**2.3.1. Giới thiệu về mã hóa AES**

**-** Vào năm 1999, cục tiêu chuẩn quốc gia Hoa Kỳ (NIST) đã ban hành một phiên bản mới của tiêu chuẩn DES chỉ ra rằng DES chỉ nên được sử dụng cho các hệ thống kế cũ và DES ba lần được sử dụng. DES ba lần có hai ưu điểm đảm bảo cho việc sử dụng rộng rãi trong vài năm tới. Đầu tiên, với độ dài khóa 168-bit, nó khắc phục được lỗ hổng đối với cuộc tấn công vét cạn của DES. Thứ hai, thuật toán mã hóa cơ bản trong DES ba lần cũng giống như trong DES. Thuật toán này đã được giám sát kỹ lưỡng hơn bất kỳ thuật toán mã hóa nào khác trong một khoảng thời gian dài và không có cuộc tấn công phá mã hiệu quả nào dựa trên thuật toán thay vì vét cạn được tìm thấy. Do đó, DES ba lần có khả năng chống phá mã rất tốt. Nếu bảo mật là yếu tố duy nhất được xem xét, thì DES ba lần sẽ là lựa chọn thích hợp cho thuật toán mã hóa tiêu chuẩn trong nhiều thập kỷ tới. Hạn chế chính của DES ba lần là thuật toán tương đối chậm trong phần mềm. DES ban đầu được thiết kế để triển khai bằng phần cứng giữa những năm 1970 và không tạo ra mã phần mềm hiệu quả. DES ba lần, có số vòng gấp ba lần DES, do đó thực hiện chậm hơn DES ban đầu. Một nhược điểm phụ là cả DES và DES ba lần đều sử dụng kích thước khối 64-bit. Vì lý do cả hiệu quả và bảo mật, kích thước khối lớn hơn là cần thiết. Vì những nhược điểm này, DES ba lần không phải là ứng cử viên thích hợp để sử dụng lâu dài. Để thay thế, vào năm 1997 NIST đã đưa ra lời kêu gọi đề xuất Tiêu chuẩn mã hóa nâng cao (AES) mới, tiêu chuẩn này phải có sức mạnh bảo mật bằng hoặc tốt hơn DES ba lần và cải thiện đáng kể hiệu quả. Ngoài các yêu cầu chung này, NIST quy định rằng AES phải là mật mã khối đối xứng với độ dài khối 128 bit và hỗ trợ độ dài khóa có thể là 128, 192 và 256 bit.Trong vòng đánh giá đầu tiên, 15 thuật toán được đề xuất đã được chấp nhận. Vòng thứ hai thu hẹp còn 5 thuật toán. NIST đã hoàn thành quá trình đánh giá của mình và xuất bản tiêu chuẩn cuối cùng vào tháng 11 năm 2001. NIST đã chọn Rijndael làm thuật toán AES được đề xuất. Hai nhà nghiên cứu đã phát triển và gửi Rijndael cho AES đều là những nhà mật mã học đến từ Bỉ: Tiến sĩ Joan Daemen và Tiến sĩ Vincent Rijmen. Cuối cùng, AES được thiết kế để thay thế DES ba lần, nhưng quá trình này sẽ mất một số năm. NIST dự đoán rằng DES ba lần vẫn sẽ là một thuật toán được sử dụng trong tương lai gần.

