5 thuật toán mã hóa phổ biến bạn nên biết

Bạn đã từng nghe hoặc sử dụng mã hóa và biết tầm quan trọng của nó như thế nào. Phần lớn các dịch vụ Internet sử dụng mã hóa để giữ thông tin người dùng an toàn. Tuy nhiên, mã hóa vẫn là một thứ gì đó khó hiểu. Có nhiều loại mã hóa và được sử dụng với nhiều mục đích. Làm thế nào bạn biết được kiểu mã hóa "tốt nhất"? Chúng ta hãy xem xét cách thức hoạt động của một số loại mã hóa chính sau đây nhé và lý do tại sao bạn không nên tạo mã hóa của riêng mình.

So sánh kiểu mã hóa với độ mạnh mã hóa

Những thuật ngữ mã hóa như kiểu mã hóa, thuật toán mã hóa và độ mạnh mã hóa thường khiến người dùng nhầm lẫn, hãy phân tích nó nhé:

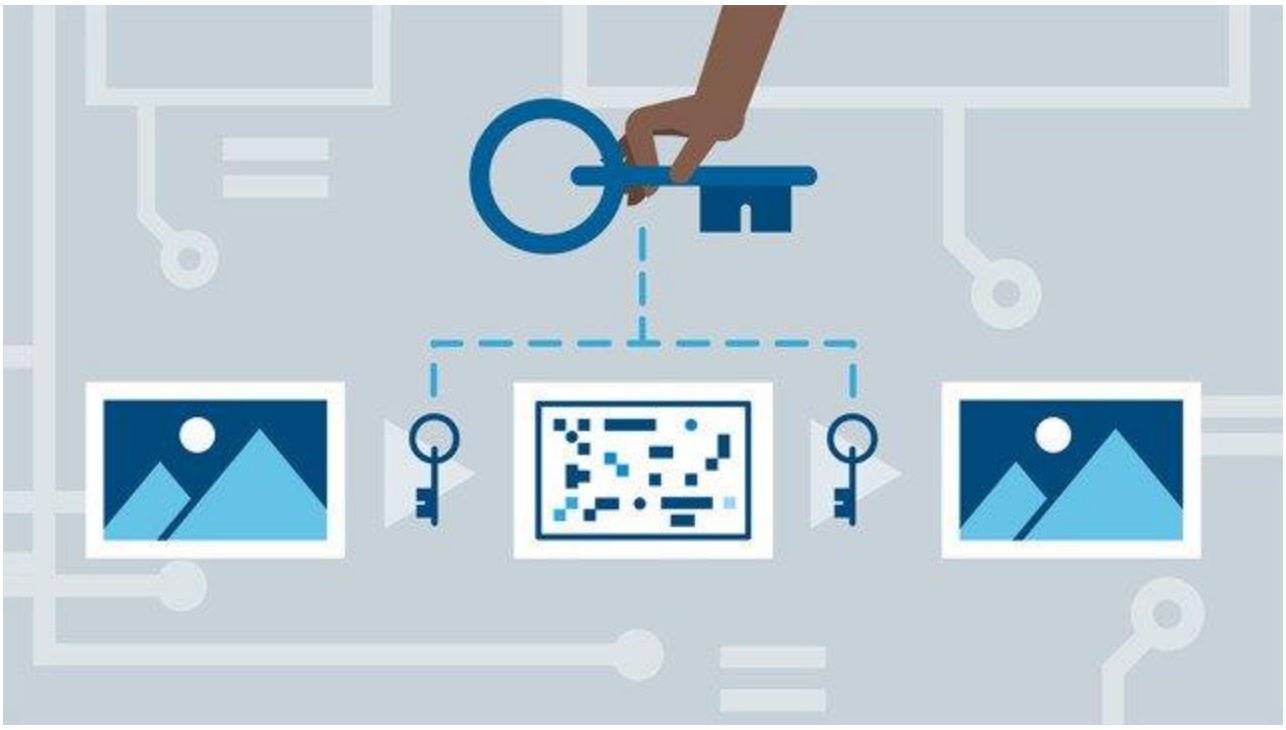
- **Kiểu mã hóa**: là loại mã hóa liên quan đến cách mã hóa được hoàn thành. Ví dụ, mã hóa đối xứng (asymmetric cryptography) là một trong những kiểu mã hóa phổ biến nhất trên Internet.
- **Thuật toán mã hóa**: Khi nói về độ mạnh mã hóa, chúng ta thường nói về một thuật toán mã hóa cụ thể. Các thuật toán có tên thú vị như Triple DES, RSA hoặc AES. Tên thuật toán mã hóa thường đi kèm với giá trị bằng số, như AES-128. Con số này đề cập đến kích thước khóa mã hóa và xác định thêm độ mạnh của thuật toán.

