**BỘ CÔNG THƯƠNG**

**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**

-----🙞🙜🕮🙞🙜-----



**BÀI TẬP LỚN**

**Môn học: An toàn và bảo mật thông tin**

**ĐỀ TÀI: TÌM HIỂU VỀ CHỮ KÍ ĐIỆN TỬ ELGAMAL**

**VÀ VIẾT ỨNG DỤNG MINH HỌA**

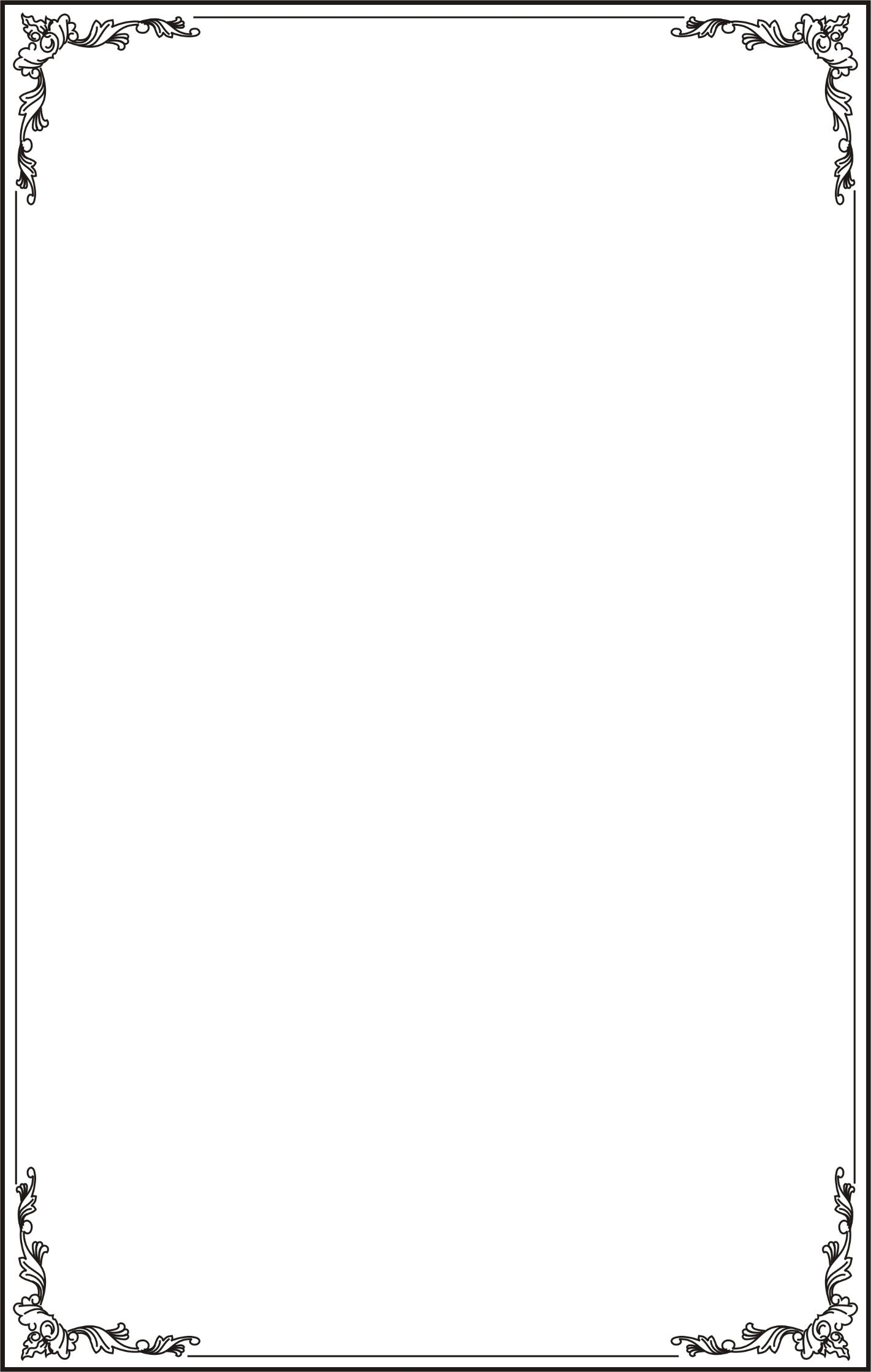
**Giảng viên hướng dẫn: ThS. Trần Phương Nhung**

**Nhóm sinh viên thực hiện: 13**

**Thành viên nhóm:**

|  |  |
| --- | --- |
| 1. **Nguyễn Tiến Trung** 2. **Kiều Anh Tuân** 3. **Trần Anh Tuấn** 4. **Trần Quốc Tuấn** | * **2019605201** * **2019605674** * **2019604098** * **2021608940** |

Hà Nội, 2022

**BỘ CÔNG THƯƠNG**

**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**

-----🙞🙜🕮🙞🙜-----



**BÀI TẬP LỚN**

**Môn học: An toàn và bảo mật thông tin**

**ĐỀ TÀI: TÌM HIỂU VỀ CHỮ KÍ ĐIỆN TỬ ELGAMAL**

**VÀ VIẾT ỨNG DỤNG MINH HỌA**

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

**Nhóm viên thực hiện: 13**

**Thành viên nhóm:**

|  |  |
| --- | --- |
| 1. **Nguyễn Tiến Trung** 2. **Kiều Anh Tuân** 3. **Trần Anh Tuấn** 4. **Trần Quốc Tuấn** | * **2019604201** * **2019605674** * **2019604098** * **2021608940** |

Hà Nội, 2022

**MỤC LỤC**

[LỜI NÓI ĐẦU 1](#_Toc113553103)

[CHƯƠNG 1. TỔNG QUAN 2](#_Toc113553104)

[1.1 Giới thiệu chung về chữ kí số 2](#_Toc113553105)

[1.2 Định nghĩa chữ kí số 2](#_Toc113553106)

[1.3 Sơ đồ chữ kí Elgamal 3](#_Toc113553107)

[1.4 Phương pháp mã hóa bất đối xứng ứng dụng trong chữ kí điện tử 6](#_Toc113553108)

[1.4.1 Mã hóa bất đối xứng là gì? 6](#_Toc113553109)

[1.4.2 Hệ mật mã Elgamal 7](#_Toc113553110)

[1.5 Hàm băm SHA 8](#_Toc113553111)

[1.5.1 Khái quát về hàm băm SHA 8](#_Toc113553112)

[1.5.2 Hàm băm SHA-2 9](#_Toc113553113)

[1.5.3 Ưu nhược điểm hàm băm SHA-2 9](#_Toc113553114)

[CHƯƠNG 2. KẾT QUẢ NGHIÊN CỨU 10](#_Toc113553115)

[2.1 Giới thiệu 11](#_Toc113553116)

[2.2 Nội dung thuật toán 11](#_Toc113553117)

[2.3 Thiết kế và cài đặt chương trình demo thuật toán 11](#_Toc113553118)

[2.3.1 Giao diện chương trình demo 11](#_Toc113553119)

[2.4 Cài đặt và triển khai 11](#_Toc113553120)

[2.4.1 Giới thiệu công cụ 11](#_Toc113553121)

[2.4.2 Hướng dẫn cài đặt và chạy chương trình demo đã cài đặt 11](#_Toc113553122)

[2.5 Thực hiện bài toán 11](#_Toc113553123)

[2.5.1 Phân công công việc 11](#_Toc113553124)

[2.5.2 Nguyễn Tiến Trung – Nghiên cứu và tìm hiểu về sơ đồ chữ kí số 11](#_Toc113553125)

[2.5.3 Kiều Anh Tuân – Nghiên cứu và tìm hiểu về sơ đồ chữ kí Elgamal 11](#_Toc113553126)

[2.5.4 Trần Anh Tuấn – Nghiên cứu và tìm hiểu về hàm băm SHA 11](#_Toc113553127)

[2.5.5 Trần Quốc Tuấn – Nghiên cứu và tìm hiểu về mã hóa bất đối xứng và ứng dụng trong chữ kí điện tử 11](#_Toc113553128)

[CHƯƠNG 3. KIẾN THỨC LÍNH HỘI VÀ BÀI HỌC KINH NGHIỆM 10](#_Toc113553129)

[3.1 Nội dung đã thực hiện 10](#_Toc113553130)

[3.1.1 Các kiến thức đã học được 10](#_Toc113553131)

[3.1.2 Những kỹ năng đã học được 10](#_Toc113553132)

[3.1.3 Những bài học kinh nghiệm được rút ra 11](#_Toc113553133)

[3.2 Hướng phát triển 11](#_Toc113553134)

[3.2.1 Tính khả thi của chủ đề nghiên cứu 11](#_Toc113553135)

[3.2.2 Những thuận lợi và khó khăn trong quá trình nghiên cứu đề tài 12](#_Toc113553136)

[3.2.3 Hướng phát triển và mở rộng của đề tài 12](#_Toc113553137)

[TÀI LIỆU THAM KHẢO 13](#_Toc113553138)

# LỜI NÓI ĐẦU

Đi cùng với quá trình phát triển của loài người thì có một lượng thông tin lớn được sinh ra, vì vậy vấn đề bảo mật thông tin luôn dành được sự quan tâm lớn trong mọi thời đại. Từ xa xưa con người đã sáng tạo ra các hệ mật mã cổ điển để đáp ứng nhu cầu bảo mật thông tin. Mật mã học là một ngành có lịch sử từ hàng nghìn năm nay. Trong phần lớn thời gian phát triển của mình (ngoại trừ vài thập kỷ trở lại đây), lịch sử mật mã học chính là lịch sử của những phương pháp mật mã học cổ điển các phương pháp mật mã hóa với bút và giấy, đôi khi có hỗ trợ từ những dụng cụ cơ khí đơn giản.

