Journal of educational equipment: Applied research, Volume 2, Issue 305 (January 2024)
ISSN 1859 - 0810

Mã hóa dựa trên định danh IBE, cung cấp một giải pháp bảo mật thông tin trong trường học

Mai Thị Hoa Huê*

**Trường Đại học Hạ Long*

Received: 2/11/2023; Accepted: 22/11/2023; Published: 20/12/2023

Abstract: *IBE identity-based encryption provides an easy-to-implement solution that still ensures data confidentiality. Not only ensuring integrity, availability, authenticity and non-repudiation. They are more easily provided by digital signatures because the keys are generated and managed by a traditional public key system.*

Keywords: *IBE identifier.*

1. Đặt vấn đề

Giấu thông tin là một kỹ thuật nhúng thông tin vào trong một nguồn đa phương tiện gọi là các phương tiện chứa mà không cần gây ra sự nhận biết về sự tồn tại của thông tin giấu. Phương pháp giấu tin là làm cho người khác khó có thể biết được có thông tin giấu bên trong đó do tính chất ẩn của thông tin được giấu.

Việc giấu thông tin, cụ thể hơn, mật mã học là ngành học nghiên cứu về những cách thức chuyển đổi thông tin từ dạng "có thể hiểu được" thành dạng "không thể hiểu được" và ngược lại. Mã hóa dựa trên định danh trở thành một giải pháp hiệu quả trong sử dụng mật mã khóa công khai để mã hóa thông tin.

2. Nội dung nghiên cứu

Khái niệm Mã hoá: Mã hóa dựa trên định danh (Indetity based encryption -IBE) hiện nay đang được xem là một công nghệ mật mã mới có nhiều thuận tiện trong thực thi ứng dụng so với các thuật toán khóa công khai khác. Đối với các hệ mật mã khóa công khai truyền thống, việc cài đặt là khó khăn và tốn kém, ứng dụng thành công nhất của công nghệ khóa công khai là việc sử dụng rộng rãi của SSL, nó yêu cầu tương tác tối thiểu với người sử dụng khi được dùng để xác thực máy chủ và mã hóa các truyền thông với máy chủ đó. Các ứng dụng mà yêu cầu người sử dụng quản lý hoặc sử dụng các khóa công khai thì không thành công được như vậy. IBE là một công nghệ mã hoá khoá công khai, cho phép một người sử dụng tính khoá công khai từ một chuỗi bất kỳ. Chuỗi này như là biểu diễn định danh của dạng nào đó và được sử dụng không chỉ như là một định danh để tính khoá công khai, mà còn có thể chứa thông tin về thời hạn hợp lệ của khoá để tránh cho một người sử dụng dùng mãi một khoá IBE hoặc để đảm bảo rằng người sử dụng sẽ nhận được các khoá khác nhau từ các hệ thống IBE khác nhau. Trong chuỗi này có chứa thông tin là duy nhất đối với mỗi cài đặt IBE cụ thể, chẳng hạn như URL mà định danh máy chủ được sử dụng trong cài đặt của các hệ thống IBE khác nhau. Khả năng tính được các khoá như mong muốn làm cho các hệ thống IBE có các tính chất khác với các tính chất của các hệ thống khoá công khai truyền thống, những tính chất này tạo ra các ưu thế thực hành đáng kể trong nhiều tình huống. Bởi vậy, có một số ít tình huống không thể giải quyết bài toán bất kỳ với các công nghệ khoá công khai truyền thống, nhưng lại có thể giải quyết được với IBE và sử dụng IBE có thể đơn giản hơn nhiều về cài đặt và ít tốn kém hơn về nguồn lực để hỗ trợ

2.1. Mật mã dựa trên định danh

2.1.1.Mật mã dựa trên định danh

IBE (Indetity Base Encryption) là một công nghệ mã hoá khoá công khai, cho phép một người sử dụng tính khoá công khai từ một chuỗi bất kỳ.

2.1.2.Ưu thế IBE trong các ứng dụng thực tế

IBE cho phép người sử dụng giao tiếp an toàn, có thể xác minh chữ ký dễ dàng mà không cần trao đổi các mã khóa công khai hoặc khóa riêng. Không cần lưu giữ bí mật các thư mục quan trọng, cũng như không cần sử dụng dịch vụ của bên thứ ba.

