**Chương 1: Tổng quan**

**1.1. Tổng quan về an ninh mạng**

An ninh mạng là một lĩnh vực thiết yếu trong việc bảo vệ hệ thống, dữ liệu và thông tin trước các mối đe dọa từ không gian mạng. Trong kỷ nguyên số, nơi thông tin đóng vai trò cốt lõi, an ninh mạng không chỉ đảm bảo tính bảo mật, tính toàn vẹn và tính sẵn sàng của dữ liệu, mà còn là tấm lá chắn bảo vệ uy tín và sự ổn định của các cá nhân, tổ chức và quốc gia.

Các mối đe dọa an ninh mạng ngày càng tinh vi và phức tạp. Phổ biến nhất là các phần mềm độc hại, tấn công từ chối dịch vụ, lừa đảo qua mạng , tấn công mạng xã hội và khai thác lỗ hổng bảo mật. Những hình thức tấn công này có thể gây ra những hậu quả nghiêm trọng, từ đánh cắp dữ liệu cá nhân, làm gián đoạn hoạt động doanh nghiệp, đến tổn thất tài chính và uy tín trên diện rộng.

Để đối phó với những thách thức đó, việc xây dựng một hệ thống phòng thủ mạnh mẽ là điều cần thiết. Các biện pháp công nghệ như triển khai tường lửa, mã hóa dữ liệu và phần mềm chống mã độc kết hợp cùng quy trình bảo mật hiệu quả là những giải pháp then chốt.

Dù vậy, ngành an ninh mạng vẫn phải đối mặt với nhiều thách thức như sự thiếu hụt chuyên gia, sự gia tăng không ngừng của các cuộc tấn công tinh vi và khả năng phát hiện sớm còn hạn chế.

An ninh mạng không chỉ là câu chuyện của công nghệ, mà còn là sự phối hợp giữa quy trình, công cụ và ý thức con người. Một hệ thống mạng an toàn không chỉ bảo vệ dữ liệu mà còn tạo niềm tin, đảm bảo sự phát triển bền vững trong thế giới số hóa hiện nay.

### **1.2. Các cơ sở kiến thức về toán học, thuật toán và ngôn ngữ lập trình**

**1.2.1. Cơ sở toán học**

Chuẩn mã hóa AES (Advanced Encryption Standard) là một thuật toán mã hóa đối xứng, được thiết kế để mã hóa và giải mã dữ liệu một cách an toàn và hiệu quả. AES sử dụng các phép toán toán học cơ bản nhưng rất mạnh mẽ và khó phá vỡ. Các cơ sở toán học quan trọng bao gồm:

* **Trường Galois (Galois Field):** AES hoạt động trong một trường Galois GF(2^8), nghĩa là tất cả các phép toán trong AES đều được thực hiện với các số nguyên có giá trị từ 0 đến 255 (tương đương với 8 bit). Các phép toán cơ bản trong AES như cộng (XOR) và nhân được thực hiện trong trường này.
* **Hàm băm và S-box:** AES sử dụng một bảng thay thế (S-box) để thực hiện phép thay thế byte (SubBytes). Đây là một bảng 16x16 chứa các giá trị hex, được xây dựng dựa trên các hàm băm toán học để tạo ra các giá trị khó dự đoán và không dễ bị tấn công.
* **Phép nhân và phép cộng:** Phép nhân trong AES là phép nhân trong trường Galois GF(2^8), trong đó mỗi phần tử được nhân với một hằng số cố định và kết quả được rút gọn theo modulo x^8 + x^4 + x^3 + x + 1.
* **Đại số tuyến tính:** AES sử dụng các phép toán đại số tuyến tính trong quá trình xử lý dữ liệu. Cụ thể, phép **MixColumns** trong AES sử dụng phép nhân ma trận trên các cột của khối dữ liệu, nhằm tạo ra sự khuếch tán dữ liệu và tăng cường bảo mật.

**1.2.2. Cơ sở thuật toán**

Thuật toán mã hóa AES bao gồm các bước mã hóa và giải mã được mô tả như sau:

* **Mã hóa AES:** AES mã hóa dữ liệu theo các vòng (round) được lặp lại nhiều lần, với số vòng phụ thuộc vào độ dài khóa:
  + **AES-128:** 10 vòng.
  + **AES-192:** 12 vòng.
  + **AES-256:** 14 vòng.
* Các bước trong một vòng bao gồm:
  + **SubBytes:** Mỗi byte trong khối dữ liệu được thay thế bằng giá trị tương ứng từ bảng S-box.
  + **ShiftRows:** Di chuyển các hàng của ma trận khối theo một số bước nhất định để tăng cường tính khuếch tán.
  + **MixColumns:** Thực hiện phép toán ma trận trên các cột để làm tăng sự khuếch tán dữ liệu.
  + **AddRoundKey:** XOR khóa vòng vào dữ liệu.
* **Giải mã AES:** Quá trình giải mã AES là một phiên bản ngược lại của mã hóa. Các bước được thực hiện theo thứ tự ngược lại và sử dụng các phép toán ngược, chẳng hạn như việc đảo ngược S-box và MixColumns.
* **Khóa AES:** Khóa AES được mở rộng từ khóa ban đầu thông qua một quá trình gọi là **key expansion**, trong đó khóa gốc được phân tách thành nhiều khóa con cho mỗi vòng mã hóa.

**1.2.3. Cơ sở về lập trình và ứng dụng trong Java, C#**

Để triển khai chuẩn AES trong mã hóa dữ liệu, các ngôn ngữ lập trình như Java và C# cung cấp các thư viện mã hóa mạnh mẽ cho phép dễ dàng sử dụng AES trong ứng dụng.

