

**TRƯỜNG ĐẠI HỌC SÀI GÒN**

**KHOA CÔNG NGHỆ THÔNG TIN**

BÁO CÁO AN TOÀN BẢO MẬT

HỆ THỐNG THÔNG TIN

Tên đề tài:

MÃ HÓA AES TRONG PHẦN MỀM QUẢN LÝ THƯ VIỆN

Họ tên thành viên trong nhóm:

|  |  |
| --- | --- |
| **Nguyễn Tấn Hòa** | **3119410135** |
| **Nguyễn Thanh Hải** | **3119410105** |
| **Phạm Văn Lợi** | **3118410256** |
| **Nguyễn Thanh Châu** | **3118410038** |

**GIÁO VIÊN HƯỚNG DẪN: Huỳnh Nguyễn Khắc Huy**

**TP. HỒ CHÍ MINH, năm 2022**

0

**MỤC LỤC**

[LỜI MỞ ĐẦU 2](#_Toc104503274)

[I. THUẬT TOÁN MÃ HÓA KHÓA ĐỐI XỨNG AES 3](#_Toc104503275)

[1.1. Tổng quan về AES 3](#_Toc104503276)

[1.2. Xây dựng thuật toán 3](#_Toc104503277)

[1.2.1. Xây dựng bảng S-box 3](#_Toc104503278)

[1.2.2. Giải thuật sinh khóa phụ 4](#_Toc104503279)

[1.2.3. Quá trình mã hóa 5](#_Toc104503280)

[1.3. Quá trình giải mã 8](#_Toc104503281)

[1.3.1. Tổng quan 8](#_Toc104503282)

[1.3.2. Thuật toán giải mã 8](#_Toc104503283)

[1.4. Các dạng tấn công vào AES và phương pháp phòng chống 9](#_Toc104503284)

[1.4.1. Side-channel attack 9](#_Toc104503285)

[1.4.2. Known attacks 9](#_Toc104503286)

[1.4.3. Các phương pháp phòng chống 9](#_Toc104503287)

[II. ÁP DỤNG AES VÀO PHẦN MỀM QUẢN LÝ THƯ VIỆN 11](#_Toc104503288)

[2.1. Giao diện mô tả mã hóa 11](#_Toc104503289)

[2.2. Coding function 14](#_Toc104503290)

[III. TỔNG KẾT 16](#_Toc104503291)

[3.1. Kết quả đạt được 16](#_Toc104503292)

[3.2. Đánh giá thuật toán 16](#_Toc104503293)

[TÀI LIỆU THAM KHẢO 17](#_Toc104503294)

# LỜI MỞ ĐẦU

Vấn đề đảm bảo an ninh, an toàn thông tin dữ liệu là nội dung nghiên cứu thiết thực, là chủ đề luôn được các cấp, các ngành quan tâm trong lĩnh vực công nghệ thông tin. Nhu cầu đảm bảo an ninh thông tin dữ liệu trên mạng máy tính là cấp thiết trong các hoạt động kinh tế xã hội, đặc biệt là đối với các mạng máy tính chuyên dùng phục vụ công tác an ninh, quốc phòng, đối ngoại của các cơ quan Đảng, Nhà nước... Thực tế ứng dụng công nghệ thông tin trong các lĩnh vực liên quan đến an ninh chính trị, quốc phòng luôn gặp phải những rủi ro đột nhập trái phép, tấn công, lấy cắp thông tin,...

Với việc sử dụng kiến thức về mã hóa của mình. Chúng em đã thực hiện mã hóa phần mềm: “*Quản lý thư viện*”, một phần để tổng hợp kiến thức, phần là tích lũy kinh nghiệm cho bản thân. Với sự giúp đỡ tận tình của giảng viên chúng em đã hoàn thành được đề tài. Mặc dù vậy do sự phức tạp của đề tài nên chúng em vẫn còn những sai sót. Mong bạn đọc và giảng viên góp ý kiến để nhóm em chỉnh sửa bổ sung.

Chúng em xin chân thành cảm ơn.

# THUẬT TOÁN MÃ HÓA KHÓA ĐỐI XỨNG AES

## Tổng quan về AES

AES (viết tắt của từ tiếng anh: Advanced Encryption Standard, hay Tiêu chuẩn mã hóa nâng cao) là một thuật toán mã hóa khối được chính phủ Hoa Kỳ áp dụng làm tiêu chuẩn mã hóa.

