BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC QUẢN LÝ VÀ CÔNG NGHỆ HẢI PHÒNG

ĐỒ ÁN TỐT NGHIỆP

NGÀNH : CÔNG NGHỆ THÔNG TIN

Sinh viên : Trần Đức Tường

Giảng viên hướng dẫn: Hồ Văn Canh

HẢI PHÒNG – 2021

BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC QUẢN LÝ VÀ CÔNG NGHỆ HẢI PHÒNG

TÌM HIỂU VỀ VAI TRÒ CỦA CHUẨN CHỮ KÝ SỐ TRONG DỊCH VỤ HÀNH CHÍNH ĐIỆN TỬ

ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC HỆ CHÍNH QUY

NGÀNH: CÔNG NGHỆ THÔNG TIN

Sinh viên : Trần Đức Tường

Giảng viên hướng dẫn: Hồ Văn Canh

HẢI PHÒNG – 2021

BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC QUẢN LÝ VÀ CÔNG NGHỆ HẢI PHÒNG

NHIỆM VỤ ĐỀ TÀI TỐT NGHIỆP

Sinh viên: Trần Hải Đăng **Mã SV**: 1712101001

Lớp : CT2101C

Ngành : Công nghệ thông tin

Tên đề tài: Tìm hiểu về vai trò của chuẩn chữ ký số trong dịch vụ hành chính điện tử.

MỤC LỤC

DANH MỤC CÁC HÌNH ẢNH

CÁC CHỮ VIẾT TẮT

B

B2B	Business to Business – Doanh nghiệp với Doanh nghiệp
B2C	Business to Customer – Doanh nghiếp với khách hàng.

C

CA	Certificate Authority – Cơ quan chứng thực
CBC	Cipher Block Chaining - Xích khối bản mã.
CERT	Computer Emergency Response Team - Đội phản ứng khẩn cấp máy tính.
CFB	Cipher FeedBack - Phản hồi bản mã.

D

DES	Data Encryption Standard - Chuẩn mã hóa dữ liệu.
DS	Digital Signature – Ký số.
DSA	Digital Signature Algorithm - Thuật toán ký số
DSS	Digital Signature Standard - Chuẩn chữ ký số

E

EDI	Electric Data Interchange -Trao đổi dữ liệu điện tử
EPO	Electronic Payment Order – Thứ tự thanh toán điện tử.

F

FIPS	U.S. Federal Information Processing Standard- Tiêu chuẩn xử lý thông tin của Mỹ

G

GCD	Greatest Common Divisor - Ước số chung lớn nhất

I

IP Internet Protocol - Giao thức internet

ISP Internet Service Provider - Nhà cung cấp dịch vụ internet

J

JCA Java Cryptography Architecture – Kiến trúc mật mã Java

JCE Java Cryptography Extension – Mở rộng mật mã Java.

M

MD Message Digest - số hóa thông điệp

N

NIC New Industrial Country- Nước có nền công nghiệp mới nổi.

P

PK Public Key- khóa công khai.

PKC Public Key Cryptography - Mật mã khóa công khai.

Pký Public Key Infrastructure - Cơ sở hạ tầng khóa công khai

R

RSA Rivest, Shamir and Adleman

S

SET Secure Electronic Transmission – Truyền tải điện tử an toàn.

SHA Secure Hash Algorithm – Thuật toán băm an toàn.

SHS Secure Hash Standard – Tiêu chuẩn hàm băm an toàn.

SSL Secure Sockets Layer - Bảo mật lớp gói an toàn

T

TCP/IP	Transmission Control Protocol/Internet Protocol – Giao thức điều khiển tuyền tin / Giao thức internet.
TTP	Trusted Third Party – Chứng thực bên thứ 3 tin cậy.
X	
X.509	Chuẩn chứng chỉ số X.509

LỜI GIỚI THIỆU

Trong những năm gần đây, sự phát triển của mạng thông tin toàn cầu đã có ảnh hưởng sâu sắc tới mọi mặt của đời sống kinh tế, xã hội. Internet trở thành mạng truyền dữ liệu được sử dụng phổ biến trên toàn thế giới. Nó được dùng để truyền thư điện tử, truy nhập các Website, kết nối tới các công sở ở xa, giám sát hệ thống từ xa, truyền tệp, làm việc tại nhà, liên lạc với khách hàng và sử dụng các dịch vụ ngân hàng...Tuy nhiên, điều này cũng đặt ra một thách thức lớn đó là vấn đề đảm bảo an toàn cho các thông tin được trao đổi qua mạng.

Cùng với sự hình thành và phát triển của Internet, giao dịch thương mại đã và đang có nhiều thay đổi lớn. Hiện nay, trong dịch vụ hành chính điện tử, đặc biệt trong bối cảnh đại dịch Covid-19 chưa có dấu hiệu giảm nhiệt, các hoạt động trao đổi dữ liệu điện tử, các dịch vụ thực hiện từ xa cho phép thực hiện các thủ tục hành chính một cách nhanh chóng, hiệu quả, đảm bảo an toàn phòng chống dịch. Dịch vụ hành chính điện tử giúp thực hiện các giao dịch, đăng ký thủ tục, truyền những cơ sở dữ liệu liên quan đến các thông tin nhạy cảm, cần phải bảo mật của khách hàng.

Một trong những vấn đề người dùng quan tâm hàng đầu khi thực hiện giao dịch thương mại qua Internet đó là *tính bí mật và tính toàn toàn vẹn* của các thông tin nhạy cảm như thông tin tài khóa n, thông tin cá nhân, *tính xác thực* của đối tác giao dịch. Sở dĩ là vì việc truyền thông tin qua mạng Internet hiện nay chủ yếu sử dụng giao thức TCP/IP [8]. TCP/IP cho phép các thông tin được gửi từ một máy tính này tới một máy tính khác đi qua một loạt các máy trung gian hoặc các mạng riêng biệt trước khi nó có thể đi tới được đích. Chính vì điểm này, giao thức TCP/IP đã tạo cơ hội cho "bên thứ ba" có thể thực hiện các hành động gây mất an toàn thông tin trong giao dịch, dễ dàng can thiệp, theo dõi và giả mạo các bức điện trên Internet. Lý do này khiến nhiều người đang đắn đo trong việc sử dụng mạng Internet cho các ứng dụng về tài chính và các số liệu nhạy cảm về tính pháp lý...

Trong các hệ thống xác thực, bảo mật trên website nói chung và dịch vụ hành chính điện tử nói riêng, hiện nay, nhiều giải pháp công nghệ được đưa ra để đảm bảo an toàn cho các giao dịch. *Kỹ thuật mã hóa thông tin*, *Chữ ký điện tử* và *chứng thực điện tử* được sử dụng để đáp ứng yêu cầu trên.

Mã hoá là quá trình chuyển đổi thông tin từ dạng có thể đọc được sang dạng không thể đọc được đối với những người không được nhận thông tin đó. *Giải mã* là quá trình chuyển đổi thông tin từ dạng không đọc được sang dạng có thể đọc được. Các thuật toán mã hoá là các hàm toán học đặc biệt. Mã hóa là một kỹ thuật khá phổ biến, có khả năng đảm bảo các yêu cầu sau:

- Đảm bảo tính toàn vẹn của thông điệp
- Chống phủ định
- Đảm bảo tính xác thực
- Đảm bảo tính bí mật của thông tin

Quá trình mã hóa thông tin được thực hiện trên cơ sở sử dụng một khóa chính là phương pháp để chuyển văn bản gốc thành văn bản mã hóa. Có hai kỹ thuật cơ bản thường được dùng để mã hóa thông tin trên Internet là "Mã hóa khóa bí mật" và "Mã hóa khóa công khai".

Chữ ký điện tử thực hiện chức năng giống chữ ký viết thông thường: là điều kiện cần và đủ để quy định tính duy nhất của văn bản điện tử cụ thể, xác định rõ ai là người chịu trách nhiệm trong việc tạo ra văn bản đó; và bất ký thay đổi nào (về nội dung, hình thức...) của văn bản trong quá trình lưu chuyển đều làm thay đổi tương quan giữa phần bị thay đổi và chữ ký.

Về mặt công nghệ, *chữ ký điện tử* là một dạng của mã hóa khóa công khai, là kết quả của việc áp dụng quá trình mã hóa lên một thông tin cụ thể. Chữ ký điện tử của một bản tin là một số phụ thuộc vào thông tin bí mật (khóa bí mật) mà chỉ người ký biết và phụ thuộc vào nội dung của bản tin được ký. Chữ ký điện tử đảm bảo được các yêu cầu an toàn thông tin sau:

- Tính toàn vẹn dữ liệu
- Xác thực gốc dữ liệu
- Chống phủ định

Khi một cá nhân sử dụng *chữ ký điện tử* để ký cho một tài liệu và gửi đi thì không thể chối cãi là đã không gửi tài liệu đó. Người nhận sẽ kiểm tra được tính toàn vẹn của dữ liệu và bất kỳ một sự thay đổi nào, hay thông tin về người gửi không chính xác. Điều này giúp các cơ quan chức năng thẩm tra rõ mọi vấn đề khi có tranh chấp xảy ra trong giao dịch điện tử.

