**AES ( Advanced Encryption Standard )**

**1.Mã hóa AES là gì ?**

- AES là thuật toán khóa đối xứng và sử dụng mật mã khóa đối xứng.

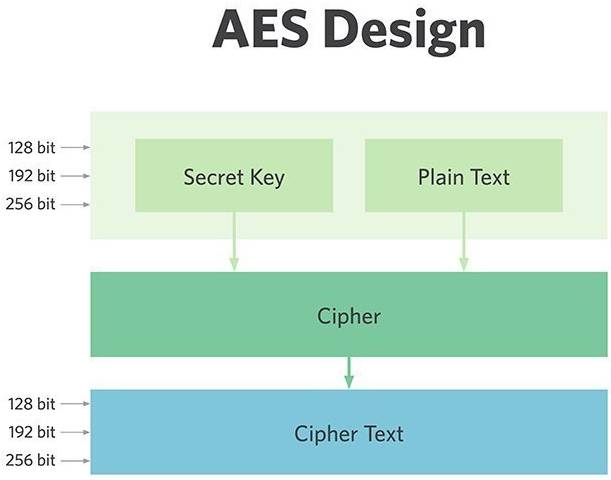
- Nó hoạt động dựa trên thuật toán Pijindael được phát triển bới hai nhà mật mã học người Bỉ là: Joan Daemen và Vincent Rijmen.

- Các tác vụ của AES được thực hiện ở cả phần cứng và phần mềm trên nhiều thiết bị để mã hóa 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 và tạo một rào chắn vững chắc để bảo vệ dữ liệu.

- Đặc biệt so với các tiêu chuẩn khác thì AES có khả năng thực hiện tác vụ trong môi trường hạn chế như thẻ thông minh.

**2. Cách thức hoạt động của AES :**

- AES bao gồm ba mật mã khối là: 128 bit, 192 bit và 256 bit. Hơn nữa, có các vòng mã hóa khác nhau cho mỗi kích thước khóa. Mỗi vòng là quá trình chuyển văn bản thô thành văn bản mã hóa. Đối với 128 bit có 10 vòng ( round ), 192 bit có 12 vòng và 256 bit có 14 vòng. Mỗi vòng đều thực hiện 3 bước : thay thế, biến đổi và hòa trộn khối pain text (văn bản thuẩn túy) đầu vào để biến nó thành ciphertext (văn bản đã mã hóa).



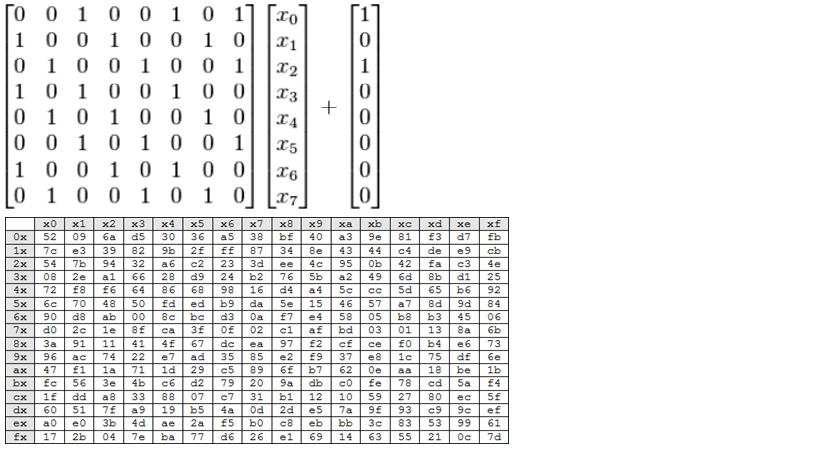
**3. Xây dựng thuật toán:**

1. **Xây dựng bảng S-box:**

* Trong mật mã học, S-box (substitution-box) là thành phần cơ bản của thuật toán mã khóa đối xứng, được dùng để thực hiện các phép thay thế phi tuyến. Trong mã khối, chúng thường được sử dụng để che giấu mối quan hệ giữa khóa mật mã và bản mã — tính hỗn loạn do Shannon đề xuất. Rijndael S-box là một sbox được sử dụng trong mật mã Rijndael, dựa trên đó để tạo ra thuật toán mã hóa AES.

