TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN ĐIỆN TỬ - VIỄN THÔNG

LÍ THUYẾT MẬT MÃ

ĐỀ TÀI: ỨNG DỤNG CHỮ KÍ SỐ SỬ DỤNG HỆ MẬT RSA VÀO THU THUẾ

Nhóm thực hiện:

Nguyễn Nguyên Bách (20150239) – Điện tử 08 K60

Trương Công Chính (20130422) – KT ĐT-TT 08 K58

Mai Văn Hải (20141365) – Điện tử 03 K60

Nguyễn Minh Hiếu (20151336) – Điện tử 03 K60

Giảng viên hướng dẫn: TS. Hán Trọng Thanh

Hà Nội, tháng 5/2018

NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

LỜI MỞ ĐẦU

Ngành điện tử - viễn thông hiện nay là ngành mũi nhọn, được ứng dụng rộng rãi, đóng vai trò quan trọng trong sản xuất và đời sống. Với mục tiêu công nghiệp hóa, hiện đại hóa đất nước, các hệ thống máy móc ngày càng phải nhỏ gọn, tinh vi, hiệu năng tốt. Vì vậy, các ứng dụng công nghệ kỹ thuật điện tử ngày càng được mở rộng, là một phần không thể thiếu trong nền công nghiệp hiện đại.

Bản thân chúng em là sinh viên ngành điện tử - viễn thông, cần nâng cao trình độ, khả năng thực hành và ứng dụng kiến thức đã học vào thực tế. Học phần Lí thuyết mật mã đã giúp chúng em làm quen với lĩnh vực bảo mật và tìm hiểu một số ứng dụng của mật mã trong cuộc sống như bảo mật emai, tin nhắn sms, bảo mật trong ngân hàng quan đội, thông tin vệ tinh,…

Với vốn kiến thức học được trên giảng đường và tài liệu trên mạng, nhóm chúng em quyết định đưa ra đề tài "ứng dụng chữ kí số sử dụng hệ mật RSA vào thu thuế".

Mục tiêu của đề tài là bước đầu giúp nhóm làm quen với hệ mật RSA và chữ kí số, cải thiện kĩ năng lập trình và biến kiến thức thành thực tế qua phần mềm. Trong quá trình thực hiện khó tránh khỏi những sai sót nhất định, rất mong nhận được những ý kiến đóng góp từ thầy giáo cũng như các bạn để nhóm rút kinh nghiệm, giúp các lần làm đề tài sau được hoàn thiện hơn.

Chúng em xin cảm ơn Ban lãnh đạo Viện Điện tử - Viễn thông và thầy Hán Trọng Thanh đã tạo điều kiện và hướng dẫn tận tình giúp nhóm chúng em hoàn thành đề tài này.

Tóm tắt đề tài

Đề tài của nhóm là ứng dụng chữ kí số sử dụng hệ mật RSA vào thu thuế. Phần mềm được viết bằng ngôn ngữ C# và chạy bằng trình biên dịch Visual Studio trên nền Windows.

Summary of project

Our subject is application of digital signature using RSA cryptosystems in tax collection. Our software was written by programming language C# and run by the Visual Studio compiler on Windows.

MỤC LỤC

DANH MỤC HÌNH VẼ

Chương 1. Tổng quan về chữ kí số và ứng dụng

1.1 Giới thiệu chữ kí số

Chữ kí (viết tay) được sử dụng phổ biến trong các giao dịch hang ngày, như hợp đồng, giấy tờ mua bán, đơn từ, chuyển nhượng,.. như là một hình thức xác nhận bản quyền của người kí về nội dung văn bản được kí. Tuy nhiên, chữ kí viết tay tồn tại một số nhược điểm:

- Có thể bị giả mạo chữ kí.
- Trong thời đại máy tính điện tử ngày nay thì việc sử dụng chữ kí viết tay gặp một số vấn đề như: thông tin trên máy tính có thể bị thay đổi, việc thay đổi chữ kí không để lại dấu vết gì như tẩy, xóa với chữ kí viết tay, hình ảnh chữ kí có thể truyền từ máy này sang máy khác, …

⇨ Khái niệm chữ kí điện tử ra đời, là thông tin đi kèm dữ liệu nhằm xác định người chủ của dữ liệu đó, và chữ kí số là một tập con của chữ kí điện tử.

Từ đây ta có một số khái niệm về chữ kí số:

- 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 ký 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) bao gồm:
- Giải thuật kiểm tra chữ ký số.
- Phương pháp khôi phục dữ liệu từ thông điệp.

Chữ kí số bản chất là một thông điệp dữ liệu, dựa trên lí thuyết về mật mã hóa bất đối xứng, sử dụng các hệ mật hiện đại. Việc thừa nhận chữ kí số thuộc sở hữu của cơ quan, cá nhân nào đó phải được một cơ quan công an chức thực và cơ quan này phải được thừa nhận về tính pháp lí và kĩ thuật.

