mỗi khóa có cặp khóa công khai và khóa riêng. Đầu tiên, người gửi nhận được khóa công khai của người nhận. Tiếp theo, bản rõ - hoặc văn bản thông thường, có thể đọc được - được mã hóa bởi người gửi bằng khóa công khai của người nhận; điều này tạo ra bản mã. Sau đó, bản mã được gửi đến người nhận, người sẽ giải mã bản mã bằng khóa riêng của họ và trả nó về bản rõ dễ đọc.

Do tính chất một chiều của chức năng mã hóa, một người gửi không thể đọc tin nhắn của người gửi khác, mặc dù mỗi người đều có khóa công khai của người nhận.

### 1.3.3 Ứng dụng của mã hoá bất đối xứng

Mật mã không đối xứng thường được sử dụng để xác thực dữ liệu bằng chữ ký số. Chữ ký điện tử là một kỹ thuật toán học được sử dụng để xác nhận tính xác thực và tính toàn vẹn của một thông điệp, phần mềm hoặc tài liệu kỹ thuật số. Nó là dạng kỹ thuật số tương đương với chữ ký viết tay hoặc con dấu có đóng dấu.

Dựa trên mật mã không đối xứng, chữ ký điện tử có thể cung cấp bằng chứng đảm bảo về nguồn gốc, danh tính và trạng thái của một tài liệu, giao dịch hoặc thông điệp điện tử, cũng như xác nhận sự đồng ý của người ký.

Mật mã không đối xứng cũng có thể được áp dụng cho các hệ thống trong đó nhiều người dùng có thể cần mã hóa và giải mã các thông điệp, bao gồm:

Email được mã hóa - một khóa công khai có thể được sử dụng để mã hóa một tin nhắn và một khóa riêng tư có thể được sử dụng để giải mã nó.

Các giao thức mật mã SSL / TSL - thiết lập các liên kết được mã hóa giữa các trang web và trình duyệt cũng sử dụng mã hóa không đối xứng.

### 1.3.4 So sánh mã hóa bất đối xứng và mã hóa đối xứng

|  |  |
| --- | --- |
| **Mã hóa đối xứng** | **Mã hóa không đối xứng** |
| Mã hóa đối xứng bao gồm một khóa để mã hóa và giải mã | Mã hóa không đối xứng bao gồm hai khóa mật mã được gọi là khóa công khai và khóa cá nhân. |
| Mã hóa đối xứng nhanh hơn rất nhiều so với phương pháp không đối xứng | Vì mã hóa không đối xứng kết hợp hai khóa riêng biệt, quá trình này bị chậm lại đánh kể. |
| RC4 | RSA |
| AES | Diffie – Hellman |
| DES | ECC |
| 3DES | ElGamal |
| QUAD | DSA |

## 1.4 Hàm băm SHA

### 1.4.1 Định nghĩa

SHA được thiết kế dựa trên những nguyên tắc của MD4/MD, tạo ra 160-bit giá trị Băm.

A, Miêu tả SHA

Cũng giống như với MD5, bức điện được cộng thêm một bit 1 và các bit 0 ở cuối bức điện để bức điện có thể chia hết cho 512. SHA sử dụng 5 thanh ghi dịch:

A = 0x67452301

B = 0xefcdab89 C = 0x98badcfe D= 0x10325476

E = 0xc3d2e1f0

Bức điện được chia ra thành nhiều khối 512-bit. Ta cũng đặt là a, b, c, d, e thay cho A, B, C, D, E đối với khối 512-bit đầu tiên của bức điện. SHA có bốn vòng lặp chính trong 5 giá trị a, b, c, d và e, sau đó cũng được cộng và dịch như trong MD5.

SHA xác lập bốn hàm phi tuyến như sau:

ft (X, Y, Z) = (X ∧ Y) V ((¬X) ∧ Z) với 0 <= t <= 19 ft (X, Y, Z) = X Y Z với 20 <= t <= 39

ft (X, Y, Z) = (X ∧ Y) V (X ∧ Z) V (Y ∧ Z) với 40 <=t <= 59 ft (X, Y, Z) = X Y Z với 60 <= t <=79.

Bốn hằng số sử dụng trong thuật toán là:

Kt = 21/2/4 = 0x5a827999 với 0 <= t <= 19

Kt = 31/2/4 = 0x6ed9eba1 với 20 <= t <=39 Kt = 51/2/4 = 0x8f1bbcdc với 40 <=t <=59 Kt = 101/2/4 = 0xca62c1d6 với 60 <=t <= 79.

Các khối bức điện được mở rộng từ 16word đến 32-bit (M0 đến M15) thành 80 word 32-bit (W0 đến W79) bằng việc sử dụng thuật toán mở rộng:

Wt = Mt với 0 <= t <= 15

Wt = (Wt-3 Wt-8 Wt-16) với 16 <= t <= 79. Ta có thể miêu tả một vòng lặp của SHA như sau:

Diagram, schematic

Description automatically generated

*Sơ đồ một vòng lặp của SHA*

Nếu gọi Wt là biểu diễn của khối con thứ t của bức điện được mở rộng, và <<<s là biểu diễn dịch trái s bit, thì vòng lặp chính của SHA như sau:

a = A, b = B, c = C, d = D, e = E,

for t = 0 to 79

{

TEMP = (a <<<5) + ft(b, c, d) + e + Wt + Kb e = d,

d = c,

c = b <<<30,

b = a,

a = TEMP,

}

A = A + a, B = B + b, C = C + c, D = D + d, E = E + e,

1. Tính bảo mật trong SHA:

Để hiểu rõ hơn về tính bảo mật của SHA, ta hãy so sánh SHA với MD5 để có thể tìm ra những điểm khác nhau của hai hàm Băm này:

* + MD5 và SHA đều cộng thêm các bit “giả” để tạo thành những khối chia hết cho 512- bit, nhưng SHA sử dụng cùng một hàm phi tuyến f cho cả bốn vòng.
  + MD5 sử dụng mỗi hằng số duy nhất cho mỗi bước biến đổi, SHA sử dụng mỗi hằng số cho mỗi vòng biến đổi, hằng số dịch này là một số nguyên tố đối với độ lớn của word (giống với MD4).
  + Trong hàm phi tuyến thứ 2 của MD5 có sự cải tiến so với MD4, SHA thì sử dụng lại hàm phi tuyến của MD4, tức (X ∧ Y) V (X ∧ Z) V (Y ∧ Z).
  + Trong MD5 với mỗi bước được cộng kết quả của bước trước đó. Sự khác biệt đối với SHA là cột thứ 5 được cộng (không phải b, c hay d như trong MD5), điều này làm cho phương pháp tấn công của Boer-Bosslaser đối với SHA bị thất bại (den Boer và Bosselaers là hai người đã phá thành công 2 vòng cuối trong MD4).

