

TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI  
Viện Công nghệ Thông tin và Truyền thông



Tiểu luận môn học  
Nhập môn An toàn thông tin IT4015

Đề tài:

***CHỮ KÍ SỐ***

*Nhóm số 3*

<b>Nhóm sinh viên thực hiện:</b>	Lê Trọng Nhân	MSSV: 20173292
	Lê Văn Linh	MSSV: 20173235
	Lê Thái Bảo	MSSV: 20172966
	Bùi Minh Tuấn	MSSV: 20170121
	<b>Mã lớp: 115655</b>	
<b>Giáo viên hướng dẫn:</b>	PGS.TS Nguyễn Linh Giang	

*Hà Nội, tháng 4 năm 2020*

## MỤC LỤC

MỤC LỤC .....	1
MỤC LỤC HÌNH VẼ.....	3
CHƯƠNG 1. TỔNG QUAN.....	4
1.1. Chữ kí điện tử.....	4
1.2. Định nghĩa chữ kí số: .....	4
1.3. Lịch sử chữ kí số: .....	4
1.4. Một số yêu cầu đối với chữ kí số: .....	5
1.5. Việc sử dụng chữ kí số có một số ưu điểm sau: .....	5
CHƯƠNG 2. CÁC CƠ CHẾ VÀ GIAO THỨC CHỮ KÍ SỐ.....	6
2.1. Các cơ chế tạo chữ kí số .....	6
2.2. Giao thức chữ kí số .....	7
2.2.1. Chữ kí số RSA .....	7
2.2.2. Chữ kí số ElGamal.....	8
2.2.3. Chữ kí số tiêu chuẩn (Digital Signature Standard - DSS) .....	9
2.3. Tính an toàn trong chữ kí số RSA .....	9
2.3.1. Ưu điểm chữ kí số RSA .....	9
2.3.2. Nhược điểm chữ kí số RSA .....	10
2.3.3. Các kịch bản tấn công và phòng thủ.....	10
CHƯƠNG 3. CÁC DỊCH VỤ CHỮ KÍ SỐ.....	11
3.1. Dịch vụ con dấu thời gian (Time-stamp) .....	12
3.2. Dịch vụ không đồng bộ (Asynchronous) .....	12
3.3. Dịch vụ kí mã (Code-signing).....	12
3.4. Dịch vụ kí mã J2ME .....	12
3.5. Niêm phong thực thể (Entity Seal) .....	12
3.6. Dấu bưu điện điện tử (Electronic Postmark – EPM) .....	12
3.7. Dịch vụ Signature Gateway .....	12
CHƯƠNG 4. Chữ kí mù .....	13
4.1. Hoàn cảnh ra đời .....	13
4.2. Khái niệm.....	13
4.3. Yêu cầu đối với chữ kí mù.....	13
4.4. Mô hình chữ kí mù.....	14
4.4.1. Dựa trên hệ RSA.....	14

4.4.2.	Dựa trên sơ đồ chữ kí Schnorr .....	14
4.4.3.	Dựa trên bilinear pairing .....	15
4.5.	Ứng dụng của chữ kí mù.....	15
4.5.1.	Tiền điện tử .....	15
4.5.2.	Bầu cử số (e-voting) .....	16
CHƯƠNG 5. ỨNG DỤNG CHỮ KÍ SỐ .....		16
5.1.	Giao dịch thương mại điện tử: .....	16
5.2.	Kê khai thuế, nộp thuế trực tiếp qua mạng Internet.....	17
CHƯƠNG 6. TRIỂN KHAI CÀI ĐẶT.....		17
6.1.	Các công cụ sử dụng và mã nguồn .....	17
6.2.	Sơ đồ mô tả .....	17
6.2.1.	Sơ đồ mã hoá thông điệp .....	18
6.2.2.	Sơ đồ giải mã thông điệp .....	18
TÀI LIỆU THAM KHẢO .....		19

## MỤC LỤC HÌNH VẼ

Hình 2.1 Cơ chế tạo chữ kí số	6
Hình 2.2 Giao thức chữ kí số RSA.....	7
Hình 2.3 Giao thức chữ kí số ElGamal .....	8
Hình 2.4 Giao thức chữ kí số tiêu chuẩn .....	9
Hình 6.1 Sơ đồ mã hoá thông điệp .....	18
Hình 6.2 Sơ đồ giải mã thông điệp.....	18

## CHƯƠNG 1. TỔNG QUAN

### 1.1. Chữ ký điện tử

Khái niệm chữ ký điện tử được hai nhà bác học Diffie và Hellman đề xuất trong cùng bài báo nổi tiếng của các ông khai sáng nguyên lý của hệ thống mật mã công khai (1976). Ý tưởng về mô phỏng chữ ký tay trên văn bản trong đời thường đã có từ lâu, nhưng thực sự chỉ có thể thực hiện được cùng với sự ra đời của hệ mật mã KCK (khóa công khai). Như đã biết, hệ thống mật mã đối xứng đã được sử dụng phổ biến trước đó không có tính chất đại diện duy nhất cho một cá nhân. Trong khi đó, một hệ mã hóa khóa công khai (hay còn gọi là phi đối xứng) có thể được xem là được tạo lập để giúp bảo mật truyền tin trong liên lạc giữa 1 cá nhân và phần còn lại của xã hội. Nhờ có mật mã KCK, khái niệm chữ ký điện tử mới được hiện thực hóa và giúp cho giao dịch kinh tế thương mại trong đời sống có thể đi vào số hóa hoàn toàn, qua đó thúc đẩy hoạt động dịch vụ trực tuyến trên Internet phát triển như ngày này. Chữ ký điện tử (electronic signature) không phải là hình thức số hoá chữ ký viết tay rồi gửi kèm theo một thông điệp mà là một phương thức để chứng thực nguồn gốc và nội dung của một thông điệp thông qua kỹ thuật mã hoá.

### 1.2. Định nghĩa chữ ký số:

Chữ ký số (Digital signature) là một dạng chữ ký điện tử (là tập con của chữ ký điện tử) được tạo ra bằng sự biến đổi một thông điệp dữ liệu sử dụng hệ thống mật mã hoá khoá công khai, theo đó người có thông điệp dữ liệu ban đầu và khoá công khai của người ký có thể xác định được chính xác.

Chữ ký điện tử là thông tin đi kèm theo dữ liệu (văn bản, hình ảnh, video...) nhằm mục đích xác định người chủ của dữ liệu đó. Cũng có thể sử dụng định nghĩa rộng hơn, bao hàm cả mã nhận thực, hàm băm và các thiết bị bút điện tử.

### 1.3. Lịch sử chữ ký số:

Chúng ta đã sử dụng trong những hợp đồng với chữ ký dưới dạng điện tử từ hơn 100 năm nay với việc tiến hành mã Morse và điện tín. trong khoảng năm 1889, tòa án tối cao bang New Hampshire (Hoa kỳ) đã tính hiệu lực của chữ ký điện tử. mặc dù vậy, chỉ với những tiến bộ vượt bậc của khoa học công nghệ gần đây thì chữ ký số mới đi vào cuộc sống một cách phổ biến.