Con người đã sử dụng các hợp đồng dưới dạng điện tử từ hơn 100 năm nay với việc sử dụng mã Morse và điện tín. Tuy nhiên, chỉ với những phát triển của khoa học kỹ thuật gần đây thì chữ ký điện tử mới đi vào cuộc sống một cách rộng rãi.

1.2 Các ưu và nhược điểm của chữ kí số

Chữ kí số có một số ưu điểm như:

- Tính bảo mật: Đảm bảo dữ liệu được truyền đi một cách an toàn, không bị lộ nếu ai đó cố tình muốn có thông điệp gốc ban đầu. Chỉ những người được phép mới có khả năng đọc được nội dung đó.
- Tính xác thực: Giúp người nhận xác định được chắc chắn thông điệp mà họ hận là thông điệp gốc ban đầu. Người giả mạo không thể mạo danh để gửi thông đi. 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 ký số thì văn bản cần phải được mã hóa bằng hàm băm (văn bản được "băm" ra thành chuỗi, thường có độ dài cố định và ngắn hơn văn bản) sau đó dùng khóa bí mật của người chủ khóa để mã hóa, khi đó ta được chữ ký số. Khi cần kiểm tra, bên nhận giải mã (với khóa công khai) để lấy lại chuỗi gốc (được sinh ra qua hàm băm ban đầu) và kiểm tra với hàm băm của văn bản nhận được. Nếu 2 giá trị (chuỗi) này khớp nhau thì bên nhận có thể tin tưởng rằng văn bản xuất phát từ người sở hữu khóa bí mật. Tất nhiên là chúng ta không thể đảm bảo 100% là văn bản không bị giả mạo vì hệ

thống vẫn có thể bị phá vỡ. Vấn đề xác thực đặc biệt quan trọng đối với các giao dịch tài chính.

- Tính toàn vẹn: Người nhận có thể kiểm tra thông điệp không bị thay đổi trong quá trình truyền. Người giả mạo không thể thay thế dữ liệu ban đầu bằng dữ liệu giả mạo. 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 tức bị phát hiện. Quá trình mã hóa sẽ ẩn nội dung của gói tin đối với bên thứ 3 nhưng không ngăn cản được việc thay đổi nội dung của nó.
- Tính không thể chối bỏ: Người gửi và nhận không thể chối bỏ sau khi đã gửi và nhận thông điệp. 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 ký số với văn bản. Khi có tranh chấp, bên nhận sẽ dùng chữ ký này như một chứng cứ để bên thứ ba giải quyết. Tuy nhiên, khóa bí mật vẫn có thể bị lộ và tính không thể phủ nhận cũng không thể đạt được hoàn toàn.

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. Đây là hạn chế chung khi sử dụng văn bản điện tử và chữ ký số.
- 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, 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 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 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.
- 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.

