

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

**KHOA CÔNG NGHỆ THÔNG TIN I**

**BÁO CÁO BÀI TẬP LỚN**

**Môn: An Toàn Bảo Mật Hệ Thống Thông Tin**

**Đề tài : Tìm hiểu về giải thuật tạo chữ ký số sử dụng RSA**

**Giảng viên hướng dẫn: TS. Hoàng Xuân Dậu**

**Nhóm lớp học: 06**

**Nhóm BTL: G5**

**Thành viên:**

**Lê Minh Hiến - B19DCCN232.**

***Hà Nội – 2021***

**Mục Lục**

[LỜI MỞ ĐẦU 3](#_Toc7284)

[I. Giới thiệu về chữ ký số. 4](#_Toc10101)

[1. Giới thiệu về chữ ký số. 4](#_Toc24485)

[2. Phân loại chữ ký số. 4](#_Toc8172)

[II. Thuật toán trong chữ ký số. 5](#_Toc1853)

[1. Giới thiệu thuật toán RSA. 5](#_Toc28876)

[2. Giới thiệu hàm băm SHA-1 7](#_Toc19918)

[3. Quá trình vận hành chữ ký số. 11](#_Toc16682)

[III. Cài đặt giải thuật trong ngôn ngữ JAVA. 13](#_Toc412)

[1. Tạo khóa. 14](#_Toc927)

[2. Mã hóa. 14](#_Toc15040)

[3. Giải mã. 14](#_Toc2132)

[4. Demo 15](#_Toc1888)

[IV. Kết luận 16](#_Toc20694)

[1. Điểm mạnh. 16](#_Toc26320)

[2. Điểm yếu. 17](#_Toc15165)

[V. Tài liệu tham khảo. 18](#_Toc29335)

**LỜI MỞ ĐẦU**

Ngày nay với sự phát triển bùng nổ của công nghệ thông tin, hầu hết các thông tin của doanh nghiệp như chiến lược kinh doanh, các thông tin về khách hàng, nhà cung cấp, tài chính, mức lương nhân viên,... đều được lưu trữ trên hệ thống máy tính. Ngoài ra, cùng với sự phát triển yêu cầu doanh nghiệp cần phải chia sẻ thông tin của mình cho nhiều đối tượng khác nhau qua Internet. Đây chính là cơ hội để kẻ gian đánh cắp thông tin của doanh nghiệp.

Việc mất mát, rò rỉ thông tin có thể ảnh hưởng nghiêm trọng đến tài chính, danh tiếng của công ty và quan hệ với khách hàng. Các phương thức tấn công thông qua mạng ngày càng tinh vi, phức tạp có thể dẫn đến mất mát thông tin, thậm chí có thể làm sụp đổ hoàn toàn hệ thống thông tin của doanh nghiệp. Vì vậy an toàn và bảo mật thông tin là nhiệm vụ hết sức cấp bách hiện nay.

Bởi vậy mà đã tiếp cận và tìm hiểu đề tài: “Tìm hiểu về giải thuật tạo chữ ký số sử dụng RSA”. Tuy nhiên, do kiến thức còn hạn chế, đề tài không tránh khỏi những thiếu sót. Rất mong thầy giáo và các bạn đóng góp để đề tài của em được hoàn thiện hơn.

**Người thực hiện**

Hiến

Lê Minh Hiến

1. **Giới thiệu về chữ ký số.**
2. **Giới thiệu về chữ ký số.**

* Kể từ khi con người phát minh ra chữ viết, các chữ ký thường luôn được sử dụng hàng ngày, chẳng hạn như ký một biên nhận trên một bức thư nhận tiền từ ngân hàng, ký hợp đồng hay một văn bản bất kỳ nào đó. Chữ ký viết tay thông thường trên tài liệu thường được dùng để xác định người ký nó.
* Tuy nhiên, ngày nay trong lĩnh vực hợp đồng điện tử, một trong những thử thách chính là đạt được một cơ chế khác thay thế chữ ký bằng tay, nhưng nó phải thực hiện đúng chức năng như chữ ký bằng tay, cụ thể là: Đảm bảo tính đồng nhất của các bên tham gia ký kết hợp đồng, ràng buộc mỗi nhà thầu về cam kết mục đích của họ và cuối cùng là nội dung của hợp đồng.
* Điểm khác nhau cơ bản giữa chữ ký thông thường và chữ ký số. Đầu tiên là vấn đề ký một tài liệu. Với chữ ký thông thường nó là một phần vật lý của tài liệu. Tuy nhiên, một chữ ký điện tử không gắn theo kiểu vật lý vào bức điện nên thuật toán được dùng phải là “không nhìn thấy” theo cách nào đó trên bức điện.
* Thứ hai là vấn đề kiểm tra. Chữ ký thông thường được kiểm tra bằng cách so sánh nó với các chữ ký xác thực khác. Ví dụ, ai đó ký một tấm séc để mua hàng, người bán sẽ so sánh chữ ký trên mảnh giấy đó với chữ ký nằm ở mặt sau thẻ tín dụng để kiểm tra. Mặt khác, chữ ký số có thể kiểm tra băng một thuật toán kiểm tra một cách công khai. Như vậy, bất kỳ ai cũng có thể kiểm tra được chữ ký số. Việc sử dụng một sơ đồ ký an toàn có thể ngăn chặn được khả năng giả mạo.