Đến năm 1976, khái niệm chữ ký điện tử được hai nhà bác học Diffie và Hellman đề xuất trong cùng bài báo nổi tiếng của các ông khai sáng nguyên lý của hệ thống mật mã công khai

Vào thập kỷ 1980, các tổ chức và một số đơn vị bắt đầu áp dụng máy fax để truyền tải các tài liệu quan trọng. Mặc dù chữ ký trên các tài liệu này vẫn thể hiện trên giấy, nhưng quá trình truyền và nhận chúng hoàn toàn dựa trên tín hiệu điện tử và được coi là chữ ký điện tử.

Hiện nay, theo quan niệm thông dụng trong giao dịch quốc tế, chữ kí điện tử có thể bao hàm các cam kết gửi bằng email, nhập các số định dạng cá nhân (PIN) vào các máy ATM (của Vietcombank chẳng hạn) để rút tiền, chấp nhận các điều khoản người dùng (EULA) khi cài đặt phần mềm máy tính (như phần mềm Office của Microsoft chẳng hạn), kí các hợp đồng điện tử online.

#### 1.4. Một số yêu cầu đối với chữ kí số:

- Phải là một mẫu bit phụ thuộc vào tin nhắn được nó kí.
- Phải sử dụng thông tin là duy nhất cho người gửi để ngăn chặn giả mạo và phủ nhận gửi.
- Phải được khởi tạo một cách tương đối dễ dàng.
- Có thể nhận dạng và xác thực chữ kí một cách tương đối dễ dàng.
- Nó phải không thể được tính toán được để giả mạo dù bằng cách xây dựng một tin nhắn mới bằng chữ kí số hiện có hay tạo ra một chữ kí số giả mạo cho một tin nhắn nhất định sẵn có.
- Có thể được giữ lại như một bản sao chữ kí số trong bộ nhớ

#### 1.5. Việc sử dụng chữ kí số có một số ưu điểm sau:

- Khả năng xác định nguồn gốc:

Các hệ thống mật mã hóa khóa công khai cho phép mật mã hóa văn bản với khóa bí mật mà chỉ có người chủ của khóa biết. Để sử dụng Chữ kí số thì văn bản cần phải được mã hóa hàm băm (là giải thuật nhằm sinh ra các giá trị băm tương ứng với mỗi khối dữ liệu: có thể là một chuỗi kí tự, một đối tượng trong lập trình hướng đối tượng, v.v.... Giá trị băm đóng vai gần như một khóa để phân biệt các khối dữ liệu). Sau đó dùng khóa bí mật của người chủ khóa để mã hóa, khi đó ta được Chữ kí số. Khi cần kiểm tra, bên nhận giải mã với khóa công khai để lấy lại hàm băm và kiểm tra với hàm băm của văn bản nhận được. Nếu hai giá trị này khớp nhau thì bên nhận có thể tin tưởng rằng văn bản đó xuất phát từ người sở hữu khóa bí mật.

- Tính toàn vẹn.

Cả hai bên tham gia vào quá trình thông tin đều có thể tin tưởng là văn bản không bị sửa đổi trong khi truyền vì nếu văn bản bị thay đổi thì hàm băm cũng sẽ thay đổi và lập thức bị phát hiện. Quy trình mã hóa sẽ ẩn nội dung đối với bên thứ ba.

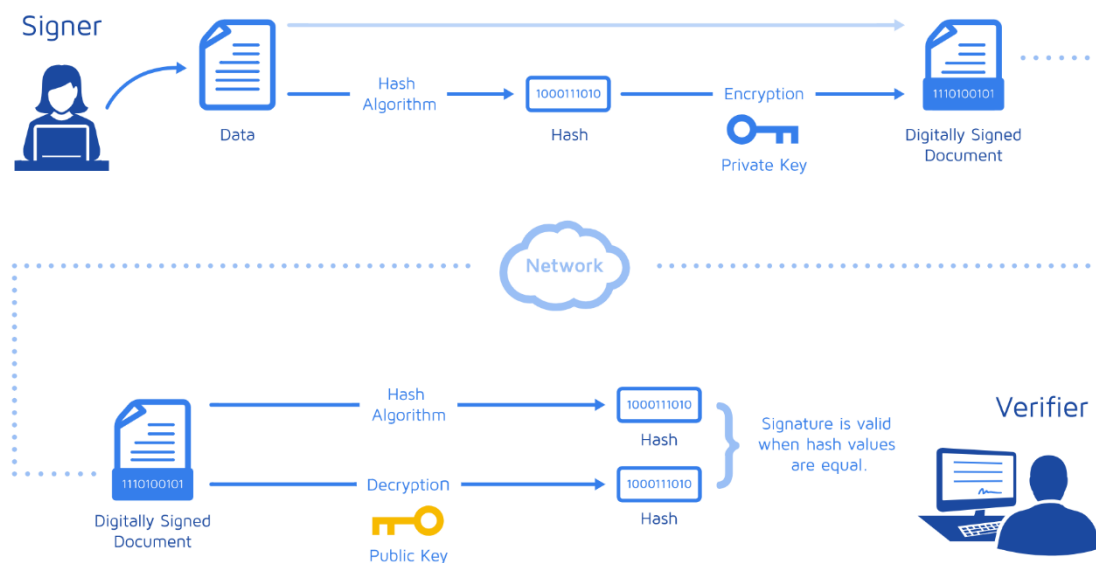
- Tính không thể phủ nhận.

Trong giao dịch, một bên có thể từ chối nhận một văn bản nào đó là do mình gửi. Để ngăn ngừa khả năng này, bên nhận có thể yêu cầu bên gửi phải gửi kèm chữ kí số với văn bản. Khi có tranh chấp, bên nhận sẽ dùng chữ kí này như một chứng cứ để bên thứ ba giải quyết.

## CHƯƠNG 2. CÁC CƠ CHẾ VÀ GIAO THỨC CHỮ KÍ SỐ

### 2.1. Các cơ chế tạo chữ ký số

Chữ ký số dựa trên công nghệ mã khoá công khai (RSA), mỗi người phải có một cặp khoá (key pair) gồm khoá riêng (Private key) và khoá công khai (Public key). Người ký sẽ giữ private key và dùng để mã hoá thông tin tạo ra chữ ký số, người nhận phải có public key của người ký tương ứng cặp với private key để giải mã chữ ký số nhằm đối chiếu thông tin.



Hình 2.1 Cơ chế tạo chữ ký số

Chữ ký số được thực hiện qua 2 quá trình:

- Quá trình kí:
  - + Tính toán chuỗi đại diện (message digest/hash value) của thông điệp sử dụng một giải thuật băm (Hashing algorithm).
  - + Chuỗi đại diện được kí sử dụng khóa riêng (Private key) của người gửi và một giải thuật tạo chữ kí (Signature/Encryption algorithm). Kết quả là chữ ký số (Digital signature) của thông điệp hay còn gọi là chuỗi đại diện được mã hóa (Encrypted message digest).
  - + Thông điệp ban đầu (message) được ghép với chữ ký số (Digital signature) tạo thành thông điệp đã được kí (Signed message).
  - + Thông điệp đã được kí (Signed message) được gửi cho người nhận.
- Quá trình kiểm tra:
  - + Tách chữ ký số và thông điệp gốc khỏi thông điệp đã kí 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 kí).
- + Sử dụng khóa công khai (Public key) của người gửi để giải mã chữ kí số => chuỗi đại diện thông điệp MD2.
- + So sánh MD1 và MD2:

Nếu  $MD1 = MD2 \Rightarrow$  chữ kí 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  $MD1 \neq MD2 \Rightarrow$  chữ kí không hợp lệ. Thông điệp có thể đã bị sửa đổi hoặc không thực sự xuất phát từ người gửi.

