**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH**

**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN**

KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG



Môn học : **AN TOÀN MẠNG MÁY TÍNH**

**BÁO CÁO CUỐI KỲ**

**ĐỀ TÀI : AES VÀ DES**

Lớp : **NT101.N12.MMCL**

Giảng viên hướng dẫn : **TÔ NGUYỄN NHẬT QUANG**

**Nhóm 2**

Nguyễn Mạnh Cường 20520421

Lê Quang Minh 20520245

Nguyễn Trần Đức Anh 20520932

Hoàng Văn Anh Đức 20520890

*Thành phố Hồ Chí Minh*

*Ngày 1 tháng 4 năm 2022*

# **Mục lục**

[**Mục lục** 2](#_Toc100306909)

[**I.** **GIỚI THIỆU ĐỀ TÀI** 3](#_Toc100306910)

[**a.** **Sơ lược về trò chơi** 3](#_Toc100306911)

[**b.** **Cách chơi** 3](#_Toc100306912)

[**c.** **Hướng phát triển** 3](#_Toc100306913)

[**II.** **CHI TIẾT ĐỀ TÀI** 3](#_Toc100306914)

[**a.** **Mô tả ứng dụng** 3](#_Toc100306915)

[**b.** **Mô hình phân rã** 4](#_Toc100306916)

[**c.** **Giao diện ứng dụng** 4](#_Toc100306917)

[**d.** **Network Stack** 8](#_Toc100306918)

[**III.** **PHÂN CÔNG CÔNG VIỆC** 9](#_Toc100306919)

1. **BÁO CÁO CHI TIẾT**
   1. **Mã hóa đối xứng (symmetric key encryption)**

* Ở phương pháp mã hóa đối xứng, chìa khóa để mã hóa và giải mã là như nhau nên người ta mới gọi là đối xứng, tiếng Anh là symmetric. Theo một số tài liệu thì mã hóa đối xứng là giải pháp được sử dụng nhất phổ biến hiện nay
* Giả sử ta cần mã hóa một tập tin để gửi cho người khác, thì quy trình sẽ như sau:
  + Dùng giải thuật ngẫu nhiên mã hóa + key để mã hóa dữ liệu gửi đi.
  + Bằng cách nào đó, key của người gửi sẽ được gửi đến cho người nhận, có thể là giao trước hoặc sau khi mã hóa file đều được.
  + Khi người nhận nhận được dữ kiệu, họ sẽ dùng key này để giải mã dữ liệu để có được dữ liệu chuẩn.
* Vấn đề ở đây, đó là mình phải làm sao để chuyển khóa cho bạn một cách an toàn. Nếu khóa này bị lộ ra thì bất kì ai cũng có thể xài thuật toán nói trên để giải mã tập tin, như vậy thì tính bảo mật sẽ không còn nữa.
  1. **DES**
     1. **Sơ lược về thuật toán DES**
* **Data Encryption Standard (DES) hay còn được gọi là Tiêu chuẩn mã hóa dữ liệu bằng phương pháp khóa đối xứng**. Vào đầu những năm 1970 DES được nghiên cứu và công bố bởi các nhà nghiên cứu của IBM.
* Bắt đầu sử dụng rộng rãi vào năm 1977 trước khi bị thay thế bởi AES và năm 2001
* Dữ liệu được mã hóa theo từng khối 64 bit và sử dụng 56 bit khóa
* Kích thước của khối mã hóa bằng kích thước khối ban đầu
  + 1. **Nguyên lý hoạt động**
* **Key mật mã**: DES sử dụng phương pháp mật mã khối, điều này có nghĩa là mỗi khối dữ liệu sẽ được áp dụng bởi một key mật mã và thuật toán. DES sẽ nhóm plain text (văn bản thuần túy) thành các khối 64 bit. Bằng cách kết hợp và hoán vị các khối của plain text sẽ được chuyển đổi thành Ciphertext (văn bản đã mã hóa).
* **Vòng mã hóa**: Dữ liệu sẽ được DES mã hóa 16 lần với bốn chế độ khác nhau. Từng khối riêng lẻ sẽ được mã hóa hoặc bắt buộc các khối mật mã phải phụ thuộc vào những khối trước đó. Riêng về giải mã thì đơn giản chỉ là nghịch đảo của mã hóa, tức là quy trình thực hiện tương tự nhưng đảo ngược thứ tự các key.
* **Phím 64 bit**: Thực tế cho thấy mặc dù DES sử dụng key 64 bit nhưng có 8 bit trong số đó đã được dùng để kiểm tra chẵn lẻ. Vì lẽ đó là key hiệu dụng chỉ có 56 bit.
* **Thay thế và hoán vị**: Đây là hai quy trình mà Ciphertext phải trải qua trong quá trình mã hóa.
* **Khả năng tương thích ngược** (tương thích với phiên bản cũ): Trong một số trường hợp DES cũng cung cấp khả năng này.