1. **Phân loại chữ ký số.**

**2.1. Phân loại chữ ký theo khả năng khôi phục thông điệp gốc.**

* Chữ ký có thể khôi phục theo khả năng khôi phục thông điệp gốc

Là loại chữ ký trong đó người nhận có thể khôi phục lại thông điệp gốc, đã được “ký” bởi “chữ ký” này.

VD: Chữ ký RSA

* Chữ ký không thể khôi phục thông điệp gốc:

Là loại chữ ký trong đó người nhận không thể khôi phục lại thông điệp gốc.

VD: Chữ ký Elgamal.

**2.2. Phân loại chữ ký theo mức an toàn.**

* Chữ ký “không thể phủ nhận”

Để tránh việc chối bỏ chữ ký hay nhân bản chữ ký để sử dụng nhiều lần, người gửi chữ ký cũng tham gia trực tiếp vào việc kiểm thử chữ ký. Điều đó được thực hiện bằng giao thức kiểm thử, dưới dạng một giao thức mời hỏi và trả lời.

* Chữ ký “một lần”.

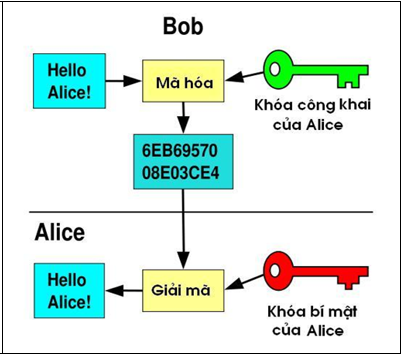
Để đảm bảo an toàn, “khóa ký” chỉ dùng một lần trên một tài liệu.

**2.3. Phân loại chữ ký theo ứng dụng đặc trưng.**

* Chữ ký “mù”.
* Chữ ký “nhóm”.
* Chữ ký “bội”.
* Chữ ký “mù nhóm”.
* Chữ ký “mù bội”.

1. **Thuật toán trong chữ ký số.**
2. **Giới thiệu thuật toán RSA.**
   1. **Mô tả sơ lược.**

* Trong mật mã học, RSA là một thuật toán mật mã hóa khóa công khai. Đây là thuật toán đầu tiên phù hợp với việc tạo ra chữ ký điện tử đồng thời với việc mã hóa. RSA đang được sử dụng phổ biến trong thương mại điện tử và được cho là đảm bảo an toàn với điều kiện độ dài khóa đủ lớn.
* Thuật toán RSA có hai khóa: **khóa công khai** (public key) và **khóa bí mật** (private key). Mỗi khóa là những số cố định sử dụng trong quá trình **mã hóa** và **giải mã**. Khóa công khai được công bố rộng rãi cho mọi người và được dùng để mã hóa. Những thông tin được mã hóa bằng khóa công khai chỉ có thể được giải mã bằng khóa bí mật tương ứng. Nói cách khác, mọi người đều có thể mã hóa nhưng chỉ có người biết khóa cá nhân (private key) mới có thể giải mã được.



**Hình ảnh minh họa thuật toán RSA**

* 1. **Quá trình tạo khóa.**

Giả sử Alice và Bob cần trao đổi thông tin bí mật thông qua một kênh không an toàn (ví dụ như Internet). Với thuật toán RSA, Alice đầu tiên cần tạo ra cho mình cặp khóa gồm **khóa công khai** và **khóa bí mật** theo các bước sau:

* Bước 1: Alice cần tạo ra hai số nguyên tố lớn ngẫu nhiên p và q.
* Bước 2: Tính n = p\*q và tính (n) = (p-1)\*(q-1).
* Bước 3: Chọn một số ngẫu nhiên e ( 0 < e < (n)) sao cho e nguyên tố cùng nhau với (n) .
* Bước 4: Tính d sao cho d\*e = 1 mod (n) .
* Bước 5: Khi đó n và e là khóa công khai (public key) và d là khóa bí mật (private key).

