Mã hóa dữ liệu là gì? Những điều cần biết về mã hóa dữ liệu

Một trong những phương thức bảo mật dữ liệu an toàn và được sử dụng phổ biến trong thời đại kỹ thuật số hiện nay là mã hóa dữ liệu. Tuy nhiên, không phải ai cũng hiểu rõ mã hóa dữ liệu là gì, nó có chức năng ra sao và quá trình mã hóa diễn ra như thế nào. Trong bài viết này, Quản Trị Mạng sẽ cùng với các bạn tìm hiểu những kiến thức cơ bản về mã hóa dữ liệu nhé.

1. Mã hóa dữ liệu là gì?

Mã hóa dữ liệu là chuyển dữ liệu từ dạng này sang dạng khác hoặc sang dạng code mà chỉ có người có quyền truy cập vào khóa giải mã hoặc có **mật khẩu** mới có thể đọc được nó. Dữ liệu được mã hóa thường gọi là ciphertext, dữ liệu thông thường, không được mã hóa thì gọi là plaintext.

Hiện tại, mã hóa dữ liệu là một trong những phương pháp bảo mật dữ liệu phổ biến và hiệu quả nhất, được nhiều tổ chức, cá nhân tin tưởng. Thực chất việc mã hóa dữ liệu sẽ không thể nào ngăn việc dữ liệu có thể bị đánh cắp, nhưng nó sẽ ngăn việc người khác có thể đọc được nội dung của tập tin đó, vì nó đã bị biến sang thành một dạng ký tự khác, hay nội dung khác.

Có hai loại mã hóa dữ liệu chính tồn tại: mà hóa bất đối xứng, còn được gọi là mã hóa khóa công khai, và mã hóa đối xứng.

2. Chức năng chính của mã hóa dữ liệu

Mục đích của việc mã hóa dữ liệu là bảo vệ dữ liệu số khi nó được lưu trữ trên các hệ thống máy tính và truyền qua Internet hay các mạng máy tính khác. Các thuật toán mã hóa thường cung cấp những yếu tố bảo mật then chốt như xác thực, tính toàn vẹn và không thu hồi. Xác thực cho phép xác minh nguồn gốc của dữ liệu, tính toàn vẹn chứng minh rằng nội dung của dữ liệu không bị thay đổi kể từ khi nó được gửi đi. Không thu hồi đảm bảo rằng người người không thể hủy việc gửi dữ liệu.

Quá trình mã hóa sẽ biến nội dung sang một dạng mới, vì thế sẽ tăng thêm một lớp bảo mật cho dữ liệu. Như vậy cho dù dữ liệu của bạn bị đánh cắp thì việc giải mã dữ liệu cũng vô cùng khó khăn, tốn nhiều nguồn lực tính toán và cần rất nhiều thời gian. Với những công ty, tổ chức thì việc sử dụng mã hóa dữ liệu là điều cần thiết. Điều này sẽ tránh được những thiệt hại khi những thông tin mật nếu vô tình bị lộ ra ngoài, cũng khó lòng giải mã ngay lập tức.

Hiện nay có rất nhiều ứng dụng tin nhắn đều sử dụng mã hóa nhằm bảo mật tin nhắn cho người dùng. Chúng ta có thể kể đến Facebook, WhatApps với loại mã hóa sử dụng được gọi là End-to-End.

3. Quá trình mã hóa dữ liệu

Dữ liệu hoặc plaintext được mã hóa với một thuật toán mã hóa và một key mã hóa, tạo ra một ciphertext. Dữ liệu sau khi mã hóa chỉ có thể xem được dưới dạng ban đầu nếu giải mã với các key chính xác.

Mã hóa đối xứng sử dụng cùng một khóa bí mật để mã hóa và giải mã dữ liệu. Mã hóa đối xứng nhanh hơn nhiều so với mã hóa bất đối xứng, vì khi mã hóa bất đối xứng người gửi phải trao đổi khóa mã hóa với người nhận trước khi người nhận có thể giải mã dữ liệu. Vì các công ty cần phải phân phối một cách an toàn và quản lý số lượng lớn các khóa, nên hầu hết các dịch vụ mã hóa dữ liệu cũng nhận thấy điều này và đều sử dụng mã hóa bất đối xứng để trao đổi khóa bí mật sau khi sử dụng một thuật toán đối xứng để mã hóa dữ liệu.

Thuật toán mã hóa bất đối xứng còn được gọi là mã hóa khóa công khai, sử dụng 2 khóa khác nhau, một công khai và một riêng tư. Chúng ta sẽ tìm hiểu về hai khóa này trong phần tiếp theo.