Diagram, schematic

Description automatically generated

* + 1. **Ưu điểm và nhược điểm của DES**

|  |  |
| --- | --- |
| **Ưu Điểm** | **Nhược Điểm** |
| * Độ an toàn của DES được thể hiện qua các yếu tố: số vòng mã, độ dài khóa, cấu trúc hàm thay thế * Sử dụng 56 bit khóa ⬄ 7.2\*10^6 khóa nên hoạt động rất hiệu quả với công nghệ ở thời điểm trước thập niên 90 | * Chỉ sử dụng 56 bit khóa nên số lượng khóa không đủ mạnh để chống lại brute-force của các máy tính ở thời điểm hiện tại |

* + 1. **Ứng dụng của DES ở thời điểm hiện tại**
* DES và 3DES là các tiêu chuẩn đã ngừng hoạt động nhưng người dùng vẫn có thể dùng chúng và đồng nghĩa với đó là phải chấp nhận rủi ro. Trước đây DES được dùng ở các giao dịch tài chính của chính phủ Mỹ thì bây giờ nó chỉ được áp dụng cho các dịch vụ tài chính và các ngành công nghiệp khác.
* Tóm lại DES vẫn được dùng ở mức hạn chế. Ngày nay nó được sử dụng để các chuyên gia giảng dạy, đào tạo về mật mã. Trong học thuật công nghệ này vẫn có giá trị để chứng minh một số vấn đề liên quan đến mật mã kỹ thuật số.
  + 1. **Các chế độ thao tác mã khối**
* **Chế độ sách mã điện tử ECB (Electronic Code Book):** ECB là chế độ mã hóa từng khối bit độc lập. Với cùng một khóa mã K, mỗi khối plaintext ứng với một giá trị ciphertext cố định và ngược lại: Ci = Ek(Mi); Mi = Dk(Ci), trong đó Ek và Dk là các phép mã hoá và giải mã theo khoá mật K.

Diagram

Description automatically generated

* Ưu điểm:
  + Thiết kế phần cứng đơn giản. Vấn đề cần quan tâm chính là thiết kế logic cho thuật toán mã hóa.
  + Lỗi bit không bị lan truyền. Nếu lỗi bit xuất hiện trên một ciphertext của một khối dữ liệu thì nó chỉ ảnh hưởng đến việc giải mã khối dữ liệu đó chứ không ảnh hưởng đến việc giải mã khác khối dữ liệu khác.
  + Có thể thực hiện mã hóa/giải mã song song (parallel) nhiều khối dữ liệu cùng lúc. Điều này giúp tăng tốc độ xử lý trong các hệ thống đòi hỏi mã hóa/giải mã tốc độ cao.
* Nhược điểm:
  + Khả năng bảo mật kém. Do giá trị plaintext và ciphertext được ánh xạ độc lập một-một nên thông tin mã hóa dễ bị sửa đổi bằng cách như xóa bớt khối dữ liệu, chèn thêm khối dữ liệu, hoán đổi vị trí khối dữ liệu để làm sai lệch thông tin tại nơi nhận.
* **Chế độ xích liên kết khối mã CBC (Cipher block Chaining):** Trong chế độ này, đầu tiên người ta tạo ra một xâu nhị phân 64 bit được gọi là véc-tơ khởi đầu và thông báo cho nhau. Trong bước đầu tiên khối dữ liệu rõ M1 được cộng với véc-tơ khởi đầu theo phép cộng bit, kết quả nhận được sẽ được biến đổi qua các phép mã hóa để được đầu ra là khối mã C1. Ở các bước sau, mỗi khối Mi của bản rõ được cộng theo modulo 2 với bản mã trước đó Ci-1 và được mã hoá:

Ci = Ek(Mi r Ci-1)

Mi =Dk(Ci) r Ci-1

Diagram

Description automatically generated

* Ưu điểm:
  + Khả năng bảo mật cao hơn ECB. Ciphertext của một khối dữ liệu plaintext có thể khác nhau cho mỗi lần mã hóa vì nó phụ thuộc vào IV hoặc giá trị mã hóa (ciphertext) của khối dữ liệu liền trước.
  + Quá trình giải mã (mã hóa nghịch) vẫn có thể thực hiện song song nhiều khối dữ liệu.
* Nhược điểm
  + Thiết kế phần cứng phức tạp hơn ECB ngoài logic thực thi thuật toán mã hóa, người thiết kế cần thiết kế thêm:
  + Logic quản lý độ dài chuỗi dữ liệu sẽ được mã hóa, cụ thể là số lượng khối dữ liệu trong chuỗi dữ liệu.
  + Bộ tạo giá trị ngẫu nhiên cho IV.
  + Lỗi bit bị lan truyền. Nếu một lỗi bit xuất hiện trên ciphertext của một khối dữ liệu thì nó sẽ làm sai kết quả giải mã của khối đữ liệu đó và khối dữ liệu tiếp theo.
  + Không thể thực thi quá trình mã hóa song song vì xử lý của khối dữ liệu sau phụ thuộc vào ciphertext của khối dữ liệu trước, trừ lần mã hóa đầu tiên.
* **Chế độ mã liên kết ngược CFB (Cipher Feed Back):** CFB là chế độ mã hóa mà ciphertext của lần mã hóa hiện tại sẽ được phản hồi (feedback) đến đầu vào của lần mã hóa tiếp theo. Nghĩa là, ciphertext của lần mã hóa hiện tại sẽ được sử dụng để tính toán ciphertext của lần mã hóa kế tiếp. Chế độ này này khác với chế độ CBC, tại bước đầu tiên véc-tơ khởi đầu được mã hóa bằng Ek rồi cộng theo modulo 2 với khối rõ. Kết quả thu được lại làm véc-tơ khởi đầu cho bước tiếp theo, rồi lại thực hiện tương tự chế độ CBC:

Ci = Mi r Ek(Ci-1)

Mi =Ci r Dk(Ci-1)

A picture containing text, receipt, screenshot

Description automatically generated

* So sánh với chế độ CBC, chế độ CFB có những điểm khác biệt sau đây:
  + Thuật toán mã hóa không áp dụng trực tiếp trên plaintext mà dùng để biển đổi một khối dữ liệu sinh ra từ IV và ciphertext
  + Số lượng bit dữ liệu được mã hóa, giải mã có thể nhỏ hơn hoặc bằng số lượng bit mà thuật toán mã hóa hỗ trợ, 1 ≤ s ≤ b
* Ưu điểm:
  + Khả năng bảo mật cao hơn ECB. Ciphertext của một khối dữ liệu plaintext có thể khác nhau cho mỗi lần mã hóa vì nó phụ thuộc vào IV hoặc giá trị mã hóa (ciphertext) của khối dữ liệu liền trước.
  + Quá trình giải mã (mã hóa nghịch) vẫn có thể thực hiện song song nhiều khối dữ liệu.
  + Tùy biến được độ dài khối dữ liệu mã hóa, giải mã thông qua thông số s
* Nhược điểm:
  + Thiết kế phần cứng phức tạp hơn CBC. Ngoài những thành phần logic như CBC, CFB cần thêm logic để chọn số bit cần được xử lý nếu s là thông số cấu hình được.
  + Lỗi bit bị lan truyền. Nếu một lỗi bit xuất hiện trên ciphertext của một khối dữ liệu thì nó sẽ làm sai kết quả giải mã của khối đữ liệu đó và khối dữ liệu tiếp theo.
  + Không thể thực thi quá trình mã hóa song song vì xử lý của khối dữ liệu sau phụ thuộc vào ciphertext của khối dữ liệu trước, trừ lần mã hóa đầu tiên
* **Chế độ đầu ra liên kết ngược OFB (Output Feedback):** Thực chất của chế độ OFB là tạo ra khóa dòng rồi cộng theo modulo 2 với bản rõ. Khóa dòng được tạo như sau: Đầu tiên lấy véc-tơ khởi đầu s0 rồi mã hóa qua phép mã khối Ek được s1. Tiếp đó, s1 lại được mã hóa qua Ek để được s2,.. và cứ thế thực hiện cho đến khi tạo được khóa dòng có độ dài bằng dữ liệu cần mã.