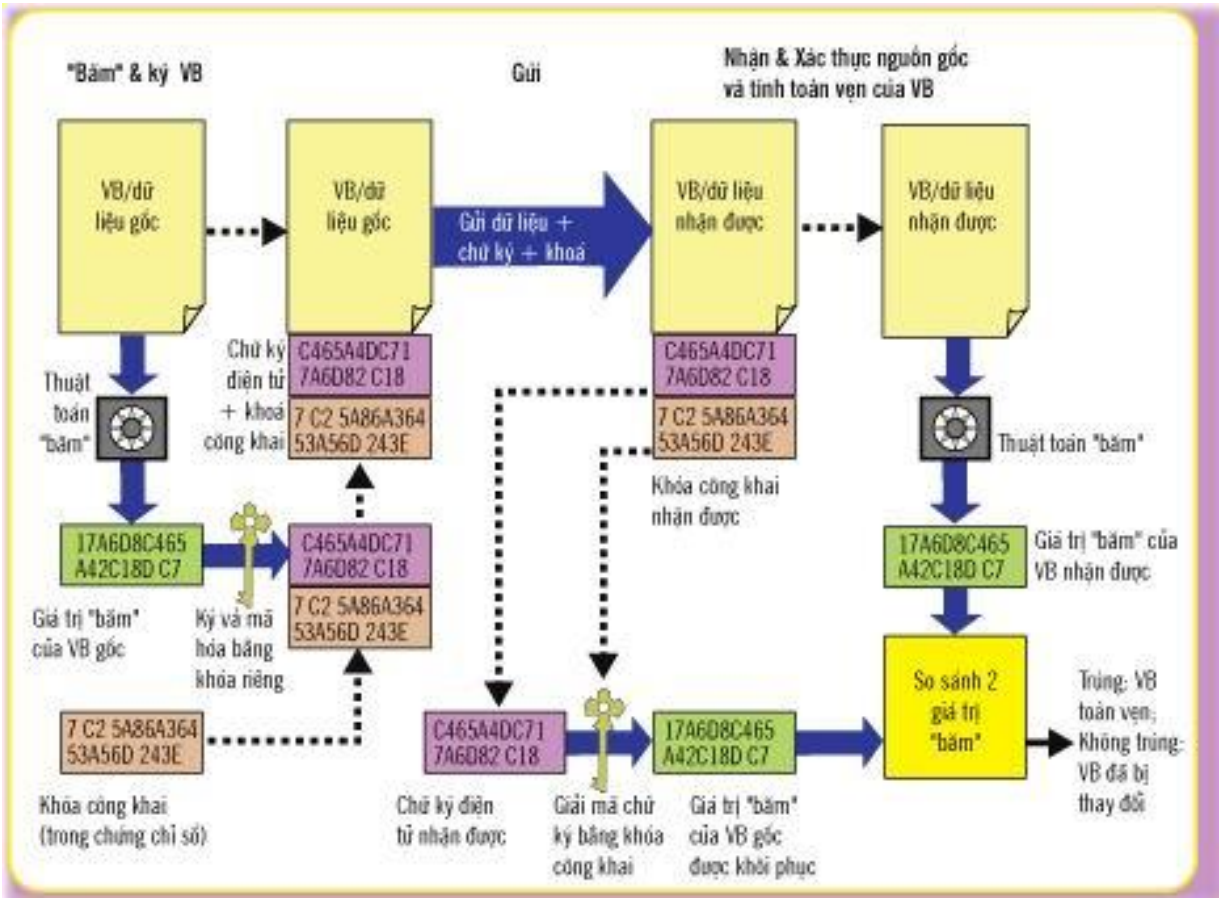
1.3 Ứng dụng của chữ kí số

Hiện nay, chữ ký số có rất nhiều ứng dụng trong thực tế như:

- Cam kết gửi bằng email. xác thực email trong đổi thông tin trong doanh nghiệp và giữa các doanh nghiệp với nhau.
- Sử dụng trong thương mại điện tử, đặt hàng online.
- Kiểm soát trong ngân hàng điện tử, thanh toán điện tử (mã PIN trong thanh toán bằng ATM, mã OTP).
- Ứng dụng trong đầu tư chứng khoán, giao dịch điện tử, ký hợp đồng.
- Nộp thuế trực tuyến, kê khai hải quan, thông quan trực tuyến, bảo hiểm xã hội điện tử.
- …

1.4 Sơ đồ chung của chữ kí số

Sơ đồ chung của chữ kí số được thể hiện ở hình 1.1.



Hình 1.1 Sơ đồ chung của chữ kí số

Trong sơ đồ trên, hàm băm (Hash Funtion) làm 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.

Người gửi đăng ký một chứng chỉ số với cơ quan có thẩm quyền,người gửi được cấp một khóa riêng (khóa bí mật). Trước khi gửi văn bản, người gửi áp dụng một thuật toán phần mềm để nhận giá trị băm của văn bản gốc. Sau đó người gửi mã hóa giá trị

băm bằng khóa riêng (ký lên giá trị băm), thu được chữ ký số. Văn bản gốc được gửi đi cùng với chữ ký số và khóa công khai của người gửi đến người nhận

Người nhận sau khi nhận thư sẽ sử dụng khóa công khai giải mã chữ ký số để biết người gửi, đồng thời thu được giá trị băm của văn bản gốc. Người nhận cũng dùng thuật toán băm để thu được giá trị băm của văn bản nhận được. Sau khi so sánh 2 giá trị hàm băm, người nhận xác nhận được chữ kí của người gửi và tính toàn vẹn của dữ liệu.