## 2.2. Giao thức chữ kí số

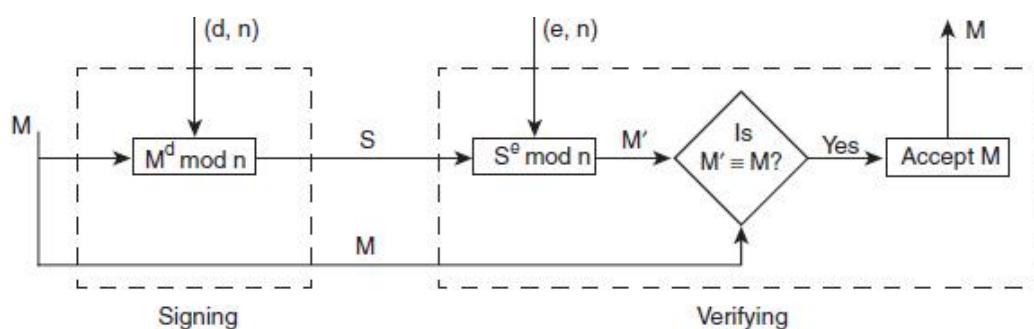
Giao thức kí số (Digital Signature Protocol) là quá trình sử dụng chữ kí số, gồm các pha làm việc bắt đầu từ tạo chữ kí số với một định dạng xác định, gắn vào văn bản, gửi văn bản được đính kèm với chứng thực, kiểm tra chữ kí số.

Bên kí A sử dụng một hàm băm (hash function) sinh một chuỗi đại diện (message digest) và mã hoá chuỗi đó với khoá riêng của A (private key). Nội dung bản tin và chữ kí được gửi cùng nhau. Bên nhận B cũng sử dụng hash function để tính toán message digest, và dùng khoá công khai của A để giải mã chữ kí của gói tin. Nếu message digest và chữ kí được giải mã thỏa mãn điều kiện, bên nhận B sẽ xác nhận chữ kí, ngược lại sẽ từ chối bản tin.

Mỗi một chuẩn kí số đều có thể coi là một giao thức làm việc, phải thống nhất giữa 2 bên gửi và nhận.

### 2.2.1. Chữ kí số RSA

Bên cạnh việc mã hoá và giải mã bản tin, thuật toán RSA còn có thể được sử dụng để kí và xác thực bản tin. Trong trường hợp này, nó được coi là chữ kí số RSA. Ở phía bên gửi, bản tin M cần được kí được đưa vào hàm sử dụng private key của bên gửi để sinh chữ ký số S. Phía gửi sẽ truyền toàn bộ bản tin và chữ kí cho người nhận. Tại phía người nhận, một hàm sử dụng chữ kí S và public key của người gửi để tính bản sao M'. Sau đó, so sánh M và M', nếu phù hợp thì người nhận sẽ chấp nhận bản tin, ngược lại thì bỏ qua bản tin. Lược đồ kí số RSA như sau:



Hình 2.2 Giao thức chữ kí số RSA



- Quá trình sinh khoá: Người gửi sinh một cặp khoá công khai và khoá riêng (public key và private key) như sau:

(i) Người gửi chọn 2 số nguyên tố  $p, q$  và tính các giá trị:

$$n = p * q$$

$$\Phi(n) = (p - 1)(q - 1)$$

(ii) Chọn số  $e$  thoả mãn  $1 < e < \Phi(n)$ . Tính  $d$  thoả mãn  $e * d \equiv 1 \pmod{\Phi(n)}$

- Quá trình kí: Bên gửi tạo chữ kí số  $S$  sử dụng khoá riêng  $d$  như sau:

$$S = M^d \pmod{n}$$

Trong đó,  $M$  là bản tin cần được kí

- Quá trình xác thực:

(i) Người nhận nhận bản tin  $M$  và chữ kí  $S$ , sử dụng khoá công khai  $(e, n)$  của người gửi để tính một bản tin bản sao như sau:  $M' = S^e \pmod{n}$

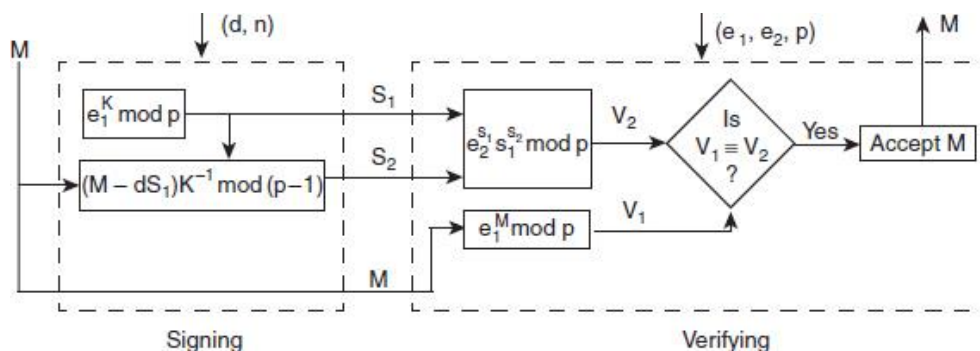
(ii) So sánh  $M'$  với  $M$ , nếu  $M' \equiv M$  thì bản tin được chấp nhận, ngược lại sẽ bỏ qua bản tin

- Sử dụng lược đồ kí số RSA trên chuỗi đại diện (message digest):

RSA còn có thể áp dụng trên chuỗi đại diện của bản tin. Khi đó, bản tin  $M$  cần sử dụng một hàm băm  $h$  đủ mạnh để tạo ra chuỗi đại diện  $D$ , sau đó được mã hoá với khoá riêng của bên gửi sinh ra chữ kí  $S$ . Người gửi gửi bản tin  $M$  và chữ kí  $S$  cho phía nhận. Ở phía người nhận, một hàm băm  $h$  tương tự được áp dụng với bản tin nhận được  $M$  để tính  $D$ , sau đó giải mã chữ kí  $S$  với khoá công khai của bên gửi thu được  $D'$ . So sánh  $D$  và  $D'$ , nếu phù hợp thì bản tin được chấp nhận, ngược lại, bỏ qua bản tin.

### 2.2.2. Chữ kí số ElGamal

Lược đồ kí số ElGamal gồm 3 phần khác nhau: Sinh khoá, kí và xác thực. Cả 3 phần đều sử dụng các thuật toán riêng. Trong lược đồ kí, có 4 hàm được sử dụng, trong đó có 1 hàm giống nhau ở cả quá trình kí và quá trình xác thực, nhưng khác nhau về dữ liệu đầu vào. Do vậy, tổng lại có 3 hàm khác nhau được sử dụng trong cả quá trình.