Từ trước đến nay chúng ta đã rất quen thuộc với chữ kí tay trên những văn bản quan trọng như hợp đồng mua bán, giấy khai sinh,…nhằm xác nhận người đã kí nó. Trong thời đại hiện nay, những thông tin quan trọng không chỉ nằm trên các tài liệu vật lý nữa mà nó còn là những tệp tin trên máy tính, chính vì vậy người ta đã nghiên cứu ra sơ đồ chữ kí số - là phương pháp kí một bức điện lưu dưới dạng điện tử.

Dựa trên sự hướng dẫn của giảng viên - ThS. Trần Phương Nhung, các thành viên trong nhóm đã tiến hành thực hiện đề tài *Tìm hiểu về chữ kí điện tử Elgamal và viết ứng dụng minh họa*. Trong suốt quá trình hoàn thiện bài tập lớn, nhóm chúng em đã cố gắng hết sức, chúng em rất mong nhận được sự góp ý từ phía cô để bài tập lớn của nhóm được hoàn thiện hơn.

***Sinh viên thực hiện!***

# TỔNG QUAN

## Giới thiệu chung về chữ kí số

Sơ đồ chữ kí điện tử là phương pháp kí một bức điện lưu dưới dạng điện tử. Chẳng hạn một bức điện có kí hiệu được truyền trên mạng máy tính. Ta sẽ thảo luận trên một vài khác biệt cơ bản giữa các chữ kí thông thường và chữ kí số.

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

Thứ hai là vấn đề về kiểm tra. Chữ kí thông thường được kiểm tra bằng cách so sánh nó với các chữ kí xác thực khác. Ví dụ, ai đó kí một tấm séc để mua hàng, người bán phải so sánh chữ kí trên mảnh giấy với chữ kí nằm ở mặt sau của thẻ tín dụng để kiểm tra. Dĩ nhiên, đây không phải là phương pháp an toàn vì nó dể dàng giả mạo. Mặt khác, các chữ kí số có thể được kiểm tra nhờ dùng một thuật toán kiểm tra công khai. Như vậy, bất kỳ ai cũng có thể kiểm tra được chữ kí số. Việc dùng một sơ đồ chữ kí an toàn có thể sẽ ngăn chặn được khả năng giả mạo.

Sự khác biệt cơ bản khác giữa chữ kí số và chữ kí thông thường bản copy tài liệu được kí bằng chữ kí số sẽ đồng nhất với bản gốc, còn copy tài liệu có chữ kí trên giấy thường có thể khác với bản gốc. Điều này có nghĩa là phải cẩn thận ngăn chăn một bức kí số khỏi bị dùng lại. Vì thế, bản thân bức điện cần chứa thông tin (Chẳng hạn như ngày tháng) để ngăn nó khỏi bị dùng lại.

## Định nghĩa chữ kí số

Một sơ đồ chữ kí số thường chứa hai thành phần: Thuật toán kí và thuật toán xác minh. Người B có thể kí bức điện x dùng thuật toán kí an toàn. Chữ kí y = sig(x) nhận được có thể kiểm tra bằng thuật toán xác minh công khai ver(x,y). Khi cho trước cặp (x,y), thuật toán xác minh có giá trị TRUE hay FALSE tùy thuộc vào chữ kí được thực hiện như thế nào. Dưới đây là định nghĩa hình thức của chữ kí

***Định nghĩa:*** Một sơ đồ chữ kí số là bộ 5 (P, A, K, S, V) thỏa mãn các điều kiện dưới đây:

1. P là tập hữu hạn các bức điện có thể.
2. A là tập hữu hạn các chữ kĩ có thể.
3. K không gian khóa là tập hữu hạn các khóa có thể.
4. Với mỗi k thuộc K tồn tại một thuật toán kí sigk S và là một thuật toán xác minh verk V. Mỗi sigk: P A và verk: Pa {true, false} là những hàm sao cho mỗi bức điện x P và mỗi chữ kí y A thỏa mãn phương trình dưới đây

***ver(x,y) =***

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 các 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 vậy nếu có đủ thời gian, C luôn có thể giả mạo chữ ký của B. Như vậy, mục đích của chúng ta là tìm ra 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 cacsch 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 từ một xác suất rất nhỏ. Có thể dùng các hàm băm (Hash function) như MD4, MD5, SHA trong việc tính kết nối các sơ đồ chữ ký điện tử sẽ loại phương pháp giả mạo này.

## Sơ đồ chữ kí Elgamal

Sơ đồ chữ ký Elgamal được giới thiệu trong một bài báo vào năm 1985. Bản cải tiến của sơ đồ này đã được Viện Tiêu chuẩn và Công nghệ Quốc Gia Mỹ (NIST) chấp nhận làm chữ kí số. Sơ đồ Elgamal (E) được thiết kế với mục đích giành riêng cho chữ kí số, khác với sơ đồ RSA dùng cho cả hệ thống mã hóa công khai lẫn chữ kí số.

Sơ đồ Elgamal là không tất định giống như hệ thống mã khóa công khai Elgamal. Điều này có nghĩa là có nhiều chữ kí hợp lệ trên bức điện cho trước bất kỳ. Thuật toán xác minh phải có khả năng chấp nhận bất kì chữ kí hợp lệ khi xác thực. Cụ thể, sơ đồ chữ kí Elgamal được miêu tả như sau:

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

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

Trong đó giá trị p, là công khai, còn a là bí mật. Với K = { p,, a, } và chọn một số ngẫu nhiên k Zp-1\*, định nghĩa:

sigk(x, k) = ()

trong đó mod p, và (x - a)k-1mod (p-1). Với x, Zp\* và Zp-1, định nghĩa:

ver(x,x mod p

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

mod p mod p

Trong đó: a + kmod (p-1). B sẽ tính toán chữ kí bằng việc sử dụng cả giá trị bí mật a (một phần của khóa) và số bí mật ngẫu nhiên k (giá trị để kí 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, = 2, a = 127. Ta tính: = 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 (UCLN(213, 466) = 1 và 213-1 mod 466 = 431). Sau đó tính:

2213mod 467 = 29 và = (100 – 127 x 29)x431 mod 466 = 51

Bất kì ai cũng có thể xác minh chữ kí bằng cách kiểm tra:

13229 x 2951 189 mod 467 và 2100

* Chữ ký là hợp lệ.

Xét độ bảo mật của sơ đồ chữ kí E, giả sử kẻ thứ ba là C muốn giả mạo chữ kí của B trên bức điện x mà không biết số bí mật a. Nếu C chọn một giá trị và cố gắng tìm , anh ta phải tính một làm logarit rời rạc . Mặt khác, nếu đầu tiên anh ta chọn để cố gắng tìm thì anh ta phải tính 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 , và x. Cho i, j là số nguyên với 0 <= i, j<= p-2, và UCLN(j, p-1) = 1. Sau đó tính:

mod p

j-1 mod (p-1)

x = - ij-1 mod (p-1)

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

mod p

mod p

mod p

mod p

mod p

*Ví dụ:* Như ví dụ trên, ta chọn p = 467, = 2, = 132. Giả sử C sẽ chọn i = 99 và j = 179. Anh ta sẽ tính:

= 299132179 mod 467 = 117

= -117\*151 mod 466 = 41

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 () 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(h, p-1) = 1. Ta thực hiện tính toán sau:

mod p

mod (p-1)

x’ = (hx + i)mod (p-1)

Ta có thể kiểm tra mod p và do đó () là cặp giá trị chữ kí của bức điện x’.

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 () là chữ kí trên bức điện x1 và () là chữ kí trên bức điện x2. Việc kiểm tra sẽ được thực hiện như sau:

mod p

mod p

Do đó: mod p.

Đặt , khi đó x1 – x2 = k() mod (p-1).

Bây giờ đặt d = UCLN(,p-1). Vì d | () và d | (p-1) nên suy ra d | (x1 – x2). Ta đặt tiếp:

x’ = (x1 – x2)/d

’ = (/d

p’ = (p-1)/d

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

= (’)-1 mod p’

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

k = x’mod p’ = x’ + ip’ mod p

Với 0 <= i <= d-1, ta có thể tìm được giá trị k duy nhất bằng hàm kiểm tra: k mod p.

## Phương pháp mã hóa bất đối xứng ứng dụng trong chữ kí điện tử

### Mã hóa 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 công khai (Public key cryptosystem).

Nhiều giao thức dựa trên mật mã bất đối xứng, bao gồm giao thức bảo mật lớp truyền tải (TLS) và giao thức lớp cổng bảo mật (SSL) giúp HTTPS khả thi. Quá trình mã hóa cũng được sử dụng trong các chương trình phần mềm – chẳng hạn như trình duyệt – cần thiết lập kết nối an toàn qua mạng không an toàn như Internet hoặc cần xác thực chữ ký điện tử.

