Tìm hiểu về AES (Advanced Encryption Standard)

AES là viết tắt của Advanced Encryption Standard, chuẩn mã hóa dữ liệu rất phổ biến, dùng cho nhiều mục đích và được cả chính phủ Mỹ sử dụng để bảo vệ các dữ liệu tuyệt mật.

AES là kiểu mã hóa đối xứng dạng khối, nghĩa là mỗi khối văn bản có một kích thước nhất định (128 bit) được mã hóa, khác với mã hóa dạng chuỗi khi từng kí tự được mã hóa. Đối xứng nghĩa là khóa để mã hóa và giải mã đều là một.

Lịch sử AES

AES được phát triển từ cuối những năm 90s để thay thế chuẩn mã hóa trước đó là Data Encryption Standard (DES) do IBM tạo ra đầu những năm 70s. Nó được chính phủ Mỹ dùng trong năm 1977 nhưng sau đó có nhiều lỗ hổng dễ bị tấn công (brute force, phân tích mật mã khác biệt/tuyến tính) do dựa trên thuật toán 56 bit, nên không còn hữu ích nữa khi vi xử lý máy tính ngày càng mạnh hơn.

Vào năm 1998, DES trở thành 3DES hay còn gọi là Triple DES, dùng thuật toán DES để truyền thông điệp 3 lần liên tiếp với 3 khóa mã hóa khác nhau. 3DES khiến dữ liệu an toàn hơn trước kiểu tấn công brute force thời đó.

15 thuật toán được đề xuất thay thế DES, bắt đầu quy trình 5 năm của chính phủ Mỹ. AES được hai nhà mật mã học là Vincent Rijmen và Joan Daemen đề xuất, sau được gọi là "đơn Rijindael".

AES là chuẩn mở vì khi đó chuẩn thực sự cũng chưa được xác định. Trong quá trình thiết kế, nó cũng nhận bình luận, góp ý. Nó được Viện tiêu chuẩn và kỹ thuật quốc gia Hoa Kỳ phát triển với mục tiêu dễ dùng cho cả phần cứng và phần mềm. Một số thay đổi về khóa và khối được thực hiện để tăng tính an toàn.

NSA cũng tham gia xem xét 15 bản đề xuất. Tới tháng 8/1999 chỉ còn 5 thuật toán (Rijndael, Serpent, RC6, Twofish và MARS). Các "ứng viên" được phân tích thêm về độ bảo mật, tính dễ sử dụng, bản quyền, tốc độ, độ chính xác khi mã hóa và giải mã.

Người chiến thắng sau cùng là Rijndael, sau đó được đưa lên cho chính phủ Mỹ vào năm 2002 và cả NSA cùng các tổ chức khác. Đến giờ, AES vẫn được dùng cho các tài liệu tuyệt mật, được cho là FIPS (Federal Information Processing Standard -

tiêu chuẩn xử lý thông tin liên bang). Sau đó nó được dùng trong khối tư nhân, là chuẩn mã hóa phổ biến nhất với mã hóa khóa đối xứng.

AES là chuẩn mã hóa khối đối xứng phổ biến

AES hoạt động như thế nào?

AES là kiểu mã hóa khối, mỗi khối kích thước 128 bit. Khóa đối xứng với 3 kích thước là 128, 192 và 256 bit, trong đó 2 kích thước sau được chính phủ Mỹ dùng cho các tài liệu mật cấp cao, được gọi là "Top Secret".

Rijndael ban đầu được phép thêm khối và tăng độ dài khóa nhưng chuẩn sau này bị bỏ, giữ chuẩn kích thước như đã nói ở trên. AES là chuẩn mã hóa duy nhất được phát hành rộng rãi được NSA chấp thuận dùng để bảo vệ thông tin chính phủ ở mức cao cấp nhất.

AES dùng thuật toán mã hóa khối mạng thay thế hoán đổi (SPN - Substitution Permutation Network). Dữ liệu được chuyển thành dạng an toàn trong vài bước, bắt đầu là khối plain text kích thước chuẩn, sau đó chèn vào hàng và sau đó là mã hóa. Mỗi lần đều có các bước thay thế, chuyển đổi, hòa trộn.

Cũng như 3DES có 3 bước mã hóa, AES cũng có nhiều bước nhưng được thực hiện nhiều hơn, phụ thuộc vào độ dài khóa, với khóa 128 bit là 10 lần, khóa 192 bit là 12 lần và khóa 256 bit là 14 lần.

Trong quá trình này, khóa mã hóa được tạo và cũng phải có khóa này để giải mã. Nếu không, dữ liệu sẽ chỉ là mớ lộn xộn không thể đọc được. Cả người gửi và người nhận đều phải biết khóa mã hóa và giải mã.