**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**

**KHOA CÔNG NGHỆ THÔNG TIN**

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***



BÁO CÁO THỰC NGHIỆM

HỌC PHẦN: AN NINH MẠNG

Đề tài:

**CHUẨN AES VÀ ỨNG DỤNG TRONG MÃ HÓA DỮ LIỆU**

|  |  |  |  |
| --- | --- | --- | --- |
| GVHD: | TS. Phạm Văn Hiệp | | |
| Lớp: | 20241IT6070001 |  |  |
| Nhóm: | 10 |  |  |
| Sinh viên: | Nguyễn Văn Hậu Giang | - | 2022604193 |
|  | Khổng Thị Linh | - | 2022603748 |
|  | Phạm Việt Long | - | 2022600752 |
|  | Lê Tuấn Minh | - | 2022605662 |
|  | 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 thầy 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!

**MỤC LỤC**

[DANH MỤC HÌNH VẼ 1](#_Toc185791332)

[DANH MỤC BẢNG BIỂU 2](#_Toc185791333)

[LỜI NÓI ĐẦU 3](#_Toc185791334)

[CHƯƠNG 1. TỔNG QUAN 4](#_Toc185791335)

[1.1. Tổng quan về an ninh mạng 4](#_Toc185791336)

[1.1.1. Khái niệm về an ninh mạng 4](#_Toc185791337)

[1.1.2. Mục tiêu của an ninh mạng 4](#_Toc185791338)

[1.1.3. Tầm quan trọng của an ninh mạng 5](#_Toc185791339)

[1.1.4. Các mối đe dọa an ninh mạng 6](#_Toc185791340)

[1.1.5. Các biện pháp bảo vệ an ninh mạng 7](#_Toc185791341)

[1.2. Lý do chọn đề tài 8](#_Toc185791342)

[1.3. Nội dung nghiên cứu 9](#_Toc185791343)

[1.4. Các kiến thức cơ sở 9](#_Toc185791344)

[1.4.1. Cơ sở toán học 9](#_Toc185791345)

[1.4.1.1. Phép XOR 9](#_Toc185791346)

[1.4.1.2. Phép nhân ma trận 10](#_Toc185791347)

[1.4.2. Ngôn ngữ lập trình 11](#_Toc185791348)

[1.4.2.1. Ngôn ngữ Java 11](#_Toc185791349)

[1.4.2.2. Ngôn ngữ C# 12](#_Toc185791350)

[CHƯƠNG 2. KẾT QUẢ NGHIÊN CỨU 14](#_Toc185791351)

[2.1. Nghiên cứu và tìm hiểu về hệ mã hóa khóa bí mật 14](#_Toc185791352)

[2.1.1. Các khái niệm cơ bản 14](#_Toc185791353)

[2.1.2. Các yêu cầu đối với hệ mã hóa khóa bí mật 15](#_Toc185791354)

[2.2. Nghiên cứu và tìm hiểu về chuẩn mã nâng cao AES 16](#_Toc185791355)

[2.2.1. Giới thiệu về AES 16](#_Toc185791356)

[2.2.2. Mã hóa và giải mã AES 17](#_Toc185791357)

[2.2.2.1. Thay thế byte (Substitute bytes) 19](#_Toc185791358)

[2.2.2.2. Dịch dòng (Shift rows) 21](#_Toc185791359)

[2.2.2.3. Trộn cột (Mix columns) 21](#_Toc185791360)

[2.2.2.4. Cộng với khóa (Add round key) 23](#_Toc185791361)

[2.2.2.5. Mở rộng khóa (Key expansion) 24](#_Toc185791362)

[2.2.3. Minh họa quá trình mã hóa và giải mã AES 25](#_Toc185791363)

[2.2.4. Độ an toàn của AES 26](#_Toc185791364)

[2.2.5. Nhận xét về AES 26](#_Toc185791365)

[2.2.5.1. Ưu điểm 26](#_Toc185791366)

[2.2.5.2. Nhược điểm 26](#_Toc185791367)

[2.2.6. Ứng dụng của AES 27](#_Toc185791368)

[2.3. Thiết kế chương trình và cài đặt thuật toán 27](#_Toc185791369)

[2.3.1. Thiết kế kịch bản chương trình 27](#_Toc185791370)

[2.3.2. Cài đặt thuật toán và giao diện chương trình với Java 27](#_Toc185791371)

[2.3.3. Cài đặt thuật toán và giao diện chương trình với C# 27](#_Toc185791372)

[CHƯƠNG 3. KẾT LUẬN VÀ BÀI HỌC KINH NGHIỆM 28](#_Toc185791373)

[3.1. Kiến thức kỹ năng học được trong quá trình thực hiện đề tài 28](#_Toc185791374)

[3.2. Bài học kinh nghiệm 28](#_Toc185791375)

[3.3. Tính khả thi của chủ đề nghiên cứu 28](#_Toc185791376)

[3.3.1. Thuận lợi 28](#_Toc185791377)

[3.3.2. Khó khăn 28](#_Toc185791378)

[TÀI LIỆU THAM KHẢO 29](#_Toc185791379)

[PHỤ LỤC 30](#_Toc185791380)

# DANH MỤC HÌNH VẼ

[Hình 1.1: Tam giác bảo mật CIA 4](#_Toc185779455)

[Hình 1.2: Minh họa tích ma trận AB của hai ma trận A và B 11](#_Toc185779456)

[Hình 2.1: Mô hình của hệ mã hóa khóa bí mật 15](#_Toc185779457)

[Hình 2.2: Sơ đồ tổng quát mã hóa và giải mã AES 17](#_Toc185779458)

[Hình 2.3: Đầu vào, mảng trạng thái và đầu ra 18](#_Toc185779459)

[Hình 2.4: Khóa và mở rộng khóa 18](#_Toc185779460)

[Hình 2.5: Minh họa một vòng mã AES 19](#_Toc185779461)

[Hình 2.6: Hộp S 19](#_Toc185779462)

[Hình 2.7: Hộp S đảo 20](#_Toc185779463)

[Hình 2.8: Minh họa việc tra cứu hộp S 20](#_Toc185779464)

[Hình 2.9: Minh họa phép thay thế byte 20](#_Toc185779465)

[Hình 2.10: Minh họa phép dịch dòng 21](#_Toc185779466)

[Hình 2.11: Ví dụ minh họa phép dịch dòng 21](#_Toc185779467)

[Hình 2.12: Minh họa phép trộn cột 21](#_Toc185779468)

[Hình 2.13: Ví dụ minh họa phép trộn cột 22](#_Toc185779469)

[Hình 2.14: Ví dụ minh họa phép cộng khóa 23](#_Toc185779470)

[Hình 2.15: Minh họa cách xác định khóa của vòng 1 25](#_Toc185779471)

# DANH MỤC BẢNG BIỂU

[Bảng 1.1: Bảng chân lý cho phép XOR 9](#_Toc185779478)

[Bảng 1.2: Ví dụ phép XOR đối với số hệ nhị phân 10](#_Toc185779479)

[Bảng 1.3: Ví dụ phép XOR đối với số hệ 16 10](#_Toc185779480)

[Bảng 2.1: Tham số của AES 17](#_Toc185779481)

[Bảng 2.2: Giá trị của RC[j] 24](#_Toc185779482)

[Bảng 2.3: Xác định khóa cho vòng 9 khi khóa tại vòng 8 25](#_Toc185779483)

# 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, **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 sẽ 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.

# TỔNG QUAN

## Tổng quan về an ninh mạng

### Khái niệm về an ninh mạng

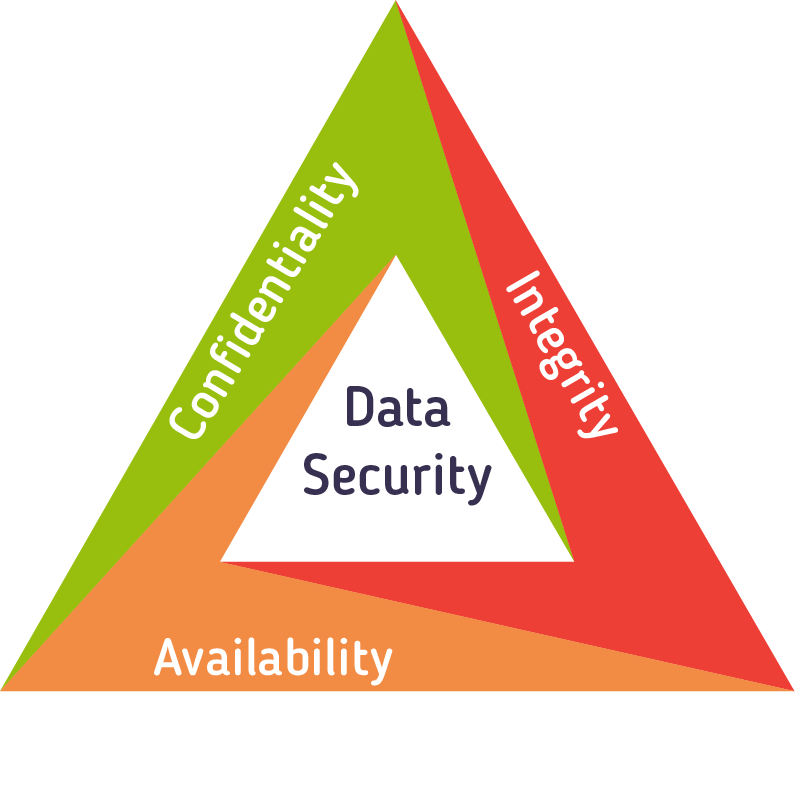
An ninh mạng là tập hợp các biện pháp, công nghệ và quy trình được thiết kế để bảo vệ an toàn cho máy tính, mạng, ứng dụng phần mềm, hệ thống và dữ liệu khỏi các mối đe dọa tiềm ẩn từ không gian mạng.

