GIẢI PHÁP ỨNG DỤNG CHỮ KÝ ĐIỆN TỬ TRONG QUÁ TRÌNH GỬI VÀ NHẬN VĂN BẢN

APPLICATION OF ELECTRONIC SIGNATURES TO THE PROCESS OF SENDING AND RECEIVING TEXTS

Phan Huy Khánh, Hồ Phan Hiếu

Trường Đại học Bách khoa, Đại học Đà Nẵng

TÓM TẮT

Hiện nay, việc đảm bảo an toàn thông tin, tránh mọi nguy cơ bị thay đổi, sao chép hoặc mất mát dữ liệu trong các ứng dụng trên mạng luôn là vấn đề bức xúc, được nhiều người quan tâm. Trong bài báo này, chúng tôi sẽ trình bày những vấn đề liên quan về mã hóa thông tin, thuật toán băm MD5, thuật toán mã hóa RSA và chữ ký điện tử. Từ đó, ứng dụng thuật toán MD5 và RSA để phân tích quá trình hoạt động của chữ ký điện tử. Trên cở sở đó, chúng tôi đề ra giải pháp ứng dụng chữ ký điện tử trên cơ sở kết hợp giữa thuật toán băm MD5 và thuật toán mã hóa RSA trong quá trình gửi và nhận các tệp văn bản.

ABSTRACT

Information security including protection of information and information system against unauthorized access, use, disclosure, disruption, modification or destruction, is currently an urgent issue. In this paper, we present decryption using RSA, Message Digest 5 algorithm (MD5) and electronic signatures. Then comes the application of MD5 and RSA algorithm to analyzing the operation of electronic signatures. Hence, we propose a solution for applying electronic signatures to text files sending and receiving process on the basis of the combination between and decryption using RSA and MD5 algorithm

1. Đặt vấn đề

Trên thực tế, chữ ký điện tử (Digital Signature) đã được ứng dụng rộng rãi trong các ứng dụng trên mạng. Một trong những ứng dụng quan trọng của chữ ký điện tử là đảm bảo an toàn dữ liệu khi truyền trên mạng. Tuy nhiên, khi xây dựng một ứng dụng, các nhà phát triển thường chỉ tập trung xây dựng các chức năng của hệ thống, ít quan tâm đến vấn đề an toàn trong quá trình truyền tin.

Nhằm giải quyết vấn đề xử lý các giao dịch trao đổi văn bản trên mạng, đến nay đã có nhiều giải pháp liên quan đến vấn đề mã hóa văn bản, nhưng chúng tôi chọn và đề xuất giải pháp ứng dụng chữ ký điện tử trên cơ sở kết hợp giữa thuật toán băm MD5 và thuật toán mã hóa RSA trong quá trình gửi và nhận tệp văn bản của hệ thống phần mềm quản lý.

Bảo mật thông tin là lĩnh vực rất rộng, nên đây chỉ là bước khởi đầu để chúng tôi tiếp tục nghiên cứu và ứng dụng các thuật toán mã hóa trong việc xây dựng ứng dụng.

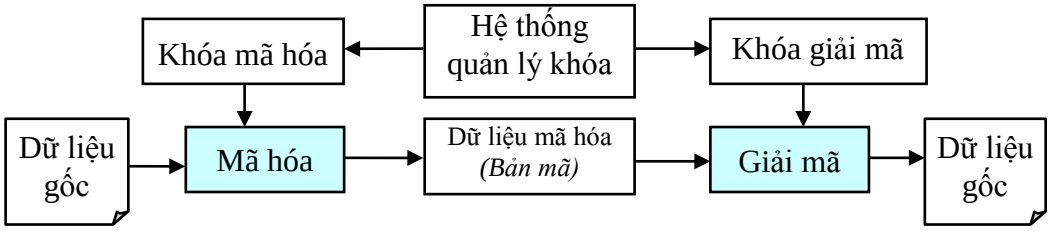
Trong bài báo này, chúng tôi trình bày những nội dung chính như sau: Đầu tiên chúng tôi giới thiệu một số vấn đề liên quan trong lĩnh vực mã hóa dữ liệu. Tiếp theo chúng tôi trình bày vắn tắt thuật toán băm MD5 và thuật toán mã hóa RSA. Phần cuối,

chúng tôi tập trung trình bày giải pháp ứng dụng chữ ký điện tử sử dụng MD5, RSA và đề ra cách thức vận dụng, triển khai trong quá trình gửi và nhận tệp văn bản.