### Hệ mật mã Elgamal

Elgamal đã phát triển một hệ mật mã khóa công khai dựa trên bài toán logarit rời rạc. Bài toán logarit rời rạc được phát biểu như sau:

+ I = (p, ) trong đó p là số nguyên tố, ZP là phần tử nguyên thủy, ZP\*.

+ Mục tiêu: Hãy tìm một số nguyên duy nhất a, 0 <= a <= p-2 sao cho:

a mod p

Ta sẽ xác định số nguyên a bằng (a = mod p )

#### Tạo khóa

***Bước 1:*** Cho p là số nguyên tố sao cho bài toán logarit rời rạc trong Zp là khó giải

***Bước 2:*** Chọn phần tử nguyên thủy ZP\*

***Bước 3:*** Chọn a {2,3,4,….p-2} là khó bí mật thứ nhất (Khóa của người nhận)

***Bước 4:*** Tính mod p

***Bước 5:*** Ta có: Kpub=(p, ; Kpri = (a).

#### Hàm mã hóa

Chọn một số ngẫu nhiên bí mật k Zp-1. Ta xác định eKpub(x,k) = (y1,y2) trong đó:

y1 = k mod p

y2 = x k mod p

#### Hàm giải mã

y1, y2 ZP\* ta xác định: dk(y1,y2) = y2(y1a)-1 mod p

#### Ưu nhược điểm của hệ mật mã Elgamal

* **Ưu điểm:**
* Độ phức tạp của bài toán logarit lớn nên độ an toàn cao
* Bản mã phụ thuộc vào bản rõ x và giá trị ngẫu nhiên nên từ một bản rõ ta có thể có nhiều bản mã khác nhau.
* **Nhược điểm:**
* Tốc độ chậm do phải xử lý với số nguyên lớn
* Dung lượng bộ nhớ dùng cho việc lưu trữ khóa yêu cầu phải lớn.

## Hàm băm SHA

### Khái quát về hàm băm SHA

SHA (Sercure Hash Algorithm – thuật giải băm bảo mật) gồm năm thuật giải được chấp nhận bởi FIPS 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. Những thuật giải này được gọi là “an toàn”, theo chuẩn FIPS 180-2 phát hành ngày 1 tháng 8 năm 2002.

Năm thuật giải SHA là 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), và SHA-512 (trả lại kết quả dài 512 bit). Thuật giải SHA là thuật giải băm được phát triển bởi cục An ninh Quốc Gia Mỹ (NSA – National Security Agency) và được xuất bản thành chuẩn của chính phủ Mỹ bởi Viện Công nghệ và chuẩn Quốc Gia Mỹ (NIST-National Institue of Standards and Technology). Bốn thuật giải sau thường được gọi chung là SHA-2.

Hiện nay, SHA-1 không còn được coi là an toàn bởi đầu năm 2005, ba nhà mật mã học người Trung Quốc đã phát triển thành công một thuật giải dùng để tìm được hai đoạn dữ liệu nhất định có cùng kết quả băm tạo ra bởi SHA-1. Mặc dù chưa có ai làm được điều tương tự với SHA-2, nhưng vì về thuật giả, SHA-2 không khác biệt mấy so với SHA-1. Hiện này đã có thông tin về một hàm băm mới là SHA-3 nhưng còn ở dạng dự thảo. Họ SHA-2 được coi là an toàn để sử dụng hiện nay.

### Hàm băm SHA-2

SHA-2 bao gồm bốn phiên bản SHA-224, SHA-256, SHA-384 và SHA-512. Ba giải thuật SHA-256, SHA-384 và SHA-512 được phát hành lần đầu năm 2001 trong bản phác thảo FIPS PUB 180-2. Năm 2002, FIPS PUB 180-2 SHA-2 được chuẩn hóa và phát hành chính thức. Năm 2004, FIPS PUB 180-2 bổ sung thêm một biến thể SHA-2 đó là SHA-224, với mục đích tạo ra một biến thể SHA-2 có độ dài khóa trùng với DES ba lần với 2 khóa (2TDES) – 112 bit. Những biến thể SHA-2 này được đăng ký bằng sáng chế Hoa Kỳ số 6.829.355

### Ưu nhược điểm hàm băm SHA-2

#### Ưu điểm:

SHA-2 hay SHA nói chung được coi là họ hàm băm an toàn nhất bởi:

* Từ giá trị băm được tạo ra bởi một giải thuật băm SHA, việc tìm lại được đoạn dữ liệu gốc là không khả thi.
* Hai đoạn dữ liệu có cùng kết quả băm tạo ra bởi một trong những giải thuật SHA là không thể xảy ra. Chỉ cần một sự thay đổi nào trên đoạn dữ liệu gốc dù nhỏ cũng sẽ tạo nên một giá trị băm khác hoàn toàn so với xác hiệu ứng nở tuyết.

#### Nhược điểm

Hiện nay SHA-1 không còn được coi là an toàn tuyệt đối tuy SHA-2 vẫn an toàn. Tuy nhiên thuật toán SHA-2 không khác biệt nhiều so với SHA-1 do đó việc phá được nó chỉ là không lâu nữa. Do đó, cần phải phát triển các thuật toán băm mới an toàn hơn cho tương lai.

# KẾT QUẢ NGHIÊN CỨU

## Giới thiệu

* Tên đề tài nghiên cứu: Tìm hiểu chữ ký điện tử Elgamal và viết ứng dụng minh họa.
* Các bước thực hiện triển khai đề tài bao gồm:
* Nghiên cứu nội dung các thuật toán, các nội dung liên quan đến yêu cầu đề tài.
* Thiết kế và cài đặt chương trình demo theo đề tài.
* Hình thức sản phẩm: Bài tập lớn, Chương trình demo
* Kết quả đạt được: Nghiên cứu, cài đặt chương trình demo đề tài.

## Nội dung thuật toán

***Bước 1:*** Tạo cặp khóa Kpub, Kpri

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

+ Chọn phần tử nguyên thủy Zp\*

+ Chọn a {2, 3, 4, 5….p-2} là khó a bí mật thứ nhất

+ Tính mod p

* Xác định Kpub={p,}; Kpri={a}.

***Bước 2:*** Ký số

+ Chọn số ngẫu nhiên bí mật k sao cho k Zp-1

+ Tính k mod p; = (x-a\*) k-1 mod (p-1)

+ Chữ ký trên x p là y = sigk(x,y) =

***Bước 3:*** Kiểm tra chữ ký

+ ver(x, ) = TRUE ⬄ x mod p

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

### Giao diện chương trình demo

#### Giao diện demo theo ngôn ngữ Java

Graphical user interface, application

Description automatically generated

#### Giao diện demo theo ngôn ngữ Javascript

Graphical user interface, text

Description automatically generated

#### Giao diện demo theo ngôn ngữ Python

Graphical user interface, application

Description automatically generated

#### Giao diện demo theo ngôn ngữ C#

Graphical user interface, application

Description automatically generated

## Cài đặt và triển khai

### Giới thiệu công cụ

#### Giới thiệu công cụ Netbeans

Netbeans được biết đến là một công cụ hỗ trợ lập trình cũng như viết mã code hoàn toàn miễn phí, chủ yếu được tin dùng bởi các lập trình viên xây dựng và phát triển phần mềm Java.

Xuất hiện trên thị trường từ năm 1996, Netbeans đã được nghiên cứu và cải thiện trong suốt 25 năm qua để vươn lên trở thành môi trường lập trình sử dụng rộng rãi ở thời điểm hiện tại.

Để mang đến sự tiện lợi tối đa trong quá trình sử dụng, Netbeans hiện đã hỗ trợ 3 hệ điều hành phổ biến nhất trên máy tính là Windows, macOS và Linux. Nhưng dung lượng của công cụ này khá nặng nên bạn cần có một thiết bị với cấu hình cao để có thể tận hưởng trải nghiệm tốt nhất.

#### Giới thiệu công cụ Visual Studio Code

Visual Studio Code (VS Code hay VSC) là một trong những trình soạn thảo mã nguồn phổ biến nhất được sử dụng bởi các lập trình viên. Nhanh, nhẹ, hỗ trợ đa nền tảng, nhiều tính năng và là mã nguồn mở chính là những ưu điểm vượt trội khiến VS Code ngày càng được ứng dụng rộng rãi.

Visual Studio Code hỗ trợ nhiều ngôn ngữ lập trình như C/C++, C#, F#, Visual Basic, HTML, CSS, JavaScript, … Vì vậy, nó dễ dàng phát hiện và đưa ra thông báo nếu chương chương trình có lỗi.

#### Giới thiệu công cụ PyCharm

PyCharm là một nền tảng phát triển tích hợp tối đa nền tảng (IDE) được thiết kế dành riêng cho các lập trình viên Python. Phần mềm này được JetBrains phát triển nhằm mục đích cung cấp tất cả các công cụ cần thiết để tăng năng suất của các lập trình viên Python. Pycharm được trang bị sẵn các yếu tố mở rộng bao gồm biên dịch mã, điều hướng project nhanh, tô sáng cú pháp, công cụ cơ sở dữ liệu và trình soạn thảo văn bản có lập trình để thúc đẩy phát triển Web.

Tương tự như Python, PyCharm là một trong những IDE được nhiều người tin tưởng và sử dụng rộng rãi nhất trong các ngôn ngữ lập trình. Ngày nay, những doanh nghiệp có sức ảnh hưởng như Twitter, Symantec và Pinterest cũng đang dùng công cụ Pycharm để làm IDE Python.