Để xác minh một chữ ký điện tử, người nhận phải truy nhập tới khóa công khai của người ký và đảm bảo rằng nó tương ứng với khóa bí mật của người đó. Cần có chiến lược để kết hợp một cách tin cậy một người hay một thực thể cụ thể với cặp khóa này nhằm đảm bảo tính xác thực của mỗi bên tham gia giao dịch. Giải pháp cho vấn đề này được đưa ra là sử dụng một bên chứng thực thứ ba để kết hợp nhận dạng của người ký với một khóa công khai. Bên chứng thực thứ ba được biết đến như là tổ chức cấp chứng thực (Certification Authority - CA) trong hầu hết các chuẩn kỹ thuật được dùng.

Để kết hợp một cặp khóa với một người ký, tổ chức cấp chứng thực đưa ra một ***c****hứng thực điện tử*, là một bản ghi điện tử ghi lại một khóa công khai, nhận dạng của người sở hữu khóa và các thông tin về chứng chỉ như hạn sử dụng, số tuần tự. Chứng thực điện tử do cơ quan chứng nhận CA cấp là căn cứ để xác thực các bên tham gia giao dịch, là cơ sở đảm bảo tin cậy đối với các giao dịch thương mại điện tử.

Mục đích của đồ án là nghiên cứu các kỹ thuật mã hóa, chữ ký điện tử nhằm đảm bảo an toàn thông tin trong các giao dịch hành chính điện tử; và ứng dụng vào xây dựng mô phỏng một hệ thanh toán điện tử an toàn.

Nội dung nghiên cứu của đồ án bao gồm:

- Nghiên cứu hai kỹ thuật mã hóa phổ biến là Mã hóa khóa bí mật và Mã hóa khóa công khai, các thuật toán mã hóa được dùng trong mỗi phương

pháp bao gồm thuật toán mã hóa khóa bí mật theo chuẩn DES và thuật toán mã hóa khóa công khai RSA.

- Nghiên cứu các thao tác trong quá trình tạo và xác minh chữ ký điện tử, hai loại chữ ký điện tử là chữ ký với phụ lục và chữ ký khôi phục bản tin, thuật toán chữ ký điện tử DSA và thuật toán băm được dùng SHA.
- Nghiên cứu vai trò của chữ ký số trong Chính phủ điện tử và Hành chính điện tử.
- Xây dựng thuật toán mã hóa công khai RSA trong thực hiện thủ tục hành chính điện tử.

Với hệ thống thực hiện hành chính điện tử, một giao dịch bắt đầu khi người dùng đăng ký tài khoản với các thông tin chủ yếu như: Số chứng minh nhân dân / Căn cước công dân, họ tên ... Khi đăng ký thành công, người dùng sẽ được tự động tạo ra các thành phần cần có để tạo chữ ký số. Sau khi đăng ký và đăng nhập thành công, người dùng sẽ lựa chọn thủ tục cần làm. Ở đây, do trong khuôn khổ đồ án tốt nghiệp nên chỉ thực hiện 3 thủ tục hành chính đơn giản: Đăng ký tạm trú, thông báo lưu trú, thường trú. Sau khi lựa chọn thủ tục, người dùng điền các thông tin cần thiết và gửi thông tin về server. Trong quá trình gửi dữ liệu về server là quá trình xác thực bằng chữ ký số, đảm bảo tính chính xác, toàn vẹn dữ liệu từ lúc người dùng nhập tới khi lưu trong server. Giao dịch kết thúc. Người dùng sẽ chờ cơ quan chức năng có thẩm quyền xét duyệt và thông báo đến ký, nhận hồ sơ.

Đồ án được tổ chức thành 3 chương như sau:

Chương 1: Chữ ký số và vai trò của nó trong chính phủ điện tử

Chương này trình bày khái quát về chữ ký điện tử và các khái niệm liên quan, việc sử dụng chữ ký điện tử để giải quyết vấn đề xác thực, quá trình tạo và xác minh chữ ký điện tử, hai phân loại chữ ký điện tử. Ứng dụng chữ ký điện tử trong xử lý các thủ tục hành chính, những thực tế, rào cản, khó khăn trong việc số hóa thủ tục hành chính.

Chương 2: Tìm hiểu về hành chính điện tử và mật mã khóa công khai

Chương này trình bày các khái niệm về chính phủ điện tử và hành chính điện tử, những ưu điểm, khó khăn, tồn tại và hạn chế để thực hiện chính phủ điện tử, khái niệm hồ sơ điện tử do cấp có thẩm quyền định nghĩa; vấn đề về mật mã học, khái niệm mã hóa và giải mã, các phương pháp mã hoá và giải mã thông tin, lý thuyết mã khóa bí mật, mã hóa khóa công khai, các giải thuật được sử dụng để xây dựng các ứng dụng bảo mật như DES, RSA ... tóm tắt quá trình phân tích, số hóa thủ tục hành chính.

Chương 3: Xây dựng ứng dụng Cổng dịch vụ công quốc gia

Chương này xây dựng ứng dụng hành chính công quốc gia với 3 thủ tục hành chính được số hóa: Đăng ký tạm trú, thông báo lưu trú, thường trú. Một số hình ảnh của ứng dụng.

Kết luận

Phần cuối cùng là kết luận và một số vấn đề cần quan tâm nghiên cứu hơn nữa trong phát triển các ứng dụng.

Nhìn chung, toàn bộ đồ án của em là đưa ra một cách khái quát về việc nghiên cứu, tìm hiểu kỹ thuật mật mã được dùng trong an toàn các giao dịch, thực hiện thủ tục hành chính công qua hệ thống mạng. Song do thời gian thực hiện còn hạn hẹp, các kiến thức chuyên môn còn hạn chế, nên đồ án chắc chắn còn nhiều hạn chế, thiếu sót. Rất mong được sự góp ý, giúp đỡ của các thầy cô trong khoa công nghệ thông tin, các chuyên gia về lĩnh vực này và tất cả các bạn quan tâm đến vấn đề an toàn bảo mật trên mạng Internet để đồ án của tôi được hoàn thiện hơn.

Chương 1

CHỮ KÝ SỐ VÀ VAI TRÒ CỦA NÓ TRONG CHÍNH PHỦ ĐIỆN TỬ VÀ MẬT MÃ HÓA CÔNG KHAI

- Khái niệm chữ ký điện tử
- Chữ ký điện tử và vấn đề xác thực
- Vai trò của chữ ký điện tử trong Chính phủ điện tử và hành chính điện tử.
- Hoạt động của một hệ thống chữ ký điện tử
- Phân loại các hệ thống chữ ký điện tử
- Giải thuật chữ ký điện tử DSA
- Giải thuật hàm băm bảo mật SHA
- Kỹ thuật mã hóa khóa công khai
- Mã hóa khóa công khai RSA

1.1 Giới thiệu

Trong môi trường thương mại hiện nay, để thiết lập một cơ cấu cho việc xác thực thông tin dựa trên máy tính đòi hỏi những hiểu biết về các khái niệm và các ký năng chuyên ngành trong cả hai lĩnh vực an toàn máy tính và luật pháp. Một trong những ký thuật được sử dụng rộng rãi hiện nay đó là sử dụng *chữ ký số* (Digital Signature) và các cơ chế mã hóa. Chữ ký số (điện tử) có đầy đủ chức năng và đóng vai trò như chữ ký viết tay cùng với dấu xác thực người ký trong các giao dịch truyền thống qua mạng.

Xét trên quan điểm an toàn thông tin, chữ ký điện tử là kết quả của việc áp dụng quá trình mã hóa lên một thông tin cụ thể. Chữ ký điện tử của một bản tin là một số phụ thuộc vào thông tin bí mật (khóa bí mật) mà chỉ người ký biết và phụ thuộc vào nội dung của bản tin được ký. Các chữ ký phải xác minh được, nếu xảy ra tranh cãi như việc xác định xem có đúng một người đã ký vào tài liệu hay không (vấn đề chối bỏ nguồn gốc), một bên thứ ba tin cậy có thể giải quyết vấn đề này mà không truy nhập đến thông tin bí mật của người ký.

Chữ ký điện tử có nhiều ứng dụng trong an toàn thông tin, bao gồm xác thực (authentication), toàn vẹn dữ liệu (data integrity), không chối bỏ nguồn gốc (non-repudiation). Một trong những ứng dụng quan trọng nhất của chữ ký điện tử là chứng chỉ khóa công khai trong các mạng lớn. Chứng chỉ là một phương tiện cho bên thứ ba tin cậy (Trusted Third Party - TTP) kết hợp nhận dạng của người dùng với một khóa công khai, vì vậy tại một thời điểm sau đó các thực thể khác có thể xác thực khóa công khai mà không cần sự hỗ trợ của bên thứ ba.

Trong hành chính điện tử, liên quan nhiều đến thủ tục hành chính, pháp luật, đòi hỏi thông tin phải chính xác và xác thực đúng người có nhu cầu làm thủ tục. Chính vì vậy sẽ không tránh khỏi những tác nhân bên ngoài chống phá, đặc biệt là các thế lực thù địch thay đổi thông tin, phá hoại hệ thống, nhằm hạ

uy tín cơ quan chức năng, làm chậm tiến độ cải cách hành chính mà Đảng và Nhà nước đề ra.