5 thuật toán mã hóa phổ biến nhất

Các loại mã hóa tạo thành nền tảng cho thuật toán mã hóa, trong khi thuật toán mã hóa chịu trách nhiệm về độ mạnh mã hóa. Chúng ta nói về độ mạnh mã hóa theo bit. Dưới đây là một số thuật toán mã hóa phổ biến nhất.

1. Data Encryption Standard (Tiêu chuẩn mã hóa dữ liệu - DES)

Data Encryption Standard là tiêu chuẩn mã hóa ban đầu của chính phủ Mỹ. Ban đầu nó được cho là không thể phá vỡ nhưng sự ra tăng về sức mạnh máy tính và giảm chi phí phần cứng đã khiến mã hóa 56-bit lỗi thời. Điều này đặc biệt đúng với dữ liệu nhạy cảm.

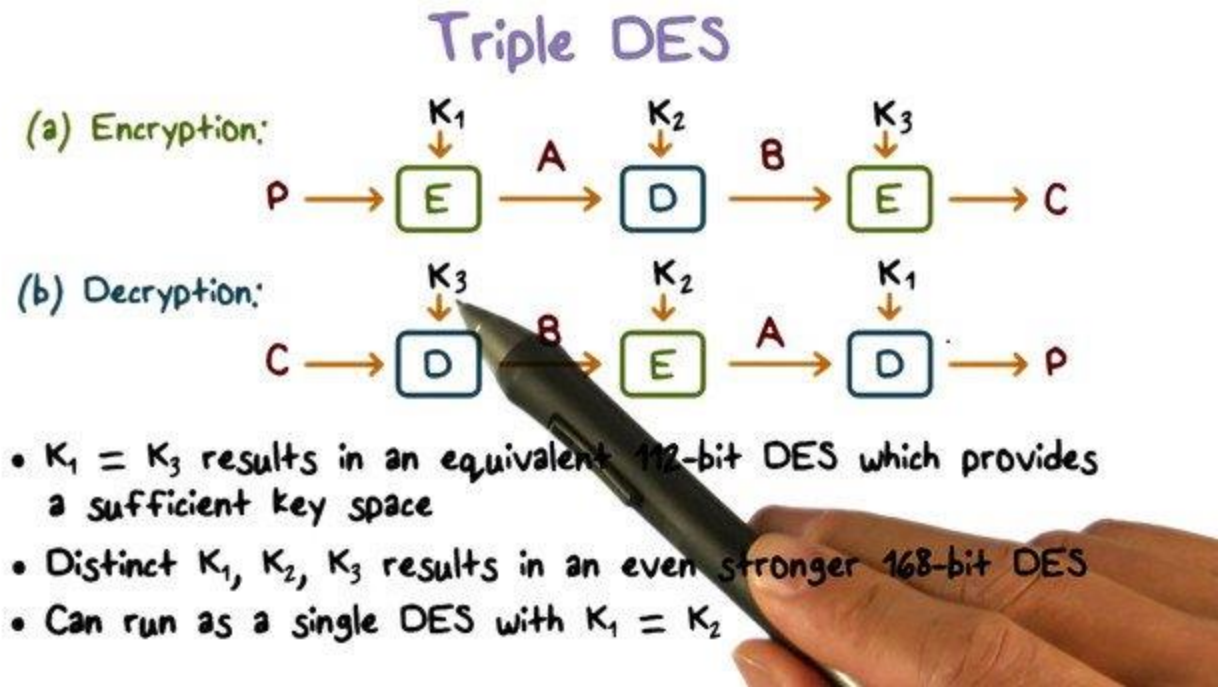


John Gilmore, người đồng sáng lập EFF, đứng đầu dự án Deep Crack, đã nói: “Khi thiết kế hệ thống an toàn và cơ sở hạ tầng cho xã hội, hãy lắng nghe các nhà mật mã học, chứ không phải các chính trị gia”. Ông cảnh báo cho những người sử dụng mã hóa DES để lưu trữ dữ liệu riêng tư rằng thời gian kỷ lục để crack DES ngắn, do đó nên cẩn thận khi dùng.

