# I. Mở đầu

Ngày nay trong mọi hoạt động của con người thông tin đóng một vai trò quan trọng không thể thiếu. Xã hội càng phát triển nhu cầu trao đổi thông tin giữa các thành phần trong xã hội ngày càng lớn. Mạng máy tính ra đời đã mang lại cho con người rất nhiều lợi ích trong việc trao đổi và xử lý thông tin một cách nhanh chóng và chính xác. Chính từ những thuận lợi này đã đặt ra cho chúng ta một câu hỏi, liệu thông tin đi từ nơi gửi đến nơi nhận có đảm bảo tuyệt đối an toàn, ai có thể đảm bảm thông tin của ta không bị truy cập bất hợp pháp. Thông tin được lưu giữ, truyền dẫn, cùng sử dụng trên mạng lưới thông tin công cộng có thể bị nghe trộm, chiếm đoạt, xuyên tạc hoặc phá huỷ dẫn đến sự tổn thất không thể lường được. Đặc biệt là đối với những số liệu của hệ thống ngân hàng, hệ thống thương mại, cơ quan quản lý của chính phủ hoặc thuộc lĩnh vực quân sự được lưu giữ và truyền dẫn trên mạng. Nếu như vì nhân tố an toàn mà thông tin không dám đưa lên mạng thì hiệu suất làm việc cũng như hiệu suất lợi dụng nguồn dữ liệu đều sẽ bị ảnh hưởng. Trước các yêu cầu cần thiết đó, việc mã hoá thông tin sẽ đảm bảo an toàn cho thông tin tại nơi lưu trữ cũng như khi thông tin được truyền trên mạng.

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 tổ chức. Vì vậy an toàn thông tin là nhiệm vụ quan trọng, nặng nề và khó đoán trước đối với các hệ thống thông tin.

Một trong những ứng dụng của an toàn thông tin là chữ ký số. Với đặc điểm là đơn giản cho người sử dụng mà vẫn đảm bảo được tính bảo mật, kỹ thuật sử dụng chữ ký số là một trong những kỹ thuật được sử dụng phổ biến, đa dạng trong hầu hết các lĩnh vực, nhất là Tài chính, Ngân hang, Kế toán…Vì lý do đó, tôi quyết định nghiên cứu về “Giải thuật tạo chữ ký số sử dụng thuật toán RSA”.

# II. Tổng quan về an toàn thông tin

## **1. Khái niệm an toàn thông tin**

An toàn thông tin là các hoạt động bảo vệ tài sản thông tin và là một lĩnh vực rộng lớn. Nó bao gồm cả những sản phẩm và những quy trình nhằm ngăn chặn truy cập trái phép, hiệu chỉnh, xóa thông tin,…

An toàn thông tin liên quan đến hai khía cạnh đó là an toàn về mặt vật lý và an toàn về mặt kỹ thuật.

- Mục tiêu cơ bản của an toàn thông tin

+ Đảm bảo tính bảo mật

+ Đảm bảo tính toàn vẹn

+ Đảm bảo tính xác thực

+ Đảm bảo tính sẵn sàng

## **2. Sự cần thiết của an toàn thông tin**

Hệ thống thông tin là thành phần thiết yếu trong mọi cơ quan, tổ chức và đem lại khả năng xử lý thông tin, là tài sản quan trọng nhưng hệ thống thông tin cũng chứa rất nhiều điểm yếu và rủi do. Do máy tính được phát triển với tốc độ rất nhanh để đáp ứng nhiều yêu cầu của người dùng, các phiên bản được phát hành liên tục với các tính năng mới được thêm vào ngày càng nhiều, điều này làm cho các phần mềm không được kiểm tra kỹ trước khi phát hành và bên trong chúng chứa rất nhiều lỗ hổng có thể dễ dàng bị lợi dụng. Thêm vào đó là việc phát triển của hệ thống mạng, cũng như sự phân tán của hệ thống thông tin, làm cho người dùng truy cập thông tin dễ dàng hơn và tin tặc cũng có nhiều mục tiêu tấn công dễ dàng hơn.