Thuật toán được xây dựng dựa trên Rijndael Cipher phát triển bởi 2 nhà mật mã học người Bỉ: Joan Daemen và Vincent Rijmen.

AES làm việc với các khối dữ liệu 128bit và độ dài khóa 128bit, 192bit hoặc 256bit. Các khóa mở rộng sử dụng trong chu trình được tạo ra bởi thủ tục sinh khóa Rijndael.

Hầu hết các phép toán trong thuật toán AES đều thực hiện trong một trường hữu hạn của các byte. Mỗi khối dữ liệu đầu vào 128bit được chia thành 16byte, có thể xếp thành 4 cột, mỗi cột 4 phần tử hay một ma trận 4x4 của các byte, nó gọi là ma trận trạng thái.

Tùy thuộc vào độ dài của khóa khi sử dụng 128bit, 192bit hay 256bit mà thuật toán được thực hiện với số lần lặp khác nhau.

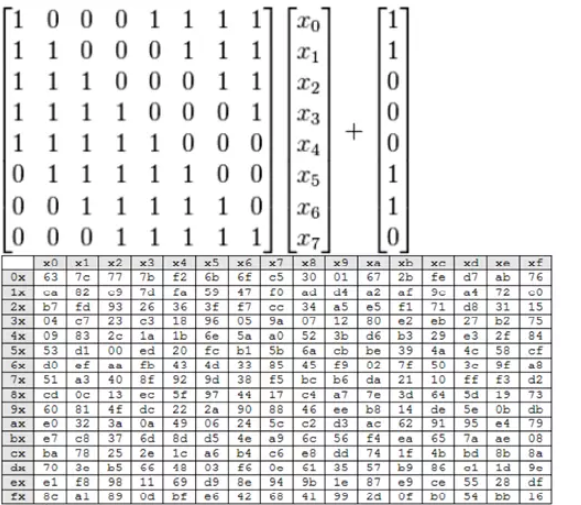
## Xây dựng thuật toán

### Xây dựng bảng S-box

1. Bảng S-box thuận

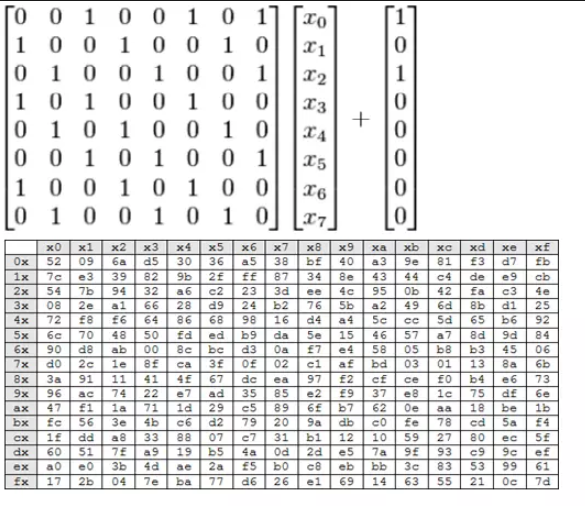
Bảng S-box thuận được sinh ra bằng việc xác định nghịch đảo cho một giá trị nhất định trên GF(28) = GF(2)[x] / (x8+x4+x3+x+1) (trường hữu hạn Rijindael). Giá trị 0 không có nghịch đảo thì được ánh xạ với 0. Những nghịch đảo được chuyển đổi thông qua phép biến đổi affine.

Công thức tính các giá trị bảng S-box và bảng S- box tương ứng:



1. Bảng S-box nghịch đảo

S-box nghịch đảo chỉ đơn giản là S-box chạy ngược. Nó được tính bằng phép biến đổi affine nghịch đảo các giá trị đầu vào. Phép biến đổi affine nghịch đảo được biểu diễn như sau:



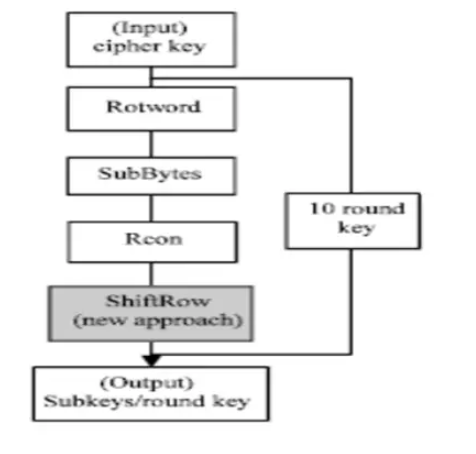
### Giải thuật sinh khóa phụ

Quá trình sinh khóa gồm 4 bước:

* Rotword: quay trái 8 bít
* SubBytes
* Rcon: tính giá trị Rcon(i) Trong đó :

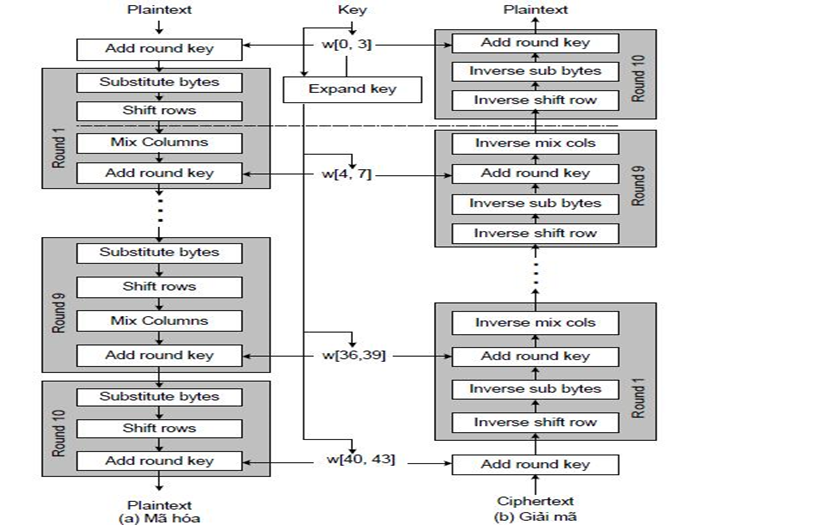
***Rcon(i) = x(i-1) mod (x8 + x4 + x3 + x + 1).***

* ShiftRow



### Quá trình mã hóa

1. Sơ đồ tổng quát



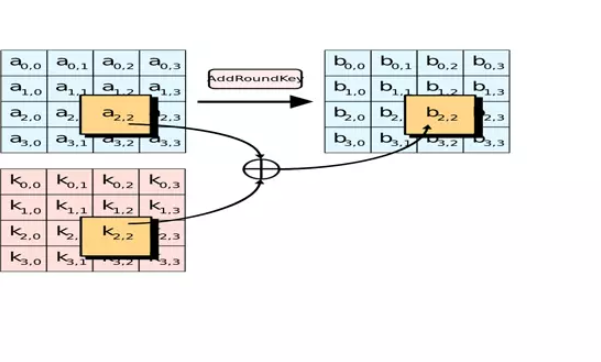
1. Hàm AddRoundKey

Được áp dụng từ vòng lặp thứ 1 tới vòng lặp Nr

Trong biến đổi Addroundkey(), một khóa vòng được cộng với state bằng một phép XOR theo từng bit đơn giản.

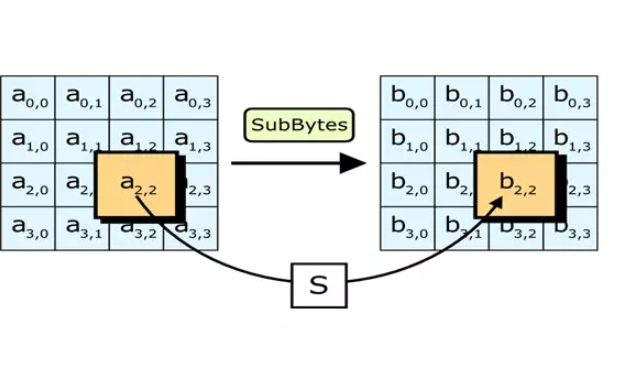
Mỗi khóa vòng gồm có 4 từ (128 bit) được lấy từ lịch trình khóa. 4 từ đó được cộng vào mỗi cột của state, sao cho:

***[S’0,c, S’1,c, S’2,c, S’3,c ] = [S0,c, S1,c, S2,c, S3,c ]  [W(4\*i + c)] với 0 <= c < 4.***



1. Hàm SubBytes

Biến đổi SubBytes() thay thế mỗi byte riêng rẽ của state Sr,c bằng một giá trị mới S’ r,c sử dụng bảng thay thế (S - box) được xây dựng ở trên.



