Nhom4 Bao Cao BTL Atbmtt 20221 IT6001001

Cơ bản công nghệ thông tin (Trường Đại học Công nghiệp Hà Nội)

TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI

KHOA CÔNG NGHỆ THÔNG TIN

-----□□□□□-----

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

CBHD: *ThS. Trần Phương Nhung*

Nhóm: 4

Thành viên nhóm

Nguyễn Khắc Hiếu – 2019602187

Vũ Huy Hoàng – 2019601826

Nguyễn Đình Hoàng – 2020602666

Vũ Văn Hiếu - 2019606157

Nguyễn Khắc Hùng - 2018602426

HÀ NỘI - 2022

LỜI CẢM ƠN

Báo cáo bài tập lớn với đề tài "**Tìm hiểu về chữ ký điện tử ElGamal và viết ứng dụng minh họa**" là kết quả của quá trình cố gắng không ngừng của cả nhóm, động viên khích lệ, giúp đỡ của giảng viên Trần Phương Nhung. Qua trang viết này chúng em xin gửi lời cảm ơn tới những người đã giúp đỡ chúng em trong thời gian học tập - nghiên cứu vừa qua.

Chúng em xin tỏ lòng kính trọng và biết ơn sâu sắc đối với cô giáo Trần Phương Nhung đã trực tiếp tận tình hướng dẫn cũng như cung cấp tài liệu thông tin khoa học cần thiết cho bài tập này của chúng em.

Cuối cùng chúng em kính chúc cô dồi dào sức khỏe và thành công trong sự nghiệp cao quý.

Nhóm 4 thực hiện

MỤC LỤC

DANH SÁCH CÁC HÌNH

Chương 1. Tổng quan

1.1 Tổng quát về đề tài

Ngày nay cùng với sự phát triển của khoa học kỹ thuật hiện đại, công nghệ thông tin đã giúp nhiều trong các lĩnh vực đời sống của con người. Mạng Internet với tốc độ nhanh, lượng thông tin trao đổi có thể rất lớn và đặc biệt không hạn chế người sử dụng, giúp cho con người có thể trao đổi với nhau nhanh hơn, chính xác hơn và hiệu quả hơn. Sự ra đời của văn bản điện tử đã kéo theo sự xuất hiện của giao dịch điện tử, từ đó phát sinh nhu cầu ký trên văn bản điện tử để thực hiện được các giao dịch ấy, và đó cũng là lúc mà chữ ký số ra đời và đóng vai trò quan trọng trong việc xác minh tính toàn vẹn của văn bản, thông điệp.

Qua dự án lần này nhóm sinh viên chúng em đã đi sâu tìm hiểu về lược đồ chữ ký điện tử Elgamal , nắm được những kiến thức cơ bản trong phương pháp mã hóa bất đối xứng và có những hiểu biết về hàm băm SHA(Hash).Và từ đó mỗi cá nhân trong nhóm có thể ứng dụng và tạo ra chương trình “Chữ ký điện tử Elgamal” bằng những ngôn ngữ khác nhau: Java, C++, C#, python, javascript,... có thể xác minh tính toàn vẹn của tài liệu.

1.2 Lý do chọn đề tài

Bảo mật thông tin luôn là vấn đề quan trọng hàng đầu trong các lĩnh vực tình báo, quân sự, ngoại giao, và đây cũng là một vấn đề đã được nghiên cứu hàng nghìn năm nay. Bảo mật thông tin là duy trì tính bảo mật, tính toàn vẹn và tính sẵn sàng

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

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

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

1.3 Nội dung nghiên cứu

- Tìm hiểu về chữ ký điện tử

  - Giới thiệu về chữ ký điện tử

- Khái niệm thế nào là chữ ký điện tử ?
- Ứng dụng của chữ ký điện tử
- Tầm quan trọng
- Một số ưu nhược điểm của chữ ký điện tử.

➢ Chữ ký điện tử ElGamal

- Lược đồ chữ ký điện tử ElGamal.
- Ví dụ minh hoạ.
- Độ an toàn của chữ ký điện tử ElGamal

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

- Mã hóa bất đối xứng là gì?
- Đặc điểm
  - Ưu điểm
  - Hạn chế
- Ứng dụng trong chữ ký số
  - Chữ ký số
  - Chữ ký số sử dụng hệ mật mã Elgamal
  - Ưu điểm
  - Ý nghĩa

➢ Tìm hiểu về hàm băm SHA

- Giới thiệu hàm băm Hash
- Tính chất cơ bản của hàm băm Hash
- Danh sách các hàm băm mật mã học
- Ứng dụng hàm băm Hash

- Thuật toán hàm băm SHA-1
  - Giới thiệu hàm băm SHA-1
  - Thuật toán băm SHA-1
- Thuật toán hàm băm SHA-256
  - Mã hoá SHA-256 là gì ?
  - Ứng dụng của SHA-256

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

1.4 Các kiến thức cần có

➢ Các kiến thức về thuật toán, định lý:

- Nắm rõ các kiến thức cơ bản về Chữ ký điện tử (Định nghĩa, lợi ích, vai trò,...)
- Kiến thức về chữ ký điện tử Elgamal(Lược đồ chữ ký điện tử Elgamal, cách tạo chữ ký , cách xác minh chữ ký ,...)
- Phương pháp mã hóa bất đối xứng , và ứng dụng của phương pháp mã hóa bất đối xứng vào trong quá trình tạo và xác minh chữ ký điện tử
- Kiến thức về hàm Băm(Hash) và ứng dụng của nó trong quá trình tạo chữ điện tử

➢ Các kiến thức ngôn ngữ lập trình :

+ Java
+ C#
+ C++
+ JavaScript

+ Python

- Kiến thức về sử dụng các công cụ lập trình
  + Đối với Java : Eclipse
  + Đối với C++ : Visual studio 2019/ DevC++
  + Đối với C# : Visual studio 2019
  + Đối với Python : PyCharm/ Visual studio code
  + Đối với JavaScript : Sublime text/Visual studio code

1.5 Lĩnh vực hoạt động

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

quan trọng nhất là minh bạch hóa thông tin, làm thay đổi phương pháp, tác phong công tác, phương thức làm việc...

Ứng dụng chữ ký số:

- Trong chính phủ điện tử
  - Khai báo hải quan điện tử, thuế điện tử
  - Khai sinh, khai tử
  - Cấp các loại giấy tờ và chứng chỉ
  - Hệ thống nộp hồ sơ xin phép: xuất bản, xây dựng, y tế, giáo dục...
- Trong thương mại điện tử
  - Chứng thực danh tính người tham gia giao dịch, xác thực tính an toàn của giao dịch điện tử qua mạng Internet.
  - Chứng thực tính nguyên vẹn của hợp đồng, tài liệu...
  - Ứng dụng xác thực trong Internet banking
  - Ứng dụng xác thực trong giao dịch chứng khoán
  - Ứng dụng xác thực trong mua bán, đấu thầu qua mạng

Chương 2. Kết quả nghiên cứu

2.1 Giới thiệu

- **Tên đề tài:** *Tìm hiểu về chữ ký điện tử ElGamal và viết ứng dụng minh họa*.
- **Nghiên cứu nội dung các thuật toán**
  - Tìm hiểu về thuật toán sơ đồ chữ ký điện tử Elgamal, cách tạo chữ ký, xác minh chữ ký.

- Tìm hiểu về phương pháp mã hóa bất đối xứng , ứng dụng trong chữ ký điện tử.
- Tìm hiểu về hàm băm ,ứng dụng trong chữ ký điện tử.

➢ **Thiết kế chương trình**

✓ Phần tạo khoá:

Bước 1: Tại giao diện tạo khoá chúng ta cần nhấn vào phần tạo khoá để sinh ra khoá công khai và khoá bí mật

✓ Phần ký văn bản:

Bước 2: Tại giao diện văn bản ta lần lượt thực hiện các bước sau:

- Tải văn bản cần ký
- Ký vào văn bản đó
- Sau khi đã ký xong thì lưu lại chữ ký

✓ Phần xác nhận văn bản:

Bước 3: Tại giao diện xác nhận văn bản ta thực hiện các bước

- Tải văn bản đã ký và cần xác nhận lên.
- Tải chữ ký kèm theo đã được ký ở văn bản
- Xác nhận chữ ký

✓ Kiểm tả sự toàn vẹn của tài liệu/văn bản

- Nếu văn bản đã được chỉnh sửa hoặc chữ ký kèm theo không chính xác sẽ xuất ra thông báo là văn bản đã được chỉnh sửa hoặc chữ ký không chính xác.
- Nếu văn bản và chữ ký đều chính xác thì chương trình sẽ thông báo chữu ký đã chính xác.

2.2 Nội dung thuật toán

Thuật toán Ơ clit mở rộng tìm phần tử nghịch đảo

Cho 2 số nguyên r_0, r_1 tìm r_1^{-1} theo mod r_0

Intput : r_0, r_1

Output : r_1^{-1} theo mod r_0 (Nếu tồn tại)

- Dùng thuật toán Euclide mở rộng để tìm các số nguyên s và t sao cho s. r_0 +t. r_1 = gcd(r_0, r_1) =d
- Nếu d>1 thì r_1^{-1} mod r_0 không tồn tại. Ngược lại nếu d=1 thì return(t)

Để tìm được s, t ta dùng công thức sau :

$s_0 = 1$, $t_0 = 0$

$s_0 = 0$, $t_0 = 1$

$s_i = s_{(i-2)} - q_{(i-1)} * s_{(i-1)}$

$t_i = t_{(i-2)} - q_{(i-1)} * t_{(i-1)}$

Trong đó: Với i=0,1,2,3,..

$r_i = q_{i+1} * r_{i+1} + r_{i+2}$

Thuật toán dừng lại khi phần dư $r_{i+2} = 0$

Thuật toán : Bình phương và nhân

Công thức đệ quy: để tính luỹ thừa tự nhiên bậc n của x thực hiện như sau:

Với n=0 thì $x^n = 1$

Với n>0 ta có công thức bình phương và nhân :

$$f(n) = \begin{cases} (x^k)^2, & \text{khi } n = 2k \\ (x^k)^2 * x, & \text{khi } n = 2k+1 \end{cases}$$

Như vậy phép tính x^n được đệ quy về một số phép bình phương và phép nhân

Thuật toán: Sơ đồ chữ ký điện tử Elgamal

Sơ đồ chữ ký Elgamal là được viện tiêu chuẩn và vông nghệ quốc gia Mỹ sửa đổi thành chuẩn chữ ký số. Sơ đồ

chữ ký Elgamal không nhất thiết phải giống như hệ thống mã hóa công khai Elgamal. Điều này có nghĩa là có nhiều chữ ký hợp lệ cho cùng một thông điệp bất kỳ . Thuật toán xác minh phải có khả năng chấp nhận bất kỳ chữ ký hợp lệ nào khi xác minh.

Sơ đồ Elgamal được định nghĩa như sau:

- **Tạo cặp khoá(bí mật, công khai) (a, k) :**

  + Chọn phần tử nguyên tử **$\alpha \in Z_p^*$**. Đặt **$P = Z_p^*$** , **$A = Z_p^* \times Z_{p-1}$**

  + Chọn khoá bí mật là **$\alpha \in Z_p^*$**. Tính khoá công khai **$\beta \equiv \alpha^a \bmod p$**.

  + Định nghĩa tập khoá: **$=\{(p, \alpha, a, \beta) : \beta \equiv \alpha^a \bmod p\}$.**

  + Các giá trị **p, α, β** được công khai, phải giữ bí mật **a.**

- **Ký số**

  + Dùng 2 khoá ký: khoá **a** và số ngẫu nhiên **$k \in Z_{p-1}^*$**

  + Vì **$k \in Z_{p-1}^*$**, nên nguyên tố cùng p-1, do đó tồn tại $k^{-1} \bmod (p-1)$

  + Chữ ký trên **$x \in P$ là $y = sig_k(x, k) = (\gamma, \delta), y \in A$**

    Trong đó **$\gamma \in Z_p^*$, $\delta \in Z_{p-1}^*$:**

    $\gamma = \alpha^k \bmod p$ và

    $\delta = (x - a * \gamma) * k^{-1} \bmod (p-1)$

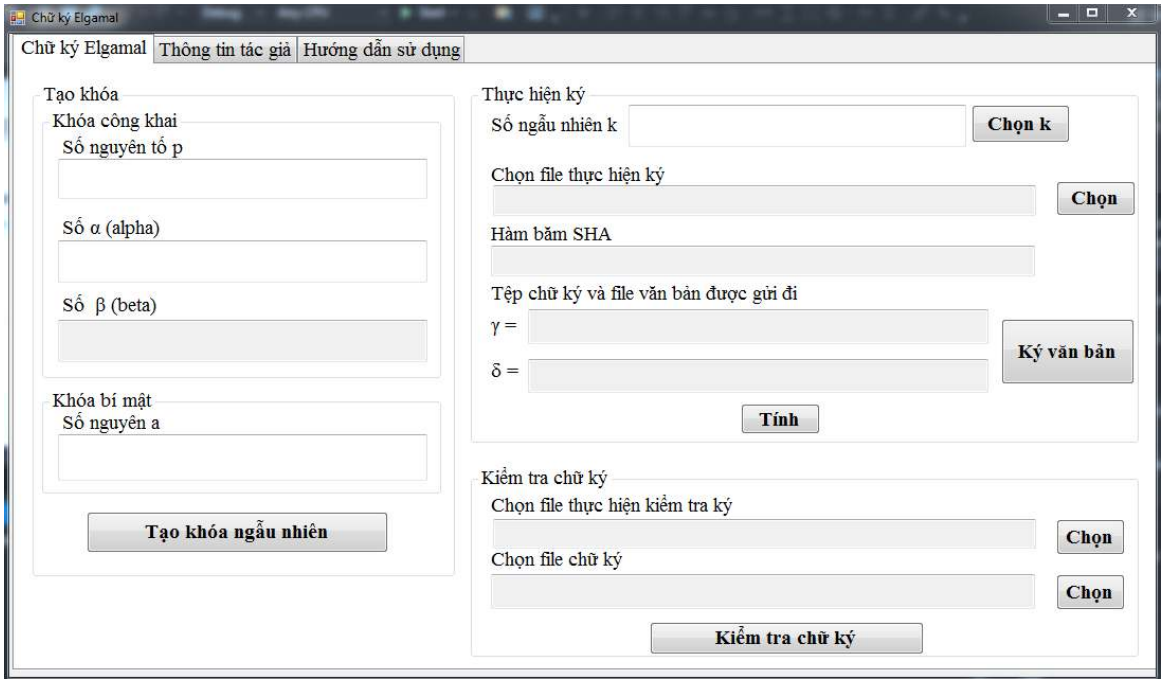
- **Kiểm tra chữ ký**

  $ver_k(x, \gamma, \delta) = TRUE \Leftrightarrow \beta^\gamma * \gamma^\delta \equiv \alpha^x \bmod p$

2.3 Thiết kế, cài đặt chương trình đề mô thuật toán

2.3.1 Giao diện chương trình đề mô

2.3.1.1 Chương trình C#



Thực hiện tạo chữ ký :

Bước 1:

Cách 1: Kích vào "Tạo Khóa Ngẫu Nhiên", chương trình sẽ tự động sinh ra kết quả số p ,alpha , beta, a và k

Cách 2: Nhập từ bản phím :

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

Ở đây thực hiện bắt lỗi nhập liệu :

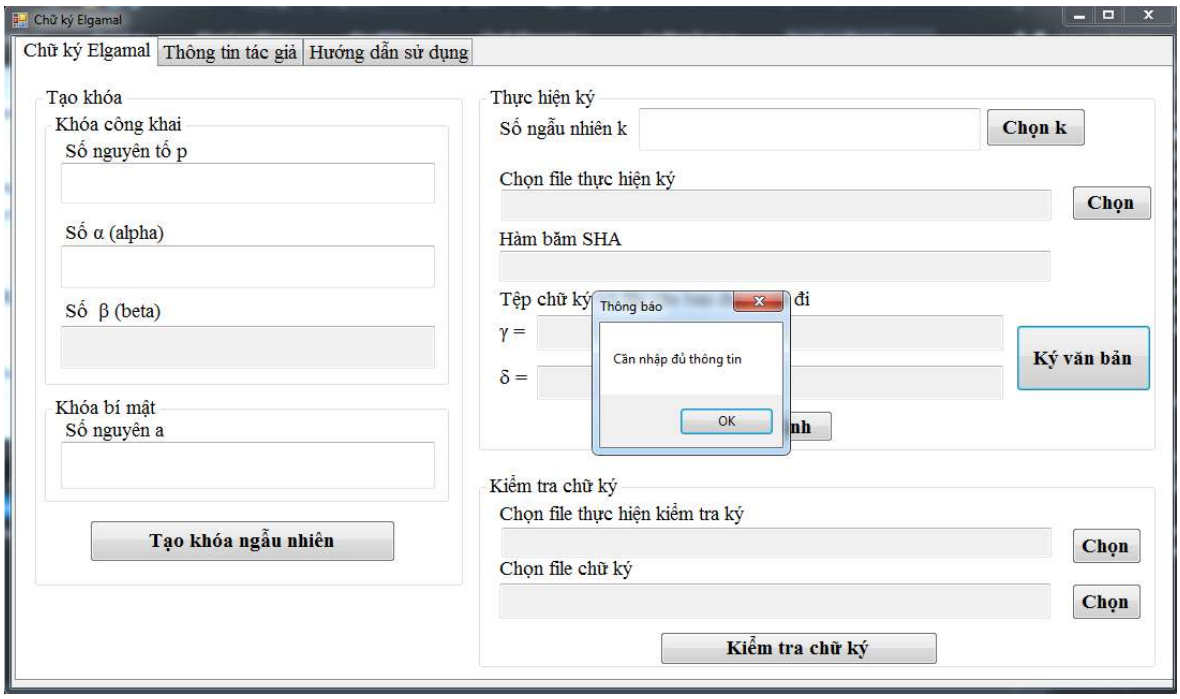
+ Chưa nhập đủ thông tin

+ Kiểm tra số p đã là số nguyên tố chưa. Hiển thị thông báo p không phải số nguyên tố.

+ Kiểm tra số k có thỏa mãn GCD(p,k) = 1 không ?

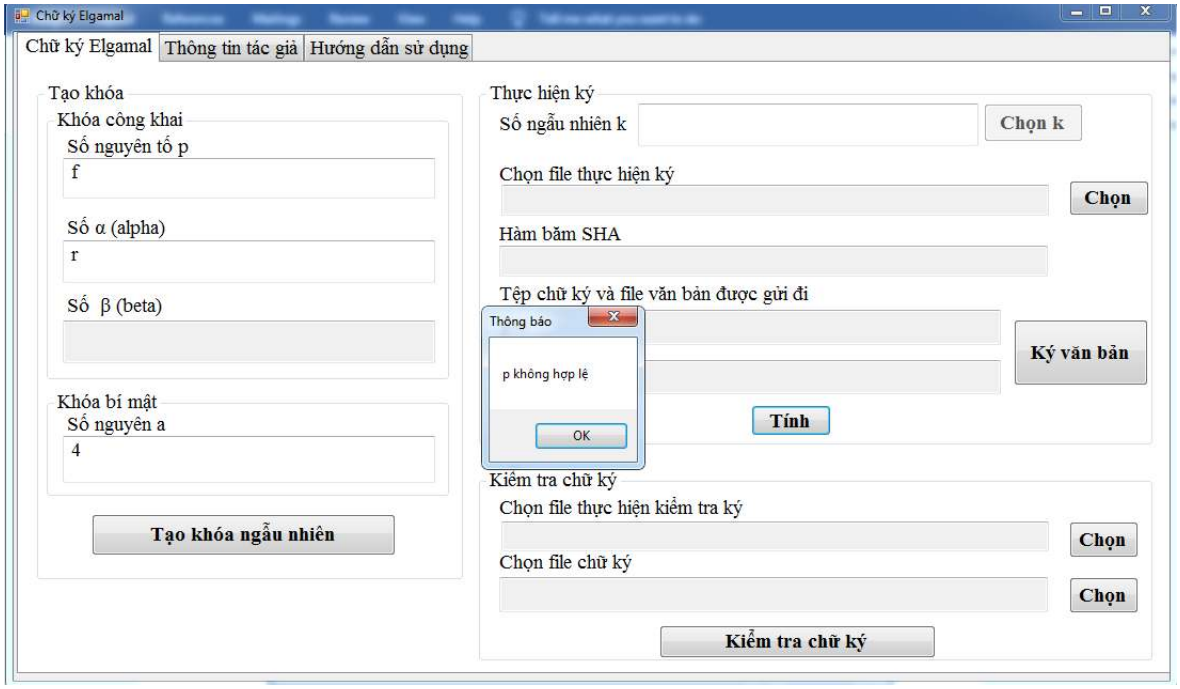
Hình ảnh minh họa về một số lỗi nhập liệu:

- Lỗi chưa nhập đủ thông tin

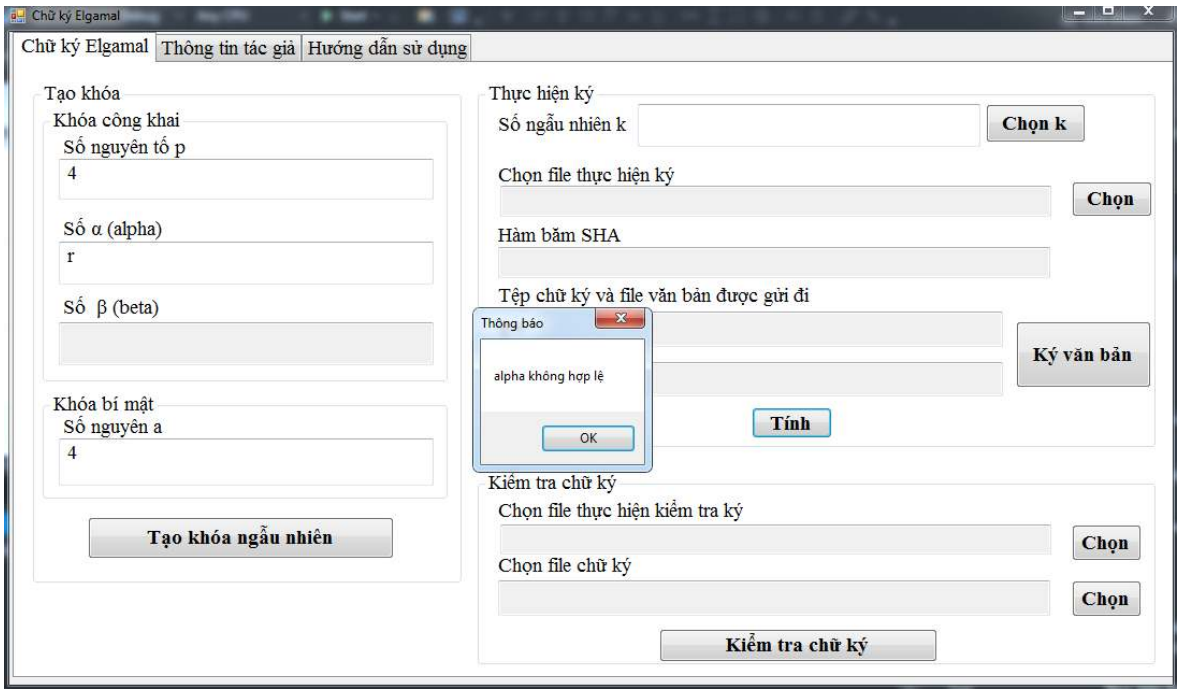


- Lỗi nhập thông tin không hợp lệ.