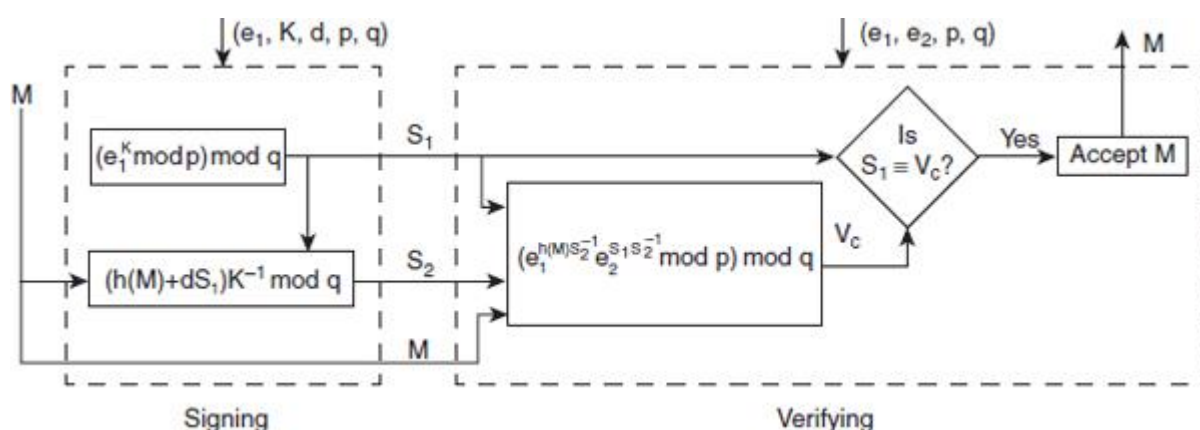


Hình 2.3 Giao thức chữ kí số ElGamal

Trong quá trình kí, F1 và F2 lần lượt được sử dụng để tạo 2 chữ kí S1 và S2 khác nhau. Bản tin M, S1, S2 được gửi tới người nhận. Bên nhận sau khi nhận được bản tin và chữ kí, sẽ tính 2 mã xác thực V1 và V2 sử dụng hàm F1 và F3. Sau đó, phía người nhận sẽ so sánh 2 mã V1 và V2, nếu phù hợp thì bản tin được chấp nhận, ngược lại sẽ từ chối.

### 2.2.3. Chữ kí số tiêu chuẩn (Digital Signature Standard - DSS)

DSS được công bố bởi National Institute of Standards and Technology (NIST) vào tháng 8/1991. DSS được chỉnh sửa lại năm 1993, và đến năm 2000, một phiên bản hoàn chỉnh của DSS đã ra đời. Chữ kí số sử dụng giải thuật băm an toàn (Secure Hash Algorithm - SHA) và đưa ra một lược đồ kí số mới là Digital Signature Algorithm (DSA).



Hình 2.4 Giao thức chữ kí số tiêu chuẩn

Giống như chữ kí ElGamal, cũng sử dụng 2 hàm F1 và F2 để lần lượt tạo 2 chữ kí khác nhau là S1 và S2. Tuy nhiên, khác ElGamal, DSS sử dụng chuỗi đại diện (Message Digest) để tạo chữ kí S2. Phía gửi truyền đi S1, S2 và M tới phía nhận. Sau khi nhận được bản tin, người nhận tính Message Digest sử dụng cùng hàm băm tương tự, và sử dụng hàm F3 để tính mã xác nhận  $V_c$ . So sánh  $V_c$  với S1, nếu phù hợp thì bản tin được chấp nhận, ngược lại thì từ chối bản tin.

Chữ kí DSS được cho là tốt hơn RSA và ElGamal vì so với RSA, việc tính toán DSS ít phức tạp hơn so với RSA với cùng giá trị  $p$ , còn so với ElGamal thì DSS cho chữ kí có kích thước nhỏ hơn ElGamal (vì  $q < p$ ).

## 2.3. Tính an toàn trong chữ kí số RSA

### 2.3.1. Ưu điểm chữ kí số RSA

Bên cạnh những ưu điểm của chữ kí số nói chung, chữ kí số RSA còn có một số ưu điểm sau:

- Không cần bộ sinh số ngẫu nhiên để tạo chữ kí như DSA hay ElGamal
- Có khả năng chống tấn công vét cạn bằng cách tăng độ lớn của  $p$  và  $q$  khi sinh khoá (tăng độ phức tạp giải mã)

- RSA có thể kí mà không cần phải mã hoá bản tin (sử dụng hàm băm)

### 2.3.2. Nhược điểm chữ kí số RSA

Đối với chữ kí số sử dụng thuật toán RSA có một số vấn đề cần quan tâm như sau:

**Chọn số nguyên tố lớn p, q:** các số nguyên tố bí mật này cần phải đủ lớn để bên tấn công không thể tìm ra trong thời gian đa thức. Bên cạnh đó, các số nguyên tố này cũng không được quá lớn, nhằm đảm bảo thời gian tính toán.

**Mối quan hệ nhân** (Multiplicative relationships): nếu độ dài mã hash đầu ra ngắn hơn số module thì hệ thống có khả năng bị tấn công bởi tính toán chỉ số (index calculus).

**Giả mạo chữ kí:** việc thực hiện thao tác (1) Kí trước, mã hoá sau hoặc (2) Mã hoá trước, kí sau có ảnh hưởng đến sự an toàn của chữ kí.

### 2.3.3. Các kịch bản tấn công và phòng thủ

- Tấn công dạng 1: Tìm cách xác định khoá bí mật

**Bị lộ một trong các giá trị như p, q,  $\Phi(n)$**

**Kịch bản tấn công:** Nếu trong quá trình lập khóa mà người sử dụng vô tình để lộ nhân tử p, q hoặc  $\Phi(n)$  ra ngoài thì kẻ tấn công sẽ dễ dàng tính được khóa bí mật e theo công thức:  $e * d \equiv 1 \pmod{\Phi(n)}$

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

**Kịch bản phòng thủ:** Quá trình tạo lập khóa phải được tiến hành ở một nơi kín đáo, bí mật. Sau khi thực hiện xong thì phải giữ cẩn thận khóa bí mật e, đồng thời hủy hết các giá trị trung gian p, q,  $\Phi(n)$ .

**Tấn công dựa theo khoá công khai n và d của người kí**

**Kịch bản tấn công:** Bên tấn công sẽ dựa theo giá trị n đã biết để khai thác ra hai thừa số nguyên tố p và q. Khi đó, dựa theo công thức:  $\Phi(n) = (p - 1)(q - 1)$ , ta tính được  $\Phi(n)$ . Cuối cùng, ta có thể tính được khóa bí mật e.

**Kịch bản phòng thủ:** Ta cần triển khai phòng chống như sau: Cần chọn p và q là hai số nguyên tố đủ lớn để việc khai thác ra hai số p và q là khó thực hiện trong thời gian thực. Trong thực tế, để đảm bảo việc này thì người ta thường sinh ngẫu nhiên các số ít nhất có 100 chữ số, từ đó kiểm tra tính nguyên tố của các số thu được và kiểm tra tính nguyên tố của nó.

**Sử dụng giá trị “modulo n” nhỏ**

**Kịch bản tấn công:** Trong sơ đồ chữ kí RSA thì công thức để tính giá trị chữ ký y trên bản rõ x như sau:  $y = x^e \pmod{n}$  với ( $y \in A$ ,  $x \in P$ ,  $P = A = \mathbb{Z}_n$ ) Lúc này, kẻ tấn công có thể tính được khóa bí mật a theo công thức sau: do các giá trị: x, y, n là công khai. Đây chính là việc giải bài toán logarit rời rạc trên vành. Bởi vậy, nếu như giá trị modulo

n mà nhỏ thì bằng cách áp dụng các thuật toán đã trình bày ở trên kẻ tấn công có thể tìm ra được khóa bí mật e.