* 1. **Quá trình mã hóa.**

Sau khi Bob nhận được khóa công khai của Alice. Bob cần thực hiện các công việc sau để mã hóa.

* Bước 1: Biểu diễn thông tin cần gửi thành số m (m < n) theo một hàm có thể đảo ngược (từ m có thể xác định lại M) được thỏa thuận trước.
* Bước 2: Tính c = mod n.
* Bước 3: Gửi c cho Alice.
  1. **Quá trình giải mã.**

Sau khi Alice nhận được thông điệp c do Bob gửi. Alice cần giải mã nó. Tính m = mod n. (Với m là thông tin nhận được).

* 1. **Các dạng tấn công thường gặp nhất.**
* **Số n nhỏ**

- Nếu số n nhỏ ( chiều dài n < 256 bit), số n có thể bị tách ra thành các thừa số nguyên tố dễ dàng bởi các công cụ có sẵn như factordb.

- Nhưng đã có những trường hợp số n lớn, nhưng phân tách của n thành thừa số nguyên tố đã có sẵn trong cơ sở dữ liệu của các trang như factordb hoặc alpertron.

- Đây là 1 cách tìm p và q rất dễ nên thường được thử đầu tiên.

→ Giải pháp phòng tránh: Chiều dài của số n được khuyến cáo là 1024 bit.

* **Bị lộ một trong các giá trị: p, q, (n).**

- Nếu quá trình lập khóa mà người sử dụng vô tình để lộ p,q hoặc (n) ra ngoài thì kẻ tấn công sẽ dễ dàng tính được khóa bí mật theo công thức sau: d\*e = 1 mod (n)

- Biết được khóa bí mật, kẻ tấn công sẽ giả mạo chữ ký người dùng.

→ Giải pháp phòng tránh: Quá trình tạo khóa phải được tiến hành ở một nơi bí mật. Sau khi thực hiện xong thì cần phải giữ cẩn thận khóa bí mật d, đồng thời hủy hết các giá trị trung gian p, q, (n).

* **Tấn công dựa vào khóa công khai n và e của người ký.**

- Lúc này, kẻ tấn công sẽ tìm cách phân tích giá trị n ra 2 thừa số nguyên tố p và q. Từ đó, tính ra được (n) = (p-1)\*(q-1). Cuối cùng, tính ra được khóa bí mật d.

→ Giải pháp phòng tránh: Lựa chọn số nguyên p và q đủ lớn để việc phân tích n thành hai thừa số nguyên tố là khó có thể thực hiện được trong thời gian thực.

* **Phân phối khoá**

Giả sử C có thể gửi cho A một khóa bất kỳ và có thể khiến cho A tin đó là khóa công khai của B. Đồng thời C có thể đọc thông tin trao đổi giữa A và B. Khi đó, C sẽ gửi cho A khóa công khai của chính mình ( mà A nghĩ rằng đó là khóa của B ). Sau đó C sẽ đọc tất cả văn bản mã hóa do A gửi, giải mã với khóa bí mật của mình, giữ 1 bản copy, đồng thời mã hóa bằng khóa công khai của B và gửi cho B.

1. **Giới thiệu hàm băm SHA-1**
   1. **Mô tả sơ lược về hàm băm SHA-1.**

* Hàm băm (hash function) là giải thuật nhằm sinh ra các giá trị băm tương ứng với mỗi khối dữ liệu (có thể là một chuỗi ký tự, một đối tượng trong lập trình hướng đối tượng, v.v...). Một Hàm băm mật mã học (Cryptographic hash function) là một hàm băm với một số tính chất bảo mật nhất định để phù hợp việc sử dụng trong nhiều ứng dụng bảo mật thông tin đa dạng, chẳng hạn như chứng thực (authentication) và kiểm tra tính nguyên vẹn của thông điệp (message integrity). Một hàm băm nhận đầu vào là một xâu ký tự dài (hay thông điệp) có độ dài tùy ý và tạo ra kết quả là một xâu ký tự có độ dài cố định, đôi khi được gọi là tóm tắt thông điệp (message digest) hoặc chữ ký số (digital fingerprint).
* Trong nhiều chuẩn và ứng dụng, hai hàm băm thông dụng nhất là MD5 và SHA-1.
* SHA-1 là 1 phần trong các ứng dụng bảo mật được sử dụng rộng rãi trong các giao thức như:TLS và SSL,PGP,SSH và IPSEC.. Các SHA-1 có thể được sử dụng với các DSA trong thư điện tử,chuyển tiền điện tử,phân phối phần mềm,lưu trữ dữ liệu,và các ứng dụng khác cần đảm bảo tính toàn vẹn DL và xác thực nguồn gốc DL. SHA-1 cũng có thể sử dụng bất cứ khi nào nó là cần thiết để tạo ra 1 phiên bản đặc của tin nhắn. Hàm SHA-1 còn được sử dụng trên Wii của Nintendo để xác minh chữ ký thời gian khởi động.
  1. **Thuật toán.**

Giải thuật gồm 5 bước thao tác trên các khối 512 bits.