1.2 Một số khái niệm cơ bản

- **Chữ ký số (Digital Signature)**

Chữ ký số là sự biến đổi của một bản tin sử dụng một hệ thống mã hóa khóa bất đối xứng (asymmetric cryptosystem) và một hàm băm mà một người có bản tin ban đầu và khóa công khai của người ký có thể xác định chính xác được:

1. Sự biến đổi có được tạo ra bằng cách sử dụng khóa bí mật tương ứng với khóa công khai của người ký hay không.
2. Bản tin ban đầu có bị thay đổi do sự biến đổi của nó gây ra hay không.

Chữ ký số (hay chữ ký điện tử) là ứng dụng quan trọng nhất của mã hoá khóa công khai. *Chữ ký điện tử* là một hình thức để đảm bảo tính pháp lý của các cam kết. Người gửi mã hóa đoạn tin (ký) bằng khóa bí mật của mình, người nhận giải mã bằng khóa công khai của người gửi. Chữ ký được áp dụng đối với thông điệp hay với một khối dữ liệu nhỏ tương ứng với thông điệp. Nó phải đáp ứng được các yêu cầu sau:

- Phải tương đối dễ dàng để tạo ra chữ ký điện tử.
- Phải tương đối dễ dàng để xác định và kiểm tra chữ ký điện tử.
- Phải không có khả năng tính toán để giả mạo một chữ ký điện tử, hoặc tạo một đoạn tin mới cho một chữ ký điện tử có sẵn.
- Người nhận có thể xác thực được đặc điểm nhận dạng của người gửi, nói cách khác, chữ ký phải sử dụng một số thông tin duy nhất đối với người gửi để chống cả giả mạo và phủ nhận. Vì vậy, người gửi sau này không thể chối bỏ được nội dung của bản tin mà mình đã gửi.
- Người nhận không thể bịa đặt hay thay đổi bản tin nhận được.

- **Chứng chỉ (Certificate)**

Chứng chỉ là một bản tin thực hiện các chức năng sau:

1. Xác định tổ chức cấp chứng chỉ (Certification authority - CA) phát hành chứng chỉ đó.
2. Gọi tên hoặc nhận dạng người sử dụng chứng chỉ (subscriber).
3. Chứa khóa công khai của người sử dụng chứng chỉ
4. Xác định thời hạn hợp lệ (operational period) của chứng chỉ (tức khóa ng thời gian mà thông tin trong chứng chỉ còn hiệu lực).
5. Xác định chứng chỉ đã được ký một cách số hóa bởi tổ chức cấp chứng chỉ phát hành nó.

Một người muốn xác minh một chữ ký điện tử thì ít nhất cần phải có: (1) khóa công khai tương ứng với khóa bí mật được dùng để tạo chữ ký, và (2) chứng cứ chắc chắn rằng khóa công khai (và do đó cả khóa bí mật tương ứng của cặp khóa) là của người ký. Mục đích cơ bản của chứng chỉ là đáp ứng cả hai yêu cầu này theo cách thức tin cậy.

Một chứng chỉ thông thường sẽ ở dạng các bản ghi nhị phân (binary record) nằm trong quá trình trao đổi dữ liệu điện tử (Electric Data Interchange - EDI) hiện thời. Việc sử dụng các trường bổ sung hay các mở rộng nhằm cung cấp thêm thông tin hay các thuộc tính bổ sung (ví dụ như sự xác nhận người sử dụng chứng chỉ (subscriber) như một tác nhân, hay tham chiếu chéo đến các cơ sở dữ liệu khác cung cấp thông tin về người sử dụng) là không bắt buộc.

Tổ chức cấp chứng chỉ (CA) cần phải ký một cách số hóa lên chứng chỉ, nhằm hai mục đích: (1) Bảo vệ tính toàn vẹn thông tin của chứng chỉ, và (2) cho phép xác nhận chữ ký điện tử của tổ chức cấp chứng chỉ.

Chữ ký điện tử của tổ chức cấp chứng chỉ (CA) cũng như chữ ký điện tử của người sử dụng chứng chỉ (subscriber) cần có một dấu thời gian (time - stamp) để thuận tiện cho việc chứng minh rằng chữ ký điện tử (của tổ chức cấp

chứng chỉ hay của người sử dụng chứng chỉ) được tạo ra trong thời gian hiệu lực của một chứng chỉ hợp lệ, do đó chữ ký điện tử có khả năng kiểm định một chứng chỉ.

- **Xác nhận hợp lệ (Validation)**

Thông tin trong một chứng chỉ có thể thay đổi theo thời gian. Một người sử dụng chứng chỉ (*certificate user*) cần phải đảm bảo là dữ liệu trong chứng chỉ là đúng (gọi là *xác nhận hợp lệ chứng chỉ*). Có hai phương pháp cơ bản để *xác nhận hợp lệ chứng chỉ*:

- Người sử dụng có thể trực tiếp hỏi CA về tính hợp lệ của chứng chỉ mỗi lần sử dụng nó. Đây là yếu tố xác nhận tính hợp lệ trực tuyến (*online validation*)
- CA có thể chứa thêm thời hạn hợp lệ vào trong mỗi chứng chỉ - một bộ thời gian sẽ định nghĩa khóa ng thời gian mà các thông tin chứa trong chứng chỉ được cho là hợp lệ (còn hiệu lực). Đây là xác nhận hợp lệ không trực tuyến (*offline validation*).

- **Thu hồi chứng chỉ**

Thu hồi chứng chỉ là kết thúc vĩnh viễn thời hạn hợp lệ (operational period) của một chứng chỉ xét từ một thời điểm xác định trở đi. Sự *thu hồi chứng chỉ* là quá trình báo cho người sử dụng biết khi thông tin trong một chứng chỉ bất ngờ mất hiệu lực. Việc này có thể xảy ra khi một chủ thể của khóa riêng bị lộ, hay khi thông tin định danh của một chứng chỉ thay đổi (thí dụ như chủ thể có một số điện thoại mới).

- **Xác thực (Authentication)**

Xác thực là một quá trình được dùng để xác định nhận dạng của một người hoặc tính toàn vẹn của một thông tin cụ thể. Đối với một bản tin, sự xác thực bao gồm việc xác định nguồn gốc bản tin và xác định nó chưa bị sửa đổi hoặc thay thế trong quá trình truyền thông.

Khi một CA chứng thực một thực thể và người sử dụng xác nhận sự hợp lệ của chứng thực đó, thực thể được gọi là *xác thực*. Mức độ mà người sử dụng tin tưởng vào các thông tin của chứng chỉ và sự hợp lệ của nó là cách để đánh giá độ mạnh (*strength of Authentication*) của sự *xác thực*. Ví dụ, nếu bạn nhìn Alice và thấy mắt cô ta màu xanh, khi đó bạn có một sự xác thực mạnh mẽ về màu mắt của Alice, mặt khác nếu bạn nghe ai đó nói về điều đó thì sự xác thực là yếu và bạn chưa hoàn toàn tin tưởng vào điều đó.

- **Hàm băm**

Hàm băm là một thuật toán ánh xạ hay chuyển đổi một chuỗi bit có độ dài tùy ý thành một chuỗi bit khác thường có kích thước cố định (thường là bé hơn) (gọi là kết quả băm). Hàm băm có các đặc tính sau:

(1) Độ dài kết quả băm là như nhau tại mọi thời điểm khi thuật toán được thực thi sử dụng đối với mọi bản tin đầu vào.

(2) Về mặt tính toán, không thể khôi phục được bản tin từ kết quả băm nhận được và từ thuật toán băm.

(3) Về mặt tính toán, không thể tìm được hai bản tin khác nhau cho cùng một kết quả băm từ thuật toán băm.

Hàm băm đôi khi được gọi là "hàm một chiều" (one – way function) hay "Thuật toán rút gọn bản tin" (message digest algorithm).

Hàm băm thường được kết hợp để xây dựng chữ ký điện tử vừa đảm bảo an toàn (không thể cắt dán), định danh được người gửi, mặt khác lại vừa có thể dùng để kiểm tra tính toàn vẹn của thông điệp. Với việc sử dụng *hàm băm* ta có thể có được một phương pháp xác thực mà không cần phải mã hoá toàn bộ bản tin.

- **Kết quả băm**

Kết quả băm là đầu ra của thuật toán băm khi xử lí một bản tin.