Một trong những ưu thế vượt trội của việc sử dụng PyCharm là nó cung cấp API cho các nhà phát triển và cho phép họ viết các plugin của riêng mình để mở rộng các tính năng. Phần mềm này tương thích với Windows, Linux và macOS, hỗ trợ các lập trình viên Python tiết kiệm được rất nhiều thời gian trong lúc viết nhiều ứng dụng một cách hiệu quả.

### Hướng dẫn cài đặt và chạy chương trình demo đã cài đặt

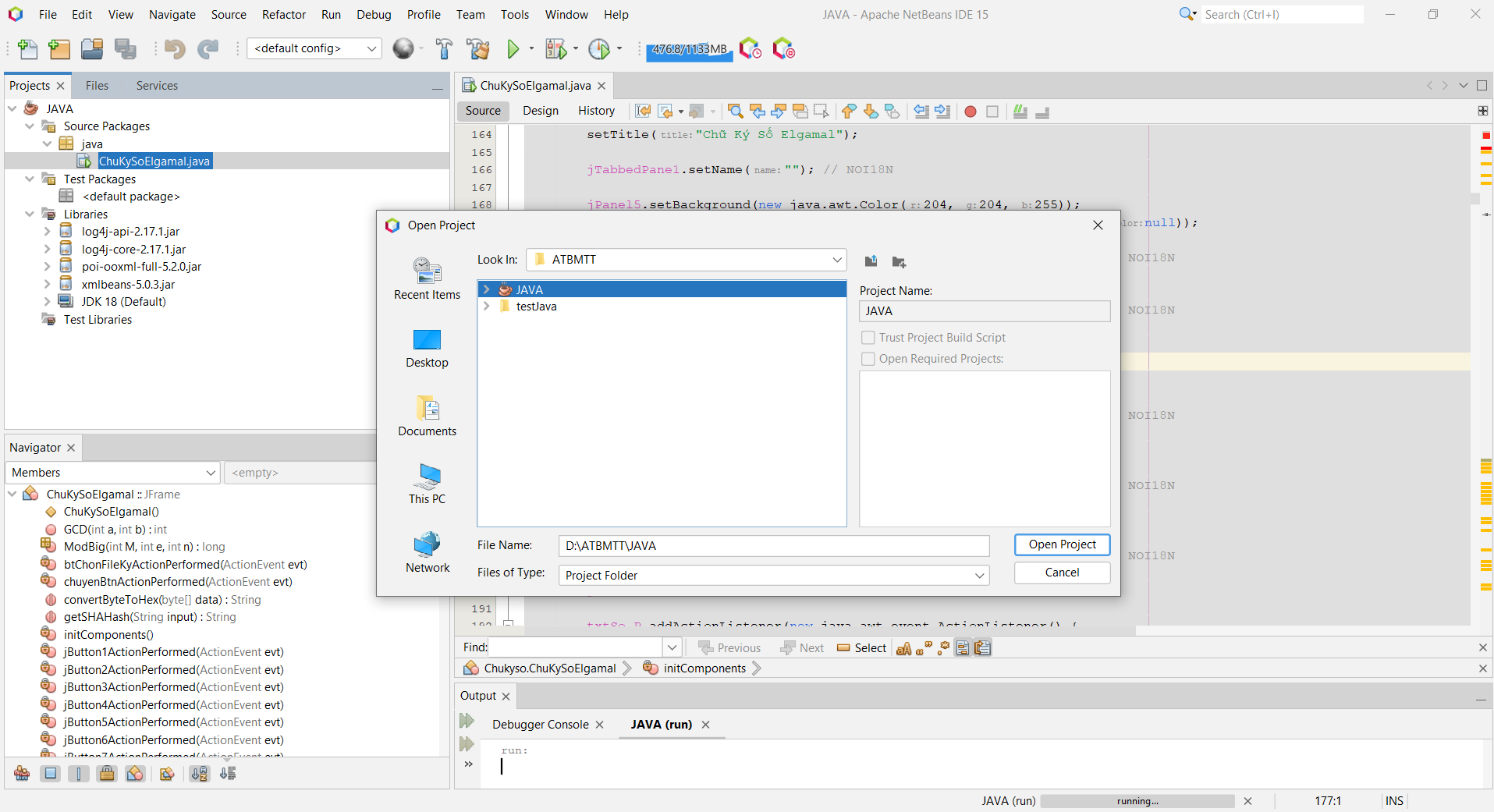
#### Cài đặt Netbeans và chạy chương trình demo

***Cài đặt Netbeans:***

* Bước 1: Truy cập trang https://netbeans.apache.org/ để tải công cụ Netbeans IDE về máy
* Bước 2: Mở file sau khi đã tải thành công
* Bước 3: Ấn theo hướng dẫn cài đặt của phần mềm
* Bước 4: Thiết lập biến môi trường
* Bước 5: Mở công cụ và hoàn tất cài đặt

***Chạy chương trình demo:***

* B1: Ở giao diện làm việc của Netbeans IDE, vào file chọn open project rồi chọn project cần chạy.

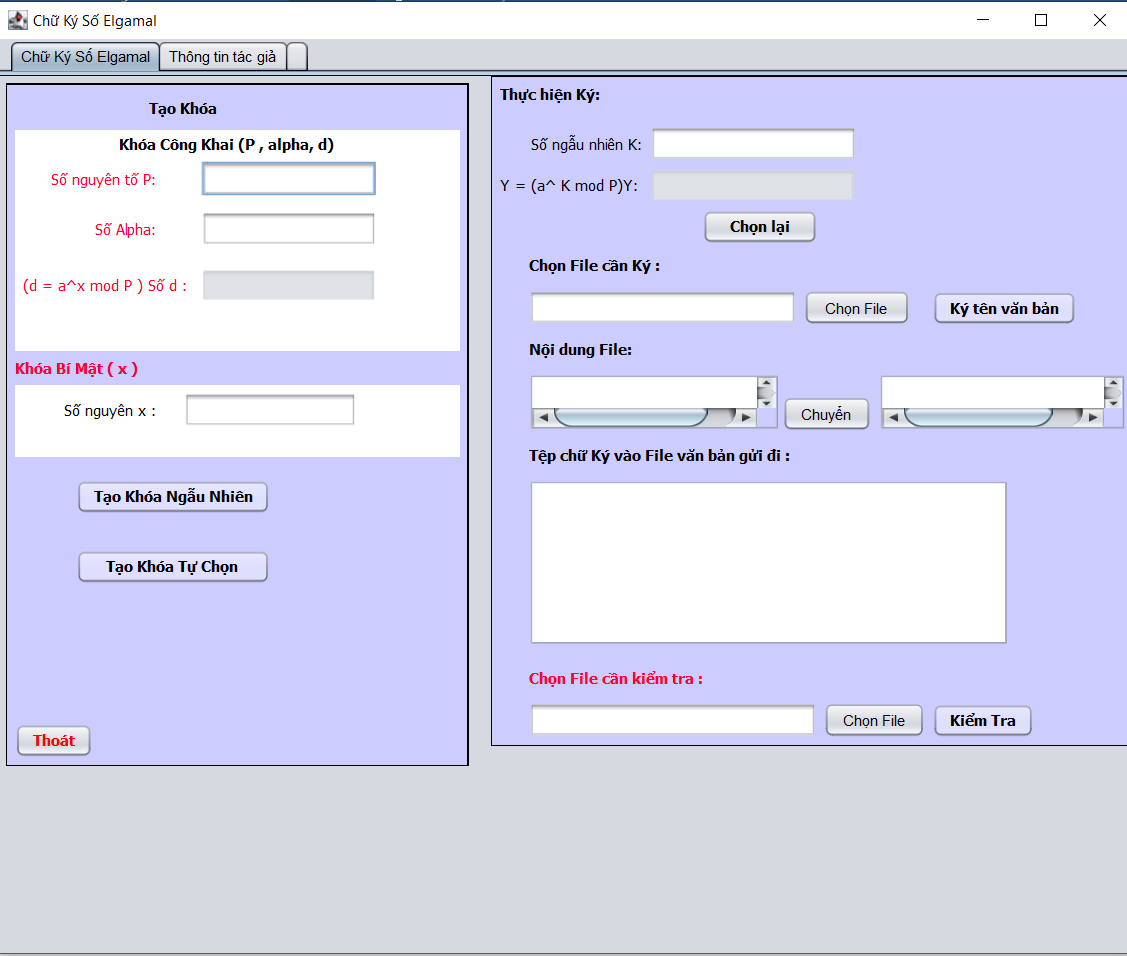


* B2: Click vào nút run trên thanh công cụ hoặc nhấp chuột phải vào tên project và chọn run.

Graphical user interface, application

Description automatically generated

* B3: Lúc này chương trình demo bắt đầu chạy. Đây là giao diện chưong trình:



* B4: Để sử dụng chương trình thì người dùng ấn nút "Tạo khóa ngẫu nhiên" và "Tạo khóa tự chọn" để chương trình tự sinh ra khóa:

Graphical user interface, application, Word

Description automatically generated

* B5: Tiếp theo người dùng sẽ nhấn open file rồi chọn file chứa thông điệp muốn ký.