Tuy nhiên, bạn vẫn sẽ tìm thấy DES trong nhiều sản phẩm vì nó mã hóa ở mức độ thấp dễ thực hiện mà không đòi hỏi một lượng lớn công suất tính toán.

2. TripleDES

TripleDES (đôi khi được viết là 3DES hoặc TDES) là phiên bản DES mới hơn, an toàn hơn. Khi DES bị crack trong thời gian chưa đầy 23 giờ, người ta nhận ra vấn đề, do vậy, đây là lý do mà TripleDES được sinh ra. TripleDES tăng tốc quy trình mã hóa bằng cách chạy DES ba lần.



Dữ liệu được mã hóa, giải mã và sau đó được mã hóa một lần nữa, đem đến độ dài khóa hiệu quả là 168 bit. Nó đủ dài cho những dữ liệu nhạy cảm nhất. Tuy nhiên, mặc dù TripleDES dài hơn tiêu chuẩn DES nhưng nó cũng có những sai sót.

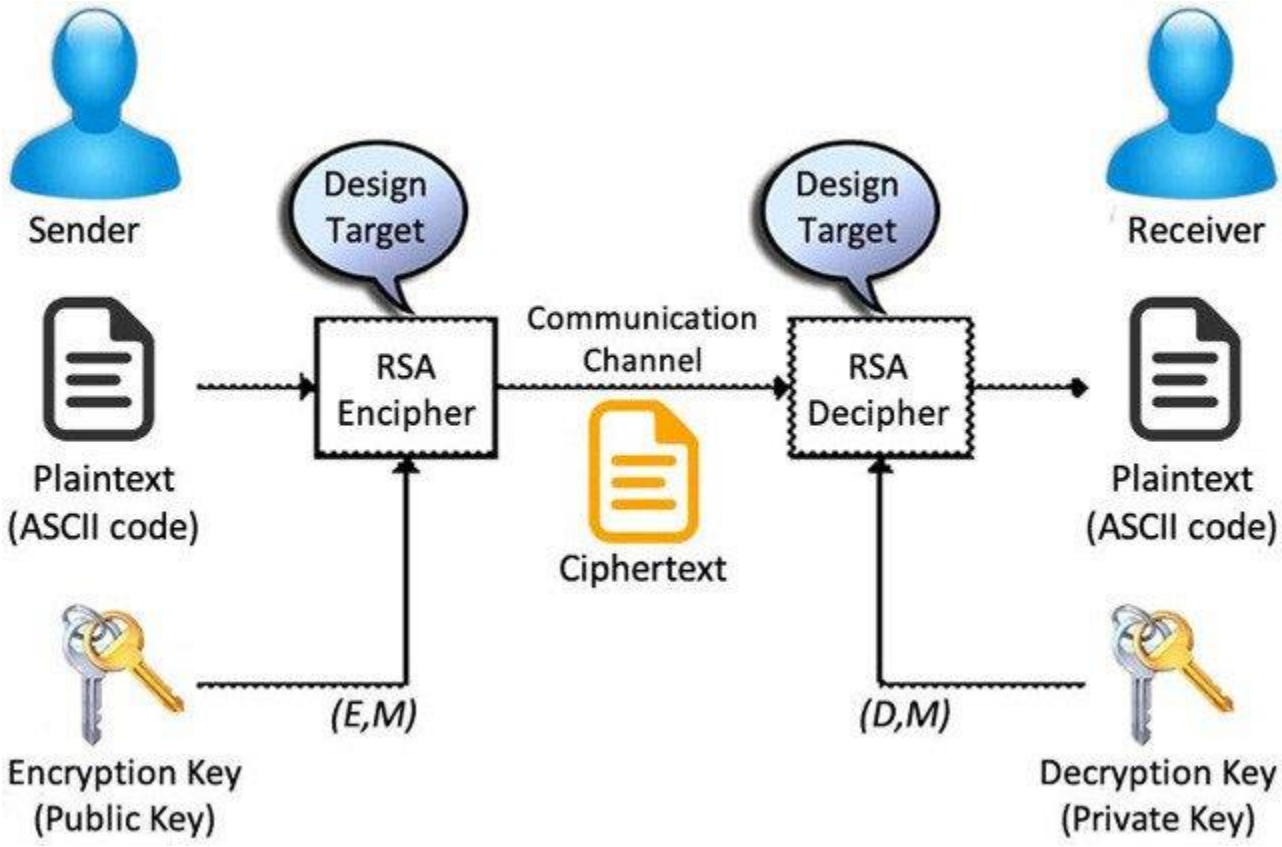
TripleDES có ba tùy chọn khóa:

- **Tùy chọn Key 1:** Tất cả ba khóa đều độc lập. Phương pháp này cung cấp cường độ khóa mạnh nhất: 168 bit.
- **Tùy chọn Key 2**: Key 1 và Key 2 là độc lập, trong khi Key 3 giống với Key 1. Phương pháp này cung cấp cường độ khóa hiệu quả là 112 bit (2 × 56 = 112).
- **Tùy chọn Key 3**: Cả ba khóa đều giống nhau. Phương pháp này cung cấp khóa 56 bit.

Tùy chọn Key 1 là mạnh nhất. Tùy chọn Key 2 không mạnh, nhưng vẫn cung cấp sự bảo vệ nhiều hơn gấp hai lần so với mã hóa DES. TripleDES là một thuật toán mã hóa khối, nghĩa là dữ liệu được mã hóa theo một kích thước khối cố định. Tuy nhiên, kích thước khối TripleDES nhỏ 64 bit, làm cho nó hơi nhạy cảm với các cuộc tấn công nhất định (như xung đột khối).

3. RSA

RSA (được đặt tên theo người sáng tạo của nó là Ron Rivest, Adi Shamir và Leonard Adleman) là một trong những thuật toán mã hóa khóa công khai đầu tiên. Nó sử dụng hàm mã hóa bất đối xứng một chiều.



