**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**

KHOA CÔNG NGHỆ THÔNG TIN

------🙙🕮🙛-------



**BÁO CÁO THỰC NGHIỆM**

Học phần: An ninh mạng

**Chủ đề**: **CHUẨN AES VÀ ỨNG DỤNG TRONG MÃ HÓA DỮ LIỆU**

.

|  |  |
| --- | --- |
| **Giảng viên hướng dẫn :** | **TS. Phạm Văn Hiệp** |
| **Mã lớp học phần :** |  |
| **Nhóm sinh viên thực hiện:** | Nhóm 10 |
|  | 1. Nguyễn Văn Hậu Giang - 2022604193 |
|  | 2. Khổng Thị Linh - 2022603748 |
|  | 3. Phạm Việt Long - 2022600752 |
|  | 4. Lê Tuấn Minh - 2022605662 |
|  | 5. Tống Đăng Quang - 2022603783 |

**Hà Nội** - **Năm 2024**

**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**

KHOA CÔNG NGHỆ THÔNG TIN

------🙙🕮🙛-------



**BÁO CÁO THỰC NGHIỆM**

Học phần: An ninh mạng

**Chủ đề**: **CHUẨN AES VÀ ỨNG DỤNG TRONG MÃ HÓA DỮ LIỆU**

.

|  |  |
| --- | --- |
| **Giảng viên hướng dẫn :** | **TS. Phạm Văn Hiệp** |
| **Mã lớp học phần :** |  |
| **Nhóm sinh viên thực hiện:** | Nhóm 10 |
|  | 1. Nguyễn Văn Hậu Giang - 2022604193 |
|  | 2. Khổng Thị Linh - 2022603748 |
|  | 3. Phạm Việt Long - 2022600752 |
|  | 4. Lê Tuấn Minh - 2022605662 |
|  | 5. Tống Đăng Quang - 2022603783 |

**Hà Nội** - **Năm 2024**

**LỜI CẢM ƠN**

Lời đầu tiên, nhóm 10 xin được gửi lời cảm ơn chân thành nhất đến thầy Phạm Văn Hiệp – người đã truyền tải nội dung bộ môn An ninh mạng trong kỳ học này cho chúng em. Trong quá trình học tập, thầy không chỉ đơn thuần giúp sinh viên tiếp cận được nội dung môn học, mà còn chia sẻ những kinh nghiệm hết sức quý báu với sinh viên. Hình thức truyền tải nội dung đặc biệt của thầy đã giúp tất cả sinh viên trong lớp ai cũng có cơ hội được đưa ra quan điểm về nội dung bài học. Điều đó đã giúp sinh viên trở nên chủ động hơn trong việc tìm hiểu kiến thức để trình bày trước lớp nội dung bài học đã chuẩn bị, từ đó giúp sinh viên hình thành và biết bảo vệ quan điểm đúng đắn của mình, đồng thời qua những góp ý của cô và các sinh viên khác trong lớp giúp rút ra kinh nghiệm, sửa chữa những quan điểm sai về nội dung bài học. Thầy đã thành công trong việc định hướng sinh viên tự khám phá nội dung bài học, cùng với đó là sinh viên đã có cả một học kỳ được rèn giũa kỹ năng mềm cho bản thân mình.

Trong quá trình thực hiện đề tài “Chuẩn AES và ứng dụng trong mã hóa dữ liệu”, nhóm đã vận dụng kiến thức được học trong những tuần lên lớp tìm hiểu cùng với thầy. Hơn thế nữa, sự tận tình chỉ dẫn của thầy đã giúp nhóm đi đúng hướng ban đầu đề ra và hoàn thành báo cáo thực nghiệm này.

Một lần nữa, chúng em xin chân thành cảm ơn!

Nhóm sinh viên thực hiện

Nhóm 10

MỤC LỤC

[DANH MỤC CÁC TỪ VIẾT TẮT 5](#_Toc183805256)

[DANH MỤC HÌNH ẢNH 6](#_Toc183805257)

[DANH MỤC BẢNG BIỂU 7](#_Toc183805258)

[LỜI NÓI ĐẦU 8](#_Toc183805259)

[CHƯƠNG 1. TỔNG QUAN 9](#_Toc183805260)

[1.1. Tổng quan về an ninh mạng 9](#_Toc183805261)

[1.2. Lý do chọn đề tài 9](#_Toc183805262)

[1.3. Nội dung nghiên cứu 10](#_Toc183805263)

[1.4. Các kiến thức cơ sở 11](#_Toc183805264)

[1.4.1. Cơ sở toán học 11](#_Toc183805265)

[1.4.2. Cơ sở thuật toán 11](#_Toc183805266)

[1.4.3. Cơ sở về ngôn ngữ lập trình Java và C# 12](#_Toc183805267)

[1.5. Ứng dụng trong thực tế 13](#_Toc183805268)

[CHƯƠNG 2. KẾT QUẢ NGHIÊN CỨU 15](#_Toc183805269)

[2.1. Nghiên cứu, tìm hiểu hệ mã hóa bí mật 15](#_Toc183805270)

# DANH MỤC CÁC TỪ VIẾT TẮT

# DANH MỤC HÌNH ẢNH

[Hình 1.1. Ngôn ngữ lập trình Java 12](#_Toc183805245)

[Hình 1.2. Ngôn ngữ lập trình C# 13](#_Toc183805246)

# DANH MỤC BẢNG BIỂU

# LỜI NÓI ĐẦU

Trong thời đại công nghệ bùng nổ, thông tin đã trở thành một trong những tài sản quý giá nhất của con người. Tuy nhiên, sự phát triển nhanh chóng của hệ thống mạng và các nền tảng số cũng kéo theo những nguy cơ mất an toàn thông tin ngày càng phức tạp và khó lường. Việc bảo mật dữ liệu không chỉ là yêu cầu bắt buộc đối với các tổ chức lớn như ngân hàng, cơ quan chính phủ, mà còn là mối quan tâm của mỗi cá nhân khi giao dịch và lưu trữ thông tin trên không gian mạng.