Graphical user interface, application

Description automatically generated

* B6: Click chuột vào nút "Ký tên văn bản" để có được tệp chữ ký:

Graphical user interface, application

Description automatically generated

* B7: Người dùng bấm “Chọn file” để chọn file muốn kiểm tra trước khi ký:

Graphical user interface, application

Description automatically generated

* B8: Click chuột vào nút "Kiểm tra" để xem file có bị sửa đổi hay chưa:

Graphical user interface, application

Description automatically generated

* B9: Click vào nút “Chọn lại” để xóa toàn bộ thông tin trên cửa sổ chương trình, chương trình sẽ trở về ban đầu như khi ta khởi động chương trình.

Graphical user interface, application

Description automatically generated

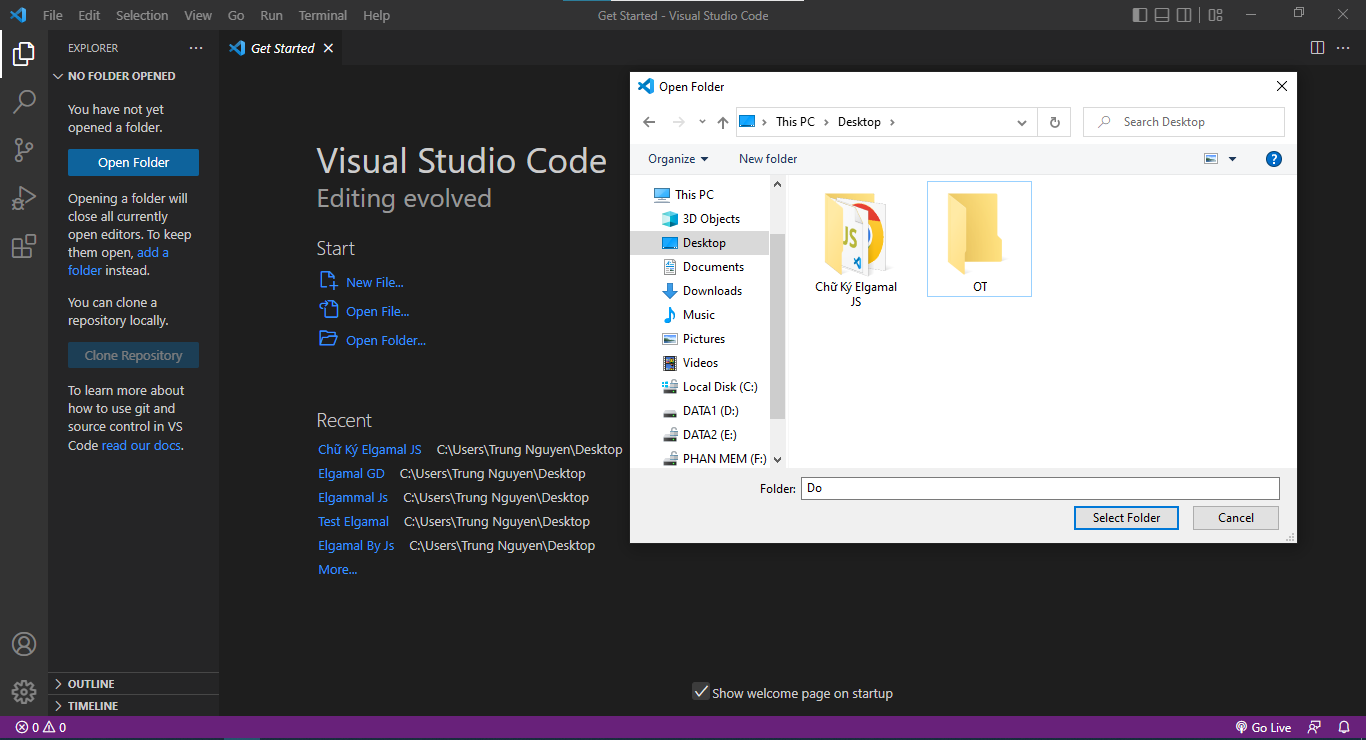
#### Cài đặt Visual Studio Code và chạy chương trình demo

***Cài đặt Visual Studio Code***

* Bước 1. Tải file cài đặt Visual Studio Code cho Windows.
* Bước 2. Sau khi tải xong, tiến hành khởi chạy file đã tải ở bước 1, file đó sẽ có tên dạng VSCodeUserSetup-{version}.exe.
* Bước 3. Nhấp vào Next để cài đặt. Tiếp theo đồng ý điều khoản sử dụng.
* Bước 4: Lựa chọn nơi cài đặt (Nếu bạn không rành, nên để mặc định, ổ C) sau đó nhấn Next để cài.
* Bước 5. Các bước tiếp theo tiếp tục nhấn Next cho tới khi hoàn tất. Trong quá trình này, mình khuyên các bạn nên tích chọn vào 2 chức năng: (1) Add “Open with Code” action to Windows Explorer file context menu và (2) Add “Open with Code” action to Windows Explorer directory context menu. Việc này giúp bạn có thể click chuột phải vào thư mục sẽ có lựa chọn mở bằng VS Code.
* Bước 6. Cài đặt hoàn tất, bạn có thể trải nghiệm.

***Chạy chương trình demo:***

* B1: Ở giao diện làm việc của Visual Studio Code, vào open folder chọn thư mục chứa file Chữ ký Elgamal.



* B2: Chọn và mở file html trên trình duyệt:

A screenshot of a computer

Description automatically generated with medium confidence

* B3: Nhập khóa hoặc tự động nhập

Graphical user interface, text, application

Description automatically generated

* B4: Chọn file văn bản cần ký

Graphical user interface, text, application

Description automatically generated

* B5:Thực hiện ký văn bản:

Graphical user interface

Description automatically generated

* B6: Lưu Văn Bản Ký:

Text

Description automatically generated

* B7: Chọn file văn bản cần kiểm tra:

Graphical user interface, text, application

Description automatically generated

* B8: Hiển thị thông báo:

Graphical user interface, text

Description automatically generated

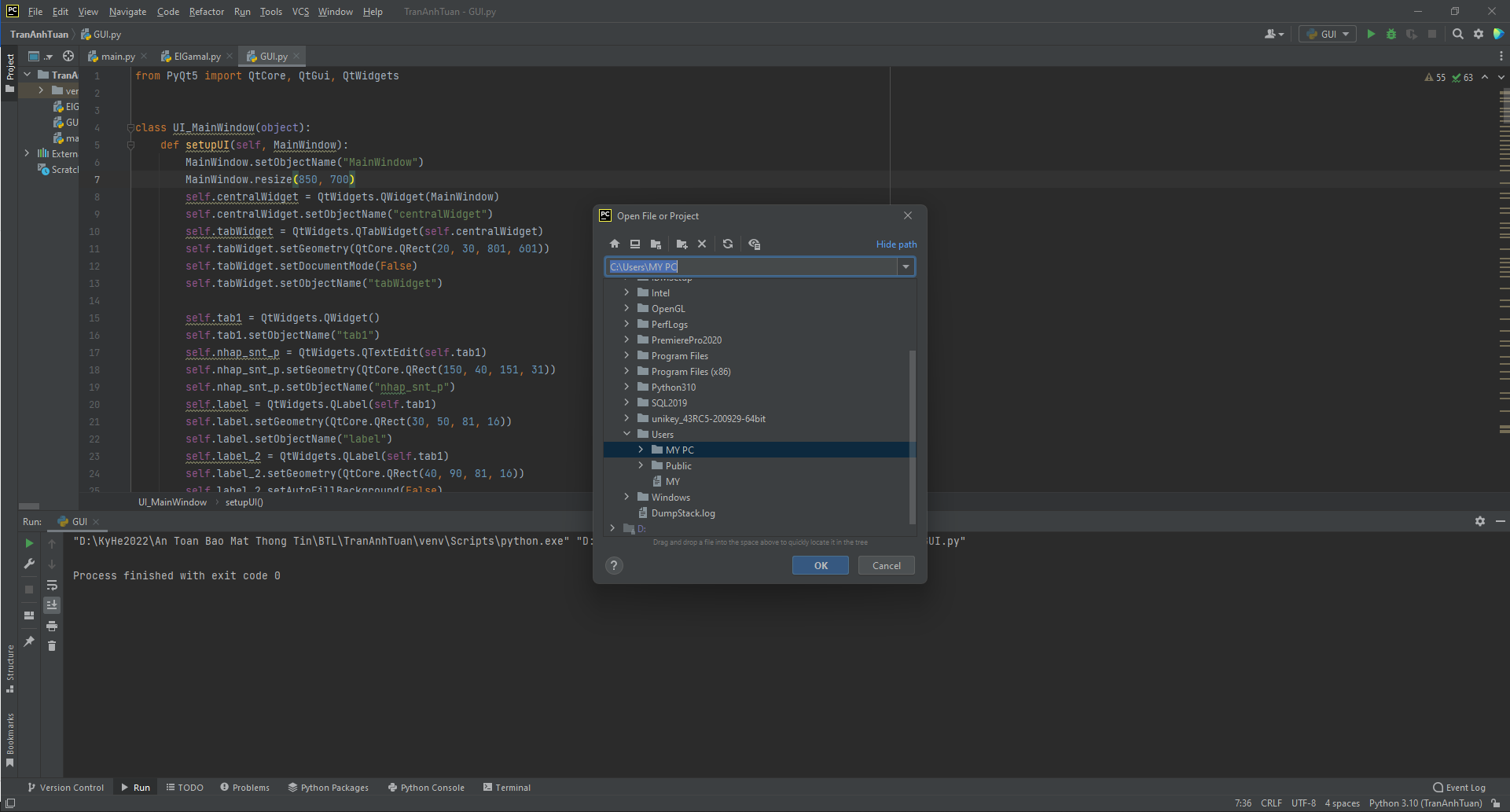
#### Cài đặt PyCharm và chạy chương trình demo