1.3 Vấn đề xác thực và chữ ký điện tử

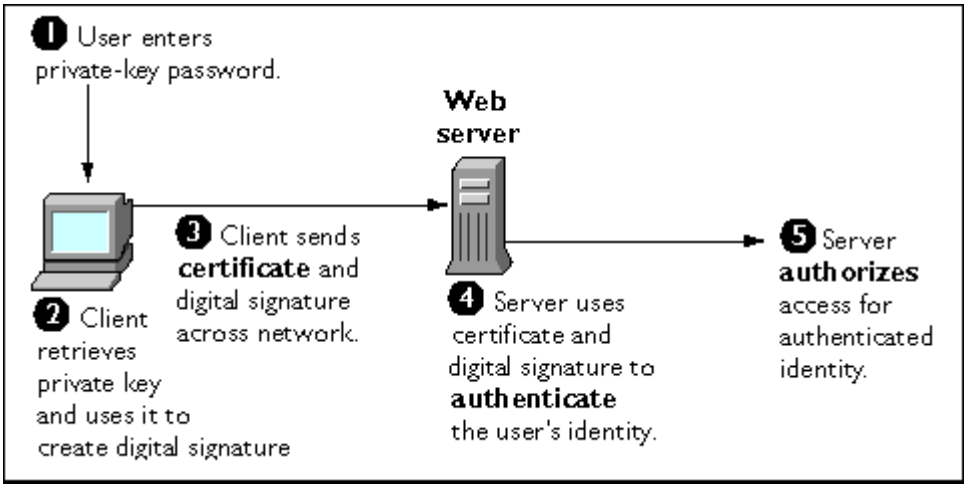
Xác thực (Athentication) là một kỹ thuật để xác minh xem người tham gia hội thoại là đúng người cần hội thoại hay là kẻ mạo danh. Việc *xác thực* là để đảm bảo thông tin trao đổi giữa hai người A và B không bị một kẻ đột nhập (*intruder*) nào đó can thiệp, xem trộm hay sửa chữa nội dung. Vì vậy có thể nói *xác thực* là một thành phần rất cần thiết của một hệ thống bảo mật đối với bất cứ một doanh nghiệp nào quan tâm đến việc bảo vệ tài sản thông tin và muốn biết ai đang cố gắng truy nhập vào mạng của họ. Việc *xác thực* trở nên đặc biệt quan trọng khi một số những phương thức truyền thông phức tạp được sử dụng.

Ngoài việc chứng minh người sử dụng, các hệ thống xác thực cũng được sử dụng để xác định những thông tin được yêu cầu nào có thể truy nhập – ví dụ, một cơ sở dữ liệu tài nguyên hoặc cơ sở dữ liệu tài chính của một tổ chức. Một hệ thống xác thực đúng đắn thường là sự kết hợp của 2 hoặc 3 thành phần sau:

- ✔ Người dùng có gì (smart card, giấy chứng nhận - certificate)
- ✔ Người dùng biết gì (mật khẩu - password)
- ✔ Một thuộc tính vật lý (vân tay hoặc những thông tin sinh học khác).

Việc *xác thực* thường đạt được thông qua yêu cầu và phản hồi (*Challenge and response*), chứng chỉ số (*Digital Certificate*), hoặc thông điệp được băm (*Message digest* - MD) và chữ ký điện tử (*Digital Signature*).

Xác thực dùng *chữ ký điện tử* được mô tả như trong hình sau:



Hình 1.0.1 Sơ đồ minh hoạ việc xác thực sử dụng chứng chỉ số và chữ ký điện tử

- Trước tiên, User đưa vào mật khẩu truy nhập khóa riêng của mình cho Client
- Sau đó, Client truy lục khóa riêng và sử dụng nó để tạo chữ ký điện tử cho User
- Tiếp theo, Client gửi chứng chỉ và chữ ký điện tử của User tới Server qua mạng
- Server sử dụng chứng chỉ và chữ ký nhận được để xác thực định danh của User
- Nếu đúng, Server xác thực quyền truy nhập cho User và cho phép User bắt đầu phiên làm việc giữa Client và Server.

Quá trình ký số diễn ra như sau:

- Giả sử, anh A muốn gửi qua mạng một thông báo X có độ dài tùy ý cho một đối tác B nào đó, và giả sử ta sử dụng lược đồ ký RSA với tham số n có độ dài 1024 bít. Khi đó, nếu độ dài thông báo X (sau khi đã số hóa) bé hơn hoặc bằng 1024 bít thì ta thực hiện ký như sau: Mã hoá thông điệp X bằng khóa riêng (*private key*) của mình để tạo ra chữ ký điện tử được ký hiệu là S.
- Gắn chữ ký này vào thông điệp X cần gửi cặp (X,S) đến người nhận B. Sau khi B nhận được cặp (X,S), người nhận B sẽ kiểm tra chữ ký và tính

toàn vẹn của thông báo X bằng cách dùng khóa công khai của người gửi A để mã hóa chữ ký S trên thông điệp X. Nếu kết quả trùng với X thì chữ ký là hợp lệ và bản thông báo coi như được xác thực, còn nếu trái lại thì hoặc chữ ký bị giả mạo hoặc thông báo X bị sửa đổi. – Trường hợp độ dài bản thông báo X lớn hơn 1024 bít (Tức là lớn hơn 128 ký tự) thì người ký bản thông báo X phải sử dụng hàm băm để rút gọn X thành h(X) = Y. Lúc này Y sẽ có độ dài không vượt quá 1024 bít và người gửi A sẽ ký trên Y thay vì ký trên X. Hiện tại có hai loại hàm băm là MD5 và SHA. Nếu dùng hàm băm MD5 thì độ dài Y sẽ là 128 bít còn nếu dunhf SHA thì tùy theo phiên bản mà Y sẽ có độ dài 128, 192 hoặc 256 bít.

1.4 Hoạt động của một hệ thống chữ ký điện tử

Chữ ký số hay chữ ký điện tử (Digital Signature) được tạo ra và xác minh dựa trên mã hóa khóa công khai, sử dụng một thuật toán dùng hai khóa khác nhau nhưng có quan hệ toán học với nhau

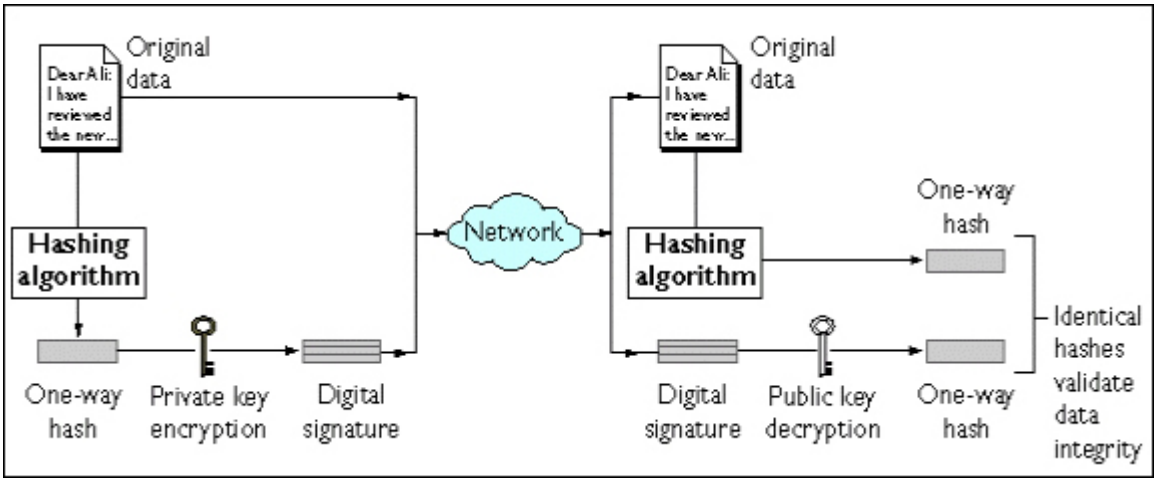
Các khóa của một hệ thống mã hóa bất đối xứng dùng cho chữ ký điện tử bao gồm một khóa bí mật (*private key*) được dùng để tạo chữ ký và chỉ người ký biết được khóa này, và một khóa công khai (*public key*) được công khai cho tất cả mọi người cần biết và do một bên tin tậy dùng để xác minh chữ ký điện tử. Nếu có nhiều người cùng muốn xác minh một chữ ký, khóa công khai cần được phân phối tới tất cả mọi người. Khi đó, khóa công khai có thể được đặt trong một thư mục hay một kho chứa trực tuyến. Mặc dù các khóa có quan hệ về mặt toán học với nhau nhưng xét về mặt tính toán, không thể khôi phục được khóa bí mật từ khóa công khai. Do đó, mặc dù nhiều người cùng biết khóa công khai của người ký và dùng nó để xác minh chữ ký, nhưng không thể tìm ra được khóa bí mật và dùng khóa bí mật này để giả mạo chữ ký. Nguyên lí này được gọi là nguyên lí không thể đảo ngược.

Một phương pháp cơ bản là sử dụng một hàm băm để tạo và xác minh chữ ký. Một hàm băm là một thuật toán tạo ra một biểu diễn số dưới dạng một giá trị băm có chiều dài không đổi và thường nhỏ hơn bản tin và là duy nhất đối với mọi bản tin. Bất cứ thay đối nào đối với bản tin đều tạo nên một giá trị băm khác khi sử dụng cùng một hàm băm. Với một hàm băm bảo mật, thì không thể khôi phục được bản tin nguyên gốc từ giá trị băm của nó. Do đó, một hàm băm cho phép tạo chữ ký điện tử trên dữ liệu nhỏ hơn, có kich thước xác định và liên quan chặt chẽ với nội dung bản tin. Bằng cách đó, đảm bảo được rằng không có sự sửa đổi bản tin khi nó được ký số.

Việc sử dụng chữ ký điện tử bao gồm hai tiến trình, một được tiến hành bởi người ký và một bởi người nhận chữ ký.

- **Tạo chữ ký điện tử** (Digital signature creation). Việc sử dụng giá trị băm duy nhất nhận được từ bản tin được ký và khóa bí mật cho trước. Vì giá trị khóa bí mật được bảo mật, do đó về thực hành, không có khả năng tạo ra chữ ký $S^1 = S$, tức là hai người khác nhau không thể cho cùng một chữ ký.