Cho đến nay, chưa có công bố nào được đưa ra trong việc tấn công SHA, bởi vì độ dài của hàm Băm SHA là 160-bit, nó có thể chống lại phương pháp tấn công bằng vét cạn (kể cả Birthday attack) tốt hơn so với hàm Băm MD5 128-bit.

### 1.4.2 Ứng dụng của hàm băm

Ứng dụng chính của hàm Băm là sử dụng với hệ chữ ký điện tử, trong đó thay vì ký trực tiếp lên các văn bản, thông điệp (mà trong đa số trường hợp là rất lớn, tốc độ chậm) người ta sẽ ký lên giá trị băm đại diện cho toàn bộ văn bản đó. Điều này đặc biệt quan trọng và hiệu quả bởi vì chúng ta biết rằng các hệ chữ ký điện tử đều làm việc với các phép tính số học số lớn nên bản thân chúng đã tương đối chậm, việc sử dụng giá trị băm thay cho toàn bộ văn bản là giải pháp toàn diện khắc phục được yếu điểm này của các hệ chữ ký điện tử. Ngoài việc sử dụng với các hệ chữ ký điện tử hàm Băm còn được sử dụng vào các mục đích khác như: xác thực hóa thông điệp, xác thực hóa người dùng.

Đối với các ứng dụng không cần giữ bí mật thông điệp mà chỉ cần đảm bảo thông điệp không bị thay đổi trên đường truyền người ta sẽ sử dụng hàm băm cho mục đích xác thực tính nguyên vẹn của thông điệp đó. Chẳng hạn chúng ta có một phần mềm mã nguồn mở ở dạng setup muốn phân phối cho người dùng, rõ ràng việc gửi phần mềm đó tới máy tính của người dùng là không cần phải mã hóa, tuy nhiên nếu như phần mềm đó (khi đó phần mềm chính là thông điệp). Người dùng sẽ download cả phần mềm và giá trị băm nhận được, sau đó tiến hành băm lại, đối sánh hai giá trị này nếu khớp nhau thì có thể đảm bảo phần mềm không bị sửa đổi trên đường truyền. Hiện nay đa số các phần mềm mã nguồn mở đều được phân phối theo cách này.

Trong các hệ thống yêu cầu có xác thực người dùng như các hệ quản trị cơ sở dữ liệu, hệ điều hành, các ứng dụng web, ứng dụng dạng desktop application, để lưu mật khẩu người dùng người ta cũng sử dụng các hàm Băm hoặc các hệ mã trong các vai trò của hàm Băm (không sử dụng khóa). Khi đó mỗi tài khoản của người dùng thay vì lưu dưới dạng tên truy cập (user name) và mật khẩu (password) sẽ được lưu dưới dạng: tên người dùng, giá trị băm của mật khẩu. Khi một người dùng đăng nhập vào hệ thống, hệ thống sẽ lấy tên truy cập, mật khẩu họ nhập vào, kiểm tra xem có tên truy cập nào như vậy hay không. Nếu có sẽ tiến hành băm giá trị mật khẩu do người dùng nhập vào.

# CHƯƠNG 2. KẾT QUẢ NGHIÊN CỨU

## 2.1 Giới thiệu

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

Nội dung nghiên cứu

* Tạo khóa ElGamal
* Ký văn bản
* Xác nhận văn bản
* Kiểm tra sự toàn vẹn của tài liệu/văn bản
* Demo chương trình
* Các bước thực hiện triển khai đề tài bao gồm:
* Nghiên cứu, tìm hiểu cách mã hóa và giải mã của hệ mật mã ElGamal
* Thiết kế và cài đặt chương trình demo thuật toán ElGamal
* Hình thức sản phẩm: Sản phẩm bản mẫu
* Kết quả đạt được:
* Quyển báo cáo bài tập lớn
* Chương trình demo ứng dụng thuật toán ElGamal

## 2.2 Nội dung thuật toán

- Tạo cặp khóa (bí mật, công khai)(a, h) :

• Chọn số nguyên tố p sao cho bài toán logarit rời rạc trong Zp là “khó” giải.

• Chọn phần tử nguyên thuỷ g ∈ Zp\* . Đặt P = Zp\*, A = Zp\* x Zp-1 .

• Chọn khóa bí mật là a ∈ Zp\* .

Tính khóa công khai h = g a mod p.

• Các giá trị p, g, h được công khai, phải giữ bí mật a. - Ký số:

• Dùng 2 khóa ký: khóa a và khóa ngẫu nhiên bí mật r ∈ Zp-1 \* . (Vì r ∈ Zp-1 \* , nên nguyên tố cùng p -1, do đó tồn tại r -1 mod (p -1) ).