Chương 2. Hệ mật RSA

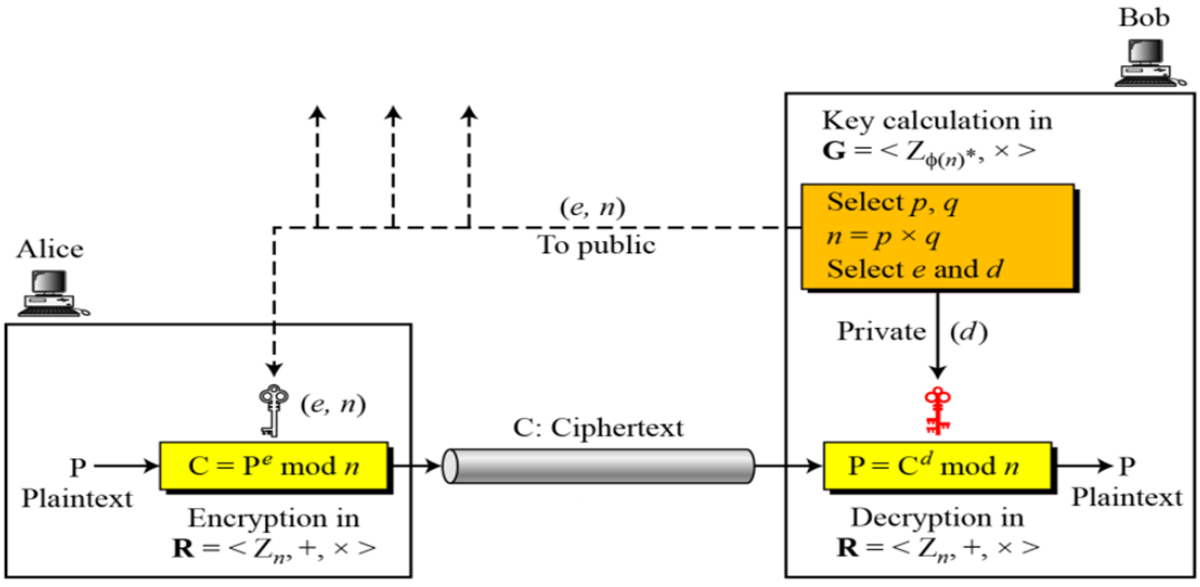
2.1 Giới thiệu hệ mật RSA

RSA là một thuật toán mật mã hóa khóa công khai, là thuật toán đầu tiên phù hợp với việc tạo ra chữ ký điện tử đồng thời với việc mã hóa, đánh dấu một sự tiến bộ vượt bậc của lĩnh vực mật mã. 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. RSA là một hệ mật hiện đại, tên được lấy từ 3 tác giả Ron Rivest, Adi Shamir và Len Adleman công bố lần đầu năm 1977 tại Viện Công nghệ Massachusetts (MIT).

RSA hoạt động trên cơ chế sử dụng 2 khóa: khóa công khai và khóa bí mật. Khóa công khai được công khai cho mọi người biết, sử dụng trong quá trình mã hóa. Tuy nhiên tất cả các thông tin mã hóa bằng khóa công khai chỉ có thể giải mã bằng khóa bí mật tương ứng với khóa công khai đó. Như vậy, mọi người đều có thể sử dụng khóa công khai để mã hóa dữ liệu nhưng chỉ có người giữ khóa bí mật mới có thể giải mã

2.2 Thuật toán hoạt động hệ mật RSA

Sơ đồ thuật toán hệ mật RSA được thể hiện ở hình 2.1.



Hình 2.1 Sơ đồ thuật toán hệ mật RSA

Các bước thực hiện thuật toán mã hóa như sau:

- Chọn 2 số nguyên tố p,q đủ lớn (thường được chọn bằng phương pháp thử xác suất)
- Tính n=p*q
- Tính giá trị ham Euler Φ(n)= Φ(p)* Φ(q)=(p-1)*(q-1)
- Chọn 1 số tự nhiên e (1<e< Φ(n)) sao cho e và Φ(n) là 2 số nguyên tố cùng nhau (gcd(e, Φ(n))=1)
- Tính d=e^{-1} mod Φ(n)

Ta có khóa công khai là e và n, khóa bí mật là d.

Giả sử m là kí tự ở bản rõ, c là kí tự bản mã hóa. c được tính theo công thức:

$$c=m^e(\text{mod } n)$$

Hàm trên có thể tính sử dụng phương pháp tính hàm mũ (theo môđun) bằng thuật toán bình phương và nhân

Quá trình giải mã được thực hiện như sau:

Người nhận nhận được c và biết khóa bí mật d thì có thể tìm được m bằng công thức:

$$m=c^d(\text{mod } n)$$

2.3 Các dạng tấn công hệ mật RSA

2.3.1 Tấn công lặp

Simon và Norris đã chỉ ra rằng hệ thống RSA có thể bị tấn công khi sử dụng tấn công lặp. Đó là khi kẻ tấn công biết khóa công khai (e,n) và bản mã c thì có thể tính chuỗi:

$$c_1=c^e(\text{mod } n),\ c_2={c_1}^e(\text{mod } n),\ldots\ c_i={c_{i-1}}^e(\text{mod } n),\ldots$$

Nếu có một phần tử c_i trong chuỗi sao cho c_i= c thì sẽ tìm được m=c_{i-1} vì:

$$c_i={c_{i-1}}^e=c,\ \text{mà } c=m^e\ (\text{mod } n)\ \text{nên } m=c_{i-1}$$

2.3.2 Tấn công module n dùng chung

Simon và Norris cũng chỉ ra hệ thống RSA có thể bị tấn công khi dùng module n dùng chung. Nếu m được mã hóa bằng 2 khóa công khai e_1 và e_2 từ 2 thành viên trong hệ thống thì ta có:

$$c_1=m^{e_1},\ c_2=m^{e_2}$$

Sau đó kẻ tấn công dùng thuật toán Euclid mở rộng tìm a, b sao cho

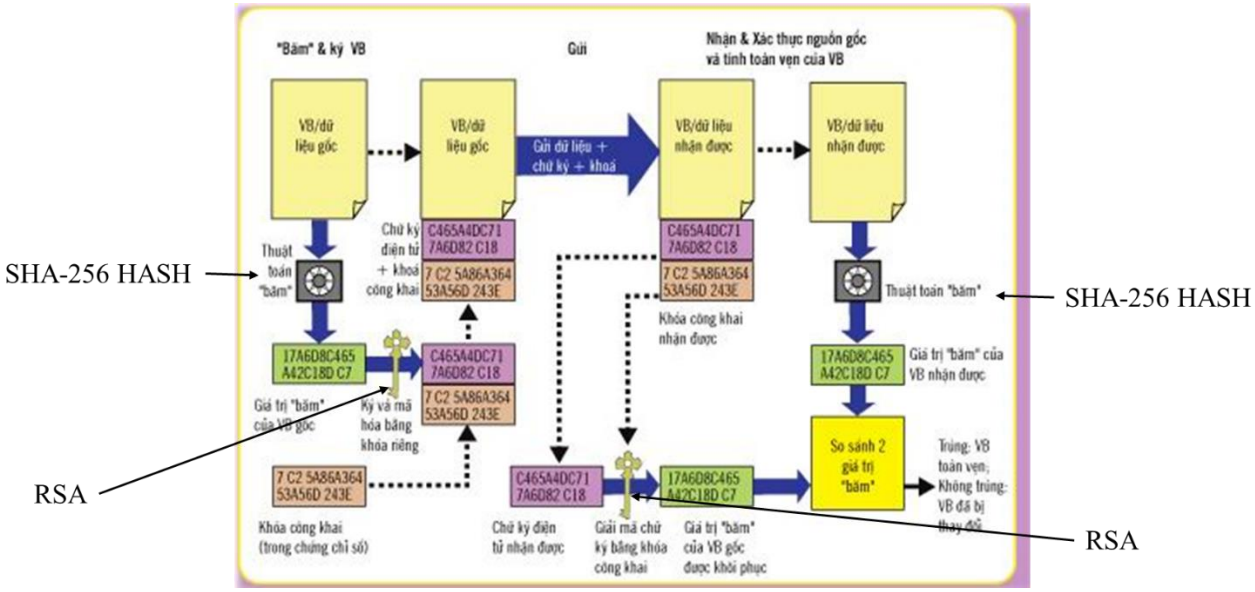
$$a.e_1+ b.e_2,\ \gcd(a,b)=1\ \text{thì}\ m={c_1}^a.{c_2}^b$$

2.3.3 Tấn công dựa trên thời gian

Vào năm 1995, Paul Kocher mô tả một dạng tấn công mới lên RSA: nếu kẻ tấn công nắm đủ thông tin về phần cứng thực hiện mã hóa và xác định được thời gian giải mã đối với một số bản mã lựa chọn thì có thể nhanh chóng tìm ra khóa d. Dạng tấn công này có thể áp dụng đối với hệ thống chữ ký điện tử sử dụng RSA. Năm 2003, Dan Boneh và David Brumley chứng minh một dạng tấn công thực tế hơn: phân tích thừa số RSA dùng mạng máy tính (Máy chủ web dùng SSL). Tấn công đã khai thác thông tin rò rỉ của việc tối ưu hóa định lý số dư Trung quốc mà nhiều ứng dụng đã thực hiện.

2.4 Chữ kí số sử dụng hệ mật RSA

Sơ đồ chữ kí số sử dụng hệ mật RSA được thể hiện ở hình 2.2.



Hình 2.2 Sơ đồ chữ kí số sử dụng hệ mật RSA

Sử dụng sơ đồ chữ kí số ở phần trước, với một số đặc điểm

- Hàm băm là SHA-256 HASH.
- Hệ mật là RSA.

SHA (Secure Hash Algorithm) là 5 giải thuật được chấp nhận bởi FIPS dùng để chuyển một đoạn dữ liệu nhất định thành một đoạn dữ liệu có chiều dài không đổi với xác suất khác biệt cao. SHA an toàn vì 2 lí do chính:

- Cho một giá trị băm nhất định được tạo nên bởi một trong những thuật giải SHA, việc tìm lại được đoạn dữ liệu gốc là không khả thi.
- Việc tìm được hai đoạn dữ liệu khác nhau có cùng kết quả băm tạo ra bởi một trong những thuật giải SHA là không khả thi. Bất cứ thay đổi nào trên đoạn dữ liệu gốc cũng sẽ tạo nên một giá trị băm hoàn toàn khác với xác suất rất cao.