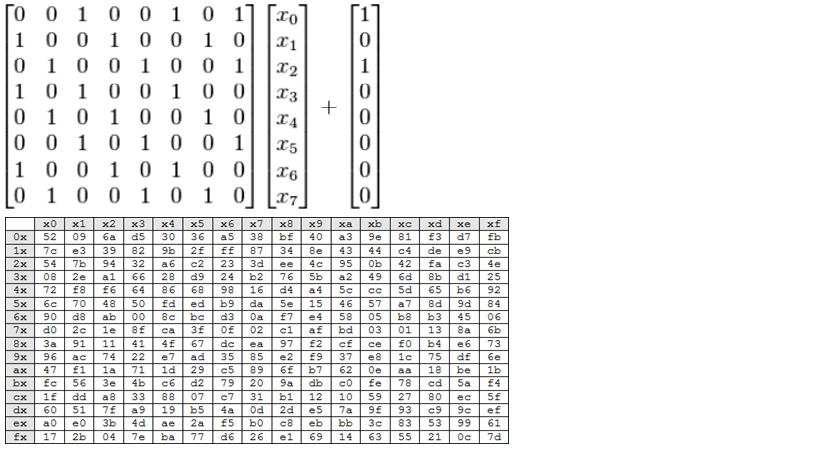
1. **Bảng S-box thuận:**

* Bảng S-box thuận được sinh ra bằng việc xác định 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 afine.
* 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:

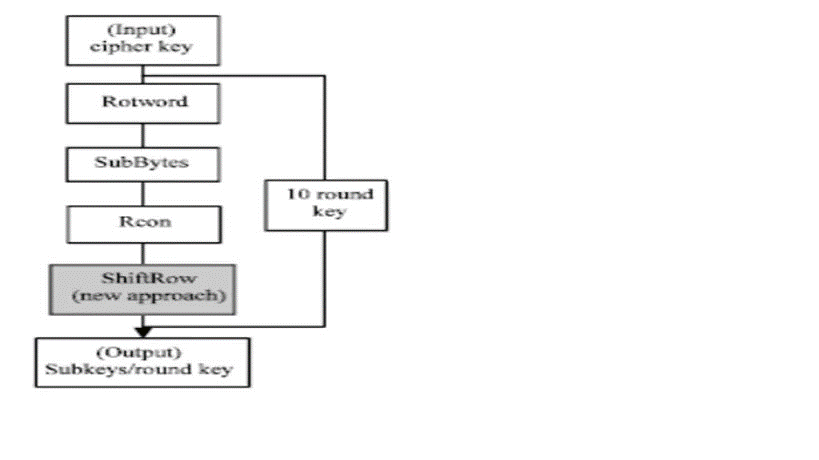


1. **Giải thuật sinh khóa phụ:**

* Quá trình sinh khóa gồm 4 bước:
* Rotword: quay trái 8 bit
* SubBytes
* Rcon: tính giá trị Rcon(i) trong đó:

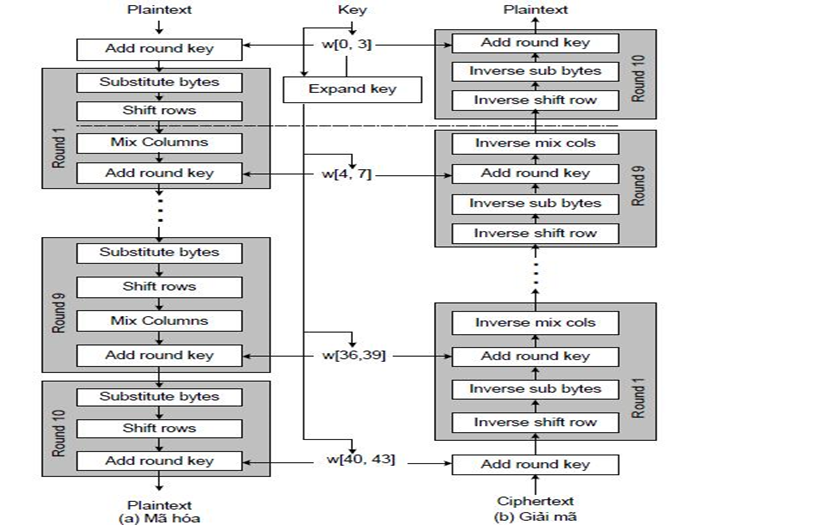
Rcon(i) = x(i-1) mod (x8 + x4 + x3 + x + 1).