Trong kỷ nguyên kỹ thuật số hiện nay, an ninh mạng không chỉ là một bộ phận hỗ trợ, mà còn là nền tảng thiết yếu để duy trì sự an toàn và bền vững trong mọi hoạt động.

Vì dữ liệu ngày càng phổ biến và ngày càng có nhiều người làm việc cũng như kết nối từ mọi nơi, nên những kẻ xấu đã đối phó bằng cách phát triển các phương pháp tinh vi để có được quyền truy nhập vào các tài nguyên cũng như lấy cắp dữ liệu, phá hoại doanh nghiệp hoặc tống tiền. Mỗi năm số cuộc tấn công tăng lên và những kẻ tấn công tiếp tục phát triển các phương pháp tránh bị phát hiện mới. Một chương trình an ninh mạng hiệu quả thường bao gồm con người, quy trình và giải pháp công nghệ cùng nhau giảm rủi ro gây gián đoạn kinh doanh, tổn thất tài chính và tổn thất uy tín từ các cuộc tấn công.

### Mục tiêu của an ninh mạng

An ninh mạng là sự bảo vệ cho các hệ thống nhằm đạt được được các mục tiêu đó là duy trì tính bí mật, tính toàn vẹn và tính sẵn sàng của tài nguyên hệ thống.



Hình 1.1: Tam giác bảo mật CIA

*Tính bí mật (Confidentiality)* là sự ngăn chặn việc thông tin bị truy cập hoặc tiết lộ trái phép. Đảm bảo chỉ những người hoặc hệ thống được ủy quyền mới có thể truy cập vào dữ liệu. Mọi truy cập trái phép đều phải bị ngăn chặn.

*Tính toàn vẹn (Integrity)* là sự phát hiện và ngăn chặn việc sửa đổi trái phép về dữ liệu, thông tin và hệ thống. Dữ liệu cần phải chính xác, đầy đủ và không bị chỉnh sửa bởi các yếu tố không được phép. Việc thay đổi hoặc xóa dữ liệu có thể gây ra những tổn hại nghiêm trọng.

*Tính sẵn sàng (Availability)* là sự đảm bảo dữ liệu và hệ thống luôn sẵn sàng cho người dùng hợp pháp truy cập khi cần thiết. Nếu hệ thống không thể truy cập được, các hoạt động sẽ bị gián đoạn và ảnh hưởng nghiêm trọng.

### Tầm quan trọng của an ninh mạng

An ninh mạng là yếu tố vô cùng quan trọng trong thời đại số hiện nay. Với sự phát triển nhanh chóng của công nghệ thông tin và việc kết nối toàn cầu qua Internet, an ninh mạng đang dần trở nên quan trọng hơn bao giờ hết.

*Bảo vệ dữ liệu cá nhân:* Thông tin cá nhân, như tên, địa chỉ, số thẻ tín dụng và mật khẩu, có thể bị lộ nếu không có hệ thống bảo mật thích hợp. Các cuộc tấn công mạng có thể dẫn đến việc đánh cắp thông tin cá nhân, gây tổn thất cho người dùng. Bảo vệ dữ liệu cá nhân không chỉ giúp tránh các cuộc tấn công mà còn giữ gìn sự riêng tư của mỗi cá nhân trong không gian mạng.

*Bảo vệ tài sản doanh nghiệp:* Các tổ chức và công ty sở hữu nhiều dữ liệu nhạy cảm như thông tin khách hàng, dữ liệu tài chính, nghiên cứu và phát triển sản phẩm. Nếu bị xâm nhập, dữ liệu này có thể bị rò rỉ hoặc đánh cắp, gây ảnh hưởng nghiêm trọng đến uy tín và tài chính của doanh nghiệp. Việc bảo vệ an ninh mạng giúp ngăn chặn các mối đe dọa này và duy trì hoạt động ổn định của doanh nghiệp.

*Ngăn chặn các cuộc tấn công mạng:* Các cuộc tấn công mạng như virus, ransomware, tấn công từ chối dịch vụ (DDoS), … có thể làm gián đoạn hoạt động của các hệ thống công nghệ, gây thiệt hại nặng nề cho cá nhân và tổ chức. Những cuộc tấn công này có thể dẫn đến mất mát dữ liệu, thiệt hại về tài chính và làm gián đoạn các dịch vụ quan trọng. Việc đảm bảo an ninh mạng giúp bảo vệ hệ thống khỏi các tấn công này.

*Bảo vệ quyền lợi quốc gia:* Các quốc gia có thể là mục tiêu của các cuộc tấn công mạng nhắm vào cơ quan chính phủ, hệ thống hạ tầng quan trọng hoặc các tổ chức chiến lược. Việc bảo vệ an ninh mạng quốc gia là rất quan trọng để duy trì sự ổn định và bảo vệ an ninh quốc gia, đồng thời ngăn ngừa các mối đe dọa từ các đối tượng tấn công có ý đồ xấu.

*Đảm bảo tính toàn vẹn và sẵn sàng của hệ thống:* An ninh mạng giúp đảm bảo rằng các hệ thống công nghệ hoạt động ổn định, không bị xâm nhập hay thay đổi trái phép, từ đó duy trì sự liên tục trong hoạt động của cá nhân, tổ chức và xã hội. Điều này đặc biệt quan trọng đối với các hệ thống thiết yếu như điện lực, giao thông và chăm sóc sức khỏe.

### Các mối đe dọa an ninh mạng

Sự gia tăng của các cuộc tấn công mạng là kết quả tất yếu của quá trình chuyển đổi số nhanh chóng, nhưng nhiều tổ chức và doanh nghiệp lại chưa có sự đầu tư đầy đủ cho an toàn thông tin. Trong quá trình cải tiến công nghệ, các tổ chức này vô tình để lộ những điểm yếu do không chú trọng đến an ninh mạng ngay từ giai đoạn thiết kế. Chính những điểm yếu này đã biến họ thành mục tiêu dễ dàng cho tin tặc, khiến các cuộc tấn công mạng ngày càng trở nên tinh vi hơn về cả quy mô và phương thức.

*Phần mềm độc hại (Malware):* Phần mềm độc hại bao gồm virus, worm, trojan, ransomware, spyware và adware. Các phần mềm này xâm nhập vào hệ thống máy tính mà không được phép, có thể đánh cắp thông tin, phá hoại hệ thống, hoặc chiếm quyền kiểm soát máy tính. Trong đó, malware thường xâm nhập qua các tệp đính kèm email, website không an toàn, hoặc phần mềm bị nhiễm độc. Một số loại malware có thể tự nhân bản và lan truyền qua mạng nội bộ hoặc Internet.

*Tấn công từ chối dịch vụ (DDos):* DDoS là một trong những hình thức tấn công phổ biến nhất. Kẻ tấn công sử dụng nhiều máy tính bị lây nhiễm để gửi lượng lớn yêu cầu đến một máy chủ hoặc hệ thống, làm cho nó quá tải và không thể hoạt động bình thường. Mục tiêu của DDoS là làm gián đoạn hoặc ngưng trệ hoạt động của dịch vụ, khiến người dùng hợp pháp không thể truy cập vào dịch vụ hoặc thông tin họ cần.

*Lừa đảo (Phishing):* Phishing là hành vi lừa đảo qua email hoặc trang web giả mạo nhằm đánh cắp thông tin cá nhân, thông tin đăng nhập, hoặc dữ liệu tài chính của người dùng. Kẻ tấn công thường giả mạo các tổ chức hoặc cá nhân tin cậy để lừa người dùng cung cấp thông tin nhạy cảm. Các email hoặc website phishing thường rất tinh vi, khiến người dùng khó phân biệt với email hoặc trang web hợp pháp. Chúng có thể chứa liên kết đến các trang web giả mạo hoặc yêu cầu người dùng cung cấp thông tin cá nhân.