## **3. Mục đích của an toàn thông tin**

*\* Bảo vệ tài nguyên của hệ thống*

Các hệ thống máy tính lưu giữ rất nhiều thông tin và tài nguyên cần được bảo vệ. Trong một tổ chức, những thông tin và tài nguyên này có thể là dữ liệu kế toán, thông tin nguồn nhân lực, thông tin quản lý, bán hàng, nghiên cứu, sáng chế, phân phối, thông tin về tổ chức và thông tin về các hệ thống nghiên cứu. Đối với rất nhiều tổ chức, toàn bộ dữ liệu quan trọng của họ thường được lưu trong một cơ sở dữ liệu và được quản lý và sử dụng bởi các chương trình phần mềm.

Các tấn công vào hệ thống có thể xuất phát từ những đối thủ của tổ chức hoặc cá nhân do đó, các phương pháp để bảo đảm an toàn cho những thông tin này có thể rất phức tạp và nhạy cảm. Các tấn công có thể xuất phát từ nhiều nguồn khác nhau, cả từ bên trong và bên ngoài tổ chức. Hậu quả mà những tấn công thành công để lại sẽ rất nghiêm trọng.

*\* Bảo đảm tính riêng tư*

Các hệ thống máy tính lưu giữ rất nhiều thông tin cá nhân cần được giữ bí mật. Những thông tin này bao gồm: Số thẻ bảo hiểm xã hội, số thẻ ngân hàng, số thẻ tín dụng, thông tin về gia đình,...

Tính riêng tư là yêu cầu rất quan trọng mà các ngân hàng, các công ty tín dụng, các công ty đầu tư và các hãng khác cần phải đảm bảo để gửi đi các tài liệu thông tin chi tiết về cách họ sử dụng và chia sẻ thông tin về khách hàng. Các hãng này có những quy định bắt buộc để bảo đảm những thông tin cá nhân được bí mật và bắt buộc phải thực hiện những quy định đó để bảo đảm tính riêng tư. Hậu quả nghiêm trọng sẽ xảy ra nếu một kẻ giả mạo truy nhập được những thông tin cá nhân.

## **4. Một số kỹ thuật an toàn và bảo mật thông tin**

*\* Mã hóa thông tin*

Trong khoa học mật mã là việc sử dụng các kỹ thuật thích hợp để biến đổi một bản thông điệp có ý nghĩa thành một dãy mã ngẫu nhiên để liên lạc với nhau giữa người gửi và người nhận mà người ngoài cuộc có thể có được sự hiện hữu của dãy mã ngẫu nhiên đó nhưng khó có thể chuyển thành bản thông điệp ban đầu nếu không có “khóa” để giải mã của thông điệp.



*\* Giấu tin*

Giấu tin là kỹ thuật nhúng một lượng thông tin số (ảnh, audio, video) vào trong một đối tượng dữ liệu số khác. Một trong những yêu cầu cơ bản của giấu tin là đảm bảo tính chất ẩn của thông tin được giấu, đồng thời không làm ảnh hưởng đến chất lượng của dữ liệu gốc. Mục đích của giấu tin là làm cho thông tin đã giấu không thể nghe thấy hoặc nhìn thấy được, người ngoài cuộc không thể nhận thấy được sự tồn tại của thông tin đã giấu.

Kỹ thuật giấu tin gồm 2 phần là thuật toán giấu tin và thuật toán tách thông tin đã giấu trong ra khỏi phương tiện mang tin đã giấu.



*\* Thủy vân số*

Thủy vân số là kỹ thuật nhúng thông tin vào dữ liệu (dữ liệu có thể là văn bản, hình ảnh, audio, video hay cơ sở dữ liệu,...) trước khi phân phối dữ liệu trên môi trường trao đổi thông tin nhằm xác định thông tin về chủ sở hữu hoặc nhận biết sự tấn công trái phép từ bên ngoài đối với dữ liệu đã được thủy vân. Thông tin giấu trong dữ liệu được gọi là thủy vân (watermark).



