# **Tổng quan**

## **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.

## **Lý do chọn đề tài**

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

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

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

## **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

## **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

* 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 JavaScript : Sublime text/Visual studio code

## **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