*Tấn công khai thác lỗ hổng:* Kẻ tấn công có thể tận dụng các lỗ hổng bảo mật trong phần mềm, hệ điều hành, hoặc ứng dụng để xâm nhập vào hệ thống, chiếm quyền kiểm soát hoặc đánh cắp dữ liệu.

*Tấn công qua mạng xã hội:* Tấn công qua mạng xã hội là hình thức tấn công mà kẻ tấn công thao túng tâm lý con người để lừa họ tiết lộ thông tin mật hoặc thực hiện các hành động không an toàn. Một ví dụ phổ biến là việc giả làm đồng nghiệp hoặc đối tác kinh doanh để yêu cầu người dùng cung cấp mật khẩu hoặc thông tin đăng nhập vào hệ thống.

*Tấn công mã hóa tống tiền (Ransomware):* Ransomware là một loại malware mã hóa các tệp dữ liệu quan trọng trên máy tính hoặc hệ thống mạng và yêu cầu một khoản tiền chuộc để giải mã chúng. Các doanh nghiệp và cá nhân bị tấn công ransomware có thể mất hoàn toàn quyền truy cập vào dữ liệu của mình, gây ra thiệt hại nghiêm trọng về tài chính và danh tiếng.

*Tấn công xem giữa:* Bên ngoài cố gắng truy cập trái phép vào mạng trong khi trao đổi dữ liệu.

*Mối đe dọa nội bộ:* Một rủi ro an ninh do nhân viên có ý định xấu trong một tổ chức gây ra, làm mất ổn định an ninh hệ thống từ bên trong.

### Các biện pháp bảo vệ an ninh mạng

Theo khoản 1 Điều 5 Luật An ninh mạng 2018 có 13 biện pháp bảo vệ an ninh mạng bao gồm:

* Thẩm định an ninh mạng.
* Đánh giá điều kiện an ninh mạng.
* Kiểm tra an ninh mạng.
* Giám sát an ninh mạng.
* Ứng phó, khắc phục sự cố an ninh mạng.
* Đấu tranh bảo vệ an ninh mạng.
* Sử dụng mật mã để bảo vệ thông tin mạng.
* Ngăn chặn, yêu cầu tạm ngừng, ngừng cung cấp thông tin mạng; đình chỉ, tạm đình chỉ các hoạt động thiết lập, cung cấp và sử dụng mạng viễn thông, mạng Internet, sản xuất và sử dụng thiết bị phát, thu phát sóng vô tuyến theo quy định của pháp luật.
* Yêu cầu xóa bỏ, truy cập xóa bỏ thông tin trái pháp luật hoặc thông tin sai sự thật trên không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.
* Thu thập dữ liệu điện tử liên quan đến hoạt động xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên không gian mạng.
* Phong tỏa, hạn chế hoạt động của hệ thống thông tin; đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin, thu hồi tên miền theo quy định của pháp luật.
* Khởi tố, điều tra, truy tố, xét xử theo quy định của Bộ luật Tố tụng hình sự.
* Biện pháp khác theo quy định của pháp luật về an ninh quốc gia, pháp luật về xử lý vi phạm hành chính.

## Lý do chọn đề tài

Trong thời đại công nghệ số, lượng dữ liệu được lưu trữ, truyền tải và xử lý ngày càng lớn, kéo theo đó là nguy cơ mất an toàn thông tin. Việc bảo vệ dữ liệu trước các mối đe dọa như tấn công mạng, đánh cắp dữ liệu và xâm phạm quyền riêng tư là một yêu cầu cấp thiết. Trong bối cảnh đó, các phương pháp mã hóa đóng vai trò trọng yếu trong việc đảm bảo tính bí mật, toàn vẹn và sẵn sàng của dữ liệu và hệ thống.

AES (Advanced Encryption Standard), được phê chuẩn bởi Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ (NIST), là một trong những thuật toán mã hóa đối xứng phổ biến và hiệu quả nhất hiện nay. Với khả năng bảo mật mạnh mẽ, tốc độ xử lý cao và hiệu quả trong nhiều ứng dụng, AES đã được công nhận và sử dụng rộng rãi trên toàn cầu, trở thành lựa chọn hàng đầu trong nhiều hệ thống bảo mật. AES không chỉ được sử dụng trong các hệ thống lớn như ngân hàng, thương mại điện tử hay các cơ quan chính phủ mà còn xuất hiện trong các ứng dụng đời thường như mã hóa dữ liệu cá nhân trên điện thoại di động, đĩa cứng và truyền thông qua Internet. Tìm hiểu và áp dụng AES sẽ giúp nâng cao kỹ năng thực hành trong bảo mật thông tin, đồng thời mở ra cơ hội phát triển các hệ thống an toàn và tối ưu hơn.

Nghiên cứu chuẩn AES mang lại cơ hội hiểu sâu về cơ chế hoạt động của các thuật toán mã hóa hiện đại. Đề tài cũng là cơ hội để triển khai các ứng dụng thực tế, như phát triển chương trình mã hóa, qua đó kiểm chứng lý thuyết và nâng cao năng lực ứng dụng công nghệ.

Bên cạnh đó, việc xây dựng chương trình mã hóa và giải mã AES cũng là một cơ hội cho việc phát triển, nâng cao kỹ năng lập trình và hiểu sâu hơn về bảo mật thông tin.

Đề tài không chỉ mang tính học thuật mà còn góp phần nâng cao nhận thức của cộng đồng về bảo mật dữ liệu, khuyến khích sử dụng các biện pháp an toàn trong lưu trữ và truyền thông thông tin. Điều này đặc biệt quan trọng trong bối cảnh các mối đe dọa an ninh mạng ngày càng gia tăng.

## Nội dung nghiên cứu

Hệ mã hóa khóa bí mật: Các khái niệm cơ bản, cách hoạt động, mô hình và các yêu cầu khi sử dụng.

Chuẩn mã nâng cao AES: Giới thiệu, cách hoạt động, độ an toàn, ưu nhược điểm và ứng dụng.

Ngôn ngữ lập trình sử dụng cho việc xây dựng chương trình mã hóa và giải mã AES: Java, C#.

Kỹ thuật để xây dựng ra một chương trình mã hóa và giải mã: Cách xây dựng thuật toán, cách xây dựng giao diện phù hợp và dễ thao tác.

Triển khai, kiểm thử và sửa lỗi chương trình: Thiết kế kịch bản cho chương trình, chạy thử chương trình, kiểm tra tất cả các tính năng đã xây dựng và sửa lỗi nếu có.

## Các kiến thức cơ sở

### Cơ sở toán học

#### Phép XOR

Phép XOR (viết tắt của Exclusive OR) là một phép toán logic được sử dụng trong nhiều lĩnh vực, đặc biệt là trong khoa học máy tính, điện tử và mật mã học.

Phép XOR lấy hai dãy bit có cùng độ dài và thực hiện XOR trên mỗi cặp bit tương ứng. Phép XOR trả về đúng (True) nếu hai toán hạng khác nhau và sai (False) nếu hai toán hạng giống nhau.

Bảng 1.1: Bảng chân lý cho phép XOR

|  |  |  |
| --- | --- | --- |
| **A** | **B** | **A XOR B** |
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

Ví dụ, thực hiện phép XOR đối với số hệ nhị phân: 0101 XOR 0011.

Bảng 1.2: Ví dụ phép XOR đối với số hệ nhị phân

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| A | 0 | 1 | 0 | 1 |
| B | 0 | 0 | 1 | 1 |
| A XOR B | 0 | 1 | 1 | 0 |

Ví dụ, thực hiện phép XOR đối với số hệ 16: A5 XOR 3F.

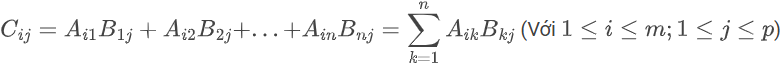
Bảng 1.3: Ví dụ phép XOR đối với số hệ 16

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Chuyển đổi sang hệ nhị phân sau đó thực hiện phép XOR. | | | | | | | | |
| A516 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 |
| 3F16 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 |
| A5 XOR 3F | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |
| Chuyển đổi kết quả về lại hệ 16: 1001 1010 = 9A | | | | | | | | |

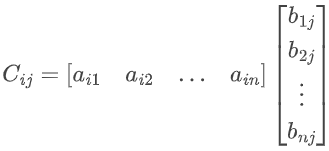
#### Phép nhân ma trận

Phép nhân hai ma trận chỉ thực hiện được khi số lượng cột trong ma trận thứ nhất phải bằng số lượng hàng trong ma trận thứ hai. Ma trận kết quả, được gọi là ma trận tích, có số lượng hàng của ma trận đầu tiên và số cột của ma trận thứ hai.