2. Một số vấn đề về mã hóa dữ liệu

2.1. Khái niệm mã hóa dữ liệu

Mã hóa dữ liệu là sử dụng một phương pháp biến đổi dữ liệu từ dạng bình thường sang một dạng khác, mà một người không có thẩm quyền, không có phương tiện giải mã thì không thể đọc hiểu được. Giải mã dữ liệu là quá trình ngược lại, là sử dụng một phương pháp biến đổi dữ liệu đã được mã hóa về dạng thông tin ban đầu.



Hình 1. *Quy trình mã hóa dữ liệu*

Sau đây là một số khái niệm và kí hiệu liên quan về vấn đề mã hóa dữ liệu :

- *Mã hóa* (Encryption): Quá trình chuyển đổi dữ liệu gốc thành dữ liệu được mã hóa sao người khác không thể đọc hiểu được *(kí hiệu E);*
- *Giải mã* (Decryption): Quá trình ngược lại của mã hóa, biến đổi dữ liệu đã được mã hóa thành dạng gốc ban đầu *(kí hiệu D);*
- *Thông điệp* (Message), *bản gốc* (Plaintext): Tệp dữ liệu chưa mã hóa *(kí hiệu M)*.
- *Bản mã* (Ciphertext): Tệp dữ liệu đã được mã hóa *(kí hiệu C)*.

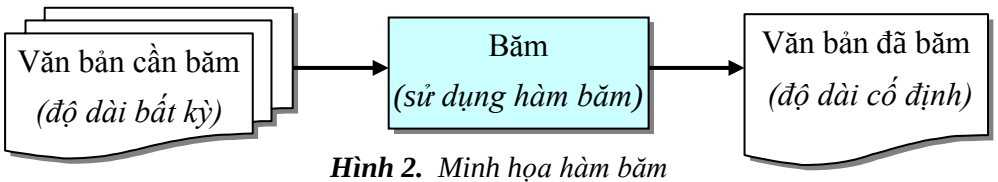
Theo quy ước, khi mã hóa thì C = E(M) và khi giải mã thì M = D(C) = D(E(M))

Theo phương pháp truyền thống, người ta thường dùng cùng một khóa để mã hóa và giải mã. Lúc đó, khóa phải được giữ bí mật tuyệt đối. Người ta gọi đây là hệ thống mã hóa cổ điển (hay còn gọi là mã hóa đối xứng, một khóa, khóa bí mật,...).

Phương pháp khác sử dụng khóa công khai (còn gọi là phương pháp mã hóa bất đối xứng, hay hệ thống hai khóa) trong đó khóa để mã hóa và khóa để giải mã là khác nhau. Các khóa này tạo thành một cặp chuyển đổi ngược nhau và không khóa nào có thể suy ra được từ khóa kia. Phần tiếp theo của bài báo sẽ đề cập đến kỹ thuật mã hóa này.

2.2. Thuật toán MD5

Hàm băm (Hash Function) nhận giá trị vào (Input) là một thông điệp M ở có chiều dài bất kỳ, để biến (băm) thành một giá trị h ở đầu ra (Output) có chiều dài cố định, h được gọi là giá trị băm (Hash Value).



Hình 2. *Minh họa hàm băm*

Thuật toán MD5 (Message Digest 5), do Ronald Rivest thiết kế năm 1991, là xây dựng một hàm băm để mã hóa một tín hiệu vào có chiều dài bất kỳ và đưa ra một tín hiệu (Digest) ở đầu ra có chiều dài cố định 128 bit (tương ứng với 32 chữ số hệ 16). [2]

Dưới đây là các ví dụ mô tả các kết quả sau khi thực hiện hàm băm MD5.