**Kịch bản phòng thủ:** Nên chọn các số nguyên tố p và q đủ lớn để việc giải bài toán logarit rời rạc trên vành  $Z_n$  là khó có thể thực hiện được trong thời gian thực.

*Sử dụng các tham số (p-1) hoặc (q-1) có các ước nguyên tố nhỏ*

**Kịch bản tấn công:** Người sử dụng bất cẩn trong việc chọn các tham số p và q để cho (p-1) hoặc (q-1) có các ước nguyên tố nhỏ thì sơ đồ chữ ký sẽ trở nên mất an toàn. Bởi vì, khi (p-1) hoặc (q-1) có các ước nguyên tố nhỏ thì ta có thể dùng thuật toán (p-1) của Pollard để phân tích giá trị modulo n thành thừa số một cách dễ dàng.

**Kịch bản phòng thủ:** Chọn các tham số p và q sao cho (p - 1) và (q - 1) phải có các ước nguyên tố lớn.

- **Tấn công dạng 2: Giả mạo chữ ký**

Với việc tập trung vào giả mạo chữ ký, bên tấn công sẽ không thực hiện tính toán trực tiếp khoá bí mật. Người gửi gửi tài liệu x cùng chữ ký y đến người nhận, sẽ có hai cách để thực hiện: (1) Ký trước, mã hoá sau hoặc (2) Mã hoá trước, ký sau

**Kịch bản tấn công:** Bên tấn công lấy trộm được thông tin trên đường truyền từ người gửi đến người nhận.

+ Trong cách (1), bên tấn công lấy trộm, thu được thông tin Z.

+ Trong cách (2), bên tấn công lấy trộm, thu được thông tin (M', S).

Trong cả hai trường hợp, bên tấn công đều phải giải mã thông tin lấy được để có thể tấn công vào tài liệu. Tuy nhiên, nếu muốn tấn công vào chữ ký, có hai cách ứng với hai trường hợp (1) và (2):

+ Trong trường hợp (1), để tấn công vào chữ ký, bên tấn công phải giải mã Z để nhận được y.

+ Trong trường hợp thứ (2), do chữ ký không được mã hoá chung với văn bản, lúc này, bên tấn công chỉ việc thay chữ ký v bằng chữ ký v' có sẵn.

**Kịch bản phòng thủ:** Cần tiến hành ký trước rồi mã hoá sau như cách (1) để có thể đảm bảo an toàn cả cho chữ ký, giảm thiểu tối đa khả năng giả mạo.

### CHƯƠNG 3. CÁC DỊCH VỤ CHỮ KÝ SỐ

Thông số kỹ thuật của dịch vụ chữ ký số (Digital Signature Service – DSS) mô tả hai giao thức dựa trên XML là yêu cầu (request) và phản hồi (respond) – một là giao thức ký, một là giao thức xác nhận. Các giao thức này có thể hữu ích trong nhiều trường hợp, ví dụ như cho phép người dùng tạo và xác nhận chữ ký mà không cần cấu hình và phần mềm phức tạp.

Phần này sẽ liệt kê một số dịch vụ chữ ký số đang được sử dụng hiện tại.

### 3.1. Dịch vụ con dấu thời gian (Time-stamp)

Dịch vụ này được định nghĩa nhằm hỗ trợ việc tạo và xác minh dấu thời gian – chuỗi kí tự hoặc thông tin được mã hoá xác định khi có một sự kiện xảy ra.

### 3.2. Dịch vụ không đồng bộ (Asynchronous)

Đây là dịch vụ trừu tượng, dùng để định nghĩa cơ chế cho yêu cầu kí và xác minh không đồng bộ. Các dịch vụ kế thừa cho phép người dùng gửi yêu cầu mà server không phản hồi ngay lập tức. Thay vào đó, người dùng có thể thăm dò server cho đến khi phản hồi sẵn sàng.

### 3.3. Dịch vụ kí mã (Code-signing)

Kí mã kế thừa dịch vụ không đồng bộ, cho phép người dùng nhận được sự đảm bảo về nguồn gốc và tính toàn vẹn của chương trình phần mềm. Người dùng có thể sử dụng thông tin này để đưa ra quyết định tin cậy về việc cài đặt hoặc thực thi chương trình.

Việc sinh chữ kí được tập trung hoá trong quá trình kí mã phân chia vai trò của người phát triển phần mềm và người tạo mã. Điều này tạo thuận lợi cho việc quản lý khoá, kiểm soát truy cập khoá và các chính sách kí khoá được thực thi nghiêm ngặt

### 3.4. Dịch vụ kí mã J2ME

Kí mã J2ME kế thừa dịch vụ kí mã, được dùng cho việc yêu cầu sinh chữ kí trong J2ME và MIDP 2.0.

### 3.5. Niêm phong thực thể (Entity Seal)

Dịch vụ này hỗ trợ việc tạo và xác minh của một dấu niêm phong (seal) tạo bởi một thực thể hoặc tổ chức trên dữ liệu điện tử. Dấu này là một loại chữ kí điện tử:

- Dùng để bảo vệ tính toàn vẹn của tài liệu.
- Bao gồm thời điểm niêm phong chứng minh dữ liệu tồn tại tại thời điểm đó.
- Bao gồm danh tính của thực thể yêu cầu dấu niêm.

Con dấu này có thể bao gồm một thông báo về mục đích sử dụng.

### 3.6. Dấu bưu điện điện tử (Electronic Postmark – EPM)

Dấu bưu điện điện tử là một tiêu chuẩn được chứng thực bởi Liên minh bưu chính quốc tế nhằm cung cấp dịch vụ tạo chữ kí phổ thông, xác minh chữ kí, đánh dấu thời gian và dịch vụ biên nhận.

### 3.7. Dịch vụ Signature Gateway

Signature Gateway mô tả việc sử dụng DSS nhằm hỗ trợ chuyển đổi chữ kí, bao gồm cả công nghệ kí và quản lý chứng chỉ. Công nghệ kí (signing technology) là cơ chế tạo và xác minh chữ kí. Quản lý chứng chỉ mô tả cách thức phân phối chứng chỉ cho các bên từ xa; phương tiện liên quan cho sự tin cậy phân tán.

## CHƯƠNG 4. Chữ kí mù

### 4.1. Hoàn cảnh ra đời

Nhu cầu trao đổi thông tin ngày nay là một trong những nhu cầu thiết yếu của con người, đặc biệt trong bối cảnh Internet phát triển, trao đổi thông tin có thể được tiến hành từ xa. Tuy nhiên, tùy vào từng mục đích, nhu cầu, có những văn bản ta không muốn công khai cho một số người nhưng vẫn cần họ đảm bảo tính xác thực (ví dụ như phiếu bầu cử hay giao dịch ngân hàng, mô hình tiền điện tử). Khi đó, sử dụng chữ kí số đơn thuần không thể giải quyết được vấn đề trên. Điều này dẫn đến sự hình thành nên một chữ kí đặc biệt - chữ kí mù.