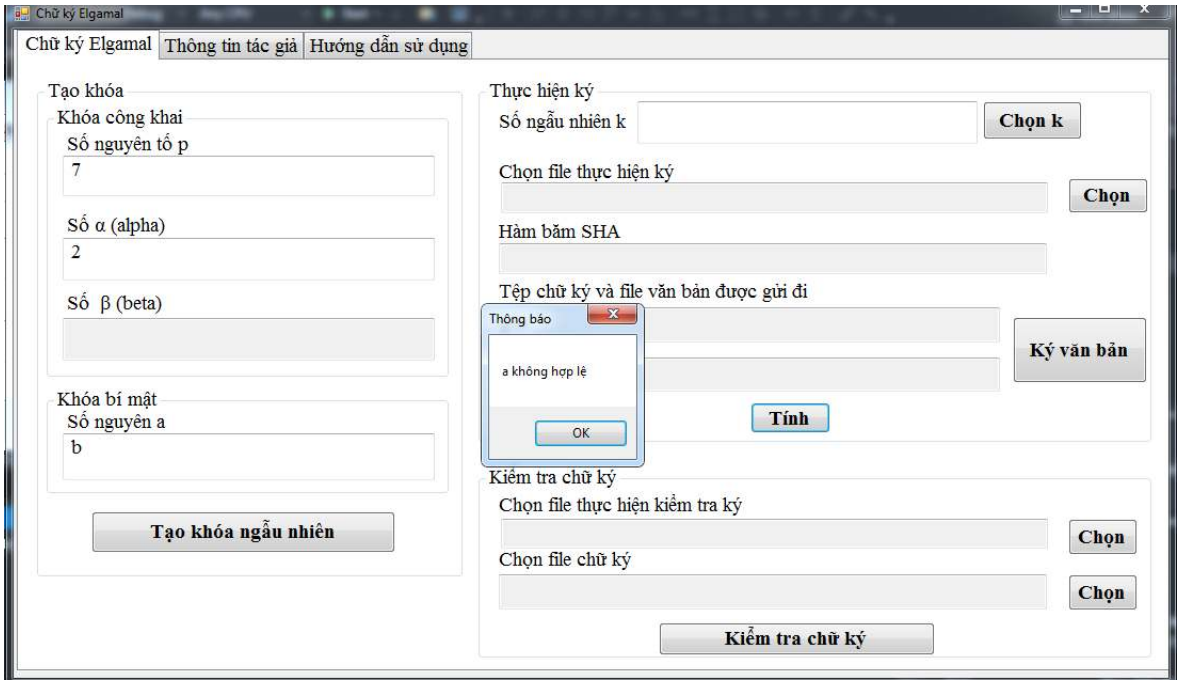
+ p không hợp lệ



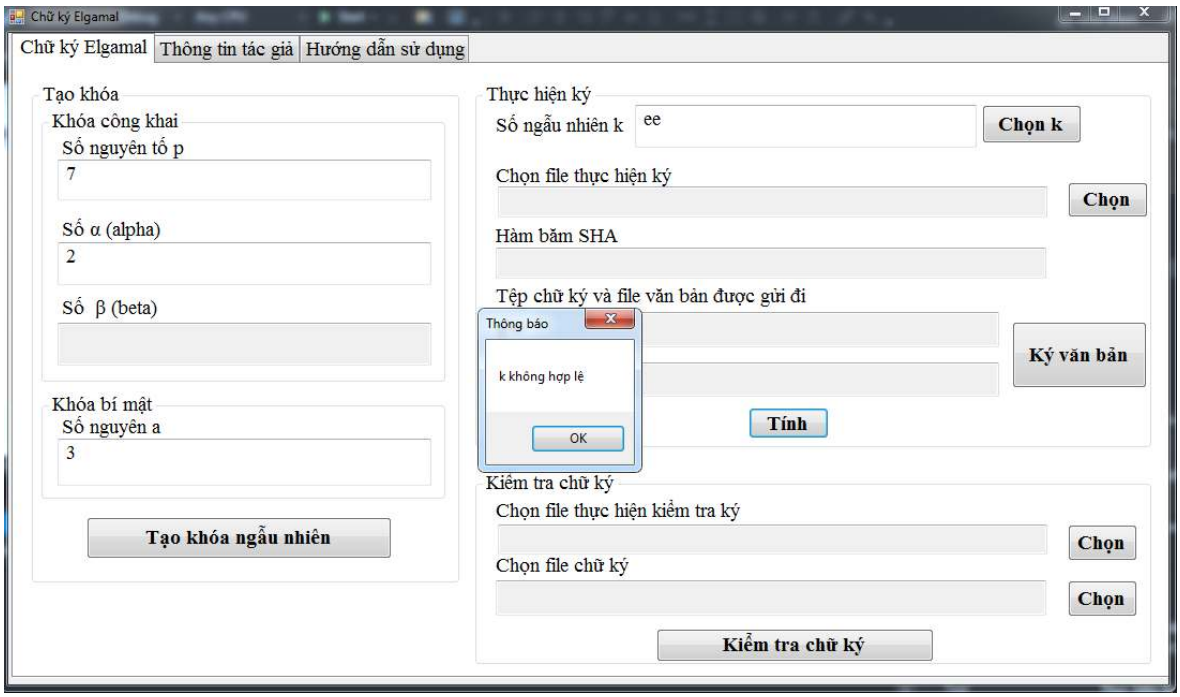
+ alpha không hợp lệ



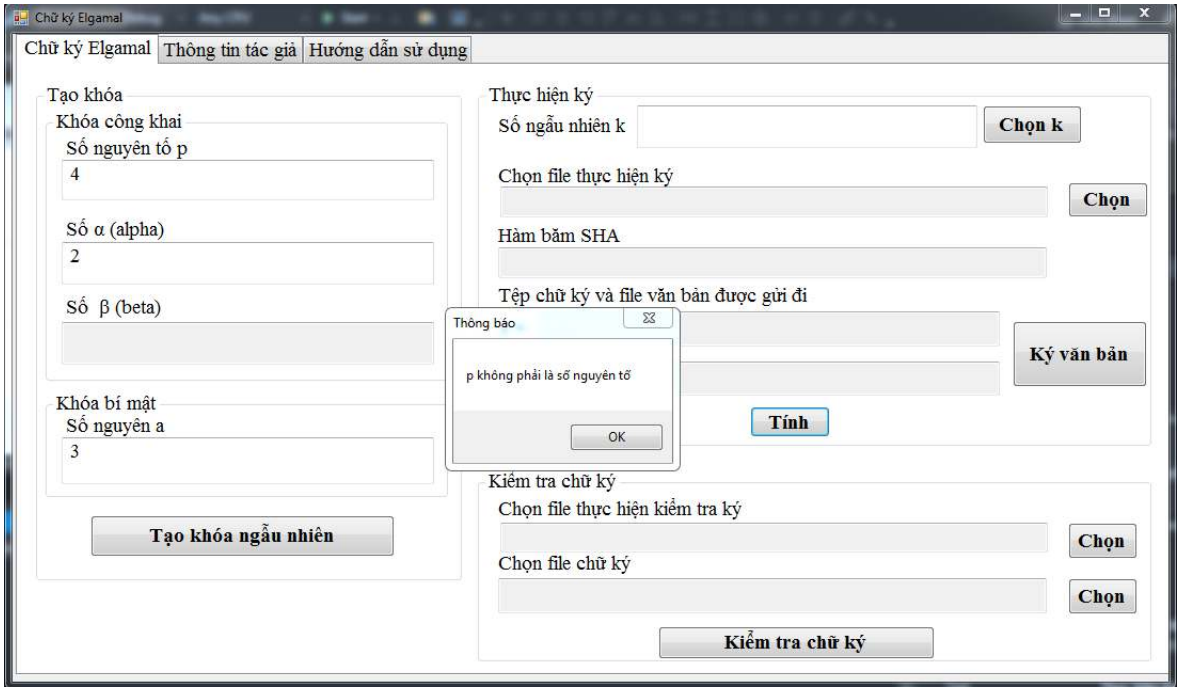
+ a không hợp lệ



+ k không hợp lệ



-Lỗi số p chưa phải là số nguyên tố



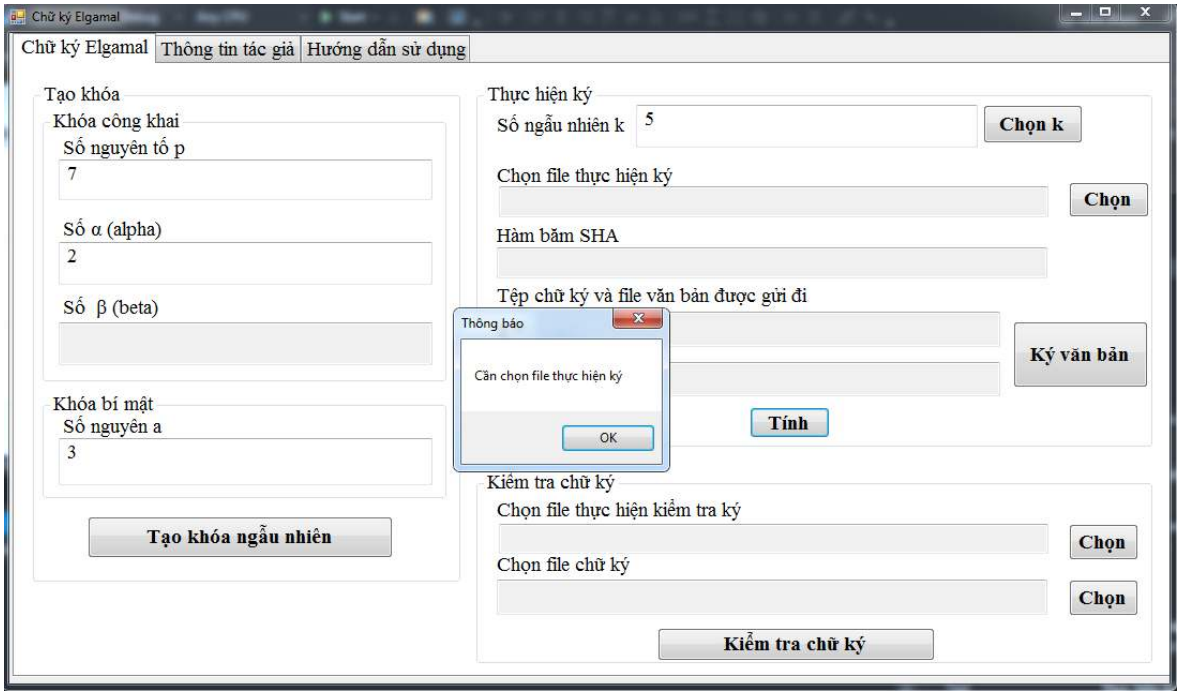
Thực hiện ký:

Bước 2:

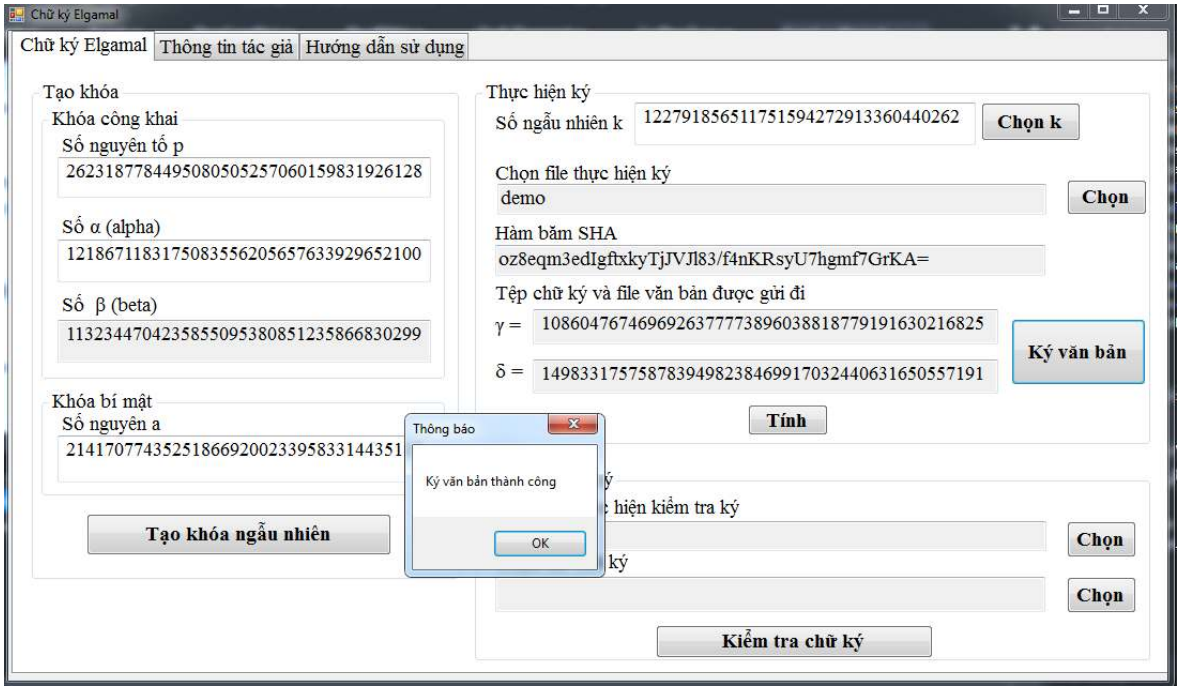
- Chọn file văn bản cần ký
- Chọn “Tính” và kích nút “ Ký văn bản”
- Sau khi ký xong thì lưu lại chữ ký.

Ở đây thực hiện bắt lỗi nhập liệu : Chưa chọn file chữ ký

- Lỗi chưa chọn File:



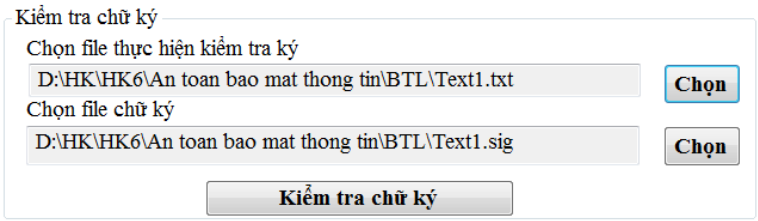
Khi thực hiện ký văn bản thành công, chương trình sẽ hiển thị nội dung của file thực hiện chữ ký, hàm băm, tệp chữ ký và file văn bản được gửi đi như sau:



Kiểm tra chữ ký :

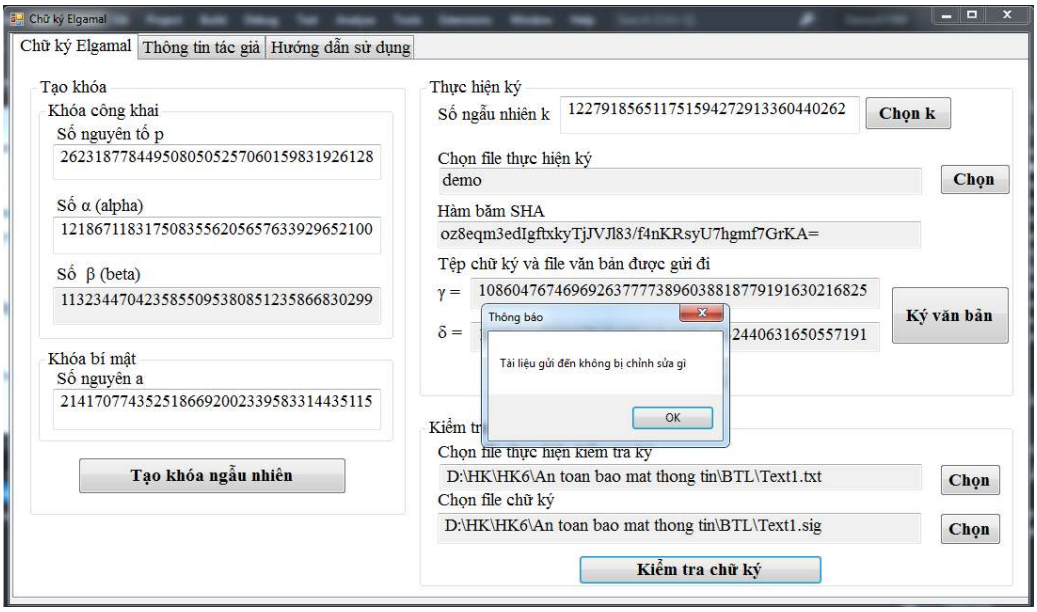
Bước 3:

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

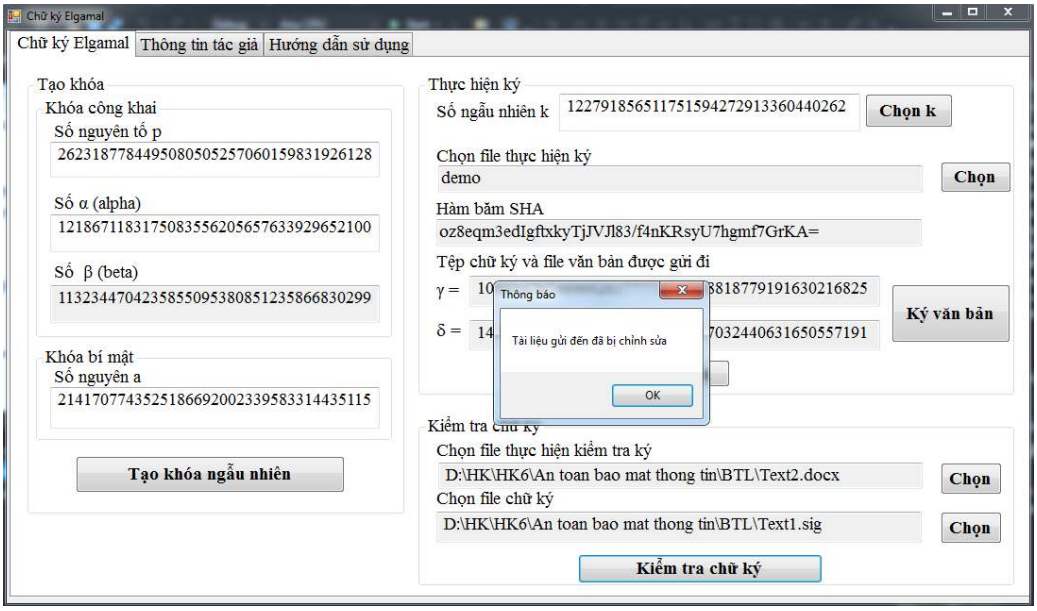


Kết quả:

+ Nếu tài liệu chưa bị chỉnh sửa:

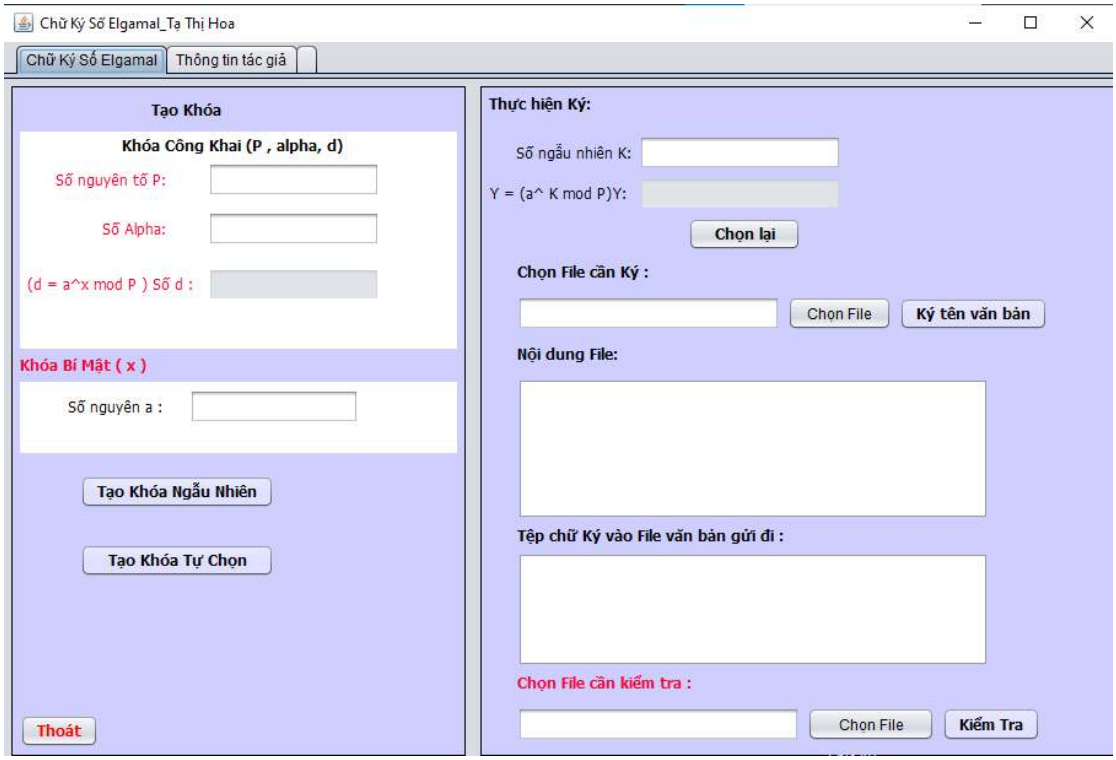


+ Nếu tài liệu đã bị chỉnh sửa :



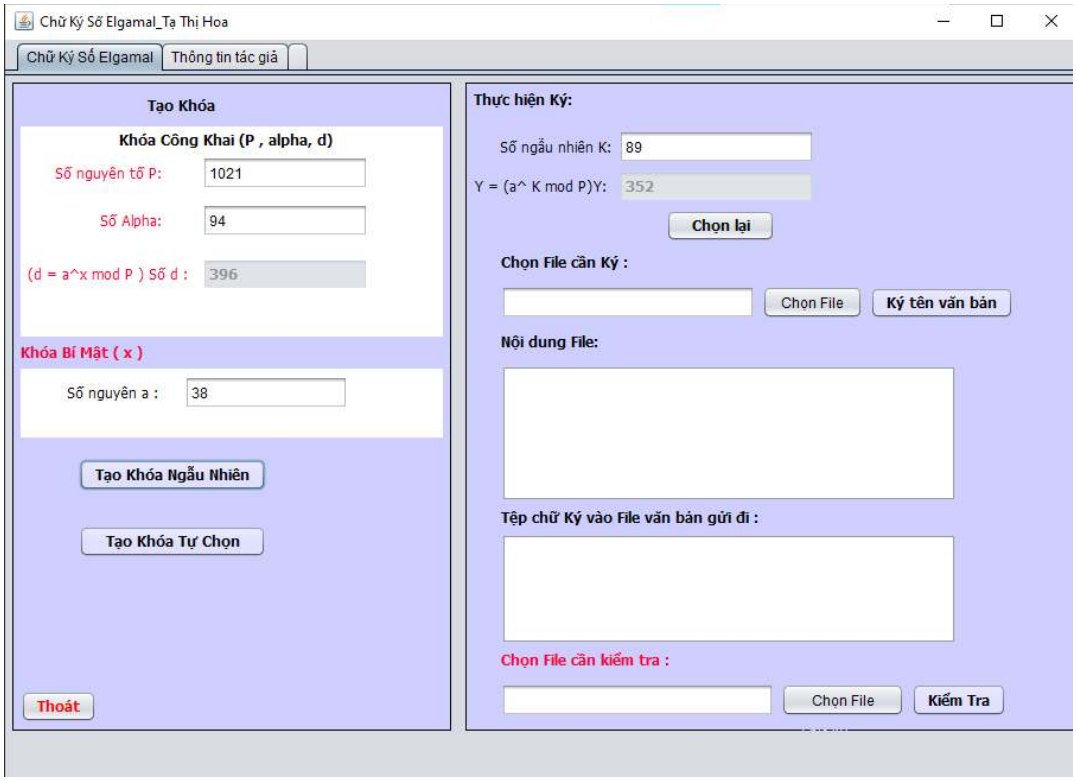
2.3.1.2 Chương trình Java

- Giao diện chương trình :



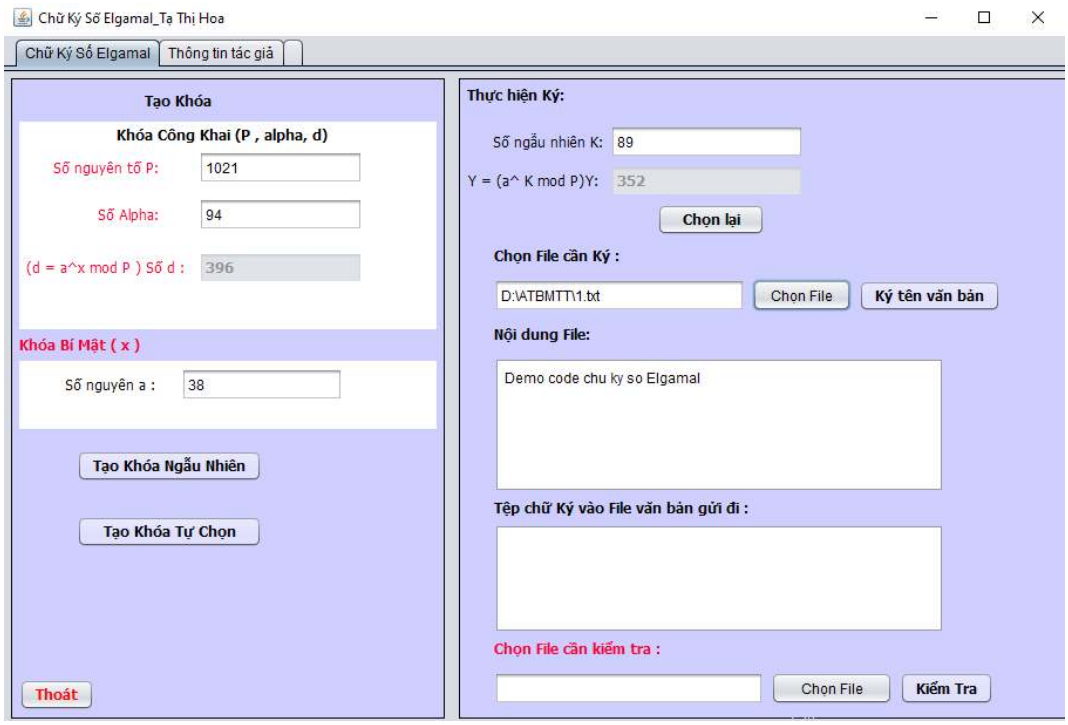
- Thực hiện tạo chữ ký :

+Khi kích vào nút “Tạo khóa ngẫu nhiêm” , số P ,Alpha , a và K, Chương trình sẽ tự động sinh ra kết quả của Số d và số Y tương ứng

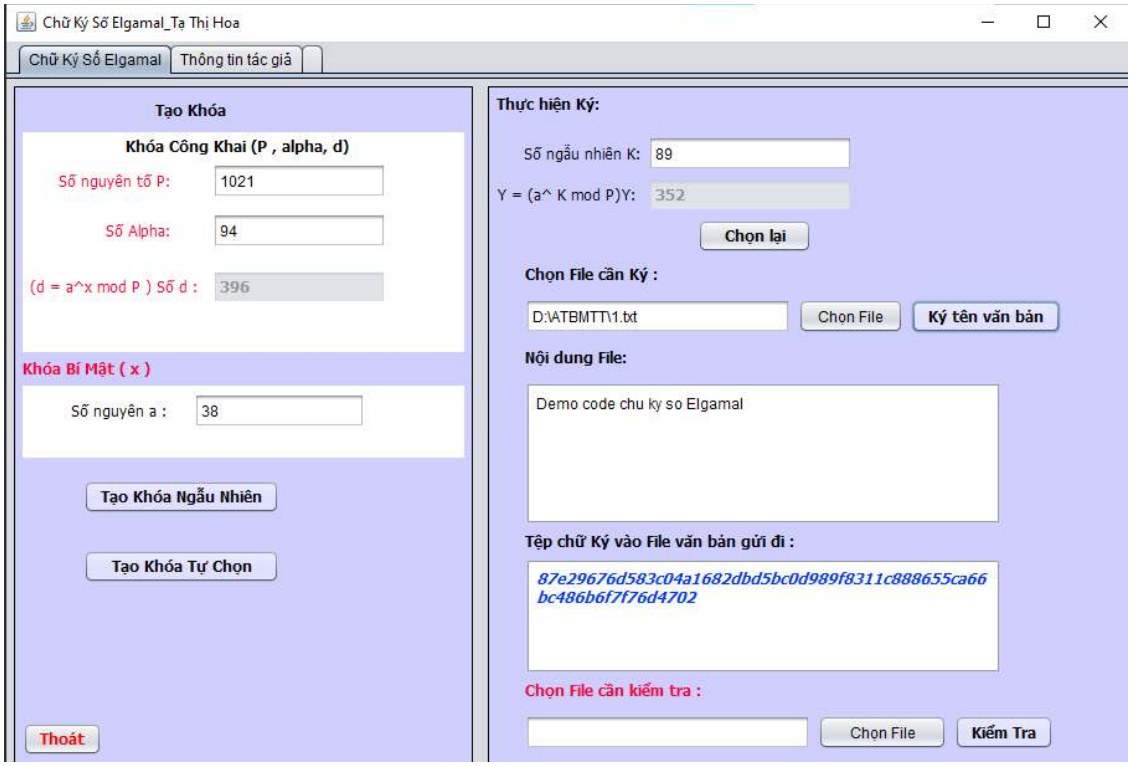


- Sau khi tạo khóa thành công, thực hiện ký

+Chọn File cần tạo chữ ký :



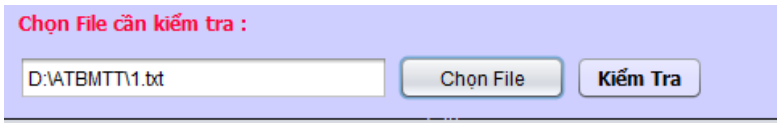
+ Kích vào “Ký lên văn bản” để thực hiện tạo chữ ký điện tử:



Thực hiện tạo chữ Ký thành công

Thực hiện Xác minh chữ ký :

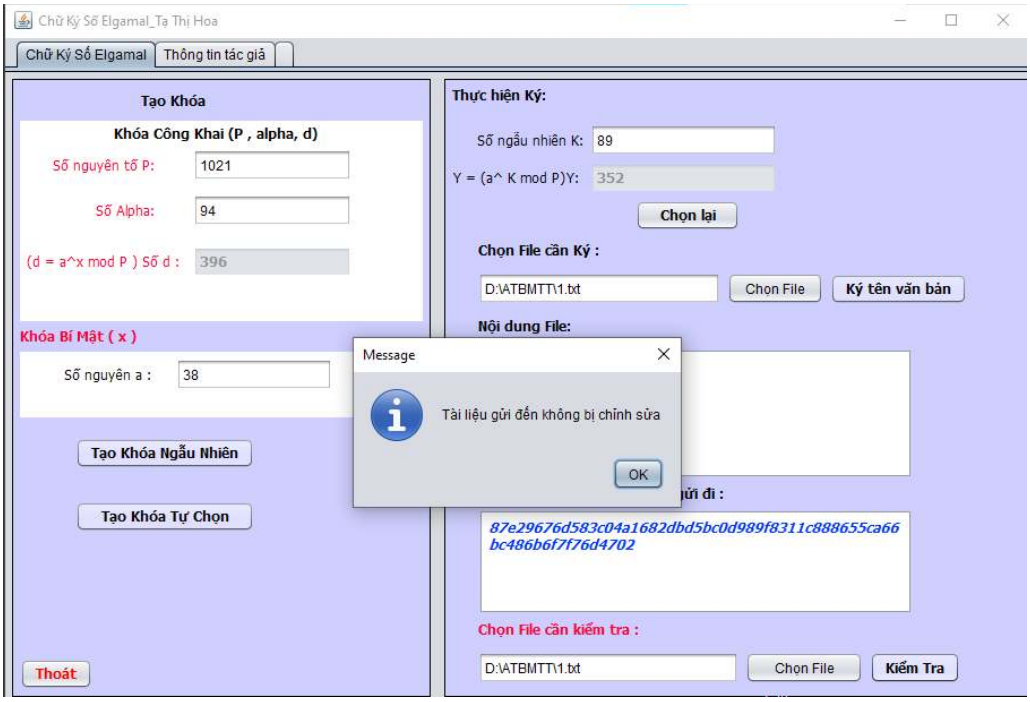
+Chọn File cần xác minh chữ ký



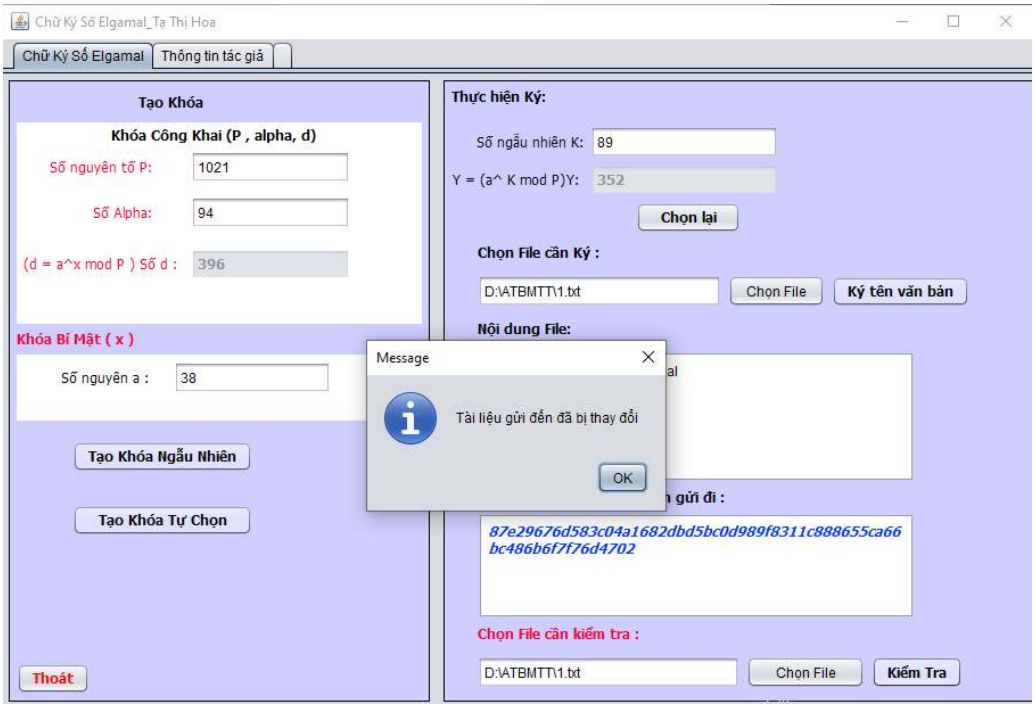
+Kích nút “Kiểm Tra chữ ký ”

