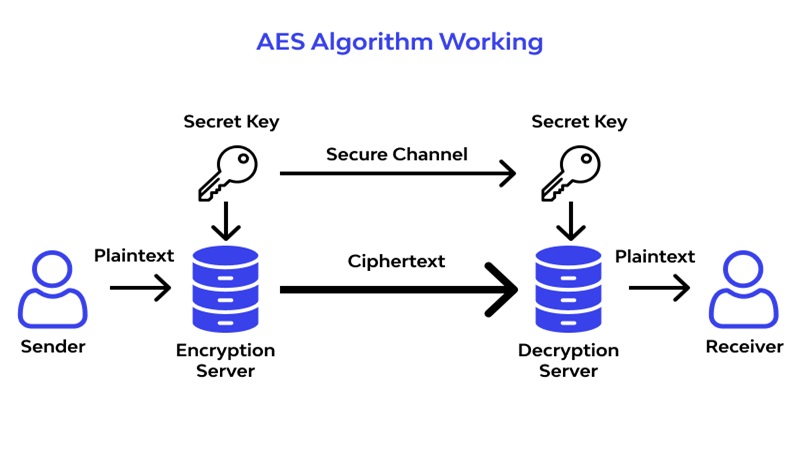
**Giới thiệu**

Tiêu chuẩn **Advanced Encryption Standard** (AES) - Tiêu chuẩn mã hóa nâng cao là một thuật toán tiêu chuẩn của chính phủ Hoa Kỳ nhằm mã hóa và giải mã dữ liệu do Viện Tiêu chuẩn và Công nghệ quốc gia Hoa Kỳ (National Institute Standards and Technology– NIST) phát hành ngày 26/11/2001 và được đặc tả trong Tiêu chuẩn Xử lý thông tin Liên bang 197 (Federal Information Processing Standard – FIPS 197) sau quá trình kéo dài 5 năm trình phê duyệt, AES tuân theo mục 5131 trong Luật Cải cách quản lý công nghệ thông tin năm 1996 và Luật An toàn máy tính năm 1997.

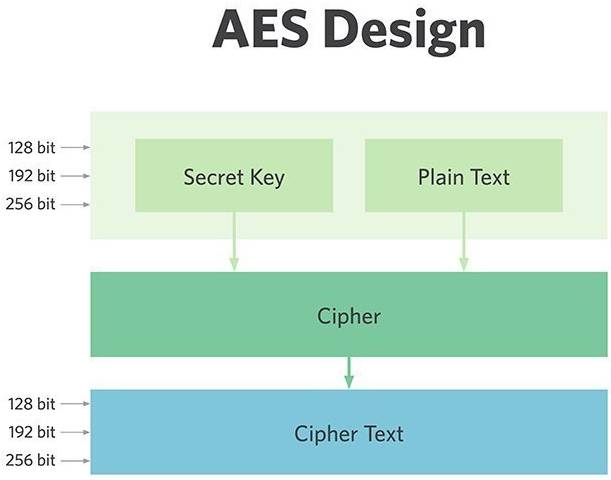


**Hình 1. 1 Advanced Encryption Standard là một thuật toán mã hóa đối xứng**

AES là một thuật toán “**mã hóa khối**” (block cipher) **đối xứng** ban đầu được tạo ra bởi hai nhà mật mã học người Bỉ là Joan Daemen và Vincent Rijmen. Kể từ khi được công bố là một tiêu chuẩn, AES trở thành một trong những thuật toán mã hóa phổ biến nhất sử dụng khóa mã đối xứng để mã hóa và giải mã (một số được giữ bí mật dùng cho quy trình mở rộng khóa nhằm tạo ra một tập các khóa vòng). Ở Việt Nam, thuật toán AES đã được công bố thành tiêu chuẩn quốc gia TCVN 7816:2007 năm 2007 về Thuật toán mã hóa dữ liệu AES.

**Nguyên lí hoạt động**

AES là một thuật toán mã hóa khối đối xứng với độ dài khóa là **128 bít** (một chữ số nhị phân có giá trị 0 hoặc 1), **192** **bít** và **256 bít** tương ứng được gọi là AES-128, AES-192 và AES-256. AES-128 sử dụng 10 vòng (round), AES-192 sử dụng 12 vòng và AES-256 sử dụng 14 vòng. Mỗi vòng đều thực hiện ba bước thay thế, biến đổi và hòa trộn khối plain text (bản rõ) đầu vào để biến nó thành Ciphertext (bản mã).



Thông tin được chính phủ phân loại theo ba cấp độ: bảo mật, bí mật, tối mật. Tất cả các độ dài của key từ 128, 192 và 256 bit đều được dùng ở cấp độ bảo mật, bí mật. Riêng với những thông tin tối mật để đảm bảo không xảy ra bất cứ sai sót nào phải cần đến key 192 hoặc 256 bit. Mật mã sẽ dùng một key riêng tư để mã hóa và giải mã dữ liệu và tất nhiên cả người gửi và người nhận đều phải nhận biết và sử dụng được key này.