Năm 1983, trong bài báo Blind Signatures for Untraceable Payments (Chữ kí mù cho thanh toán không thể truy vết), chữ kí mù được Chaum giới thiệu với mục đích để tạo ra chữ kí trên một văn bản mà chính người kí cũng không biết nội dung - tuy nhiên vẫn tạo ra được chữ kí hợp lệ. Đặc trưng của chữ kí này là: Chỉ có duy nhất người chủ của chữ kí mới có khả năng tạo ra chữ kí hợp lệ cho một văn bản và chữ kí cho một văn bản đó có thể được kiểm tra tính đúng đắn bởi bất cứ ai.

### 4.2. Khái niệm

Theo khái niệm mà David Chaum đưa ra vào năm 1982, chữ kí mù được hiểu là một dạng chữ kí số mà trong đó thông điệp đã được mã hoá trước khi nó được kí. Do đó, người kí sẽ không thể đọc được nội dung của thông điệp mà mình đã kí. Sau đó, thông tin sẽ được giải mã và lúc này, chữ kí mù có thể coi như là một dạng chữ kí số thông thường và có thể được nó có thể được đối chiếu công khai với thông điệp gốc. Chữ kí mù thường được sử dụng trong các giao thức mang tính riêng tư khi mà người kí và chủ tin nhắn là các bên khác nhau.

Chữ kí mù cũng có thể được sử dụng để cung cấp khả năng không liên kết (unlinkability), ngăn người kí có thể liên kết thông điệp mù đã kí với phiên bản không bị mù cần xác minh sau đó bằng cách giữ lại bản ghi blog của thông điệp bị làm mù đã kí. Trong trường hợp này, người kí sẽ tiến hành xác thực theo cách mà chữ kí số duy trì tính hợp lệ cho các thông điệp không bị mù. Sau đó, dựa theo kết quả nhận được, người dùng sẽ có thể tiến hành loại bỏ tính mù để thu được thông điệp gốc với chữ kí xác thực.

### 4.3. Yêu cầu đối với chữ kí mù

Tính xác thực: Như một chữ kí số thông thường, chữ kí mù đòi hỏi tính xác thực. Nghĩa là:

- Những ai có khoá công khai của Dave đều có thể xác thực chữ kí của anh ta trong thông điệp, văn bản (document) là hợp lệ.
- Chữ kí của Dave không thể bị làm giả hoặc chuyển sang thông điệp, văn bản khác, đồng thời Dave cũng không thể phủ nhận được chữ kí của anh ta.

Tính không liên kết: Là đặc trưng của chữ kí mù. Yêu cầu này đòi hỏi Dave không thể liên hệ được thông điệp công khai đã được xoá mù với thông điệp mù mà anh ta đã kí.

#### 4.4. Mô hình chữ kí mù

Thành phần quan trọng nhất cho tính ẩn danh trong các hệ thống sử dụng chữ kí mù ngoại tuyến (ví dụ như trong các hệ thống tiền điện tử ngoại tuyến) là tính an toàn cho chữ kí mù. Chữ kí số được thiết kế tạo ra phiên bản mù dựa trên một sơ đồ gốc ứng với một hệ chữ kí số cơ bản nào đó với mục đích là sử dụng được loại chữ kí số đó cho văn bản mù. Thiết kế của một số lược đồ chữ kí cơ bản có thể được xác nhận bằng một bằng chứng trong mô hình được gọi là ngẫu nhiên, nhưng tính bảo mật của lược đồ chữ kí gốc không bao hàm sự bảo mật đối với phiên bản mù. Do đó, yêu cầu cần đặt ra là có thể có một mô hình, một ví dụ cụ thể có thể được chuyển đổi thành công trong sơ đồ chữ kí mù an toàn mà có thể chứng minh được. Sau đây, chúng em xin trình bày về một số mô hình đó.

##### 4.4.1. Dựa trên hệ RSA

- Các bước thực hiện:

+ Người nhận chữ kí: Tiến hành làm mù thông điệp  $M$  bằng phần tử "làm mù"  $p$  ngẫu nhiên được chọn. Tuy nhiên,  $p$  phải thoả mãn có thể tính được nghịch đảo của  $p$  khi mod  $N$  là duy nhất. Giá trị "mù" của  $M$  lúc này sẽ là:

$$M' = \text{blind}(M) = M \cdot p^b \pmod{N}.$$

Trong đó,  $M'$  là thông điệp "mù".

+ Người kí: Tạo chữ kí trên  $M'$  (hay chữ kí "mù" trên  $M$ )

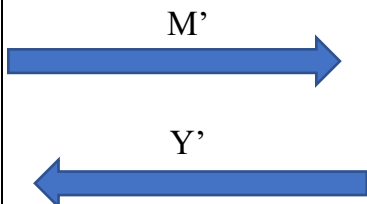
$$Y' = S(M') = (M \cdot p^b)^a \pmod{N} = M^a \cdot p^{ba} = M^a \cdot p \pmod{N}$$

Trong đó  $Y'$  là thông điệp mù đã có chữ kí.

+ Người nhận chữ kí: Xoá mù trên chữ kí  $Y'$  để nhận được chữ kí  $Y$  trên  $M$ :

$$Y = \text{unblind}(Y') = Y' / p \pmod{N} = M^a \pmod{N}$$

Trong đó,  $Y$  là thông điệp đã được xoá mù với chữ kí ở trên. Như vậy ở bước này, thông điệp đã được đính kèm chữ kí thành công.

Người nhận chữ kí	Thông điệp	Người kí
<ul style="list-style-type: none"> <li>- Chọn <math>p</math> ngẫu nhiên, <math>p \in \mathbb{Z}_q^*</math></li> <li>- Làm mù thông điệp được <math>M'</math></li> </ul>	 <p style="text-align: center;"><math>M'</math></p> <p style="text-align: center;"><math>Y'</math></p>	<ul style="list-style-type: none"> <li>- Tạo thông điệp với chữ kí là <math>Y'</math>.</li> </ul>
<ul style="list-style-type: none"> <li>- Xoá mù thông điệp, thu được thông điệp với chữ kí mù.</li> </ul>	$(M, Y)$	

##### 4.4.2. Dựa trên sơ đồ chữ kí Schnorr

- Các bước thực hiện:

Vòng 1: Người kí thực hiện.

+ Chọn ngẫu nhiên phần tử bí mật  $r' \in Z_q^*$ .

+ Tính  $t' = g^{r'} \pmod{N}$ , gửi  $t'$  cho người nhận chữ kí.

Vòng 2: Người nhận chữ kí thực hiện: Làm “mù” thông điệp cần kí.

+ Chọn ngẫu nhiên phần tử bí mật  $\gamma, \delta \in Z_q^*$ .

+ Tính  $t = t' \cdot g^\gamma \cdot h^\delta \pmod{N}$ ,  $c = H(m, t)$ .

+ Tính  $c' = c - \delta \pmod{q}$ . Gửi  $c'$  cho người kí.

Đến đây, thông điệp  $m$  đã được làm “mù”, người kí khó có thể nhận ra.

Vòng 3: Người kí thực hiện

+ Tính  $s' = r' - c' \cdot a \pmod{q}$ . Gửi  $s'$  cho người nhận.

Vòng 4: Người nhận chữ kí thực hiện: Xoá mù chữ kí.