Kết quả:

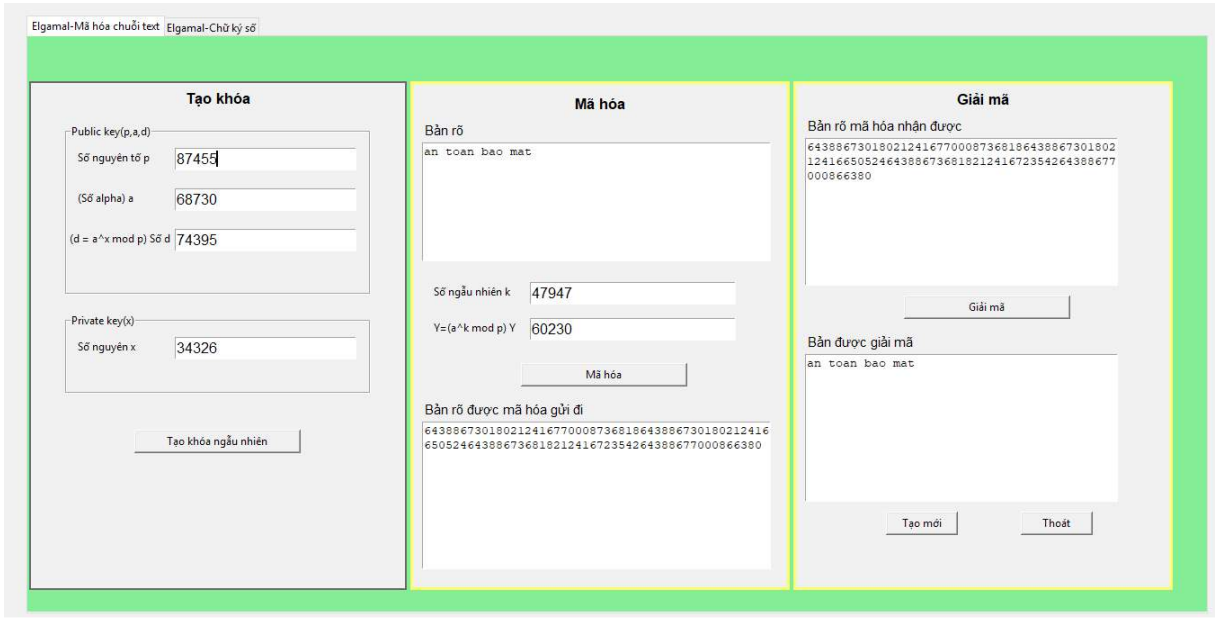
+ Nếu tài liệu chưa bị sửa đổi:

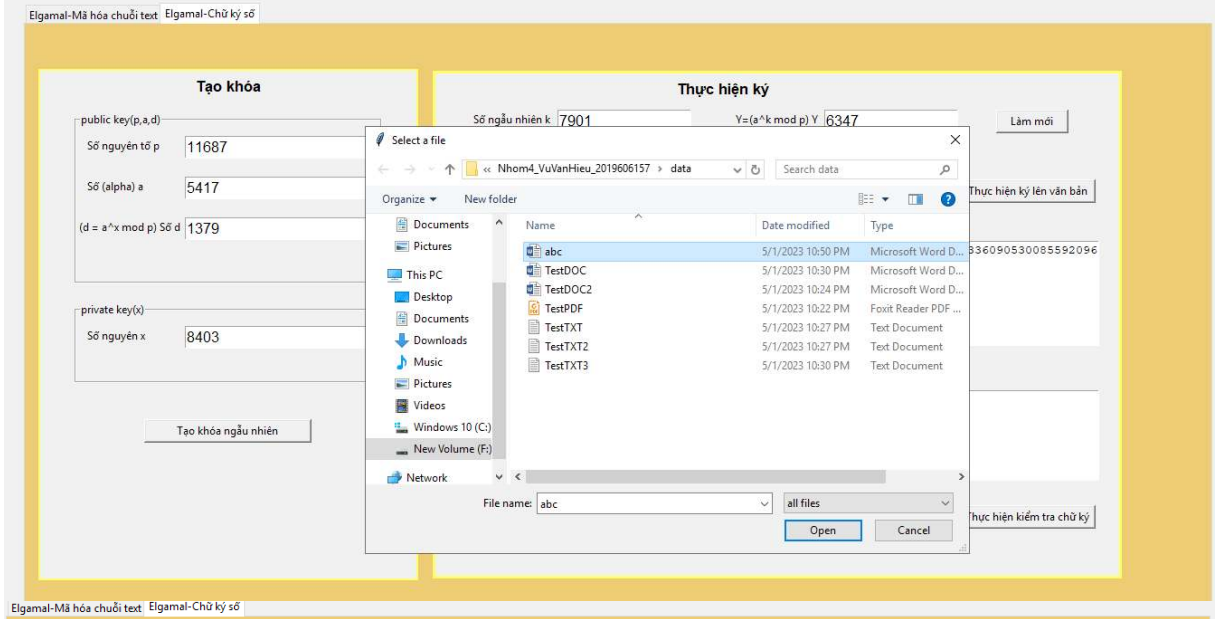


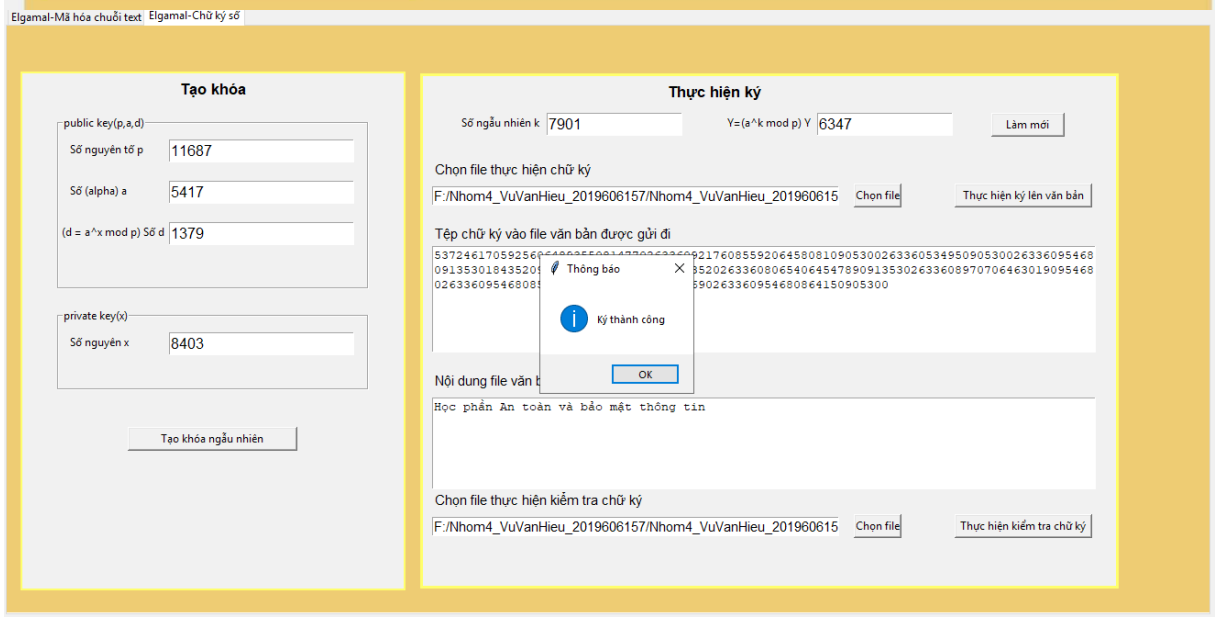
+Nếu Tài liệu đã bị sửa đổi :

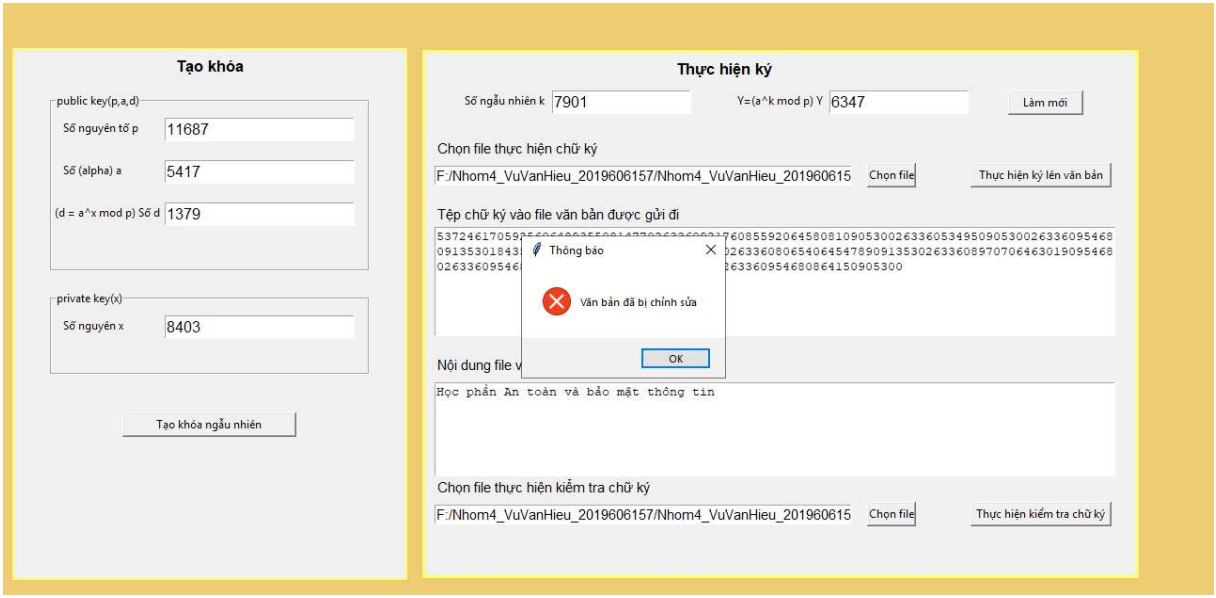


2.3.1.3 Chương trình Python

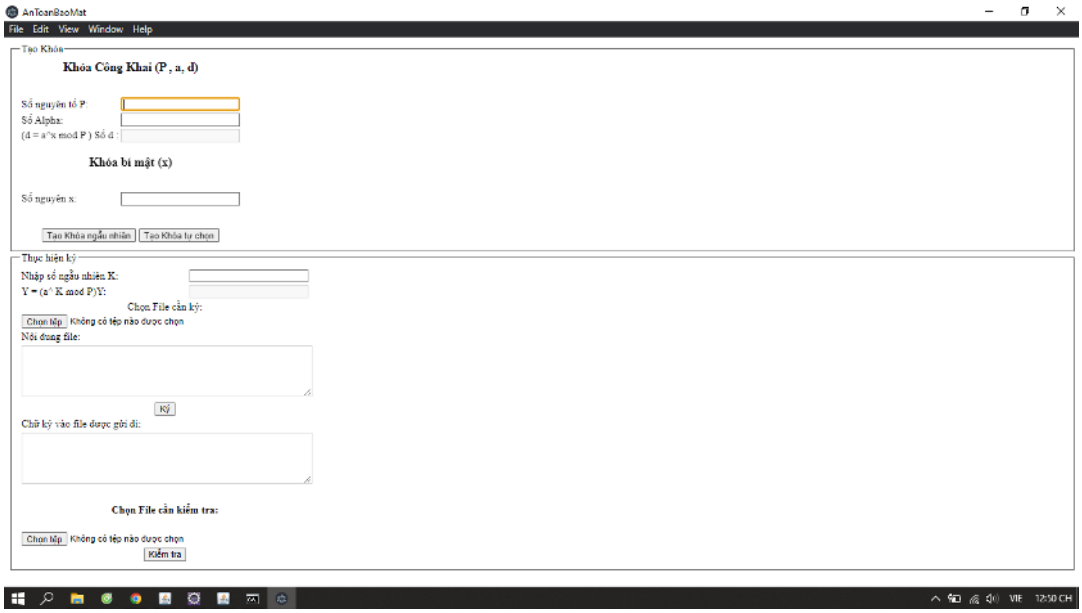








2.3.1.4 Chương trình JavaScript



- *Giao diện chương trình :*

Thực hiện tạo chữ ký :

Cách 1: Tạo Khóa ngẫu nhiên:

Kích vào “Tạo Khóa Ngẫu Nhiên”

+ Chương trình sẽ tự động chọn Khóa Công Khai , Khóa bí mật và chọn Số K ngẫu nhiên thỏa mãn GCD(K,P) =1

Cách 2: Tạo Khóa tự chọn :

Nhập thông Số Nguyên tố P , số x , số Alpha, và số K để thực hiện quá trình ký số.

Ở đây thực hiện bắt lỗi nhập liệu :

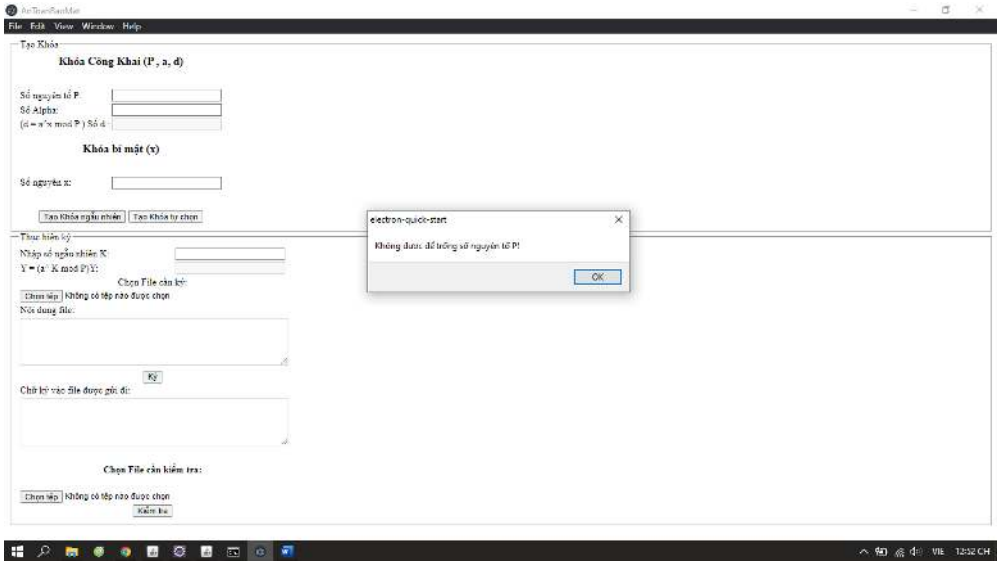
+ Để trống chưa nhập đầy đủ thông tin

+ Kiểm tra số P đã là số nguyên tố chưa. Nếu chưa, yêu cầu nhập lại

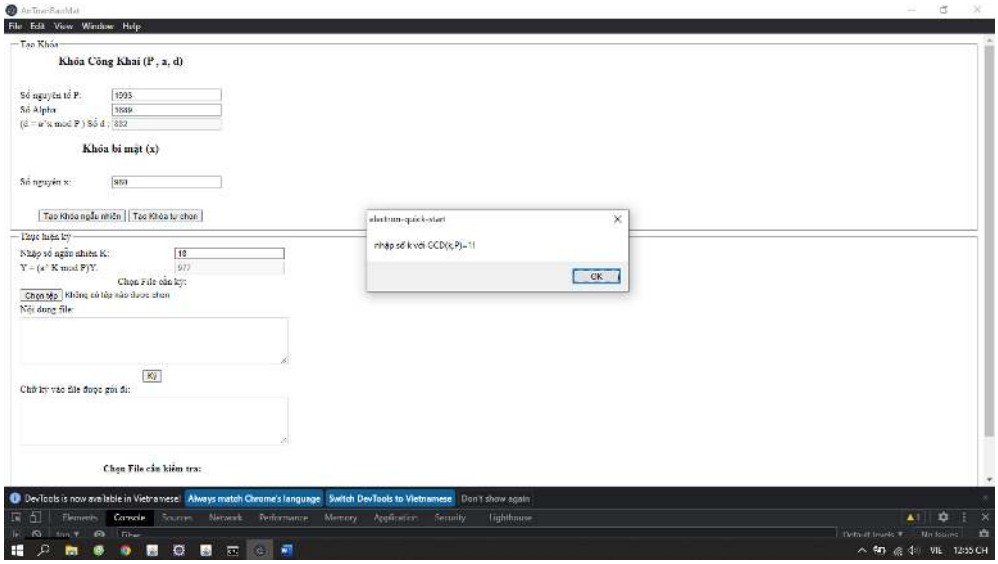
+Kiểm tra số K có thỏa mãn GCD(P,K) = 1 không ?

Hình ảnh minh họa về một số lỗi nhập liệu:

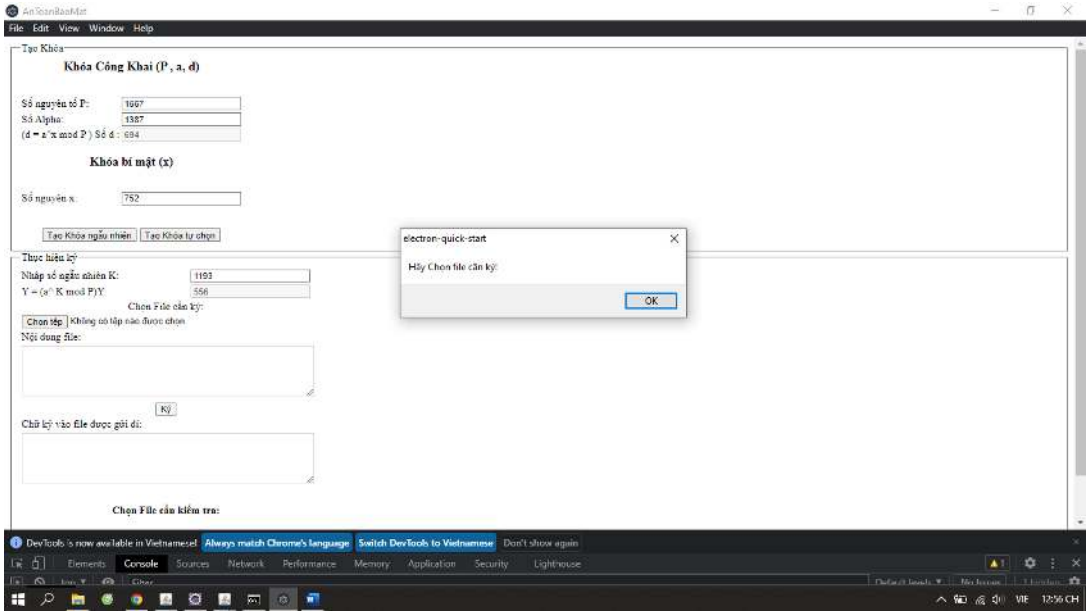
- Lỗi chưa điền đầy đủ thông tin Khóa.



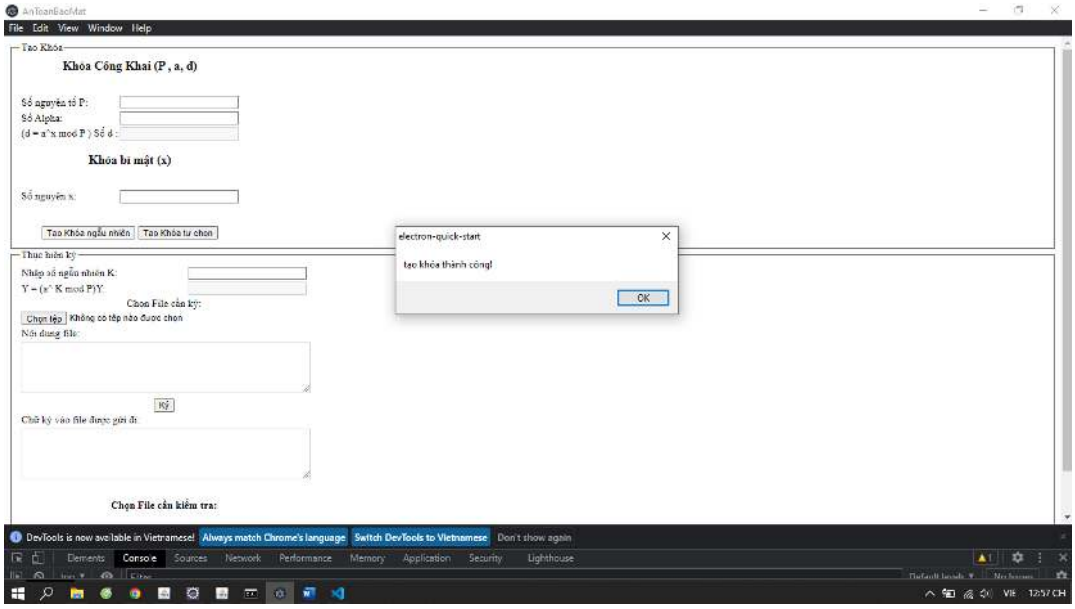
-Lỗi số P chưa phải là số nguyên tố



-Lỗi chưa chọn File:

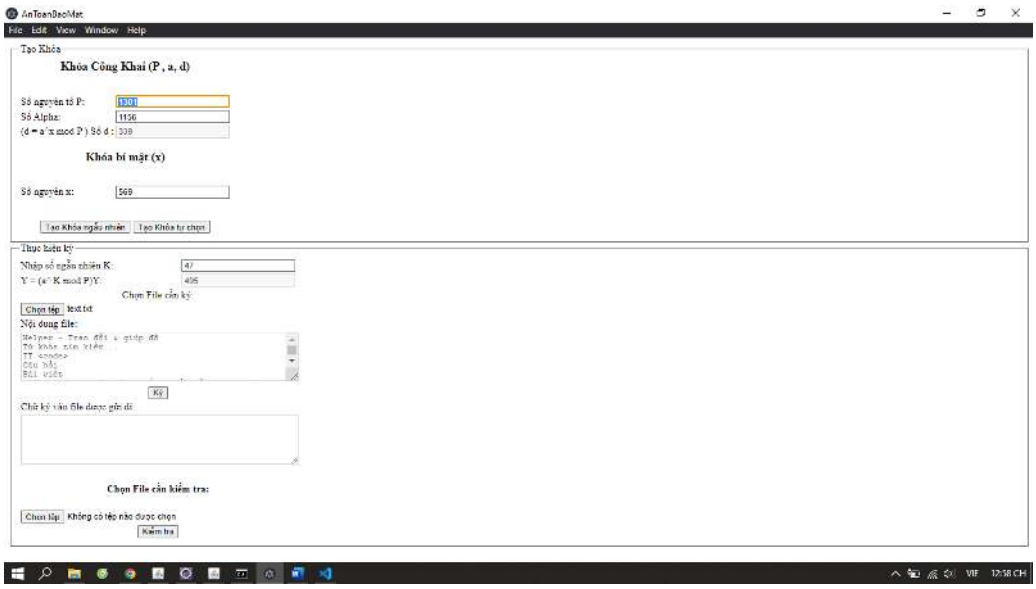


Khi nhập đầy đủ Số P ,Alpha , x và K, Chương trình sẽ tự động sinh ra kết quả của Số D và số Y tương ứng và hiện thông báo.

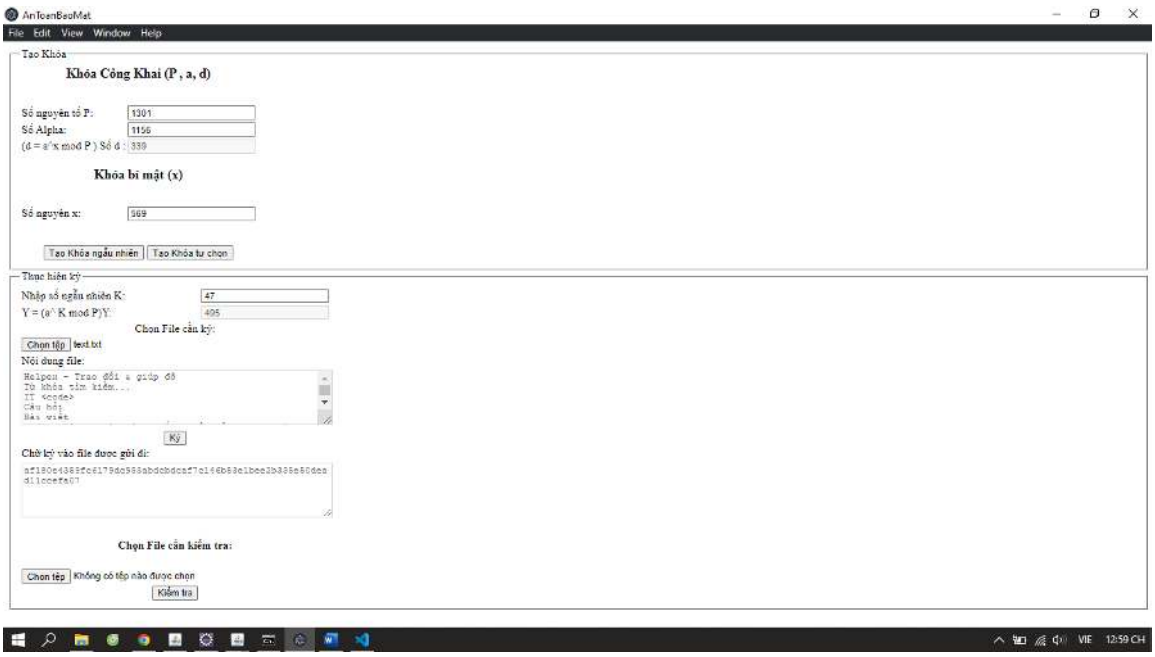


Sau khi thấy thông báo “Tạo Kháo thành công” thì có thế thực hiện Ký:

+Chọn File càn tạo chữ ký :



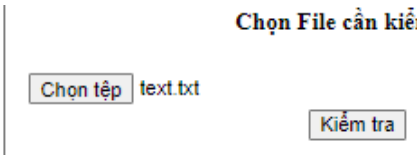
+ Kích vào “Ký” để thực hiện tạo chữ ký điện tử:



- Thực hiện tạo chữ Ký thành công

Thực hiện Xác minh chữ ký :

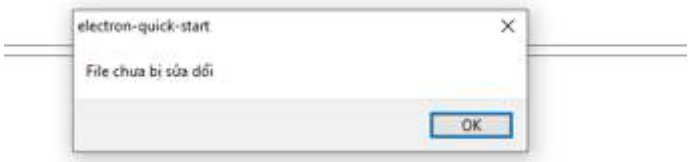
+Chọn File cần xác minh chữ ký



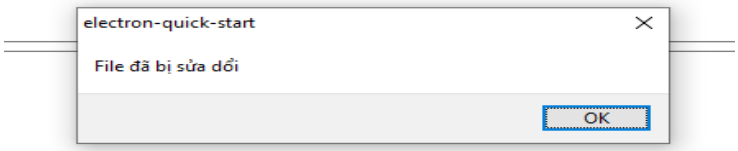
+Kích nút “Kiểm Tra”

- Kết quả:

+ Nếu tài liệu chưa bị sửa đổi:

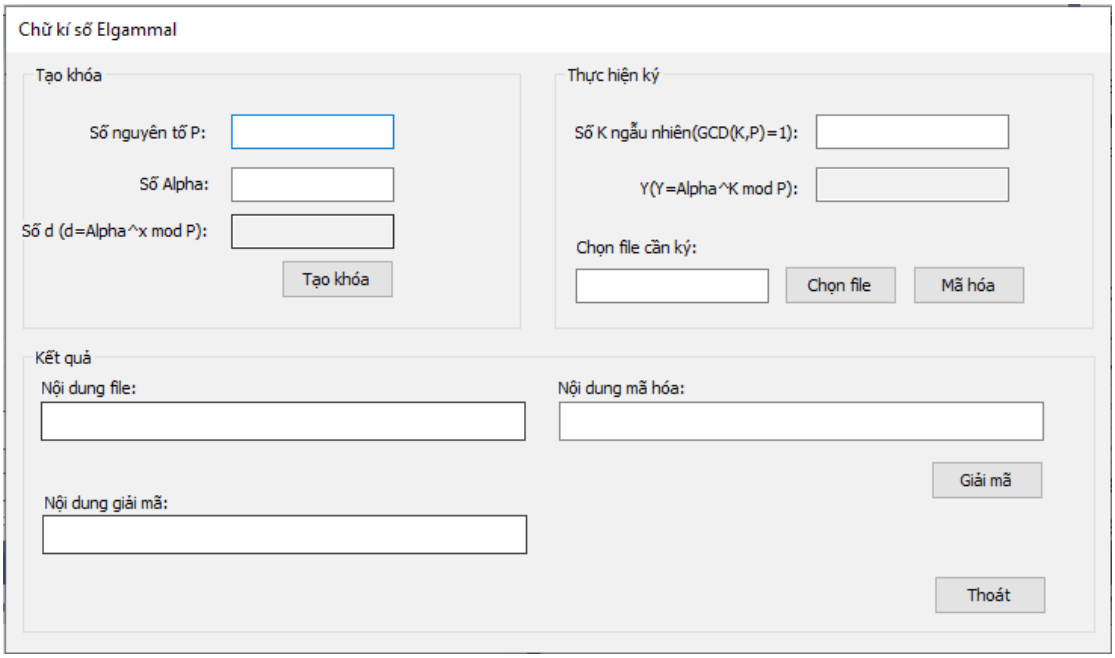


+Nếu Tài liệu đã bị sửa đổi :



2.3.1.5 Chương trình C++

- Giao diện chương trình :



Thực hiện tạo chữ ký :

Tạo Khóa:

Nhập thông Số Nguyên tố P , số x , số Alpha, và số K để thực hiện quá trình ký số.

