**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ ĐÔNG Á**

**KHOA: CÔNG NGHỆ THÔNG TIN**



**BÀI TẬP LỚN**

**HỌC PHẦN: AN TOÀN BẢO MẬT THÔNG TIN**

**Đề tài 9: Nghiên cứu hệ thống bảo mật tập tin sử dụng hệ mã hoá AES**

|  |  |  |
| --- | --- | --- |
| **Sinh viên thực hiện** | **Lớp** | **Khóa** |
| **Trần Thị Nhật Linh** | **DCCNTT12.10.12** | **K12** |
| **Dương Công Kiên** | **DCCNTT12.10.12** | **K12** |
| **Nguyễn Anh Duy** | **DCCNTT12.10.12** | **K12** |
| **Nguyễn Trung Hiếu** | **DCCNTT12.10.12** | **K12** |
| **Vũ Tùng Dương** | **DCCNTT12.10.12** | **K12** |

**Bắc Ninh, năm 2023**

**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ ĐÔNG Á**

**KHOA: CÔNG NGHỆ THÔNG TIN**

**BÀI TẬP LỚN**

**HỌC PHẦN: AN TOÀN BẢO MẬT THÔNG TIN**

**Đề tài 9: Nghiên cứu hệ thống bảo mật tập tin sử dụng hệ mã hoá AES**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **STT** | **Sinh viên thực hiện** | **Mã sinh viên** | **Điểm bằng số** | **Điểm bằng chữ** |
| **1** | **Trần Thị Nhật Linh** | **20213347** |  |  |
| **2** | **Dương Công Kiên** | **20213350** |  |  |
| **3** | **Nguyễn Anh Duy** | **20213313** |  |  |
| **4** | **Nguyễn Trung Hiếu** | **20213613** |  |  |
| **5** | **Vũ Tùng Dương** | **20213443** |  |  |

|  |  |
| --- | --- |
| **CÁN BỘ CHẤM 1**  *(Ký và ghi rõ họ tên)* | **CÁN BỘ CHẤM 2**  *(Ký và ghi rõ họ tên)* |

# MỤC LỤC

[MỤC LỤC 2](#_Toc164037405)

[Danh mục hình ảnh 3](#_Toc164037406)

[Lời nói đầu 4](#_Toc164037407)

[Chương 1: Đặt vấn đề 5](#_Toc164037408)

[1. Giới thiệu đề tài 5](#_Toc164037409)

[2. Mục đích 5](#_Toc164037410)

[3. Ý nghĩa 6](#_Toc164037411)

[4. Công cụ sử dụng 6](#_Toc164037412)

[Chương 2: Giải quyết vấn đề 9](#_Toc164037413)

[1. Đầu vào: tệp tin (hình ảnh, văn bản,..) 9](#_Toc164037414)

[2. Cơ sở lý thuyết 9](#_Toc164037415)

[3. AES hoạt động như thế nào? 11](#_Toc164037416)

[Chương 3: Giới thiệu chương trình máy tính 16](#_Toc164037417)

[1. Giới thiệu mã hóa 16](#_Toc164037418)

[2. Hình ảnh 16](#_Toc164037419)

[3. Kết luận 19](#_Toc164037420)

[4. Bài học rút ra 20](#_Toc164037421)

[Danh mục tham khảo 21](#_Toc164037422)

# Danh mục hình ảnh

[Hình 2.1 Hình mô tả hệ thống đầu vào của AES 9](#_Toc164037681)

[Hình 2.2: Tính ứng dụng của AES 10](#_Toc164037682)

[Hình 2.3: Mô hình hoạt động của AES 12](#_Toc164037683)

[Hình 2.5: mô tả phép ShiftRows 13](#_Toc164037684)

[Hình 2.6: mô tả phép MixColumns 13](#_Toc164037685)

[Hình 2.7: mô tả phép AddRoundKey 14](#_Toc164037686)

[Hình 2.8: Mô hình mở rộng khóa 15](#_Toc164037687)

[Hình 3.1: Ảnh sau khi mã hóa file đầu vào của thuật toán AES 16](#_Toc164037688)

[Hình 3.2: Bước 1 chọn file và đặt pass 17](#_Toc164037689)

[Hình 3.2: Bước 2 ấn vào encrypt để mã hóa 18](#_Toc164037690)

[Hình 3.2: Bước 3 ấn vào decrypt để giải mã hóa và trở về giống bước 1 ( là để chọn file) 19](#_Toc164037691)

# Lời nói đầu

Từ trước công nguyên con người đã phải quan tâm tới việc làm thế nào để đảm bảo an toàn bí mật cho các tài liệu, văn bản quan trọng, đặc biệt là trong lĩnh vực quân sự, ngoại giao. Ngày nay với sự xuất hiện của máy tính, các tài liệu văn bản giấy tờ và các thông tin quan trọng đều được số hóa và xử lý trên máy tính, được truyền đi trong môi trường mạng- một môi trường mà mặc định là không an toàn.