*\* Chữ ký số*

Chữ ký điện số là thông tin đi kèm theo dữ liệu (văn bản, âm thanh,hình ảnh, video...) nhằm mục đích xác định người chủ của dữ liệu đó.

Chữ ký điện số là chuỗi thông tin cho phép xác định nguồn gốc, xuất xứ, thực thể đã tạo ra 1 thông điệp.

Chữ ký số khóa công khai là mô hình sử dụng các kỹ thuật mật mã để gắn với mỗi người sử dụng một cặp khóa công khai - bí mật, qua đó có thể ký các văn bản điện tử cũng như trao đổi các thông tin mật.

Khóa công khai thường được phân phối thông qua chứng thực khóa công khai.



# III. Giới thiệu về chữ ký số.

## **1. Một số khái niệm**

*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.

*Hàm băm (Hash Funtion)* là hàm toán học chuyển đổi thông điệp (message) có độ dài bất kỳ (hữu hạn) thành một dãy bít có độ dài cố định (tùy thuộc vào thuật toán băm). Dãy bít này được gọi là thông điệp rút gọn (message disgest) hay giá trị băm (hash value), đại diện cho thông điệp ban đầu.

+ Trong đó, Hàm băm SHA-1: Thuật toán SHA-1 nhận thông điệp ở đầu vào có chiều dài k<264 bit, thực hiện xử lý và đưa ra thông điệp thu gọn (message digest) có chiều dài cố định 160 bits. Quá trình tính toán cũng thực hiện theo từng khối 512bits, nhưng bộ đệm xử lý dùng 5 thanh ghi 32-bits. Thuật toán này chạy tốt với các bộ vi xử lý có cấu trúc 32 bits.

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.

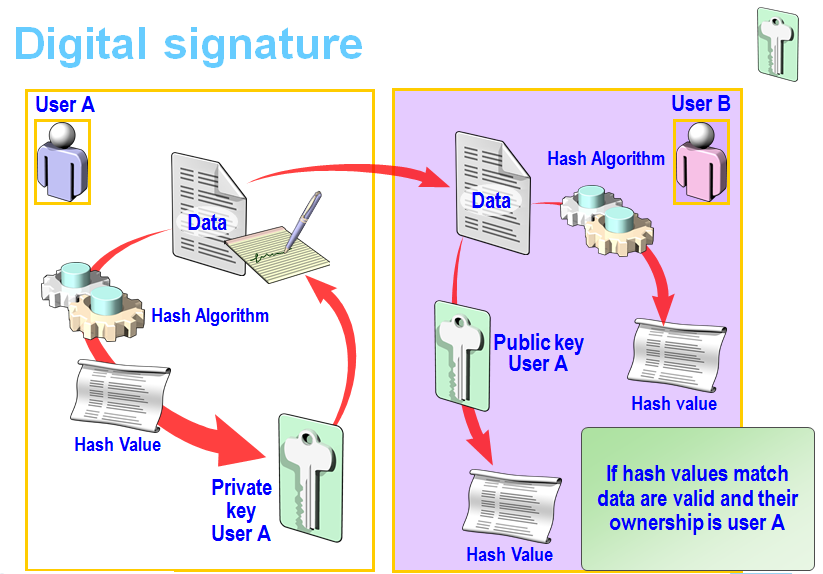
*Lược đồ chữ ký số RSA* : độ an toàn của lược đồ chữ ký RSA dựa vào độ an toàn của hệ mã RSA. Lược đồ bao gồm cả chữ ký số kèm theo bản rõ và tự khôi phục thông điệp từ chữ ký số.