Ở đây thực hiện bắt lỗi nhập liệu :

+ Để trống chưa nhập đầy đủ thông tin

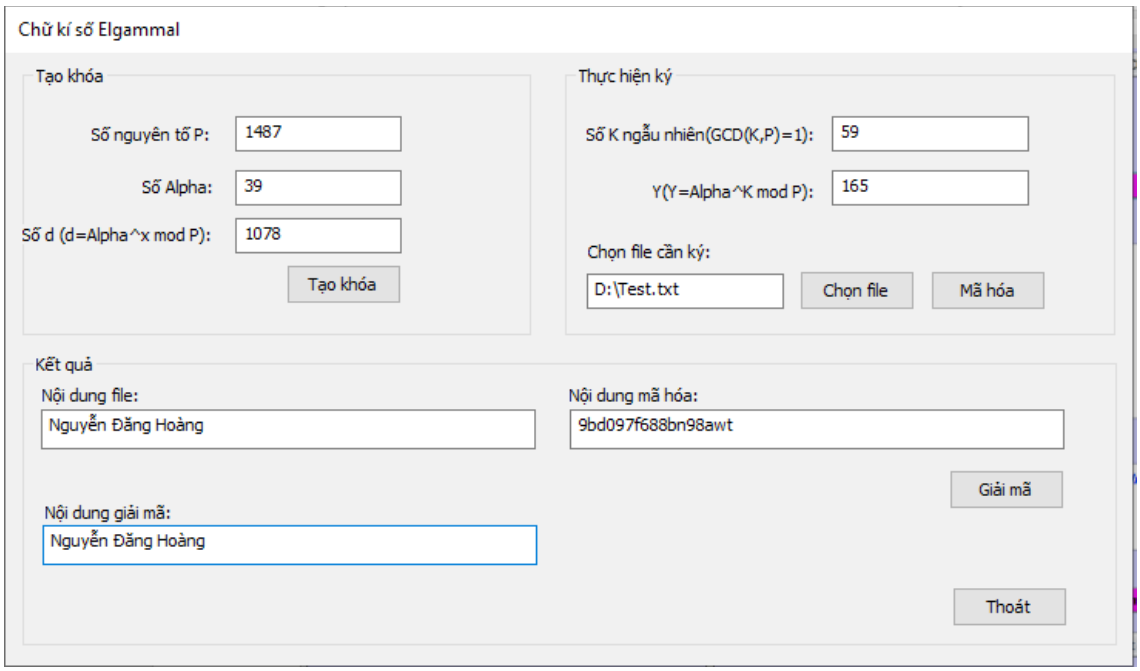
+ Kiểm tra số P đã là số nguyên tố chưa. Nếu chưa, yêu cầu nhập lại

+Kiểm tra số K có thỏa mãn GCD(P,K) = 1 không ?

Hình ảnh minh họa về một số lỗi nhập liệu:

Khi nhập đầy đủ Số P ,Alpha , x và K, Chương trình sẽ tự động sinh ra kết quả của Số D và số Y tương ứng và hiện thông báo.

+Chọn File càn tạo chữ ký :



+ Kích vào “Mã hóa” để thực hiện tạo chữ ký điện tử:

Thực hiện tạo chữ Ký thành công

2.4 Cài đặt và triển khai

Các công cụ sử dụng để thực hiện đề tài :

+ Báo cáo word : Phần mềm Microsoft office

+ Đối với Java : Phần mềm Eclipse

Eclipse là một môi trường phát triển tích hợp dùng cho lập trình máy tính. Nó chứa một không gian làm việc cơ sở và một hệ thống plug-in để mở rộng để tùy chỉnh môi trường. Eclipse được viết chủ yếu bằng Java và nó được dùng chủ yếu cho lập trình ứng dụng Java, nhưng nó cũng có thể dùng để lập trình ứng dụng bằng các ngôn ngữ khác thông qua plug-ins, bao gồm

Ada, ABAP, C, C++, C#, Clojure, COBOL, D, Erlang, Fortran, Groovy, Haskell, HTML, JavaScript, Julia Lasso, Lua, NATURAL, Perl, PHP, Prolog, Python, R, Ruby (Bao gồm Ruby on Rails framework), Rust, Scala, và Scheme. Nó cũng có thể dùng để phát triển các tài liệu bằng LaTeX (thông qua một plug-in TeXlipse) và các gói tin cho phần mềm Mathematica. Môi trường phát triển bao gồm Eclipse Java development tools (JDT) cho Java và Scala, Eclipse CDT cho C/C++, và Eclipse PDT for PHP, và những gói khác.

+ Đối với C++ : Phần mềm Dev-C++

Dev-C++ là một trong những phần mềm lập trình C++ cơ bản dành cho máy tính chạy hệ điều hành Windows với mã nguồn mở, bạn có thể hợp tác cải thiện phần mềm như tìm lỗi, sửa lỗi (bug), cập nhật với các công nghệ mới hoặc tạo ra các tính năng mới với nhà phát hành. Đặc biệt, Dev-C++ hoàn toàn miễn phí, phù hợp với sinh viên và người đi làm.

+ Đối với C# : Phần mềm Visual studio 2019

Microsoft Visual Studio là một môi trường phát triển tích hợp (IDE) từ Microsoft. Microsoft Visual Studio còn được gọi là "Trình soạn thảo mã nhiều người sử dụng nhất thế giới ", được dùng để lập trình C++ và C# là chính. Nó được sử dụng để phát triển chương trình máy tính cho Microsoft Windows, cũng như các trang web, các ứng dụng web và các dịch vụ web. Visual Studio sử dụng nền tảng phát triển phần mềm của Microsoft như Windows API, Windows Forms, Windows Presentation Foundation, Windows Store và Microsoft Silverlight. Nó có thể sản xuất cả hai ngôn ngữ máy và mã số quản lý.

+ Đối với Python : Phần mềm PyCharm

PyCharm là một môi trường phát triển tích hợp (IDE) được sử dụng trong lập trình máy tính , đặc biệt cho ngôn ngữ lập trình Python . Nó được phát triển bởi công ty JetBrains của Séc (trước đây gọi là IntelliJ). Nó cung cấp phân tích mã, trình gỡ lỗi đồ họa, trình kiểm tra đơn vị tích hợp, tích hợp với hệ thống kiểm soát phiên bản (VCSes) và hỗ trợ phát triển web với Django cũng như khoa học dữ liệu với Anaconda .

+ Đối với JavaScript : Phần mềm Sublime Text 3

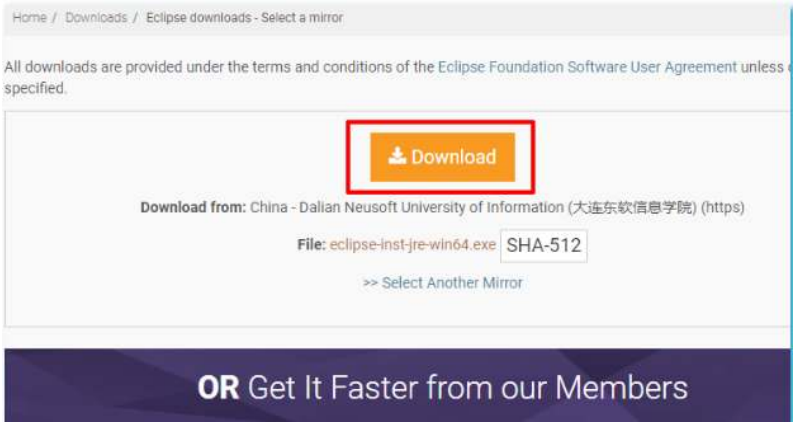
Sublime Text là một trình soạn thảo mã nguồn đa nền tảng phần mềm chia sẻ . Nó hỗ trợ nhiều ngôn ngữ lập trình và ngôn ngữ đánh dấu . Người dùng có thể mở rộng chức năng của nó bằng các plugin , thường do cộng đồng xây dựng và duy trì theo giấy phép phần mềm miễn phí . Để tạo điều kiện cho các plugin, Sublime Text có API Python .

Hướng dẫn cài đặt và chạy chương trình :

Phần mềm Eclipse chạy java

Cài đặt chương trình :

Bước 1: Đầu tiên, bạn vào trang chủ của Eclipse. Sau đó nhấn chọn “Download” để tải file cài đặt về



Bước 2: Sau khi download về xong. Bạn hãy click đúp chuột vào file setup vừa download về để chạy eclipse installer.

Bước 3: Đây chính là giao diện cũng như một vài option để các bạn có thể lựa chọn trước khi cài đặt.

(1) Là cài đặt phiên bản Eclipse cho các lập trình viên Java. Bên dưới họ có ghi một số chức năng mà họ đang hỗ trợ.

(2) Phiên bản Eclipse cho java EE thường được sử dụng trong các dự án về web application sử dụng ngôn ngữ lập trình Java.

(3) Nếu thích các bạn hoàn toàn có thể sử dụng Eclipse để lập trình C/C++ (Thực tế mình thấy ít ai dùng vì có nhiều công cụ hỗ trợ C/C++ tốt hơn, hai nữa Eclipse thường được gắn liến với Java hơn)

Sau khi lựa chọn một trong các option trên thì màn hình sẽ chuyển sang bước cài đặt. Ở đây các bạn lưu ý hai điểm đó là:

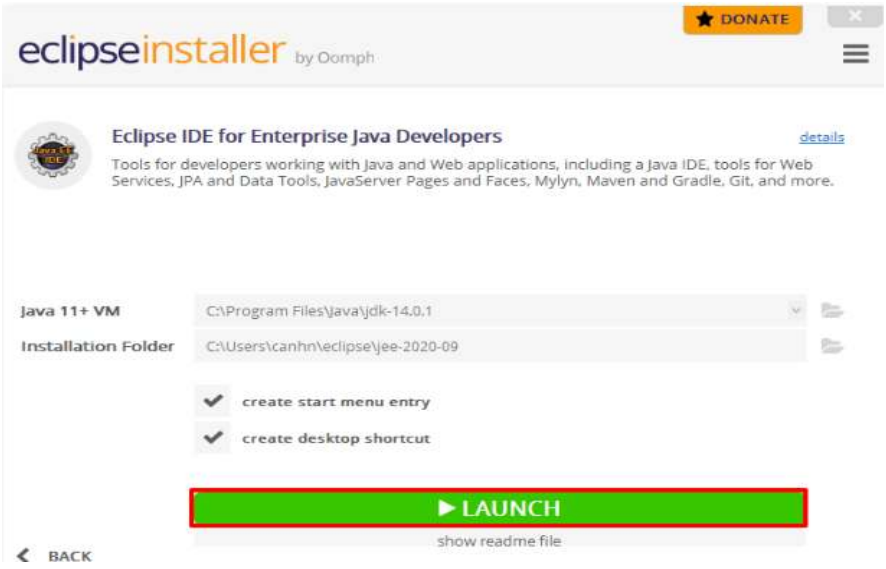
(1) Phiên bản JDK mà các bạn sử dụng (các bạn có thể chọn các version khác). Hoặc chỉ đến thư mục các bạn cài đặt bằng cách bấm vào biểu tượng folder bên phải.

(2) Vị trí thư mục elipse sẽ được cài đặt (như trong ảnh là đường dẫn mặc định, các bạn hoàn toàn có thể thay đổi bằng cách bấm vào biểu tượng folder bên cạnh).

=> Bấm INSTALLquá trình cài đặt sẽ bắt đầu.

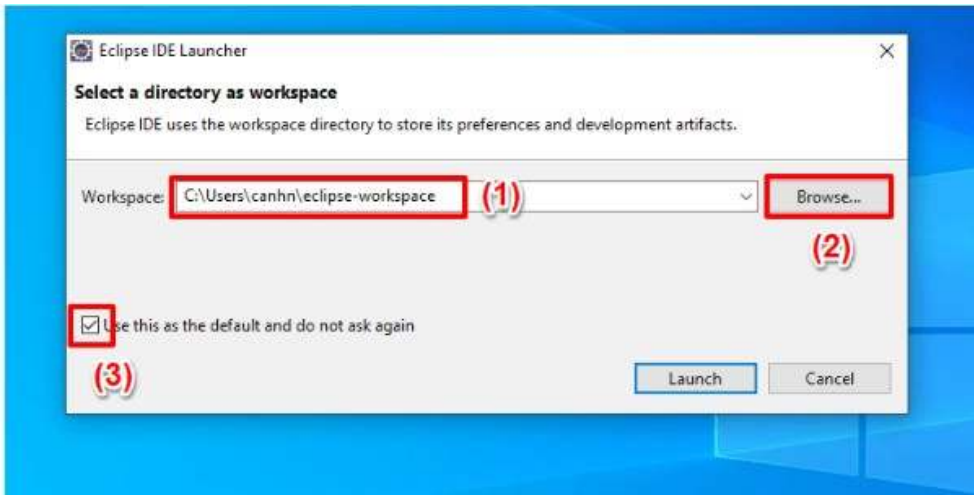
Bước 4: Quá trình cài đặt có thể diễn ra hơi lâu một chút (5-7 phút). Nguyên nhân cũng được Eclipse thông báo như bên dưới. Vậy nên các bạn có thể tranh thủ làm gì đó, làm tack càfê chẳng hạn ^^

Bước 5: Đến bước này quá trình cài đặt đã hoàn tất, các bạn có thể bấm LAUNCH để khởi chạy công cụ.



Bước 6: Thông thường trong lần khởi chạy đầu tiên thì Eclipse sẽ hỏi chúng ta vị trí lưu Workspace (là nơi chứa các Project của Eclipse) với đường dẫn mặc định như hình bên dưới.

Nếu bạn để mặc định thì tích vào => và checkbox bên dưới để lần sau mở lên sẽ không bị hỏi nữa. Còn bạn nào không thích có thể bấm vào Browse và chọn tới thư mục các bạn muốn lưu Workspace.

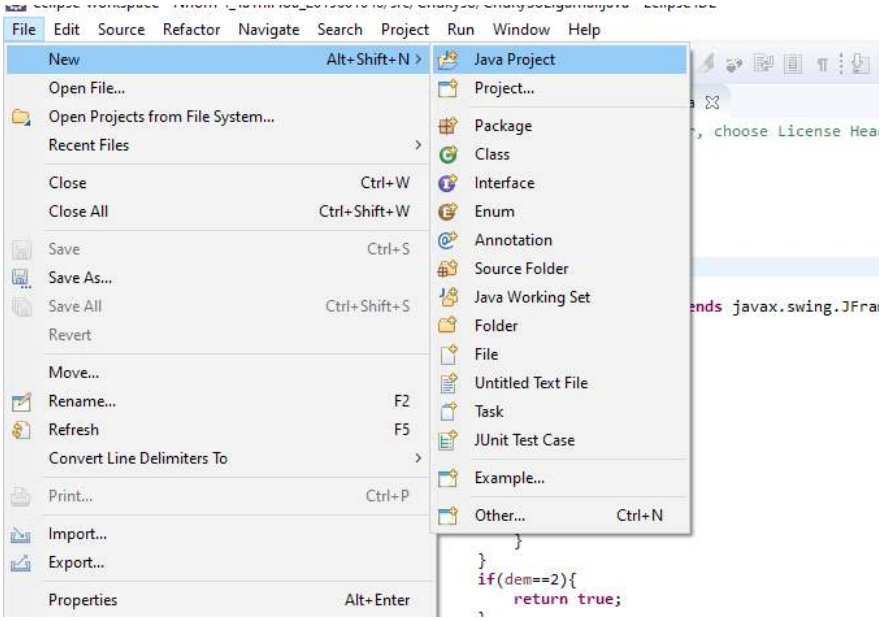


Công cụ đang được khởi chạy.

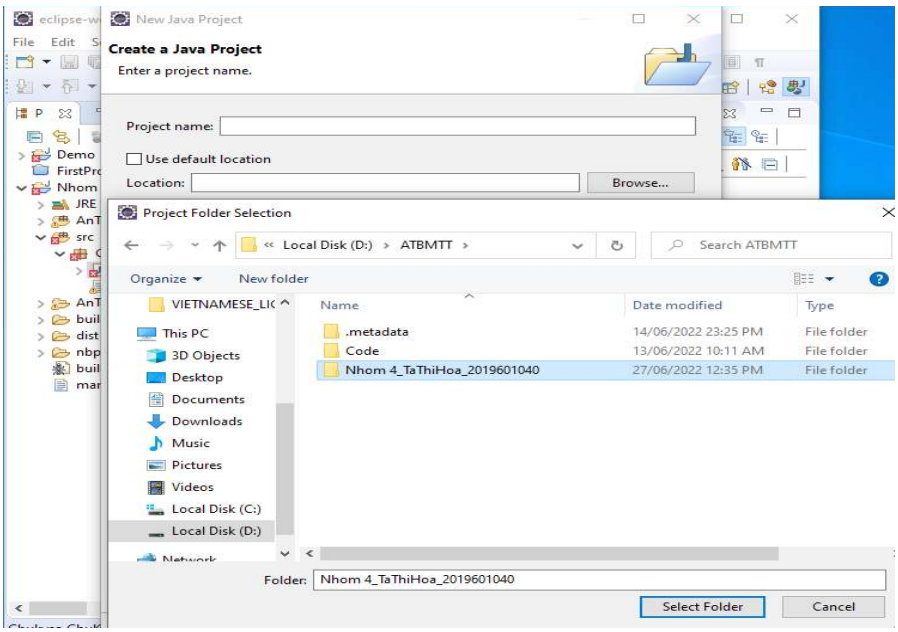
Ok, và đây là giao diện mở đầu của Eclipse.

Chạy chương trình demo :

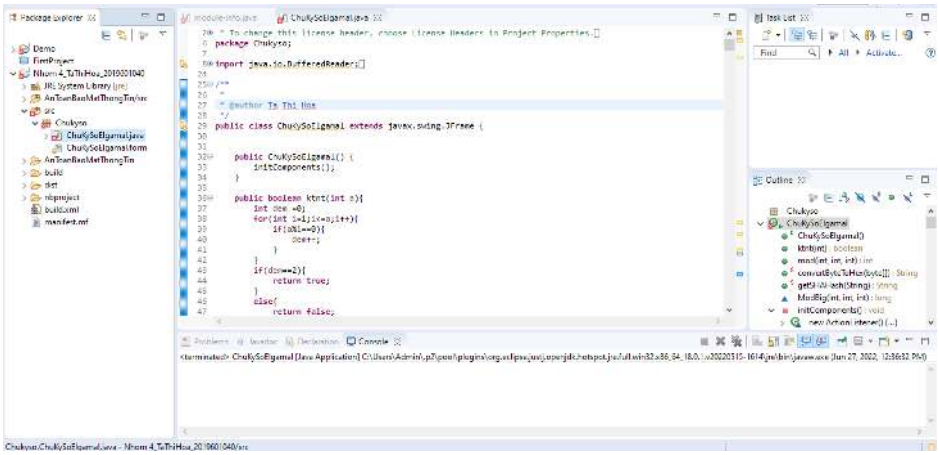
- Bước 1: Chọn “Java Project”



- Bước 2: Chọn thư mục demo bằng cách ấn vô “Browse”



- Bước 3: Nhấn vào scr và mở đuôi .jv chương trình sẽ hiện ra.

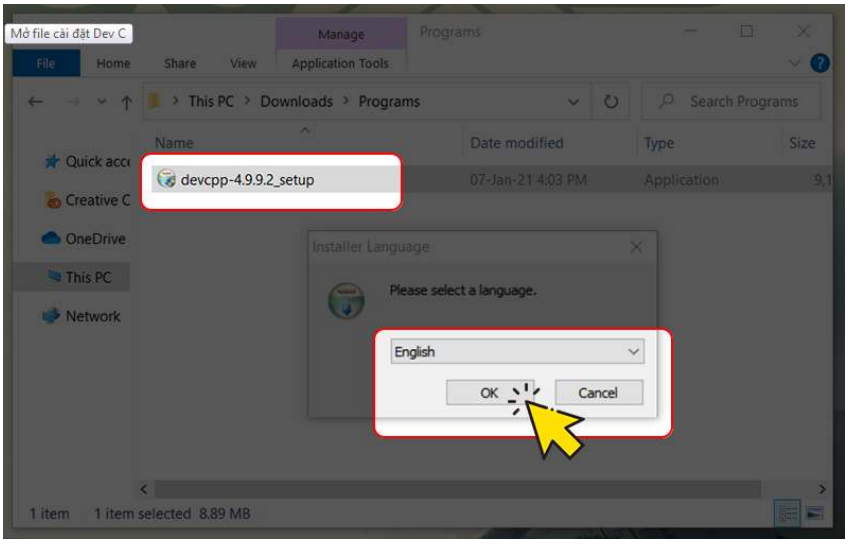


Bước 4: Nhấn “Run” để chạy chương trình

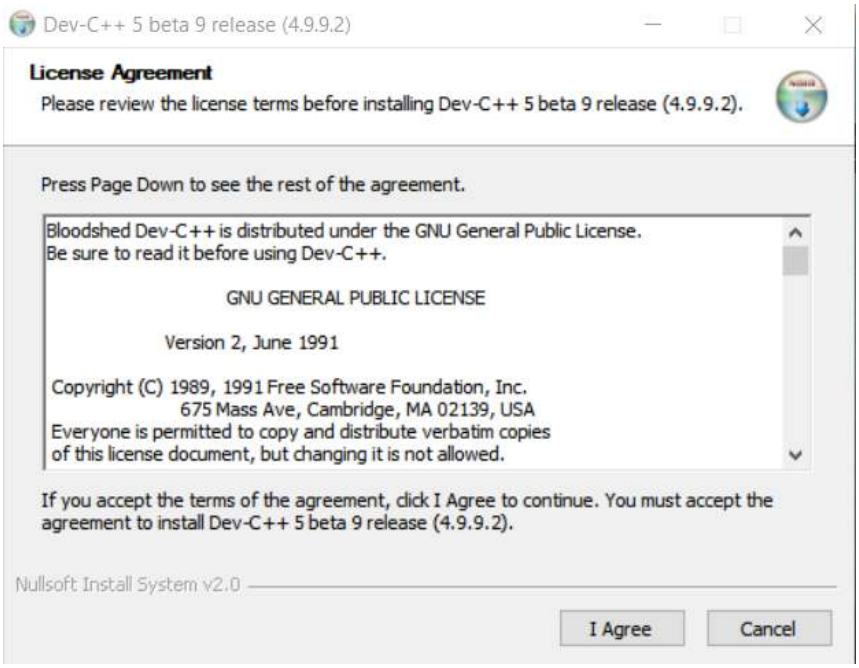
Phần mềm Dev-C++ chạy C++

Cài đặt chương trình :

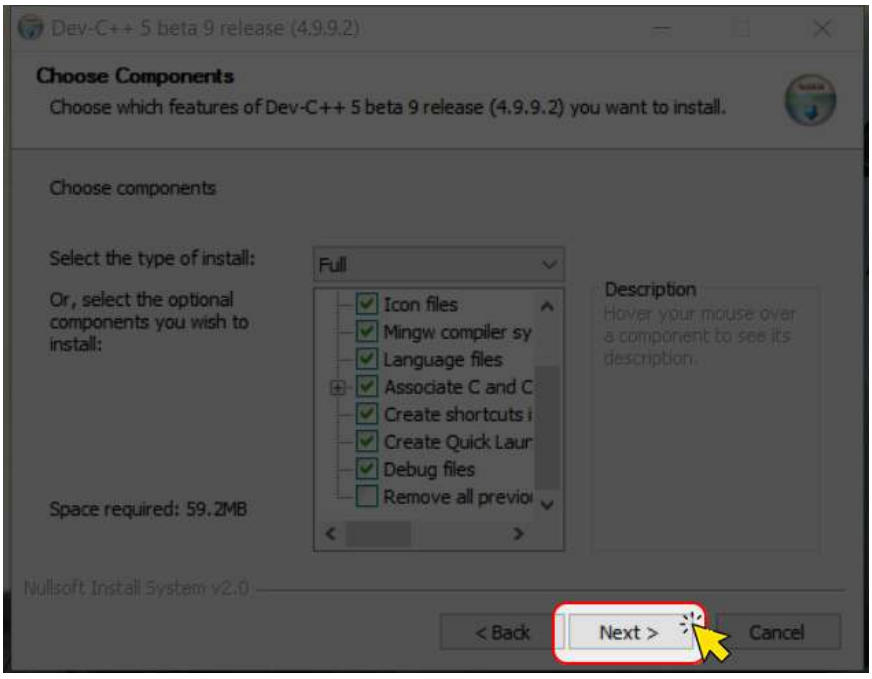
Bước 1: Mở file cài đặt Dev C++, chọn ngôn ngữ tiếng Anh (English) và bấm OK.



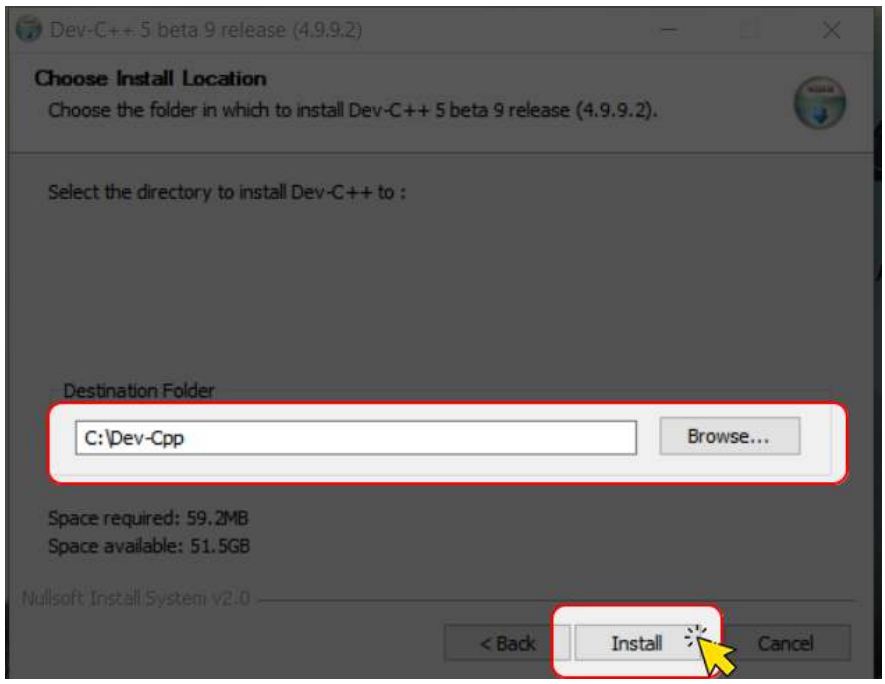
Bước 2: Cửa sổ License Agreement hiện lên, bấm Agree.



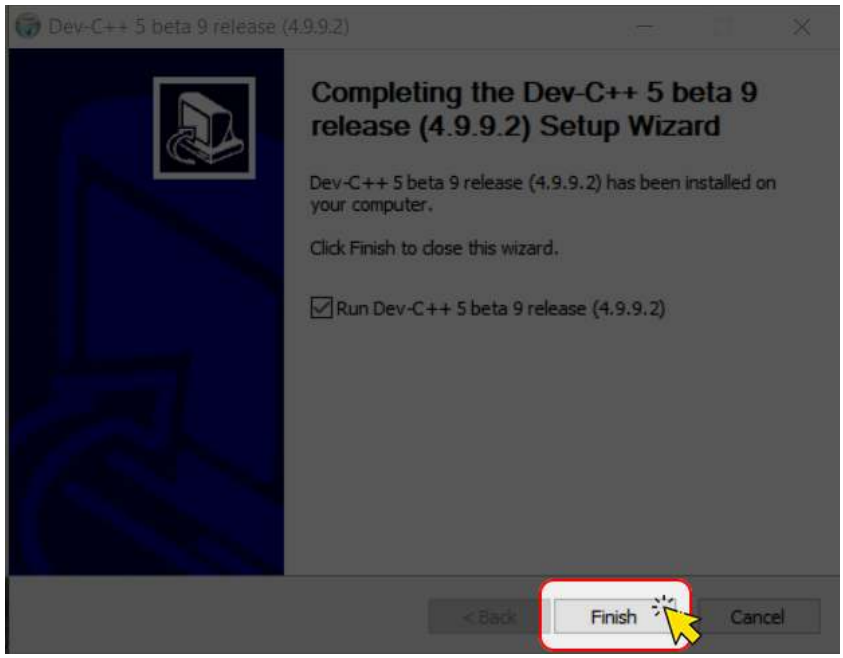
Bước 3: Ở cửa sổ Choose Components, tiếp tục bấm Next.