***Cài đặt PyCharm***

* Bước 1: Truy cập vào trang chủ của PyCharm và nhấn Download để tải phần mềm về máy tính. Lưu ý: Chọn bản Commynity
* Bước 2. Sau khi tải xong, tiến hành khởi chạy file đã tải ở bước 1, file đó sẽ có tên dạng pycharm-community.exe.
* Bước 3. Nhấp vào Next để cài đặt. Tiếp theo đồng ý điều khoản sử dụng.
* Bước 4: Lựa chọn nơi cài đặt (Nếu bạn không rành, nên để mặc định, ổ C) sau đó tiếp tục nhấn Next để hoàn tất .
* Bước 5: Cài đặt hoàn tất, ứng dụng sẵn sàng cho bạn trải nghiệm

***Chạy chương trình demo***

* B1: Trong giao diện làm việc của PyCharm bạn chọn File Open… rồi chọn tới project cần chạy.



* B2: Chọn vào file main.py, sau đó kích vào biểu tượng Run góc phải màn hình hoặc ấn tổ hợp phím Ctrl + Shift + F10 để chạy chương trình.

A screenshot of a computer

Description automatically generated

* B3:Lúc này chương trình demo sẽ được chạy. Đây là giao diện chương trình:

Graphical user interface, application

Description automatically generated

* B4: Để sử dụng chương trình người dùng có thể nhập các giá trị p, alpha, Xa, k vào hoặc ấn vào “Sinh khóa tự động” để chương trình sinh ra khóa

Graphical user interface, application

Description automatically generated

* B5: Sau đó người dùng ấn nút Tạo khóa công khai để chương trình tạo khóa công khai từ các khóa vừa được sinh tự động

Graphical user interface, application

Description automatically generated

* B6: Tiếp theo người dùng ấn “Chọn tệp” để chọn tệp chứa thông điệp muốn kí

A picture containing text, screenshot, monitor, black

Description automatically generated

* B6: Click chuột vào nút “Gửi” để ký băn bản và gửi cho người nhận xác thực

Graphical user interface, application

Description automatically generated

* B7: Để xác thực văn bản ta ấn sang tab “Xác thực” khi đó khóa công khai đã được chuyển sang. Ta click vào “Chọn file xác thực” sau đó chọn file cần xác thực. Kết quả sẽ hiện lên mà hình:

Graphical user interface, text, application

Description automatically generated

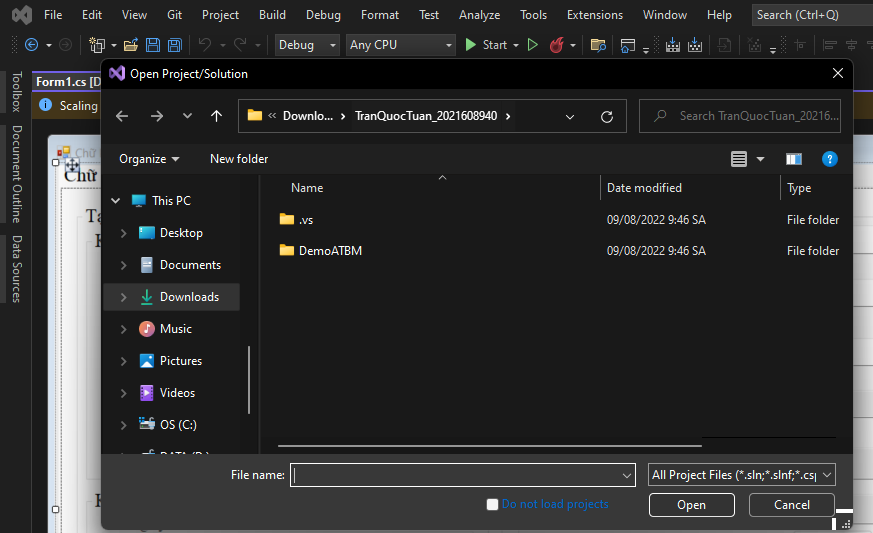
#### Cài đặt Visual Studio và chạy chương trình demo

***Cài đặt Visual Studio***

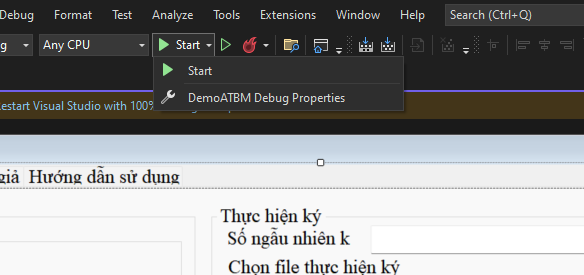
* Bước 1: Truy cập trang Visual Studio, tải xuống và cài đặt theo hướng dẫn của chương trình
* Bước 2: Mở file sau khi đã tải thành công
* Bước 3: Ấn theo hướng dẫn cài đặt của phần mềm
* Bước 4: Thiết lập biến môi trường
* Bước 5: Mở công cụ và hoàn tất cài đặt

***Chạy chương trình demo***

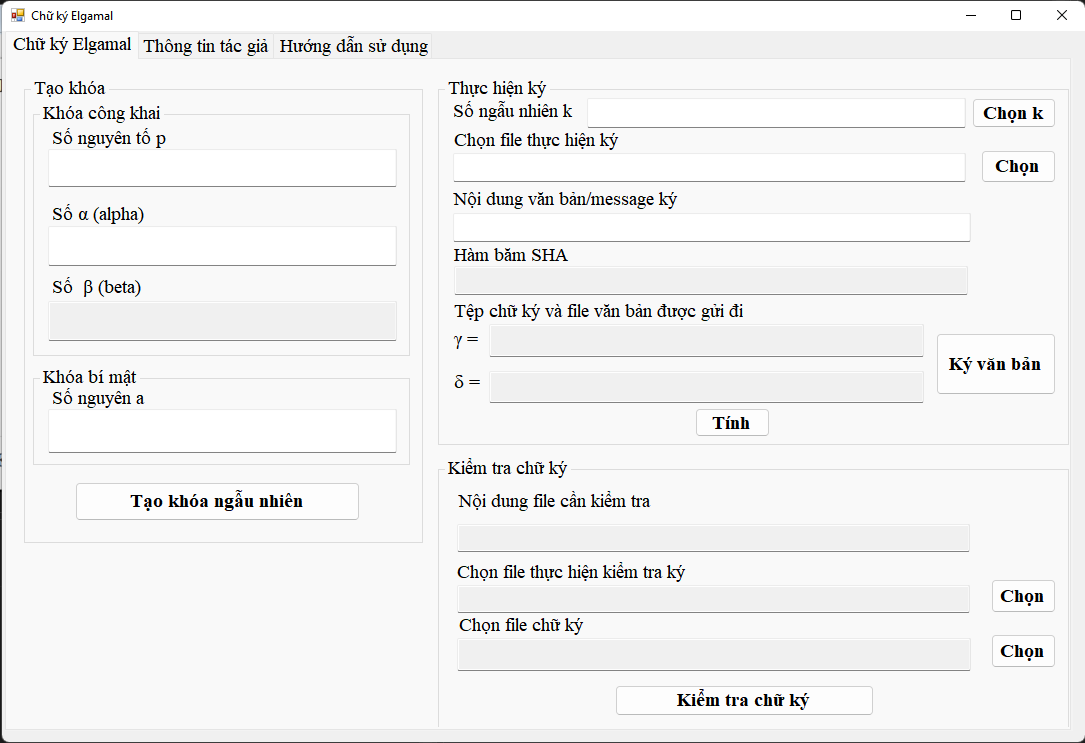
* B1: Ở giao diện làm việc của Visual Studio, Vào file chọn Open sau đó chọn Open File/Solution và chọn Solution cần chạy