Trong số các phương pháp bảo mật, mã hóa dữ liệu được xem là một giải pháp hiệu quả và đáng tin cậy nhất. Trong đó, chuẩn **Advanced Encryption Standard (AES)** đã chứng minh vai trò vượt trội của mình như một chuẩn mã hóa quốc tế, được sử dụng rộng rãi trong nhiều lĩnh vực nhờ tính bảo mật cao, hiệu năng tốt và khả năng ứng dụng linh hoạt.

Đề tài **"Chuẩn AES và ứng dụng trong mã hóa dữ liệu"** tập trung vào việc xây dựng chương trình mã hóa và giải mã mật mã hóa công khai AES. Đề tài được xây dựng thành ba chương với nội dung chính như sau:

**- Chương 1: Tổng quan về đề tài nghiên cứu**

**- Chương 2: Kết quả nghiên cứu**

**- Chương 3: Kết luận và bài học kinh nghiệm**

Qua quá trình thực hiện đề tài, chúng em đã có cơ hội tìm hiểu sâu về chuẩn mã hóa AES và vai trò của nó trong lĩnh vực bảo mật dữ liệu. Từ việc phân tích chi tiết và cài đặt thuật toán, chúng em hiểu rõ hơn về cách AES đảm bảo tính an toàn và hiệu quả trong việc bảo vệ thông tin. Đề tài không chỉ giúp chúng em nâng cao kiến thức chuyên môn mà còn rèn luyện kỹ năng nghiên cứu và tư duy phản biện, tạo nền tảng cho những nghiên cứu và ứng dụng trong tương lai.

# 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. 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.

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.

## 1.3. Nội dung nghiên cứu

Trong báo cáo này, nhóm chúng em sẽ 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, …

*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.

## 1.4. Các kiến thức cơ sở

### 1.4.1. Cơ sở toán học

Để xây dựng thành công đề tài, nhóm chúng em phải dựa trên nhiều kiến thức về các định lý toán học và thuật toán tiêu biểu dưới đây:

- Định lý Fermat.

- Hàm số Euler.

- Thuật toán Euclid mở rộng.

- Thuật toán lũy thừa.

…

Nhằm triển khai các thuật toán trên và xây dựng giao diện cho chương trình, chúng em đã tìm hiểu và sử dụng ngôn ngữ Java vad C# để lập trình.

Bên cạnh đó, chúng em còn phải nghiên cứu về phương pháp mã hóa AES một cách thành thạo dựa trên những tài liệu trong nước lẫn ngoài nước. Sao cho chương trình xây dựng được có tính sát với thực tiễn nhất.

### 1.4.2. 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.

### 1.4.3. Cơ sở về ngôn ngữ lập trình Java và C#



Hình 1.1. Ngôn ngữ lập trình Java

Java là một ngôn ngữ lập trình hướng đối tượng được phát triển bởi Sun Microsystems vào năm 1995 và hiện thuộc sở hữu của Oracle. Java nổi bật với khả năng đa nền tảng, nhờ vào Java Virtual Machine (JVM), cho phép chương trình viết một lần có thể chạy trên nhiều hệ điều hành khác nhau. Ngoài ra, Java có bộ thư viện phong phú, hỗ trợ phát triển đa dạng các loại ứng dụng, từ ứng dụng web, di động (đặc biệt là Android), đến các hệ thống lớn. Java hỗ trợ nhiều thuật toán mã hóa thông qua thư viện **Java Cryptography Architecture (JCA) và Java Cryptography Extension (JCE).** Những công cụ này cho phép lập trình viên triển khai các phương thức mã hóa đối xứng (AES, DES), mã hóa bất đối xứng (RSA) và hàm băm (SHA, MD5).



Hình 1.2. Ngôn ngữ lập trình C#

C# là ngôn ngữ lập trình hướng đối tượng được phát triển bởi Microsoft vào năm 2000, nằm trong hệ sinh thái .NET. C# có cú pháp gọn gàng, dễ học, và tích hợp chặt chẽ với nền tảng Windows, giúp tối ưu hóa hiệu suất cho các ứng dụng chạy trên hệ điều hành này. C# được ưa chuộng trong phát triển ứng dụng desktop, web (thông qua ASP.NET) và đặc biệt là game với Unity. C# được ưa chuộng trong các ứng dụng và phần mềm bảo mật trên nền tảng Windows nhờ tích hợp tốt với **.NET Framework** và các API mã hóa như **System.Security.Cryptography**. C# hỗ trợ các thuật toán mã hóa mạnh mẽ như AES, RSA và SHA thông qua các lớp mã hóa sẵn có, giúp triển khai dễ dàng các giải pháp bảo mật như mã hóa dữ liệu, xác thực người dùng và bảo vệ thông tin khi truyền qua mạng.

## 1.5. 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.

# CHƯƠNG 2. KẾT QUẢ NGHIÊN CỨU

## 2.1. Nghiên cứu, tìm hiểu hệ mã hóa bí mật