Đầu vào: thông điệp với độ dài tối đa 264 bits.

Đầu ra: giá trị băm (message digest) có độ dài 160 bits.

* **Bước 1**: Nhồi dữ liệu

- Thông điệp luôn luôn được nhồi thêm các bit sao cho độ dài L mod 512 luôn đồng dư là 448.

- Số bit nhồi thêm phải nằm trong khoảng [1-512].

- Phần thêm vào cuối dữ liệu gồm 1 bit 1 và theo sau là các bit 0.

* **Bước 2**: Thêm độ dài

- Độ dài của khối dữ liệu ban đầu sẽ được biểu diễn dưới dạng nhị phân 64 bit và được thêm vào cuối chuỗi nhị phân mà ta thu được của bước 1

- Độ dài được biểu diễn dưới dạng nhị phân 64 bit không dấu

- Kết quả thu được từ 2 bước là 1 khối dữ liệu có độ dài là bội số của 512.(với cứ 512 bit là 1 khối dữ liệu)

* **Bước 3**: Khởi tạo bộ đệm MD (MD Buffer)

- Một bộ đệm 160-bit được dùng lưu trữ các giá trị băm trung gian và kết quả. Bộ đệm được biểu diễn bằng 5 thanh ghi 32-bit với các giá trị khởi tạo ở dạng big-endian (byte có trọng số lớn nhất trong từ nằm ở địa chỉ thấp nhất) và có 2 bộ đệm.5 thanh ghi của bộ đệm đầu tiên được đánh đặt tên là A,B,C,D,E và tương tự cho bộ đệm thứ 2 là H0,H1,H2,H3,H4.Có giá trị như sau (theo dạng Hex):

H0=67452301

H1=EFCDAB89

H2=98BADCFE

H3=10325476

H4=C3D2E1F0

* **Bước 4**: Xử lý các khối dữ liệu 512 bit

- Trọng tâm của giải thuật bao gồm 4 vòng lặp thực hiện tất cả 80 bước

- 4 vòng lặp có cấu trúc như nhau, chỉ khác nhau ở các hàm logic ft

|  |  |  |
| --- | --- | --- |
| Bước | Hàm | Giá trị |
| (0 ≤ t ≤ 19) | ft = f(B,C,D) | (B AND C) OR ((NOT B) AND D) |
| (20 ≤ t ≤ 39) | ft = f(B,C,D) | B XOR C XOR D |
| (40 ≤ t ≤ 59) | ft = f(B,C,D) | (B AND C) OR (B AND D) OR (C AND D) |
| (60 ≤ t ≤ 79) | ft = f(B,C,D) | B XOR C XOR D |

- Mỗi vòng có đầu vào gồm khối 512-bit hiện thời và một bộ đệm 160-bit A,B,C,D,E. Các thao tác sẽ cập nhật giá trị bộ đệm

- Chia khối dữ liệu đã nhồi thêm (cuối bước 2) thành 16 nhóm (mỗi nhóm gồm 32 bit) và đặt theo thứ tự là:W0, W1, ... , W15.

- Mở rộng từ 16 nhóm 32 bit lên 80 nhóm 32 bit bằng vòng lặp:

For t = 16 to 79 let

Wt = S^1 (Wt-3 XOR Wt-8 XOR Wt- 14 XOR Wt-16)

Gán A=H0,B=H1, C=H2, D=H3, E=H4.

- Mỗi vòng lặp sử dụng theo công thức chung với một hằng số Kt (0 ≤ t ≤ 79) như sau:

For t = 0 to 79 do

TEMP = S5 (A) + ft(B,C,D) + E + Wt + Kt;

E = D;

D = C;

C = S30(B);

B = A;

A = TEMP;

Với:

Kt = 5A827999 (0 ≤ t ≤ 19)

Kt = 6ED9EBA1 (20 ≤ t ≤ 39)

Kt = 8F1BBCDC (40 ≤ t ≤ 59)

Kt = CA62C1D6 (60 ≤  t ≤ 79)

- Đầu ra của 4 vòng (bước 80) được cộng với giá trị của bộ đệm để tạo ra 1 chuỗi kết quả dài 160 bit

