TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI

KHOA CÔNG NGHỆ THÔNG TIN

------\*\*\*-------



**BÁO CÁO THỰC NGHIỆM**

Học phần: An toàn & Bảo mật thông tin

**Chủ đề**: **Tìm hiểu về hệ chữ ký DSA và viết ứng dụng minh họa (Sử dụng ngôn ngữ C++, C#)**

.

Giáo viên hướng dẫn : TS. Phạm Văn Hiệp

Nhóm sinh viên thực hiện :

1. Nguyễn Lương Chiến Mã SV: 2021601975

2. Dương Văn Chung Mã SV: 2022600137

3. Nguyễn Xuân Sơn Mã SV:

4. Nguyễn Minh Quang Mã SV: 2021603794

5. Lê Trung Hiếu Mã SV:

Mã Lớp học phần:  20241IT6001002

Nhóm: 13

Hà Nội - Năm 2024

DANH MỤC CÁC TỪ VIẾT TẮT

|  |  |  |
| --- | --- | --- |
| **STT** | **TỪ VIẾT TẮT** | **NỘI DUNG** |
| 1 | ECC | Elliptic Curve Cryptography |
| 2 | DSA | Digital Signature Algorithm |
| 3 | P | Plaintext |
| 4 | C | Ciphertext |
| 5 | K | Key |
| 6 | E | Encryption |
| 7 | D | Decryption |

# LỜI CẢM ƠN

Để bài tập lớn kết thúc môn học được thực hiện thành công, em xin cảm ơn giảng viên hướng dẫn TS. Phạm Văn Hiệp, Khoa Công nghệ thông tin, Trường đại học Công nghiệp Hà Nội đã chia sẻ những kiến thức quý báu, hướng dẫn tận tình và có những góp ý trong suốt quá trình thực hiện đề tài để chúng em có thể hoàn thành tiểu luận một cách tốt nhất.

Sau khi nghiên cứu đề tài và kết thúc khóa học, chúng em đã học hỏi và tích lũy được kiến thức và kinh nghiệm từ thầy đi trước để hoàn thiện và phát triển bản thân. Bên cạnh đó, đây cũng là cơ hội giúp chúng em nhận ra mình cần hoàn thiện thêm những gì để chuẩn bị cho một hành trình dài phía trước.

Do kiến thức của bản thân còn hạn chế và thiếu kinh nghiệm thực tiễn nên nội dung bài nghiên cứu khó tránh những thiếu sót. Chúng em rất mong nhận được ý kiến đóng góp của thầy, cô giáo và những người quan tâm đến đề tài này để đề tài này của chúng em được hoàn thiện hơn nữa.

Chúng em xin chân thành cảm ơn!

Nhóm sinh viên thực hiện

Nhóm 13

# LỜI NÓI ĐẦU

Trước đây khi công nghệ máy tính chưa phát triển, khi nói đến vấn đề an toàn bảo mật thông tin, chúng ta thường hay nghĩ đến các biện pháp nhằm đảm bảo cho thông tin được trao đổi hay cất giữ một cách an toàn và bí mật, chẳng hạn là các biện pháp như: Đóng dấu và ký niêm phong một bức thư để biết rằng lá thư có được chuyển nguyên vẹn đến người nhận hay không, dùng mật mã mã hóa thông điệp để chỉ có người gửi và người nhận hiểu được thông điệp, lưu giữ tài liệu trong các két sắt có khóa tại nơi được bảo vệ nghiêm ngặt.

Ngày nay với sự phát triển của khoa học công nghệ, đặt biệt là sự phát triển của Internet, việc sử dụng máy tính và điện thoại cá nhân càng trở lên rộng rãi, dẫn đến càng nhiều thông tin được lưu trữ trên máy tính và gửi đi trên mạng Internet. Do đó nhu cầu về an toàn và bảo mật thông tin trên máy tính càng nhiều và việc sử dụng mật mã mã hóa càng được phổ biến. Trong báo cáo này, nhóm em tìm hiểu về hệ chữ ký DSA và viết ứng dụng minh họa. Báo cáo này gồm 3 chương:

Chương 1 : Tổng quan.

Chương 2 : Kết quả nghiên cứu.

Chương 3 : Kết luận và bài học kinh nghiệm.