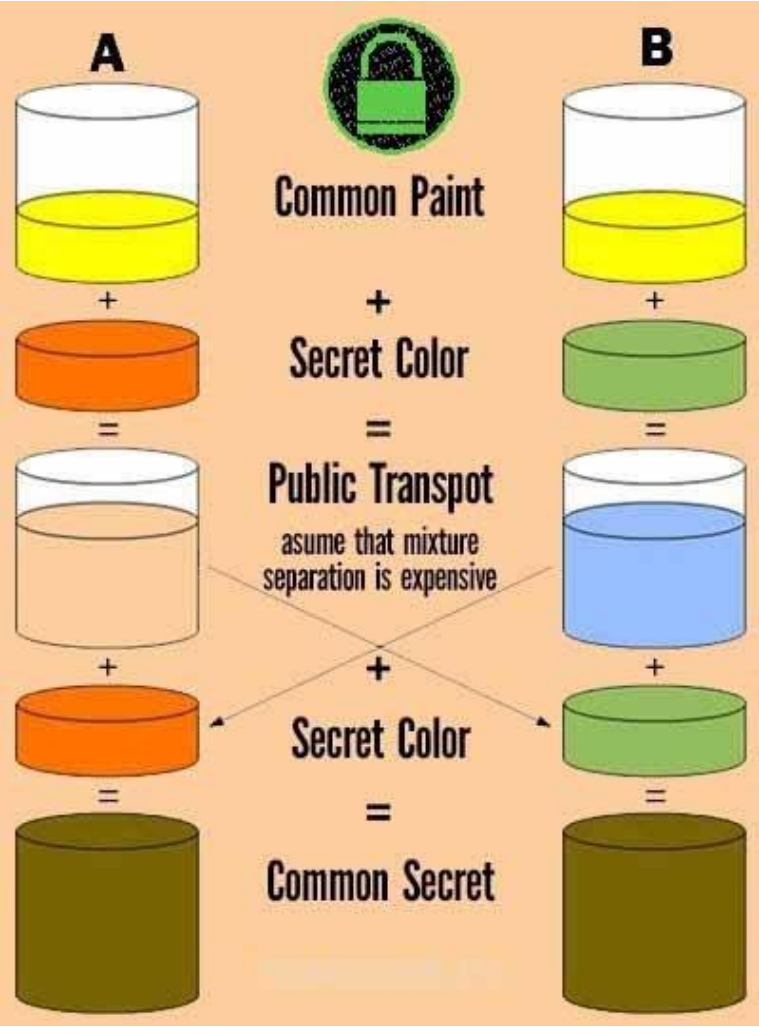
4. Mã hóa dữ liệu End-to-End là gì?

End-to-End Encryption (E2EE) là phương thức mã hóa mà chỉ người nhận và gửi có thể hiểu được thông điệp mã hóa này mà thôi. Sẽ không ai biết được những nội dung mà chúng ta đang truyền tải, kể cả những nhà cung cấp dịch vụ Internet.

Phương thức mã hóa này sử dụng mã khóa giữa người nhận và người gửi đang trực tiếp tham gia vào quá trình gửi dữ liệu. Trừ khi bên thứ 3 biết được mã khóa này thì sẽ không thể nào giải mã được.

Cơ chế hoạt động của loại mã hóa End-to-End thông qua giao thức trao đổi khóa Diffie-Hellman. Chúng ta có thể hiểu qua ví dụ gửi tin nhắn, 2 người sẽ tiến hành gửi đi một mã khóa công khai và một mã khóa bí mật. Tin nhắn lúc đó sẽ được tiến hành mã hóa bằng khóa bí mật kết hợp với khóa công khai. Và lúc đó người nhận sẽ sử dụng khóa bí mật để có thể giải mã được thông tin và nội dung tin nhắn.

Vậy khóa bí mật và khóa công khai là gì?