Do đó yêu cầu về việc có một cơ chế, giải pháp để bảo vệ sự an toàn và bí mật của các thông tin nhạy cảm, quan trong ngày càng trở nên cấp thiết. An toàn bảo mật thông tin là môn học đảm bảo cho mục đích này. Khó có thể thấy một ứng dụng Tin học có ích nào lại không sử dụng các thuật toán mã hóa thông tin.

Trong thời gian học tập tại trường Đại học Công Nghệ Đông Á, được sự giúp đỡ tận tình của giảng viên, chúng em đã có thêm những kiến thức về môn học cũng như ứng dụng của học phần an toàn bảo mật thông tin trong thực tế. Trong phạm vi bài tập lớn, chúng em sẽ tìm hiểu về hệ mã hóa AES (Advanced Encryption Standard) là một thuật toán mã hóa khối được chính phủ Hoa Kỳ áp dụng làm tiêu chuẩn mã hóa. Mục tiêu của AES được sinh ra nhằm bảo vệ các dữ liệu thông qua quá trình mã hoá và giải mã dữ liệu, và tính đến hiện nay, AES được sử dụng vô cùng phổ biến, kể cả tại Việt Nam

Chúng em xin chân thành cảm ơn giảng viên đã giúp đỡ chúng em hoàn thành bài tập này!

# Chương 1: Đặt vấn đề

## Giới thiệu đề tài

Nhu cầu bảo mật dữ liệu ngày càng cao trong thời đại công nghệ số. Các phương thức bảo mật truyền thống dần bộc lộ hạn chế về khả năng bảo mật và tốc độ xử lý. Nhằm đáp ứng nhu cầu cấp thiết này, thuật toán mã hóa AES (Advanced Encryption Standard) ra đời và nhanh chóng trở thành tiêu chuẩn quốc tế được áp dụng rộng rãi.

Bài báo cáo sau đây chúng em xin trình bày về hệ mã hóa AES.Đây là thuật toán mã hóa đối xứng được NIST (Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ) công nhận vào năm 2001. Nhờ sở hữu những ưu điểm vượt trội như tính bảo mật cao, tốc độ xử lý nhanh và khả năng triển khai linh hoạt, AES đã trở thành lựa chọn hàng đầu cho các ứng dụng bảo mật dữ liệu trong nhiều lĩnh vực khác nhau.

Với vai trò quan trọng trong việc bảo vệ thông tin nhạy cảm, thuật toán AES hứa hẹn sẽ tiếp tục đóng góp to lớn cho sự phát triển của công nghệ bảo mật trong tương lai.

## Mục đích

Nâng cao kiến thức chuyên môn: Thuật toán AES là một trong những thuật toán mã hóa phổ biến và được ứng dụng rộng rãi nhất hiện nay. Việc nghiên cứu đề tài này giúp chúng em hiểu sâu hơn về nguyên tắc hoạt động, cấu trúc, ưu nhược điểm của AES cũng như các ứng dụng thực tế của nó. Thông qua nghiên cứu, chúng em có cơ hội trau dồi kỹ năng phân tích, đánh giá và so sánh các thuật toán mã hóa khác nhau. Nắm bắt được các xu hướng phát triển mới nhất trong lĩnh vực mật mã học, từ đó định hướng nghiên cứu và phát triển bản thân trong tương lai.

Góp phần nâng cao nhận thức về tầm quan trọng của bảo mật dữ liệu: Trong thời đại công nghệ số, bảo mật dữ liệu là một vấn đề vô cùng quan trọng. Việc nghiên cứu và giới thiệu thuật toán AES giúp nâng cao nhận thức của cộng đồng về tầm quan trọng của việc bảo vệ thông tin cá nhân và dữ liệu nhạy cảm. Cung cấp cho người dùng những kiến thức cơ bản về cách thức hoạt động của thuật toán mã hóa, từ đó giúp họ lựa chọn phương thức bảo mật phù hợp cho nhu cầu của bản thân.

Ứng dụng kiến thức vào thực tế: Kiến thức thu thập được từ việc nghiên cứu đề tài có thể áp dụng vào các dự án thực tế liên quan đến bảo mật dữ liệu, phát triển phần mềm hoặc hệ thống an ninh mạng. Nâng cao khả năng giải quyết vấn đề và ứng dụng kiến thức chuyên môn vào thực tiễn.