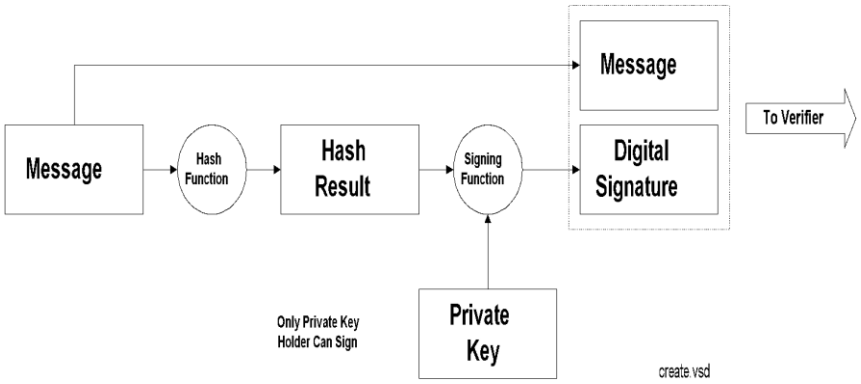
- **Xác minh chữ ký điện tử** (Digital signature verification) là quá trình kiểm tra chữ ký điện tử sử dụng bản tin nguyên gốc và một khóa công khai cho trước, bằng cách này xác định được chữ ký điện tử có phải được tạo ra từ bản tin đó sử dụng khóa bí mật tương ứng với khóa công khai hay không.



Hình 1.0.2 Sơ đồ minh hoạ quá trình truyền thông điệp sử dụng chữ ký điện tử

1.4.1 Quá trình tạo chữ ký.

Xét trên quan điểm ký thuật, quá trình ký số một bản tin được tiến hành gồm hai bước:



Hình 1.0.3 Quá trình tạo chữ ký số cho một bản tin

Bước 1: **Tính toán giá trị băm của bản tin** (Caculate the Message Digest)

Trong bước đầu tiên của quá trình, giá trị băm của bản tin (thường gọi là bản tin thu gọn – message digest) được tính bằng cách áp dụng các thuật toán băm (hashing algorithm) như MD2, MD4, MD5, SHA1… Giá tị băm tìm được

của bản tin là một chuỗi bit, thường có độ dài cố định, được tách ra từ bản tin theo một cách thức nào đó.

Tất cả các thuật toán tính giá trị băm tin cậy sử dụng các chuyển đổi toán học thỏa mãn khi một bit từ bản tin đầu vào bị thay đổi sẽ dẫn đến thay đổi toàn bộ giá trị băm. Nhờ đặc tính này, các thuật toán này rất khó bị tấn công, nói cách khác, không thể tìm được bản tin ban đầu từ giá trị băm cho trước của bản tin đó. Giá trị băm của một bản tin có kích thước nhỏ hơn hàng trăm lần so với bản tin đầu vào. Các tài nguyên tính toán cần dùng cho tìm bản tin từ giá trị băm của nó lớn đến mức trên thực tế là không thể thực hiện được.

Xét trên lí thuyết, có thể có hai bản tin khác nhau có cùng một giá trị băm được tính bởi cùng một thuật toán, nhưng khả năng xảy ra trường hợp này rất nhỏ mà trên thực tế có thể bỏ qua.

Bước 2: Tính toán chữ ký số (Caculate the Digital Signature)

Trong bước hai của quá trình ký số một bản tin, thông tin nhận được từ bước thứ nhất – giá trị băm của bản tin (Bản tin thu gọn – message digest) được mã hóa với khóa bí mật của người ký, thu được giá trị băm đã mã hóa, gọi là **chữ ký số** (digital signature). Để thực hiện việc này, các thuật toán mã hóa tính toán chữ ký điện tử từ bản tin thu gọn cho trước được dùng. Các thuật toán phổ dụng nhất là RSA (dựa trên lý thuyết số), DSA (dựa trên lý thuyết logarit rời rạc), và ECDSA (dựa trên lý thuyết đường elip). Sau đó, chữ ký số thu được sẽ được đính kèm vào bản tin theo một định dạng xác định và được gửi đi cùng với bản tin.

1.4.2 Quá trình xác minh chữ ký

Công nghệ chữ ký điện tử cho phép người nhận bản tin đã ký số xác minh nguồn gốc thực và tính toàn vẹn của bản tin đó. Quá trình xác minh chữ ký điện tử nhằm mục đích xác định xem một bản tin có được ký bởi khóa bí mật tương ứng với khóa công khai đã cho hay không. Nếu ta cần kiểm tra người ký, ta cần có được khóa công khai thực sự của người dó theo một cách thức nào đó (thường là do một CA cung cấp). Nếu không nhận được khóa công khai

của người ký, ta không thể kiểm tra được bản tin có thực sự do người đó ký hay không.

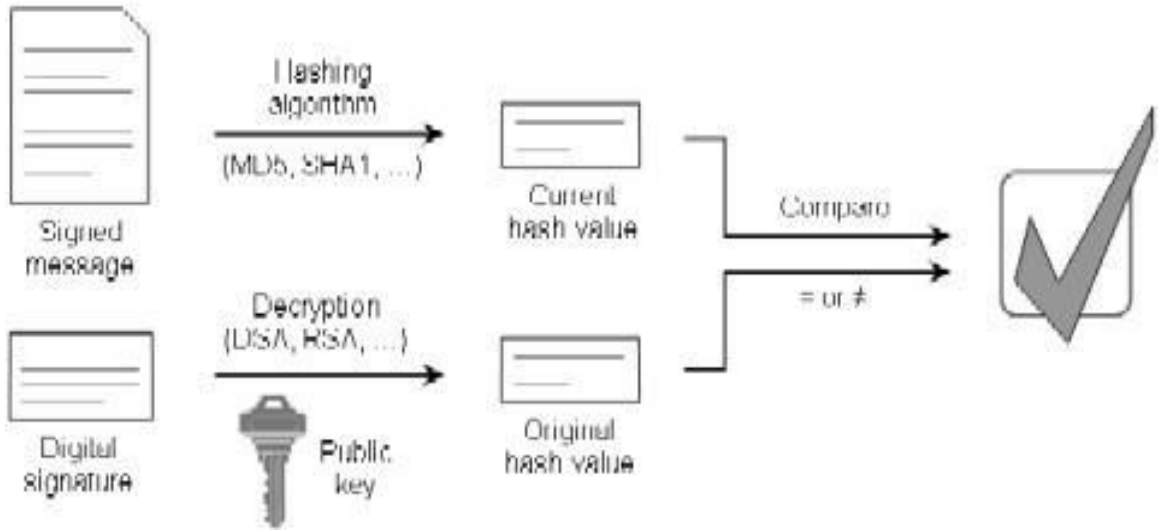
Quá trình xác minh chữ ký điện tử được tiến hành gồm ba bước:

Bước 1: Tính toán giá trị băm hiện thời (Caculate the Curent Hash - Value)

Trong bước một, thực hiện tính giá trị băm của bản tin đã ký. Khi tính toán sử dụng cùng một thuật toán băm như trong quá trình ký số bản tin. Giá trị băm nhận được gọi là giá trị băm hiện thời vì nó được tính từ trạng thái hiện thời của bản tin.

Bước 2: Tính giá trị băm ban đầu (Caculate the Original Hash - Value)

Trong bước thứ hai của quá trình xác minh chữ ký, chữ ký số được giải mã với cùng một thuật toán dùng trong quá trình ký số bản tin. Việc giải mã được thực hiện bởi khóa công khai tương ứng với khóa bí mật dùng trong quá trình ký. Kết quả chúng ta nhận được giá trị băm ban đầu (Original Hash - Value) được tính từ bản tin nguyên gốc dùng trong bước đầu của quá trình ký số (the original message digests).



Hình 1.0.4 Quá trình xác minh một chữ ký số

Bước 3: So sánh giá trị băm hiện thời và giá trị băm ban đầu (The current and the Original Hash - Values).

Trong bước thứ ba, chúng ta so sánh giá trị băm hiện thời nhận được trong bước một với giá trị băm ban đầu nhận được trong bước hai. Nếu hai giá trị băm giống nhau, việc xác minh đã thành công và chứng minh được bản tin đã được ký bằng khóa bí mật tương ứng với khóa công khai dùng trong quá trình xác minh. Nếu hai giá trị băm khác nhau, thì chữ ký số là không hợp lệ và việc xác minh chữ ký là thất bại.

Nguyên nhân dẫn đến chữ ký không hợp lệ:

Một chữ ký số là không hợp lệ có thể có ba nguyên nhân sau:

- Nếu chữ ký số bị giả mạo (không thực) và nó được giải mã với khóa công khai, giá trị băm nhận được không phải là giá trị băm của bản tin nguyên gốc.
- Nếu bản tin bị thay đổi (bị giả mạo) sau khi ký, giá trị băm hiện thời nhận được từ bản tin giả sẽ khác với giá trị băm ban đầu vì hai bản tin khác nhau tương ứng với hai giá trị băm khác nhau.
- Nếu khóa công khai không tương ứng với khóa bí mật đã dùng trong quá trình ký số, giá trị băm ban đầu nhận được khi giải mã chữ ký sẽ là một giá trị sai.