2.1.3. Hệ thống nhận dạng IBE

Một cách tổng quan, hệ thống bảo mật IBE phụ thuộc vào những vấn đề sau đây:

A. Bảo mật của chức năng mã hóa cơ bản.

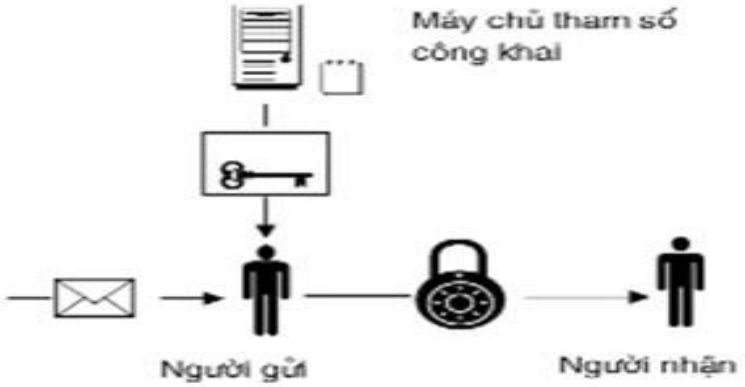
B. Lưu trữ và giữ bí mật tuyệt đối các thông tin cá nhân tại trung tâm tạo mã.

C. Kiểm tra triệt để danh tính khách hàng trước khi cấp phát hành thẻ cho người dùng.

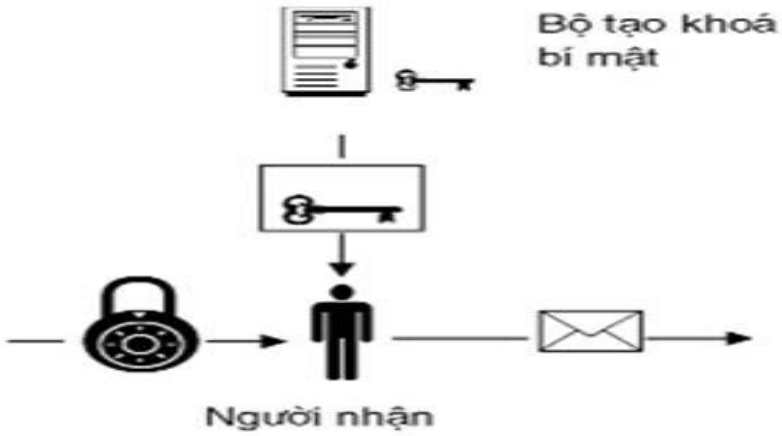
D. Các biện pháp phòng ngừa được thực hiện bởi người sử dụng để ngăn chặn sự mất mát, sao chép, hoặc sử dụng trái phép thẻ của họ.

2.2. Mã hóa dựa trên định danh IBE

IBE lần đầu tiên được Adi Shamir nói tới vào năm 1984, khi ông mô tả một cách khái lược về các tính chất và cách thức sử dụng một hệ thống như vậy. Mặc dù ông chưa thực hiện được một công nghệ an toàn và khả thi hoạt động như đã mô tả, song các ưu thế về khả năng sử dụng của IBE so với các công nghệ khác.



Mã hoá bằng hệ thống IBE



Giải mã bằng hệ thống IBE

3. Kết luận

Mã hóa dựa trên định danh IBE cung cấp một giải pháp dễ thực thi mà vẫn đảm bảo tính bí mật của dữ liệu. Không những bảo đảm tính toàn vẹn, tính sẵn sàng, tính xác thực và không chối bỏ. Chúng được cung cấp dễ hơn bởi các chữ ký số nhờ các khoá đã được tạo ra và quản lý bởi hệ thống khoá công khai truyền thống. Ưu thế của IBE là cung cấp một giải pháp tốt cho một số trường hợp ứng dụng. Một giải pháp pha trộn sử dụng IBE cho mã hoá và hệ thống khoá công khai truyền thống để cung cấp các chữ ký số có thể là một giải pháp kết hợp được những đặc tính tốt nhất của mỗi công nghệ.

Tài liệu tham khảo

[1] Trần Duy Lai (2009), *"Mã hóa dựa trên định danh*", Tạp chí An toàn thông tin số 3- ISSN 1859-1256

[2] Hồ Văn Hương, Đào Thị Ngọc Thuỳ, *Ứng dụng hệ thống kiểm soát truy nhập mạng theo mô hình truy nhập một lần*, Tạp chí An toàn thông tin, số 1 (025) 2013.

[3] Hồ Văn Hương, Nguyễn Quốc Uy, *Giải pháp bảo mật cơ sở dữ liệu*, Tạp chí An toàn thông tin, số 3 (027) năm 2013.

[4] Hồ Văn Hương, Nguyễn Quốc Uy, Nguyễn Anh Đoàn, Tích hợp giải pháp bảo mật và xác thực cho mạng riêng ảo, *Tạp chí nghiên cứu Khoa học và Công nghệ Quân sự số 28,* 2013.