Dữ liệu cần được chia thành các khối 16 byte và được lưu trữ trong một ma trận 4x4 gọi là trạng thái. Nếu dữ liệu không đủ 16 byte, có thể sử dụng các kỹ thuật như đệm (padding) hay chuẩn hóa (normalization) để bổ sung.

Khóa bí mật cũng cần được chia thành các khối 16 byte và được lưu trữ trong một ma trận 4x4 gọi là khóa vòng. Tùy vào độ dài của khóa ban đầu, có thể sinh ra từ 10 đến 14 khóa vòng khác nhau bằng cách sử dụng các phép biến đổi như hoán vị, thay thế và XOR.

Quá trình mã hóa gồm có nhiều vòng lặp (round), tùy vào độ dài của khóa ban đầu.Vòng lặp chính của AES thực hiện các hàm sau: SubBytes(), ShiftRows(), MixColumns() và AddRoundKey(). Ba hàm đầu của một vòng AES được thiết kế để ngăn chặn phân tích mã bằng phương thức “mập mờ“ (confusion) và phương thức “khuếch tán“ (diffusion), còn hàm thứ tư mới thực sự được thiết kế để mã hóa dữ liệu. Trong đó “khuếch tán“ có nghĩa là các kiểu mẫu trong bản rõ (Dữ liệu đầu vào của phép mã hóa hoặc dữ liệu đầu ra của phép giải mã) được phân tán trong các bản mã (Dữ liệu đầu ra của phép mã hóa hoặc dữ liệu đầu vào của phép giải mã), “mập mờ“ nghĩa là mối quan hệ giữa bản rõ và bản mã bị che khuất. Một cách đơn giản hơn để xem thứ tự hàm AES là: Trộn từng byte (SubBytes), trộn từng hàng (ShiftRows), trộn từng cột (MixColumns) và mã hóa (AddRoundKey).

**Ứng dụng của AES**

Bên cạnh ứng dụng trong việc đảm đảm an toàn cho các tài liệu chính phủ, AES cũng được áp dụng nhiều trong các lĩnh vực khác nhau. Cụ thể:

* Ứng dụng cho tất cả người dùng phổ thông trong quá trình giải mã dữ liệu bằng cách truy cập vào trang web AES Encryption, nhập dữ liệu và áp mã khoá. Tuy nhiên, đây chỉ là phương pháp áp dụng cho các tác vụ thông thường và tính bảo mật thường không cao.
* Mã hoá thông tin trên phần mềm với các ngôn ngữ lập trình như C/C++, Java hay Assembler. AES hỗ trợ rất nhiều cho các hệ điều hành như Linux hay Windows.
* AES áp dụng cho các thiết bị phần cứng bao gồm dòng thiết bị dựa trên hoạt động của hệ vi xử lý và dòng thiết bị cắm qua cổng USB hoặc thẻ thông minh Smart Card.
* Ứng dụng trong truyền thông tin qua Internet thông qua kết nối HTTPS: Dữ liệu sẽ được mã hoá và giải mã thông qua thuật toán AES, thông tin được bảo mật tốt hơn khi so sánh với kết nối HTTP. Bên cạnh đó, wifi hiện nay cũng được ứng dụng thuật toán AES, khi kết hợp với giao thức WPA2, giao tiếp này trở nên an toàn, hiệu quả hơn nhiều và ngăn chặn tấn công trung gian. Bên cạnh đó, AES cũng được sử dụng để mã hoá wifi trên router, kết hợp với giao thức phổ biến WPA2 được gọi là AES/WPA2. AES còn được sử dụng nhằm hỗ trợ mã hoá SSL.

**So sánh AES và DES**

DES được xem như tiêu chuẩn mã hóa lâu đời được Hoa Kỳ phát triển cách đây hơn 40 năm. Chức năng chính của DES là mang tới tiêu chuẩn chung, an toàn cho các hệ thống của Chính phủ, đồng thời tạo điều kiện để các hệ thống liên kết với nhau một cách nhanh chóng.

Trong nhiều thập niên, DES đã và đang trở thành trụ cột để bảo vệ an ninh quốc gia của Hoa Kỳ. Mãi đến năm 1999, key 56 bit của DES bị phá vỡ bởi các nhà nghiên cứu. Do đó đến năm 2000, AES đã được nghiên cứu thành công và trở thành giải pháp thay thế cho DES. Tuy DES hiện đã trở nên ít thông dụng hơn nhưng vẫn được sử dụng trong một số trường hợp cụ thể.