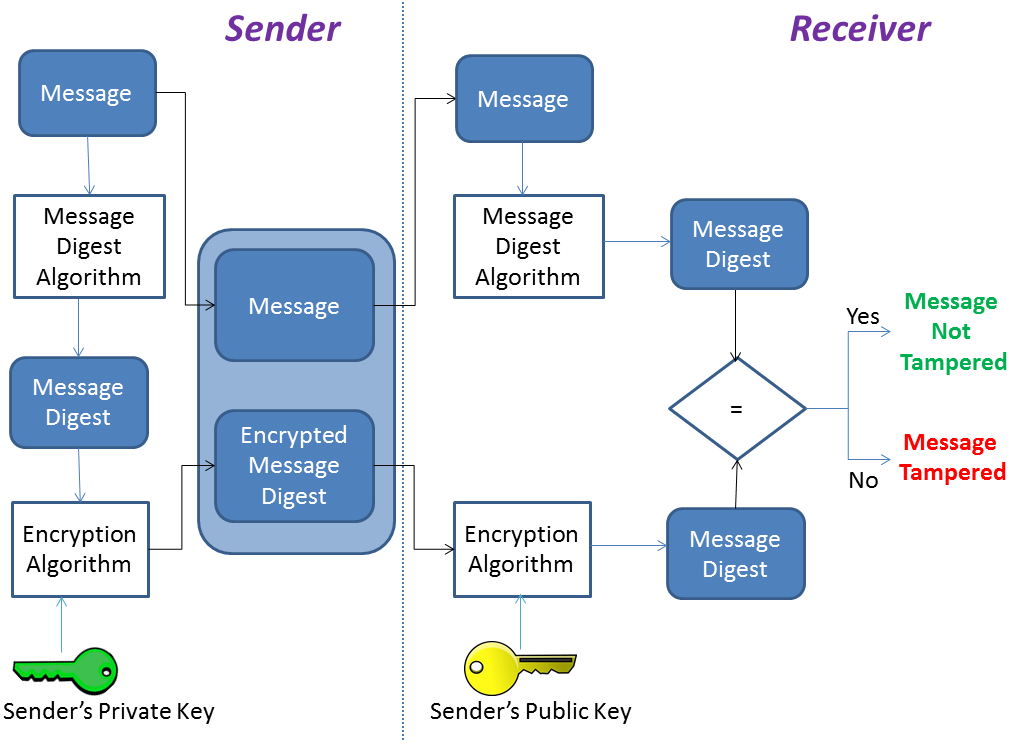
+ Thuật toán sinh khóa cho lược đồ chữ ký RSA

+ Thuật toán sinh chữ ký RSA

+ Thuật toán chứng thực chữ ký RSA

## **2. Kiến trúc chữ ký số tổng quát**





***2.1 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

***2.2 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

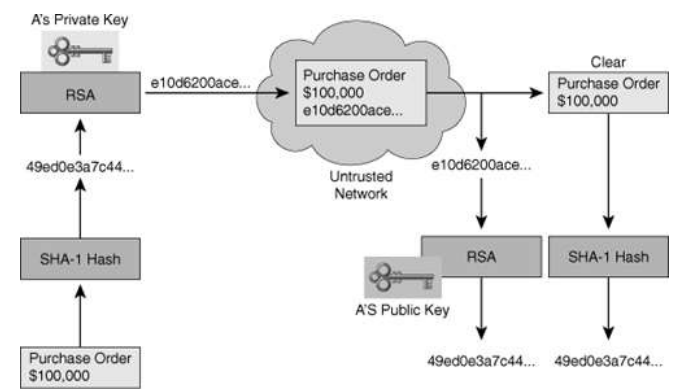
So sánh MD1 và MD2:

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).