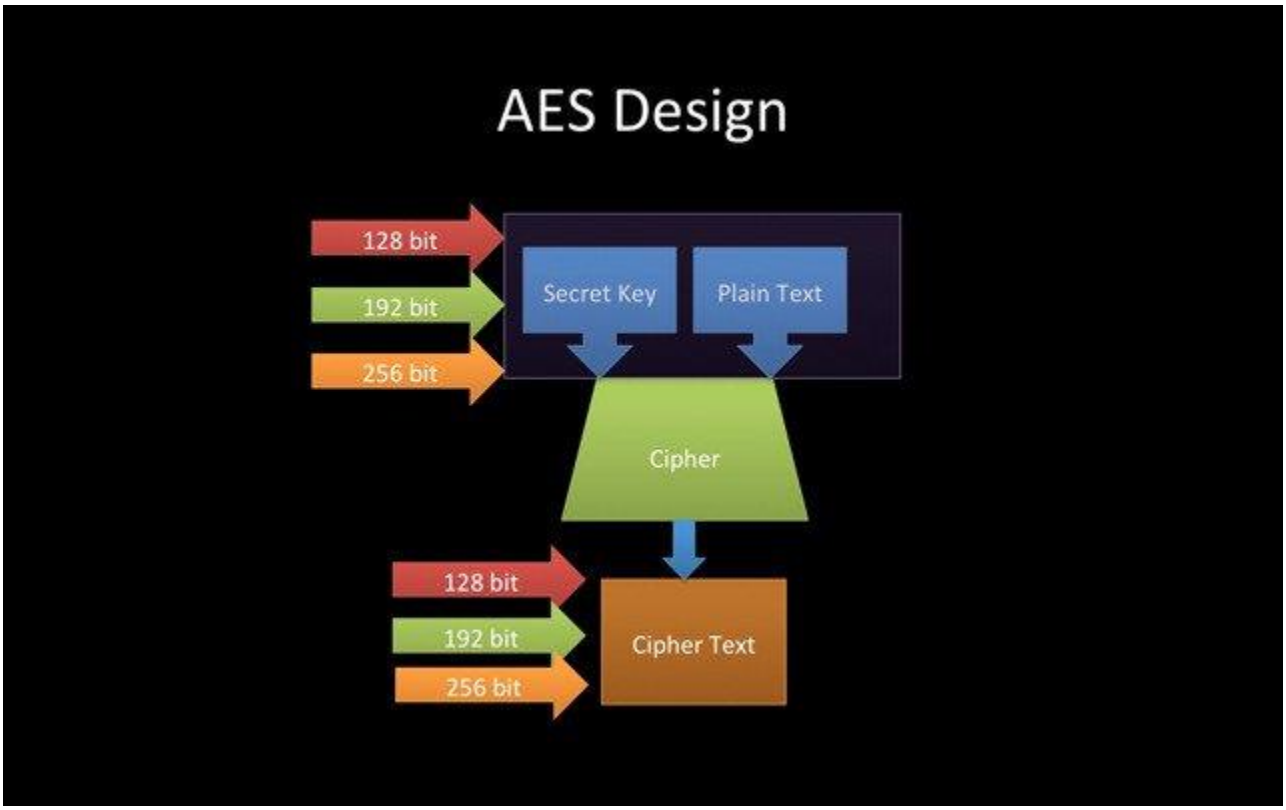
Thuật toán RSA được sử dụng rộng rãi trên Internet. Nó là tính năng chính của nhiều giao thức bao gồm SSH, OpenPGP, S/MIME và SSL/TLS. Ngoài ra, trình duyệt sử dụng RSA để thiết lập giao tiếp an toàn qua mạng không an toàn.

RSA vẫn rất phổ biến do độ dài khóa của nó. Một khóa RSA thường dài 1024 hoặc 2048 bit. Tuy nhiên, các chuyên gia bảo mật tin rằng không mất nhiều thời gian để crack RSA 1024 bit, do đó nhiều tổ chức phải chuyển sang khóa 2048 bit mạnh mẽ hơn.

4. Advanced Encryption Standard (Tiêu chuẩn mã hóa tiên tiến - AES)

Advanced Encryption Standard (AES) hiện là tiêu chuẩn mã hóa của Chính phủ Hoa Kỳ sử dụng. Nó dựa trên thuật toán Rijndael được phát triển bởi hai nhà mật

mã người Bỉ, Joan Daemen và Vincent Rijmen. Các nhà mật mã học người Bỉ đã gửi thuật toán của họ đến Viện Tiêu chuẩn và Kỹ thuật Quốc gia (National Institute of Standards and Technology - NIST), cạnh tranh với 14 thuật toán mã hóa khác để trở thành kiểu mật mã tiếp theo sau DES. Rijndael "thắng" và được chọn là thuật toán AES được đề xuất vào tháng 10 năm 2000.



AES là thuật toán khóa đối xứng và sử dụng mật mã khối đối xứng. Nó bao gồm ba kích thước chính: 128, 192 hoặc 256 bit. Hơn nữa, có các vòng mã hóa khác nhau cho mỗi kích thước khóa. Một 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.