Với những mục đích trên, chúng em tin rằng việc nghiên cứu đề tài về thuật toán AES sẽ mang lại nhiều lợi ích cho bản thân, góp phần nâng cao kiến thức chuyên môn và kỹ năng nghiên cứu khoa học, đồng thời đóng góp vào việc nâng cao nhận thức về tầm quan trọng của bảo mật dữ liệu trong cộng đồng.

## Ý nghĩa

Thuật toán mã hóa (AES) là một trong những công cụ quan trọng nhất trong lĩnh vực bảo mật thông tin hiện đại. Sự ra đời và phát triển của AES đã góp phần quan trọng vào việc bảo vệ dữ liệu trực tuyến và tạo ra một môi trường truyền thông an toàn hơn cho mọi người.

Với mục tiêu chính là bảo vệ dữ liệu, AES đã trở thành một phần không thể thiếu trong các hệ thống bảo mật thông tin. Bằng cách sử dụng một chuỗi các vòng lặp mã hóa phức tạp, AES có khả năng biến dữ liệu ban đầu thành dữ liệu đã mã hóa một cách an toàn và không thể đoán trước. Điều này đảm bảo rằng người dùng có thể chia sẻ thông tin mà không lo lắng về việc bị lộ thông tin cá nhân hay tài liệu quan trọng.

Không chỉ đơn giản là một công cụ bảo mật, AES còn phản ánh sự tiến bộ và sự phát triển của con người trong việc tạo ra các giải pháp bảo mật tiên tiến. Việc phát triển AES yêu cầu sự kết hợp của kiến thức toán học, khoa học máy tính và công nghệ thông tin, và nó là một minh chứng cho sự nỗ lực không ngừng của con người trong việc đối phó với các thách thức về bảo mật thông tin.

Ngoài ra, ý nghĩa của AES còn nằm ở việc đảm bảo an toàn thông tin trong xã hội ngày nay. Trong thế giới mạng hiện đại, dữ liệu trở thành một tài nguyên quý giá và việc bảo vệ thông tin cá nhân, doanh nghiệp và quốc gia trở nên càng quan trọng hơn bao giờ hết. AES đóng vai trò quan trọng trong việc tạo ra một môi trường an toàn hơn cho việc trao đổi thông tin và góp phần vào sự phát triển bền vững của xã hội thông tin.

Tóm lại, AES không chỉ là một công cụ mã hóa thông tin, mà còn là biểu tượng cho sự tiến bộ và quan trọng của việc bảo vệ thông tin trong thời đại kỹ thuật số. Đối với mọi người, AES không chỉ là một công nghệ, mà còn là một sự đảm bảo cho sự riêng tư và an toàn trực tuyến.

Tóm lại, AES không chỉ là một công cụ mã hóa thông tin, mà còn là một biểu tượng cho sự tự do và quyền riêng tư trực tuyến. Với ảnh hưởng sâu sắc đến cuộc sống hàng ngày của tôi và sự tự tin trong việc sử dụng internet, AES đã trở thành một phần không thể tách rời của cuộc sống và công việc của tôi.

## Công cụ sử dụng

Để thực hiện bài tập lớn này, chúng em sử dụng visual studio code - một IDE được phát triển bởi Microsoft và được nhiều người sử dụng bởi khả năng hỗ trợ đa ngôn ngữ lập trình của IDE này.

Cụ thể, Microsoft Visual Studio IDE hỗ trợ lên đến 36 ngôn ngữ lập trình khác nhau, bao gồm JavaScript, TypeScript, C, C++,...

Trước hết, Visual Studio cung cấp một loạt các tính năng mạnh mẽ để hỗ trợ việc phát triển phần mềm, từ việc soạn thảo mã nguồn đến gỡ lỗi và triển khai ứng dụng. Với giao diện người dùng thân thiện và dễ sử dụng, Visual Studio giúp tạo điều kiện làm việc hiệu quả và tiết kiệm thời gian cho nhà phát triển.

Thứ hai, Visual Studio có khả năng tích hợp tốt với ngôn ngữ lập trình C#, một trong những ngôn ngữ phổ biến được sử dụng để triển khai thuật toán AES. Việc có sẵn các công cụ và tính năng hỗ trợ cho C# trong Visual Studio giúp nhà phát triển dễ dàng viết và kiểm tra mã nguồn, tăng hiệu suất làm việc và giảm thời gian triển khai.