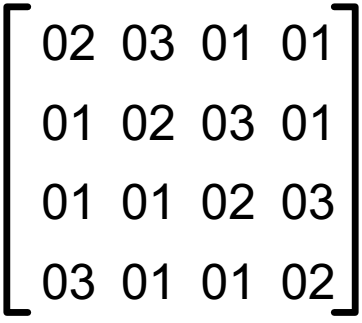
Cả AES và DES đều là mật mã khối đối xứng nhưng AES vẫn nhỉnh hơn về hiệu quả bởi độ dài key của nó. Có thể thấy rằng, các key 128 bit, 192 bit và 256 bit của AES mạnh gấp nhiều lần so với 56 bit của DES. Không chỉ vậy, mã hóa AES cũng nhanh hơn so với DES.

**Biểu đồ so sánh**

|  |  |  |
| --- | --- | --- |
| **Cơ sở để so sánh** | **DES (Tiêu chuẩn mã hóa dữ liệu)** | **AES (Tiêu chuẩn mã hóa nâng cao)** |
| **Căn bản** | Trong DES, khối dữ liệu được chia thành hai nửa. | Trong AES, toàn bộ khối dữ liệu được xử lý dưới dạng một ma trận. |
| **Nguyên tắc** | DES hoạt động trên cấu trúc mật mã Feistel. | AES hoạt động trên Nguyên tắc thay thế và hoán vị. |
| **Văn bản thô** | Bản rõ là 64 bit | Bản rõ có thể là 128,192 hoặc 256 bit |
| **Kích thước khóa** | DES so với AES có kích thước khóa nhỏ hơn. | AES có kích thước khóa lớn hơn so với DES. |
| **Vòng** | 16 vòng | 10 vòng cho thuật toán 128 bit 12 vòng cho thuật toán 192 bit 14 vòng cho thuật toán 256-bit |
| **Tên vòng** | Extended License, Xor, S-box, P-box, Xor và Swap. | Subbyte, Shiftbow, MixColumns, Addroundkeys. |
| **Bảo vệ** | DES có khóa nhỏ hơn, kém an toàn hơn. | AES có khóa bí mật lớn tương đối do đó, an toàn hơn. |
| **Tốc độ** | DES tương đối chậm hơn. | AES nhanh hơn. |

**MixColumns**

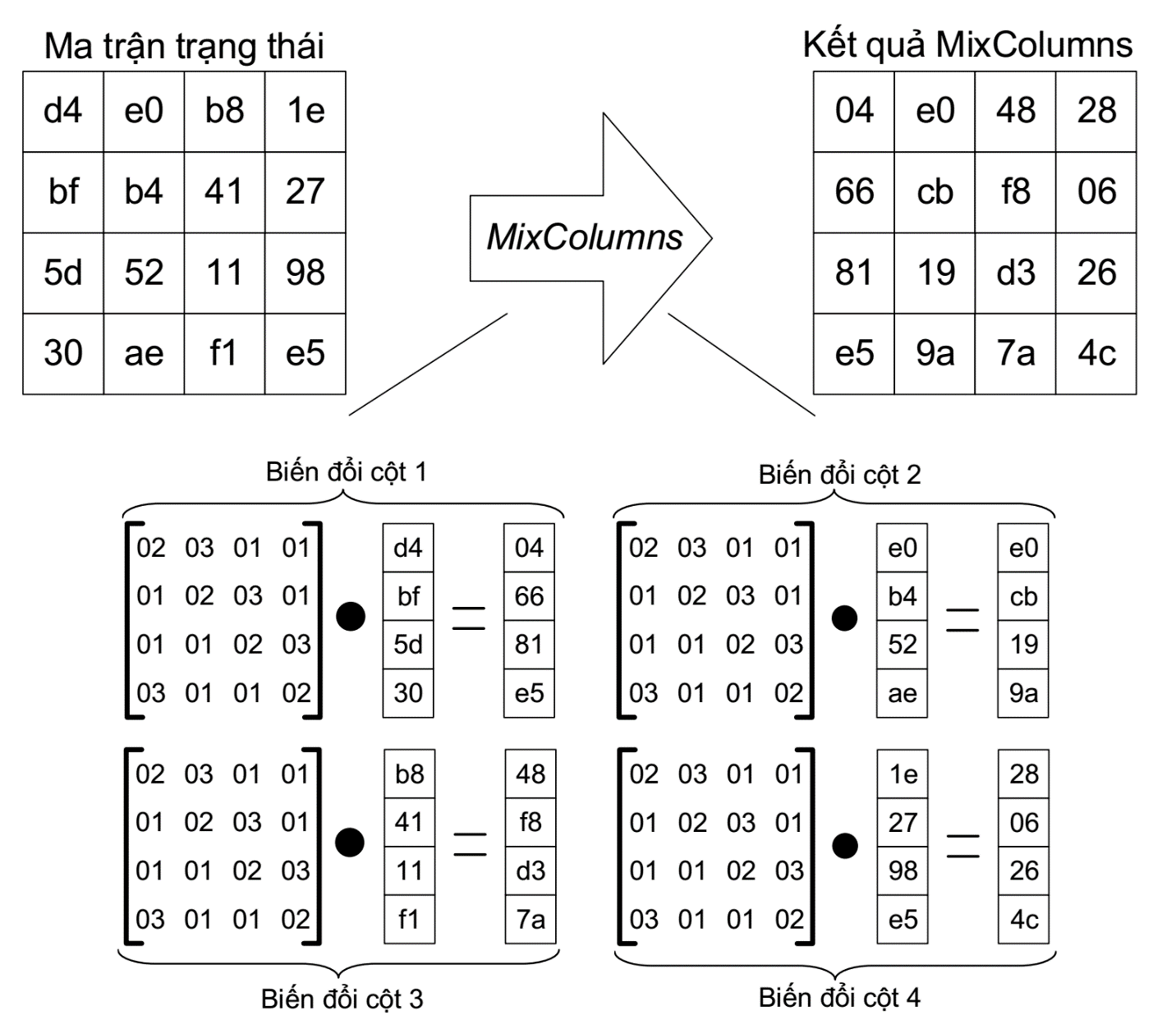
Chức năng MixColumns thực hiện nhân từng cột của ma trận trạng thái, ngõ ra của ShiftRows, với một ma trận chuyển đổi quy định bởi chuẩn AES.