5 giải thuật SHA là SHA-1 (trả lại kết quả 160 bit), SHA-224 (trả lại kết quả 224 bit), SHA-256 (trả lại kết quả 256 bit), SHA-384 (trả lại kết quả 384 bit), và SHA-512

(trả lại kết quả 512 bit). Thuật giải SHA là thuật giải băm mật được phát triển bởi cục an ninh quốc gia Mĩ (NSA) và được xuất bản thành chuẩn của chính phủ Mĩ bởi viện công nghệ và chuẩn quốc gia Mĩ (NIST). 4 giải thuật sau thường được gọi chung là SHA-2. Sơ lược về 5 giải thuật được thể hiện ở hình 2.3.

Thuật toán	Kích thước (đơn vị: bit)				Độ an toàn[2] (đơn vị: bit)
	Thông điệp	Khối	Từ	Thông điệp rút gọn	
SHA-1	$< 2^{64}$	512	32	160	80
SHA-224	$< 2^{64}$	512	32	224	112
SHA-256	$< 2^{64}$	512	32	256	128
SHA-384	$< 2^{128}$	1024	64	384	192
SHA-512	$< 2^{128}$	1024	64	512	256

Hình 2.3 Sơ lược về 5 giải thuật SHA

SHA có một số ứng dụng như:

- Sử dụng 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 dữ liệu và xác thực nguồn gốc dữ liệu. 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.

- SHA-1 thuật toán băm an toàn theo yêu cầu của pháp luật để sử dụng trong Chính Phủ Mỹ, bao gồm cả sử dụng trong các thuật toán mã hóa khác và ác giao thức, để bảo vệ thông tin mật nhạy cảm. Nhưng hiện nay thì Chính Phủ không còn sử dụng SHA-1 nữa mà thay vào đó là SHA-2, vì SHA-1 không còn được coi là an toàn bởi đầu năm 2005, ba nhà mật mã học người Trung Quốc đã phát triển thành công một thuật giải dùng để tìm được hai đoạn dữ liệu nhất định có cùng kết quả băm tạo ra bởi SHA-1. Còn với SHA-2 thì chưa thể làm điều tương tự.

SHA-256 là 1 trong 4 giải thuật SHA-2, được công bố năm 2001 trong bản thảo FIPS PUB 180-2.