1.4.3 Các chứng chỉ khóa công khai

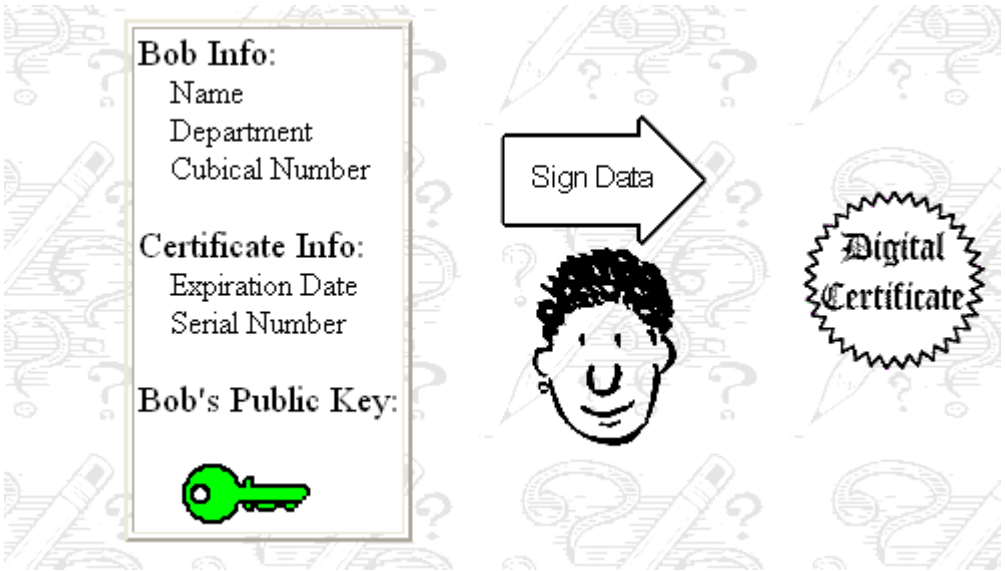
Để xác minh một chữ ký số, bên xác minh phải truy nhập tới khóa công khai của người ký và đảm bảo rằng nó tương ứng với khóa bí mật của người ký. Tuy nhiên, một cặp khóa bí mật và khóa công khai về bản chất không gắn với bất cứ người nào, nó đơn giản chỉ là một cặp số. Cần có chiến lược để kết hợp một cách tin cậy một người hay một thực thể cụ thể với cặp khóa này [9].

Trong một giao dịch chỉ có hai bên tham gia, mỗi bên có thể truyền khóa công khai của cặp khóa mà bên kýa sẽ dùng. Phương pháp nhận dạng này khó thực hiện nhất là khi giữa hai bên có khóa ng cách địa lí, thường kiểm soát truyền thông nhờ một kênh không an toàn như Internet; các bên tham gia không

phải là con người mà là các công ty hay các thực thể nhân tạo hoạt động thông qua các agent. Khi thương mại điện tử đang dần chuyển từ môi trường song phương sang kiến trúc nhiều – nhiều của World Wide Web trên Internet, các giao dịch quan trọng (*significant transaction*) diễn ra giữa những người không quen biết, không có liên hệ bằng hợp đồng và không bao giờ gặp lại nhau, vấn đề xác thực / không chối bỏ trở thành một yếu tố của tính hiệu quả và tính tin cậy. Một hệ thống truyền thông mở như Internet cần có một hệ thống xác thực nhận dạng để quản lý tình huống này.

Giải pháp cho vấn đề này được đưa ra là sử dụng một bên chứng thực thứ ba để kết hợp nhận dạng của người ký với một khóa công khai. Bên chứng thực thứ ba được biết đến như là tổ chức cấp chứng chỉ (Certification Authority - CA) trong hầu hết các chuẩn ký thuật được dùng.

Để kết hợp một cặp khóa với một người ký, tổ chức cấp chứng thực đưa ra một chứng chỉ, là một bản ghi điện tử ghi lại một khóa công khai, nhận dạng của người sở hữu khóa và các thông tin về chứng chỉ như hạn sử dụng, số tuần tự. Một người nhận được chứng chỉ có thể dùng khóa công khai được lưu trong chứng chỉ để xác minh chữ ký điện tử có được tạo ra từ khóa bí mật tương ứng hay không.



Hình 1.0.5 Một chứng chỉ khóa công khai

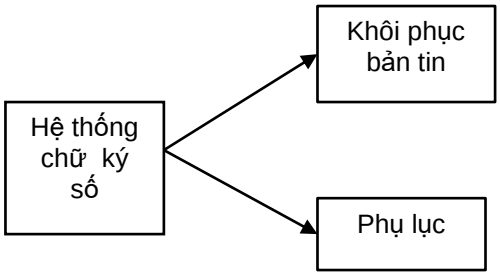
Để đảm bảo tính xác thực cho cả bản tin và chứng chỉ, tổ chức cấp chứng chỉ thực hiện ký số lên chứng chỉ. Chữ ký số cần có một dấu thời gian tin cậy cho phép người xác minh xác định được chữ ký số có được tạo ra trong thời hạn hợp lệ ghi trong chứng chỉ hay không.

Để một khóa công khai và nhận dạng của một người dùng cụ thể là sẵn dùng cho quá trình xác minh, chứng chỉ cần được đặt trong một kho chứa sẵn dùng. Kho chứa này là các cơ sở dữ liệu trực tuyến chứa các chứng chỉ và các thông tin khác sẵn sàng để lấy ra và dùng trong xác minh chữ ký số. Việc lấy thông tin có thể thực hiện tự động nhờ một chương trình xác minh thực hiện truy vấn trực tiếp cơ sở dữ liệu để nhận được các chứng chỉ khi cần.

1.5 Phân loại các hệ thống chữ ký điện tử

Các hệ thống chữ ký điện tử bao gồm hai phân lớp tổng quát nhất, có thể mô tả tóm lược như sau [1]:

1. Các hệ thống chữ ký số với phụ lục (Digital Signature Schemes with appendix) yêu cầu đầu vào của thuật toán xác minh là bản tin nguyên gốc
2. Các hệ thống chữ ký số với hồi phục bản tin (Digital Signature Schemes with message recovery) không yêu cầu đầu vào của thuật toán xác minh là bản tin nguyên gốc. Trong trường hợp này, bản tin gốc được khôi phục từ chữ ký.



1.5.1 Chữ ký điện tử với phụ lục

Các hệ thống chữ ký số với phụ lục được sử dụng rộng rãi trong thực tế. Chúng dựa vào các hàm băm mã hóa (*cryptographic*) và ít bị tấn công [1].

1. Định nghĩa:

Các hệ thống chữ ký số yêu cầu đầu vào của thuật toán xác minh là bản tin nguyên gốc được gọi là hệ thống chữ ký số với phụ lục.

Các ví dụ của cơ chế chữ ký điện tử với phụ lục là các hệ thống chữ ký số DSA, ElGamal, Schnorr. Các ký hiệu được dùng cho bởi bảng 3.1 sau:

Ký hiệu	Ý nghĩa
$\boldsymbol{M}$	Tập các phần tử được gọi là không gian bản tin (*message space*)
$\boldsymbol{M_S}$	Tập các phần tử được gọi là không gian ký số (*sigining space*)
$\boldsymbol{S}$	Tập các phần tử được gọi là không gian chữ ký (*signature space*)
$\boldsymbol{R}$	Ánh xạ 1 - 1 từ M đến M_S gọi là hàm dư thừa (*redundancy function*)
$\boldsymbol{M_R}$	Ảnh của R ($M_R = Im(R)$)
$\boldsymbol{R^{-1}}$	Hàm ngược của R ($R^{-1} : M_R \rightarrow M$)
R	Tập các phần tử được gọi là tập chỉ số (*indexing set of signing*)
$\boldsymbol{h}$	Hàm một chiều trên miền M
$\boldsymbol{M_h}$	Ảnh của h (h: $M \rightarrow M_h$); $M_h \subseteq M_S$ được gọi là không gian giá trị
	Băm

Bảng 1.1 Các ký hiệu toán học

2. Thuật toán tạo khóa

Mỗi thực thể tạo một khóa bí mật dùng để ký các bản tin, và một khóa công khai tương ứng cho các thực thể khác dùng để xác minh chữ ký.

1. Mỗi thực thể A cần chọn một khóa bí mật định nghĩa một tập

   $S_A = \{S_{A,k} : k \in R\}$ các phép biến đổi. Mỗi $S_{A,k}$ là một ánh xạ 1 – 1 từ M_h tới

   S và được gọi là một phép biến đổi ký (*signing transformation*).

2. S_A định nghĩa một ánh xạ tương ứng V_A từ $M_h \times S$ tới tập {true, false} thỏa mãn:

$$V_A\left(\overrightarrow{m, s^*}\right) = \begin{cases} true & khi\ S_{A,k}\left(\overrightarrow{m}\right) = s^* \\ false & \neq \end{cases}$$

Với tất cả $\overrightarrow{m} \in M_h$, $s^* \in S$; $\overrightarrow{m} = h(m)$ với $m \in M$. V_A được gọi là phép biến đổi xác minh (*verification transformation*) và được xây dựng bằng các tính

toán mà không cần biết khóa bí mật của người ký.

3. khóa công khai của A là V_A ; khóa bí mật của A là tập S_A

3. *Thuật toán tạo chữ ký và xác minh chữ ký*

Thực thể A tạo một chữ ký $s \in S$ cho bản tin $m \in M$, mà sau đó thực thể B có thể xác minh.