H0 = H0 + A

H1 = H1 + B

H2 = H2 + C

H3 = H3 + D

H4 = H4 + E

* **Bước 5**: Xuất kết quả

- Sau khi thao tác trên toàn bộ N khối dữ liệu (blocks), kết quả của khối thứ N là chuỗi băm 160-bit: H=H0 H1 H2 H3 H4**.**

* 1. **Đánh giá.**
* **Ưu điểm**:

- Bảng băm là một cấu trúc dung hòa giữa thời gian truy xuất và dung lượng bộ nhớ:

- Nếu không có sự giới hạn về bộ nhớ: có thể xây dựng bảng băm với mỗi khóa ứng với một địa chỉ với mong muốn thời gian truy xuất tức thời.

- Nếu dung lượng bộ nhớ có giới hạn: tổ chức một số khóa có cùng địa chỉ, tốc độ truy xuất giảm. Các phép toán trên bảng băm hạn chế số lần so sánh, giảm được thời gian truy xuất.

* **Nhược điểm**:

- Hiện nay thì vấn đề bảo mật của SHA-1 không còn được tin tưởng sử dụng như trước đó.

- Đầu năm 2005, Rijmen và Oswald đã công bố 1 cuộc tấn công vào phiên bản rút gọn của SHA-1 bằng cách tìm đụng độ bằng cách tính ít hơn 280 phép tính

- 2/2005,một cuộc tấn công bởi 3 nhà mật mã học thuộc đại học Shandong (Trung Quốc) đã tìm ra được sự đụng độ trong phiên bản SHA-1 đầy đủ với chỉ với 269 phép tính nhanh hơn khoảng 2000 lần so với cách tấn công Brute-Force.

- 8/2005,tại hội nghị Mật Mã,họ đã công bố và thuyết trình về việc tấn công này và chỉ ra 1 vụ va chạm tại vòng 58 của SHA-1 chỉ với 233 phép tính băm.

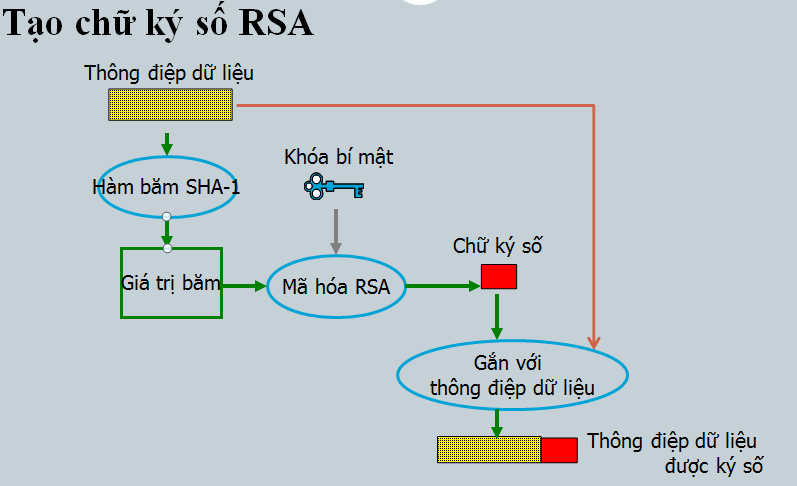
- 18/12/2007,các báo cáo chi tiết kết quả này được giải thích và xác nhận bởi Martin Cochran.

- Ngoài ra còn nhiều cuộc nghiên cứu tấn công khác nữa.

- Nhưng nhìn chung là SHA-1 không có được sự bảo mật tốt nhất như khi nó được công bố năm 2004 bởi NIST tại hội nghị Mật Mã 2004.