- MD5("xin chao") = 2201c07c37755e663c07335cfd2f44c6

Chỉ cần một thay đổi nhỏ (chẳng hạn viết hoa chữ x thành X) cũng làm thay đổi hoàn toàn kết quả trả về :

- MD5("Xin chao") = e05c1d9f05f5b9eb56fe907c36f469d8

Thuật toán cũng cho kết quả đối với chuỗi rỗng :

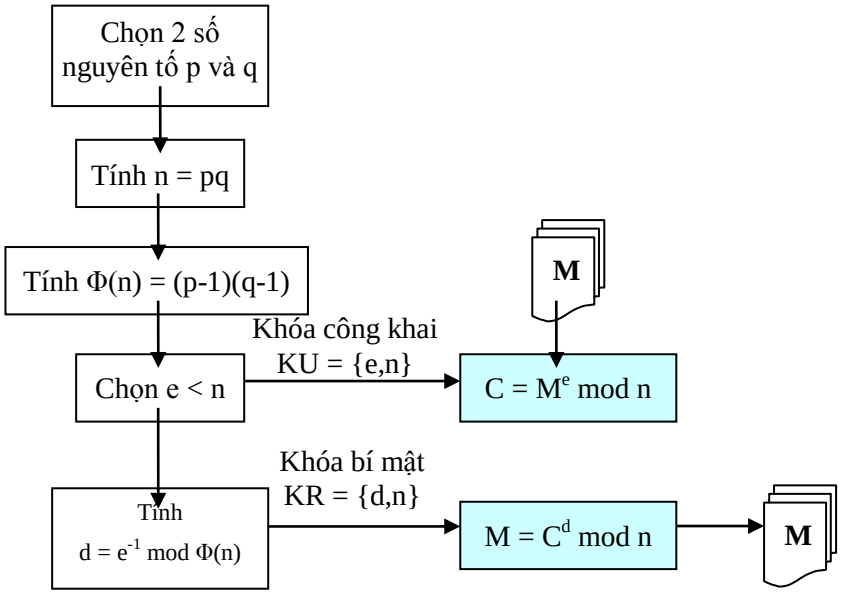
- MD5(" ") = d41d8cd98f00b204e9800998ecf8427e

2.3. Thuật toán RSA

Phương pháp sử dụng thuật toán mã hóa khóa công khai RSA (được đặt tên từ ba nhà phát minh là Ron **R**ivest, Adi **S**hamir và Leonard **A**dleman), được sử dụng nhiều nhất, thuật toán sử dụng biểu thức với hàm mũ để mã hóa bản gốc thành các khối, mỗi khối có một giá trị nhị phân nhỏ hơn n.

Giả sử khối bản gốc của người gửi là M và khối bản mã của người nhận là C, quá trình mã hóa và giải mã RSA là: $C = M^e \bmod n$ và $M = C^d \bmod n$

Cả người gửi và người nhận phải biết giá trị n. Người gửi biết giá trị e và chỉ người nhận biết giá trị d. Đây là một thuật toán mã hóa khóa công khai với khóa công khai KU = {e,n} và khóa riêng KR = {d,n} [4].



Hình 3. *Sơ đồ biểu diễn thuật toán mã hóa RSA*

3. Chữ ký điện tử

Chữ ký điện tử (Digital Signature) dựa trên kỹ thuật sử dụng mã hóa khóa công khai. Trong đó, cả người gửi và người nhận, mỗi người có một cặp khóa là khóa bí mật, hay riêng tư (Private Key) và khóa công khai (Public Key).

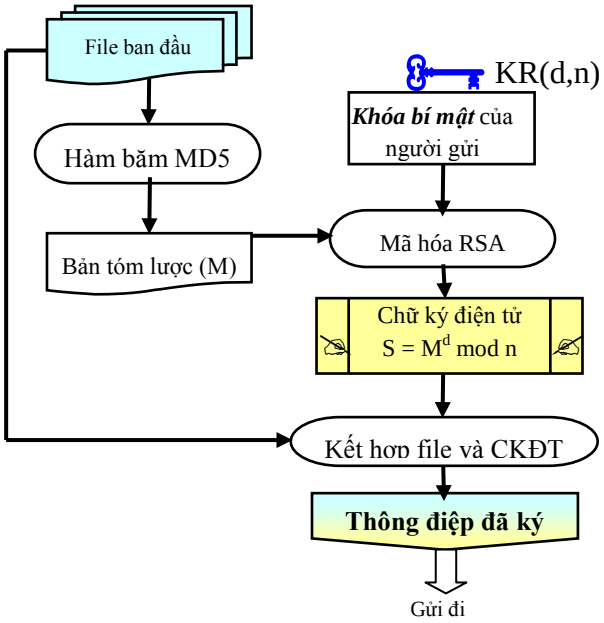
Chữ ký điện tử hoạt động khi một người gửi một thông điệp, người đó dùng khóa riêng của mình để mã hóa thông điệp sang một dạng khó nhận dạng. Người nhận dùng khóa công khai của người gửi để mã hóa thông điệp. Tuy nhiên, để an toàn thật sự phải có các bước bổ sung. Do đó, thuật toán băm MD5 và thuật toán mã hóa RSA có thể được áp dụng để xây dựng ứng dụng chữ ký điện tử.