1. Tạo chữ ký. Thực thể A thực hiện các công việc sau:

(a) Chọn một phần tử $k \in R$.

(b) Tính $\overrightarrow{m} = h(m)$ và $s^* = S_{A,k}(\overrightarrow{m})$

(c) Chữ ký của A cho bản tin m là s^*. Cả m và s^* là sẵn dùng cho các

thực thể muốn xác minh chữ ký.

2. Xác minh chữ ký. Thực thể B thực hiện các công việc sau:

(a) Nhận khóa công khai đã xác thực của A là V_A

(b) Tính $\overrightarrow{m} = h(m)$ và $u = V_A(\overrightarrow{m}, s^*)$.

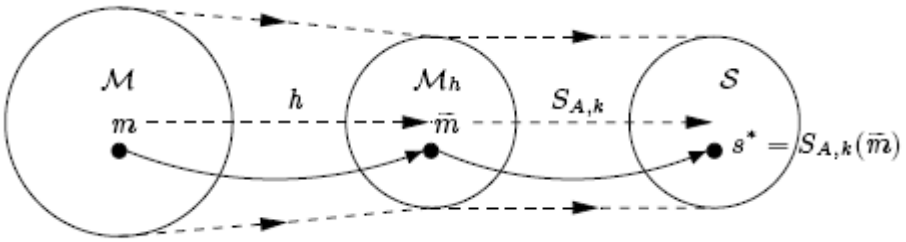
(c) Chấp nhận chữ ký nếu và chỉ nếu $u = true$

Hình sau cho thấy cái nhìn tổng quan về mặt ngữ nghĩa của một hệ thống chữ ký số với phụ lục. Các phép biến đổi ký số và xác minh chữ ký yêu cầu các đặc tính sau:

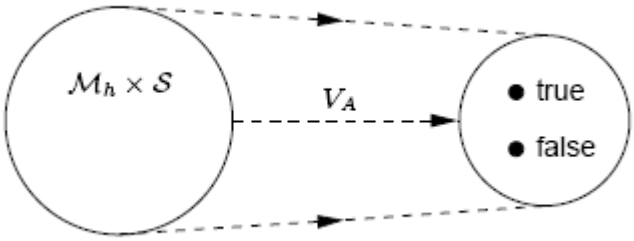
(i) Với mỗi $k \in R$, $S_{A,k}$ phải tính được.

(ii) V_A phải tính được

(iii) Về mặt tính toán, không một thực thể nào ngoài A có thể tìm được một giá trị $m \in M$ và một $s^* \in S$ mà $V_A(\square^{m}, s^*) = \text{true}$ với $\square^{m} = h(m)$



(a). Quá trình ký số bản tin



(b). Quá trình xác minh chữ ký.

Hình 1.0.6 Tổng quan về hệ thống chữ ký số với phụ lục

4. Chú ý

Hầu hết các hệ thống chữ ký số với hồi phục bản tin được áp dụng với các bản tin có độ dài cố định, trong khi các hệ thống chữ ký số với phụ lục được áp dụng cho các bản tin có độ dài tùy biến. Hàm một chiều ***h*** trong thuật toán tạo và xác minh chữ ký thường được lựa chọn là một hàm băm không xung đột (*collision – free function*). Một phương pháp băm khác là chia nhỏ bản tin thành các khối có chiều dài cố định, các khối này được ký riêng lẻ sử dụng hệ thống chữ ký số với hồi phục bản tin.

1.5.2 Chữ ký điện tử với khôi phục bản tin

1. Định nghĩa

Một hệ thống chữ ký số với khôi phục bản tin là một hệ thống chữ ký số trong đó thuật toán xác minh chữ ký không yêu cầu sử dụng bản tin ban đầu[1].

Các hệ thống chữ ký số loại này có đặc tính là bản tin được ký có thể khôi phục được từ chữ ký. Đặc tính này có được là do việc sử dụng các bản tin ngắn.

Các ví dụ của cơ chế chữ ký điện tử với hồi phục bản tin là các hệ thống chữ ký số RSA, Rabin, Nyberg – Rueppel [1].

2. Thuật toán tạo khóa (Key generation Algorithm)

Mỗi thực thể tạo một khóa bí mật dùng để ký các bản tin, và một khóa công khai tương ứng cho các thực thể khác dùng để xác minh chữ ký.

1. Mỗi thực thể A lựa chọn một tập $S_A = \{S_{A,k} : k \in \mathrm{R}\ \}$ các phép biến đổi. Mỗi $S_{A,k}$ là một ánh xạ 1 – 1 từ M_S tới S và được gọi là một phép biến đổi ký (*signing transformation*).
2. S_A định nghĩa một ánh xạ V_A có đặc tính là: $V_A \square S_{A,k}$ là ánh xạ đồng nhất trên M_S (identity map) với tất cả $k \in \mathrm{R}$. V_A được gọi là phép biến xác minh chữ ký được xây dựng bằng các tính toán mà không cần biết khóa bí mật của người ký.
3. khóa bí mật của A là V_A; khóa công khai của A là tập SA.

3. Thuật toán tạo chữ ký và xác minh chữ ký

Thực thể A tạo một chữ ký $s \in S$ cho bản tin $m \in M$, mà sau đó thực thể B có thể xác minh. Bản tin m được hồi phục từ s.

1. Tạo chữ ký (Signature Generation Algorithm)

Thực thể A thực hiện các công việc sau:

(a) Chọn một phần tử $k \in \mathrm{R}$

(b) Tính $\overset{\sqcup}{m}' = R(m)$ và $s^* = S_{A,k}(\overset{\sqcup}{m}')$. ($R$ là một hàm dư thừa)

(c) Chữ ký của A cho bản tin m là s^*; s^* là sẵn dùng cho các thực thể muốn xác minh chữ ký và bản tin m được khôi phục từ s^*

2. Xác minh chữ ký (Verification Algorithm)

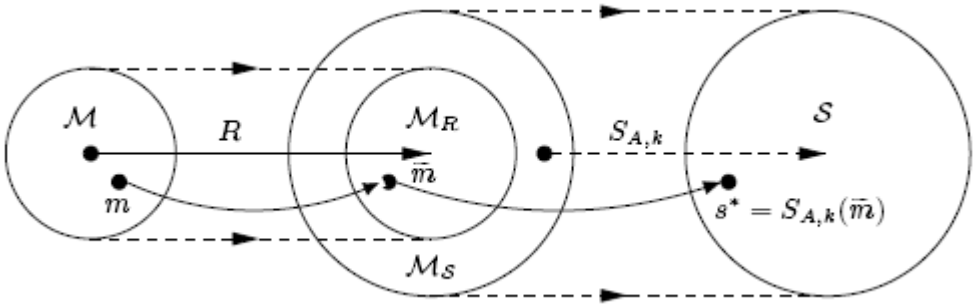
Thực thể B thực hiện các công việc sau:

(a) Nhận khóa công khai đã xác thực của A là V_A

(b) Tính $\overline{\sqcup}' = V_A(s^*)$.

(c) kiểm tra $\overline{\sqcup}' \in M_R$. Nếu $\overline{\sqcup}' \notin M_R$, loại bỏ chữ ký

(d) Hồi phục m từ bằng cách tính $R^{-1}(\overline{\sqcup}')$



Hình 1.0.7 Tổng quan về hệ thống chữ ký số hồi phục bản tin

Hình 1.7 cho thấy cái nhìn tổng quan về mặt ngữ nghĩa của một hệ thống chữ ký số hồi phục bản tin. Các phép biến đổi ký số và xác minh chữ ký yêu cầu các đặc tính sau:

(i) Với mỗi $k \in R$, $S_{A,k}$ phải tính được.

(ii) V_A phải tính được

(iii) Về mặt tính toán, không một thực thể nào ngoài A có thể tìm được

một giá trị $s^* \in S$ mà $V_A(s^*) \in M_R$

4. Chú ý

Hàm dư thừa R và hàm ngược của nó R^{-1} được phổ biến công khai. Lựa chọn một hàm R phù hợp là hết sức quan trọng đối với tính bảo mật của hệ thống.

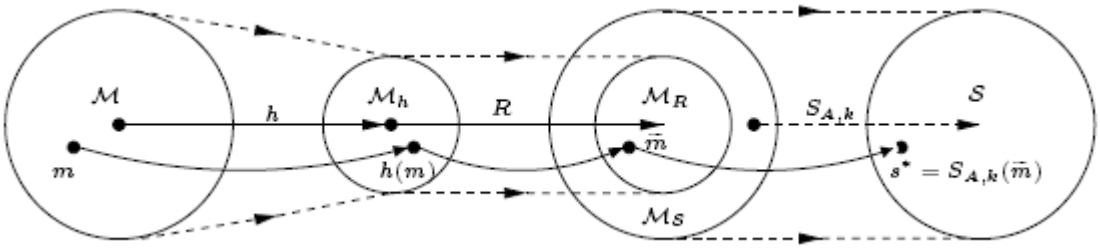
Giả sử $M_R = M_S$. Giả sử R và $S_{A,k}$ tương ứng là các song ánh từ M tới M_R và từ M_S tới S. Điều này suy ra M và S có cùng số phần tử. Vì $s^* \in S$, $V_A(s^*) \in M_R$, ta dễ dàng tìm được bản tin m và chữ ký tương ứng s^* theo thuật toán xác minh chữ ký sau:

1. Chọn ngẫu nhiên $k \in$ R và $s^* \in S$.
2. Tính $\sqcup\!\!\!\!\cdot\ m = V_A(s^*)$.
3. Tính $m = R^{-1}(\sqcup\!\!\!\!\cdot\ m)$

Phần tử s^* là chữ ký hợp lệ cho bản tin m và được tạo ra mà không cần sử dụng tập các phép biến đổi ký số S_A.