• Chữ ký trên x ∈ P là y = Sig a(x, r) = (γ, δ), y ∈ A(E1)

• Trong đó γ∈Zp\*, δ∈ Zp-1: γ = g r mod p và δ = (x–a\*γ) \* r -1 mod (p -1)

- Kiểm tra chữ ký:

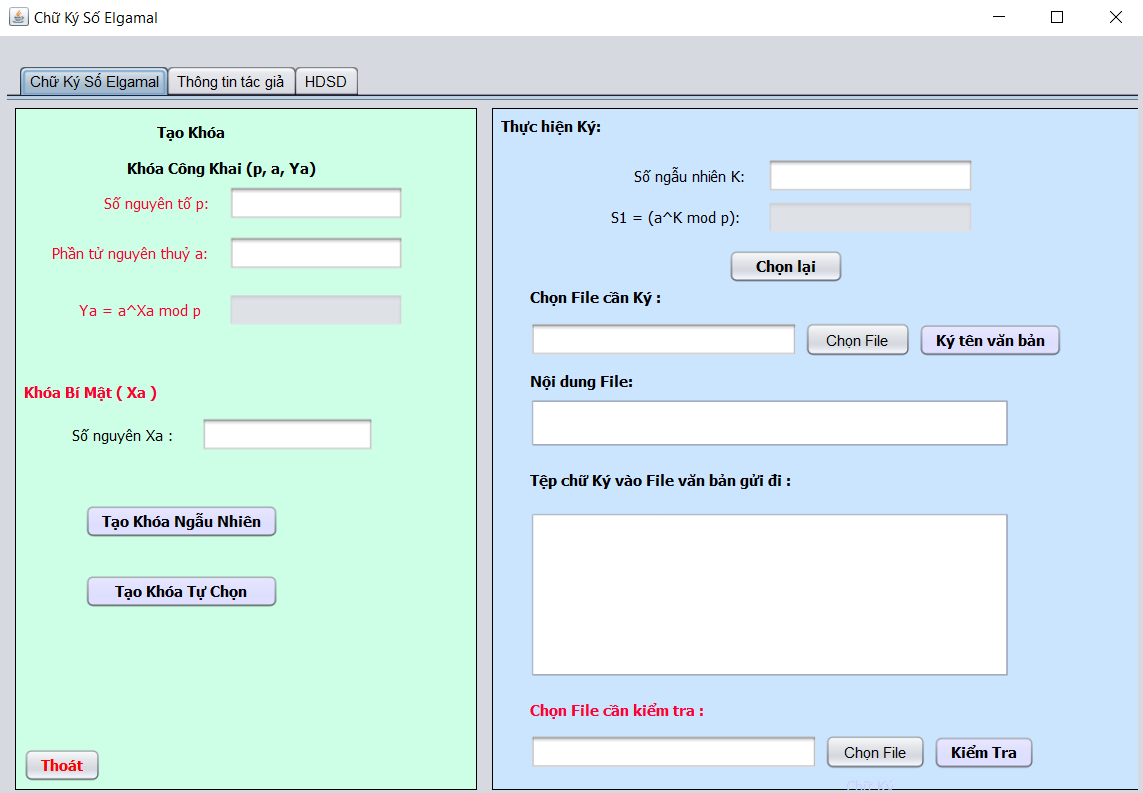
• Verk (x, γ, δ) = True ⇔ h γ \* γ δ ≡ g x mod p. (E2)

• Chú ý: Nếu chữ ký được tính đúng, kiểm thử sẽ thành công vì h γ \* γ δ ≡ g aγ \* g r \* δ mod p ≡ g (aγ +r\* δ) mod p ≡ g x mod p.

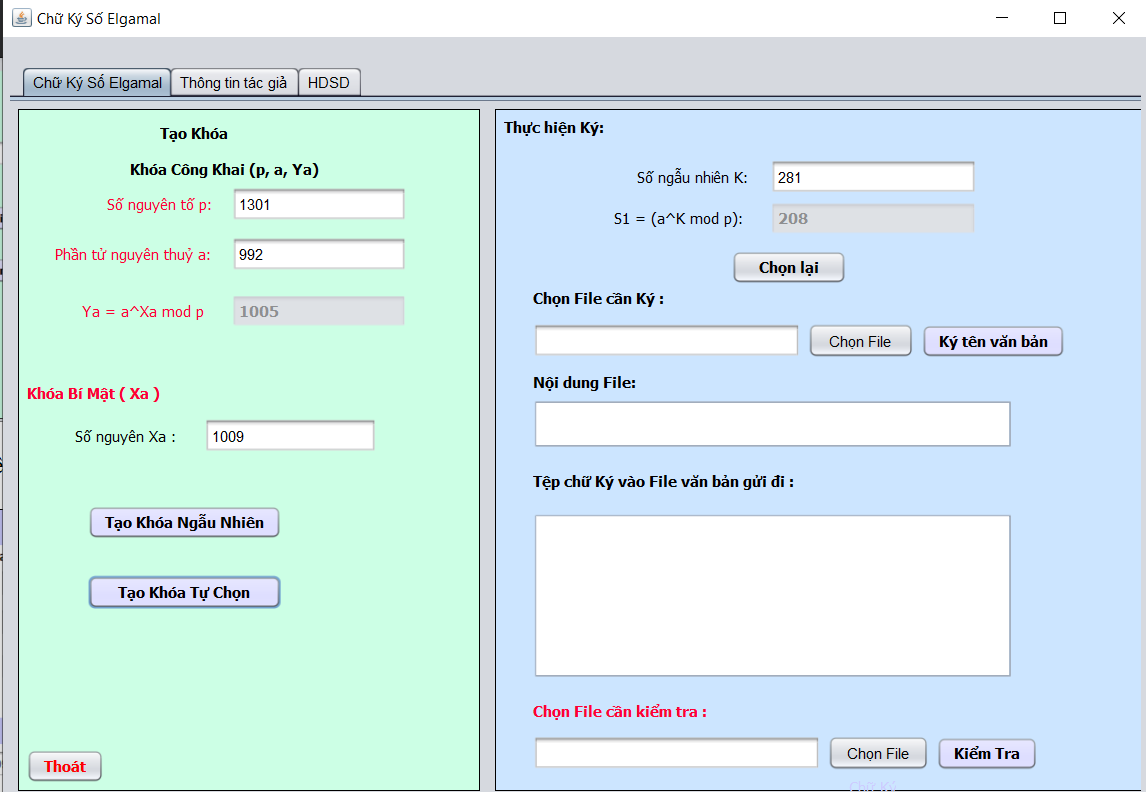
• Do δ = (x–a\*γ ) \* r -1 mod (p -1) nên (a\*γ + r\*δ) ≡ x mod (p-1).