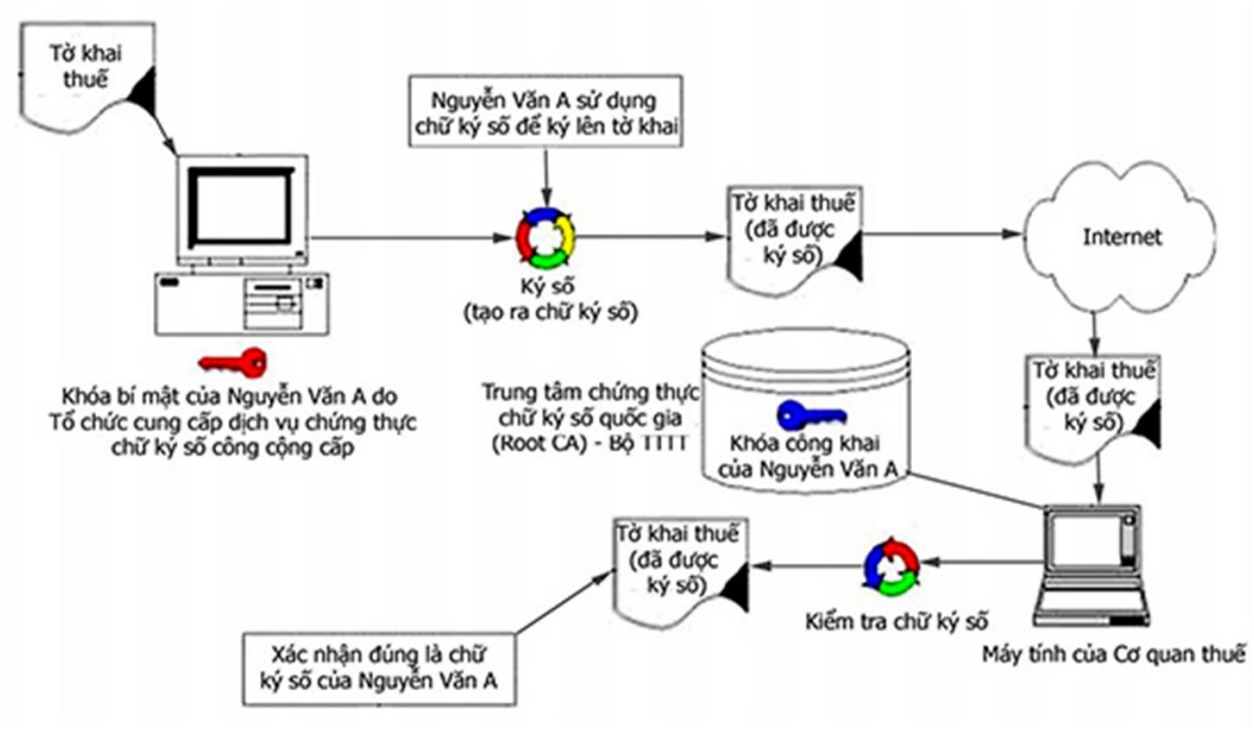
2.5 Đánh giá hệ mật RSA

- 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). Vì vậy, RSA không được dùng để mã hóa khối lượng dữ liệu lớn mà thường dùng để mã hóa dữ liệu nhỏ.
- 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.
- Việc chọn p và q còn cần được chọn không quá gần nhau để phòng trường hợp phân tích n bằng phương pháp phân tích Fermat. Ngoài ra, nếu p-1 hoặc q-1 có thừa số nguyên tố nhỏ thì n cũng có thể dễ dàng bị phân tích và vì thế p và q cũng cần được thử để tránh khả năng này. Thêm nữa, khóa bí mật d phải đủ lớn. Năm 1990, Wiener chỉ ra rằng nếu giá trị của p nằm trong khoảng q và 2q (khá phổ biến) và d $< \frac{n^{\frac{1}{4}}}{3}$ thì có thể tìm ra được d từ n và e. Mặc dù e đã từng có giá trị là 3 nhưng hiện nay các số mũ nhỏ không còn được sử dụng do có thể tạo nên những lỗ hổng (đã đề cập ở phần chuyển đổi văn bản rõ). Giá trị thường dùng hiện nay là 65537 vì được xem là đủ lớn và cũng không quá lớn ảnh hưởng tới việc thực hiện hàm mũ.

Chương 3. Ứng dụng thu thuế bằng chữ kí số

3.1 Sơ đồ thu thuế bằng chữ kí số

Sơ đồ thu thuế bằng chữ kí số được thể hiện ở hình 3.1.



Hình 3.1 Sơ đồ thu thuế bằng chữ kí số

Giả sử Nguyễn Văn A là người đi nộp thuế sử dụng chữ kí số. Nguyễn Văn A sử dụng khóa bí mật do trung tâm chứng thực chữ kí số quốc gia cấp để kí lên tờ khai thuế. Sau đó tờ khai thuế được gửi đến máy tính của cơ quan thuế.

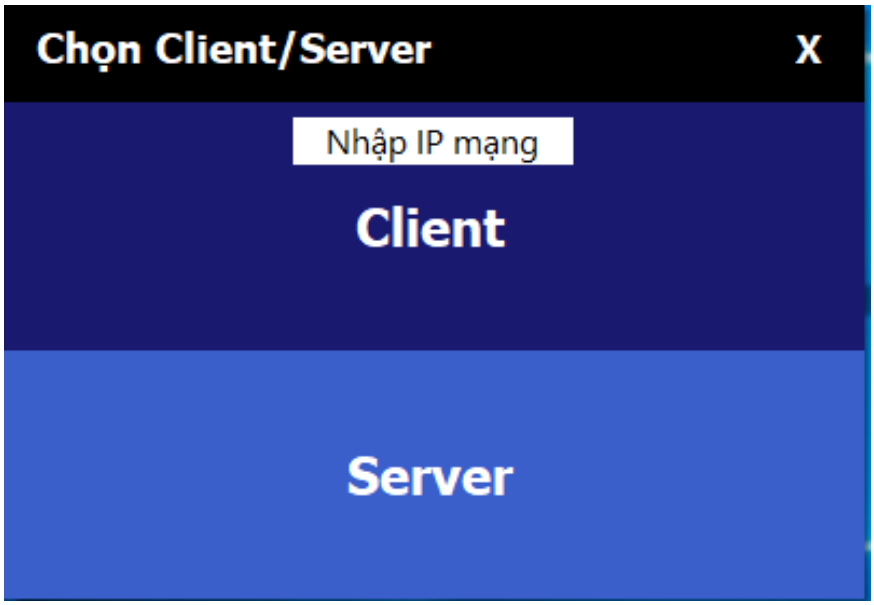
Cơ quan thuế sử dụng khóa công khai của trung tâm chứng thực chữ kí số quốc gia để kiểm tra chữ kí số, xác nhận xem chữ kí số đúng của Nguyễn Văn A không.