Nếu ma trận *A* có kích thước và ma trận *B* có kích thước thì ma trận tích có kích thước . Phần tử đứng ở hàng thứ *i*, cột thứ *j* được xác định bởi công thức:

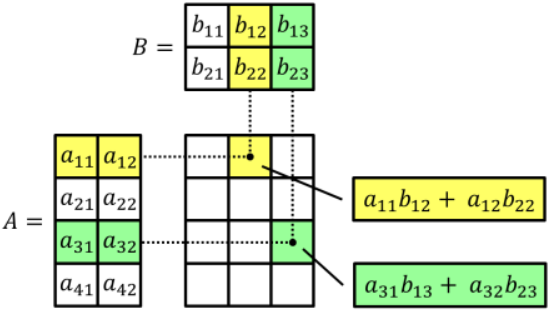


Hay có thể viết:



Tức là phần tử ở hàng thứ *i*, cột thứ *j* của *C* là tích của vector hàng thứ *i* của ma trận *A* với vector cột thứ *j* của ma trận *B*.

Minh họa tích ma trận *AB* của hai ma trận *A* và *B*:



Hình 1.2: Minh họa tích ma trận AB của hai ma trận A và B

Ví dụ, tính *C = AB*, biết:



Ta được ma trận tích:

### Ngôn ngữ lập trình

#### Ngôn ngữ Java

Java được khởi đầu bởi James Gosling và bạn đồng nghiệp ở Sun MicroSystem năm 1991. Ban đầu Java được tạo ra nhằm mục đích viết phần mềm cho các sản phẩm gia dụng, và có tên là Oak. Java được chính thức phát hành năm 1994, đến năm 2010 được Oracle mua lại từ Sun MicroSystem.

Java là ngôn ngữ lập trình đa nền tảng (cross-platform), được phát triển bởi James Gosling tại Sun Microsystems (nay là Oracle Corporation). Ngôn ngữ lập trình này ra đời vào năm 1995 và được thiết kế để có thể chạy trên các nền tảng khác nhau, từ máy tính cá nhân đến thiết bị di động, các máy chủ và thiết bị nhúng.

Java sử dụng cấu trúc lập trình hướng đối tượng (Object-Oriented Programming - OOP) và được xây dựng trên cơ sở của ngôn ngữ lập trình C++. Nó cung cấp một môi trường chạy ảo (virtual machine) gọi là Java Virtual Machine (JVM), giúp các chương trình Java có thể chạy trên nhiều nền tảng khác nhau mà không cần phải biên dịch lại.

Đặc điểm của Java:

* Hướng đối tượng hoàn toàn.
* Có thể chạy trên nhiều nền tảng khác nhau.
* Quản lý bộ nhớ tự động.
* Hỗ trợ đa luồng.
* Tính bảo mật cao.
* Hỗ trợ thư viện và các công cụ mạnh mẽ.

Ưu điểm của Java:

* Độ tin cậy cao.
* Tính đa nền tảng.
* Quản lý bộ nhớ tự động.
* Công cụ phát triển phong phú.
* Hỗ trợ đa luồng.

Nhược điểm của Java:

* Tốc độ chậm hơn so với các ngôn ngữ lập trình gần sát với phần cứng, chẳng hạn như C hoặc C++.
* Java có thể chạy trên nhiều nền tảng khác nhau, nhưng ứng dụng này có thể cần đến một trình biên dịch hoặc máy ảo Java riêng biệt để có thể chạy trên các thiết bị di động.
* Sử dụng bộ nhớ lớn hơn so với một số ngôn ngữ lập trình khác.
* Cú pháp phức tạp hơn so với một số ngôn ngữ lập trình khác

#### Ngôn ngữ C#

C# (hay C sharp) là một ngôn ngữ lập trình đơn giản, được phát triển bởi đội ngũ kỹ sư của Microsoft vào năm 2000. C# là ngôn ngữ lập trình hiện đại, hướng đối tượng và được xây dựng trên nền tảng của hai ngôn ngữ mạnh nhất là C++ và Java.

Trong các ứng dụng Windows truyền thống, mã nguồn chương trình được biên dịch trực tiếp thành mã thực thi của hệ điều hành.

Trong các ứng dụng sử dụng .NET Framework, mã nguồn chương trình (C#, VB.NET) được biên dịch thành mã ngôn ngữ trung gian MSIL (Microsoft Intermediate Language). Sau đó mã này được biên dịch bởi Common Language Runtime (CLR) để trở thành mã thực thi của hệ điều hành.

C# với sự hỗ trợ mạnh mẽ của .NET Framework giúp cho việc tạo một ứng dụng Windows Forms hay WPF (Windows Presentation Foundation), phát triển game, ứng dụng Web, ứng dụng Mobile trở nên rất dễ dàng.

Đặc điểm của C#:

* Là một ngôn ngữ thuần hướng đối tượng.
* Là ngôn ngữ khá đơn giản, chỉ có khoảng 80 từ khóa và hơn mười mấy kiểu dữ liệu được dựng sẵn.
* Cung cấp những đặc tính hướng thành phần (component-oriented) như Property, Event, …
* C# không khuyến khích sử dụng con trỏ như trong C++ nhưng khi thực sự muốn sử dụng thì phải đánh dấu đây là mã không an toàn (unsafe).
* C# có bộ Garbage Collector sẽ tự động thu gom vùng nhớ khi không còn sử dụng nữa.
* C# đã loại bỏ đa kế thừa trong C++ mà thay vào đó C# sẽ hỗ trợ thực thi giao diện interface.

Ưu điểm của C#:

* Gần gũi với các ngôn ngữ lập trình thông dụng (C++, Java, Pascal).
* Xây dựng dựa trên nền tảng của các ngôn ngữ lập trình mạnh nên thừa hưởng những ưu điểm của những ngôn ngữ đó.
* Cải tiến các khuyết điểm của C/C++.
* Dễ tiếp cận, dễ phát triển.
* Được sự chống lưng của .NET Framework.

Nhược điểm của C#:

* Nhược điểm lớn nhất của C# là chỉ chạy trên nền Windows và có cài .NET Framework.
* Thao tác đối với phần cứng yếu hơn so với ngôn ngữ khác. Hầu hết phải dựa vào Windows.

# KẾT QUẢ NGHIÊN CỨU

## Nghiên cứu và tìm hiểu về hệ mã hóa khóa bí mật

### Các khái niệm cơ bản

Mã hóa khóa bí mật là một phương pháp mã hóa, trong đó cùng một khóa được sử dụng cho cả việc mã hóa và giải mã dữ liệu. Đây là một trong những hình thức mã hóa phổ biến nhất, được sử dụng rộng rãi để bảo vệ thông tin trong các hệ thống truyền thông và lưu trữ dữ liệu.

Người gửi và người nhận nhờ chia sẻ khóa chung K, mà họ có thể trao đổi bí mật với nhau. Ta xét hai hàm ngược nhau: E là hàm biến đổi bản rõ thành bản mã và D là hàm biến đổi bản mã trở về bản rõ. Giả sử X là văn bản cần mã hóa và Y là văn bản đã được biến đổi qua việc mã hóa. Khi đó ta kí hiệu:

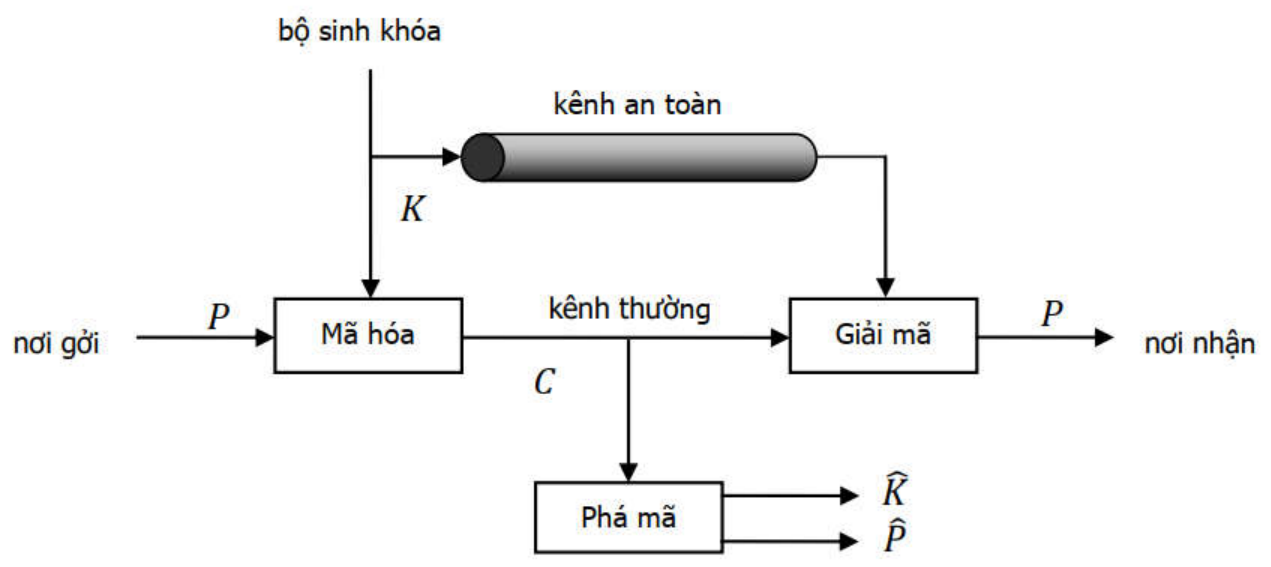
Y = EK(X)

X = DK(Y)

Các hệ mã hóa khóa bí mật được phát minh ra trước các hệ mã hóa khóa công khai. Hiện nay các hệ mã hóa khóa bí mật và công khai vẫn tiếp tục phát triển và hoàn thiện. Mã công khai ra đời hỗ trợ mã bí mật chứ không thay thế nó, do đó mã bí mật đến nay vẫn được sử dụng.