Bước 4: Bấm Browse để chọn nơi cài đặt Dev C++ (nếu cần) và bấm Install để tiến hành cài đặt.

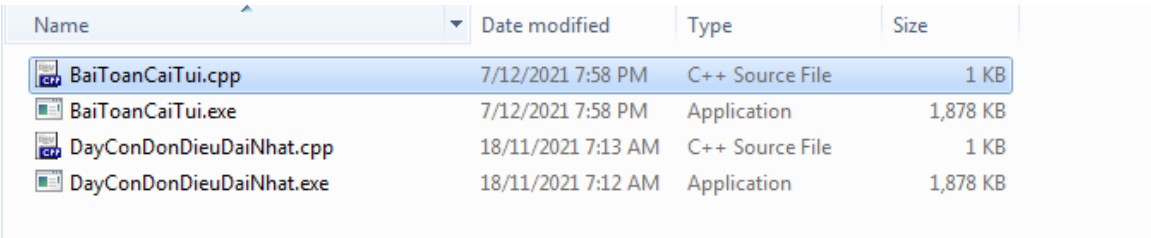


Bước 5: Bấm Finish để hoàn thành cài đặt.

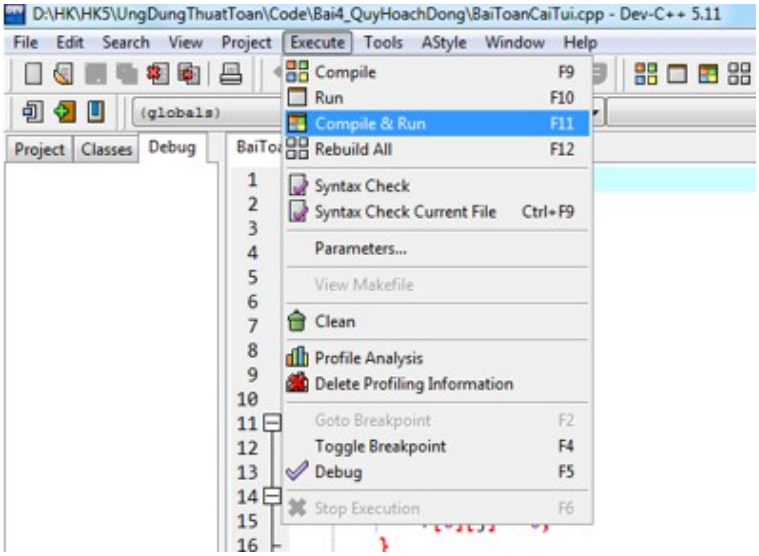


Chạy chương trình demo :

- Bước 1: Mở thư mục demo sau khi giải nén
- Bước 2: Kích đúp chuột vào file .cpp để mở chương trình



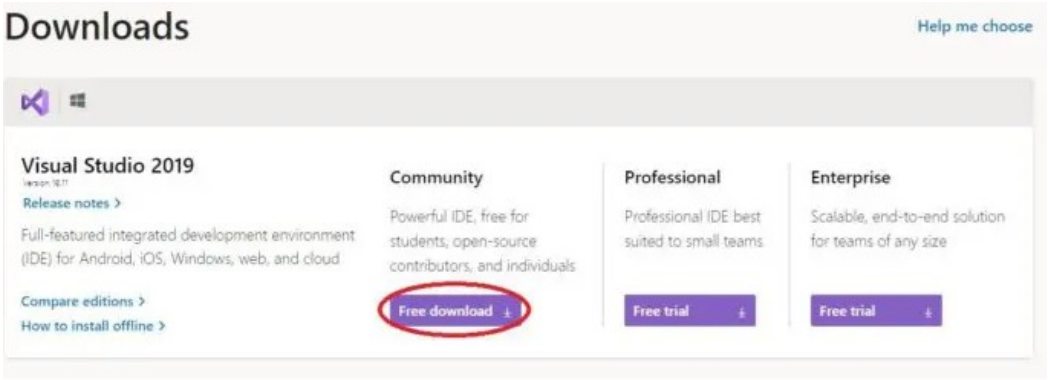
- Bước 3: Chọn Excute → Compile & Run để chạy chương trình



Phần mềm Visual studio 2019 chạy C#

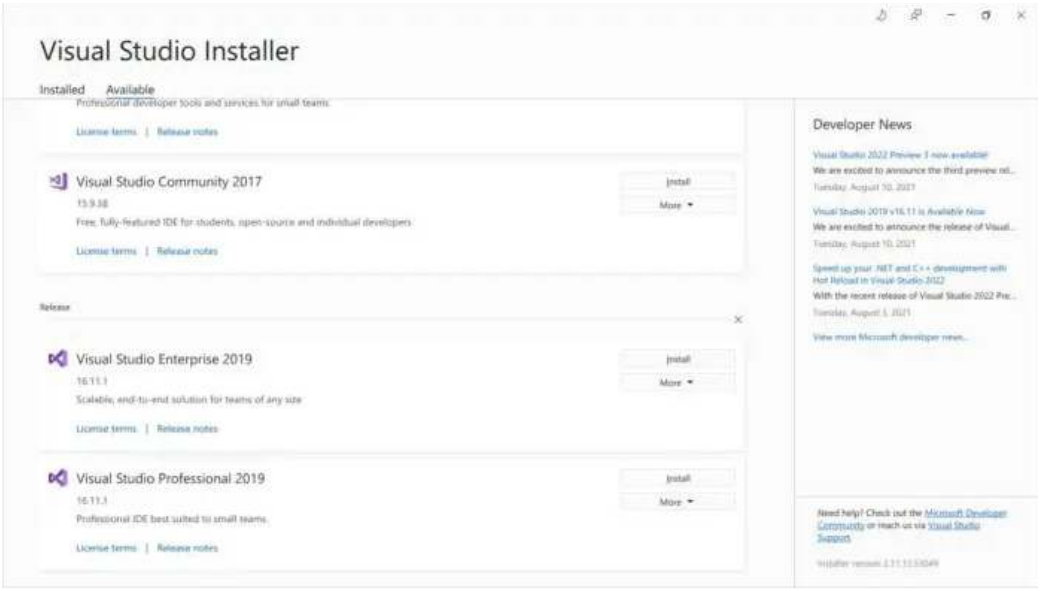
Cài đặt chương trình :

Bước 1: Download bộ cài Visual Studio



Bước 2. Tiến hành cài đặt

Sau khi download bộ cài, các bạn mở lên chờ một lúc để bộ cài tự giải nén, khi giải nén xong các bạn sẽ có được giao diện như hình dưới đây.

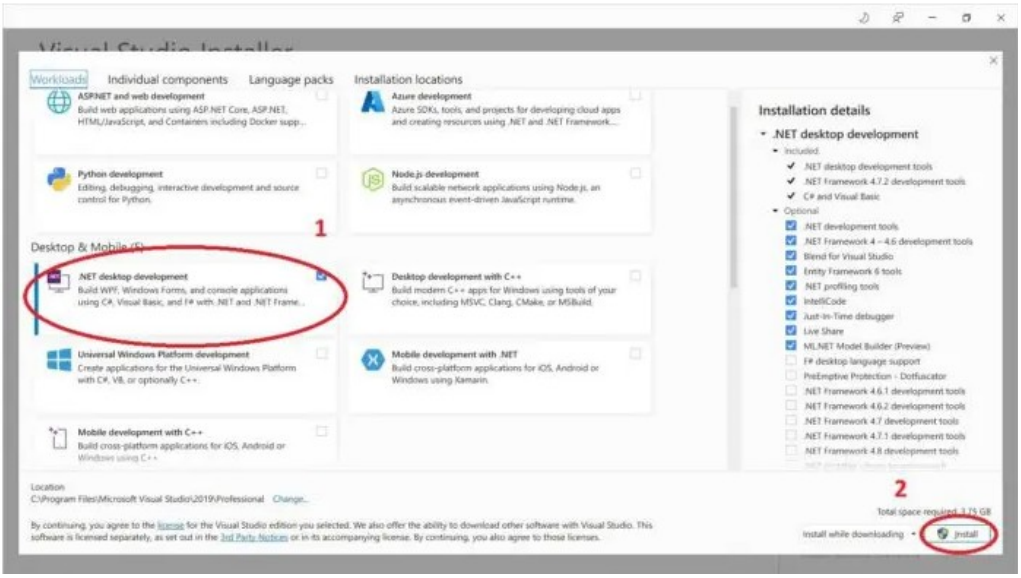


Vì ở đây mình đã cài đặt Visual Studio 2019 Community rồi nên nó sẽ không hiện ở đây. Đối với các bạn chưa cài đặt các bạn tìm tới ô Visual Studio 2019 Community rồi ấn vào Install nhé.

Bước 3: Cài đặt gói hỗ trợ C#

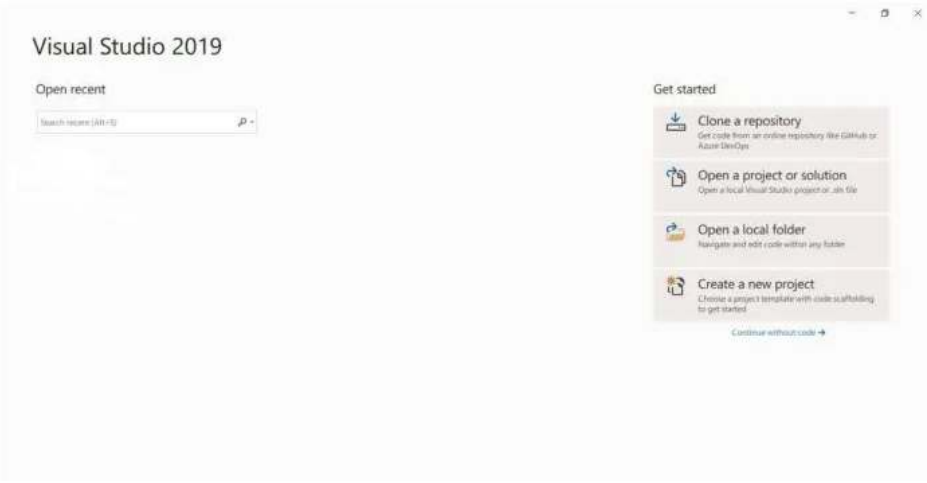
Để có thể sử dụng C# trong Visual Studio bạn cần phải cài đặt thêm gói hỗ trợ .NET trong Visual Studio trong gói hỗ trợ này bao gồm 2 ngôn ngữ khác nhau là C# và F# nhưng chúng ta chỉ quan tâm tới C# trong suốt khóa học này. Đối với gói hỗ trợ này, bạn có thể viết ra được các ứng dụng Desktop, Web, Console … bằng ngôn ngữ lập trình C#.

Bạn tích vào ô .NET desktop development sau đó chọn Install như trong hình.



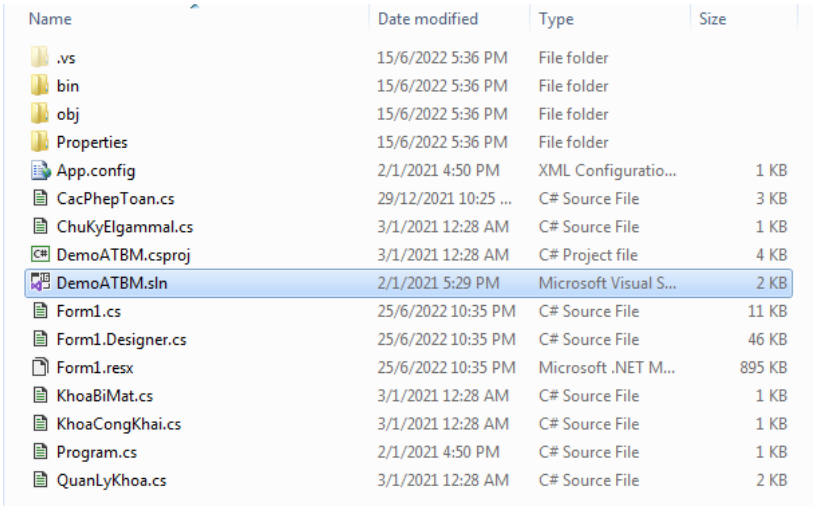
Bước 4: Kết thúc quá trình cài đặt

Sau khi quá trình cài đặt diễn ra hoàn tất, bộ cài sẽ tự động mở Visual Studio cho bạn và chuẩn bị cho lần thử đầu tiên. Ở bước này bạn cứ làm theo những gì mà họ bảo là được.

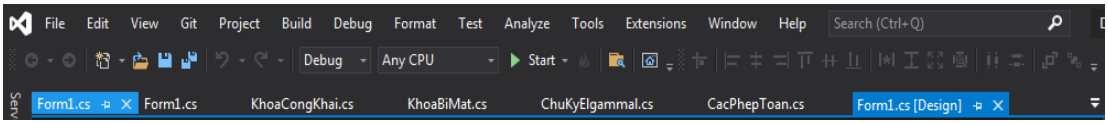


Chạy chương trình demo :

- Bước 1: Mở thư mục demo sau khi giải nén
- Bước 2: Kích đúp chuột vào file .sln để mở chương trình



- Bước 3: Nhấn “Start” để chạy chương trình



Phần mềm Pycharm chạy python

Cài đặt chương trình:

Bước 1: Đầu tiên, bạn vào trang chủ của Pycharm

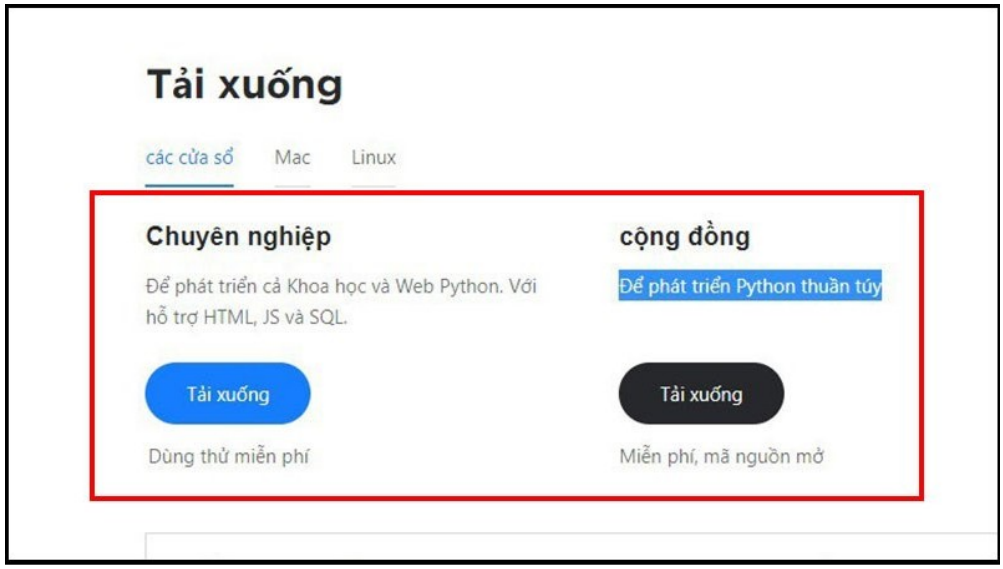
Sau đó nhấn chọn Tải xuống

Lúc này, giao diện sẽ hiển thị ra 2 danh mục mới cho bạn lựa chọn tải về

- Chuyên nghiệp: Để phát triển cả Khoa học và Web Python. Với hỗ trợ HTML, JS và SQL. Bạn sẽ được

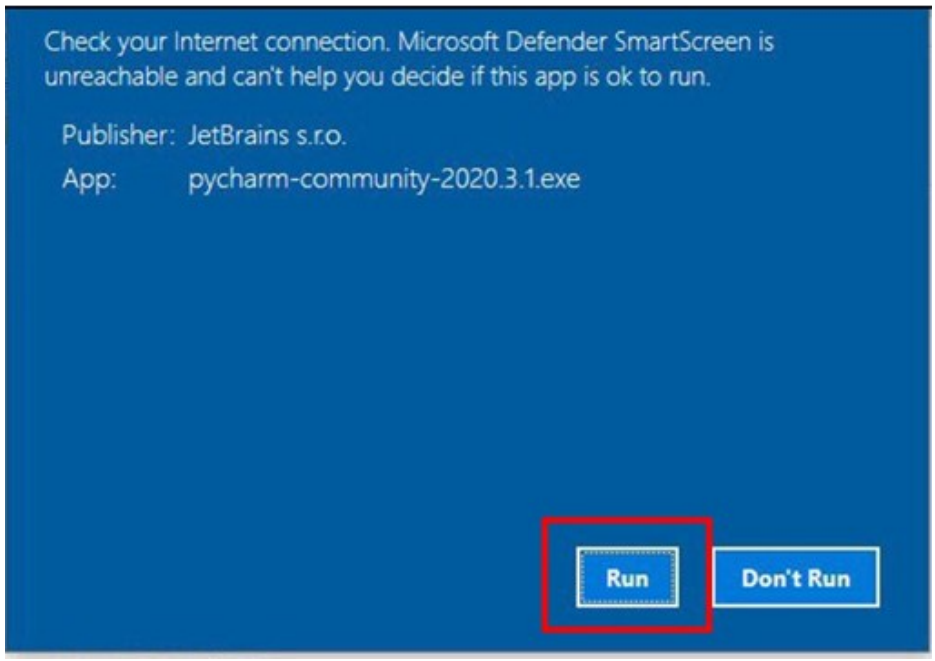
dùng thử miễn phí, nếu muốn dùng luôn bạn sẽ phải trả phí bản quyền

- Cộng đồng: Để phát triển Python thuần túy. Được sử dụng miễn phí.

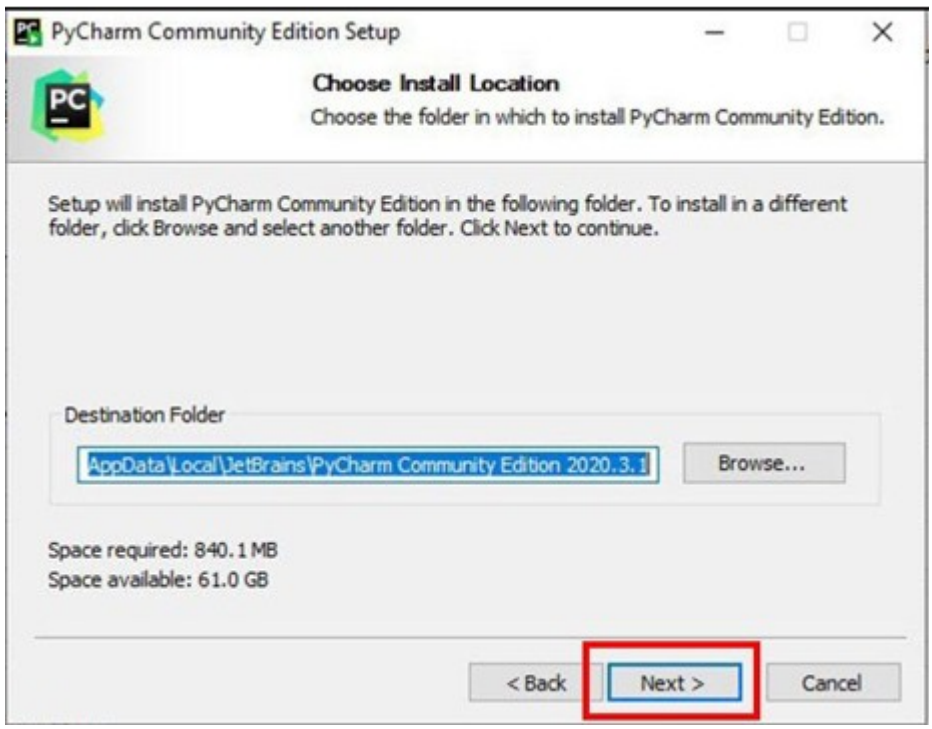


Bước 2: Quá trình tải xuống mất khoảng 3 phút

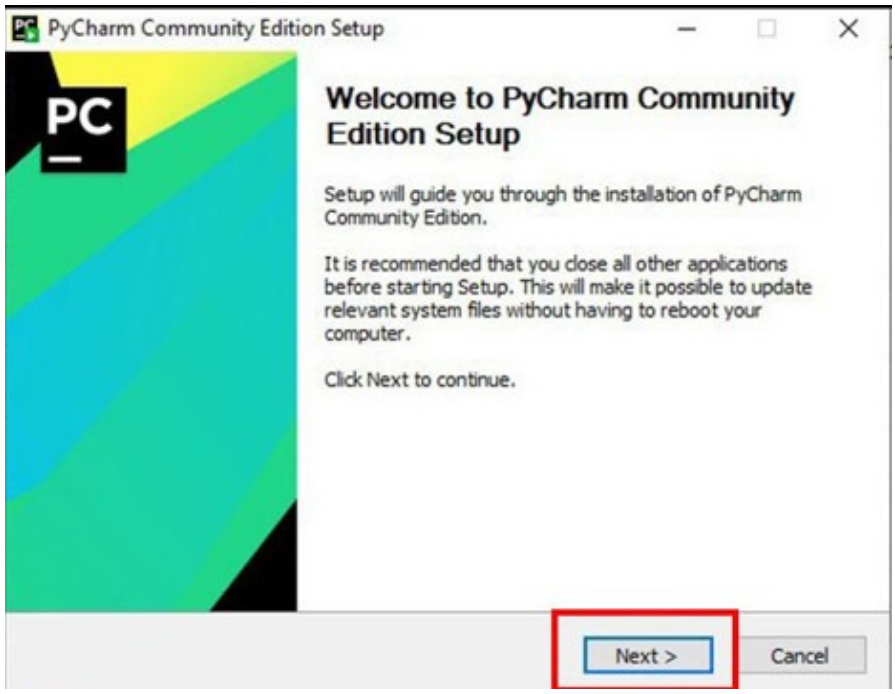
Hoàn tất tải xuống, bạn nhấn vào file vừa được tải về, sau đó nhấn vào mục Run



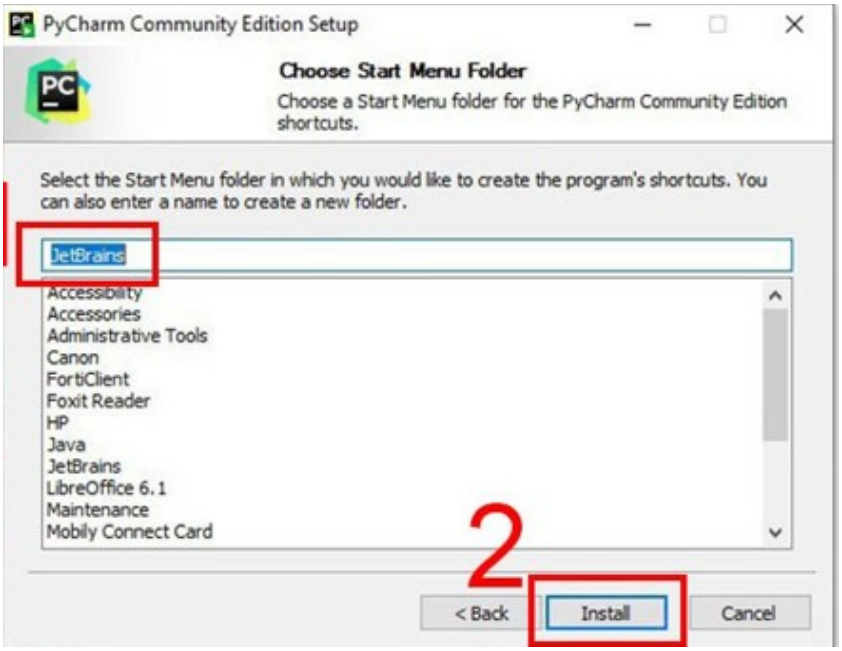
Bước 3: Sau đó, bạn mở file lên, nhấn chọn Next



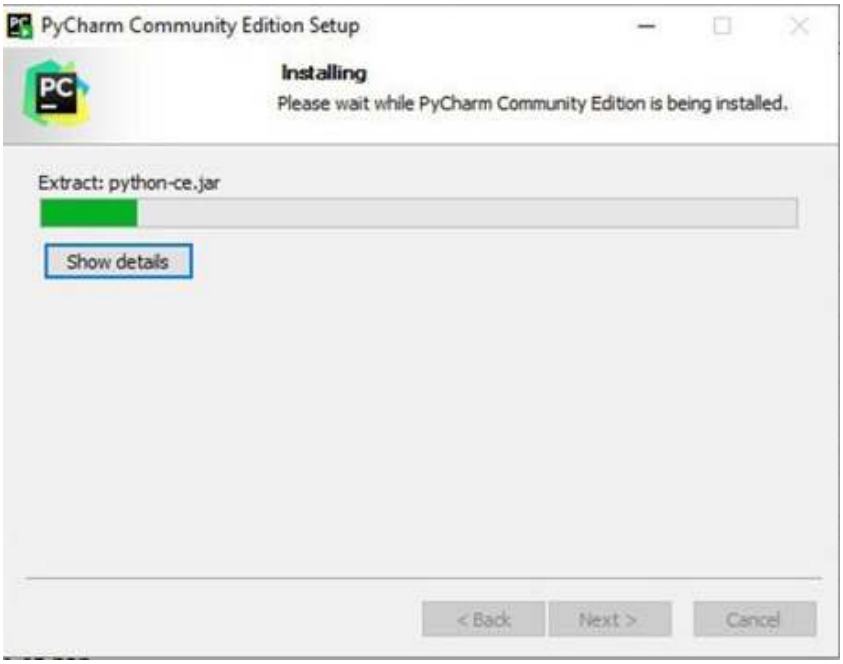
Bước 4: Tiếp tục nhấn chọn Next



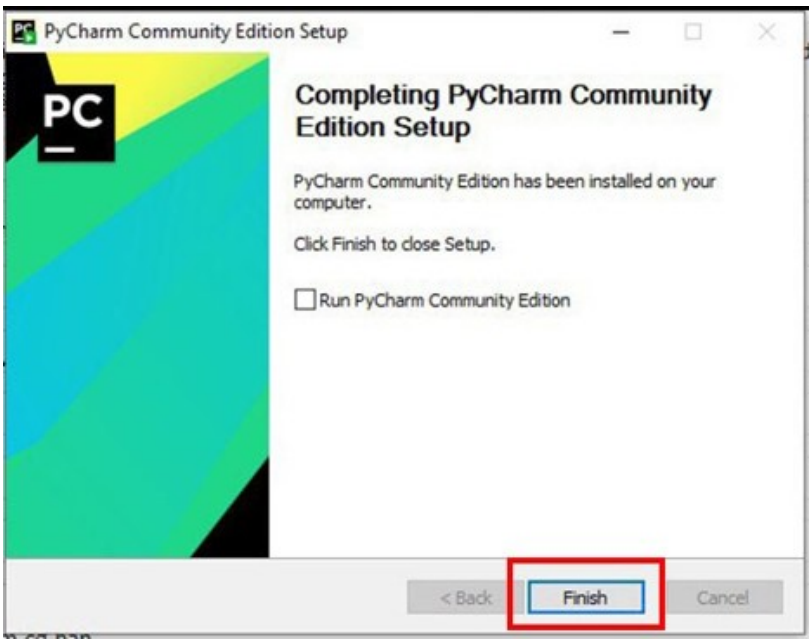
Bước 5: Tại thanh công cụ, tùy chỉnh sang mục JetBrains, sau đó nhấn chọn Install



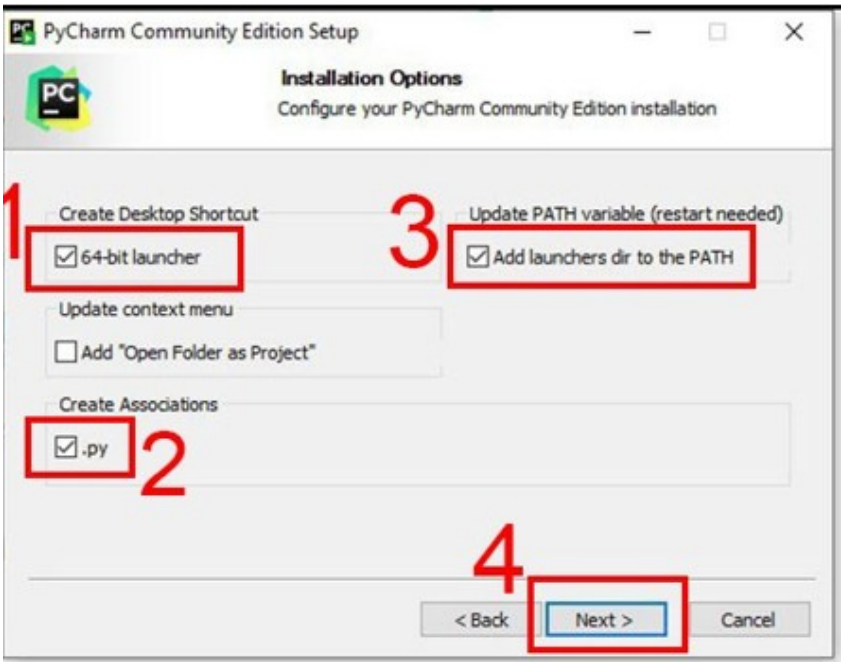
Bước 6: Đợi quá trình Installing diễn ra