Ngoài ra, Visual Studio cung cấp các công cụ mạnh mẽ để gỡ lỗi và kiểm tra hiệu suất ứng dụng, giúp nhà phát triển phát hiện và sửa lỗi một cách dễ dàng và nhanh chóng. Điều này rất quan trọng khi triển khai thuật toán AES, nơi sự chính xác và đáng tin cậy của mã nguồn là rất quan trọng.

Chúng em chọn ngôn ngữ C# để thực hiện, bởi đây là học phần chúng em đã được học và với mong muốn ứng dụng thực hành những gì đã học để có thể hoàn thiện hơn nữa

Đầu tiên, C# là một ngôn ngữ lập trình mạnh mẽ và linh hoạt, được phát triển bởi Microsoft, với cú pháp dễ hiểu và dễ học. Với cú pháp gần gũi với ngôn ngữ tự nhiên và cung cấp nhiều tính năng hiện đại, C# là một lựa chọn lý tưởng cho việc triển khai các thuật toán phức tạp như AES.

Thứ hai, C# được tích hợp chặt chẽ với framework .NET của Microsoft, cung cấp một bộ thư viện phong phú và mạnh mẽ cho việc phát triển phần mềm. Trong trường hợp triển khai thuật toán AES, framework .NET cung cấp các lớp và phương thức hỗ trợ để thực hiện việc mã hóa và giải mã dữ liệu một cách dễ dàng và hiệu quả.

Thứ ba, C# là một ngôn ngữ phổ biến trong cộng đồng phát triển phần mềm, điều này có nghĩa là có nhiều tài liệu, hướng dẫn và hỗ trợ từ cộng đồng phát triển. Khi gặp phải vấn đề hoặc cần tìm kiếm các giải pháp, việc có sẵn tài nguyên và hỗ trợ từ cộng đồng sẽ giúp tiết kiệm thời gian và nỗ lực trong quá trình triển khai thuật toán AES.

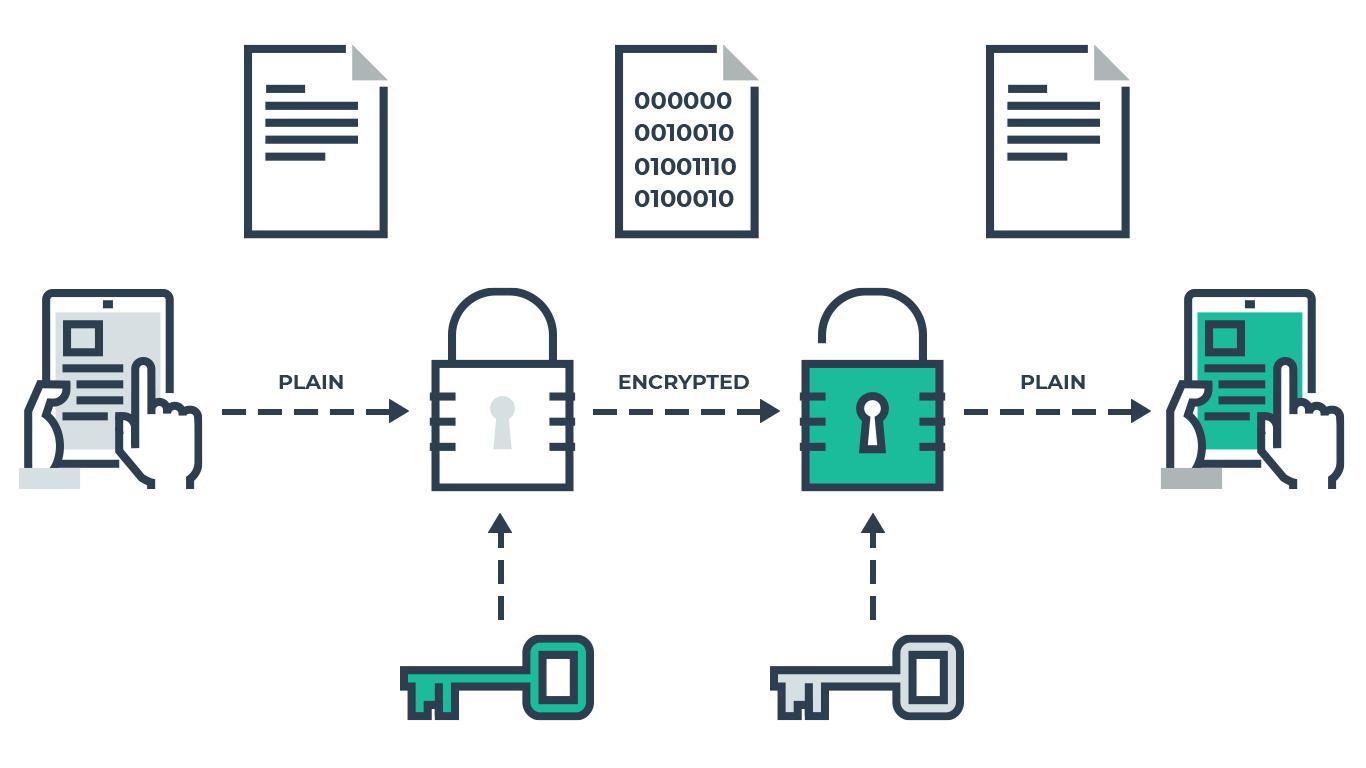
Cuối cùng, việc sử dụng C# để triển khai thuật toán AES cũng tạo ra sự liên kết chặt chẽ với hệ sinh thái công nghệ của Microsoft, giúp tích hợp dễ dàng với các ứng dụng và dịch vụ khác của Microsoft, như SQL Server, Azure, và nhiều hơn nữa.