Một số khái niệm cơ bản về mã hóa:

* Bản rõ X: Là bản tin gốc. Bản rõ có thể được chia nhỏ để có kích thước phù hơp.
* Bản mã Y: Là bản tin gốc đã được mã hóa. Ta thường xét phương pháp mã hóa mà không làm thay đổi kích thước của bản rõ, tức là chúng có cùng độ dài.
* Khóa K: Là thông tin tham số dùng để mã hóa, chỉ có người gửi và người nhận biết. Khóa độc lập với bản rõ và có độ dài phù hợp với yêu cầu bảo mật.
* Mã hóa E: Là quá trình chuyển bản rõ thành bản mã. Thông thường bao gồm việc áp dụng thuật toán mã hóa và một số quá trình xử lý thông tin kèm theo.
* Giải mã D: Là quá trình chuyển bản mã về bản rõ. Đây là quá trình ngược lại của mã hóa.
* Mật mã: Là chuyên nghành khoa học của Khoa học máy tính nghiên cứu về các nguyên lý và phương pháp mã hóa. Hiện nay người ta đưa ra nhiều chuẩn an toàn cho các lĩnh vực khác nhau.
* Thám mã: Nghiên cứu các nguyên lý và phương pháp giải mã mà không biết khóa. Thông thường khi đưa các mã mạnh ra làm chuẩn dùng chung, các mã đó được những kẻ thám mã cũng như những người phát triển mã tìm hiểu và nghiên cứu các phương pháp giải mã một phần bản mã với các thông tin không đầy đủ.
* Lý thuyết mã: Bao gồm cả mật mã và thám mã. Nó là một thể thống nhất để đánh giá một mã mạnh hay không.



Hình 2.1: Mô hình của hệ mã hóa khóa bí mật

Đặc tính quan trọng của mã hóa khóa bí mật là khóa phải được giữ bí mật giữa người gửi và người nhận, hay nói cách khác khóa phải được chuyển một cách an toàn từ người gửi đến người nhận. Có thể đặt ra câu hỏi là nếu đã có một kênh an toàn để chuyển khóa như vậy thì tại sao không dùng kênh đó để chuyển bản tin, tại sao cần đến chuyện mã hóa? Câu trả lời là nội dung bản tin thì có thể rất dài, còn khóa thì thường là ngắn. Ngoài ra một khóa còn có thể áp dụng để truyền tin nhiều lần. Do đó nếu chỉ chuyển khóa trên kênh an toàn thì đỡ tốn kém chi phí.

### Các yêu cầu đối với hệ mã hóa khóa bí mật

Một hệ mã hóa khóa bí mật có các đặc trưng là cách xử lý thông tin của thuật toán mã hóa, giải mã, tác động của khóa vào bản mã, độ dài của khóa. Mối liên hệ giữa bản rõ, khóa và bản mã càng phức tạp càng tốt, nếu tốc độ tính toán là chấp nhận được. Cụ thể hai yêu cầu để sử dụng an toàn mã khoá đối xứng là:

* Thuật toán mã hoá mạnh. Có cơ sở toán học vững chắc đảm bảo rằng mặc dù công khai thuật toán, mọi người đều biết, nhưng việc thám mã là rất khó khăn và phức tạp nếu không biết khóa.
* Khoá mật chỉ có người gửi và người nhận biết. Có kênh an toàn để phân phối khoá giữa các người sử dụng chia sẻ khóa. Mối liên hệ giữa khóa và bản mã là không nhận biết được.

## Nghiên cứu và tìm hiểu về chuẩn mã nâng cao AES

### Giới thiệu về AES

Vào năm 1999, Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ (NIST) đã ban hành một phiên bản mới của tiêu chuẩn DES chỉ ra rằng DES chỉ nên được sử dụng cho các hệ thống cũ và 3-DES được sử dụng. 3-DES có hai ưu điểm đảm bảo cho việc sử dụng rộng rãi trong vài năm tới. Đầu tiên, với độ dài khóa 168 bit, nó khắc phục được lỗ hổng đối với cuộc tấn công vét cạn của DES. Thứ hai, thuật toán mã hóa cơ bản trong 3-DES cũng giống như trong DES. Thuật toán này đã được giám sát kỹ lưỡng hơn bất kỳ thuật toán mã hóa nào khác trong một khoảng thời gian dài và không có cuộc tấn công phá mã hiệu quả nào dựa trên thuật toán thay vì vét cạn được tìm thấy. Do đó, 3-DES có khả năng chống phá mã rất tốt. Nếu bảo mật là yếu tố duy nhất được xem xét, thì 3-DES sẽ là lựa chọn thích hợp cho thuật toán mã hóa tiêu chuẩn trong nhiều thập kỷ tới.

Hạn chế chính của 3-DES là thuật toán tương đối chậm trong phần mềm. DES ban đầu được thiết kế để triển khai bằng phần cứng giữa những năm 1970 và không tạo ra mã phần mềm hiệu quả. 3-DES có số vòng gấp ba lần DES, do đó thực hiện chậm hơn DES. Một nhược điểm phụ là cả DES và 3-DES đều sử dụng kích thước khối 64 bit. Vì lý do hiệu quả và bảo mật, kích thước khối lớn hơn là cần thiết.

Vì những nhược điểm này, 3-DES không phải là ứng cử viên thích hợp để sử dụng lâu dài. Để thay thế, vào năm 1997 NIST đã đưa ra lời kêu gọi đề xuất Tiêu chuẩn mã hóa nâng cao (AES) mới, tiêu chuẩn này phải có sức mạnh bảo mật bằng hoặc tốt hơn 3-DES. Ngoài các yêu cầu chung này, NIST quy định rằng AES phải là mật mã khối đối xứng với độ dài khối 128 bit và hỗ trợ độ dài khóa có thể là 128, 192 và 256 bit.

Trong vòng đánh giá đầu tiên, 15 thuật toán được đề xuất đã được chấp nhận. Vòng thứ hai thu hẹp còn 5 thuật toán. NIST đã hoàn thành quá trình đánh giá của mình và xuất bản tiêu chuẩn cuối cùng vào tháng 11 năm 2001. NIST đã chọn Rijndael làm thuật toán AES được đề xuất. Hai nhà nghiên cứu đã phát triển và gửi Rijndael cho AES đều là những nhà mật mã học đến từ Bỉ: Tiến sĩ Joan Daemen và Tiến sĩ Vincent Rijmen.

Cuối cùng, AES được thiết kế để thay thế 3-DES, nhưng quá trình này sẽ mất một số năm. NIST dự đoán rằng 3-DES vẫn sẽ là một thuật toán được sử dụng trong tương lai gần.