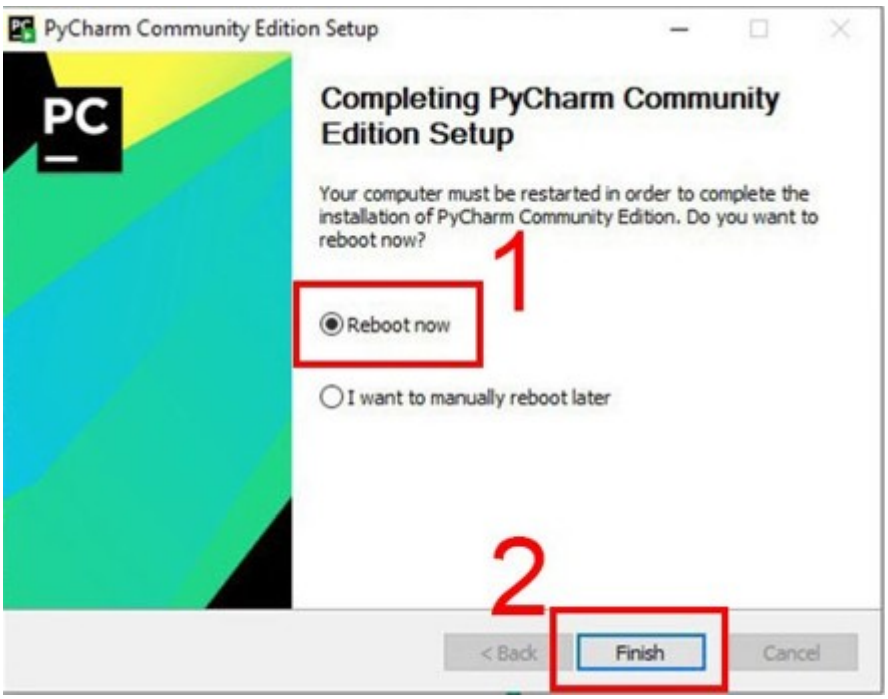
Bước 7: Nhấn chọn Finish



Bước 8: Tại giao diện tiếp theo, bạn tick vào 3 mục: 64-bit launcher, .py và Add launchers dir to the PATH nếu máy bạn chưa cài đặt Java. Sau đó nhấn Next



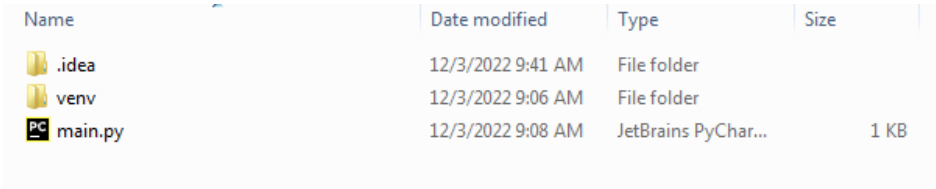
Bước 9: Tick vào Reboot now, sau đó nhấn chọn Finish để hoàn thành cài đặt



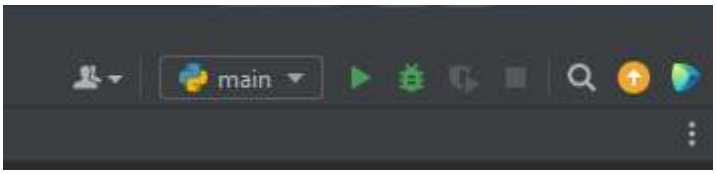
Chạy chương trình demo:

Bước 1: Mở thư mục demo sau khi giải nén

Bước 2: Kích đúp chuột vào file .py để mở chương trình



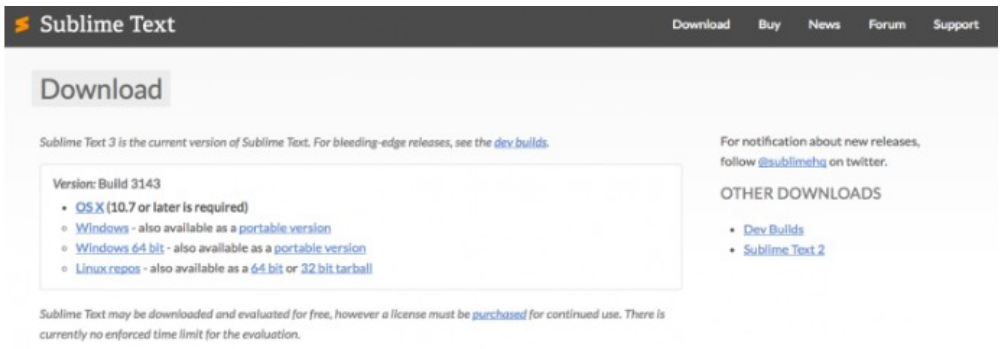
Bước 3: Ấn nút “Start” để chạy chương trình



Phầm mềm Sublime Text 3 chạy javascript

Cài đặt chương trình:

Để cài đặt Sublime Text 3 trên Windows hoặc macOS bạn truy cập vào trang tải sublime text 3 và chọn phiên bản phù hợp với hệ điều hành của mình.



Sau đó nhấp đúp vào tập tải về và tiến hành cài đặt như các phần mềm thông thường khác.Khi cài đặt xong bạn khởi động Sublime Text bằng cách tìm kiếm chương trình này trong LaunchPad (với hệ điều hành macOS) hoặc trong menu Start (đối với Windows) và nhấp vào biểu tượng chương trình.

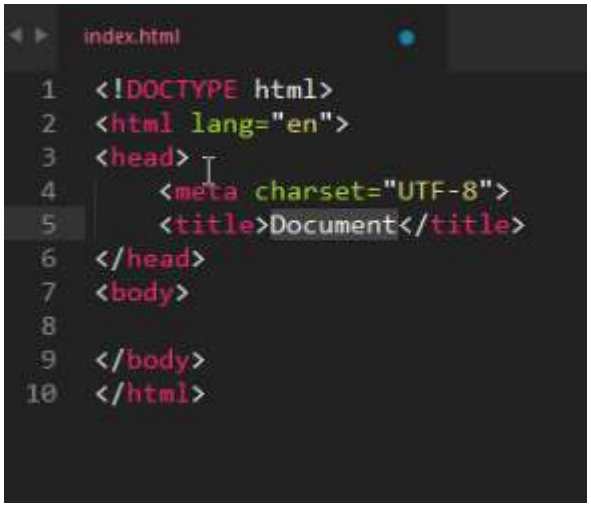
Thêm plugin cần thiết:

Ok sau khi cài đặt xong chúng ta sẽ tiến hành thêm các plugin để thao tác nhanh hơn khi code.

- Khởi động sublime text 3
- Trên thanh menu chọn Tools > Install Package Control
- Đợi hộp thoại hiện sublime text lên chọn ok
- Ấn tổ hợp phím ctrl + shift + p gõ install , chọn Package Control: install package

Gõ javascript snippets nhấn Enter đợi nó chạy khoảng 5 s. Tác dụng của plugin này là viết nhanh code js. Ví dụ như thêm function bạn chỉ cần gõ fun nhấn tab cái là nó ra cả đống code

Quay lại bước 4, gõ Emmet nhấn Enter đợi nó chạy khoảng 5s. Tác dụng cũng tương tự cái trên nhưng mà áp dụng cho HTML và CSS. Bạn gõ ! và nhấn tab một cái và xem kết quả(nhớ là save file có đuôi là html)



Tiếp tục quay lại bước 4 và gõ Bootstrap 4 snippets nhấn Enter.

Chạy chương trình demo:

Bước 1: Mở thư mục demo sau khi giải nén

Bước 2: Kích đúp chuột vào file .html để chạy chương trình

2.5 Thực hiện bài toán

1.1.1 Phân công công việc

Tên sinh viên	Tên công việc
Nguyễn Khắc Hiếu	Tìm hiểu về chữ ký điện tử • Giới thiệu về chữ ký điện tử • Khái niệm thế nào là chữ ký điện tử ? • Ứng dụng của chữ ký điện tử • Tầm quan trọng • Một số ưu nhược điểm của chữ ký điện tử. Viết chương trình đề mô với ngôn ngữ C++
Vũ Văn Hiếu	Chữ ký điện tử ElGamal • Lược đồ chữ ký điện tử ElGamal. • Ví dụ minh hoạ. • Độ an toàn của chữ ký điện tử ElGamal Viết chương trình đề mô với ngôn ngữ C#
Nguyễn Đình Hoàng	Tìm hiểu phương pháp mã hóa bất đối xứng ứng dụng trong chữ ký điện tử • Mã hóa bất đối xứng là gì? • Đặc điểm ✓ Ưu điểm ✓ Hạn chế • Ứng dụng trong chữ ký số ✓ Chữ ký số ✓ Chữ ký số sử dụng hệ mật mã Elgamal ✓ Ưu điểm ✓ Ý nghĩa Thuật toán hàm băm SHA-256 • Mã hoá SHA-256 là gì ? • Ứng dụng của SHA-256 Viết chương trình đề mô với ngôn ngữ Java
Vũ Huy Hoàng	Tìm hiểu về hàm băm SHA • Giới thiệu hàm băm Hash • Tính chất cơ bản của hàm băm Hash • Danh sách các hàm băm mật mã học • Ứng dụng hàm băm Hash Viết chương trình đề mô với ngôn ngữ Python
Nguyễn Khắc Hùng	Thuật toán hàm băm SHA-1 • Giới thiệu hàm băm SHA-1 • Thuật toán băm SHA-1

1.1.2 Nguyễn Khắc Hiếu – Tổng quan về chữ ký điện tử

1. Giới thiệu về chữ ký điện tử

Sự ra đời của văn bản điện tử đã kéo theo sự xuất hiện của giao dịch điện tử, từ đó phát sinh nhu cầu ký trên văn bản điện tử để thực hiện được các giao dịch ấy, và đó cũng là lúc mà chữ ký số được hình thành.

Khái niệm về chữ ký đã khá quen thuộc trong đời sống hàng ngày .Chữ ký được sử dụng hàng ngày để viết thư, rút tiền ở nhà băng, ký hợp đồng, ... Chữ ký viết tay thông thường trên tài liệu dùng để xác nhận một người ký nó.

Lược đồ chữ ký số là một phương pháp ký một thông điệp lưu dưới dạng điện tử.

Ví dụ như thông điệp được ký có thể truyền trên mạng máy tính. Giữa chữ ký tay và chữ ký số có một vài điều khác nhau cơ bản. Cụ thể như sau:

- Với chữ ký thông thường, nó là một phần vật lý của tài liệu. Đối với chữ ký số thì không gắn theo kiểu vật lý vào tài liệu mà gắn theo kiểu logic với tài liệu.
- Về việc kiểm tra chữ ký: Với chữ ký thông thường thì kiểm tra bằng cách so sánh nó với những chữ ký xác thực khác. Ví dụ, một người ký trên một tấm séc mua hàng, người bán phải so sánh chữ ký trên mảnh giấy với chữ ký nằm ở sau thẻ tín dụng để kiểm tra. Và ta có thể thấy đây không phải là phɋơng pháp an toàn. Mặt khác, lược đồ chữ ký số có thể được kiểm tra bằng cách sử dụng thuật toán kiểm thử công khai. Vì vậy bất kỳ ai cũng có thể kiểm thử chữ ký số. Việc dùng một sơ đồ chữ ký số an toàn có thể ngăn chặn được khả năng giả mạo.

- Còn một sự khác nhau cơ bản giữa chữ ký số và chữ ký thông thường là bản sao chép của chữ ký số đồng nhất với bản gốc. Còn của chữ ký thông thường có thể khác xa so với bản gốc .Điều này có nghĩa là phải cẩn thận ngăn chặn một thông điệp chữ ký số khỏi bị dùng lại. Ví dụ, nếu Bob ký bức điện số xác nhận Alice rút 100$ từ nhà băng, anh ta chỉ muốn Alice có thể làm điều đó một lần. Vì vậy, cần nghiên cứu những phương pháp để ngăn chặn việc chữ ký số bị dùng lại.

2. Khái niện chứ kỹ điện tử

Chữ ký điện tử là chương trình phần mềm gồm đoạn dữ liệu ngắn đính kèm văn bản gốc nhằm chứng thực tác giả của văn bản đó và giúp người nhận kiểm tra tính toàn vẹn của nội dung văn bản gốc.

Theo Điều 21 luật Giao dịch điện tử năm 2005: “Chữ ký điện tử được tạo lập dưới dạng từ, chữ, số, ký hiệu, âm thanh hoặc các hình thức khác bằng phương tiện điện tử, gắn liền hoặc kết hợp một cách logic với thông điệp dữ liệu, có khả năng xác nhận người ký thông điệp dữ liệu và xác nhận sự chấp thuận của người đó đối với nội dung thông điệp dữ liệu được ký”.

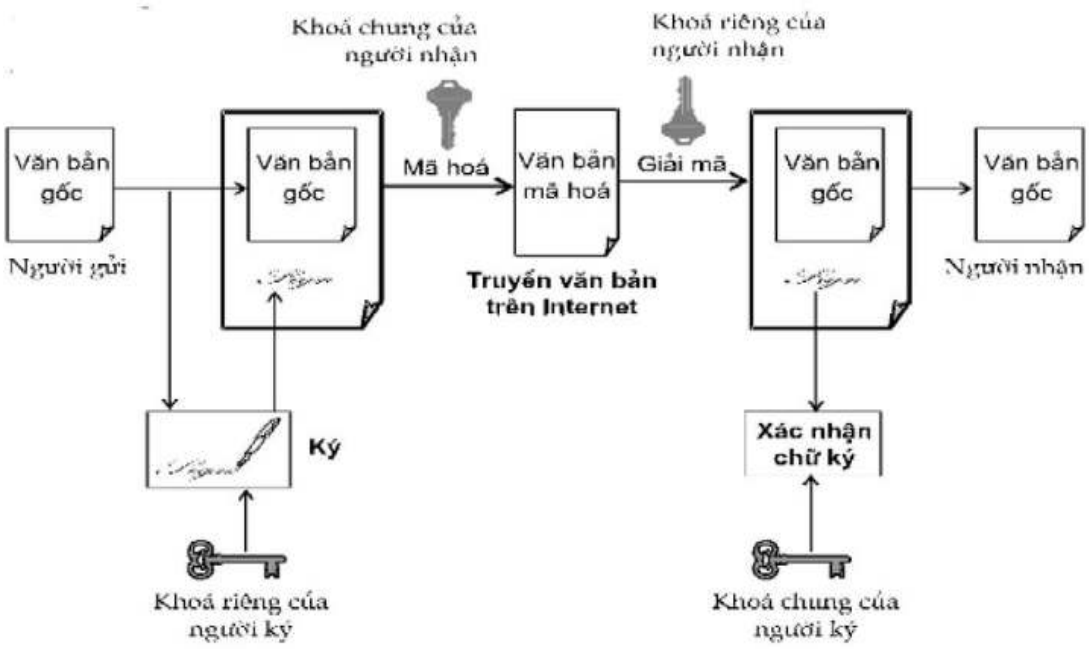
Về bản chất, chữ ký điện tử là chương trình phần mềm điện tử “được tạo ra bằng sự biến đổi một thông điệp dữ liệu sử dụng hệ thống mật mã không đối xứng. Trong đó, người đó có được thông điệp dữ liệu ban đầu và khóa công khai của người ký có thể xác định được chính xác:

- Việc biến đổi nêu trên được tạo ra bằng đúng khóa bí mật tương ứng với khóa công khai trong cùng một cặp khóa.

- Sự toàn vẹn nội dung của thông điệp dữ liệu kể từ khi thực hiện việc biến đổi nêu trên.

Như vậy, với sự xuất hiện của chữ ký điện tử, vấn đề về giá trị pháp lý của tài liệu điện tử, có thể coi như đã được giải quyết. Việc sử dụng chữ ký điện tử trong giao dịch điện tử cũng có những ưu điểm và nhược điểm nhất định.

Một lược đồ chữ ký số bao gồm 2 phần: 1 thuật toán ký và 1 thuật toán kiểm thử. Bob có thể ký trên thông điệp x bằng một thuật toán ký an toàn. Kết quả của việc ký sig(x) có thể đqợc kiểm thử bằng thuật toán công khai. Khi đưa 1 cặp (x,y), thuật toán kiểm thử trả lại câu trả lời là "True" hoặc "False" phụ thuộc vào việc chữ ký số là xác thực hay không xác thực.



Hình 1 : Sơ đồ chữ ký điện tử

3. Ứng dụng chữ ký điện tử

Ứng dụng của chữ ký số điện tử trong các hoạt động giao dịch thông thường:

- Ký và mã hóa với email

- Ký file tài liệu PDF
- Ký file Microsoft Office: Word, Excel, ...
- Đăng nhập Windows, Website
- Mã hóa và giải mã

Cụ thể:

Chữ ký số điện tử có thể sử dụng thay thế chữ ký tay trong tất cả các trường hợp giao dịch thương mại điện tử trong môi trường số :

- Sử dụng chữ ký số điện tử trong các giao dịch thư điện tử, ký vào các email để các đối tác, khách hàng của bạn biết có phải bạn là người gửi thư không.

- Sử dụng dụng chữ ký số điện tử để đầu tư chứng khoán trực tuyến, mua bán hàng trực tuyến, có thể dùng để thanh toán online, chuyển tiền trực tuyến mà không sợ bị mất cắp tiền như với đối với các tài khoản VISA, Master.

- Các đối tác có thể ký hợp đồng kinh tế hoàn toàn trực tuyến không cần gặp mặt trực tiếp với nhau, chỉ cần ký vào file hợp đồng và gửi qua e-mail.

- Dùng để kê khai, nộp thuế trực tuyến, khai báo hải quan và thông quan trực tuyến mà không phải mất thời gian in các tờ khai, trình ký đóng dấu đỏ của công ty rồi đến cơ quan thuế xếp hàng và ngồi đợi để nộp tờ khai này.

- Xác nhận đăng nhập vào một số Cổng giao dịch trực tuyến như : https://dangkykinhdoanh.gov.vn/ của Bộ Kế hoạch đầu tư; https://www.customs.gov.vn của Tổng cục Hải quan.

Bên cạnh đó, trong tương lai, các cơ quan chính phủ, nhà nước sẽ làm việc với nhân dân hoàn toàn trực tuyến và một cửa.

Việc sử dụng chữ ký số sẽ giúp các cá nhân, tổ chức , doanh nghiệp dễ dàng sử dụng với các ứng dụng chính phủ điện tử, các cơ quan nhà nước khi cần làm thủ tục hành chính hay xin một xác nhận của cơ quan nhà nước để khai vào mẫu và ký số để gửi.

Một số ứng dụng chữ ký số điện tử điển hình:

- ❖ Ứng dụng trong Chính phủ điện tử.
  + Ứng dụng của Bộ Tài chính
  + Ứng dụng của Bộ Công thương
  + Ứng dụng của Bộ KHCN, ...
- ❖ Ứng dụng trong Thương mại điện tử.
  + Mua bán, đặt hàng trực tuyến
  + Thanh toán trực tuyến, ...
- ❖ Ứng dụng trong giao dịch trực tuyến.
  + Giao dịch qua email
- ❖ Hội nghị truyền hình và làm việc từ xa với Mega e-Meeting...

4. Tầm quan trọng

- ✓ Là một công cụ trong việc xác định tính nguyên gốc, xác định tác giả.
- ✓ Bảo đảm tính toàn vẹn của tài liệu điện tử.
- ✓ Xác định địa vị pháp lý của tài liệu điện tử trong giao dịch điện tử.
- ✓ Việc sử dụng chữ ký điện tử trong phần lớn trường hợp là cơ sở khẳng định giá trị pháp lý của những văn bản điện tử tương đương với tài liệu giấy.

- ✓ Hiện nay, chữ ký điện tử là phương tiện duy nhất để xác nhận giá trị pháp lý của tài liệu điện tử.
- ✓ Việc sử dụng chữ ký số điện tử giúp doanh nghiệp tối ưu hóa các thủ tục và quy trình giao dịch trực tuyến, cụ thể như:

- Tiết kiệm được thời gian và chi phí trong quá trình hoạt động giao dịch điện tử.
- Linh hoạt trong cách thức ký kết các văn bản hợp đồng, buôn bán,...có thể diễn ra ở bất kỳ nơi đâu, ở bất kỳ thời gian nào.
- Đơn giản hóa quy trình chuyển, gửi tài liệu, hồ sơ cho đối tác khách hàng, cơ quan tổ chức.
- Bảo mật danh tính của cá nhân, doanh nghiệp an toàn.
- Thuận lợi trong việc nộp hồ sơ thuế, kê khai thuế cho doanh nghiệp khi chỉ cần sử dụng chữ ký điện tử thực hiện các giao dịch điện tử là có thể hoàn thành xong các quá trình đó.

5. Ưu, nhược điểm khi sử dụng chữ ký điện tử

- **Ưu điểm**
  - Là điều kiện 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. Văn bản điện tử có thể chuyển theo đường truyền internet trong thời gian ngắn. Như vậy, việc sử dụng chữ ký điện tử và thực hiện những giao dịch điện tử giúp tiết kiệm thời gian, sức lực và tăng hiệu quả lao động.
  - Ngăn chặn khả năng giả mạo chữ ký và có thể kiểm tra chữ ký bởi mã khóa công khai.
  - Ngăn chặn khả năng làm giả tài liệu. Bất cứ sự thay đổi nào trong tài liệu, cũng có thể bị phát hiện do chữ

ký điện tử được tạo ra bởi cặp khóa bí mật và khóa công khai. Khi nội dung tài liệu thay đổi, khóa công khai sẽ không còn tương thích với khóa bí mật và người nhận sẽ không thể dùng khóa công khai để giải mã bí mật.

- Cho phép xác định tác giả văn bản và tính nguyên gốc của văn bản.

- Nhược điểm
- Sự lệ thuộc vào máy móc và chương trình phần mềm. Để kiểm tra tính xác thực của chữ ký cần có hệ thống máy tính và phần mềm tương thích.
- Chữ ký điện tử có thời hạn. Chữ ký điện tử là chương trình phần mềm được cấp có thời hạn cho người sử dụng. Về lý thuyết, văn bản sẽ có hiệu lực pháp lý khi được ký trong thời hạn sử dụng của chữ ký.

➢ **Viết chương trình đề mô với ngôn ngữ C++**

1.1.3 Vũ Văn Hiếu, Nguyễn Đình Hoàng - Chữ ký điện tử ElGamal

1. Sơ đồ chữ ký điện tử ElGamal

➢ **Tạo cặp khoá(bí mật, công khai) (a, k) :**

+ Chọn phần tử nguyên tử **α ϵ Z_p^***. Đặt **P = Z_p^***, **A = Z_p^* x Z_{p-1}**

+ Chọn khoá bí mật là **α ϵ Z_p^***. Tính khoá công khai **β ≡ α^a mod p**.

+ Định nghĩa tập khoá: **={(p, α, a, β) : β ≡ α^a mod p}.**

+ Các giá trị **p, α, β** được công khai, phải giữ bí mật **a.**

- **Ký số**

  + Dùng 2 khoá ký: khoá **a** và số ngẫu nhiên **k ϵ Z_{p-1}^***

  + Vì **k ϵ Z_{p-1}^***, nên nguyên tố cùng p-1, do đó tồn tại k^{-1} mod (p-1)

  + Chữ ký trên **x ϵ P là y = $sig_k(x, k) = (\gamma, \delta)$, y ϵ A**

    Trong đó **$\gamma \epsilon Z_p^*$, $\delta \epsilon Z_{p-1}^*$:**

    $\gamma = \alpha^k \bmod p$ và

  $\delta = (x - a * \gamma) * k^{-1} \bmod (p-1)$

- **Kiểm tra chữ ký**

  $ver_k(x, \gamma, \delta) = TRUE \Leftrightarrow \beta^\gamma * \gamma^\delta \equiv \alpha^x \bmod p$

2. Ví dụ minh hoạ

Chứ ký ElGamal trên dữ liệu **x = 112**

a, Tạo cặp khoá (bí mật, công khai) (a, β):

- Chọn số nguyên tố p=463. Đặt **P = Z_p^*, A = $Z_p^* \times Z_{p-1}$.**
- Chọn phần tử nguyên tử **$\alpha = 2 \epsilon Z_p^*$.**
- Chọn khoá bí mật là **a** = 211 **ϵ Z_p^***.
- Tính khoá công khai **$\beta \equiv \alpha^a \bmod p$ =** 2^{211} mod 463 = 249.

Áp dụng thuật toán bình phương và nhân ta có:

+ x = 2, n= 211, m= 463

+ Đổi n=211 sang số nhị phân ta được n=211= $b_7b_6b_5b_4b_3b_2b_1b_0$=$11010011_{(2)}$

+ Khởi tạo p=1

Ta lập bảng để tính các bước theo giá trị của các bít nhị phân của 211

i	b[i]= 211_{10}	p=p*p	p=p mod 463	p=p*x	p=p mod 463
7	1	1	1	2	2
6	1	4	4	8	8
5	0	64	64	-	64
4	1	64^2	392	784	321
3	0	321^2	255	-	255
2	0	255^2	205	-	205
1	1	205^2	355	710	247
0	1	247^2	356	712	249

+ Với i = 7 : Có b_7 = 1:

- p = p*p = 1*1 = 1; p = p mod 463 = 1 mod 463 = 1
- p = p*x =1 *2 = 2; p =p mod 463 = 2 mod 463 =2

+ Với i = 6 : Có b_6 = 1:

- p = p*p = 2*2 = 4; p = p mod 463 = 4 mod 463 = 4
- p = p*x =4 *2 = 8; p =p mod 463 = 8 mod 463 = 8

+ Với i = 5 : Có b_5 = 0:

- p = p*p = 8*8 = 64; p = p mod 463 = 64 mod 463 = 64

+ Với i = 4 : Có b_4 = 1:

- p = p*p = 64*64 = 4096; p = p mod 463 = 4096 mod 463 = 392
- p = p*x =392*2 = 784; p =p mod 463 = 784 mod 463 = 321

+ Với i = 3 : Có $b_3 = 0$:

- p = p*p = 321*321 = 103041; p = p mod 463 = 103041 mod 463 = 255

+ Với i = 2 : Có $b_2 = 0$:

- p = p*p = 255*255 = 65025; p = p mod 463 = 65025 mod 463 = 205

+ Với i = 1 : Có $b_1 = 1$:

- p = p*p = 205*205 = 42025; p = p mod 463 = 42025 mod 463 = 355
- p = p*x =355*2 = 710; p =p mod 463 = 710 mod 463 = 247

+ Với i = 0 : Có $b_0 = 1$:

- p = p*p = 355*355 = 126025; p = p mod 463 = 126025 mod 463 = 356
- p = p*x =356*2 = 712; p =p mod 463 = 712 mod 463 = 249

Vậy 2^{211} mod 463 = 249

- Định nghĩa tập khoá: **$=\{(p, \alpha, a, \beta) : \beta \equiv \alpha^a \bmod p\}$.**
- Các giá trị **p**, **α, β** được công khai, phải giữ bí mật **a.**

b, Ký số: Chọn ngẫu nhiên bí mật

- **k** = 235 **є** $\mathbf{Z_{p-1}^*}$ **.** Khoá ký là **(a,k).**
- Vì **k є** $\mathbf{Z_{p-1}^*}$ **→** nguyên tố cùng **p-1, → ∃** $\mathbf{k^{-1}}$ **mod (p-1).**
- Cụ thể**: UCLN (k,p-1**)= UCLN (235,462) = 1,

  nên $\mathbf{k^{-1}}$ **mod (p-1) =** 235^{-1} mod 462 = 289.