* **Java:**
  + Java cung cấp thư viện javax.crypto để hỗ trợ việc mã hóa và giải mã AES. Lớp Cipher trong thư viện này cho phép lập trình viên dễ dàng mã hóa và giải mã dữ liệu bằng AES. Cấu trúc mã hóa cơ bản trong Java như sau:



* Java cũng hỗ trợ nhiều chế độ mã hóa khác nhau của AES, chẳng hạn như ECB (Electronic Codebook) và CBC (Cipher Block Chaining), giúp tăng cường bảo mật tùy theo ứng dụng cụ thể.

**C#:**

* Trong C#, việc sử dụng AES được thực hiện thông qua lớp AesCryptoServiceProvider trong thư viện System.Security.Cryptography. C# cung cấp một cách dễ dàng để mã hóa và giải mã dữ liệu với AES như sau:



* + C# cũng cung cấp các chế độ mã hóa như AES/CBC/PKCS7, với việc sử dụng IV (Initialization Vector) để tăng cường tính bảo mật.

**1.2.4. Ứng dụng trong thực tế**

AES được sử dụng rộng rãi trong việc bảo mật dữ liệu trên các nền tảng khác nhau, từ các giao thức truyền thông bảo mật (như SSL/TLS) đến các ứng dụng mã hóa dữ liệu trên hệ thống máy tính và di động. Các ứng dụng điển hình của AES bao gồm:

* **Bảo mật giao thức mạng:** AES thường được sử dụng để mã hóa thông tin trong các giao thức như HTTPS, VPN, và Wi-fi (WPA2).
* **Mã hóa dữ liệu trên đám mây:** AES giúp bảo vệ dữ liệu nhạy cảm khi lưu trữ và truyền tải trên các nền tảng đám mây.
* **Bảo vệ dữ liệu trên thiết bị di động:** Các ứng dụng di động thường sử dụng AES để mã hóa dữ liệu người dùng như mật khẩu, tin nhắn, và tài liệu quan trọng.

**1.3. Nội dung nghiên cứu**

* **Lý do chọn đề tài**

Trong học phần an ninh mạng, được giảng viên phân công nhiệm vụ tìm hiểu về một phương pháp mã hóa thông tin được sử dụng hiện nay. Và giữa vô vàn những phương pháp mã hóa đó, nhóm 10 chúng em xin phép nghiên cứu về “***Chuẩn AES và ứng dụng trong mã hóa dữ liệu bằng Java và C#***” bởi các lý do sau:

* *Bảo mật thông tin là một lĩnh vực quan trọng*: Trong thời đại số hóa hiện nay, bảo mật thông tin là một lĩnh vực quan trọng và được quan tâm rất nhiều. Việc hiểu và xây dựng được chương trình mã hóa và giải mã AES sẽ giúp bọn em có thêm kiến thức và kỹ năng trong lĩnh vực này.
* *AES là một trong những thuật toán mã hóa phổ biến nhất:* AES là một thuật toán mã hóa khóa công khai được sử dụng rộng rãi trong các ứng dụng bảo mật thông tin. Việc hiểu và xây dựng được chương trình mã hóa và giải mã AES giúp bọn em hiểu rõ hơn về cách hoạt động của thuật toán này.
* *Phát triển kỹ năng lập trình*: Xây dựng chương trình mã hóa và giải mã AES giúp bạn phát triển kỹ năng lập trình của mình. Trong quá trình xây dựng chương trình, chúng em phải tìm hiểu về thuật toán AES, cách thực hiện mã hóa và giải mã, cách xử lý các số nguyên lớn và các thuật toán toán học liên quan.
* *Ứng dụng thực tế:* AES được sử dụng rộng rãi trong các ứng dụng thực tế như bảo mật email, giao dịch trực tuyến, .... Việc hiểu và xây dựng được chương trình mã hóa và giải mã AES khiến chúng em hiểu rõ hơn về cách áp dụng thuật toán này trong các ứng dụng thực tế.

Tóm lại, xây dựng chương trình mã hóa và giải mã AES là một đề tài thú vị và nó mang đến cho chúng em rất nhiều lợi ích cho việc phát triển kỹ năng lập trình và hiểu về bảo mật thông tin.

* **Nội dung nghiên cứu**

Trong báo cáo thực nghiệm “***Chuẩn AES và ứng dụng trong mã hóa dữ liệu bằng Java và C#***”, nhóm 10 chúng em cùng nhau nghiên cứu về các nội dung:

* *Ngôn ngữ lập trình:* Nghiên cứu về một số ngôn ngữ lập trình phổ biến nhằm xây dựng thuật toán và giao diện cho chương trình.
* *Thuật toán AES:* Nghiên cứu cách hoạt động của thuật toán AES, bao gồm các khái niệm như khóa công khai, khóa bí mật, phép toán modulo, phép toán mũ, …
* *Tạo khóa:* Nghiên cứu cách tạo khóa công khai và khóa bí mật trong thuật toán AES. Cần tìm hiểu cách chọn các số nguyên ngẫu nhiên lớn và cách tính toán các tham số khóa.
* *Mã hóa và giải mã:* Tìm hiểu cách thực hiện mã hóa và giải mã trong thuật toán AES. Cần nghiên cứu cách chuyển đổi thông điệp thành số nguyên, cách thực hiện phép toán mũ, và cách chuyển đổi kết quả về lại thông điệp ban đầu.
* *Các tính năng khác:* Nghiên cứu và thực hiện các tính năng khác trong chương trình, bao gồm chức năng tạo khóa tự động, …
* *Kiểm thử và sửa lỗi:* Kiểm thử chương trình và sửa các lỗi phát sinh trong quá trình thực hiện.

Việc nghiên cứu tường tận, rõ ràng các nội dung trên đảm bảo chương trình được xây dựng hoạt động một cách đúng đắn và hiệu quả.