Trong quá trình thực hiện đề tài nhóm chúng em xin gửi lời cám ơn tới thầy Phạm Văn Hiệp giảng viên hướng dẫn nhóm chúng em thực hiện đề tài này. Trong quá trình nghiên cứu và thực hiện đề tài được sự chỉ bảo tận tình của các thầy cô, nhóm chúng em đã cố gắn hết sức để hoàn thiện đề tài. Tuy nhiên chúng em rất mong nhận được sự góp ý của thầy cô và các bạn.

# CHƯƠNG 1: TỔNG QUAN

## Tổng quan về An toàn bảo mật thông tin

An toàn thông tin là bảo vệ các đặc tính riêng tư (confidentiality), toàn vẹn (integrity) và khả dụng (availability) của thông tin.

* C: (Confidentiality) bảo vệ tính riêng tư của dữ liệu thông qua các cơ chế chứng thực và mã hóa, ngăn ngừa những người không hợp lệ sẽ không được đọc những thông tin. Giống như các bì thư khi phát lương thưởng được dán chữ Confidential, chúng ta có thể hình dung trong môi trường công nghệ thông tin là một người chưa đăng nhập vào Domain sẽ không được truy cập những dữ liệu chỉ chia sẻ cho các Domain User.
* I: (Integrity) bảo vệ tính toàn vẹn của dữ liệu thông qua các thuật toán RSA, SHA, MD5 ... ngăn ngừa attacker thay đổi các thông tin nhạy cảm trong quá trình truyền.
* A: (Available) bảo đảm dữ liệu luôn ở trong trạng thái sẵn sàng đáp ứng nhu cầu của người dùng.
* Non-Repudiation: Tính không thể chối bỏ, nghĩa là dữ liệu người nào gửi đi thì họ phải có trách nhiệm với các thông tin của mình thông qua các xác nhận nguồn gốc như chữ ký điện tử.

Để đảm bảo việc truyền tin an toàn và kiểm tra tính toàn vẹn của thông tin, người ta thường mã hóa thông tin trước khi truyền đi bằng các một số các hệ mật như DSA, DES, Triple, DES (3DES), RC4, AES, RSA, Rabin, Diffie-Hellman,

Elgamal,...

Qua dự án lần này nhóm sinh viên chúng em đã đi sâu tìm hiểu về xây dựng và phát triển mã hóa giải mã DSA , nắm được những kiến thức cơ bản

Trong phương pháp mã hóa và giải mã cũng như là các thuật toán cần thiết bằng các ngôn ngữ như: C#, C++..

## 1.2 Các kiến thức cơ sở

### 1.2.1 Kiến thức cơ sở về Toán học

* **Số học modulo**: Hiểu về phép toán modulo, đặc biệt là trong ngữ cảnh số nguyên lớn.
* **Lý thuyết nhóm**: Nắm vững các khái niệm cơ bản như nhóm, vành, trường, nhóm cyclic, và nhóm con.
* **Số nguyên tố và phân tích số nguyên tố**: Hiểu về các thuật toán kiểm tra tính nguyên tố và phân tích số nguyên lớn.
* **Hàm số hash**: Kiến thức về hàm băm mật mã như SHA-1, SHA-256, và cách chúng hoạt động.

### 1.2.2 Kiến thức về Thuật toán

* **Thuật toán số học**: Các thuật toán tính toán với số nguyên lớn như phép nhân, phép chia, và phép lũy thừa modulo.
* **Thuật toán Euclid mở rộng**: Dùng để tìm nghịch đảo modulo.
* **Thuật toán tạo số nguyên tố**: Hiểu cách tạo ra các số nguyên tố lớn cần thiết cho DSA.
* **Thuật toán số học hình elip (Elliptic Curve Cryptography - ECC)**: Mặc dù DSA không sử dụng ECC, kiến thức này cũng rất hữu ích trong mật mã học.

### 1.2.3. Ngôn ngữ lập trình

* **C#**
* **Cấu trúc dữ liệu**: Hiểu các cấu trúc dữ liệu cơ bản trong C# (Array, List, Map).
* **Quản lý ngoại lệ**: Biết cách xử lý ngoại lệ khi làm việc với các thao tác mã hóa.
* **C++**
* **Thư viện mã hóa C++**: Sử dụng thư viện như OpenSSL để thực hiện các chức năng mã hóa và chữ ký số.
* **Con trỏ và quản lý bộ nhớ**: Hiểu cách quản lý bộ nhớ động trong C++.
* **Xử lý lỗi**: Biết cách xử lý lỗi và ngoại lệ, đặc biệt trong ngữ cảnh mã hóa.