Tóm lại, việc chọn ngôn ngữ C# để triển khai thuật toán AES là một lựa chọn có lý do và hợp lý, nhờ vào tính linh hoạt, sức mạnh, sự hỗ trợ từ framework .NET, và sự phổ biến trong cộng đồng phát triển phần mềm.

# Chương 2: Giải quyết vấn đề

## Đầu vào: tệp tin (hình ảnh, văn bản,..)

Hệ thống bảo mật được xây dựng để làm việc với nhiều loại định dạng tệp tin khác nhau như hình ảnh (JPEG, PNG), văn bản (PDF, DOCX), file âm thanh (MP3, WAV), video (MP4, AVI), và nhiều định dạng khác. Mục tiêu chính là bảo vệ tính bí mật và toàn vẹn của dữ liệu trong các tệp tin này khi chúng được truyền tải, lưu trữ hoặc chia sẻ.



### Hình 2.1 Hình mô tả hệ thống đầu vào của AES

VD: file inputatbm.dox

Link: https://docs.google.com/document/d/1ZrRmXr\_aikFRmwJH4l6VbyvBgKf80VTM/edit?usp=sharing&ouid=116139698394634682157&rtpof=true&sd=true

## Cơ sở lý thuyết

AES là một thuật toán mã hóa đối xứng được sử dụng trong nhiều ứng dụng bảo mật. Sau đây là một số ứng dụng phổ biến của AES:

Hệ mã hóa này được sử dụng rộng rãi để mã hóa các thông tin quan trọng, đảm bảo tính bảo mật và chống lại các cuộc tấn công mạng. AES được sử dụng trong các giao thức bảo mật như SSL/TLS, SSH, IPSec, Wi-Fi Protected Access (WPA) và Virtual Private Networks (VPN).

A blue shield with a key and a pen

Description automatically generated

### Hình 2.2: Tính ứng dụng của AES

Nó còn giúp thực hiện mã hóa dữ liệu trong các thiết bị lưu trữ như [USB](https://fptshop.com.vn/phu-kien/usb-o-cung), [ổ cứng](https://fptshop.com.vn/linh-kien/o-cung) di động và [thẻ nhớ](https://fptshop.com.vn/phu-kien/the-nho), đảm bảo tính riêng tư và chống lại việc truy cập trái phép vào các thông tin quan trọng. AES cũng được sử dụng để bảo vệ phần mềm khỏi việc sao chép trái phép hoặc truy cập trái phép. Nhiều ứng dụng mã hóa phần mềm sử dụng AES để bảo vệ các thông tin nhạy cảm và đảm bảo tính bảo mật của phần mềm.

**Ưu điểm của thuật toán AES**

AES được sử dụng phổ biến, có tính ứng dụng cao với nhiều ưu điểm vượt trội:

* **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.

Bên cạnh những ưu điểm kể trên thì thuật toán AES cũng có một số hạn chế như:

* 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.

## AES hoạt động như thế nào?

Thuật toán AES khá phức tạp, được mô tả khái quát gồm 3 bước như sau:

* 1 Vòng khởi tạo chỉ gồm phép AddRoundKey
* Nr -1 Vòng lặp gồm 4 phép biển đổi lần lượt: SubBytes, ShiftRows, MixColumns, AddRoundKey.
* 1 Vòng cuối gồm các phép biến đổi giống vòng lặp và không có phép MixColumns.

