[Bài đọc] Chữ ký số sử dụng giải thuật RSA

Tổng quan

*Chữ kí số (Digital Signature)* là một chuỗi dữ liệu liên kết với một thông điệp (message) và thực thể tạo ra thông điệp.

*Giải thuật tạo ra chữ ký số (Digital Signature generation algorithm)* là một phương pháp sinh chữ ký số.

*Giải thuật kiểm tra chữ ký số (Digital Signature verification algorithm)* là một phương pháp xác minh tính xác thực của chữ ký số, có nghĩa là nó thực sự được tạo ra bởi 1 bên chỉ định.

*Một hệ chữ ký số (Figital Signature Scheme)* bao gồm giải thuật tạo chữ số và giải thuật kiểm tra chữ kỹ số.

- Quá trình tạo chữ ký số (Digital Signature signing process) bao gồm:

* Giải thuật tạo chữ ký số.
* Phương pháp chuyển dữ liệu thông điệp thành dạng có thể ký được.

- Quá trình kiểm tra chữ ký số (Digital signature verification process) :

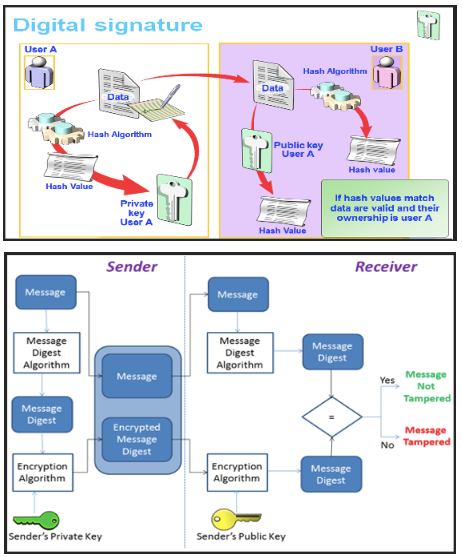
* Giải thuật kiểm tra chữ ký số.
* Phương pháp khôi phục dữ liệu từ thông điệp.

**Ví dụ :** Ta có thể mô phỏng trực quan một hệ mật mã khoá công khai như sau : Bob muốn gửi cho Alice một thông tin mật mà Bob muốn duy nhất Alice có thể đọc được. Để làm được điều này, Alice gửi cho Bob một chiếc **hộp có khóa đã mở sẵn (Khóa công khai)** và giữ lại chìa khóa. Bob nhận chiếc hộp, cho vào đó một tờ giấy viết thư bình thường và khóa lại (như loại khoá thông thường chỉ cần sập chốt lại, sau khi sập chốt khóa ngay cả Bob cũng không thể mở lại được-không đọc lại hay sửa thông tin trong thư được nữa). Sau đó Bob gửi chiếc hộp lại cho Alice. Alice mở hộp với chìa khóa của mình và đọc thông tin trong thư. Trong ví dụ này, chiếc hộp với khóa mở đóng vai trò khóa công khai, chiếc chìa khóa chính là khóa bí mật.

*Lược đồ chữ ký số RSA* : độ an toàn của lược đồ chữ ký RSA dựa vào độ an toàn của hệ mã RSA. Lược đồ bao gồm cả chữ ký số kèm theo bản rõ và tự khôi phục thông điệp từ chữ ký số.

* Thuật toán sinh khóa cho lược đồ chữ ký RSA
* Thuật toán sinh chữ ký RSA
* Thuật toán chứng thực chữ ký RSA

Kiến trúc chữ ký số tổng quát



***Quá trình ký (bên gửi)***

Tính toán chuỗi đại diện (message digest/ hash value) của thông điệp sử dụng một giải thuật băm (Hashing algorithm)

Chuỗi đại diện được ký sử dụng khóa riêng (Priavte key) của người gửi va 1 giải thuật tạo chữ ký (Signature/ Encryption algorithm). Kết quả chữ ký số (Digital signature) của thông điệp hay còn gọi là chuỗi đại diện được mã hóa (Encryted message digest)

Thông điệp ban đầu (message) được ghép với chữ ký số (Digital signature) tạo thành thông điệp đã được ký (Signed message)

Thông điệp đã được ký (Signed message) được gửi cho người nhận

***Quá trình kiểm tra chữ ký (bên nhận)***

Tách chữ ký số và thông điệp gốc khỏi thông điệp đã ký để xử lý riêng;