1. Hàm ShiftRow

Trong biến đổi ShiftRows(), các byte trong ba hàng cuối cùng của trạng thái được dịch vòng đi các số byte khác nhau (độ lệch). Cụ thể :

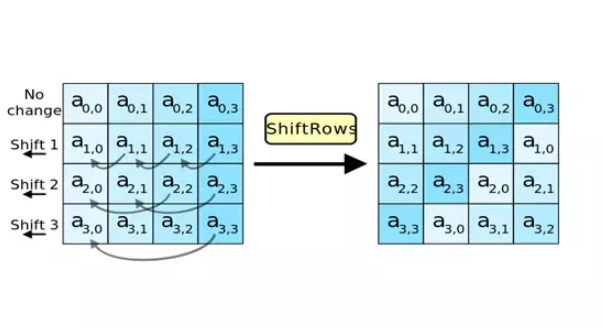
***S’r,c = Sr,(c + shift ( r, Nb)) mod Nb (Nb = 4)***

Trong đó giá trị dịch shift (r, Nb) phụ thuộc vào số hàng r như sau:

Shift(1,4) = 1, shift(2,4) = 2, shift(3,4) = 3.

Hàng đầu tiên không bị dịch, ba hàng còn lại bị dịch tương ứng:

* Hàng thứ 1 giữ nguyên.
* Hàng thứ 2 dịch vòng trái 1 lần.
* Hàng thứ 3 dịch vòng trái 2 lần.
* Hàng thứ 4 dịch vòng trái 3 lần.



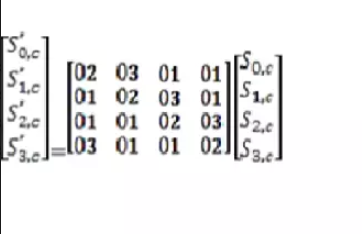
1. Hàm MixColumns

Biến đổi MixColumns() tính toán trên từng cột của state. Các cột được coi như là đa thức trong trường GF(28) và nhân với một đa thức a(x) với:

***a(x) = (03)x^3 +(01)x^2 +(01)x + (02)***

Biến đổi này có thể được trình bày như phép nhân một ma trận, mà mỗi byte được hiểu như là một phần tử trong trường GF(28): s’(x) = a(x)  s(x):

Mô tả bằng ma trận như sau :



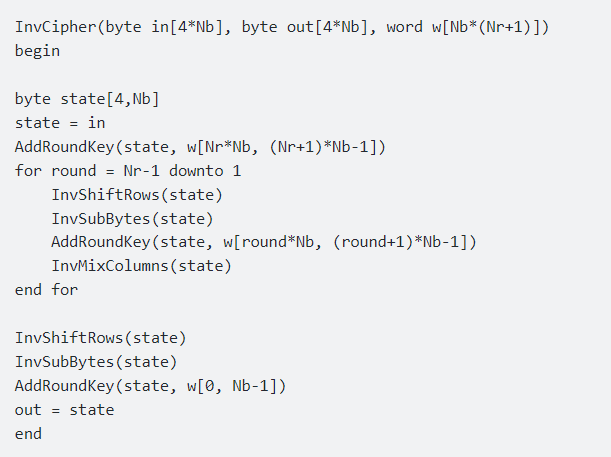
## Quá trình giải mã

### Tổng quan

Thuật toán giải mã khá giống với thuật toán mã hóa về mặt cấu trúc nhưng 4 hàm sử dụng là 4 hàm ngược của quá trình mã hóa.



### Thuật toán giải mã



Trong đó :

* In[] : Mảng dự liệu đầu vào Input.
* Out[] : Mảng dữ liệu đầu ra Output.
* Nr : Số vòng lặp.(Nr = 10).
* Nb : Số cột(Nb = 4).
* W[] : Mảng các w[i] có độ dài 4 bytes.

## Các dạng tấn công vào AES và phương pháp phòng chống

### Side-channel attack

Side Channels (Kênh kề) được định nghĩa là các kênh đầu ra không mong muốn từ một hệ thống.

Tấn công kênh bên hay còn gọi là Tấn công kênh kề là loại tấn công dễ thực hiện trong các loại tấn công mạnh chống lại quá trình triển khai mã hóa, và mục tiêu của loại tấn công này là phân tích các nguyên tố, các giao thức, modul, và các thiết bị trong mỗi hệ thống.