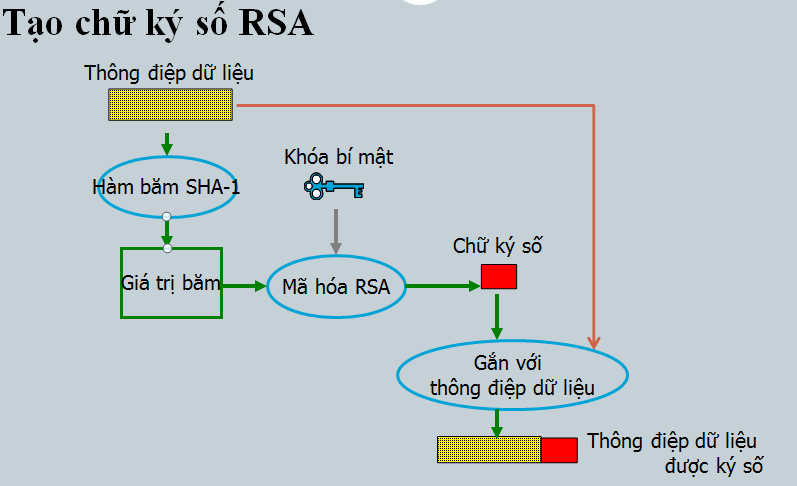
Nếu MD1 <>MD2 -> chữ ký không hợp lệ. Thông điệp có thể đã bị sửa đổi hoặc không thực sự xuất phát từ người gửi.

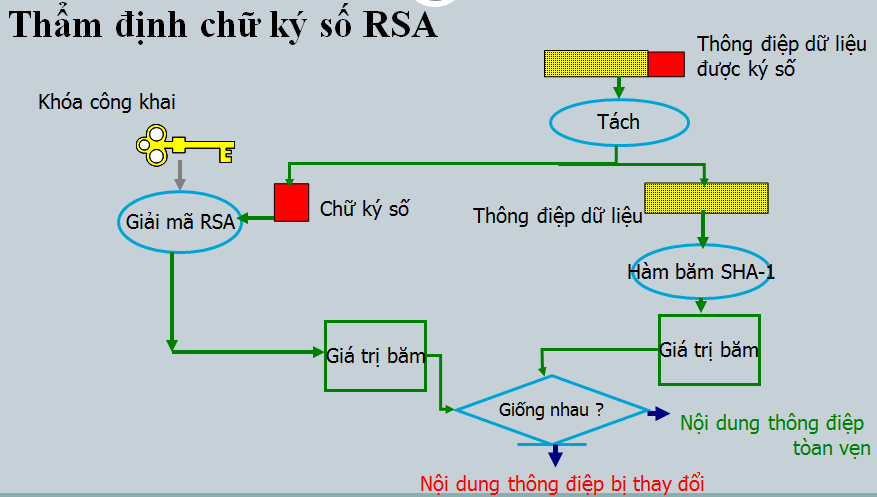
# IV. Kiến trúc chữ ký số RSA

## **1. Tổng quan**



Cụ thể hơn:





***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:

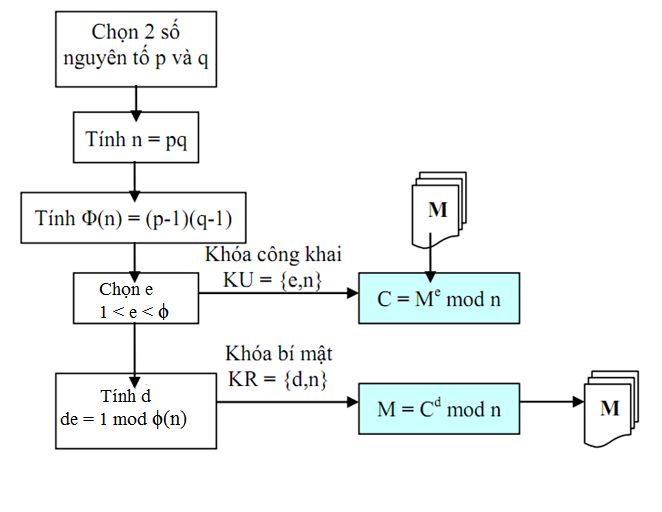
Nếu MD1 =MD2 -> chữ ký kiểm tra thành công. Thông điệp đảm bảo tính toàn vẹn và thực sự xuất phát từ người gửi (do khóa công khai được chứng thực).

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.