Diagram

Description automatically generated

* Chế độ OFB có những đặc điểm cần chú ý như sau:
  + Thuật toán mã hóa không áp dụng trực tiếp trên plaintext mà dùng để biển đổi một khối dữ liệu sinh ra từ IV và khối ngõ ra của lần mã hóa trước đó. Điểm này tương tự với CFB.
  + OFB khác với CFB là nó xử lý trên một khối dữ liệu với độ dài bit đầy đủ như thuật toán mã hóa quy định chứ không xử lý trên một phần hay một vài bit của khối dữ liệu.
* Ưu điểm:
  + Khả năng bảo mật cao hơn ECB. Ciphertext của một khối dữ liệu plaintext có thể khác nhau cho mỗi lần mã hóa vì nó phụ thuộc vào IV hoặc khối ngõ ra của lần mã hóa trước đó.
  + Lỗi bit không bị lan truyền. Khi một lỗi bit xuất hiện trên một ciphertext, nó chỉ ảnh hưởng đến kết quả giải mã của khối dữ liệu hiện tại
  + Thiết kế phần cứng đơn giản hơn CFB.
* Nhược điểm:
  + Không thể thực hiện mã hóa/giải mã song song nhiều khối dữ liệu vì lần mã hóa/giải mã sau phụ thuộc vào khối ngõ ra của lần mã hóa/giải mã liền trước nó.
  1. **AES**
     1. **Sơ lược vể thuật toán AES**
* **Advanced Encryption Standard (AES) hay còn được gọi là tiêu chuẩn mã hóa nâng cao theo phương pháp mật mã khối**. Với ưu thế bảo mật cao nó đã được chính phủ Hoa Kỳ lựa chọn để bảo vệ [dữ liệu](https://bkhost.vn/blog/data-du-lieu/), thông tin cho các tổ chức, doanh nghiệp mà người dùng.
* Các tác vụ của AES được thực hiện ở cả phần cứng và phần mềm trên nhiều thiết bị để [mã hóa](https://bkhost.vn/blog/ma-hoa/) dữ liệu nhạy cảm. Sự có mặt của nó đã góp phần bảo đảm an toàn cho máy tính của chính phủ, [an ninh mạng](https://bkhost.vn/blog/an-ninh-mang-cyber-security/) và tạo một rào chắn vững chắc để bảo vệ dữ liệu
* Hiện nay nhiều cơ quan chính phủ trên thế giới quy định tài liệu khi được gửi qua mạng phải bằng thuật toán AES
* Thuật toán AES có thể dùng nhiều kích thước ô nhớ khác nhau để mã hóa dữ liệu, thường thấy là 128-bit và 256-bit, có một số lên tới 512-bit và 1024-bit. Kích thước ô nhớ càng lớn thì càng khó phá mã hơn, bù lại việc giải mã và mã hóa cũng cần nhiều năng lực xử lý hơn.
  + 1. **Nguyên lý hoạt động**
* AES gồm ba mật mã khối AES-128, AES-192, AES-256 tương ứng với độ dài của key là 128 bit, 192 bit và 256 bit. Số vòng của key khác nhau, cụ thể 10 vòng cho 128 bit, 12 vòng cho 192 bit và 14 vòng cho 256 bit. Mỗi vòng đều thực hiện ba bước thay thế, biến đổi và hòa trộn khối plain text (văn bản thuần túy) đầu vào để biến nó thành Ciphertext (văn bản đã mã hóa)
* 4 phép toán trong AES
  + Subtitles-bytes (sub): Phép toán hoán vị các byte. Dùng để chống lại thám mã và các dạng tấn công toán học khác
  + Shift-row (shr): Phép toán tuyến tính tạo ra sự khuếch tán
  + Mix-column (mic): Hoạt đọng cơ bản cũng để tạo ra sự khuếch tán
  + Add round key (ark)