* ShiftRow



1. **Quá trình mã hóa:**

**a.Sơ đồ tổng quát:**

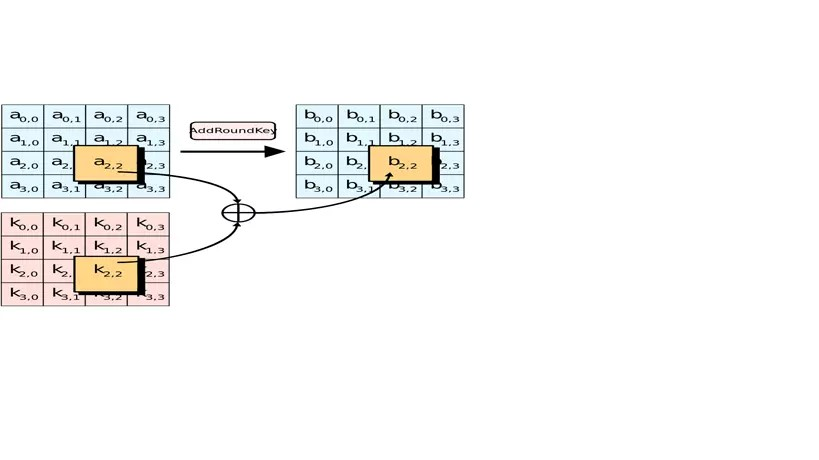


**b. Hàm AddRoundKey:**

* Được áp dụng từ vòng lặp thứ 1 tới vòng 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 (128bit) được lấy từ lịch trình khóa. 4 từ đó được cộng vào mỗi cột của state, sao cho:

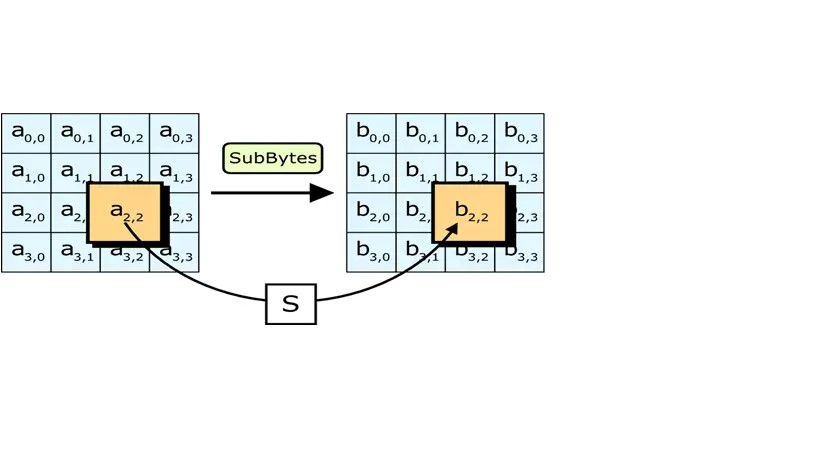
[S’0,c, S’1,c, S’2,c, S’3,c ] = [S0,c, S1,c, S2,c, S3,c ]  [W(4\*i + c)] với

0 <= c < 4.