Áp dụng thuật toán Ơ clit mở rộng ta có:

Cho $r_0 = 462$, $r_1 = 235$ Tìm 235^{-1} mod 462

Bước	r_i	q_{i+1}	r_{i+1}	r_{i+2}	s_i	t_i
0	462	1	235	227	1	0
1	235	1	227	8	0	1
2	227	28	8	3	1	-1
3	8	2	3	2	-1	2
4	3	1	2	1	29	-57
5	2	2	1	0	-59	116
6	-	-	-	-	88	-173

Bước i = 0:

- $r_i = r_0 = 462$, $r_{i+1} = r_1 = 235$. Lấy $r_0 = 462$ chia cho $r_1 = 235$ được
  - thương $q_{i+1} = q_1 = 1$
  - dư $r_{i+2} = r_2 = 227$
  - $t_0 = 0$, $s_0 = 1$

Bước i = 1:

- $r_i = r_1 = 235$, $r_{i+1} = r_2 = 227$. Lấy $r_1 = 235$ chia cho $r_2 = 227$ được
    - thương $q_{i+1} = q_2 = 1$
    - dư $r_{i+2} = r_3 = 8$
    - $t_0 = 1$, $s_0 = 0$

Bước i = 2:

- $r_i = r_2 = 227$, $r_{i+1} = r_3 = 8$. Lấy $r_2 = 227$ chia cho $r_3 = 8$ được
    - thương $q_{i+1} = q_3 = 28$
    - dư $r_{i+2} = r_4 = 3$
    - $s_i = s_2 = s_{(i-2)} – q_{(i-1)}* s_{(i-1)} = s_0 - q_1*s_1 = 1-1*0 =1$
    - $t_i = t_2 = t_{(i-2)} – q_{(i-1)}* t_{(i-1)} = t_0 - q_1*t_1 = 0-1*1 = -1$

Bước i = 3:

- $r_i = r_3 = 8$, $r_{i+1} = r_4 = 3$. Lấy $r_3 = 8$ chia cho $r_4 = 3$ được
    - thương $q_{i+1} = q_4 = 2$
    - dư $r_{i+2} = r_5 = 2$
    - $s_i = s_3 = s_{(i-2)} – q_{(i-1)}* s_{(i-1)} = s_1 - q_2*s_2 = 0-1*1 = -1$
    - $t_i = t_3 = t_{(i-2)} – q_{(i-1)}* t_{(i-1)} = t_1 - q_2*t_2 = 1-1*(-1) = 2$

Bước i = 4:

- $r_i = r_4 = 3$, $r_{i+1} = r_5 = 2$. Lấy $r_4 = 3$ chia cho $r_5 = 2$ được
    - thương $q_{i+1} = q_5 = 1$
    - dư $r_{i+2} = r_6 = 1$

- $s_i = s_4 = s_{(i-2)} – q_{(i-1)}* s_{(i-1)} = s_2 -q_3*s_3 = 1-28*(-1) = 29$
- $t_i = t_4 = t_{(i-2)} – q_{(i-1)}* t_{(i-1)} = t_2 -q_3*t_3 = (-1) -28*2 = -57$

Bước i = 5:

- $r_i = r_5 = 2$, $r_{i+1} = r_6 = 1$. Lấy $r_5 = 2$ chia cho $r_6 = 1$ được
  - thương $q_{i+1} = q_6 = 2$
  - dư $r_{i+2} = r_7 = 0$
  - $s_i = s_5 = s_{(i-2)} – q_{(i-1)}* s_{(i-1)} = s_3 -q_4*s_4 = (-1)-2*29 = -59$
  - $t_i = t_5 = t_{(i-2)} – q_{(i-1)}* t_{(i-1)} = t_3 -q_4*t_4 = 2-2*(-57) = 116$

Bước i = 6:

- $s_i = s_6 = s_{(i-2)} – q_{(i-1)}* s_{(i-1)} = s_4 -q_5*s_5 = 29-1*(-59) = 88$
- $t_i = t_6 = t_{(i-2)} – q_{(i-1)}* t_{(i-1)} = t_4 -q_5*t_5 = (-57)-1*116 = -173$

Vậy $235^{-1} \bmod 462 = -173 \pmod{462} = 289$

- Chữ ký trên dữ liệu x = 112 là **(γ, δ) =(16,108) ,** trong đó:

  $\gamma = \alpha^k \bmod p$ $= 2^{235} \bmod 463 = 16$

  Áp dụng thuật toán bình phương và nhân ta có:

+ x = 2, n= 235, m= 463

+ Đổi n=235 sang số nhị phân ta được $n=235= b_7b_6b_5b_4b_3b_2b_1b_0=11101011_{(2)}$

+ Khởi tạo p=1

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

i	b[i]= 235_{10}	p=p*p	p=p mod 463	p=p*x	p=p mod 463
7	1	1	1	2	2
6	1	4	4	8	8
5	1	64	64	128	128
4	0	128^2	179	-	179
3	1	179^2	94	188	188
2	0	188^2	156	-	156
1	1	156^2	260	520	57
0	1	57^2	8	16	16

+ Với i = 7 : Có b_7 = 1:

- p = p*p = 1*1 = 1; p = p mod 463 = 1 mod 463 = 1
- p = p*x =1 *2 = 2; p =p mod 463 = 2 mod 463 =2

+ Với i = 6 : Có b_6 = 1:

- p = p*p = 2*2 = 4; p = p mod 463 = 4 mod 463 = 4
- p = p*x =4 *2 = 8; p =p mod 463 = 8 mod 463 = 8

+ Với i = 5 : Có b_5 = 1:

- p = p*p = 8*8 = 64; p = p mod 463 = 64 mod 463 = 64
- p = p*x =64 *2= 128; p =p mod 463 = 128 mod 463 = 128

+ Với i = 4 : Có b_4 = 0:

- p = p*p = 128*128 = 16384; p = p mod 463 = 16384 mod 463 = 179

+ Với i = 3 : Có $b_3 = 1$:

- p = p*p = 179*179 = 32041; p = p mod 463 = 32041 mod 463 = 94
- p = p*x =94 *2= 188; p =p mod 463 = 188 mod 463 = 188

+ Với i = 2 : Có $b_2 = 0$:

- p = p*p = 188*188 = 35344; p = p mod 463 = 35344 mod 463 = 156

+ Với i = 1 : Có $b_1 = 1$:

- p = p*p = 156*156 = 24336; p = p mod 463 = 24336 mod 463 = 260
- p = p*x =260*2 = 520; p =p mod 463 = 520 mod 463 = 57

+ Với i = 0 : Có $b_0 = 1$:

- p = p*p = 57*57 = 3249; p = p mod 463 = 3249 mod 463 = 8
- p = p*x =8*2 = 16; p =p mod 463 = 16 mod 463 = 16

Vậy 2^{235} mod 463 =16

$\delta = (x - a * \gamma) * k^{-1} \mod (p-1) =$ (112-211*16) *289 mod 462 =108

c, Kiểm tra chữ ký:

ver_k (x, γ, δ)= đúng ⇔ $\beta^{\gamma} * \gamma^{\delta} \equiv \alpha^{x} \bmod p$

$\beta^{\gamma} * \gamma^{\delta}$ = $249^{16}*16^{108} \bmod 463 = 132$

α^{x} mod p = $2^{112} \bmod 463 = 132$

Hai giá trị đó bằng nhau, như vậy chữ ký là đúng.

3. Độ an toàn của chữ ký điện tử ElGamal

❖ Bài toán căn bản bảo đảm độ an toán của sơ đồ chữ ký ElGamal :

TH1 : Giả mạo chữ ký cùng với tài liệu được ký.

- ✓ T có thể ký trên tài liệu ngẫu nhiên bằng cách chọn trước đồng thời **x, γ, δ** .
- ✓ Chọn **x, γ, δ** thoả mãn điều kiện kiểm thử sau:
- ✓ Chọn các số nguyên I, j sao cho $0 \le i, j \le p-2$, GCD(j,p-1)=1 và tính:

$$\gamma = \alpha^{i} \beta^{j} \bmod p$$
$$\delta = -\gamma j^{-1} \bmod (p-1)$$
$$x = -\gamma ij^{-1} \bmod (p-1)$$

- ✓ Chứng minh (**γ, δ**) là chữ ký trên x, bằng cách kiểm tra điều kiện kiểm thử:

$$\beta^{\gamma} * \gamma^{\delta} \equiv \beta^{\alpha i \beta j} (\alpha^{i} \beta^{j})^{\alpha i \beta j j-1} \bmod p \equiv \alpha^{x} \bmod p$$

Ví dụ minh hoạ:

- Chọn các tham số của sơ đồ chữ ký ElGamal:
- Chọn p=463, phần tử sinh **α =**2, Khoá bí mật a =135.
- Kháo công khai **$\beta = \alpha^{a} \bmod p$** $=2^{135} \bmod 436 = 272$.
- Chọn **x, γ, δ** thoả mãn điều kiện kiểm thử như sau:

- Chọn i = 89, j = 125, 0 ≤ i, j ≤ p-2, GCD(j,p-1)=1.Tính j^{-1} mod (p-1) =377

  $\gamma = \alpha^i * \beta^j \bmod p =$ $2^{89} * 272^{125} \bmod 463 = 218$

  $\delta = -\gamma * j^{-1} \bmod (p-1) =$ $-218*377 \bmod 462 = 50$

  $x = -\gamma * i * j^{-1} \bmod (p-1) =$ $-218*89*377 \bmod 462 = 292$

- (**γ, δ**) =(218,50) là chữ ký trên x=292, vì thoả mãn điều kiện kiểm thử:

  $$\beta^{\gamma} * \gamma^{\delta} \equiv \beta^{\alpha i\, \beta j} (\alpha^i \beta^j)^{\alpha i\, \beta j\, j-1} \bmod p \equiv \alpha^x \bmod p$$

TH2: Sử dụng lại chữ ký của bức điện trước đó

- ✓ Nếu (**γ, δ**) là chữ ký trên tài liệu x có từ trước, thì có thể giả mạo chữ ký trên tài liệu x’ khác.
- ✓ Chọn số nguyên k, i, j thoả mãn 0 ≤ k, i, j ≤ p-2, $(k^{\gamma} - j^{\delta}, p-1) = 1$ và tính:

  $$\lambda = \gamma^h \alpha^i \beta^j \bmod p$$

  $$\mu = \delta \lambda (h\gamma - j\delta)^{-1} \bmod (p-1)$$

  $$x' = \lambda (h^x + i\delta) (h\gamma - j\delta)^{-1} \bmod (p-1)$$

- ✓ **(λ, μ)** là chữ ký trên x’, vì thoả mãn điều kiện kiểm thử:

  $$\beta^{\gamma} * \gamma^{\mu} \equiv \alpha^{x'} \bmod p$$

➔**Tóm lại:** Cả hai cách giả mạo nói trên đều cho chữ ký đúng trên tài liệu tương ứng, nhưng đó không phải là tài liệu được chọn theo ý của người giả mạo. Tài liệu đó đều được tính sau khi tính chữ ký, vì vậy giả mạo loại này trong thực tế cũng không có ý nghĩa nhiều.

- **Viết chương trình đề mô với ngôn ngữ C#**

1.1.4_Vũ Huy Hoàng, Nguyễn Khắc Hùng – Tìm hiểu về phương pháp mã hoá bất đối xứng ứng dụng trong chữ ký điện tử, thuật toán hàm băm SHA-256

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

1. **Khái niệm mã hoá bất đối xứng**

   Hệ mã hóa khóa bất đối xứng là một dạng mật mã hóa cho phép người sử dụng trao đổi các thông tin mật mà không cần phải trao đổi các khóa chung bí mật trước đó. Điều này được thực hiện bằng cách sử dụng một cặp khóa có quan hệ toán học với nhau là khóa công khai và khóa bí mật.

2. **Đặc điểm**

a). Ưu điểm:

+ Thuật toán viết một lần, công khai cho nhiều lần dùng, nhiều người dùng, họ chỉ cần giữ bí mật khóa riêng của mình.

+ Khi biết các tham số ban đầu của hệ mã hóa, việc tính ra cặp khóa công khai và bí mật phải là “dễ”.

+ Khả năng lộ khóa bí mật khó hơn vì chỉ có một người giữ.

+ Nếu thám mã biết khóa công khai và bản mã C, thì việc tìm ra bản rõ P là một bài toán “khó”, số phép thử là vô cùng lớn, không khả thi.

b). Hạn chế: Mã hóa và giải mã chậm hơn hệ mã hóa khóa đối xứng.

3. Ứng dụng chữ ký số

a, Chữ ký số

Chữ ký số là một dạng của chữ ký điện tử. Nó là một dạng dữ liệu dùng để chứng thực cho các dữ liệu khác.

Chữ ký số sử dụng một hệ mã hóa bất đối xứng. Trong phần lớn các trường hợp, nó còn có thể kiểm tra cả tính toàn vẹn của dữ liệu nữa. Chữ ký số tương tự như chữ ký tay trên nhiều phương diện, nhưng việc cài đặt và sử dụng chữ ký số khó khăn hơn rất nhiều.

b, Chữ ký số sử dụng hệ mật mã Elgamal

Việc ký tên và xác thực chữ ký số sử dụng hệ mã hóa Elgamal tương tự như quá trình mã hóa mà giải mã. Tuy nhiên vai trò của public key và private key thì có thay đổi đôi chút.

Để tạo chữ ký, người gửi sẽ dùng private key và người nhận sẽ dùng public key để xác thực chữ ký đó.

Tuy nhiên, vì bản tin rất dài nên việc mã hóa toàn bộ bản tin sẽ rất mất thời gian. Vì vậy, trong thực hành, chữ ký số thường sử dụng phương pháp mã hóa giá trị hash của bản tin. Việc này mang lại rất nhiều lợi ích như:

Các hàm hash là hàm 1 chiều, vì vậy dù có được hash cũng không thể biết được bản tin gốc như thế nào.

Độ dài hash là cố định và thường rất nhỏ, vì vậy chữ số sẽ không chiếm quá nhiều dung lượng.

Giá trị hash còn có thể dùng để kiểm tra lại bản tin nhận được có nguyên vẹn hay không?

Chữ ký số đem lại nhiều giá trị hơn chữ ký tay rất nhiều. Có lẽ cũng vì vậy, việc xử lý chữ ký số phức tạp hơn hẳn chữ ký tay truyền thống.

c, Ưu điểm

- Khả năng nhận thực:

Các hệ thống mật mã 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 không cần phải được mã hóa mà chỉ cần mã hóa hàm băm của văn bản đó. Khi cần kiểm tra, bên nhận giải mã để lấy lại hàm băm và kiểm tra với hàm băm của văn bản nhận được. Nếu hai giá trị 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 lỗi trong khi truyền vì nếu văn bản bị thay đổi thì hàm băm cũng thay đổi và lập tức bị phát hiện. Quá trình mã hóa sẽ ẩn nội dung của gói tin đối với bên thứ ba nhưng không ngăn cản được việc thay đổi nội dung của nó.

- Tính không thể phủ nhận:

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

khóa bí mật vẫn có thể bị lộ và tính không thể phủ nhận cũng không thể đạt được hoàn toàn.

d, Ý nghĩa

- ✓ Được sử dụng rộng rãi trong thương mại điện tử để thực hiện các giao dịch điện tử nhằm xác định rõ người kí văn bản
- ✓ Chống chối bỏ khi người ký đã ký vào văn bản thì họ không thể phủ nhận là chữ ký đó không phải của họ.
- ✓ Xác thực nội dung của văn bản ký: nhằm kiểm tra tính toàn vẹn của văn bản xem nó có bị thay đổi thông tin trong quá trình vận chuyển.
- ✓ Độ an toàn của chữ ký số rất là cao, hiện nay được sử dụng rất phổ biến trong giao dịch điện tử.

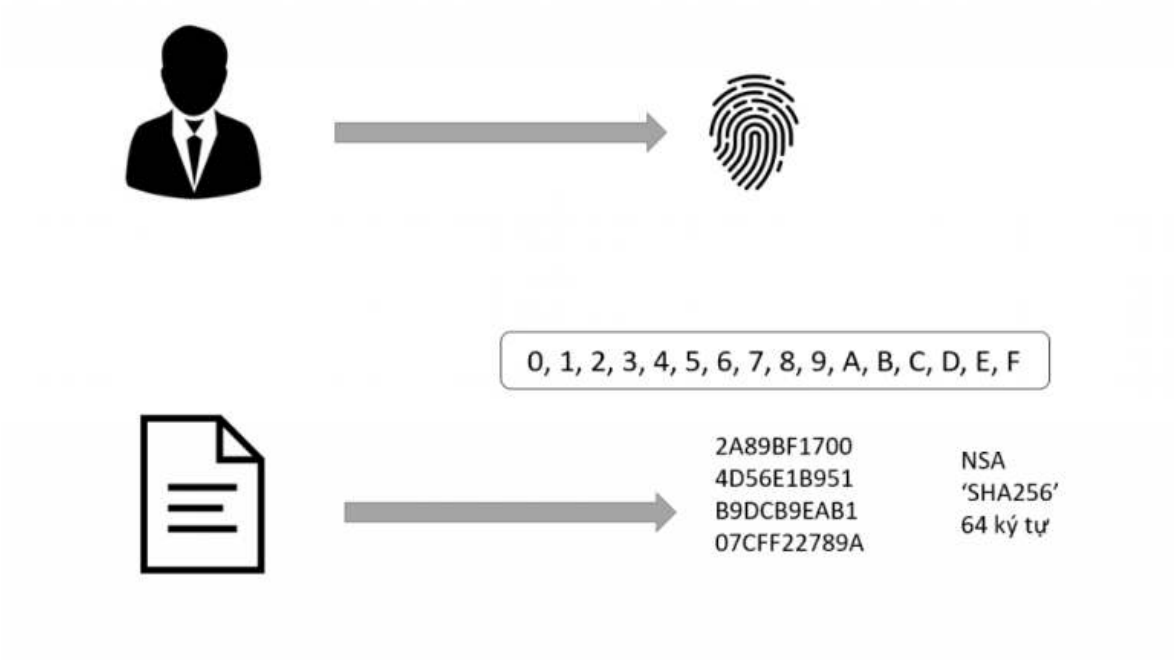
Để đảm bảo an toàn, và tăng hiệu quả của chữ ký số cần có các tổ chức chứng thực điện tử nhằm cung cấp và đảm bảo độ tin cậy cho chữ ký số. Đó là các tổ chức công an.

*** Thuật toán hàm băm SHA-256**

1. Mã hoá SHA-256 là gì ?

Mã hóa SHA256 là một trong những hàm băm kế thừa của thuật toán SHA-2. SHA-2 là một nhóm thuật toán được nâng cấp từ SHA-1, có tính bảo mật và an toàn cao hơn, giải quyết được những lỗ hổng còn tồn tại của thuật toán SHA-1. SHA-2 chứa sáu hàm băm ở các cấp độ khác nhau (224, 256, 384, 512, 512/224, 512/256). Trong đó, SHA256 được định nghĩa là thuật toán băm bảo mật 256 bit. Thuật toán này cho phép tạo ra các hàm băm mà không thể đảo ngược và mang tính duy nhất.

Ý nghĩa của con số 256 xuất hiện trong tên mã hóa là giá trị thông báo băm cuối cùng. Tức là, cho dù độ dài của thông tin trước khi được mã hóa là bao nhiêu thì sau quá trình mã hóa, giá trị băm sẽ luôn là 256 bit.



Hình 2 :Ví dụ minh hóa dễ hiểu về thuật toán SHA256 là gì?

Một số đặc điểm của Mã hóa SHA256

Mã hóa SHA256 có một số tính năng và đặc điểm nổi bật như sau:

- Độ dài của thông điệp: Độ dài của thông tin trước khi mã hóa phải nhỏ hơn 264 bit
- Độ dài của mã hóa: Độ dài của của thông tin sau khi được mã hóa sẽ luôn có giá trị là 256 bit
- Không thể đảo ngược: Theo thiết kế, mọi hàm băm như SHA256 đều không thể đảo ngược. Bạn không thể có được đoạn thông tin trước khi mã hóa một khi bạn đã tiến hành mã hoá SHA256

Hình 3:Đặc điểm của Mã hóa SHA256

2. Ứng dụng của mã hoá SHA-256

Hiện nay, mã hóa SHA256 đang được ứng dụng rất đa dạng. Kể từ năm 2008, hàm băm SHA đã được STECH sử dụng làm mã xác thực trong các gói thông tin trao đổi, làm khóa bản quyền cho một số phần mềm. Phổ biến nhất có thể kể đến một số giao thức bảo mật an toàn trên mạng internet hiện nay đang sử dụng mã hóa SHA256 như:

- Digital Signature Verification (Xác minh chữ ký số): Bản chất của chữ ký điện tử dựa trên phương pháp mã hóa bất đối xứng để xác minh tính xác thực của một tài liệu hay một tệp nào đó
- Password Hashing (Băm mật khẩu): Đối với nền tảng website, các dữ liệu mật khẩu của người dùng tồn tại ở định dạng băm vì 2 lợi ích: Tăng cường bảo mật và giảm tải cho cơ sở dữ liệu trung tâm
- SSL Handshake (Lớp bảo mật giữa máy khác và máy chủ): SSL Handshake là một phần quan trọng của các phiên duyệt web và được thực hiện bằng cách sử dụng các hàm băm SHA, trong đó có hàm SHA256. Bản chất của lớp bảo mật này là trình web của bạn và các máy chủ web đồng ý

về khóa mã hóa và xác thực băm để đảm bảo kết nối an toàn

- Integrity Check (Kiểm tra tính toàn vẹn): Việc xác minh tính toàn vẹn của một tệp thường được thực hiện trên các thuật toán SHA256 và thuật toán MD5. Những thuật toán này sẽ giúp duy trì chức năng giá trị của tệp một cách đầy đủ, đồng thời đảm bảo chúng không bị thay đổi khi thực hiện chuyển tiếp
- Xác thực giao dịch và lưu trữ dạng chuỗi Bitcoin: Đây là một trong những ứng dụng nổi tiếng, được biết đến nhiều nhất của SHA256 khi được sử dụng để xác thực các giao dịch và lưu trữ dạng chuỗi các sự kiện theo thời gian, được liên kết với nhau bởi các mã xác thực blockchain.

Hiện nay, mã hóa SHA256 được ứng dụng phổ biến nhất trên hệ thống Tiền tệ Bitcoin

Mã hóa SHA256 có an toàn không? Có thể giải mã SHA256 không?

Hiện nay, cách dùng phổ biến của nhóm mã một chiều SHA có đặc tính là tạo ra chữ ký của thông điệp bằng cách tính hàm băm của một chuỗi ghép được xác định từ một thông điệp cần xác thực với một từ khóa bí mật. Với tính chất của mã một chiều, chữ ký thông điệp này có thể công khai hoặc không, tuy nhiên, mã hoá SHA256 được gọi là an toàn vì chúng không thể truy ngược lại để tìm đoạn dữ liệu gốc hay không thể giải mã SHA256. Và việc tìm được hai đoạn dữ liệu khác nhau có cùng kết quả băm tạo ra bởi thuật giải SHA256 là không khả thi.

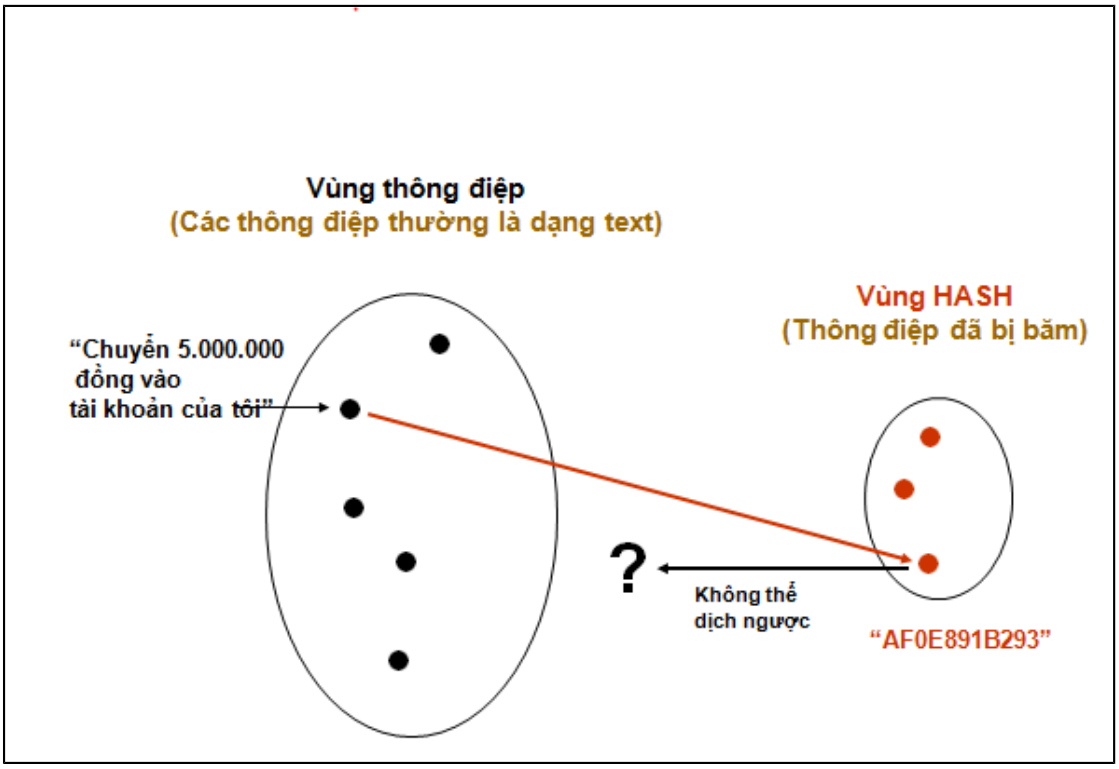
➢ **Viết chương trình đề mô với ngôn ngữ Java**

2.5.1 Vũ Huy Hoàng – Tìm hiểu về hàm băm SHA

1. **Giới thiệu hàm băm Hash**

Hàm băm (Hash function) là một hàm toán học chuyển đổi một thông điệp đầu vào có độ dài bất kỳ thành một dãy bit có độ dài cố định (tuỳ thuộc vào thuật toán băm). Dãy bit này được gọi là thông điệp rút gọn (message digest) hay giá trị băm (hash value), đại diện cho thông điệp ban đầu.

Hàm băm (hash function) là hàm một chiều mà nếu đưa một lượng dữ liệu bất kì qua hàm này sẽ cho ra một chuỗi có độ dài cố định ở đầu ra.



Hình 4: Ví dụ hàm băm hash

Mã hóa SHA là gì?

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

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

Năm thuật giải SHA chuẩn bao gồm:

SHA-1: Trả lại kết quả dài 160 bit

SHA-224: Trả lại kết quả dài 224 bit

SHA-256: Trả lại kết quả dài 256 bit

SHA-384: Trả lại kết quả dài 384 bit

SHA-512: Trả lại kết quả dài 512 bit

2. Tính chất cơ bản của hàm băm Hash

- ✓ **Tính một chiều:** không thể suy ra dữ liệu ban đầu từ kết quả, điều này tương tự như việc bạn không thể chỉ dựa vào một dấu vân tay lạ mà suy ra ai là chủ của nó được.
- ✓ **Tính duy nhất**: xác suất để có một vụ va chạm (hash collision), tức là hai thông điệp khác nhau có cùng một kết quả hash là cực kỳ nhỏ

3. Danh sách các hàm băm mật mã học

Thuật toán	Kích thước đầu ra	Kích thước trạng thái trong	Kích thước khối	Độ dài	Kích thước world	Xung đột
HAVAL	256/224/192/160/128	256	1024	64	32	Có
MD2	128	384	128	Không	8	khả năng lớn

MD4	128	128	512	64	32	Có
MD5	128	128	512	64	32	Có
PANAMA	256	8736	256	No	32	Có lỗi
RIPEMD	128	128	512	64	32	Có
RIPEMD-128/256	128/256	128/256	512	64	32	Không
RIPEMD-160/320	160/320	160/320	512	64	32	Không
SHA-0	160	160	512	64	32	Không
SHA-1	160	160	512	64	32	Có lỗi
SHA-256/224	256/224	256	512	64	32	Không
SHA-512/384	512/384	512	1024	128	64	Không
Tiger(2)-192/160/128	192/160/128	192	512	64	64	Không
VEST-4/8 (hash mode)	160/256	256/384	8	80/128	1	Không
VEST-16/32 (hash mode)	320/512	512/768	8	160/256	1	Không
WHIRLPOOL	512	512	512	256	8	Không

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

4. Ứng dụng của hàm băm Hash

- **Xác thực mật khẩu**

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

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

  Giá trị đầu vào(tin nhắn, dữ liệu...) bị thay đổi tương ứng giá trị băm cũng bị thay đổi. Do vậy nếu 1 kẻ tấn công phá hoại, chỉnh sửa dữ liệu thì server có thể biết ngay lập tức.