Phân loại :

* + Tấn công thời gian.
  + Tấn công dựa vào lỗi.
  + Tấn công phân tích năng lượng.
  + Tấn công phân tích điện từ.

### Known attacks

Vào năm 2002, Nicolas Courtois và Josef Pieprzyk phát hiện một tấn công trên lý thuyết gọi là tấn công XSL và chỉ ra điểm yếu tiềm tàng của AES.

Tuy nhiên, một vài chuyên gia về mật mã học khác cũng chỉ ra một số vấn đề trong cơ sở toán học của tấn công này và cho rằng các tác giả đã có sai lầm trong tính toán. Việc tấn công dạng này có thực sự trở thành hiện thực hay không vẫn còn để ngỏ và cho tới nay thì tấn công XSL vẫn chỉ là suy đoán.

### Các phương pháp phòng chống

Phương pháp 1: Mã hóa cực mạnh

Sử dụng các biện pháp để tăng tính bảo mật của các thuật toán mã hóa.

Phương pháp 2: Bảo vệ dữ liệu theo phương pháp vật lý

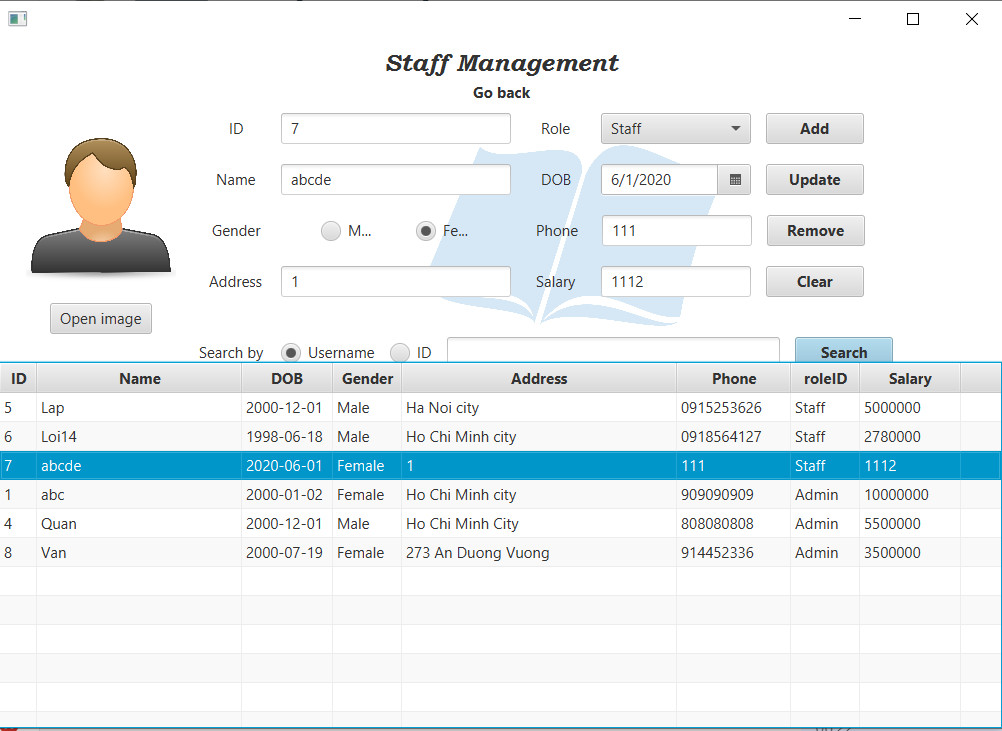
Nếu một kẻ tấn công không thể tiếp cận vật lý với dữ liệu, dĩ nhiên khả năng đánh cắp khóa mã hóa sẽ khó khăn hơn. Vì vậy, trước những cuộc tấn công qua âm thanh tiềm tàng, bạn có thể sử dụng các giải pháp bảo vệ vật lý như đặt laptop vào các hộp cách ly âm thanh, không để ai lại gần máy tính khi đang giải mã dữ liệu hoặc sử dụng các nguồn âm thanh băng rộng tần số đủ cao để gây nhiễu.

Phương pháp 3: Kết hợp cả 2 cách trên.