Diagram

Description automatically generated with medium confidence

* + 1. **Các tiêu chí cần có ở AES**
* **Bảo vệ**: Đây là một trong những tính năng hàng đầu AES cần phải có để đánh bại các đối thủ khác. Nó phải có khả năng chống lại các cuộc tấn công mạnh, quy mô lớn.
* **Chi phí**: AES mở ra nhiều cơ hội cho người dùng bằng cách phát hành trên toàn cầu và miễn phí bản quyền.
* **Khả năng thực hiện**: Linh hoạt, phù hợp và đơn giản chính là 3 yếu tố quan trọng hội tụ ở AES để đáp ứng trọn vẹn nhu cầu của người dùng.
  + 1. **Ưu nhược điểm của AES**

|  |  |
| --- | --- |
| **Ưu Điểm** | **Nhược Điểm** |
| An toàn tuyệt đối nếu được triển khai đúng quy trình | các key mã hóa AES phải được bảo vệ bằng nhiều cách khác nhau như dùng [mật khẩu](https://bkhost.vn/blog/password/) mạnh, xác thực, tường lửa hay phần mềm chống độc hại |

* 1. **Phân biệt AES và DES**
* DES , chức năng chính của nó là mang tới một tiêu chuẩn chung an toàn cho các hệ thống của chính phủ và tạo điều kiện để các hệ thống liên kết nhanh chóng với nhau.
* Trong nhiều thập niên DES trở thành trụ cột để bảo vệ an ninh quốc gia cho Hoa Kỳ. Mãi cho đến năm 1999 key 56 bit của thuật toán này bị phá vỡ bởi các nhà nghiên cứu. Năm 2000 AES đã được nghiên cứu thành công và trở thành giải pháp thay thế cho DES. Mặc dù bị “soán ngôi” nhưng trong một số trường hợp DES vẫn được sử dụng.
* Cả AES và DES đều là mật mã khối đối xứng nhưng AES mang đến hiệu quả cao bởi độ dài key mà nó sở hữu. Đem lên bàn cân có thể thấy các key 128 bit, 192 bit và 256 bit của AES mạnh gấp nhiều lần so với 56 bit của DES. Bên cạnh đó mã hóa AES cũng nhanh hơn DES.
  1. **Demo thuật toán mã hóa AES,DES**
* Chức năng & ngữ cảnh ứng dụng :
  + DES : ứng dụng cho các văn bản trong giao dịch ngân hàng sử dụng các tiêu chuẩn được hiệp hội các ngân hàng Mỹ phát triển. DES được sử dụng để mã hoá các số nhận dạng cá nhân (Pins) và các văn bản về tài khoản được máy thu ngân tự động thực hiện (ATMs) . *Trong phần demo thì DES dùng để mã hóa 1 đoạn thông điệp ngắn*
  + AES : bao gồm tự mã hóa ổ đĩa, mã hóa lưu trữ, mã hóa cơ sở dữ liệu... .*Trong phần demo là mã hóa tất cả các loại file , vd : .txt , .doc,…*
* Ngôn ngữ lập trình : C#
* Thư viện sử dụng :

using System;

using System.Collections.Generic;

using System.ComponentModel;

using System.Data;

using System.Drawing;

using System.Linq;

using System.Text;

using System.Threading.Tasks;

using System.Windows.Forms;

using System.Security.Cryptography;

using System.Runtime.InteropServices;

using System.IO;

1. **PHÂN CÔNG CÔNG VIỆC**

|  |  |
| --- | --- |
| **Tên** | **Nội dung công việc** |
| Nguyễn Mạnh Cường | Tổng hợp thông tin và làm slide |
| Lê Quang Minh | Tìm kiếm thông tin và viết báo cáo |
| Nguyễn Trần Đức Anh | Tìm kiếm thông tin |
| Hoàng Văn Anh Đức | Hiện thực demo , tìm kiếm thông tin |