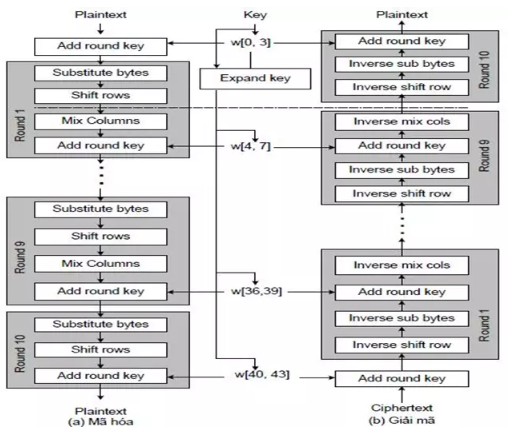
Các tham số của AES phụ thuộc vào kích thước của khóa. Chúng được thể hiện qua bảng dưới:

Bảng 2.1: Tham số của AES

|  |  |  |  |
| --- | --- | --- | --- |
| Kích thước khóa | 128 bit | 192 bit | 256 bit |
| Kích thước khối của bản rõ | 128 bit | 128 bit | 128 bit |
| Số vòng | 10 | 12 | 14 |
| Kích thước khóa tại mỗi vòng | 128 bit | 128 bit | 128 bit |
| Kích thước khóa mở rộng | 1408 bit | 1664 bit | 1920 bit |

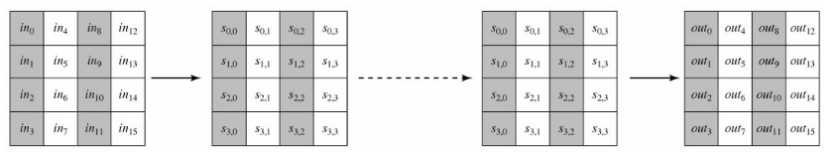
### Mã hóa và giải mã AES

Sơ đồ tổng quát của mã hóa và giải mã AES:



Hình 2.2: Sơ đồ tổng quát mã hóa và giải mã AES

Đầu vào cho thuật toán mã hóa và giải mã là một khối 128 bit, khối bit này được mô tả là một ma trận vuông, mỗi ô là 1 byte. Khối này được sao chép vào một mảng trạng thái, được sửa đổi ở mỗi giai đoạn mã hóa hoặc giải mã. Sau giai đoạn cuối cùng, mảng trạng thái này được sao chép vào một ma trận đầu ra.



Hình 2.3: Đầu vào, mảng trạng thái và đầu ra

Tương tự, khóa 128 bit được mô tả như một ma trận vuông, mỗi phần tử là 1 byte. Khóa này sau đó được mở rộng thành một mảng các từ (word), mỗi từ là 4 byte và tổng chiều dài khóa là 44 từ cho khóa 128 bit.



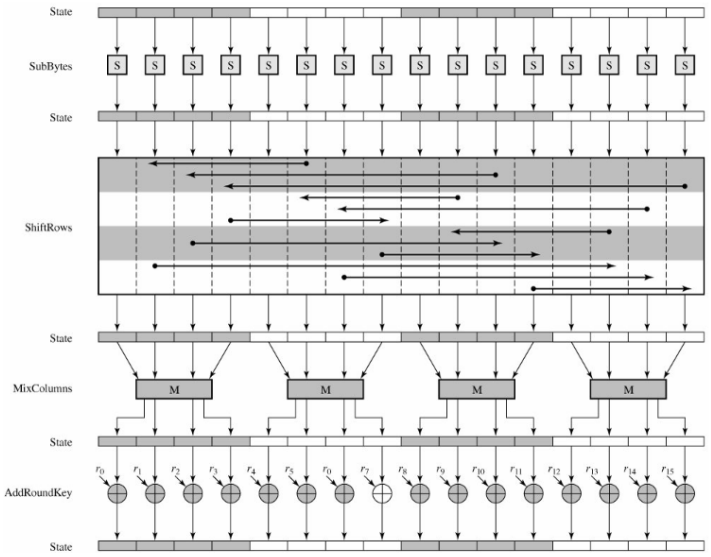
Hình 2.4: Khóa và mở rộng khóa

Thứ tự của các byte trong ma trận là theo cột. Vì vậy, 4 byte đầu tiên của bản rõ 128 bit đầu vào chiếm cột đầu tiên của ma trận, bốn byte thứ hai chiếm cột thứ hai, … Tương tự, 4 byte đầu tiên của khóa mở rộng tạo thành một từ, chiếm cột đầu tiên của ma trận.

Cấu trúc của thuật toán AES tương đối đơn giản. Cả thuật toán mã hóa và giải mã đều bắt đầu với giai đoạn Add round key, tiếp theo là 9 vòng, mỗi vòng đầy đủ 4 giai đoạn:

* Thay thế byte (Substitute bytes): Sử dụng hộp S để thực hiện việc thay thế từng byte của khối.
* Dịch dòng (Shift rows): Thực hiện hoán vị.
* Trộn cột (Mix columns): Phép thay thế sử dụng các phép toán số học trên Z256.
* Cộng với khóa (Add round key): Phép XOR của khối hiện tại với một phần của khóa được mở rộng.

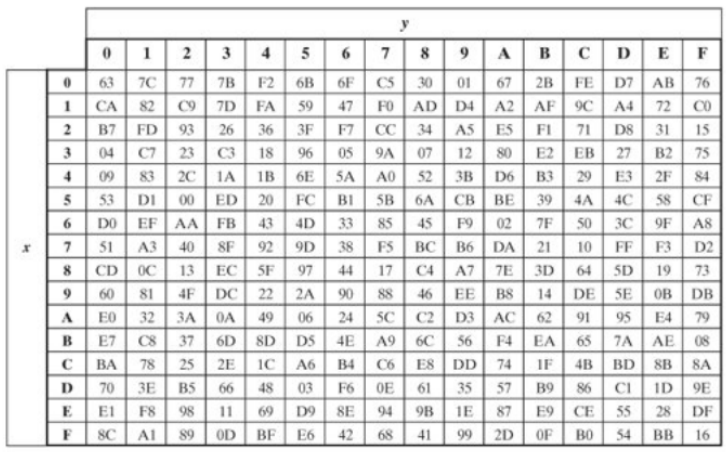
Vòng cuối cùng chỉ có 3 giai đoạn đó là: Substitute bytes, Shift rows và Add round key.



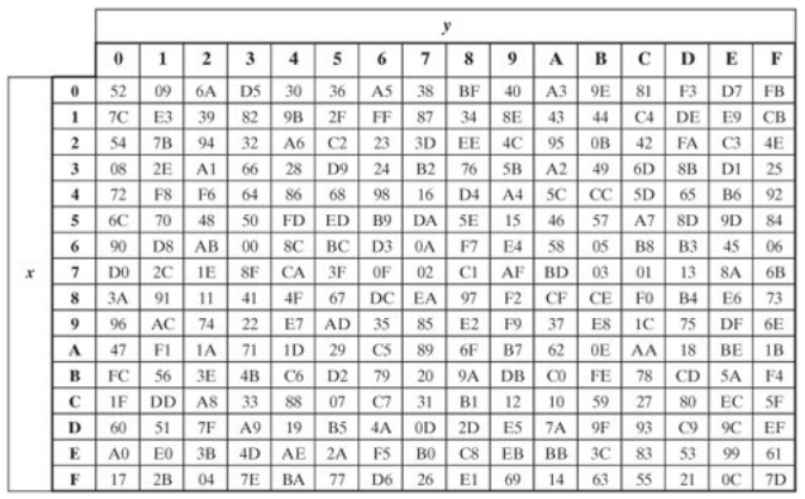
Hình 2.5: Minh họa một vòng mã AES

#### Thay thế byte (Substitute bytes)

Thay thế byte đơn giản chỉ là tra cứu trong bảng 16 x 16, mỗi ô là 1 byte và được gọi là hộp S (sử dụng trong Substitute bytes) và hộp S đảo (sử dụng trong Inverse Substitute bytes).

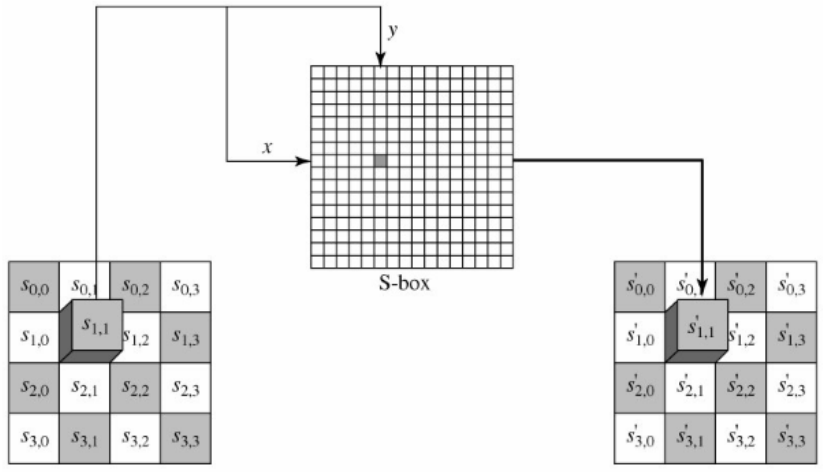


Hình 2.6: Hộp S



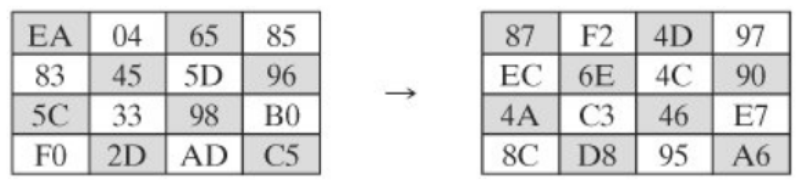
Hình 2.7: Hộp S đảo

Minh họa việc tra cứu hộp S:



Hình 2.8: Minh họa việc tra cứu hộp S

Ví dụ minh họa phép thay thế byte:

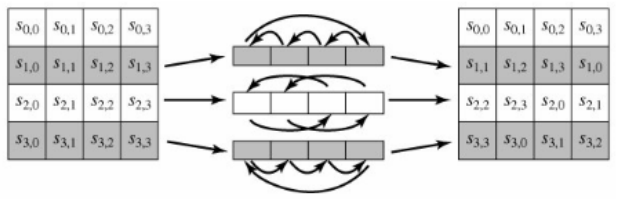


Hình 2.9: Minh họa phép thay thế byte

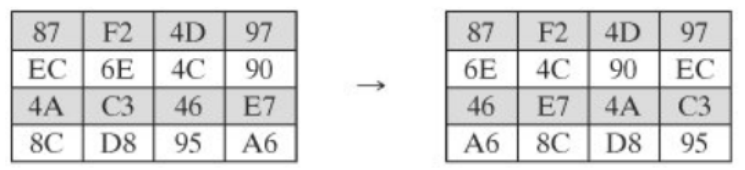
Để tìm byte thay thế của byte EA, ta tra dòng E và cột A trong hộp S thu được byte 87. Như vậy, byte EA sẽ được thay thế bằng byte 87. Tương tự, byte 04 ta tra dòng 0 và cột 4 thu được F2. Ta làm tương tự cho các byte còn lại sẽ thu được ma trận kết quả sau khi thực hiện phép thay thế.

#### Dịch dòng (Shift rows)

Minh họa phép dịch dòng. Dòng đầu tiên của ma trận trạng thái được giữ nguyên, dòng thứ hai dịch trái 1 byte, dòng thứ 3 dịch trái 2 byte và dòng cuối cùng dịch trái 3 byte.



Hình 2.10: Minh họa phép dịch dòng

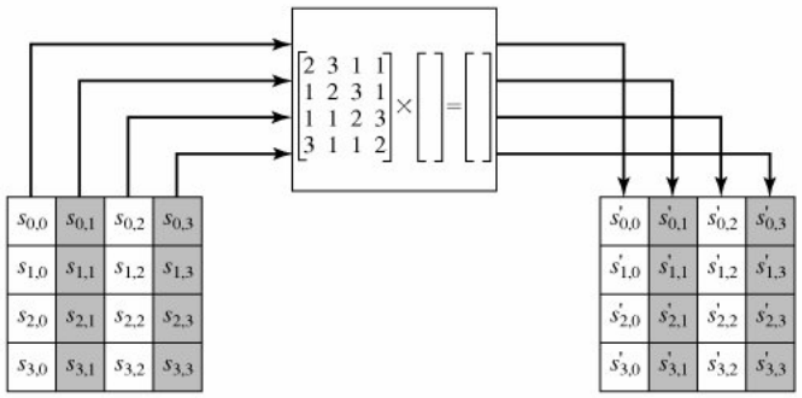


Hình 2.11: Ví dụ minh họa phép dịch dòng

Đối với thuật toán giải mã ta sử dụng phép dịch dòng ngược. Tức là, dòng đầu tiên của ma trận trạng thái giữ nguyên, dòng thứ 2 dịch phải 1 byte, dòng thứ 3 dịch phải 2 byte và dòng cuối cùng dịch phải 3 byte.

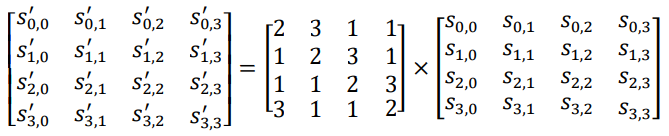
#### Trộn cột (Mix columns)

Minh họa phép trộn cột:

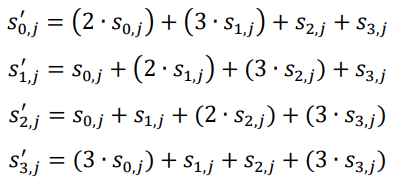


Hình 2.12: Minh họa phép trộn cột

Như vậy, kết quả của phép trộn cột sẽ được xác định theo công thức sau:

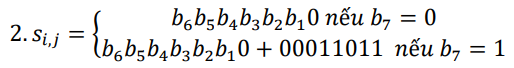


Áp dụng phép nhân hai ma trận ta thu được:



Trong đó, phép nhân (.) được thực hiện theo luật:

* Giả sử si,j được biểu diễn dưới dạng 8 bit b7b6b5b4b3b2b1b0.
* Khi nhân với 2 sẽ được thực hiện theo công thức sau:

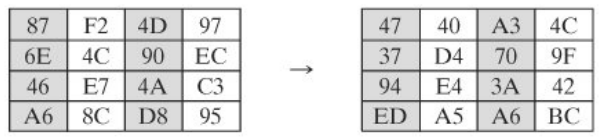


* Khi nhân với 3 sẽ được thực hiện theo công thức sau:



Phép cộng (+) trong các công thức trên là phép XOR bit.

Ví dụ minh họa phép trộn cột:



Hình 2.13: Ví dụ minh họa phép trộn cột

Diễn giải cách xác định phần tử đầu tiên trong ma trận sau khi thực hiện phép trộn cột:

s’00 = 2.(87) + 3.(6E) + 46 + A6

Chuyển các số từ hệ 16 sang hệ 2 để thực hiện các phép tính:

87h = 10000111

(b7 = 1 nên 2.(87) = 00001110 XOR 00011011 = 00010101)

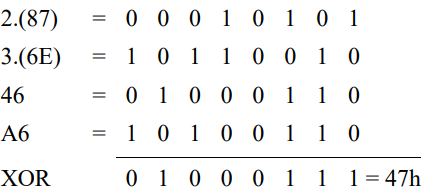
6Eh = 01101110

(b7 của 6E là 0 nên 2.(6E) = 11011100.

Do đó, 3.(6E) = 01101110 XOR 11011100 = 10110010)

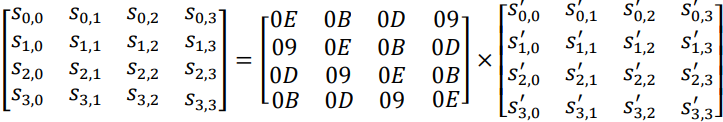
46h = 01000110

A6h = 10100110

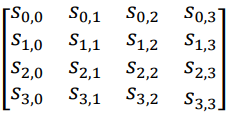


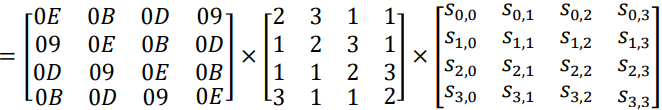
Tính toán tương tự cho các phần tử còn lại ta thu được trạng thái sau khi thực hiện phép trộn cột.

Phép trộn cột đảo (Inverse mix columns) trong thuật toán giải mã được thực hiện như sau:

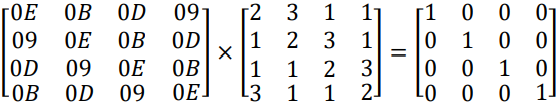


Thay thế công thức của phép trộn cột vào thì ta thu được công thức sau:





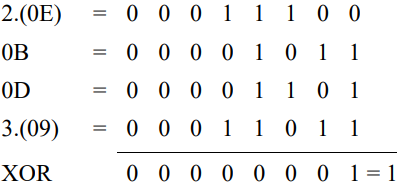
Như vậy thì công thức sau phải được thỏa mãn:



Chứng minh phần tử đầu tiên thỏa mãn yêu cầu:

2.(0E) + 0B + 0D + 3.(09)

= 00011100 + 00001011 + 00001101 + 3.(09)

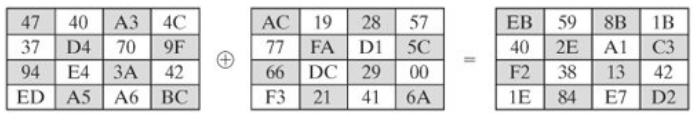


Tính toán tương tự cho các phần tử còn lại.

#### Cộng với khóa (Add round key)

Phép cộng với khóa là thực hiện phép XOR bit của 128 bit của ma trận trạng thái và 128 bit của khóa vòng tương ứng.