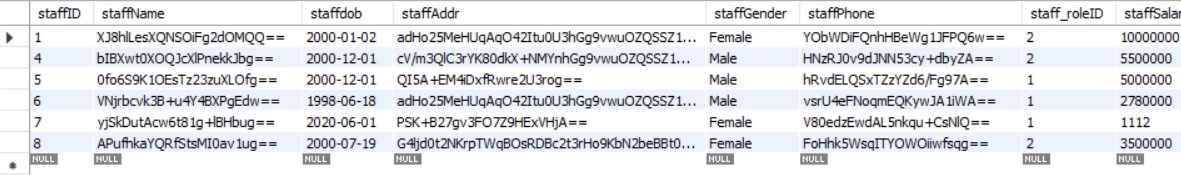
# ÁP DỤNG AES VÀO PHẦN MỀM QUẢN LÝ THƯ VIỆN

## Giao diện mô tả mã hóa

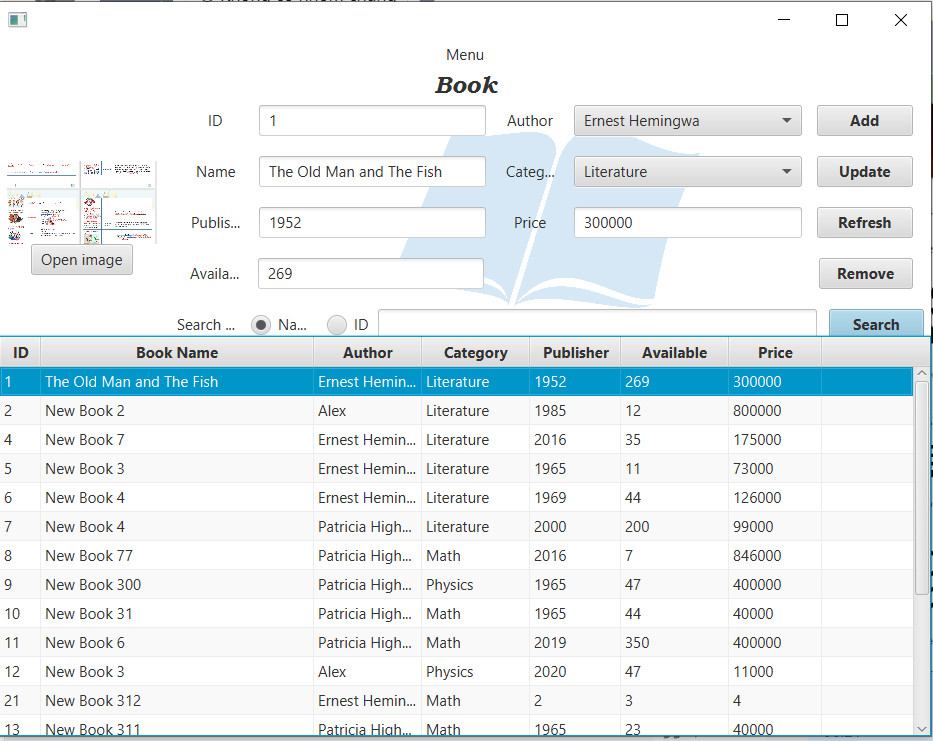
Staff Management



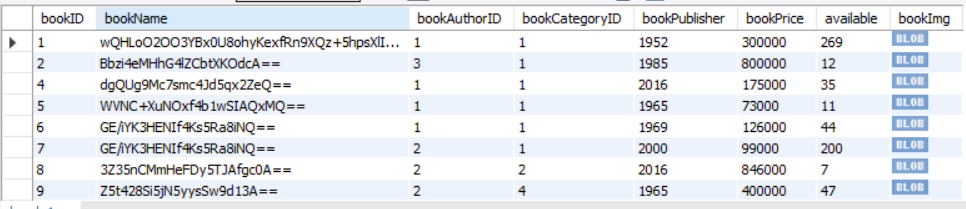
Staff sau khi được mã hóa AES:



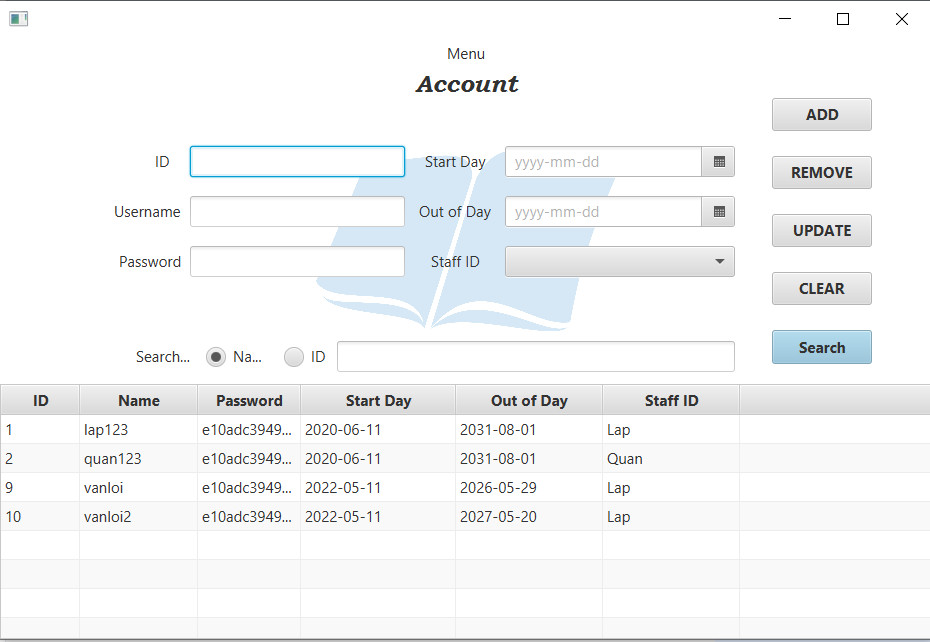
Book



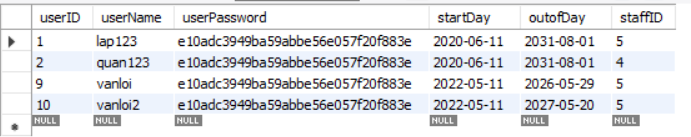
Book sau khi mã hóa AES:



Account



User Account sau khi được mã hóa AES:



## Coding function

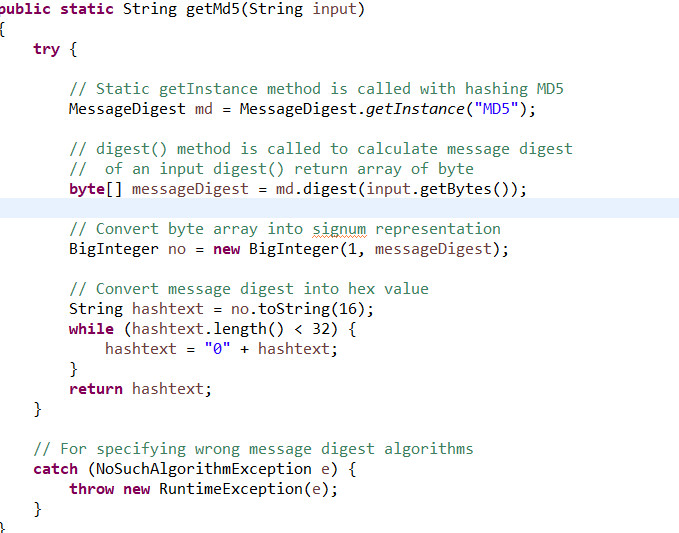
***GeneratorKey function***



***Encrypt function***



***GetMd5***



# TỔNG KẾT

## Kết quả đạt được

* Khái quát tổng quan về thuật toán mã hóa khóa đối xứng AES và áp dụng nó vào bảo mật dữ liệu phần mềm.
* Hoàn thành mã hóa dữ liệu một số dữ liệu trong hệ thống phần mềm quản lý thư viện.

## Đánh giá thuật toán

* Thiết kế và độ dài khóa của thuật toán AES (128, 192 và 256 bit) là đủ an toàn để bảo vệ các thông tin được xếp vào loại tối mật nhưng về an ninh của AES thì các nhà khoa học đánh giá là chưa cao. Nếu các kỹ thuật tấn công được cải thiện thì AES có thể bị phá vỡ.
* Một vấn đề khác nữa là cấu trúc toán học của AES khá đơn giản.

# TÀI LIỆU THAM KHẢO

# Bibliography

|  |  |
| --- | --- |
| [1] | H. N. K. Huy. [Online]. Available: https://classroom.google.com/u/0/c/NDY2OTY2ODM4MjM0. |
| [2] | B. H. Hoat, "Viblo," [Online]. Available: https://viblo.asia/p/tim-hieu-thuat-toan-ma-hoa-khoa-doi-xung-aes-gAm5yxOqldb. |
| [3] | L. Phúc, "Bài giảng," in *Bảo mật hệ thống thông tin*. |