4. Giải pháp ứng dụng chữ ký điện tử

Phần này, chúng tôi đề xuất giải pháp ứng dụng chữ ký điện tử trong hệ thống quản lý. Quá trình gửi và nhận các tệp văn bản phục vụ quản lý dựa vào thuật toán băm MD5 và thuật toán mã hóa RSA.

4.1. Quá trình ký và gửi các tệp văn bản

- Từ file cần gửi ban đầu, chương trình sẽ sử dụng hàm băm MD5 để mã hóa thành chuỗi ký tự dài 128 bit, hash value (gọi là bản tóm lược).
- Chương trình sử dụng thuật toán RSA để mã hóa khóa riêng (private key) của người gửi và bản tóm lược hash value thành một dạng khác (giá trị băm ở dạng mật mã) gọi là chữ ký điện tử.
- Kết hợp file ban đầu với chữ ký điện tử thành một thông điệp đã ký và gửi đi cho người nhận.



Hình 4. *Sơ đồ mô tả quá trình ký và gửi các tệp văn bản*

4.2. Quá trình nhận các tệp văn bản

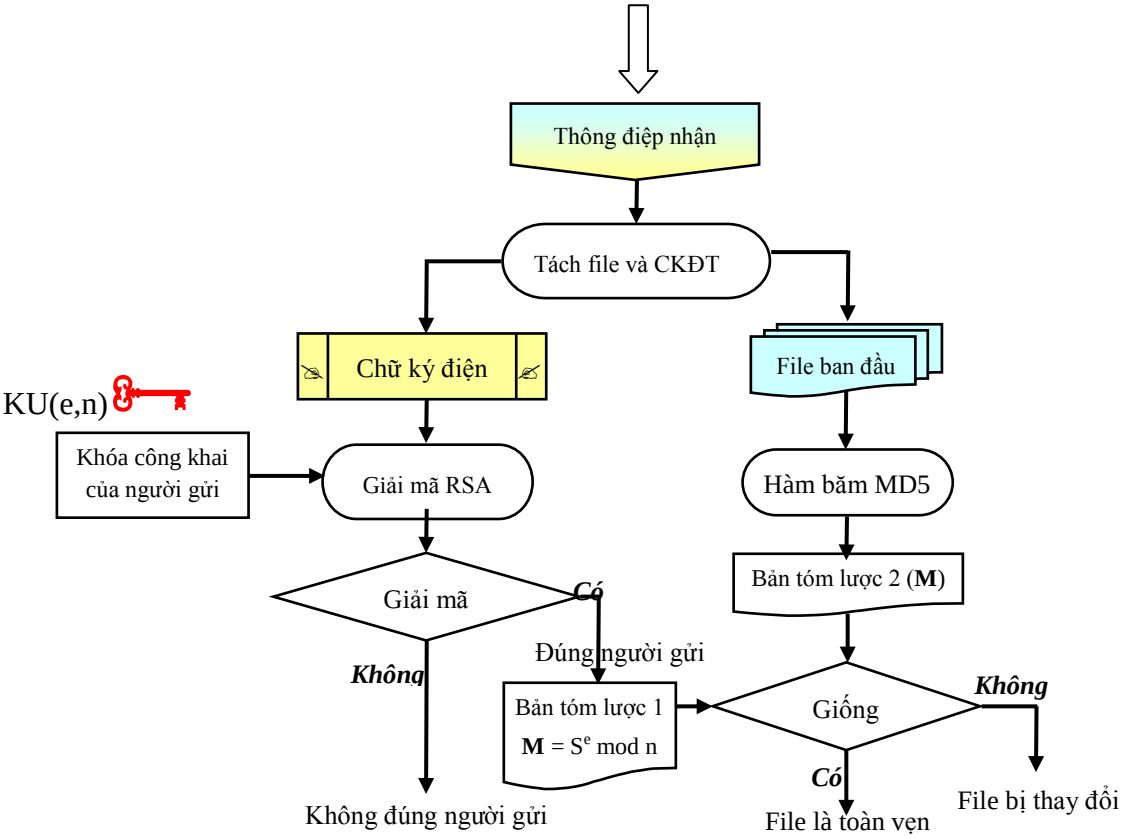
Sau khi người nhận đăng nhập vào hệ thống và thực hiện việc nhận các tệp văn bản. Hệ thống sẽ tách thông điệp đã ký thành ra file và chữ ký điện tử. Đến giai đoạn này sẽ có 2 quá trình kiểm tra :