1. **Hàm SubBytes:**

* Biến đổi SubBytes()thay thế moiox byte riêng lẻ 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:**

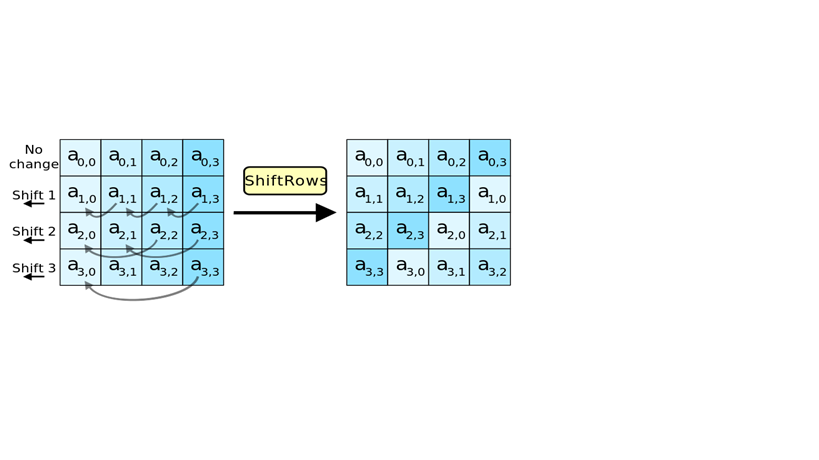
* Trong biến đổi ShiftRow(), các byte trong ba hàng cuối cùng của trạng thái được dịch vòng đi các số byte khác nhau (độ lệch). Cụ thể:

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.

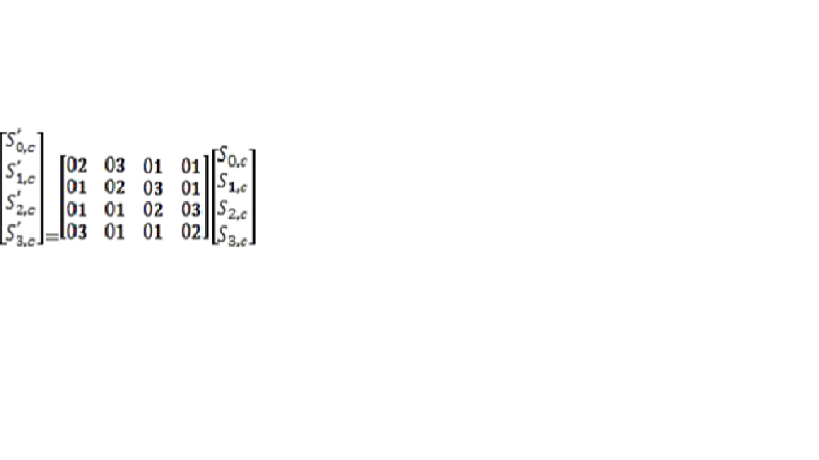


1. **Hàm MixColumns:**

* 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:



1. **Ứng dụng của thuật toán AES:**

**-** Thông thường với những ứng dụng không yêu cầu cao về hiệu nắng và tốc độ thì AES đang thực hiện ở dạng phần mềm. Với việc thực hiện trên phần mềm, thuật toán AES có thể được viết bằng nhiều ngôn ngữ lập trình như Assembler, C/C++, Visual Basic, Java, C#,… và có vận hành trên nhiều hệ điều hành như Window, Linux/Unix, Solaris..

**-** Khi thực hiện trên phần cứng, thuật toán AES hỗ trợ thực hiện hai dòng:

**+** Dòng thiết bị thứ nhất dựa vào một hệ vi xử lý phụ kết hợp với hệ vi xử lý chính của máy tính

**+** Dòng thiết bị thứ hai thường được thiết kế ở dạng thẻ thông minh ( smart card) hoặc các thiết bị cắm qua cổng USB.

**\*\*\***Mặc dù thực tế là AES được đề cập là thường được sử dụng ở mọi nơi nó được hỗ trợ, nhưng có một số ví dụ mà khả năng gặp phải nó cao hơn. Cụ thể:

* **VPN**
  + Cách thức hoạt động của VPN xoay quanh việc định tuyến lại lưu lượng truy cập của bạn, nhưng không phải trước khi mã hóa nó để người khác không thể thấy nó trong trường hợp họ đang theo dõi kết nối của bạn. Hơn thế nữa, lưu lượng truy cập cần được giải mã tại điểm thoát của nó, điều này liên quan đến nhu cầu về tiêu chuẩn mã hóa. AES-256 được sử dụng theo mặc định bởi một số nhà cung cấp VPN, bao gồm [NordVPN](https://www.addictivetips.com/go/nordvpn-discount/), [Surfshark](https://www.addictivetips.com/go/surfshark-deal/)và [ExpressVPN](https://www.addictivetips.com/go/expressvpn-discounts/).
* **Trình quản lý mật khẩu**
  + Trình quản lý mật khẩu hoạt động bằng cách cho phép bạn đặt tất cả mật khẩu của mình vào chúng và bảo vệ chúng bằng một mật khẩu duy nhất thông qua phương tiện mã hóa. Nhiều giải pháp phần mềm quản lý mật khẩu khác nhau trên thị trường đã chọn AES làm tiêu chuẩn mã hóa hoạt động của họ, vì nó dễ thực hiện, nhanh chóng và an toàn.
* **Mạng Wi-Fi**
  + Nếu không có mã hóa lưu lượng, những kẻ tấn công có thể chỉ ngồi bên ngoài mạng không dây của bạn, nắm bắt các gói tin không được mã hóa bằng bộ điều hợp WiFi thích hợp và theo dõi toàn bộ nơi ở trực tuyến của bạn mà không cần quan tâm. Rất may, mã hóa AES, thường cùng với các tiêu chuẩn bảo mật bổ sung (WPA2 là phổ biến nhất vào thời điểm hiện tại) có thể ngăn điều đó xảy ra.
* **Trình duyệt web**
  + Bạn có thể đã biết rằng lâu nay các trình duyệt web đã mã hóa kết nối của người dùng để bảo vệ họ khỏi các mối đe dọa mạng khác nhau như các cuộc tấn công MITM (Man-In-The-Middle), giả mạo hoặc giám sát lưu lượng.
* **Mã hóa đĩa**
  + Mặc dù tính năng này chủ yếu được sử dụng trên các thiết bị di động như điện thoại thông minh và máy tính bảng, nhưng mã hóa đĩa của bạn không phải là chưa từng có nếu bạn muốn tăng cường quyền riêng tư và bảo mật của mình. AES hiện là một trong những phương pháp phổ biến nhất được sử dụng để mã hóa và giải mã nội dung đĩa.
* **Phần mềm nén tệp**
  + Cho dù đó là WinRar, WinZip hay 7z mà chúng ta đang nói đến, tất cả các tiện ích lưu trữ và nén/giải nén tệp trên thị trường đều sử dụng AES làm tiêu chuẩn mã hóa để ngăn chặn rò rỉ dữ liệu ngẫu nhiên trong khi xử lý tệp của bạn.
* **Ứng dụng liên lạc**
  + WhatsApp, Signal, Telegram, Snapchat, Messenger, và những người khác mà chúng tôi chưa đề cập, sử dụng mã hóa AES để đảm bảo rằng bạn sẽ được hưởng lợi từ sự riêng tư hoàn toàn, cho dù bạn đang gửi ảnh, video, tài liệu hay đơn giản tin nhắn văn bản thông qua các ứng dụng này.
* **Thư viện ngôn ngữ lập trình**
  + Nếu bạn là một lập trình viên, bạn có thể nên biết rằng các thư viện của một số ngôn ngữ lập trình nhất định, bao gồm nhưng không giới hạn ở C ++, Java và Python, sử dụng mã hóa AES để giúp bạn bảo vệ dữ liệu và dự án của mình khỏi bị truy cập trái phép.
* **Thành phần hệ điều hành**
  + Để thêm một lớp bảo mật bổ sung, một số hệ điều hành đã thêm mã hóa AES vào một số thành phần của chúng.