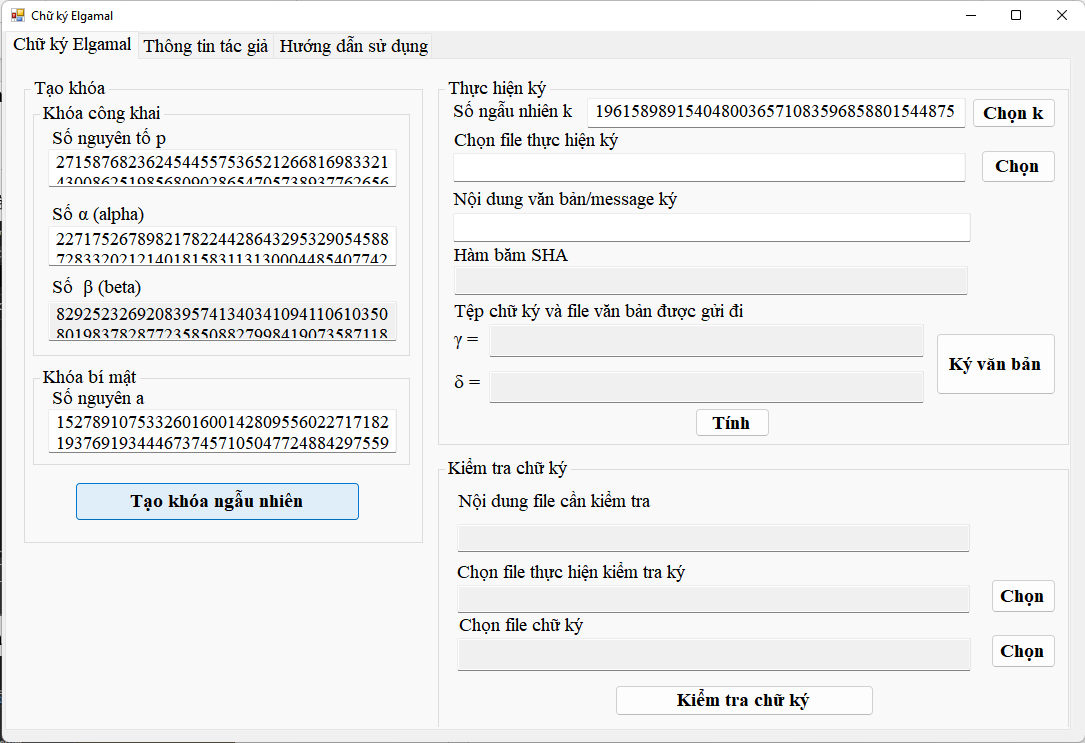
* B2: Click vào nút Start trên thanh công cụ để chạy project.



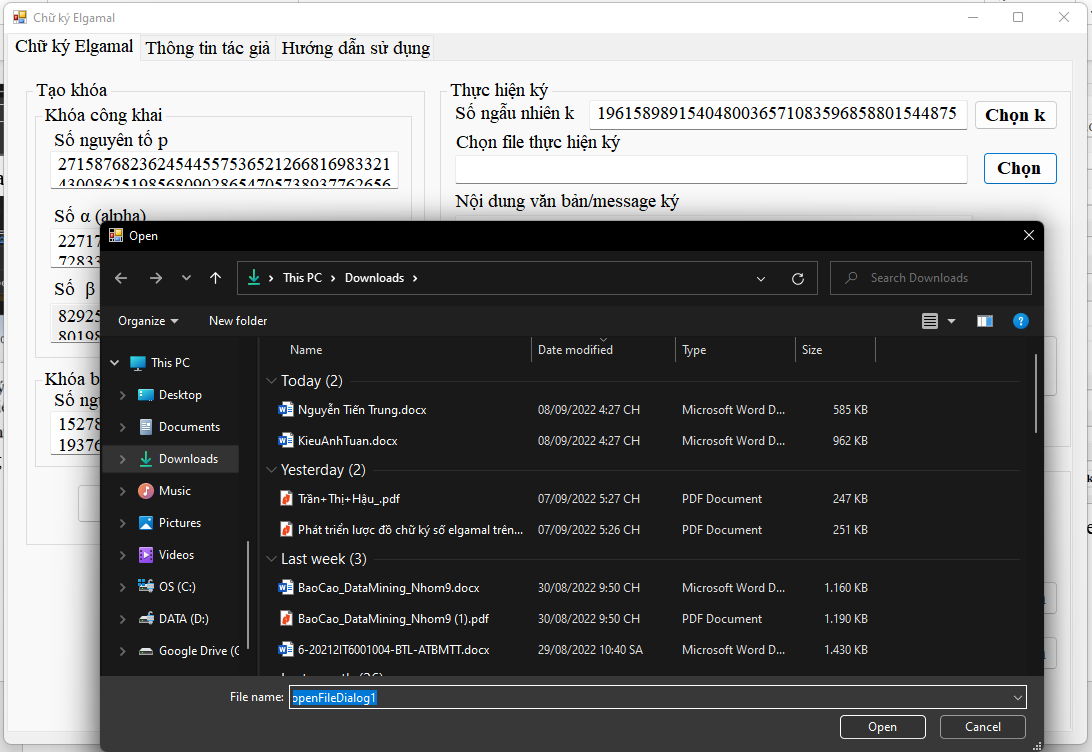
* B3: Lúc này chương trình demo bắt đầu chạy. Đây là giao diện chương trình:



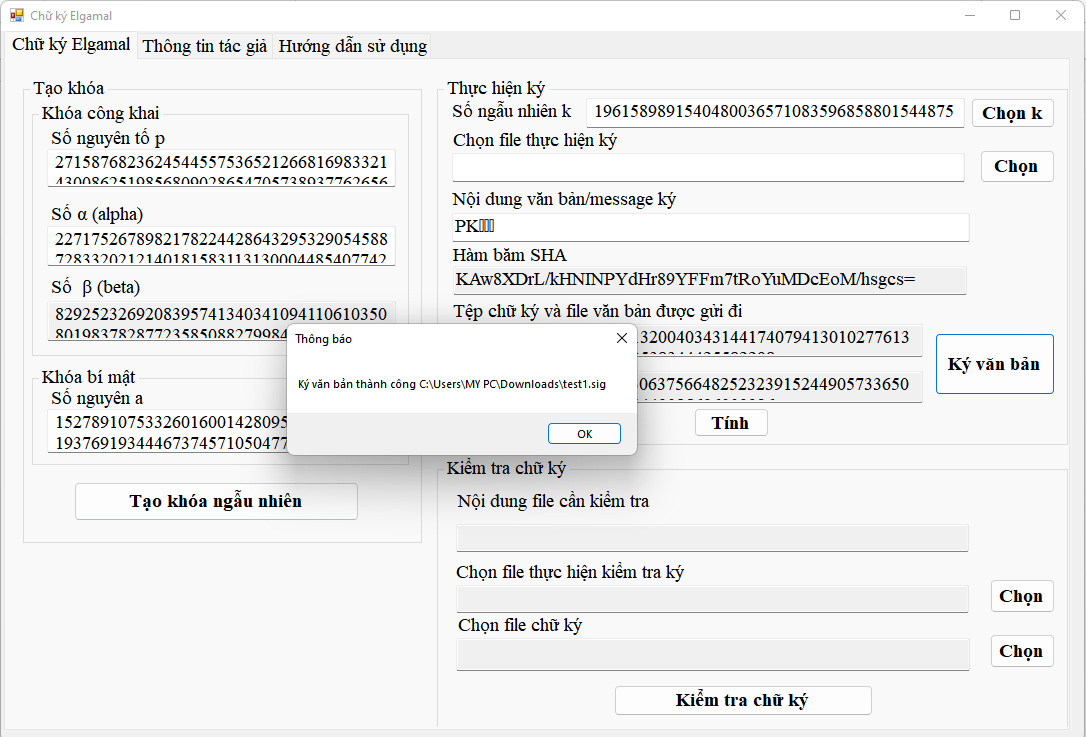
* B4: Để sử dụng chương trình thì người dùng ấn nút "Tạo khóa ngẫu nhiên" để chương trình tự sinh ra khóa:



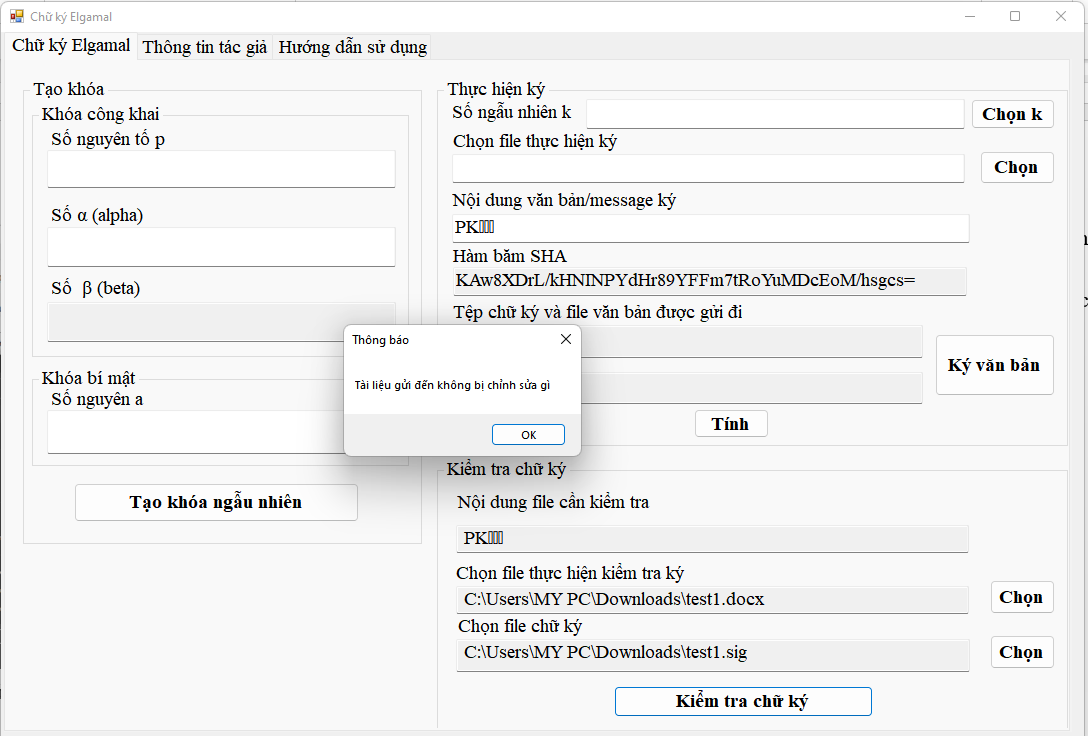
* B5: Tiếp theo người dùng ấn Chọn để chọn file muốn kí