3.2 Phần mềm mô phỏng

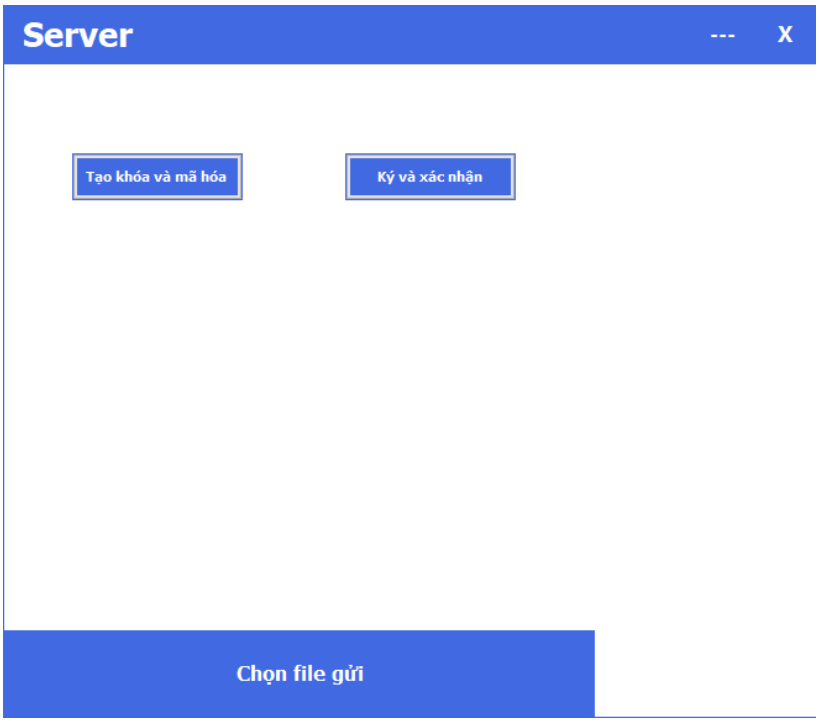
Phần mềm gồm có 3 phần chính:

- Phần gửi file giữu server và client
- Phần tạo khóa và mã hóa thử
- Phần tạo chữ kí và kiểm tra chữ kí

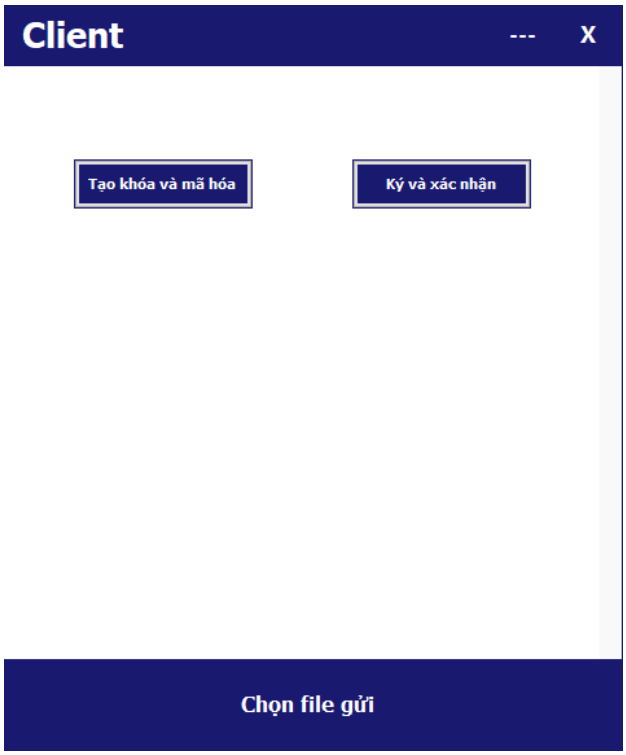
Phần mềm có chú thích đi kèm code và hướng dẫn cụ thể sử dụng phần mềm có trong file hướng dẫn.docx đi kèm. Hình ảnh giao diện phần mềm được thể hiện ở các hình từ 3.2 đến 3.6.



Hình 3.2 Giao diện phần chọn client/server



Hình 3.3 Giao diện server



Hình 3.4 Giao diện client

Hình 3.5 Giao diện tạo khóa và mã hóa

Hình 3.6 Giao diện ký và xác nhận

KẾT LUẬN

Trong đề tài này, nhóm đã kiểm tra sự hoạt động của hệ mật RSA trong ứng dụng vào chữ kí số, phần mềm đã hoạt động bình thường dù còn một số lỗi nhỏ. Phần mềm hiện tại còn đơn giản, nhóm đưa ra hướng phát triển trong tương lai cho đề tài:

- Sửa các lỗi nhỏ, cải thiện hiệu năng phần mềm.
- Làm đẹp giao diện, dễ sử dụng hơn cho người dùng.
- Cố gắng ứng dụng thu thuế qua web.

Một lần nữa, nhóm xin cảm ơn thầy Hán Trọng Thanh đã giảng dạy và giúp chúng em hiểu rõ hơn về ngành mật mã – ngành học còn mới và chưa phổ biến trong chương trình đào tạo Điện tử - Viễn thông của trường.

TÀI LIỆU THAM KHẢO

Nhóm sử dụng tài liệu tham khảo ở một số nguồn sau:

[1] https://en.wikipedia.org/wiki/RSA_(cryptosystem)

[2] https://en.wikipedia.org/wiki/Digital_signature

[3] https://chukysovnpt-ca.com/gioi-thieu-ve-chu-ky-so

[4] https://en.wikipedia.org/wiki/Secure_Hash_Algorithms