1. **Quá trình vận hành chữ ký số.**
   1. **Khái niệm chữ ký số RSA.**

* Chữ ký số là một chuỗi dữ liệu liên kết với thông điệp và thực thể tạo ra thông điệp. Chữ ký số thường được sử dụng để đảm bảo tính toàn vẹn của thông điệp.
* Giải thuật tạo 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 (Digital signature scheme) bao gồm giải thuật tạo chữ ký số và giải thuật kiểm tra chữ ký số.
* Quá trình tạo chữ ký số (Digital signature signing process) bao gồm: giải thuật tạo chữ ký số và phương pháp chuyển dữ liệu thông điệp thành dạng có thể ký được.
* Quá trình kiểm tra chữ ký số (Digital signature verification process) bao gồm: giải thuật kiểm tra chữ ký số và phương pháp khôi phục dữ liệu từ thông điệp.
  1. **Thuật toán chữ ký số sử dụng RSA.**
* Giải thuật RSA sinh ra với hai mục đích để mã hóa - giải mã thông điệp và tạo chữ ký số - kiểm tra chữ ký số cho thông điệp.
* Độ an toàn của lược đồ chữ ký RSA dựa vào độ an toàn của hệ mã RSA. Bao gồm: thuật toán sinh khóa RSA, thuật toán sinh chữ ký RSA, thuật toán kiểm tra chữ ký RSA.
  1. **Kiến trúc chữ ký số.**
* Chữ ký số có cách vận hành là dữ liệu ban đầu sẽ được cho qua một hàm băm sau đó sử dụng khóa bí mật RSA để mã hóa sinh ra một chuỗi ký tự (chuỗi đại diện RSA), chuỗi ký tự đó và dữ liệu được gửi qua môi trường internet đến người nhận. Sau khi người nhận nhận được thì sẽ chia thành 2 bước để kiểm tra tương ứng với dữ liệu và chuỗi đại diện RSA bao gồm: **Dữ liệu**: cho qua hàm băm thu được chuỗi ký tự băm (1) và **Chuỗi đại diện:** Sử dụng khóa công khai RSA để mã hóa ngược thu được chuỗi ký tự (2).
* Nếu như chuỗi ký tự (1) trùng với chuỗi ký tự (2) thì ta có thể khẳng định dữ liệu vẹn toàn.
* Dưới đây sẽ trình bày về hoạt động cho từng bước.
* **Quá trình ký:**



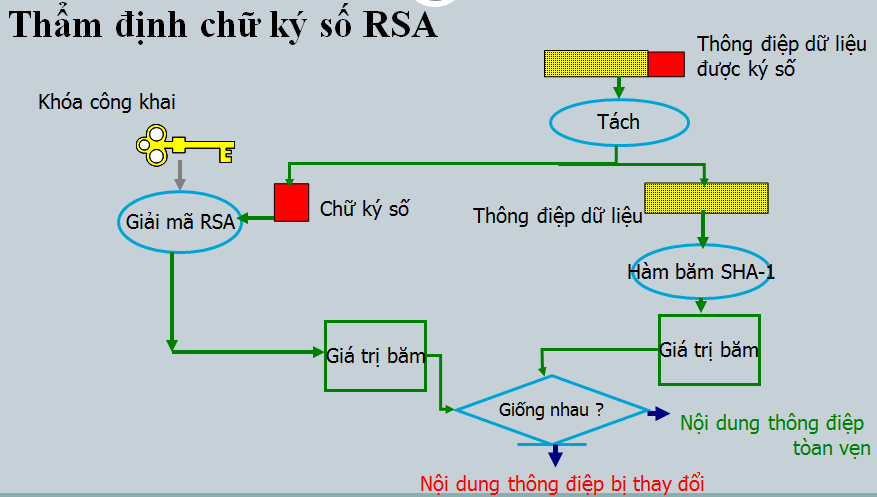
- Tính toán chuỗi đại diện (message digest/ hash value) của thông điệp sử dụng một giải thuật băm (Hashing algorithm) SHA-1

- 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:**



- 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:

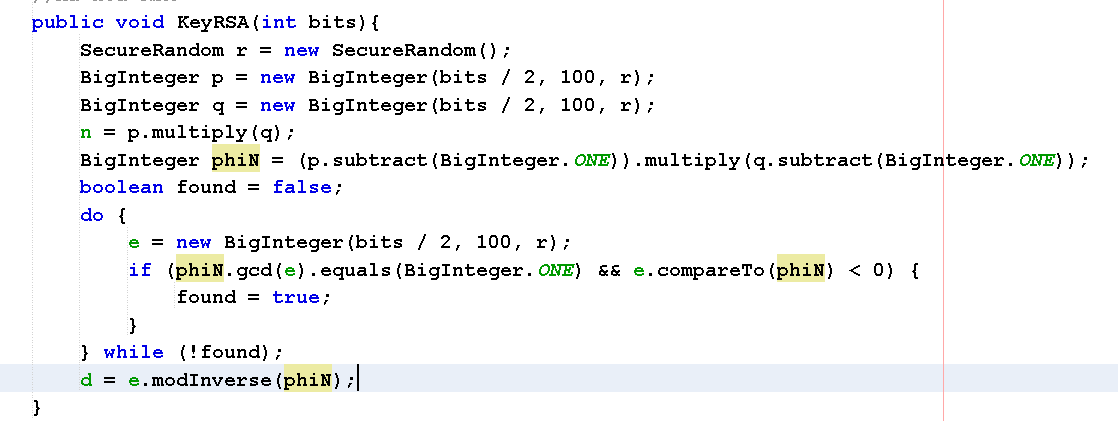
Nếu MD1 = MD2 → chữ ký kiểm tra thành công. Thông điệp đảm bảo tính toàn vẹn và thực sự xuất phát từ người gửi (do khóa công khai được chứng thực).