Tính toán chuỗi đại diện MD1 (message digest) của thông điệp gốc sử dụng giải thuật băm (là giải thuật sử dụng trong quá trình ký)

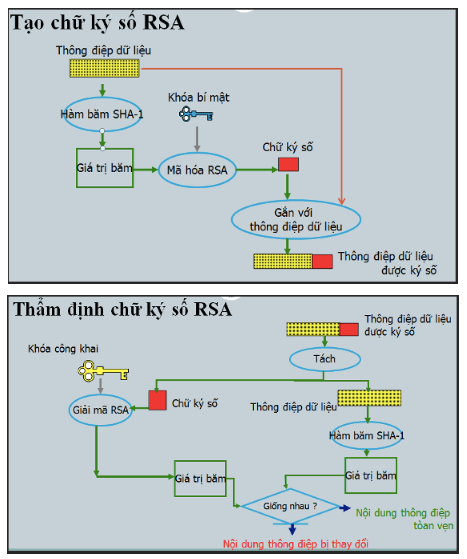
Sử dụng khóa công khai (Public key) của người gửi để giải mã chữ ký số -> chuỗi đại diện thông điệp MD2

So sánh MD1 và MD2:

Nếu MD1 =MD2 -> chữ ký kiểm tra thành công. Thông điệp đảm bảo tính toàn vẹn và thực sự xuất phát từ người gửi (do khóa công khai được chứng thực).

Nếu MD1 <>MD2 -> chữ ký không hợp lệ. Thông điệp có thể đã bị sửa đổi hoặc không thực sự xuất phát từ người gửi.

## Kiến trúc chữ ký số RSA



***Quá trình ký (bên gửi)***

Tính toán chuỗi đại diện (message digest/ hash value) của thông điệp sử dụng một giải thuật băm (Hashing algorithm) SHA-1

Chuỗi đại diện được ký sử dụng khóa riêng (Priavte key) của người gửi và giải thuật tạo chữ ký (Signature/ Encryption algorithm) RSA. Kết quả chữ ký số (Digital signature) của thông điệp hay còn gọi là chuỗi đại diện được mã hóa bởi giải thuật RSA (Encryted message digest)

Thông điệp ban đầu (message) được ghép với chữ ký số (Digital signature) tạo thành thông điệp đã được ký (Signed message)

Thông điệp đã được ký (Signed message) được gửi cho người nhận

***Quá trình kiểm tra chữ ký (bên nhận)***

Tách chữ ký số RSA và thông điệp gốc khỏi thông điệp đã ký để xử lý riêng;

Tính toán chuỗi đại diện MD1 (message digest) của thông điệp gốc sử dụng giải thuật băm (là giải thuật sử dụng trong quá trình ký là SHA-1)

Sử dụng khóa công khai (Public key) của người gửi để giải mã chữ ký số RSA-> chuỗi đại diện thông điệp MD2

So sánh MD1 và MD2:

Nếu MD1 =MD2 -> chữ ký kiểm tra thành công. Thông điệp đảm bảo tính toàn vẹn và thực sự xuất phát từ người gửi (do khóa công khai được chứng thực).

Nếu MD1 <>MD2 -> chữ ký không hợp lệ. Thông điệp có thể đã bị sửa đổi hoặc không thực sự xuất phát từ người gửi.

## Các điểm yếu của chữ ký số sử dụng giải thuật RSA

### **Chữ ký số nói chung**

Sự xuất hiện của chữ ký số và chức năng tiền định của nó, đặc biệt là vai trò của nó như là một công cụ trong việc xác định tính nguyên gốc, xác định tác giả, bảo đảm tính toàn vẹn của tài liệu số, đã đóng một vai trò vô cùng quan trọng trong việc xác định địa vị pháp lý của tài liệu số trong giao dịch số. Việc sử dụng chữ ký số trong phần lớn trường hợp là cơ sở khẳng định giá trị pháp lý của những văn bản điện tử tương đương với tài liệu giấy. Hiện nay, chữ ký số là phương tiện duy nhất để xác nhận giá trị pháp lý của tài liệu điện tử.