+ Tính  $s = s' + \gamma \pmod{q}$  và  $c = H(m, t)$ . Chữ kí thu được là  $(c, s)$

### **Chú ý:**

- Người kí không biết  $c, s$ , vì chúng được làm mù bởi các tham số ngẫu nhiên  $\gamma, \delta$
- Chữ kí là hợp lệ vì:

$$g^s \cdot h^c = g^{s'+\gamma} \cdot h^{c'+\delta} = g^{r'-c' \cdot a + \gamma + c' \cdot a} \cdot h^\delta = t' \cdot g^\gamma \cdot h^\delta = t \pmod{N}$$

Như vậy:  $c = H(m, t) = H((m, g^s \cdot h^c))$ , thoả mãn điều kiện chữ kí Schnorr.

#### 4.4.3. Dựa trên bilinear pairing

- Người nhận chữ kí thực hiện: Chọn một số ngẫu nhiên  $r$  thuộc  $Z_q^*$ . Làm mù chữ kí tạo ra  $M' = r \cdot H_1(m)$ .
- Người kí thực hiện: Tính ra  $\sigma' = x \cdot M'$ .
- Người nhận chữ kí thực hiện: Tính  $\sigma = r^{-1} \cdot \sigma'$  và nhận được thông điệp có chữ kí là  $(m, \sigma)$ .

#### 4.5. Ứng dụng của chữ kí mù

##### 4.5.1. Tiền điện tử

Tiền điện tử có thể coi là một hình thức của tiền mặt trong môi trường thanh toán điện tử. Về bản chất chỉ là một chuỗi bit được ngân hàng phát hành. Khi cần người sử dụng sẽ đến ngân hàng để rút tiền điện tử này, ngân hàng sẽ tiến hành trừ tiền tài khoản đó và cung cấp chuỗi bit ứng với tiền điện tử người dùng rút. Lúc đến cửa hàng mua thứ gì, người sử dụng cũng có thể thanh toán bằng đồng tiền điện tử này. Cửa hàng chỉ chấp nhận đồng tiền con số này khi họ kiểm định thấy đúng là do ngân hàng tạo ra với chữ kí mà ngân hàng tạo ra trên đó. Cửa hàng sau đó sẽ gửi số tiền điện tử này về ngân hàng để chuyển vào tài khoản của họ. Tuy nhiên nếu tiền điện tử do chính ngân hàng



tạo ra và phát hành cho từng người sử dụng thì ngân hàng có thể tạo ra cơ sở dữ liệu để lưu trữ các thông tin cụ thể là phát đồng tiền số nào cho người sử dụng nào. Những thông tin này nếu có thể đem kết hợp với "sổ sách" của các cửa hàng thì hoàn toàn có thể truy ra được người sử dụng đã dùng đồng tiền đó để mua gì, nghĩa là đồng tiền không phải là vô danh như là tiền mặt thông thường (tất nhiên làm được điều này phải có sự "thông đồng" của hai bên là ngân hàng và bên bán hàng; điều này có thể xảy ra khi bên bán hàng là các siêu thị lớn, muốn tìm cách nắm được thói quen mua bán của từng người mua). Chính vì thế đồng tiền này phải được tạo ra trên cơ sở phối hợp của người rút tiền (withdrawer) và ngân hàng sao cho cuối cùng ngân hàng có kí lên mà không thể biết được đồng tiền - con số đó cụ thể là gì. Với tính "mù" sẵn có, rõ ràng đây chính là ứng dụng điển hình của chữ kí mù (blind signature).

#### 4.5.2. Bầu cử số (e-voting)

Tương tự như tiền điện tử, bầu cử số cũng là một ứng dụng dễ thấy của chữ kí mù với đòi hỏi cần bảo mật cho cử tri. Với việc người kí là cơ quan bầu cử, phiếu bầu của cử tri sẽ được kí mù bởi bên này để xác nhận tính hợp lệ cũng như tính toàn vẹn, đồng thời, cơ quan này cũng phải được đảm bảo là không tìm hiểu các lựa chọn của cử tri. Một chữ kí mù không liên kết (unlinkable) đảm bảo điều này vì cơ quan có thẩm quyền sẽ không nhìn thấy nội dung của bất kỳ lá phiếu nào mà nó kí và sẽ không thể liên kết các lá phiếu bị mù mà nó kí lại với các lá phiếu không bị mù mà nó nhận được để đếm. Sau đó được xoá mù để chuyển giao cho bên kiểm phiếu. Khi đó, bên kiểm phiếu sẽ đọc được kết quả nhưng không thể biết được ai là người đã làm phiếu bầu này, chỉ biết được đây là một phiếu bầu hợp lệ.

## CHƯƠNG 5. ỨNG DỤNG CHỮ KÍ SỐ

Khi có chữ kí số, quy trình tạo lập văn bản, in ra giấy rồi kí tên - đóng dấu sẽ mất dần để chuyển sang quy trình số hóa hoàn toàn.

Hiện nay, các giao dịch điện tử ngày càng trở nên phổ biến. Để bảo đảm an toàn cho các giao dịch này, cần phải sử dụng đến giải pháp chữ kí số. Chữ kí số được sử dụng để bảo đảm tính bảo mật, tính toàn vẹn, tính chống chối bỏ của các thông tin giao dịch trên mạng Internet. Chữ kí số tương đương với chữ kí tay nên có giá trị sử dụng trong các ứng dụng giao dịch điện tử với máy tính và mạng Internet cần tính pháp lý cao.

### 5.1. Giao dịch thương mại điện tử:

Trong môi trường số không thể dùng chữ kí tay nhưng lại có rất nhiều ứng dụng phải cần đến một cơ chế kí và xác thực người sử dụng như chữ kí tay. Các công nghệ mã hóa và chữ kí số ra đời để giúp giải quyết các trường hợp giao dịch cần đến chữ kí tay nhưng lại phải thực hiện trong môi trường số.

Hiện tại công nghệ chữ kí số tại Việt Nam có thể sử dụng trong các giao dịch để mua bán hàng trực tuyến, đầu tư chứng khoán trực tuyến, chuyển tiền ngân hàng, thanh toán trực tuyến.

Khóa bí mật được tạo ra khi một người đăng ký sử dụng dịch vụ và được lưu trữ trong một thiết bị phần cứng đặc biệt an toàn là Token hoặc SmartCard. Thiết bị này đảm bảo cho khóa bí mật được lưu trữ an toàn, không thể sao chép hay nhân bản được và cũng không thể bị virus phá hỏng.

Để có thể xác thực được ai là người tạo ra các chữ ký số khi nhận được các tài liệu điện tử có chữ ký số cần phải có một nhà cung cấp dịch vụ chứng thực đứng ra chứng nhận chữ ký đó là do một người cụ thể nào đó tạo ra. Tương tự khi tiến hành giao dịch điện tử công cộng như khai báo thuế, lập tờ khai hải quan, người sử dụng là cá nhân, cơ quan hay tổ chức phải sử dụng chữ ký số công cộng do nhà cung cấp dịch vụ chứng thực chữ ký số công cộng cấp. Hiện nay Việt Nam có 5 nhà cung cấp dịch vụ.