A screenshot of a computer program

Description automatically generated

### Hình 2.3: Mô hình hoạt động của AES

AES hoạt động trên các block dữ liệu có kích thước 128 bit và có thể được cấu hình để mã hoá các block dữ liệu với các kích thước khác nhau như 192 bit hoặc 256 bit. Thuật toán này sử dụng một khóa có độ dài 128, 192 hoặc 256 bit để thực hiện quá trình mã hoá và giải mã.

Để hiểu cách hoạt động của thuật toán AES, chúng ta có thể phân tích quá trình mã hoá trong các bước sau:

Vòng Khởi Tạo (Initial Round):

* Trong bước này, dữ liệu đầu vào được thực hiện một số phép biến đổi đơn giản, bao gồm:
* AddRoundKey: Mỗi byte trong block dữ liệu sẽ được kết hợp với một byte tương ứng trong khóa bằng phép toán XOR. Điều này tạo ra một block dữ liệu mới chứa sự kết hợp của dữ liệu ban đầu và khóa.

Vòng Lặp (Rounds): Trong mỗi vòng lặp (trừ vòng cuối), block dữ liệu trải qua một chuỗi các phép biến đổi:

* SubBytes: Mỗi byte trong block dữ liệu sẽ được thay thế bằng một giá trị mới từ một bảng tham chiếu được gọi là S-box. S-box này được thiết kế sao cho quá trình này là một hàm phi tuyến, tăng cường độ phân tán của dữ liệu.

A screenshot of a computer

Description automatically generated  
Hình 2.4: mô tả phép SubBytes

* ShiftRows: Các hàng trong block dữ liệu được dịch chuyển sang bên trái. Hàng đầu tiên không thay đổi, hàng thứ hai dịch chuyển 1 byte, hàng thứ ba dịch chuyển 2 byte, và hàng thứ tư dịch chuyển 3 byte. Điều này tạo ra sự phân tán và đảo lộn dữ liệu trong block.

A red background with white text

Description automatically generated

### Hình 2.5: mô tả phép ShiftRows

* MixColumns: Trong bước này, các cột trong block dữ liệu được biến đổi tuyến tính thông qua một ma trận cụ thể. Mỗi cột được biến đổi thành một giá trị mới, giúp tăng cường độ phân tán và phức tạp hóa dữ liệu trong block.

A yellow background with black and white numbers

Description automatically generated

### Hình 2.6: mô tả phép MixColumns

* AddRoundKey: Tương tự như trong vòng khởi tạo, block dữ liệu được kết hợp với một phần của khóa sử dụng phép toán XOR.

A screenshot of a computer

Description automatically generated

### Hình 2.7: mô tả phép AddRoundKey

Vòng Cuối (Final Round):

Trong vòng cuối, các bước biến đổi tương tự như trong vòng lặp, nhưng không có phép MixColumns. Điều này giữ cho quá trình giải mã đảm bảo sự ngược đảo hoàn toàn của quá trình mã hoá.