Như vậy, với sự xuất hiện của chữ ký số, vấn đề giá trị pháp lý của tài liệu điện tử, có thể coi như đã được giải quyết. Việc sử dụng chữ ký số trong giao dịch cũng có những ưu điểm và bất cập nhất định. Dưới đây là những hạn chế của chữ ký số:

- Sự lệ thuộc vào máy móc và chương trình phần mềm: chữ ký số là một chương trình phần mềm máy tính. Để kiểm tra tính xác thực của chữ ký cần có hệ thống máy tính và phần mềm tương thích.

- Tính bảo mật không tuyệt đối: Nếu chữ ký bằng tay được thực hiện trên giấy, được ký trực tiếp và luôn đi kèm với vật mang tin, chữ ký tay không thể chuyển giao cho người khác, thì chữ ký số không như vậy. Chữ ký số là một bộ mật mã được cấp cho người sử dụng, đây là phần mềm máy tính không phụ thuộc vào vật mang tin. Chính vì vậy, trở ngại lớn nhất khi sử dụng chữ ký số là khả năng tách biệt khỏi chủ nhân của chữ ký. Nói cách khác, chủ nhân của chữ ký số không phải là người duy nhất có được mật mã của chữ ký. Tồn tại một số nhóm đối tượng có thể có được mật mã, đó là: bộ phận cung cấp phần mềm; bộ phận cài đặt phần mềm, những người có thể sử dụng máy tính có cài đặt phần mềm. Ngoài ra, mật mã có thể bị đánh cắp. Cũng có thể, chủ nhân chữ ký số chuyển giao cho người khác mật mã của mình. Như vậy, tính bảo mật của chữ ký số không phải là tuyệt đối.  
- Vấn đề bản gốc, bản chính: Nếu đối với tài liệu giấy, chữ ký được ký một lần và chỉ có một bản duy nhất (được coi là bản gốc). Bản gốc được ký bằng chữ ký sẽ không thể cùng lúc ở hai chỗ khác nhau. Có thể tin tưởng rằng, nếu bản gốc duy nhất mất đi thì sẽ không thể có bản thứ hai giống hệt như vậy. Nhưng với văn bản điện tử đã được ký bằng chữ ký số, người ra có thể copy lại và bản copy từ bản chính và bản copy từ bản copy không có gì khác biệt so với bản chính duy nhất được ký. Đây là một thách thức đối với công tác văn bản và cả nền hành chính. Khái niệm bản gốc, bản chính trong văn bản hành chính sẽ phải xem xét lại.  
- Sự có thời hạn của chữ ký điện tử. Chữ ký điện tử là chương trình phần mềm được cấp có thời hạn cho người sử dụng. Về lý thuyết, văn bản sẽ có hiệu lực pháp lý khi được ký trong thời hạn sử dụng của chữ ký. Tuy nhiên, thực tế hiệu lực pháp lý của văn bản hoàn toàn có thể bị nghi ngờ khi chữ ký số hết thời hạn sử dụng. Đây cũng là một hạn chế và thách thức rất lớn đối với việc sử dụng chữ ký số.

### **Chữ ký số sử dụng RSA**

#### **Hiệu suất thực hiện thuật toán RSA**

Tốc độ thực hiện của hệ RSA là một trong những điểm yếu so với các hệ mật mã khóa đối xứng.

Theo ước tính, thực hiện mã hóa và giải mã bằng hệ mật mã RSA chậm hơn 100 lần so với hệ mã khóa đối xứng DES (Khi thực hiện bằng phần mềm). Và chậm hơn 1000 lần so với DES (Khi thực hiện bằng phần cứng).

#### Chi phí và tốc độ thực hiện thuật toán RSA

**Chi** **phí**

Để thực hiện thuật toán RSA phần lớn tốn chi phí thực hiện các phép tính cơ bản như : Tạo khóa, mã hóa, giải mã. Quá trình mã hóa, giải mã tương được với chi phí thực hiện các phép tính lũy thừa module n. Để đảm bảo cho khóa bí mật được an toàn thì thường chọn mũ công khai e nhỏ hơn nhiều so với số mũ bí mật d, do đó chi phí thời gian để thực hiện mã hóa dữ liệu nhỏ hơn nhiều so với thời gian giải mã.

**Tốc độ của hệ RSA**

Tốc độ của RSA là một trong những điểm yếu của RSA so với các hệ mã đối xứng, so với hệ mã DSA thì RSA chậm hơn từ 100 đến 1000 lần.

Last modified: Friday, 13 August 2021, 4:44 PM