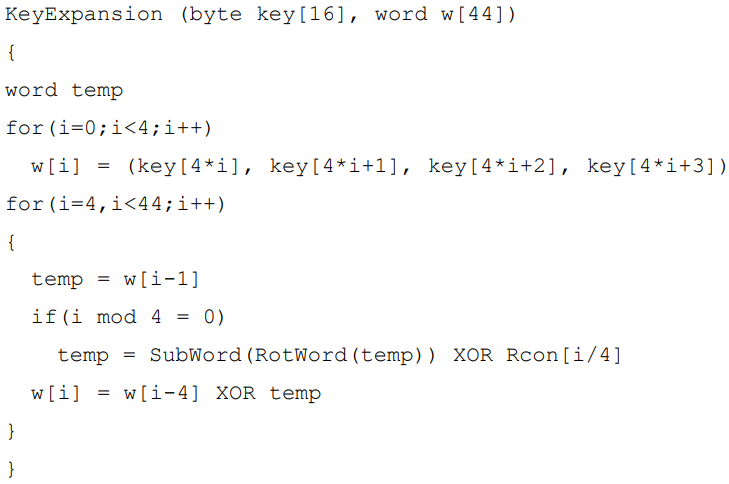
Ví dụ minh họa phép cộng khóa, ma trận đầu tiên là trạng thái và ma trận thứ hai là khóa của vòng:



Hình 2.14: Ví dụ minh họa phép cộng khóa

#### Mở rộng khóa (Key expansion)

Thuật toán mở rộng khóa có đầu vào là 4 từ (16 byte) khóa và tạo ra một mảng đầu ra 44 từ (176 byte). Mã giả của thuật toán được mô tả như sau:



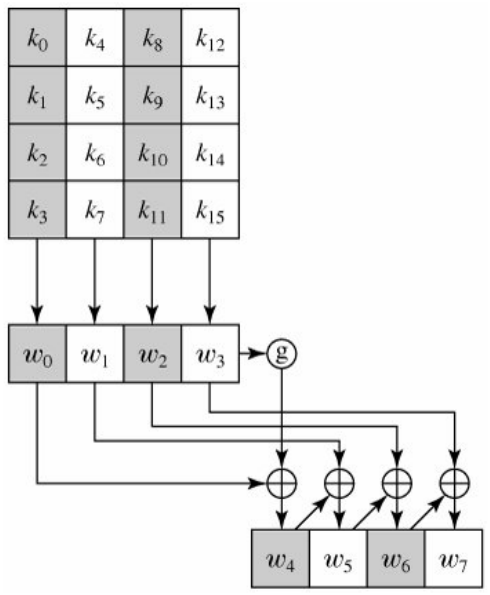
Phép toán RotWord là thực hiện phép dịch trái 1 byte, tức là đầu vào l từ có 4 byte [b0, b1, b2, b3] thì kết quả sau khi thực hiện phép dịch trái 1 byte sẽ là [b1, b2, b3, b0].

Phép toán SubWord là phép thay thế byte sử dụng bảng S.

Hằng số cho mỗi vòng khóa Rcon[j] = (RC[j], 0, 0, 0), với RC[1] = 1, RC[j] = 2.RC[j-1] và phép nhân (.) được thực hiện theo quy luật như trong thuật toán trộn cột. Giá trị của RC[j] được xác định như bảng dưới ở hệ thập lục phân (Hexadecimal).

Bảng 2.2: Giá trị của RC[j]

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| j | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| RC[j] | 01 | 02 | 04 | 08 | 10 | 20 | 40 | 80 | 1B | 36 |



Hình 2.15: Minh họa cách xác định khóa của vòng 1

Ví dụ minh họa cách xác định khóa cho vòng thứ 9 khi khóa tại vòng 8 là EA D2 73 21 B5 8D BA D2 31 2B F5 60 7F 8D 29 2F, tương ứng:

* + w[32] = [EA, D2, 73, 21]
  + w[33] = [B5, 8D, BA, D2]
  + w[34] = [31, 2B, F5, 60]
  + w[35] = [7F, 8D, 29, 2F]

Giá trị của khóa tại vòng 9 được xác định như bảng sau:

Bảng 2.3: Xác định khóa cho vòng 9 khi khóa tại vòng 8

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **i** | **Temp** | **RotWord** | **SubWord** | **Rcon(9)** | **XOR Rcon** | **w[i-4]** | **w[i] = Temp XOR w[i-4]** |
| 36 | 7F8D292F | 8D292F7F | 5DA515D2 | 1B000000 | 46A515D2 | EAD27321 | AC7766F3 |
| 37 | AC7766F3 | AC7766F3 | AC7766F3 | 1B000000 | AC7766F3 | B58DBAD2 | 19FABC21 |
| 38 | 19FABC21 | 19FABC21 | 19FABC21 | 1B000000 | 19FABC21 | 312BF560 | 28B14941 |
| 39 | 28B14941 | 28B14941 | 28B14941 | 1B000000 | 28B14941 | 7F8D292F | 575C606E |

Như vậy, khóa của vòng 9 sẽ là AC 77 66 F3 19 FA BC 21 28 B1 49 41 57 5C 60 6E.

### Minh họa quá trình mã hóa và giải mã AES

### Độ an toàn của AES

Chuẩn mã hóa nâng cao AES đã được Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ (NIST) tuyên bố là giải pháp tốt nhất để bảo vệ thông tin nhạy cảm cho Chính phủ trong thế kỷ 21.

AES là người bạn đồng hành không thể thiếu của Chính phủ, cơ quan Nhà nước và các tổ chức tư nhân.

Với độ dài khóa của thuật toán AES (128,192 và 256 bit) là đủ an toàn để bảo vệ các thông tin tối mật. Các thông tin tuyệt mật phải dùng khóa 192 hoặc 256 bit.

AES nếu được triển khai đúng quy trình thì sẽ đảm bảo an toàn tuyệt đối. Thế nhưng, một điều cần lưu ý đó là bất kỳ một hệ thống nào cũng có thể bị tấn công nếu hacker biết được khóa mã hóa. Do đó, các khóa cần được bảo vệ bằng nhiều cách khác nhau như dùng mật khẩu mạnh, xác thực tường lửa hay phần mềm chống độc hại.

### Nhận xét về AES

#### Ưu điểm

Tính bảo mật cao: AES là một thuật toán mã hóa đối xứng mạnh, có khả năng đảm bảo tính bảo mật cao trong việc mã hóa và giải mã dữ liệu.

Tốc độ nhanh: Thuật toán này có tốc độ mã hóa và giải mã rất nhanh, phù hợp với các ứng dụng đòi hỏi tốc độ cao như truyền dữ liệu qua mạng.

Linh hoạt: AES cũng có thể sử dụng các khóa với độ dài khác nhau (128, 192 hoặc 256 bit) để tăng cường tính bảo mật. Ngoài ra, thuật toán này có thể sử dụng trên các nền tảng phần cứng và phần mềm khác nhau.

Chuẩn quốc tế: AES là một chuẩn mã hóa quốc tế, được chấp nhận rộng rãi trên toàn cầu.

#### Nhược điểm

AES phụ thuộc vào độ dài khóa để đảm bảo tính bảo mật. Nếu khóa ngắn hoặc dễ đoán, AES có thể bị tấn công và dữ liệu có thể bị tiết lộ. AES cần sử dụng khóa an toàn để đảm bảo tính bảo mật. Nếu khóa bị mất hoặc rơi vào tay của kẻ xấu, dữ liệu có thể bị tiết lộ.

AES không thể đảm bảo tính bảo mật nếu hệ thống bị tấn công bởi các phương thức khác như tấn công mạng, tấn công từ chối dịch vụ (DoS), tấn công đánh cắp thông tin đăng nhập, …

Ngoài ra việc triển khai AES có thể đòi hỏi chi phí phần cứng và phần mềm khá lớn để bảo vệ dữ liệu, đặc biệt là trong các hệ thống lớn và phức tạp.

### Ứng dụng của AES

## Thiết kế chương trình và cài đặt thuật toán

### Thiết kế kịch bản chương trình

### Cài đặt thuật toán và giao diện chương trình với Java

### Cài đặt thuật toán và giao diện chương trình với C#

# KẾT LUẬN VÀ BÀI HỌC KINH NGHIỆM

## Kiến thức kỹ năng học được trong quá trình thực hiện đề tài

## Bài học kinh nghiệm

## Tính khả thi của chủ đề nghiên cứu

### Thuận lợi

### Khó khăn

# TÀI LIỆU THAM KHẢO

[1]. Nguyễn Xuân Dũng, *Bảo mật thông tin - Mô Hình và ứng dụng*, NXB Thống kê, 2009.

[2]. Bùi Doãn Khanh, Nguyễn Đình Thúc, *Mã hóa thông tin - Lý thuyết và ứng dụng*, NXB Lao động xã hội, 2011.

[3]. William Stallings**,** *Cryptography and Network Security Principles and Practices***,** Fourth Edition, Prentice Hall, 2005.

# PHỤ LỤC