1. Kiểm tra file có đúng người gửi hay không?

- Sử dụng thuật toán RSA để giải mã chữ ký điện tử bằng khóa công khai (username) của người gửi.
- Nếu giải mã không được thì file nhận được không đúng người gửi.
- Nếu giải mã thành công thì file nhận được đúng người gửi và có được Bản tóm lược 1.

2. Kiểm tra file có bị thay đổi hay không?

- Từ file được tách ra ta sử dụng hàm băm MD5 mã hóa thành Bản tóm lược 2.
- Kiểm tra Bản tóm lược 1 và Bản tóm lược 2 có giống nhau hay không? Nếu giống nhau thì file nhận được là vẹn toàn (không bị thay đổi hay tác động), ngược lại là file đã bị thay đổi.



Hình 5. *Sơ đồ mô tả quá trình nhận các tệp văn bản*

4.3. Vận dụng vào hệ thống

Để vận dụng giải pháp này trong hệ thống gửi và nhận tệp văn bản chúng ta cần tìm hiểu thêm trong các tài liệu tham khảo, từ đó có thể lựa chọn, sử dụng các thuật toán, ngôn ngữ để xây dựng chương trình. Trong khuôn khổ một bài báo, chúng tôi giới thiệu tổng quan một số bước để xây dựng các hàm và thuật toán chính như sau:

- Do sử dụng hàm băm MD5 để mã hóa văn bản gốc thành 32 kí tự nên kích thước của khóa có độ đài phải đủ lớn và trong thuật toán RSA có cả hàm mũ... nên ta cần xây dựng các hàm xử lý số có kích thước lớn với các phép toán cơ bản: cộng, trừ, nhân, chia, modulo…
- Xây dựng thuật toán phát sinh số nguyên tố;
- Xây dựng thuật toán chọn e, thuật toán chọn d;
- Sử dụng khóa riêng (n, d) để tính toán chữ ký $S = M^d \bmod n$;
- Sử dụng khóa công khai của người gửi (n, e) để tính toán lại $M = S^e \bmod n$;
- Xây dựng các hàm gửi và nhận file...

5. Kết luận

Chữ ký điện tử là nền tảng để bảo đảm an ninh trong lĩnh vực thương mại điện tử, các phần mềm quản lý có kiến trúc kiểu Client/Server. Chúng tôi đã nêu được quy trình ứng dụng chữ ký điện tử trên cơ sở kết hợp giữa thuật toán băm MD5 và thuật toán mã hóa RSA. Từ đó, chúng tôi đã đề ra giải pháp ứng dụng chữ ký điện tử trong phần mềm quản lý; cụ thể là quá trình gửi và nhận các tệp văn bản.

Từ giải pháp này, ta có thể xây dựng và cài đặt các hàm sử dụng tính năng của chữ ký điện tử trong quá trình gửi và nhận các tệp văn bản ứng dụng cho các hệ thống quản lý nhằm đảm bảo tính bảo mật của hệ thống.

TÀI LIỆU THAM KHẢO

[1] William Stallings, *Cryptography and Network Security : Principles and Practice*, Fourth Edition, Prentice Hall, 2006.

[2] R. Rivest, *The MD5 Message-Digest Algorithm*, MIT Laboratory for Computer Science and RSA Data Security, Inc, April 1992.

[3] Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

[4] R.L. Rivest, A. Shamir, and L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM, 21 (2), pp. 120-126, Feb 1978.

[5] Dương Anh Đức, Trần Minh Triết, *Mã hóa và ứng dụng*, Đại học Khoa học Tự nhiên, Đại học Quốc gia TP Hồ Chí Minh, 2005.

[6] Phan Đình Diệu, *Lý thuyết mật mã và an toàn thông tin*, Đại học Quốc gia Hà Nội, 1999.