**2.3.1.2. Các tham số, ký hiệu và hàm của thuật toán**

|  |  |
| --- | --- |
| ****AES**** | Tiêu chuẩn mã hóa nâng cao |
| ****Bit**** | Một chữ số nhị phân có giá trị bằng 0 hoặc 1. |
| ****Byte**** | Một nhóm tám bit được coi là một thực thể duy nhất hoặc là một mảng gồm 8 bit riêng lẻ. |
| ****Cipher**** | Một loạt các phép biến đổi chuyển đổi văn bản thuần túy thành bản mã bằng khóa mật mã. |
| ****Cipher Key**** | Khóa bí mật, mật mã được sử dụng bởi quy trình mở rộng khóa để tạo ra một bộ khóa tròn; có thể được hình dung như một mảng byte hình chữ nhật, có bốn hàng và cột Nk. |
| ****Ciphertext**** | Dữ liệu đầu ra từ mật mã hoặc đầu vào đến mật mã nghịch đảo |
| ****Inverse Cipher**** | Một loạt các phép biến đổi chuyển đổi bản mã thành văn bản thuần túy bằng khóa mật mã |
| ****Key Expansion**** | Thói quen được sử dụng để tạo một loạt các khóa tròn từ khóa mật mã. |
| ****Plaintext**** | Dữ liệu đầu vào mật mã hoặc đầu ra từ mật mã nghịch đảo. |
| ****Rijndael**** | Thuật toán mật mã được chỉ định trong tiêu chuẩn mã hóa nâng cao (AES). |
| ****Round Key**** | Khóa tròn là các giá trị bắt nguồn từ khóa mật mã sử dụng quy trình Mở rộng khóa; chúng được áp dụng cho Trạng thái trong Mật mã và Mật mã nghịch đảo. |
| ****S-box**** | Bảng thay thế phi tuyến tính được sử dụng trong một số phép biến đổi thay thế byte và trong quy trình mở rộng khóa để thực hiện thay thế một cho một của giá trị byte. |
| ****AddRoundKey()**** | Chuyển đổi trong mật mã và mật mã nghịch đảo trong đó khóa tròn được thêm vào trạng thái bằng cách sử dụng thao tác XOR. Độ dài của Khóa tròn bằng kích thước của trạng thái (tức là đối với Nb = 4, độ dài Khóa tròn bằng 128 bit / 16 byte). |
| ****InvMixColumns()**** | Biến đổi trong mật mã nghịch đảo là nghịch đảo của MixColumns(). |
| ****InvShiftRows()**** | Biến đổi trong mật mã nghịch đảo là nghịch đảo của ShiftRows(). |
| ****InvSubBytes()**** | Phép biến đổi trong Mật mã nghịch đảo là nghịch đảo của SubBytes(). |
| ****K**** | Khóa mật mã. |
| ****MixColumns()**** | Phép biến đổi trong mật mã lấy tất cả các cột của trạng thái và trộn dữ liệu của chúng (độc lập với nhau) để tạo ra các cột mới. |
| ****Nb**** | Số cột (từ 32 bit) bao gồm trạng thái. Đối với tiêu chuẩn này, Nb = 4. |
| ****Nk**** | Số lượng từ 32 bit bao gồm khóa mật mã. Đối với tiêu chuẩn này, Nk = 4, 6 hoặc 8. |
| ****Nr**** | Số vòng, là một hàm của Nk và Nb (được cố định). Đối với tiêu chuẩn này, Nr = 10, 12 hoặc 14. |
| ****Rcon[]**** | Mảng từ không đổi tròn. |
| ****RotWord()**** | Hàm được sử dụng trong quy trình Key Expansion lấy một từ bốn byte và thực hiện hoán vị theo chu kỳ. |
| ****ShiftRows()**** | Biến đổi trong mật mã xử lý trạng thái bằng cách dịch chuyển theo chu kỳ ba hàng cuối cùng của trạng thái bằng các phần bù khác nhau. |
| ****SubBytes()**** | Phép biến đổi trong mật mã xử lý trạng thái bằng cách sử dụng bảng thay thế byte phi tuyến (S-box) hoạt động trên mỗi byte Trạng thái một cách độc lập |
| ****SubWord()**** | Hàm được sử dụng trong quy trình Key Expansion lấy một từ đầu vào bốn byte và áp dụng một bảng S-box cho mỗi trong số bốn byte để tạo ra một từ đầu ra. |
| ****XOR**** | Toán tử Ex-OR |
| ****⊕**** | Toán tử Ex-OR |
| Ⓧ | Phép nhân của hai đa thức (mỗi đa thức có độ < 4) modulo x 4 +1. |
| ****•**** | Phép nhân trường hữu hạn. |

**2.3.3. Độ an toàn**

- Vào thời điểm năm 2006, dạng tấn công lên AES duy nhất thành công là tấn công kênh bên (side channel attack]). Vào tháng 6 năm 2003, chính phủ Hoa Kỳ tuyên bố AES có thể được sử dụng cho thông tin mật.

"Thiết kế và độ dài khóa của thuật toán AES (128, 192 và 256 bít) là đủ an toàn để bảo vệ các thông tin được xếp vào loại TỐI MẬT (secret). Các thông tin TUYỆT MẬT (top secret) sẽ phải dùng khóa 192 hoặc 256 bít. Các phiên bản thực hiện AES nhằm mục đích bảo vệ hệ thống an ninh hay thông tin quốc gia phải được NSA kiểm tra và chứng nhận trước khi sử dụng." - [4] Lưu trữ 2007-09-27 tại Wayback Machine.

Điều này đánh dấu lần đầu tiên công chúng có quyền tiếp xúc với thuật toán mật mã mà NSA phê chuẩn cho thông tin TUYỆT MẬT. Nhiều phần mềm thương mại hiện nay sử dụng mặc định khóa có độ dài 128 bít.

Phương pháp thường dùng nhất để tấn công các dạng mã hóa khối là thử các kiểu tấn công lên phiên bản có số chu trình thu gọn. Đối với khóa 128 bít, 192 bít và 256 bít, AES có tương ứng 10, 12 và 14 chu trình. Tại thời điểm năm 2006, những tấn công thành công được biết đến là 7 chu trình đối với khóa 128 bít, 8 chu trình với khóa 192 bít và 9 chu trình với khóa 256 bít

Một số nhà khoa học trong lĩnh vực mật mã lo ngại về an ninh của AES. Họ cho rằng ranh giới giữa số chu trình của thuật toán và số chu trình bị phá vỡ quá nhỏ. Nếu các kỹ thuật tấn công được cải thiện thì AES có thể bị phá vỡ. Ở đây, *phá vỡ* có nghĩa chỉ bất cứ phương pháp tấn công nào nhanh hơn tấn công kiểu duyệt toàn bộ. Vì thế một tấn công cần thực hiện 2120 cũng được coi là thành công mặc dù tấn công này chưa thể thực hiện trong thực tế. Tại thời điểm hiện nay, nguy cơ này không thực sự nguy hiểm và có thể bỏ qua. Tấn công kiểu duyệt toàn bộ quy mô nhất đã từng thực hiện là do distributed.net thực hiện lên hệ thống 64 bít RC5 vào năm 2002 (Theo định luật Moore thì nó tương đương với việc tấn công vào hệ thống 66 bit hiện nay).

Một vấn đề khác nữa là cấu trúc toán học của AES. Không giống với các thuật toán mã hóa khác, AES có mô tả toán học khá đơn giản. Tuy điều này chưa dẫn đến mối nguy hiểm nào nhưng một số nhà nghiên cứu sợ rằng sẽ có người lợi dụng được cấu trúc này trong tương lai.

Vào năm 2002, Nicolas Courtoris 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.