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

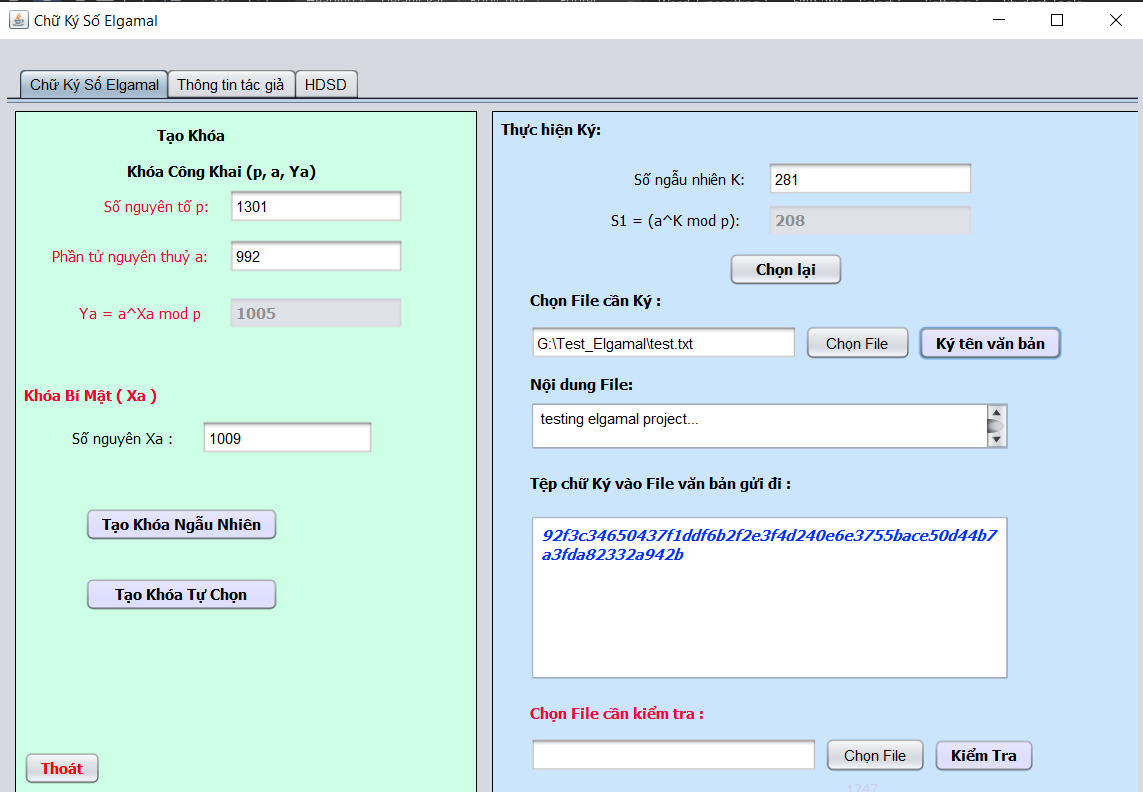
## 2.3.1. Giao diện chương trình đề mô



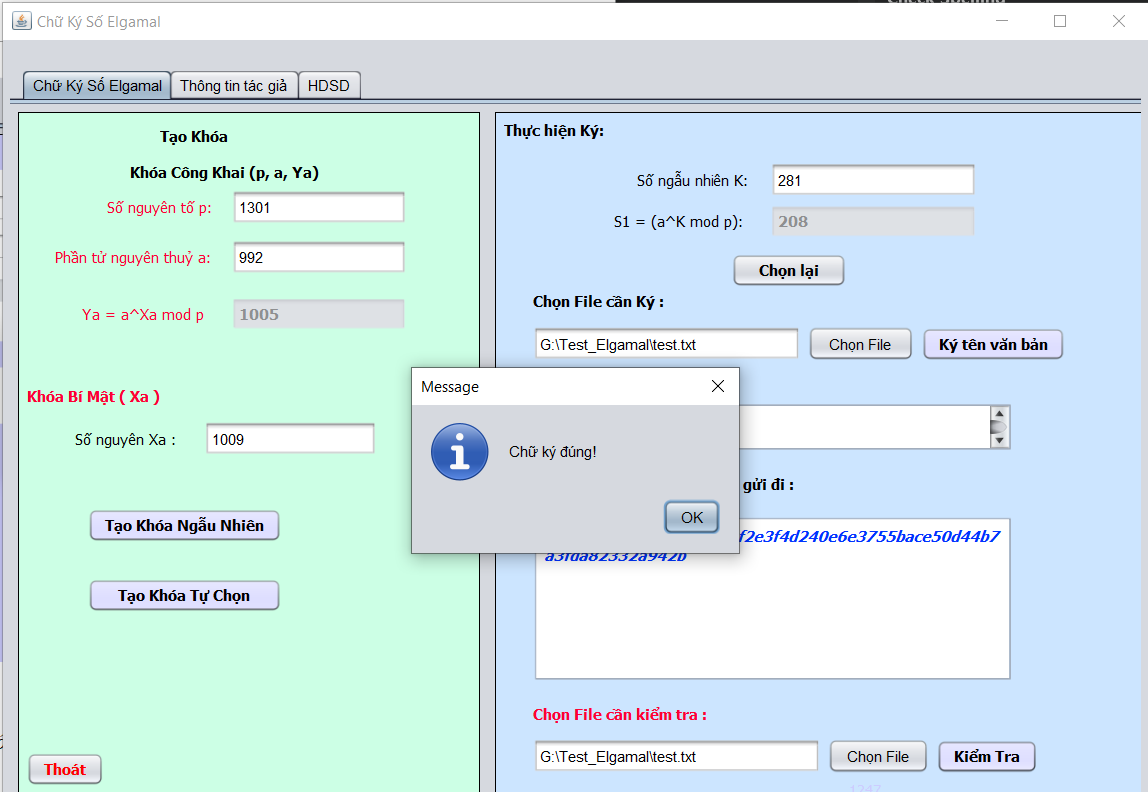
Tạo khóa ngẫu nhiên hoặc tự chọn:

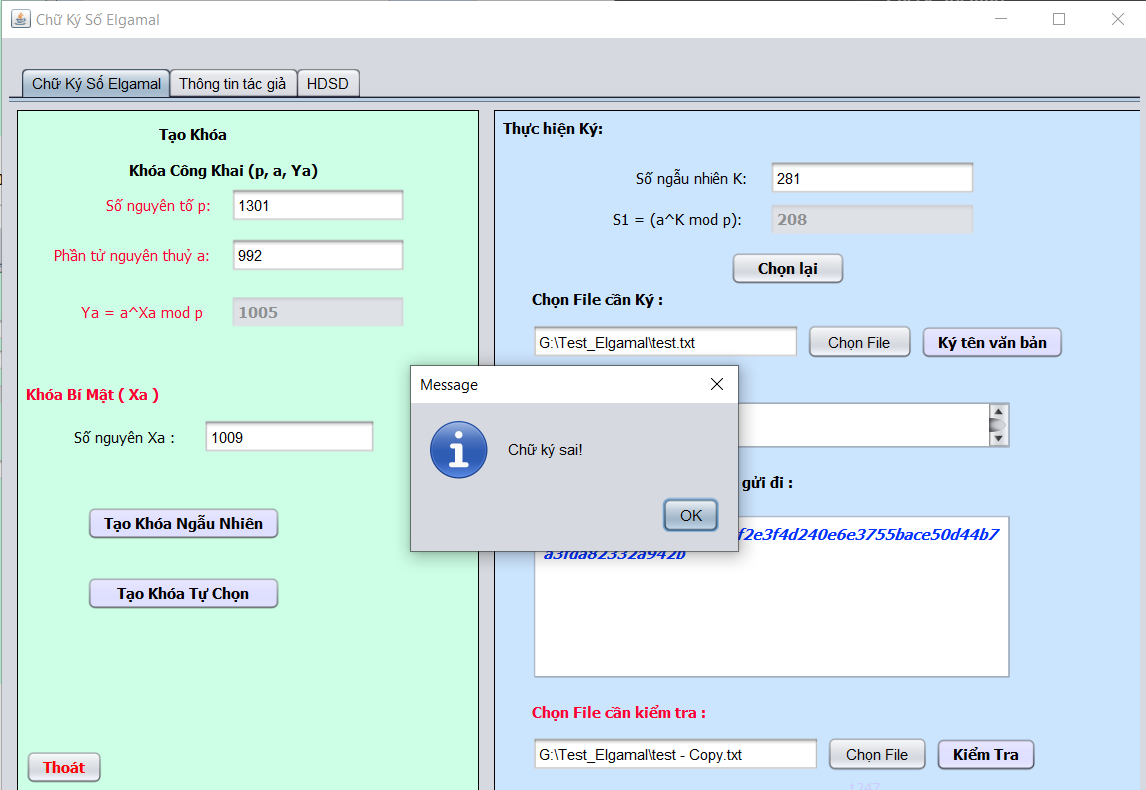


*Tải văn bản cần ký và tạo chữ ký, xác nhận ký tên..*



Xác nhận văn bản: Kiểm tra chữ ký đúng hay sai.





*Thông báo sau khi kiểm tra đúng-sai.*

## 2.4 Cài đặt và triển khai

Vì tính bảo mật trong các giao dịch thương mại, từ việc xác minh chữ ký cho đến các thẻ tín dụng, các sơ đồ định danh và các sơ đồ chia sẻ bí mật … nên phầm mềm tạo chữ ký Elgamal được xây dựng để đảm bảo tính an toàn trong quá trình chuyển file.

Phần mềm cần tự tạo khóa công khai (p, α, β) và khóa bí mật (a).

Sau khi tạo khóa ngẫu nhiên ta tải file cần thực hiện ký, file sẽ hiển thị trong txtFile.

Digest của tệp sử dụng hàm băm SHA256, tự động băm khi tải file cần thực hiện ký lên (ảnh trên).

Sau khi có chữ ký thì ký lên văn bản bằng button Ký văn bản và tự động lưu file chữ ký khi ký xong.

Sau khi ký thành công văn bản thì tải văn bản đã ký và cần xác nhận lên:Và tải file chữ ký kèm theo đã được ký ở văn bản:

## 2.5 Thực hiện bài toán

### 2.5.1 Phân công công việc

|  |  |  |
| --- | --- | --- |
| ***STT*** | ***Họ và Tên*** | ***Công Việc*** |
| ***1*** | ***Ngô Quang Đồng (PHP)*** | ***Tạo khoá*** |
| ***2*** | ***Hoàng Trần Minh Đức (Java)*** | ***Ký văn bản*** |
| ***3*** | ***Trần Văn Đức (JavaScript)*** | ***Xác nhận văn bản*** |
| ***4*** | ***Phạm Văn Dung (C#)*** | ***Kiểm tra sự toàn vẹn của tài liệu/văn bản*** |
| ***5*** | ***Nguyễn Mạnh Dũng (Python)*** | ***Thuật toán*** |

### 2.5.2 Ngô Quang Đồng – Tạo khóa (Đã trình bày ở trên)

### 2.5.3 Trần Văn Đức – Ký văn bản

**Tạo khóa**

Qua trình tạo khóa giống như quá trình tạo khóa của hệ mật ElGamal, tức là Alic chọn số nguyên tố p đủ lớn để bài toàn logarith rời rạc trên Zp là khó giải, và chọn α ϵ Z\*p là phần tử nguyên thủy, chọn xA < p – 1 là số nguyên làm khóa mật và tính khóa công cộng yA = αxA(mod p).