Có những cuộc tấn công lý thuyết chống lại thuật toán AES, nhưng tất cả đều yêu cầu lưu trữ dữ liệu cụ thể và thời gian nhất định, do đó không khả thi trong thời điểm hiện tại. Ví dụ, một cuộc tấn công vào mã hóa AES cần 38 nghìn tỷ dữ liệu, nhiều hơn tất cả dữ liệu được lưu trữ trên tất cả các máy tính trên toàn thế giới trong năm 2016. Ước tính thời gian cần thiết để tạo tấn công brute-force khóa AES-128 là hàng tỷ năm.

Như vậy, chuyên gia mật mã Bruce Schneier không “tin rằng ai có thể khám phá ra một cuộc tấn công đọc được lưu lượng truy cập Rijndael”. Thuật toán mã hóa Twofish của Schneiers (được thảo luận dưới đây) là một đối thủ của Rijndael trực tiếp trong cuộc cạnh tranh để chọn thuật toán an ninh quốc gia mới.

5. Twofish

Twofish là tiêu chuẩn được lọt vào "vòng chung kết" trong cuộc tuyển chọn thuật toán an ninh quốc gia và thua Rijndael. Thuật toán Twofish hoạt động với các kích thước khóa 128, 196 và 256 bit và có cấu trúc khóa phức tạp khiến nó khó có thể bị bẻ khóa.

Các chuyên gia bảo mật coi Twofish là một trong những thuật toán mã hóa nhanh nhất và là một lựa chọn tuyệt vời cho cả phần cứng và phần mềm. Hơn nữa, mật mã Twofish miễn phí cho tất cả người dùng. Nó xuất hiện trong một số phần mềm mã hóa miễn phí tốt nhất, chẳng hạn như VeraCrypt (mã hóa ổ đĩa), PeaZip (file lưu trữ) và KeePass (quản lý mật khẩu nguồn mở), cũng như tiêu chuẩn OpenPGP.

Tại sao không nên tạo thuật toán mã hóa riêng?

Bạn đã thấy một số thuật toán mã hóa tốt nhất, bởi vì về cơ bản chúng không thể phá vỡ, ít nhất trong thời gian này. Các thuật toán mã hóa này được thử nghiệm với sự kết hợp của các máy tính mạnh nhất cùng với những bộ não thông minh nhất. Các thuật toán mã hóa mới phải trải qua một loạt các thử nghiệm nghiêm ngặt.

Lấy thuật toán AES làm ví dụ:

- NIST đã kêu gọi các nhà mã hóa tạo ra các thuật toán mã hóa mới vào tháng 9 năm 1997.
- NIST đã nhận được 15 thuật toán AES tiềm năng vào tháng 8 năm 1998.
- Tại một hội nghị vào tháng 4 năm 1999, NIST đã chọn năm thuật toán cuối cùng: MARS, RC6, Rijndael, Serpent và Twofish.
- NIST tiếp tục kiểm tra và nhận các ý kiến đóng góp, chỉ dẫn từ cộng đồng mật mã cho đến tháng 5 năm 2000.
- Vào tháng 10 năm 2000, NIST đã xác nhận Rijndael là AES tiềm năng, sau đó bắt đầu một giai đoạn tư vấn khác.

- Rijndael, với tư cách là AES, đã được công bố như một tiêu chuẩn xử lý thông tin liên bang vào tháng 11 năm 2001. Việc xác nhận bắt đầu kiểm tra theo Chương trình phê chuẩn thuật toán mật mã.
- AES đã trở thành tiêu chuẩn mã hóa của chính phủ chính thức vào tháng 5 năm 2002.

Bạn thấy đấy, việc sản xuất mã hóa thực sự là một quá trình an toàn, lâu dài và mạnh mẽ cần có thời gian và phân tích chuyên sâu từ một số tổ chức bảo mật mạnh mẽ nhất trên hành tinh. Do đó, bạn không có tài nguyên để tạo ra một thuật toán mạnh. Như Bruce Schneier nói: “Bất cứ ai cũng có thể phát minh ra một thuật toán mã hóa mà bản thân họ không thể phá vỡ; nhưng khó phát minh ra một thứ mà không ai khác có thể phá vỡ được”.