## **2. Giải thuật và cài đặt giải thuật**

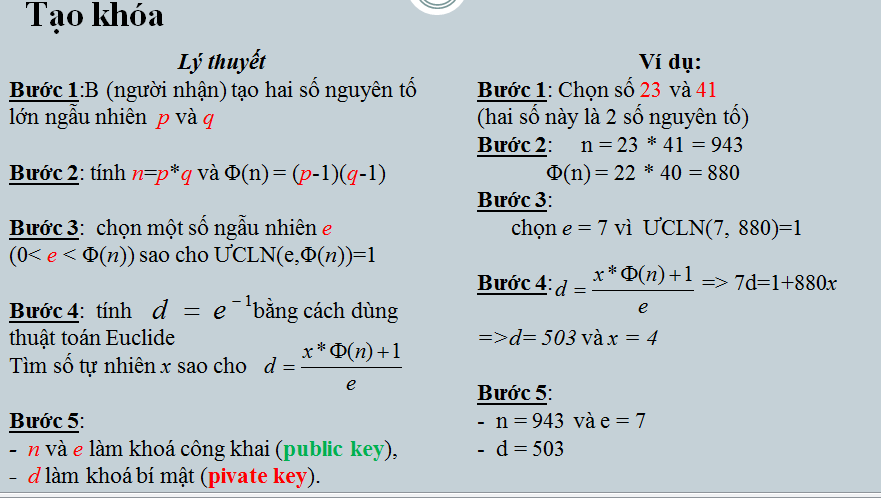
### ***2.1 Giải thuật RSA được dùng trong việc tạo khóa, mã hóa, giải mã.***

*Sơ đồ giải thuật :*

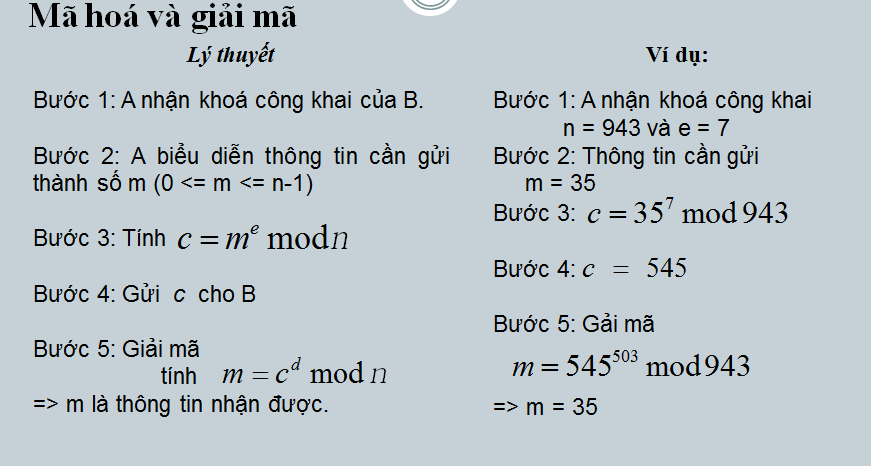
******

|  |  |
| --- | --- |
| Thuật toán RSA có hai Khóa:  **- *Khóa công khai*** (**Public key**): được công bố rộng rãi cho mọi người và được dùng để mã hóa  **-** ***Khóa bí mật*** (**Private key**):  Những thông tin được mã hóa bằng khóa công khai chỉ có thể được giải mã bằng khóa bí mật tương ứng | C:\Users\Mr Khiem\Desktop\RSA\Báo cáo\TQRSA.png |

a. Tạo khóa



b. Mã hóa và giải mã



### ***2.2 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 add(BigInteger val): cộng 2 số nguyên lớn;

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

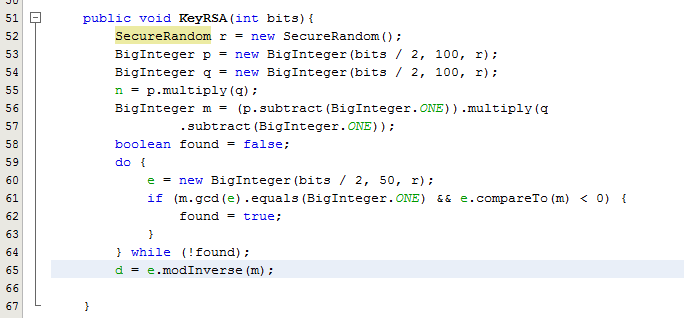
Hàm mod(BigInteger m): Tính modulo (phần dư) của phép chia nguyên;