**Tạo chữ ký**

Để ký lên bức điện m ϵ Z\*N Alice tạo ra số ngẫu nhiên k thỏa mãn k < p – 1 và UCLN(k, p -1) = 1 và hình thành nên chữ ký là cặp (r, s), ở đây *r k* (mod *p*), *s k* 1(*m x r*)(mod *p* 1).

*A*

**Sơ đồ chữ ký Schnorr**

Đây là sơ đồ chữ ký thuộc họ của Elgamal nhưng có những tính chất tốt hơn so với sơ đồ Elgamal.

**Thiết lập tham số hệ thống**

Chọn hai số nguyên tố p và q, thỏa mãn điều kiện q|p-1 và các số này được chọn sao cho kích thước p = 1024 và q = 160.

Lựa chọn phần tử g ϵ Z\*p và thực hiện lệnh *g*  *f* ( *p*1) / *q* (mod *p*). Nếu như g = 1 thì lặp lại đến khi g # 1.

Lựa chọn hàm hash H, ví dụ có thể chọn SHA256. Các tham số (p, q, g, H) sẽ phân bố giữa các người dùng hệ thống.

**Hình thành khóa mật và khóa công cộng**

Alice tạo ra số ngẫu nhiên *y*  *g* *x* (mod *p*), *x*  *Z* \*

**Chuẩn chữ ký DSS**

Đây cũng là phiên bản cản tiến của Elgamal. Nó được đề xuất năm 1991, tuy nhiên nó được chấp nhận làm chuẩn từ 01/12/1994. Giống như sơ đồ chữ ký Schnorr, chuẩn chữu ký DSS cũng có những ưu điểm so với Elgamal.

Các tham số hệ thông giống như sơ đồ chữ ký Schnorr và chuẩn DSS chọn hàm hash là SHA – 1. Các tham số của hệ thống là (p, q, g, H).

Tham số công khai của Alice bao gồm (p, q, g, y, H) còn x là tham số bí mật.

**Chuẩn chữ ký của Liên Xo Gost 34 – 10. 94**

Sơ đồ này ra đời chuẩn DSS của Mỹ nên nó được kế thừa và bổ sung những ưu việt của mình

**Hình thành tham số hệ thống**

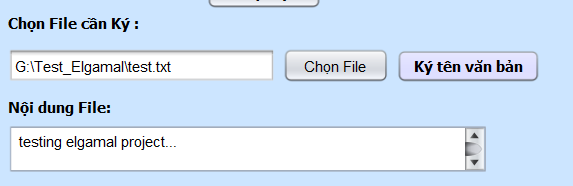
Cho p là số nguyên tố, kích thước từ 509 đến 512 bít, q là số nguyên tố sao cho q|p-1. Số g < p – 1 có bậc là q, nghĩa là *gq* <- 1(mod *p*).

**Hình thành khóa**

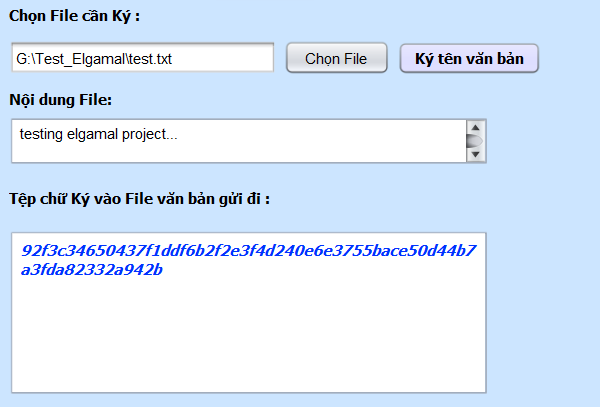
Alice chọn x < q là khóa mật và Alice đi tính khóa công khai: y = gx (mod p). Các tham số (p, q, g, y) là tham số công khai.

### 2.5.4 Hoàng Trần Minh Đức– Xác nhận văn bản

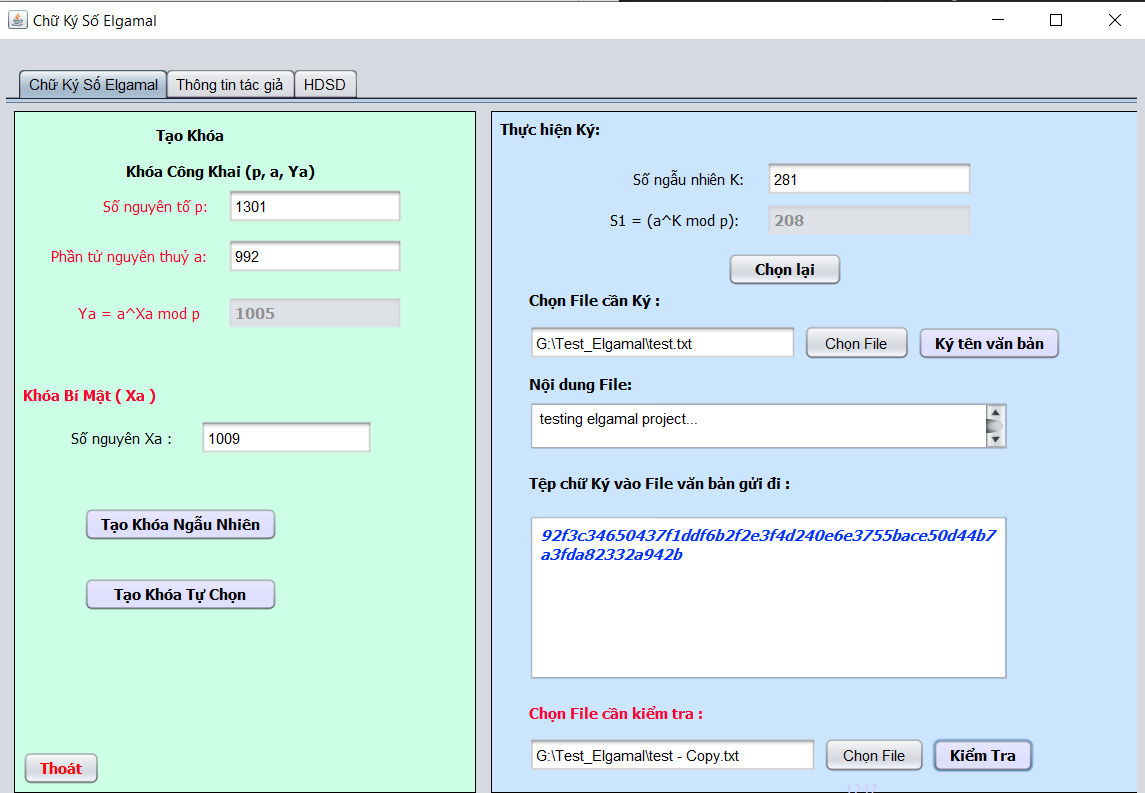
* **In ra được nội dung của file txt hoặc docx:**