## 5.2. Kế khai thuế, nộp thuế trực tiếp qua mạng Internet.

Bộ Tài chính cũng đã áp dụng chữ ký số vào kê khai, nộp thuế trực tuyến qua mạng Internet và các thủ tục hải quan điện tử như khai báo hải quan và thông quan trực tuyến mà không phải in các tờ khai, đóng dấu đỏ của công ty và chạy đến cơ quan thuế xếp hàng và ngồi đợi vài tiếng đồng hồ, có khi đến cả ngày để nộp tờ khai này.

Để sử dụng chữ ký số cần phải đăng ký chứng thư số và tạo khóa bí mật lưu vào trong PKI Token với các nhà cung cấp dịch vụ chứng thực chữ ký số. Các chương trình ứng dụng phải hỗ trợ chức năng ký số, khi đó việc sử dụng khá đơn giản, người ký chỉ cần cắm thiết bị Token vào cổng USB, nhập PIN code bảo vệ Token và nhấp chuột vào nút lệnh ký số trong chương trình ứng dụng.

Chữ ký số không giống như chữ ký bình thường ở chỗ mỗi lần ký, người sử dụng sẽ dùng khóa bí mật để tạo chữ ký và mỗi lần ký sẽ là một chữ ký khác nhau. Dựa vào các công cụ phần mềm được cung cấp, các đối tác có thể kiểm tra chứng thư để xác định chữ ký. Cách kiểm tra là so sánh tính đồng nhất của khóa công khai trên các chữ ký số của người gửi với khóa công khai của Trung tâm Chứng thực chữ ký số quốc gia (Root Certification Authority – Root CA) thuộc Bộ Thông tin – Truyền thông.

## CHƯƠNG 6. TRIỂN KHAI CÀI ĐẶT

### 6.1. Các công cụ sử dụng và mã nguồn

Nhóm thực hiện mô phỏng quá trình gửi và nhận thông điệp đã được mã hoá, kết hợp chữ ký số nhằm xác thực thông điệp. Các công cụ và thư viện sử dụng bao gồm:

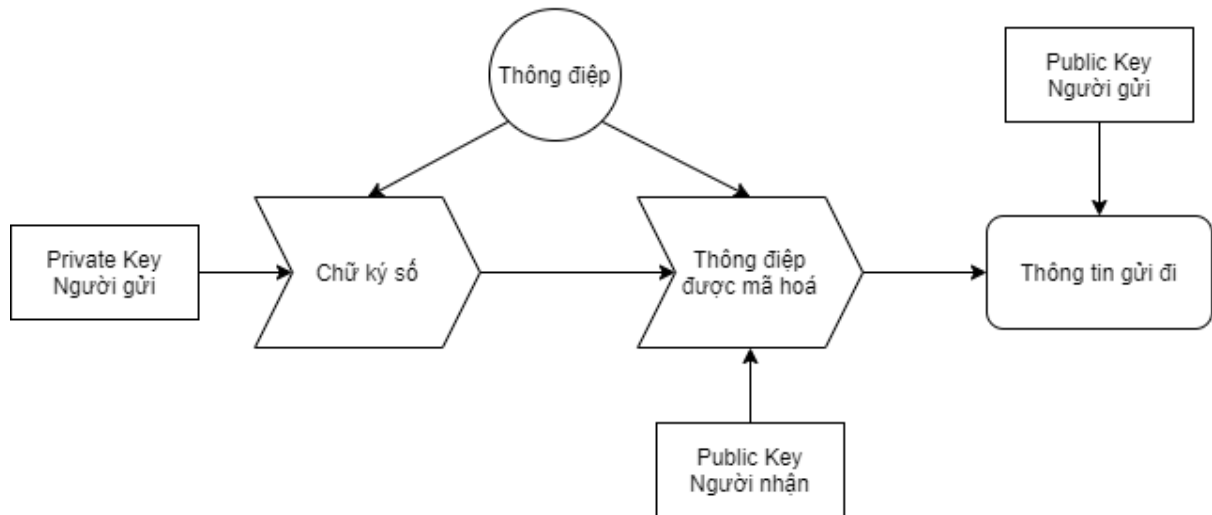
- Postman: công cụ mô phỏng quá trình gửi và nhận thông tin
- Hybrid Crypto Js: thư viện thực hiện các thao tác ký, mã hoá, giải mã và xác thực thông điệp
- ExpressJs: thực hiện HTTP request/response
- BodyParserJs: định dạng thông tin gửi đi trong HTTP request

Mã nguồn được lưu trữ trên [Github](https://github.com/tuanbmhust/nm-attt): <https://github.com/tuanbmhust/nm-attt>

### 6.2. Sơ đồ mô tả

### 6.2.1. Sơ đồ mã hoá thông điệp

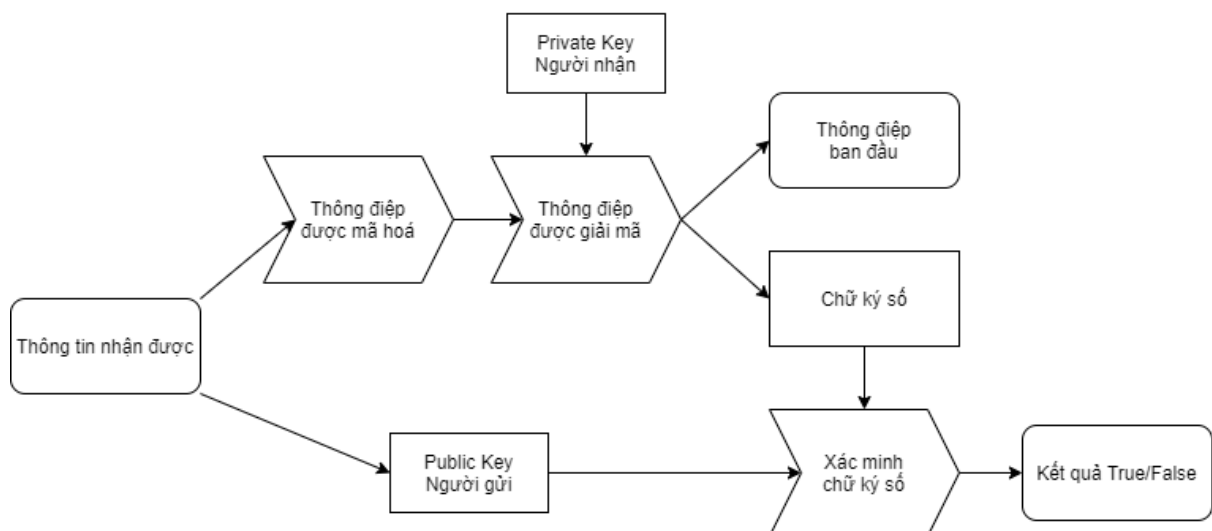
#### Sơ đồ mã hoá thông điệp



Hình 6.1 Sơ đồ mã hoá thông điệp

### 6.2.2. Sơ đồ giải mã thông điệp

#### Sơ đồ giải mã thông điệp



Hình 6.2 Sơ đồ giải mã thông điệp

## **TÀI LIỆU THAM KHẢO**

- [1] W. Stallings, Cryptography and Network Security Principles and Practice 5th Edition, 2011.
- [2] N. K. Văn, Cơ sở An toàn Thông tin, Đại học Bách Khoa Hà Nội, 2014.
- [3] Express Learning: Cryptography and Network Security, Pearson India, 2012.