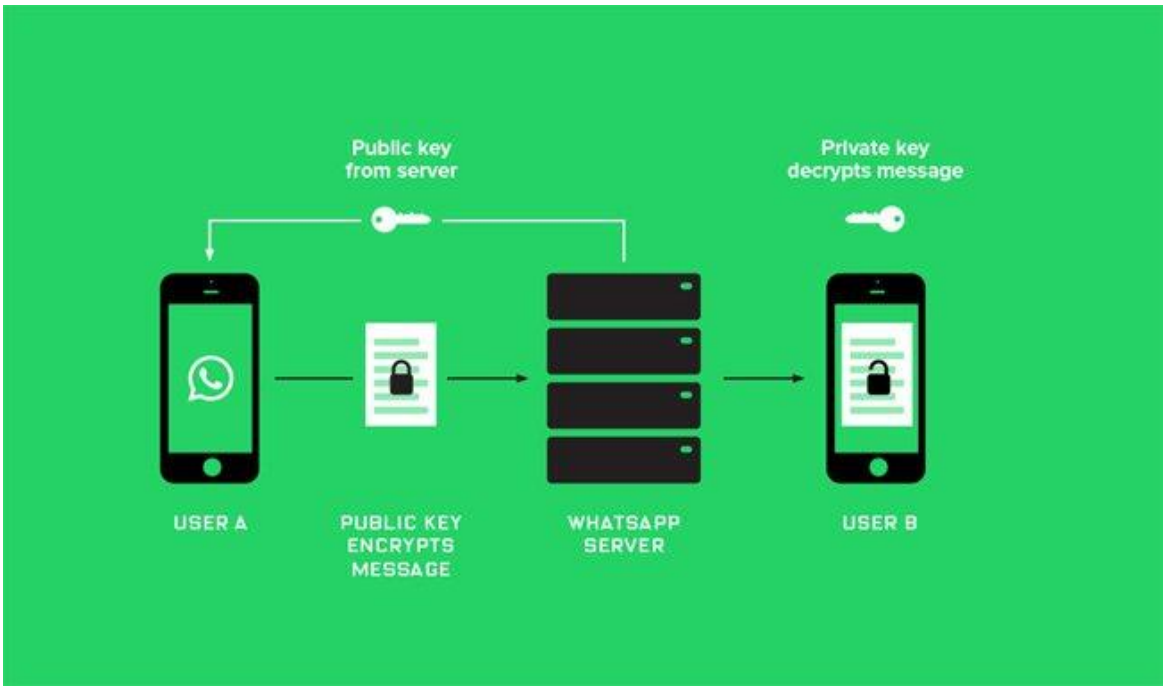


5. Khóa bí mật và khóa công khai trong End-to-End Encryption?

2 loại khóa này đều được tạo nên từ những dãy số ngẫu nhiên. Khóa công khai sẽ được chia sẻ với mọi người, nhưng khóa bí mật phải được bảo vệ, nó sẽ nằm hoàn toàn ở người có quyền giải mã. 2 mã này hoạt động với nhiệm vụ hoàn toàn khác nhau. Khóa công khai sẽ tiến hành mã hóa dữ liệu, thay đổi nội dung tài liệu. Còn khóa bí mật sẽ đảm nhận nhiệm vụ giải mã nội dung.

Như vậy khi người gửi tin nhắn mã hóa dữ liệu bằng khóa công khai, và người nhận sẽ tiến hành giải mã bằng khóa bí mật và ngược lại.

Thuật toán Rivest-Sharmir-Adleman (RSA) là hệ thống mã hóa khóa công khai, được sử dụng rộng rãi để bảo vệ dữ liệu nhạy cảm, đặc biệt là khi nó được gửi qua một mạng không an toàn như Internet. Sự phổ biến của thuật toán này là do cả khóa công khai và khóa bí mật của nó đều có thể mã hóa dữ liệu và đảm bảo tính bí mật, toàn vẹn, xác thực và không thu hồi của dữ liệu và truyền thông kỹ thuật số thông qua việc sử dụng chữ ký số.



6. Thách thức đối với mã hóa dữ liệu đương đại

Hầu hết phương thức tấn công cơ bản vào mã hóa hiện nay là Brute Force (thử và sai liên tục) và thử các khóa ngẫu nhiên cho đến khi khóa đúng được tìm thấy. Có thể giảm thiểu xác suất mở khóa bằng cách tăng chiều dài, độ phức tạp của khóa. Mã hóa càng mạnh thì tài nguyên cần để thực hiện tính toán sẽ tăng lên, cần nhiều thời gian và vật lực hơn để phá mã.

Các phương pháp phá vỡ mã hóa khác bao gồm tấn công kênh phụ và phân tích mật mã. Tấn công kênh bên xảy ra sau khi việc mã hóa hoàn tất thay vì tấn công trực tiếp vào mã hóa. Những cuộc tấn công này có khả năng thành công nếu có lỗi trong thiết kế hệ thống hoặc thực thi. Tương tự như vậy, phân tích mật mã sẽ tìm

điểm yếu trong mã hóa và khai thác nó. Kiểu tấn công này có thể thành công nếu có lỗ hổng trong mật mã.

Nhìn chung, việc mã hóa dữ liệu là điều cần thiết để chúng ta có thể tăng sự bảo mật hơn cho tài liệu, đặc biệt là những kiểu tài liệu mật, thông tin tài khoản cá nhân. Hiện nay, việc mã hóa dữ liệu có thể được thực hiện thông qua một số công cụ online như Whisply, hay Nofile.io.

Hy vọng bài viết trên hữu ích với bạn!