Hàm BigInteger modInverse(BigInteger m): tính modulo nghịch đảo (this-1mod m);

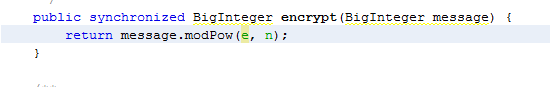
Hàm BigInteger modPow(BigInteger exponent, BigInteger m): Tính (thisexponent mod m).

Cụ thể code RSA

Tạo khóa:



Mã hóa: (code này trong RSA , còn trong chữ ký số thì d bí mật được mã hóa)



Giải mã: (code này trong RSA , còn trong chữ ký số thì e công khai được mã hóa)

C:\Users\Mr Khiem\Desktop\RSA\Báo cáo\giai ma code.PNG

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

## **1. 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.

## **2. Chữ ký số sử dụng RSA**

### ***2.1 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).

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

**a.** **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.

**b. 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.

# V. Tài liệu tham khảo

**1.**Giáo trình An Toàn Bảo Mật Hệ Thống Thông Tin\_TS Hoàng Xuân Dậu\_HVCNBCVT.(Chương 4: Các kỹ thuật mã hóa thông tin)

**2.** http://vi.wikipedia.org/wiki/RSA\_(m%C3%A3\_h%C3%B3a)

**3.** http://en.wikipedia.org/wiki/RSA

**4.** http://vi.wikipedia.org/wiki/Ch%E1%BB%AF\_k%C3%BD\_s%E1%BB%91

**5.** http://en.wikipedia.org/wiki/Digital\_signature

**6.** http://docs.oracle.com/javase/7/docs/api/java/math/BigInteger.html

**7.** http://vi.wikipedia.org/wiki/SHA

**8.** http://www.java2s.com/Tutorial/Java/0490\_\_Security/UseSHA1.htm

**9.**https://nguyendangkhiemit.wordpress.com/2014/10/19/chu-ky-so-su-dung-giai-thuat-rsa/

**MỤC LỤC**

[I. Mở đầu 1](#_Toc42498283)

[II. Tổng quan về an toàn thông tin 2](#_Toc42498284)

[1. Khái niệm an toàn thông tin 2](#_Toc42498285)

[2. Sự cần thiết của an toàn thông tin 2](#_Toc42498286)

[3. Mục đích của an toàn thông tin 2](#_Toc42498287)

[4. Một số kỹ thuật an toàn và bảo mật thông tin 3](#_Toc42498288)

[III. Giới thiệu về chữ ký số. 6](#_Toc42498289)

[1. Một số khái niệm 6](#_Toc42498290)

[2. Kiến trúc chữ ký số tổng quát 7](#_Toc42498291)

[IV. Kiến trúc chữ ký số RSA 10](#_Toc42498292)

[1. Tổng quan 10](#_Toc42498293)

[2. Giải thuật và cài đặt giải thuật 12](#_Toc42498294)

[*2.1 Giải thuật RSA được dùng trong việc tạo khóa, mã hóa, giải mã.* 12](#_Toc42498295)

[*2.2 Cài đặt giải thuật trong ngôn ngữ JAVA* 15](#_Toc42498296)

[IV. Các điểm yếu của chữ ký số sử dụng giải thuật RSA 17](#_Toc42498297)

[1. Chữ ký số nói chung 17](#_Toc42498298)

[2. Chữ ký số sử dụng RSA 18](#_Toc42498299)

[*2.1 Hiệu suất thực hiện thuật toán RSA* 18](#_Toc42498300)

[*2.2 Chi phí và tốc độ thực hiện thuật toán RSA* 18](#_Toc42498301)

[V.Tài liệu tham khảo 19](#_Toc42498302)