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.

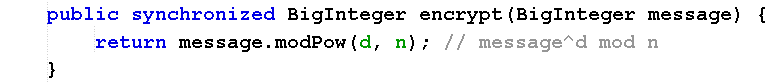
1. **Cài đặt giải thuật trong ngôn ngữ JAVA.**

* Sử dụng BigInteger trong gói java.math.\* cung cấp hầu hết các hàm dựng và các hàm số học cho phép thao tác thuận lợi với số nguyên lớn.
* Một số hàm:
  + Hàm dựng BigInteger (int bitLength, int certainty, Random rnd): sinh số nguyên tố ngẫu nhiên với số bit cho trước.
  + Hàm BigInteger subtract(BigInteger val): Trừ 2 số nguyên lớn.
  + Hàm BigInteger multiply(BigInteger val): nhân 2 số nguyên lớn.
  + Hàm gcd(BigInteger val): Tìm USCLN của 2 số lớn
  + Hàm BigInteger modInverse(BigInteger m): tính modulo nghịch đảo (this-1mod m).
  + Hàm BigInteger modPow(BigInteger exponent, BigInteger m). Tính (thisexponent mod m).

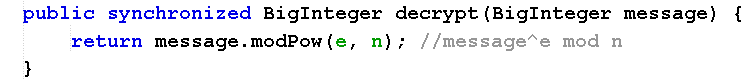
1. **Tạo khóa.**



1. **Mã hóa.**



1. **Giải mã.**



1. **Demo**

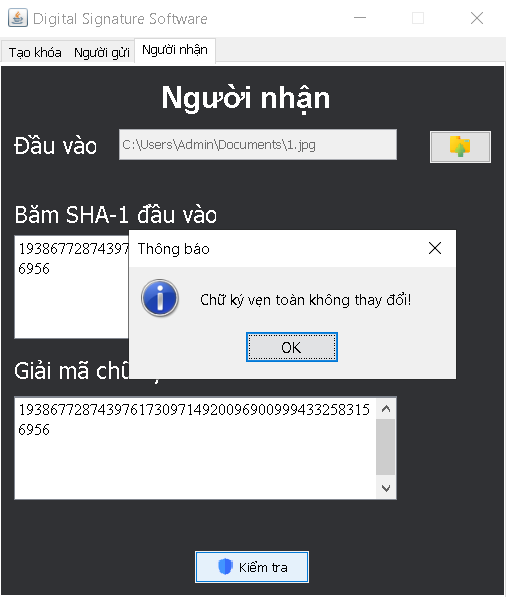
* **Tạo khóa.**



* **Quá trình ký.**



* **Quá trình kiểm tra chữ ký.**



1. **Kết luận**
2. **Điểm mạnh.**
   1. **Chữ ký số có khả năng xác định nguồn gốc chuẩn xác.**