## 1.3 Nội dung nghiên cứu

### 1.3.1 Lý do nghiên cứu

* Phải che giấu được nội dung của văn bản rõ (plaintext)
* Tạo các yếu tố xác thực thông tin, đảm bảo thông tin lưu hành trong hệ thống đến người nhận hợp pháp là xác thực
* Tổ chức các sơ đồ chữ ký điện tử, đảm bảo k có hiện tượng giả mạo, mạo danh để gửi thông tin lên mạng

### 1.3.2 Khái niệm cơ bản

* Bản rõ X: được gọi là bản tin gốc, bản rõ có thể được chia nhỏ có kích thước phù hợp.
* Bản mã Y: là bản tin gốc đã được mã hoá.
* Mã: là thuật toán mã hoá chuyển bản rõ thành bản mã, thông thường chúng ta cần thuật toán mã hoá mạnh, cho dù kẻ thù biết được thuật toán, nhưng không biết thông tin về khoá thì cũng không tìm được bản rỏ
* Khoá K: là thông tin tham số dùng để mã hoá, chỉ có người gửi và người nhận biết. Khoá là độc lập với bản rõ và có độ dài phù hợp với yêu cầu bảo mật.
* Mã hoá: là quá trình chuyển bản rõ thành bản mã.
* Giải mã: là quá trình chuyển bản mã thành bản rõ, đây là quá trình ngược lại của mã hoá.

### 1.3.3 Các thành phần của hệ mật mã

Một hệ mật mã là một hệ bao gồm 5 thành phần (P, C, K, E, D) thoả mãn:

* P (Plaintext): không gian bản rõ, là tập hợp hữu hạn các bản rõ có thể.
* C (Ciphertext): không gian bản mã, là tập hợp những bản mã có thể.
* K (Key): không gian khoá, là tập hợp các khoá có thể.
* E (Encryption): không gian hàm mã hoá, là tập hợp các quy tắc mã hoá có thể.
* D (Decryption): không gian hàm giải mã, là tập hợp các quy tắc giải mã có thể.

Đối với mỗi k thuộc K có một quy tắc mã hoá ek: P -> C thuộc E và một quy tắc giải mã tương ứng dk: C -> P thuộc D

#### 1.3.4 Giới thiệu về hệ mã DSA.

#### 1.3.4.1 Giới thiệu chung về hệ mã DSA.

Hệ chữ ký số DSA (Digital Signature Algorithm) là một phương pháp chữ ký số được thiết kế để xác minh tính toàn vẹn và nguồn gốc của thông điệp điện tử. DSA được phát triển bởi Cơ quan An toàn Quốc gia của Mỹ (NSA) và được đưa vào sử dụng trong các ứng dụng an ninh và mật mã.

#### 1.3.4.2 Tạo chữ ký và xác minh chữ ký trong DSA.

* **Tạo chữ ký (Signing):** Để tạo chữ ký cho một thông điệp, người ký sử dụng khóa bí mật của mình để tạo ra một chữ ký dựa trên nội dung của thông điệp. Quá trình này bao gồm việc áp dụng một hàm băm để tạo ra một giá trị băm, sau đó sử dụng một phép toán số học để ký kết giá trị băm đó.
* **Xác minh chữ ký (Verification):** Người nhận thông điệp sử dụng khóa công khai của người ký để xác minh tính toàn vẹn của thông điệp và tính hợp pháp của chữ ký. Quá trình này bao gồm việc sử dụng cùng một hàm băm để tạo ra một giá trị băm từ nội dung của thông điệp, sau đó so sánh giá trị băm này với giá trị băm được ký kết trong chữ ký.

#### 1.3.4.3 Ưu điểm và nhược điểm của hệ mã DSA.

* **Ưu điểm**: DSA cung cấp một cơ chế hiệu quả để xác minh tính toàn vẹn và nguồn gốc của thông điệp mà không cần phải chia sẻ khóa bí mật.
* **Nhược điểm**: DSA có thể mất nhiều thời gian để tạo và xác minh chữ ký so với các phương pháp khác như RSA. Đồng thời, việc triển khai DSA cần sự chú ý đến việc chọn các thông số an toàn và đảm bảo tính ngẫu nhiên trong quá trình tạo chữ ký.