**Ma trận chuyển đổi sử dụng trong chức năng MixColumns**

Việc biến đổi một cột của ma trận trạng thái được thực hiện bởi hai phép toán là nhân (.) và XOR (+). Biểu thức sau tạo ra phần tử H04, H là ký hiệu của số Hex, ở cột 1 trong hình minh họa "chức năng MixColumns".

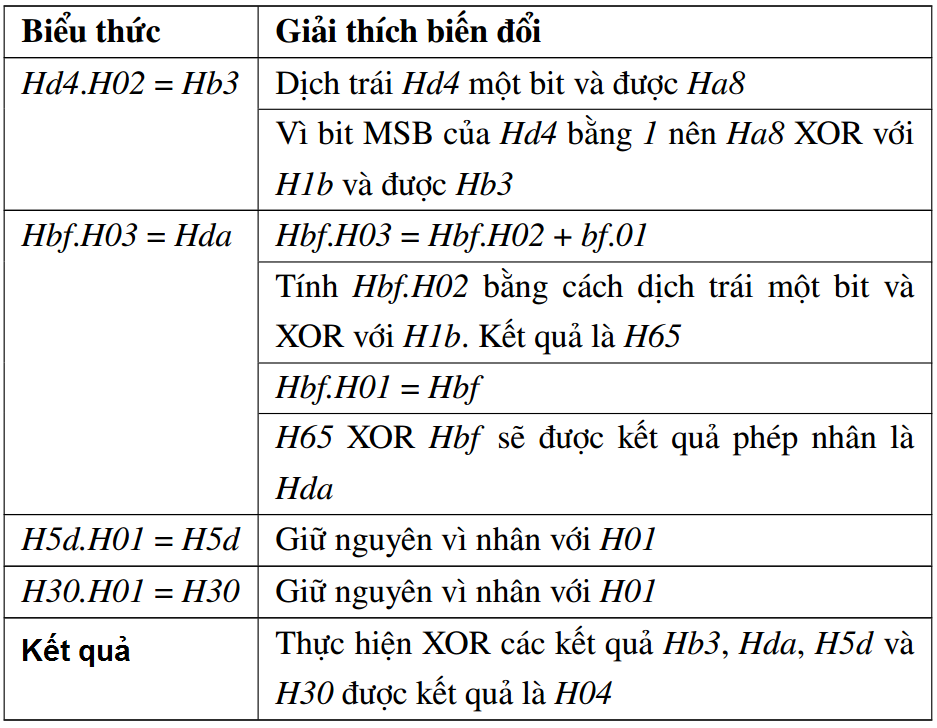
H04 = Hd4.H02 + Hbf.H03 + H5d.H01 + H30.H01=Hd4.H02 + (Hbf.H02 + Hbf.H01) + H5d.H01 + H30.H01



**Chức năng MixColumns**

Phép nhân với H01 thì giữ nguyên giá trị. Phép nhân với H02 tương đương với việc dịch trái một bit và XOR có điều kiện như sau:

* Nếu bit của giá trị được dịch bằng 1 thì giá trị sau khi dịch được XOR với H1b
* Nếu bit của giá trị được dịch bằng 0 thì giữ giá trị sau khi dịch.



**Chi tiết về cách tính MixColumns tạo ra phần tử H04 từ cột 1**