* Hệ thống mật mã hóa khóa công khai cho phép mật mã hóa văn bản với khóa bí mật mà chỉ có chủ sở hữu của khóa mới biết. Để sử dụng chữ ký số thì văn bản cần phải được mã hóa hàm băm. Sau khi sử dụng khóa bí mật của chủ khóa để mã hóa, bạn sẽ có được chữ ký số.
* Để kiểm tra, bên nhận giải mã với khóa công khai để lấy lại hàm băm và rà soát với hàm băm của văn bản nhận được. Nếu hai giá trị này đảm bảo khớp nhau thì văn bản đó chính xác là của người sở hữu khóa bí mật.
  1. **Chữ ký số có tính không thể phủ nhận.**
* Trong giao dịch, bên gửi có thể từ chối rằng văn bản đó không phải do mình gửi. Vậy nên, để phòng ngừa trường hợp này xảy ra, bên nhận có thể đề xuất bên gửi phải kèm thêm chữ ký số với văn bản. Điều này nhằm đảm bảo khi có tranh chấp, chữ ký số sẽ là một chứng cứ thuyết phục, chắc chắn để bên thứ ba giải quyết.
  1. **Tính toàn vẹn thông tin**
* Những tưởng hình thức bên ngoài của chữ ký thiết kế khá đơn giản như một chiếc USB thông thường sẽ không an toàn lưu trữ đầy đủ lượng thông tin. Tuy nhiên, bản chất thực sự của chữ ký số rất tuyệt vời, đây là một thiết bị thông tin đặc biệt và hiện đại. Nguồn thông tin dữ liệu bên trong chỉ có thể dùng xác nhận văn bản điện tử, quan trọng hơn hết là bạn không thể thay đổi hay xóa đi. Nhờ ưu điểm này, chữ ký số luôn đảm bảo sự chuẩn xác tuyệt đối, thể hiện đúng vai trò xác nhận minh bạch của nó.
* Doanh nghiệp sẽ không phải lo sợ vì tình trạng văn bản bị sửa đổi trong khi truyền đi. Bởi bất kỳ mộ thay đổi nào dù là nhỏ nhất đều dễ dàng bị phát hiện ngay lập tức. Quy trình mã hóa sẽ giúp ẩn nội dung thông tin với bên thứ ba.
  1. **Tính bảo mật**
* Đây là ưu điểm nổi bật và tuyệt vời nhất của chữ ký số mang đến cho người dùng. Về kỹ thuật công nghệ, chữ ký số được làm dựa trên hạ tầng mã hóa công khai (PKI), trong đó phần quan trọng nhất là thuật toán mã hóa công khai RSA. Nhờ vậy, chữ ký số được tạo ra tương ứng, duy nhất với một người dùng cụ thể. Nghĩa là người khác sẽ không thể giải mạo được, chỉ có chủ sở hữu khoá bí mật mới có thể tạo ra và biết thông tin lưu trữ. Có thể khẳng định rằng, chữ ký số giúp bảo mật thông tin một cách an toàn tuyệt đối.
  1. **Giúp giảm tiết kiệm thời gian chi phí.**
* Vận hành doanh nghiệp, việc sử dụng chữ ký số trở thành nhu cầu thiết yếu và cần thiết. Điều này giúp doanh nghiệp dễ dàng, tiện lợi hơn trong giao dịch với ngân hàng hoặc các cơ quan hành chính khác mà không cần phải di chuyển cồng kềnh giấy tờ, hồ sơ phức tạp. Ở tại văn phòng, doanh nghiệp chỉ cần ký chữ ký số trên máy tính và gửi văn bản điện tử đến người nhận một cách gọn nhẹ, nhanh chóng

1. **Điểm yếu.**
   1. **Phức tạp trong quá trình chứng minh nếu xảy ra sai sót, giả mạo.**

* Dù trường hợp sai sót, giả mạo chữ ký số rất hiếm khi xảy ra, tuy nhiên bạn nên dự liệu trước. Khi chữ ký số gặp trục trặc, cản trở việc xác minh người sử dụng không chính xác thì việc kiểm chứng lại chữ ký số đó sẽ khá khó khăn, tốn kém thời gian. Đây cũng là hạn chế khó tránh trong phương thức xác nhận bằng công nghệ cao. Tuy nhiên, biện pháp hiệu quả để khắc phục, hạn chế tình trạng này là cần cải thiện tính bảo mật, chắc chắn chữ ký số để giảm thiểu rủi ro cho người dùng.
  1. **Chữ ký số khi sử dụng kê khai thuế qua mạng khá khó khăn.**
* Khi ứng dụng chữ ký số vào quy trình kê khai thuế qua mạng sẽ xuất hiện một các lỗi như là: cài đặt Java, trình duyệt Internet Explorer không tương thích, lỗi hồ sơ chưa đăng ký thuế qua mạng, lỗi cấu trúc, tên tệp khai không hợp lệ,…
* Hơn nữa, phần mềm kê khai thuế qua mạng không thể cập nhật được số liệu điều chỉnh của tờ khai sau khi quá hạn nộp báo cáo. Và đường truyền công nghệ thông tin, cơ sở hạ tầng chưa đảm bảo chất lượng tốt.

1. **Tài liệu tham khảo.**

* Giáo trình An Toàn Bảo Mật Hệ Thống Thông Tin\_TS Hoàng Xuân Dậu\_HVCNBCVT.(Chương 4: Các kỹ thuật mã hóa thông tin)
* http://vi.wikipedia.org/wiki/RSA\_(m%C3%A3\_h%C3%B3a)
* http://en.wikipedia.org/wiki/RSA
* http://vi.wikipedia.org/wiki/Ch%E1%BB%AF\_k%C3%BD\_s%E1%BB%91
* http://en.wikipedia.org/wiki/Digital\_signature
* http://docs.oracle.com/javase/7/docs/api/java/math/BigInteger.html
* http://vi.wikipedia.org/wiki/SHA
* http://www.java2s.com/Tutorial/Java/0490\_\_Security/UseSHA1.htm
* Internet.