A diagram of a function

Description automatically generated

### Hình 2.8: Mô hình mở rộng khóa

# Chương 3: Giới thiệu chương trình máy tính

## Giới thiệu mã hóa

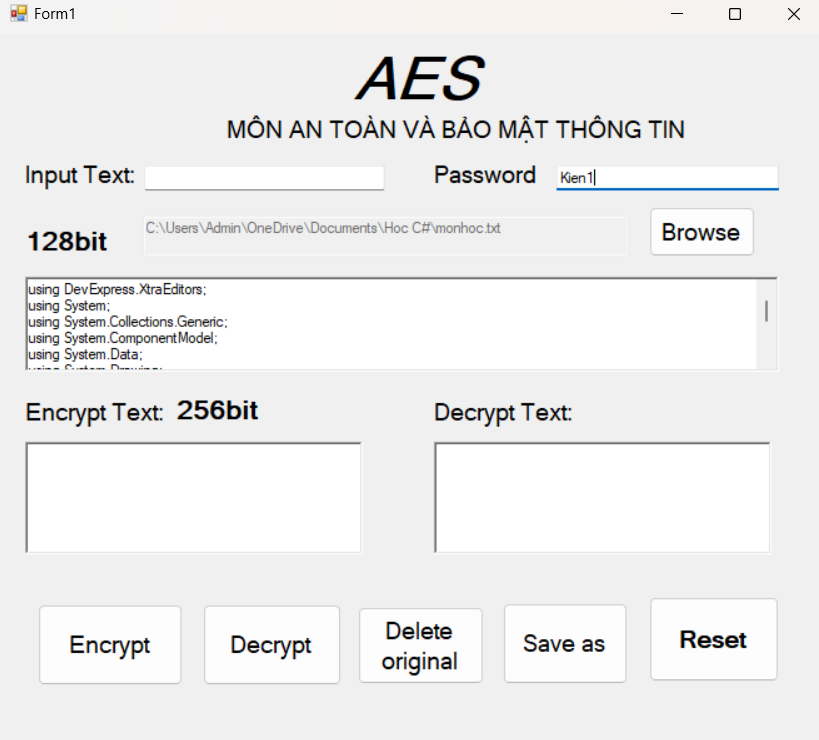
A close-up of a text

Description automatically generated

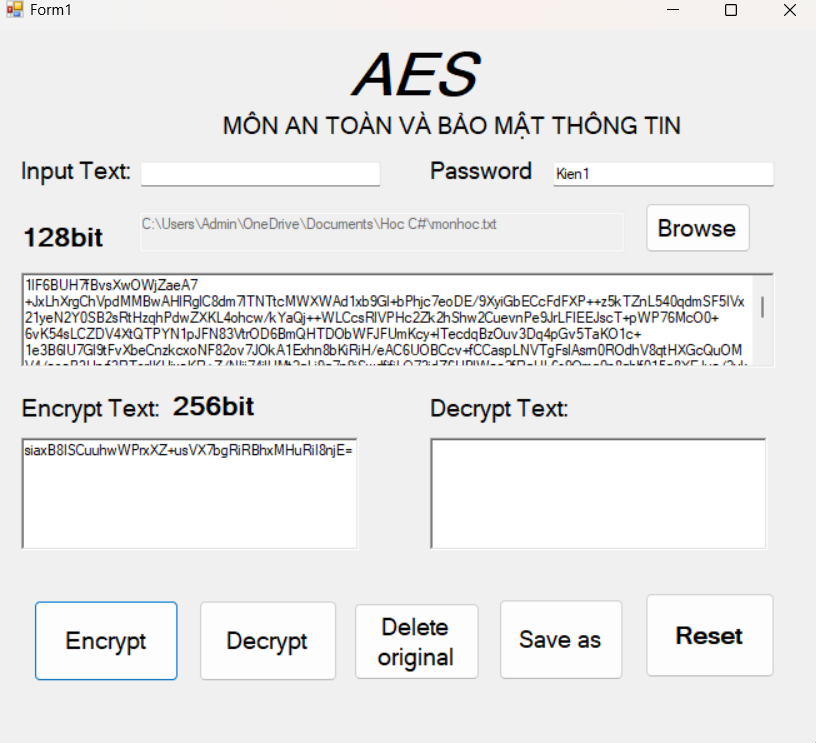
### Hình 3.1: Ảnh sau khi mã hóa file đầu vào của thuật toán AES

Link: https://docs.google.com/document/d/1ITn5fV7e3fHbvTfnGIN2kN606tgU\_W6t/edit?usp=sharing&ouid=116139698394634682157&rtpof=true&sd=true