* B6: Click chuột vào nút Tính và nút "Ký tên văn bản" để có được tệp chữ ký:



* B7: Ở phần kiểm tra chữ ký, kích chọn “Chọn” Sau Chọn file thực hiện kiểm tra ký để kiểm tra chữ ký. Sau đó ấn nút “Kiểm tra chữ k” để tiến hành kiểm tra. Kiểm tra thành công sẽ có thông báo như sau:



## Thực hiện bài toán

### Phân công công việc

|  |  |
| --- | --- |
| **Tên sinh viên** | **Tên công việc** |
| Nguyễn Tiến Trung | * Nghiên cứu và tìm hiểu về sơ đồ chữ kí số * Tìm hiểu về thuật toán tạo chữ ký số Elgamal |
| Kiều Anh Tuân | * Nghiên cứu và tìm hiểu về sơ đồ chữ kí số Elgamal * Tìm hiểu về thuật toán tạo chữ ký số Elgamal |
| Trần Anh Tuấn | * Nghiên cứu và tìm hiểu về hàm băm SHA * Tìm hiểu về thuật toán tạo chữ ký số Elgamal |
| Trần Quốc Tuấn | * Nghiên cứu và tìm hiểu về mã hóa bất đối xứng và ứng dụng trong chữ kí điện tử * Tìm hiểu về thuật toán tạo chữ ký số Elgamal |

### Nguyễn Tiến Trung – Nghiên cứu và tìm hiểu về sơ đồ chữ kí số

* Tìm hiểu, đúc kết nội dung để thêm vào bài tập lớn về công việc được phân công
* Viết chương trình demo với ngôn ngữ JavaScript

### Kiều Anh Tuân – Nghiên cứu và tìm hiểu về sơ đồ chữ kí Elgamal

* Tìm hiểu, đúc kết nội dung để thêm vào bài tập lớn về công việc được phân công
* Viết chương trình demo với ngôn ngữ Java

### Trần Anh Tuấn – Nghiên cứu và tìm hiểu về hàm băm SHA

* Tìm hiểu, đúc kết nội dung để thêm vào bài tập lớn về công việc được phân công
* Viết chương trình demo với ngôn ngữ Python

### Trần Quốc Tuấn – Nghiên cứu và tìm hiểu về mã hóa bất đối xứng và ứng dụng trong chữ kí điện tử

* Tìm hiểu, đúc kết nội dung để thêm vào bài tập lớn về công việc được phân công
* Viết chương trình demo với ngôn ngữ C#

# KIẾN THỨC LÍNH HỘI VÀ BÀI HỌC KINH NGHIỆM

## Nội dung đã thực hiện

### Các kiến thức đã học được

* Khái niệm, công dụng, định nghĩa của chữ kí số.
* Sơ đồ chữ kí số Elgamal
* Cơ sở lý thuyết xây dựng sơ đồ chữ kí số Elgamal
* Quá trình hình thành, xây dựng các khóa của sơ đồ chữ kí số Elgamal
* Tầm quan trọng, ưu, nhược điểm của sơ đồ chữ kí số Elgamal
* Phương pháp mã hóa bất đối xứng
* Hệ mật mã Elgamal (Tạo khóa, mã hóa, giải mã)
* Ứng dụng của phương pháp mã hóa bất đối xứng trong chữ kí số
* Kiến thức cơ bản về hàm băm SHA
* Các ưu nhược điểm, công dụng của hàm băm SHA

### Những kỹ năng đã học được

* Đánh giá được vai trò của bảo mật thông tin, các cơ chế, chính sách bảo mật, các kiểu tấn công và phương pháp phòng chống.
* Hiểu và áp dụng các thuật toán liên quan đến hệ mã hóa Elgamal như (thuật toán sinh khóa, thuật toán mã hóa, thuật toán giải mã cùng vời các thuật toán liên quan như thuật toán nghịch đảo của phép nhân modulo hay thuật toán bình phưong và nhân trong modulo) vào việc mã hóa và giải mã để giải quyết bài toán có tính ứng dụng vào thực tiễn.
* Nâng cao kỹ năng hoạt động nhóm
* Tìm hiểu về một vấn đề qua Internet
* Đọc hiểu tài liệu trong nước và nước ngoài (tiếng Anh)
* Tự thiết kế một chương trình bằng ngôn ngữ tự chọn, xử lý lỗi trong quá trình thực hiện.

### Những bài học kinh nghiệm được rút ra

* Các tài liệu quan trọng và chính thống liên quan đến chữ kí số Elgamal chủ yếu được viết bằng tiếng Anh nên các thành viên trong nhóm phải trau rèn khả năng ngoại ngữ để có thể đọc hiểu được một số tài liệu liên quan đến chữ kí số Elgamal và công cụ, ngôn ngữ lập trình.
* Trong quá trình thực hiện viết chương trình các thành viên trong nhóm gặp rất nhiều vấn đề về việc mã hóa và giải mã thông qua file, đặc biệt là lấy bản rõ bằng cách open file docx. Do đó các thành viên trong nhóm đã đúc kết được kinh nghiệm về việc xử lý file và hiểu được trách nhiệm phải quan tâm nhiều hơn đến dữ liệu người dùng nhập vào, người dùng có thể nhập bản rõ vào phần mềm bằng nhiều cách khác nhau và phải xử lý để các các dữ liệu đó hoạt động thật mượt mà và trơn tru.
* Mỗi thành viên trong nhóm cần học tập, thực hành nhiều hơn với các ngôn ngữ, các công cụ để thuận tiện hơn trong học tập cũng như làm việc sau này

## Hướng phát triển

### Tính khả thi của chủ đề nghiên cứu

Chủ đề nghiên cứu của nhóm khá phù hợp với thời gian được cho phép để hoàn thiện bài tập lớn, bên cạnh đó trong thời gian nhóm nghiên cứu, nhóm nhận thấy cần phải thực sự hiểu rõ về hệ mật mã Elgamal cũng như sơ đồ chữ kí Elgamal và có kỹ thuật lập trình ở mức khá là đã có thể hoàn thiện đề tài nghiên cứu.

### Những thuận lợi và khó khăn trong quá trình nghiên cứu đề tài

#### Thuận lợi

* Có kiến thức lập trình từ năm học trước nên vấn đề về phân chia ngôn ngữ lập trình cho các thành viên trong nhóm khá dễ dàng, và việc chuyển từ ngôn ngữ sở trường sang các ngôn ngữ khác đều không gặp nhiều vấn đề
* Có thể đọc hiểu được tài liệu tiếng Anh nên có thể dễ dàng tiếp cận các nguồn tài liệu chính thống
* Các thành viên trong nhóm hòa đồng, cởi mở, tương tác với các thành viên khác trong nhóm khá sôi nổi nên các công việc liên quan đến cả nhóm thường diễn ra khá suôn sẻ

#### Khó khăn

* Công đoạn thiết giao diện phần mềm mã hóa chưa được bắt mắt do chưa có nhiều kinh nghiệm trong kỹ thuật xử lý giao diện
* Ở phần xử lý về File Docx sử dụng để lấy nội dung cho vào giao diện do chưa có kinh nghiệm xử lý nên vẫn chưa có được chuẩn theo yêu cầu đề ra.

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

Với thời đại hiện nay, lượng thông tin được sử dụng là vô cùng lớn, đi cùng với đó là nhu cầu về bảo mật tính toàn vẹn, định danh của thông tin cũng phát triển bùng nổ. Vì vậy cuốn bài tập lớn này có thể nói là một bước khởi đầu cho việc xây dựng một chương trình lớn có công dụng ký những văn bản quan trọng nằm đảm bảo tính toàn vẹn của văn bản đó. Tuy nhiên đây cũng chỉ nằm ở mức tìm hiểu với những chương trình demo đơn giản, nếu muốn phát triển rộng hơn chúng ta cần nghiên cứu thêm nhiều về các cách tối ưu hóa thuật toán, ngoài ra nhóm đề xuất phát triển thêm phần đọc File có thể đọc được nhiều loại file hơn.

# TÀI LIỆU THAM KHẢO

[1]Giáo trình An toàn bảo mật thông tin – Trường đại học Công nghiệp Hà Nội.

Ngoài kiến thức của giáo trình nhóm cũng có tham khảo thêm một số nguồn khác trên Internet

[2] Mã hóa phi đối xứng và ứng dụng của nó trong chứng thực điện tử - [Link](https://viblo.asia/p/ma-hoa-phi-doi-xung-va-ung-dung-cua-no-trong-chung-thuc-dien-tu-yMnKMqpAK7P)

[3] Giới thiệu về một số hàm băm và ứng dụng trong một số sản phẩm mật mã dân sự - [Link](https://nacis.gov.vn/nghien-cuu-trao-doi/-/view-content/213743/gioi-thieu-ve-mot-so-ham-bam-va-ung-dung-trong-mot-so-san-pham-mat-ma-dan-su)