* + - * **Tải văn bản cần xác nhận lên hiển thị được nội dung và chữ ký :**



**Viết chương trình demo với ngôn ngữ Java:**



### 2.5.5 Phạm Văn Dung- Kiểm tra sự toàn vẹn của tài liệu/văn bản

* Nếu V1 ≡ V2 thì chữ ký là hợp lệ - văn bản không bị chỉnh sửa
* Ngược lại V1 ≠ V2 thì văn bản đã bị thay đổi hoặc chữ ký bị giả mạo

### 2.5.6 Nguyễn Mạnh Dũng- Thuật toán

Bài toán sử dụng hệ mã đã học để tạo chữ ký điện ElGama trải qua các bước cụ thể dựa trên bài toán logarit rời rạc:

1. Tạo khóa

a. Xác định khóa công khai Kpub = (p, alpha, beta)

b. Xác định khóa bí mật Kpr = (a)

2. Mã hóa

Xác định ekpub (x, k) = (y1, y2)

Trong đó y1 = alphak mod p

y2 = x\*betak mod p

3. Giải mã

Với y1, y2 thuộc vành Zp\* ta xác định

X = dk (y1, y2) = y2 (y1a)-1 mod p

# CHƯƠNG 3. KIẾN THỨC LĨNH HỘI VÀ BÀI HỌC KINH NGHIỆM

## 3.1 Nội dung đã thực hiện

### 3.1.1 Nội dung học được thông qua thực hiện bài tập lớn

* + - * Khái niệm về chữ ký điện tử
      * Hệ chữ ký ElGamal
      * Chuẩn chữ ký điện tử
      * Mô hình ứng dụng của chữ ký điện tử
      * Mã hóa bất đối xứng.
      * Cách hoạt động của mã hóa bất đối xứng
      * Ứng dụng của mã hóa bất đối xứng
      * Lợi ích và hạn chế của mã hóa bất đối xứng
      * So sánh mã hóa bất đối xứng và mã hóa đối xứng
      * Đặc tính của hàm băm
      * Hàm băm SHA-1 và SHA-2
      * Ứng dụng của hàm băm
      * Bài toán chữ ký điện tử ElGamal
      * Nắm vững một ngôn ngữ lập trình cơ bản (Java, C#, C++, Python) và giải được bài toán để ứng dụng vào thực tiễn

### 3.1.2 Bài học kinh nghiệm được rút ra sau khi kết thúc bài tập lớn

Trong quá trình xây dựng và phát triển phần mềm, nhóm đã gặp rất nhiều khó khăn trong việc xây dựng phần mềm do còn nhiều hạn chế về kiến thức hệ thống cũng như kiến thức về lĩnh vực hướng tới của phần mềm.

Xong hệ phần mềm đã đáp ứng các nhu cầu cơ bản. Nhưng cần bổ sung thêm một số tính năng, chỉnh sửa giao diện sao cho đẹp mắt, tối ưu nhất.

Chương trình được kiểm tra rà soát, sao cho việc xuất hiện lỗi là tối thiểu, ít nhất. Đảm bảo chương trình hoạt động một cách mượt mà nhất. Tối ưu giao diện và đơn giản hóa giúp cho việc sử dụng dễ dàng hơn.

**Mục tiêu đạt được:** Hoàn thiện một phần mềm với những chức năng cơ bản, cần thiết nhất thuận tiện cho người dùng. Hạn chế lỗi ở mức tối thiểu.

Giao diện tối giản hóa, dễ sử dụng.

**Chưa đạt được:** Giao diện cổ điển, chưa bắt mắt, ít chức năng.

Kết thúc việc xây dựng phần mềm, nhóm đã đúc kết được nhiều kinh nghiệm, học hỏi thêm được nhiều kiến thức trong việc phát triển phần mềm, góp phần hoàn thiện kỹ năng, tư duy trong xây dựng phần mềm và củng cố kiến thức đã học.

## 3.2 Hướng phát triển

### 3.2.1 Tính khả thi của chủ đề nghiên cứu

Tất cả các mô hình chữ ký số cần phải đạt được một số yêu cầu để có thể được chấp nhận trong thực tế:

* + - * Chất lượng của [thuật toán](https://vi.wikipedia.org/wiki/Thu%E1%BA%ADt_to%C3%A1n): một số thuật toán không đảm bảo an toàn tuy nhiên Elgamal đáp ứng được điều đó vì độ khó của bài toán [logarit rời](https://wivi.wiki/wiki/Discrete_logarithm) [rạc](https://wivi.wiki/wiki/Discrete_logarithm).
      * Chất lượng của [phần mềm](https://vi.wikipedia.org/wiki/Ph%E1%BA%A7n_m%E1%BB%81m)/[phần cứng](https://vi.wikipedia.org/wiki/Ph%E1%BA%A7n_c%E1%BB%A9ng) thực hiện thuật toán.
      * [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) phải được giữ an toàn.
      * Quá trình phân phối [khóa công cộng](https://vi.wikipedia.org/wiki/M%E1%BA%ADt_m%C3%A3_h%C3%B3a_kh%C3%B3a_c%C3%B4ng_khai) phải đảm bảo mối liên hệ giữa khóa và thực thể sở hữu khóa là chính xác. Việc này thường được thực hiện bởi [hạ tầng khóa công cộng](https://vi.wikipedia.org/wiki/H%E1%BA%A1_t%E1%BA%A7ng_kh%C3%B3a_c%C3%B4ng_khai) (PKI) và mối liên hệ khóa người sở hữu được chứng thực bởi những người điều hành PKI. Đối với hệ thống PKI *mở*, nơi mà tất cả mọi người đều có thể yêu cầu sự chứng thực trên thì khả năng sai sót là rất thấp. Tuy nhiên các PKI [thương mại](https://vi.wikipedia.org/wiki/Th%C6%B0%C6%A1ng_m%E1%BA%A1i) cũng đã gặp phải nhiều vấn đề có thể dẫn đến những văn bản bị ký sai.
      * Những người sử dụng (và phần mềm) phải thực hiện các quá trình đúng thủ tục (giao thức).

Chỉ khi tất cả các điều kiện trên được thỏa mãn thì chữ ký số mới là bằng chứng xác định người chủ (hoặc người có thẩm quyền) của văn bản.

### 3.2.2 Những thuận lợi, khó khăn trong quá trình nghiên cứu

* **Thuận lợi:**
  + Áp dụng được kiến thức đã học trên lớp, không phải tìm hiểu kiến thức mới.
* **Khó khăn:**
  + Thời gian còn hạn chế đối với mục tiêu là báo cáo và ứng dụng bài toán vào thực tế.
  + Nhân lực khiêm tốn.
  + Chưa có giáo trình chính thức, tài liệu ít và không thống nhất do chữ ký số Elgamal ít phổ biến hơn RSA.

### 3.2.2 Hướng phát triển và mở rộng của đề tài

* Việc sử dụng chữ ký số ngày càng nhiều ứng dụng trong thực tế, không chỉ giới hạn trong ngành CNTT, ngành mật mã mà còn được áp dụng trong trong một số lĩnh vực khác như ngân hàng để xác thực người gửi, người nhận, lĩnh vực viễn thông để sử dụng các thẻ thông minh Với mật mã khóa công khai việc tạo ra chữ ký số và ứng dụng vào các tài liệu, các văn bản điện tử là vô cùng quan trọng.
* Ưu điểm của chữ ký số nói chung và Elgamal nói riêng:
  + **Khả năng xác định nguồn gốc:**

Các hệ thống mật mã hóa khóa công khai cho phép mật mã hóa văn bản với khóa bí mật mà chỉ có người chủ của khóa biết. Để sử dụng chữ ký số thì văn bản cần phải được mã hóa bằng hàm băm (văn bản được "băm" ra thành chuỗi, thường có độ dài cố định và ngắn hơn văn bản) sau đó dùng khóa bí mật của người chủ khóa để mã hóa, khi đó ta được chữ ký số. Khi cần kiểm tra, bên nhận giải mã (với khóa công khai) để lấy lại chuỗi gốc (được sinh ra qua hàm băm ban đầu) và kiểm tra với hàm băm của văn bản nhận được. Nếu 2 giá trị (chuỗi) này khớp nhau thì bên nhận có thể tin tưởng rằng văn bản xuất phát từ người sở hữu khóa bí mật. Tất nhiên là chúng ta không thể đảm bảo 100% là văn bản không bị giả mạo vì hệ thống vẫn có thể bị phá vỡ.

* + **Tính toàn vẹn:**

Cả hai bên tham gia vào quá trình thông tin đều có thể tin tưởng là văn bản không bị sửa đổi trong khi truyền vì nếu văn bản bị thay đổi thì hàm băm cũng sẽ thay đổi và lập tức bị phát hiện. Quá trình mã hóa sẽ ẩn nội dung của gói tin đối với bên thứ 3 nhưng không ngăn cản được việc thay đổi nội dung của nó. Một ví dụ cho trường hợp này là tấn công đồng hình (homomorphism attack): tiếp tục ví dụ như ở trên, một kẻ lừa đảo gửi 2.000.000.000 đồng vào tài khoản của a, chặn gói tin (a,b) mà chi nhánh gửi về trung tâm rồi gửi gói tin (a,b4) thay thế để lập tức trở thành tit phú!Nhưng đó là vấn đề bảo mật của chi nhánh đối với trung tâm ngân hàng không hẳn liên quan đến tính toàn vẹn của thông tin gửi từ người gửi tới chi nhánh, bởi thông tin đã được băm và mã hóa để gửi đến đúng đích của nó tức chi nhánh, vấn đề còn lại vấn đề bảo mật của chi nhánh tới trung tâm của nó.

* + **Tính không thể phủ nhận:**

Trong giao dịch, một bên có thể từ chối nhận một văn bản nào đó là do mình gửi. Để ngăn ngừa khả năng này, bên nhận có thể yêu cầu bên gửi phải gửi kèm chữ ký số với văn bản. Khi có tranh chấp, bên nhận sẽ dùng chữ ký này như một chứng cứ để bên thứ ba giải quyết.

Với những ưu điểm của chữ ký số nói trên, trong tương lai nhóm em có dự định phát triển đề tài chữ ký số Elgamal để áp dụng vào thực tế - xây dựng giao diện web hoặc phần mềm tích hợp USB cho doanh nghiệp triển khai, áp dụng chữ ký số. Tất nhiên nhóm em phải tìm hiểu giá trị pháp lý của chữ ký số theo Quy định tại Điều 8 Nghị định số 130/2018/NĐ-CP ngày 27/9/2018 của Chính phủ Quy định chi tiết thi hành Luật Giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số.

**Tài liệu tham khảo**

1. Phan Đình Diệu (2002). Lí thuyết mật mã và an toàn thông tin. NXB Đại học Quốc gia Hà Nội.
2. Douglas (1994) Mật mã lí thuyết và thực hành. Người dịch: Nguyễn Bình

Tài liệu trên Internet