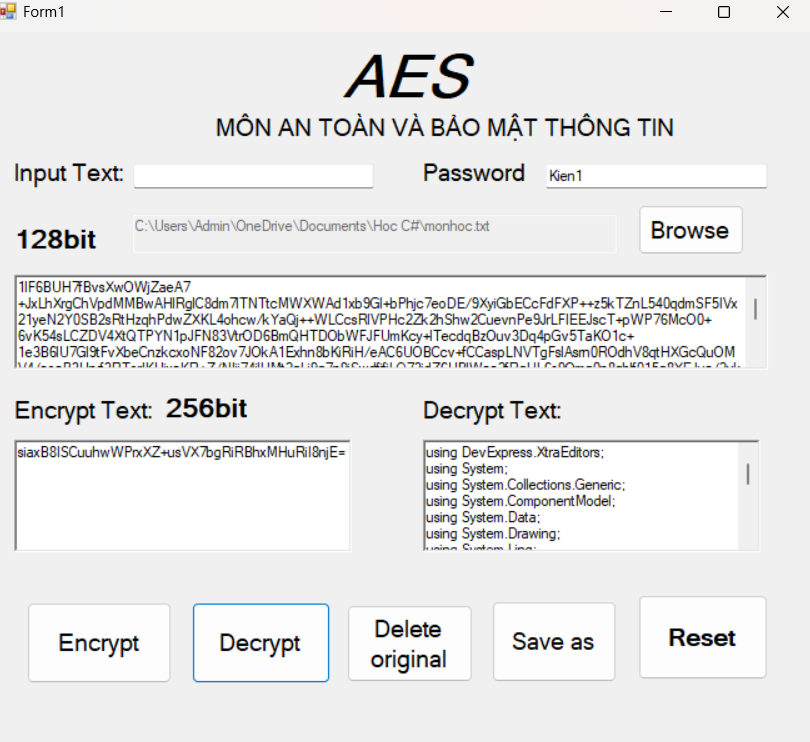
## Hình ảnh



### Hình 3.2: Bước 1 chọn file và đặt pass



### Hình 3.2: Bước 2 ấn vào encrypt để mã hóa



### Hình 3.2: Bước 3 ấn vào decrypt để giải mã hóa và trở về giống bước 1 ( là để chọn file)

## Kết luận

Trong báo cáo này, chúng em đã chứng minh rằng việc sử dụng AES để mã hoá tập tin là một phương pháp hiệu quả để bảo vệ dữ liệu trước các mối đe dọa mạng. Cơ chế mã hoá mạnh mẽ của AES đã giúp tăng cường tính bảo mật của hệ thống và bảo vệ thông tin quan trọng của người dùng khỏi việc truy cập trái phép.

Tuy nhiên, cũng cần lưu ý rằng tính bảo mật chỉ là một phần của vấn đề. Sự tiện lợi và khả dụng cũng là yếu tố quan trọng cần xem xét khi triển khai các giải pháp bảo mật. Điều này đặt ra thách thức trong việc cân bằng giữa tính bảo mật và tính tiện lợi.

Việc nghiên cứu và triển khai hệ thống bảo mật tập tin sử dụng AES không chỉ giúp chúng ta hiểu rõ hơn về quy trình bảo mật thông tin mà còn nhấn mạnh tầm quan trọng của việc duy trì tính toàn vẹn và bảo mật của dữ liệu trong một môi trường số hóa ngày càng phức tạp. Chúng ta hy vọng rằng nghiên cứu này sẽ là một bước đầu tiên trong việc xây dựng các giải pháp bảo mật hiệu quả và linh hoạt cho tương lai.

## Bài học rút ra

Từ việc nghiên cứu và triển khai hệ thống bảo mật sử dụng AES, chúng ta có thể rút ra một số bài học quan trọng:

Quan trọng của mã hoá: Việc sử dụng mã hoá mạnh mẽ như AES là yếu tố quan trọng để bảo vệ dữ liệu trước các mối đe dọa mạng.

Cân bằng giữa bảo mật và tiện lợi: Cần phải cân nhắc kỹ lưỡng giữa tính bảo mật và tính tiện lợi khi thiết kế và triển khai các hệ thống bảo mật.

Liên tục cải thiện: Bảo mật là một quá trình liên tục. Chúng ta cần liên tục cải thiện và cập nhật hệ thống để đối phó với các mối đe dọa mới.

Trong một thế giới mạng liên kết, việc hợp tác và chia sẻ kiến thức là rất quan trọng. Chia sẻ kinh nghiệm và học hỏi từ cộng đồng an toàn thông tin có thể giúp chúng ta nâng cao hiểu biết và tăng cường khả năng đối phó với các mối đe dọa mạng.

Trong tương lai, có thể nghiên cứu và phát triển các phương pháp mới để cải thiện hiệu suất và tính khả dụng của hệ thống bảo mật tập tin sử dụng AES. Cũng cần tiếp tục theo dõi và nghiên cứu các mối đe dọa mới nhằm đảm bảo rằng hệ thống của chúng ta luôn đáp ứng được những thách thức mới trong lĩnh vực an toàn thông tin

# Danh mục tham khảo

[1] <https://laptrinhvb.net/bai-viet/chuyen-de-csharp/Huong-dan-ma-hoa-va-giai-ma-su-dung-thuat-toan-AES-/7c184a5c54076c99.html?fbclid=IwAR003jvj_B6E4excQb6Tz0xbYMCzwtF7oD4D9Os2Hd_FgGQh-4BQT7g3Mi8>

[2]<https://hoanghamobile.com/tin-tuc/aes/#:~:text=AES%20ho%E1%BA%A1t%20%C4%91%E1%BB%99ng%20tr%C3%AAn%20c%C3%A1c,tr%C3%ACnh%20nghi%C3%AAn%20c%E1%BB%A9u%20k%E1%BB%B9%20l%C6%B0%E1%BB%A1ng>.

[3] <https://viettelidc.com.vn/tin-tuc/tieu-chuan-ma-hoa-du-lieu-aes-la-gi-va-cac-che-do-hoat-dong-cua-aes-phan-1>

[4] <https://viblo.asia/p/tim-hieu-thuat-toan-ma-hoa-khoa-doi-xung-aes-gAm5yxOqldb>

[5] <https://www.youtube.com/watch?v=S6zlQXj35rI>