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

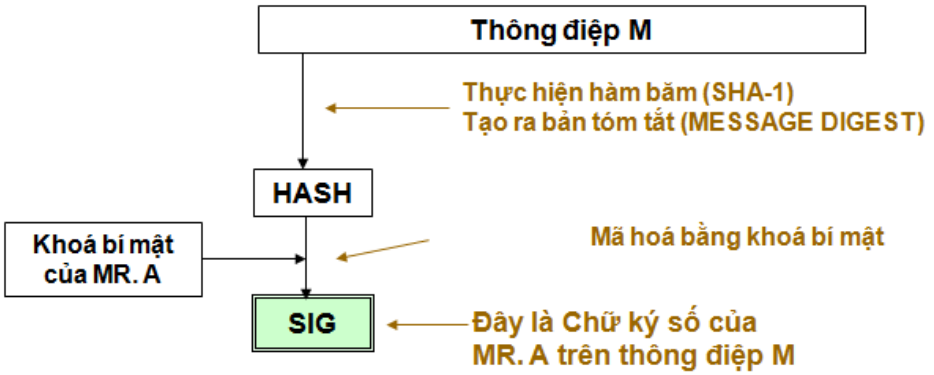
  Hàm băm mật mã có tính chất là hàm 1 chiều. Từ khối dữ liệu hay giá trị đầu vào chỉ có thể đưa ra 1 giá trị băm duy nhất. Như chúng ta đã biết đối với tính chất của hàm 1 chiều. Một người nào đó dù bắt được giá trị băm họ cũng không thể suy ngược lại giá trị, đoạn tin nhắn băm khởi điểm.

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

Hàm băm thường được dùng trong bảng băm nhằm giảm chi phí tính toán khi tìm một khối dữ liệu trong một tập hợp. Giá trị băm đóng vai trò gần như một khóa để phân biệt các khối dữ liệu.

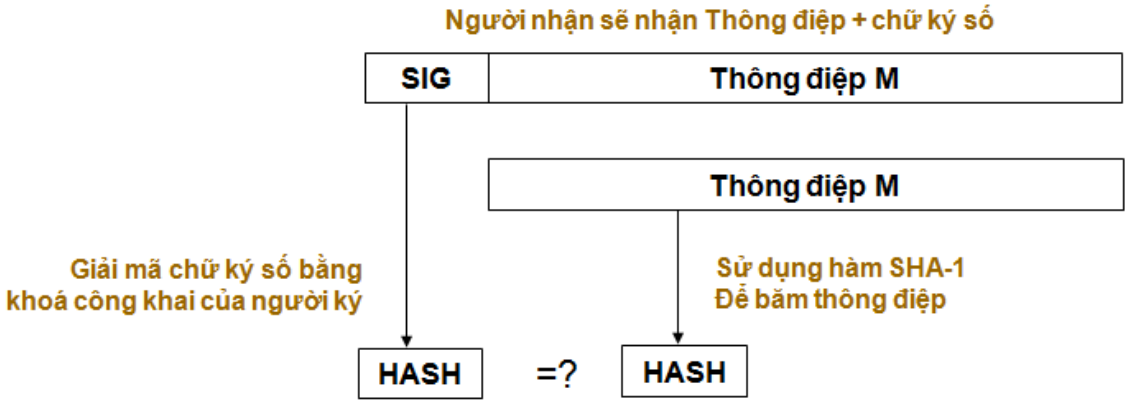
- **Tạo chữ ký điện tử (Digital signatures)**

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



Hình 5: Mã hoá thông điệp bằng khoá bí mật của người ký

Chứng thực bằng chữ ký số



Hình 6: Chứng thực chữ ký số

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

Tại sao?

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

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

➢ **Viết chương trình đề mô với ngôn ngữ JavaScript**

2.5.2 Nguyễn Khắc Hùng – Thuật toán hàm băm SHA-1

1. Giới thiệu hàm băm SHA-1

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

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

2. Thuật toán SHA-1

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

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

Giải thuật gồm 5 bước trên khối 512 bits

Bước 1: Nhồi dữ liệu

- Thông điệp được nhồi thêm các bit sao cho độ dài L mod 512 luôn đồng dư là 448.
- Thông điệp luôn luôn được nhồi thêm các bit.
- Số bit nhồi thêm phải nằm trong khoảng 1-512.

- Phần thêm vào cuối dữ liệu gồm 1 bit 1 và theo sau là các bit 0.

***Bước 2: Thêm độ dài**:*

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

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

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

=67452301

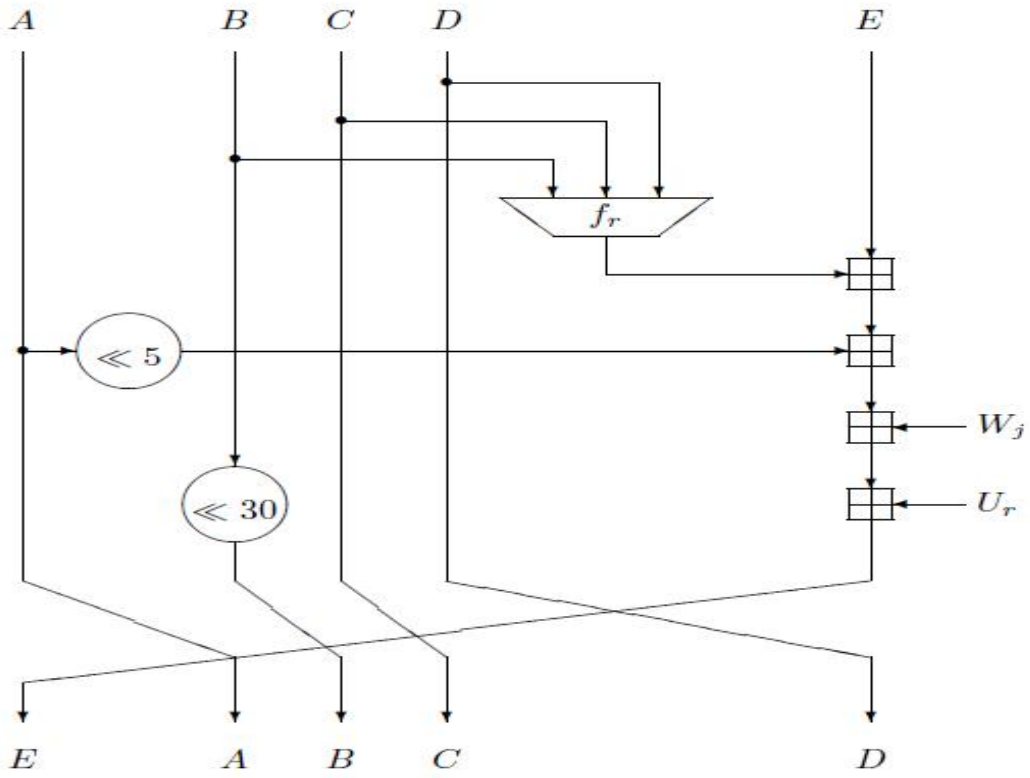
=EFCDAB89

= 98BADCFE

= 10325476

= C3D2E1F0

Bước 4: Xử lý các khối dữ liệu 512 bit



Hình 7: Sơ đồ thuật toán SHA-1

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

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

- Mỗi vòng có đầu vào gồm khối 512-bit hiện thời và một bộ điệm 160 bit A, C, B, D, E. Các thao tác sẽ cập nhật giá trị bộ đệm.
- Chia khối dữ liệu đã nhồi thêm (cuối bước 2) thành 16 nhóm (mỗi nhóm gồm 32 bit) và đặt theo thứ tự là: ,,....

- Mở rộng từ 16 nhóm 32 bit lên đến 80 nhóm 32 bit bằng vòng lặp
- For 16 to 79 let
- = (XOR XOR XOR)
- Gán A=, B=, C=, D=, E=.
- Mỗi vòng lặp sử dụng theo công thức chung với 1 hằng số = (0≤ t ≤ 79) như sau:

  For t= 0 to 79 do

  TEMP= (A)+(B,C,D)+ E + +

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

  Với:

  = 5A827999 (0≤ t ≤ 19)

  = 6ED9EBA1(20≤ t ≤ 39)

  = 8F1BBCDC(40≤ t ≤ 59)

  = CA62C1D6(60≤ t ≤ 79) .
- Đầu ra của 4 vòng (bước 80) được cộng với giá trị của bộ đệm để tạo ra 1 chuỗi kết quả dài 160 bit.

  = + A

  = + E

Bước 5: Xuất kết quả

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

  H=

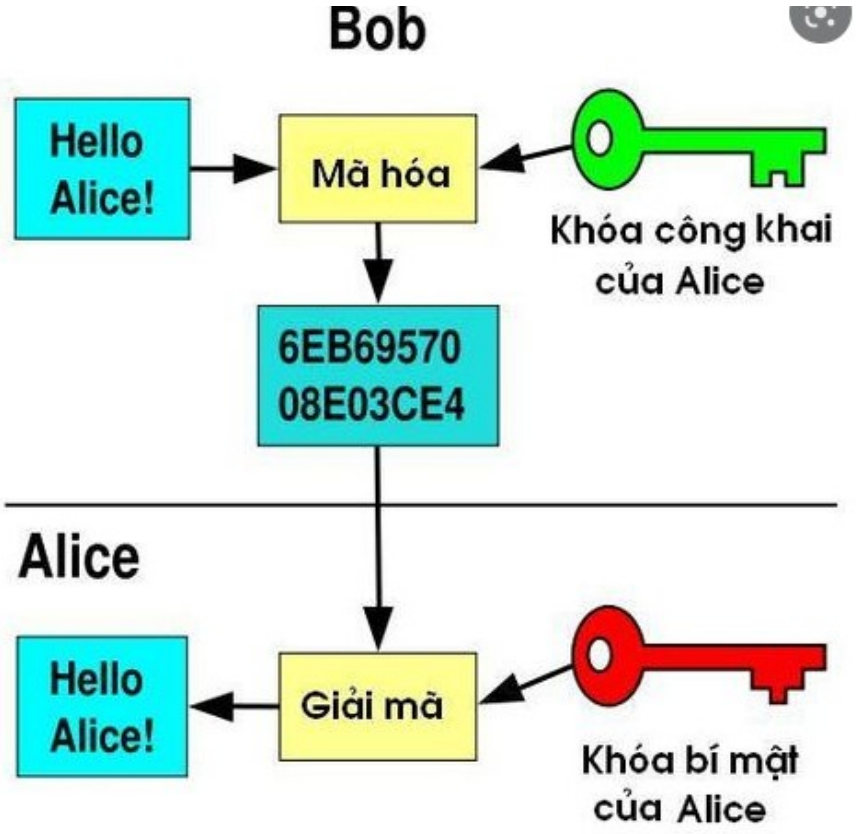
Chương 3. Phần kiến thức lĩnh hội và bài học kinh nghiệm

3.1 Nội dung đã thực hiện

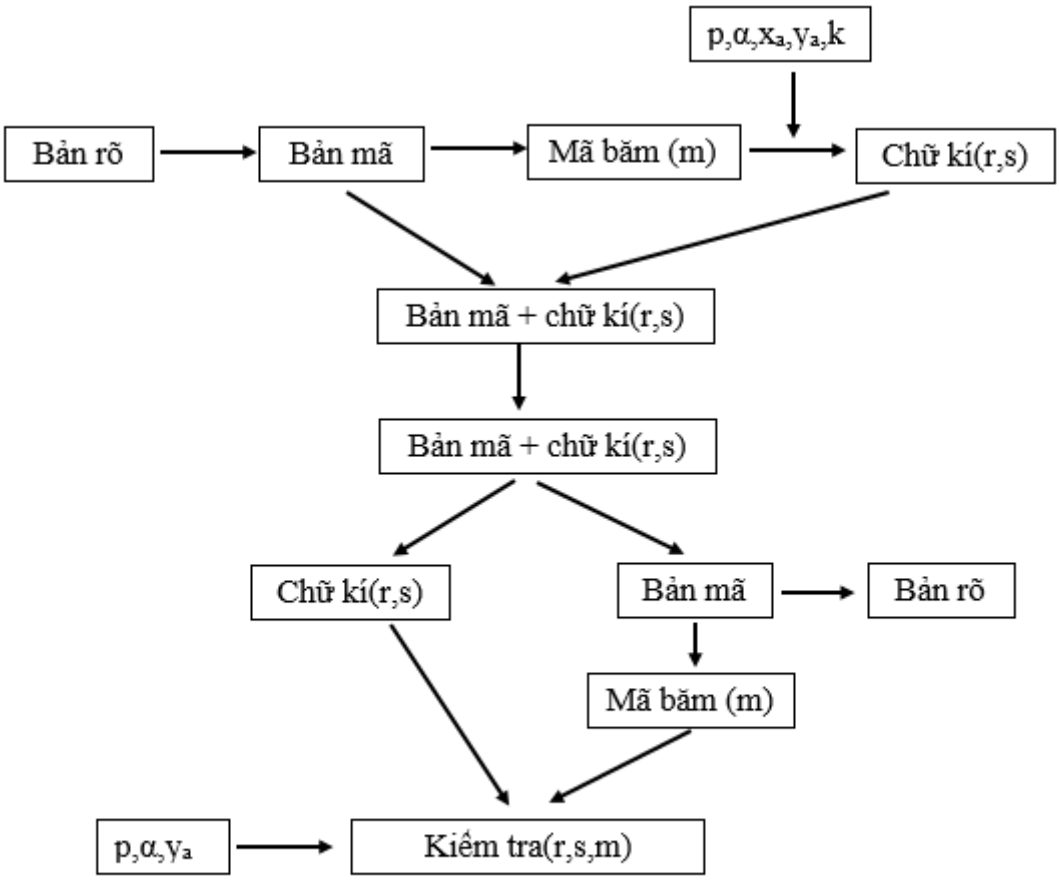
*Qua bài học nhóm chúng em đã lĩnh hội được rất nhiều kiến thức về môn học và những kiến thức bảo hàm trung quanh môn học. Đó là nhưng kiến thức lý thuyết, giải bài tập, ngoài các kỹ năng lập trình ,suy nghĩ logic cũng được cải thiện thêm rất là nhiều.

*Và một số kiến thức, kỹ năng nhóm em đã lĩnh hội được là :

- Kiến thức
  - Phương pháp mã hóa ELGamal

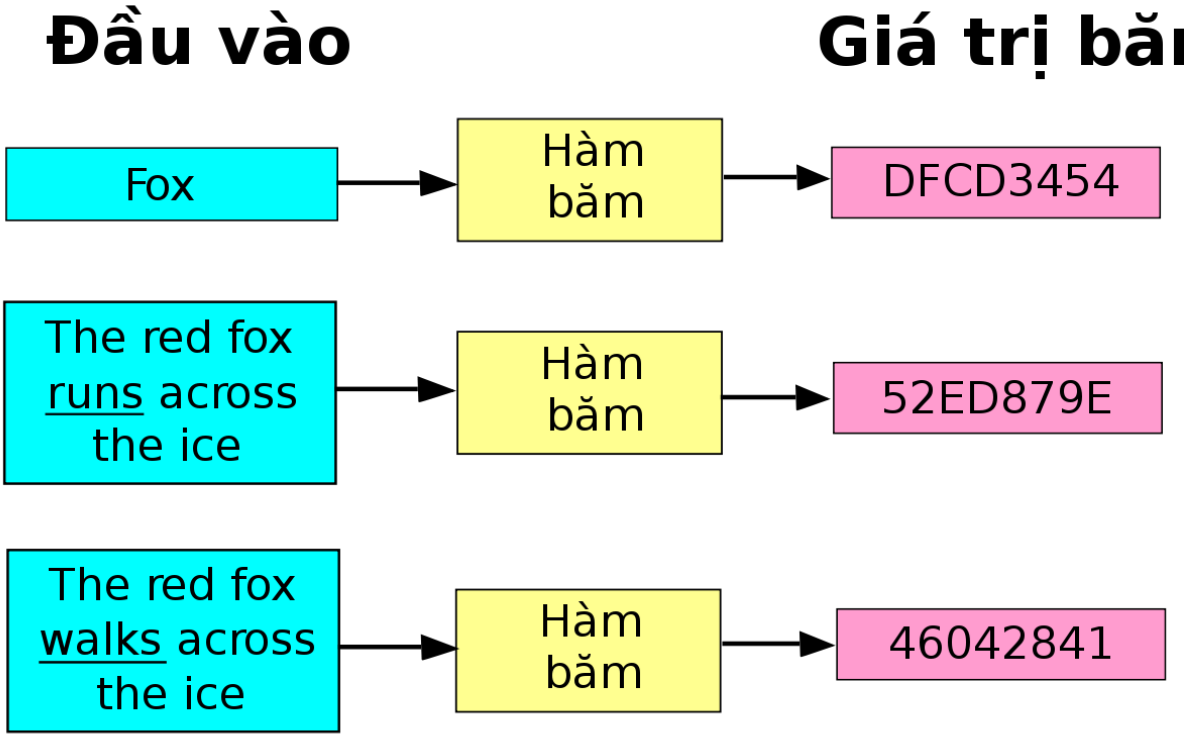


  - Chữ ký ElGamal :



Sơ đồ chữ kí số Elgamal

- Hàm băm :



- Bình phương và nhân

Ví dụ [sửa | sửa mã nguồn]

Trong ví dụ sau ta tính $37^{27} \pmod{101}$.

Đổi $n = 27$ ra số nhị phân ta được $27 = 11011_{(2)}$.

Bảng sau đây tính toán từng bước theo giá trị của các bít của 27.

Khởi tạo $p = 1$.

$b[i]$	$p = p^2$	$p = p \pmod{101}$	$p * x$	$p = \pmod{101}$
1	$1^2 = 1$	1	$1 * 37 = 37$	37
1	$37^2 = 1369$	56	$56 * 37 = 2072$	52
0	$52^2 = 2704$	78	-	78
1	$78^2 = 6084$	24	$24 * 37 = 888$	80
1	$80^2 = 6400$	37	$37 * 37 = 1369$	56

Như vậy ta có

$$37^{27} \pmod{101} = 56$$

- **Định lý Thặng dư trung Hoa.**

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ .. \\ x \equiv a_k \pmod{m_k} \end{cases}$$

trong đó $m_1, m_2, \ldots, m_k$ đôi một nguyên tố cùng nhau.

Định lý

Hệ phương trình đồng dư nói trên có nghiệm duy nhất theo modun

$$M = m_1 . m_2 \ldots m_k$$

là

$$x \equiv a_1 . M_1 . y_1 + a_2 . M_2 . y_2 + \ldots + a_k . M_k . y_k \pmod{M}$$

trong đó

$$M_1 = M/m_1, M_2 = M/m_2, \ldots, M_k = M/m_k$$
$$y_1 = (M_1)^{-1} \pmod{m_1}, y_2 = (M_2)^{-1} \pmod{m_2}, \ldots, y_k = (M_k)^{-1} \pmod{m_k}$$

Trong đó

$(M_1)^{-1} \pmod{m_1}$ *là nghịch đảo theo modulo của* m_1

với

$y_1 = (M_1)^{-1} \pmod{m_1} \Leftrightarrow y_1 M_1 = 1 \pmod{m_1}$

- Bảng Ascii,UTF-8,Unicode

Dec	Hex	Oct	Chr	Dec	Hex	Oct	HTML	Chr	Dec	Hex	Oct	HTML	Chr	Dec	Hex	Oct	HTML	Chr
0	0	000	NULL	32	20	040	&#032;	Space	64	40	100	&#064;	@	96	60	140	&#096;	`
1	1	001	Start of Header	33	21	041	&#033;	!	65	41	101	&#065;	A	97	61	141	&#097;	a
2	2	002	Start of Text	34	22	042	&#034;	"	66	42	102	&#066;	B	98	62	142	&#098;	b
3	3	003	End of Text	35	23	043	&#035;	#	67	43	103	&#067;	C	99	63	143	&#099;	c
4	4	004	End of Transmission	36	24	044	&#036;	$	68	44	104	&#068;	D	100	64	144	&#100;	d
5	5	005	Enquiry	37	25	045	&#037;	%	69	45	105	&#069;	E	101	65	145	&#101;	e
6	6	006	Acknowledgment	38	26	046	&#038;	&	70	46	106	&#070;	F	102	66	146	&#102;	f
7	7	007	Bell	39	27	047	&#039;	'	71	47	107	&#071;	G	103	67	147	&#103;	g
8	8	010	Backspace	40	28	050	&#040;	(	72	48	110	&#072;	H	104	68	150	&#104;	h
9	9	011	Horizontal Tab	41	29	051	&#041;	)	73	49	111	&#073;	I	105	69	151	&#105;	i
10	A	012	Line feed	42	2A	052	&#042;	*	74	4A	112	&#074;	J	106	6A	152	&#106;	j
11	B	013	Vertical Tab	43	2B	053	&#043;	+	75	4B	113	&#075;	K	107	6B	153	&#107;	k
12	C	014	Form feed	44	2C	054	&#044;	,	76	4C	114	&#076;	L	108	6C	154	&#108;	l
13	D	015	Carriage return	45	2D	055	&#045;	-	77	4D	115	&#077;	M	109	6D	155	&#109;	m
14	E	016	Shift Out	46	2E	056	&#046;	.	78	4E	116	&#078;	N	110	6E	156	&#110;	n
15	F	017	Shift In	47	2F	057	&#047;	/	79	4F	117	&#079;	O	111	6F	157	&#111;	o
16	10	020	Data Link Escape	48	30	060	&#048;	0	80	50	120	&#080;	P	112	70	160	&#112;	p
17	11	021	Device Control 1	49	31	061	&#049;	1	81	51	121	&#081;	Q	113	71	161	&#113;	q
18	12	022	Device Control 2	50	32	062	&#050;	2	82	52	122	&#082;	R	114	72	162	&#114;	r
19	13	023	Device Control 3	51	33	063	&#051;	3	83	53	123	&#083;	S	115	73	163	&#115;	s
20	14	024	Device Control 4	52	34	064	&#052;	4	84	54	124	&#084;	T	116	74	164	&#116;	t
21	15	025	Negative Ack.	53	35	065	&#053;	5	85	55	125	&#085;	U	117	75	165	&#117;	u
22	16	026	Synchronous idle	54	36	066	&#054;	6	86	56	126	&#086;	V	118	76	166	&#118;	v
23	17	027	End of Trans. Block	55	37	067	&#055;	7	87	57	127	&#087;	W	119	77	167	&#119;	w
24	18	030	Cancel	56	38	070	&#056;	8	88	58	130	&#088;	X	120	78	170	&#120;	x
25	19	031	End of Medium	57	39	071	&#057;	9	89	59	131	&#089;	Y	121	79	171	&#121;	y
26	1A	032	Substitute	58	3A	072	&#058;	:	90	5A	132	&#090;	Z	122	7A	172	&#122;	z
27	1B	033	Escape	59	3B	073	&#059;	;	91	5B	133	&#091;	[	123	7B	173	&#123;	{
28	1C	034	File Separator	60	3C	074	&#060;	<	92	5C	134	&#092;	\	124	7C	174	&#124;	|
29	1D	035	Group Separator	61	3D	075	&#061;	=	93	5D	135	&#093;	]	125	7D	175	&#125;	}
30	1E	036	Record Separator	62	3E	076	&#062;	>	94	5E	136	&#094;	^	126	7E	176	&#126;	~
31	1F	037	Unit Separator	63	3F	077	&#063;	?	95	5F	137	&#095;	_	127	7F	177	&#127;	Del

asciichars.com

- Kỹ năng mềm:
    - Kỹ năng giao tiếp :Ngoài những kiến thức, kinh nghiệm mà bạn đã học thì kỹ năng giao tiếp là một trong những kỹ năng quan trọng nhất để bạn dẫn đến thành công. Giao tiếp là một phương tiện cầu nối để bạn có thể giao lưu với mọi người, bạn có thể thuyết phục mọi người chấp nhận ý kiến của bạn và bạn có thể bày tỏ được nhu cầu của bạn.
    - Ký năng thuyết trình đám đông : Muốn thành công trong sự nghiệp thì bạn cần phải có kỹ năng thuyết trình để mọi người có thể chấp nhận ý kiến của bạn, chấp nhận hướng giải quyết vấn đề đúng đắn của bạn. Bạn có thể tạo dựng cho mình một thương hiệu cá nhân trong mắt người khác thông qua việc thuyết trình.
    - Kỹ năng làm việc nhóm :có thể hiểu 1 cách đơn giản là nhiều người cùng nhau kết hợp các ưu điểm của mình để thực tốt một nhiệm vụ hướng tới một mục tiêu chung. Cách làm việc này sẽ giúp các cá nhân bổ sung những thiếu sót cho nhau và hoàn thiện bản thân mình. Để công việc của nhóm đạt kết quả cao nhất, các thành viên phải có kỹ năng làm việc nhóm thuần thục. Ngoài ra, làm việc nhóm (sức mạnh của teamwork) giúp cho mỗi cá nhân đề cao tinh thần tập thể, nâng cao hiệu quả công việc và sự gắn bó.
    - Kỹ năng lãnh đạo :là một kỹ năng vô cùng quan trọng. Bạn phải lãnh đạo làm sao mà nhân viên phải kính trọng và nghe theo lời bạn. Muốn trở

thành một nhà lãnh đạo tài ba thì bạn phải là một người tài giỏi, có tầm nhìn xa trông rộng, dự đoán và đưa ra quyết định đúng đắn. Bạn phải phát hiện ra khả năng của nhân viên mình và phát huy hết tài năng của nhân viên đó. Để lãnh đạo giỏi không còn cách nào khác là bạn phải kiên trì học tập và rèn luyện.

- Kỹ năng lãnh đạo là việc dùng năng lực của mình định hướng, tạo ảnh hưởng và thúc đẩy mọi người hành động và nhanh chóng đạt được mục tiêu công việc. Người có kỹ năng lãnh đạo giỏi là người có tầm nhìn, có khả năng chiến lược và biết quản lý những nhân viên của mình để đạt được những thành công chung.
- Kỹ năng giải quyết vấn đề : Trong công việc, có rất nhiều vấn đề xảy ra một cách đột ngột mà bạn không thể biết trước được. Để giải quyết vấn đề một cách ổn thỏa bạn phải phân tích, xem xét thật kĩ. Bạn phải tìm ra nguyên nhân của vấn đề và từng bước một giải quyết chúng. Nếu thành thạo kỹ năng này thì bạn không còn phải lo lắng mỗi khi có vấn đề gì xảy ra bất ngờ nữa. Kỹ năng này giúp cho công việc của bạn tiến triển nhanh hơn
- Kỹ năng làm chủ cảm xúc: Khi bạn không quản lý cảm xúc của bạn một cách có nhận thức, não bộ của bạn sẽ “chạy tự động” và chuyển bạn vào các cảm xúc khác nhau. Tệ hơn nữa, sau một thời gian lặp đi lặp lại, nhiều cảm xúc trở thành thói quen cố hữu của bạn. Việc này giải thích tại sao

nhiều người vẫn cảm thấy buồn ngủ và không tỉnh táo cho dù đã ngủ được bảy tám giờ trước đó. Hoặc có những người khi bước vào công ty, nhìn thấy núi việc chồng chất là cảm thấy nản chí và chỉ muốn bỏ việc ngay lập tức.

- Kỹ năng sáng tạo và lối suy nghĩ thông minh được đánh giá cao ở bất cứ công việc nào. Bạn phải rèn luyện cho mình sự tập trung quan sát ở bất cứ đâu và bất cứ khi nào.

- Kỹ năng lập trình :
  Các thành viên trong nhóm thành thạo các ngôn ngữ lập trình ,C++,Java,JS,Python và giao diện của từng ngôn ngữ.

*Những bài học kinh nghiệm được rút ra sau khi kết thúc bài tập lớn

- Một số bài học sương máu khi kết thúc bài tập lớn đó là:
- Không bỏ cuộc .Ví dụ khi ta gặp một bài tập khó , chúng ta chưa thể làm được, chúng ta vẫn sẽ đi tìm hiểu qua từng giờ, từng ngày. Không bỏ cuộc giữa chừng.
- Lập kế hoạt trước khi làm bất cứ một nhiệm vụ nào: Việc lập kế hoạt trước thực sự có hiệu quả hầu như trong mọi trường hợp. Ví dụ: Khi bạn muốn hoạt động nhóm, nếu ta không nên lịch trước cho mọi người thì ta sẽ không thể kiểm soát được thời gian nào phù hợp cho mỗi người.

- Vấp gã ở đâu, đứng dậy ở đó: Trong khi làm bài tập lớn nói riêng và công việc quá khữ, tương lai nói chung sẽ có những sự thất bại nhất định, nhưng khó khăn ngay trước mắt ta vẫn phải bước tiếp, thực hiện tiếp công việc còn dang dở.

3.2 Hướng phát triển.

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

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

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

xếp hàng và ngồi đợi vài tiếng đồng hồ, có khi đến cả ngày để nộp tờ khai này.

Trong quá trình nghiên cứu để đạt được kết quả là tốt sẽ gặp rất nhiều quá khăn khi sử dụng chữ ký số cần phải cân nhắc trong việc lựa chọn đơn vị cung cấp đáng tin cậy. Nguồn nhân lực tạm ổn định vốn kiến thức, cơ cấu quản lý nhân vẫn còn đang trong quá trình phát triển, hoạt động nhóm giữa các thành viên chủ yếu là trực tuyến bởi quãng đường giữa các thành viên là xa.
Nhưng nhóm, tổ chức cũng có những thế mạnh riêng là: Mọi người trong tổ chức hoạt động với nhau một các tích cực, các thành viên có thái độ cầu tiến. trang thiết bị đầy đủ.

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

TÀI LIỆU THAM KHẢO

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

[2] https://en.wikipedia.org/wiki/ElGamal_signature_scheme

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