5. Chú ý (Các chữ ký số với phụ lục từ các hệ thống chữ ký hồi phục bản tin)

Bất cứ một hệ thống chữ ký số với hồi phục bản tin nào đều có thể chuyển thành hệ thống chữ ký số với phụ lục bằng cách băm bản tin và sau đó ký số lên giá trị băm. Lúc này thuật toán băm yêu cầu đầu vào là bản tin. *Hình 3.5* minh họa về mặt ngữ nghĩa cho tình huống này. Hàm dư thừa R không còn quan trọng đối với tính bảo mật của hệ thống nữa, và có thể là một hàm ánh xạ *1- 1* từ M_h tới M_S:



Hình 1.0.8 Hệ thống chữ ký số với phụ lục nhận được từ một hệ thống hồi phục bản tin

.

1.6 Vai trò của chữ ký điện tử trong Chính phủ điện tử và hành chính điện tử

Về giá trị pháp lý của chữ ký điện tử, theo khoản 1, Điều 21, Luật Giao dịch điện tử năm 2005, chữ ký điện tử được tạo lập dưới dạng từ, chữ, số, ký hiệu, âm thanh hoặc các hình thức khác bằng phương tiện điện tử, gắn liền hoặc kết hợp một cách lô-gíc với thông điệp dữ liệu, có khả năng xác nhận người ký thông điệp dữ liệu và xác nhận sự chấp thuận của người đó đối với nội dung thông điệp dữ liệu được ký. Như vậy, chữ ký điện tử là dạng thông tin đi kèm dữ liệu nhằm mục đích xác định người ký của dữ liệu đó và xác nhận sự chấp thuận của người đó đối với nội dung thông điệp dữ liệu được ký.

Trong hành chính điện tử, việc thực hiện các thủ tục hành chính cần các thông tin cá nhân của người dùng như: Số CMND/CCCD, họ tên, địa chỉ thường trú,... hầu hết là các thông tin nhạy cảm, cần được bảo mật. Đặc biệt là số CMND/ CCCD, các thủ tục hành chính nào trong thực tế cũng đều liên quan đến số này. Hiện tại, việc tích hợp nhiều thông tin cá nhân trong CCCD cũng tiềm ẩn rủi ro lộ lọt nhiều thông tin hơn ra bên ngoài. Sử dụng môi trường mạng để thực hiện thủ tục hành chính từ xa đòi hỏi tính bảo mật rất cao, đặc biệt trong quá trình truyền dẫn thông tin đến nơi cần xử lý. Trong hoạt động thực tiễn, chữ ký điện tử cũng có vai trò bảo mật những thông tin nhạy cảm này, đảm bảo quá trình nhận gửi thông tin, xác thực toàn vẹn dữ liệu của thủ tục hành chính điện tử.

Việc triển khai ứng dụng chữ ký số trong hoạt động của hành chính điện tử nhằm đáp ứng nhu cầu trao đổi, gửi nhận văn bản điện tử, hồ sơ, tài liệu điện tử trong các cơ quan nhà nước. Đây được xem là giải pháp hiện đại, thuận tiện, nhanh, an toàn, hiệu quả tích cực trong xây dựng chính quyền điện tử, nâng cao hiệu quả cải cách hành chính của tỉnh. Ứng dụng chữ ký số mang lại nhiều hiệu quả như giảm chi phí giấy, mực, gửi văn bản qua đường bưu điện; giảm công lao động, bảo mật dữ liệu cá nhân, dữ liệu chuyên môn. Việc triển khai ứng dụng chữ ký số trong việc gửi, nhận văn bản điện tử trong cơ quan nhà

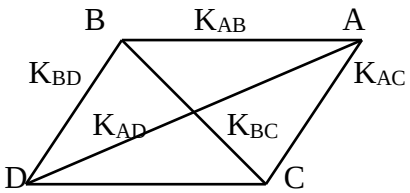
nước mang lại hiệu quả thiết thực trong công tác quản lý, điều hành. Chứng thực điện tử, chữ ký số chuyên dùng được ứng dụng hiệu quả vào hoạt động tác nghiệp hành chính của cán bộ, công chức; nâng cao mức độ an toàn, bảo mật cho giao dịch điện tử giữa các cơ quan quản lý hành chính nhà nước trên môi trường mạng. Việc ứng dụng hiệu quả chữ ký số góp phần hiện đại hóa nền hành chính, thúc đẩy kinh tế - xã hội phát triển. Điều này giúp giảm chi phí, thời gian lưu trữ, tra cứu, gửi, nhận văn bản giấy giữa các đơn vị; thay đổi tác phong, lề lối làm việc, chuyển từ giải quyết công việc trên giấy tờ sang môi trường điện tử hiện đại, nhanh, gọn phục vụ người dân, doanh nghiệp tốt hơn"

Để ứng dụng được chữ ký điện tử, ta cần hiểu được nguyên lí hoạt động và cơ sở toán học của nó. Nhiều thuật toán chữ ký đã được nghiên cứu và công bố. Trong chương này đã trình bày một thuật toán được sử dụng rộng rãi nhất, do Viện tiêu chuẩn và công nghệ quốc gia Mỹ (the U.S. National Institute of Standards and Technology) đưa ra trong chuẩn chữ ký điện tử DSS. Đó là thuật toán chữ ký điện tử DSA sử dụng thuật toán băm SHA. Thuật toán này sẽ được dùng để xây dựng ứng dụng trong phần sau của đồ án.

1.7 Kỹ thuật mã hóa khóa công khai

Mã hóa khóa đối xứng đã và đang được sử dụng rất rộng rãi, tạo ra nhiều hệ thống liên lạc một cách an toàn qua mạng công cộng. Tuy nhiên, mã hóa khóa đối xứng gặp một số vấn đề, đặc biệt đối với các hệ thống lớn:

Vấn đề quản lý khóa (Tạo, lưu mật, trao chuyển …) là rất phức tạp và ngày càng khó khi sử dụng trong môi trường trao đổi tin giữa rất nhiều người dùng. Với số lượng user là n thì số lượng khóa cần tạo lập là n(n - 1)/2. Mỗi người dùng phải tạo và lưu (n-1) khóa bí mật để làm việc với (n-1) người khác trên mạng. Như vậy rất khó khăn và không an toàn khi n tăng lớn.



Vấn đề thứ hai là trên cơ sở mã đối xứng, không thể thiết lập được khái niệm chữ ký điện tử (mà thể hiện được các chức năng của chữ ký tay trong thực tế) và cũng do đó không có dịch vụ không thể phủ nhận được (non - repudiation) cho các giao dịch thương mại trên mạng.

Xuất phát từ sự hạn chế của phương pháp mã hoá đối xứng, *mã khóa công khai* hay *mã hoá bất đối xứng* (*asymmetric algorithm*) đã ra đời và nhanh chóng tạo ra một cuộc cách mạng trong toàn bộ lịch sử mã hoá.

1.7.1 Mã khóa công khai

Diffie và Hellman trong các công trình của mình (1975 - 1976) đã đề xuất một loại hệ mã với nguyên tắc mới gọi là hệ mã với khóa công khai (public key cryptosystems), trong đó hệ mã được gắn với một người sử dụng (user) nhất định chứ không phải gắn với một cuộc truyền tin giữa một cặp người dùng.

Trong hệ thống mã hóa khóa công khai, mỗi user có hai khóa , một được gọi là khóa bí mật (secret key hay private key) và một được gọi là khóa công

khai (public key). khóa thứ nhất chỉ mình user biết và giữ bí mật, khóa thứ hai được phổ biến công khai. khóa thứ nhất thường đi liền với thuật toán giải mã, còn khóa thứ hai thường đi liền với thuật toán sinh mã, tuy nhiên điều đó không phải là bắt buộc. ký hiệu z là khóa riêng và Z là khóa công khai.

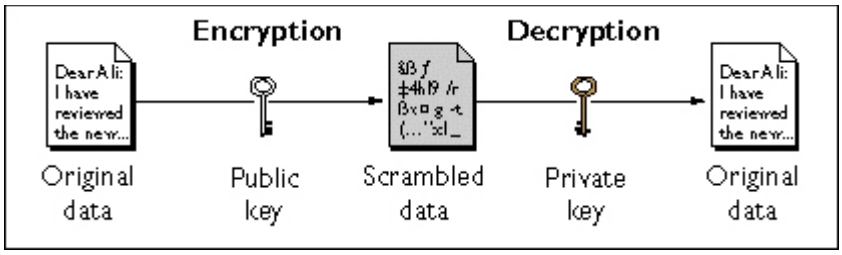
Hoạt động của chúng là đối xứng:

$$X = D(z, E(Z,X)) \qquad (1)$$

Và $$X = E(Z, D(z,X)) \qquad (2)$$

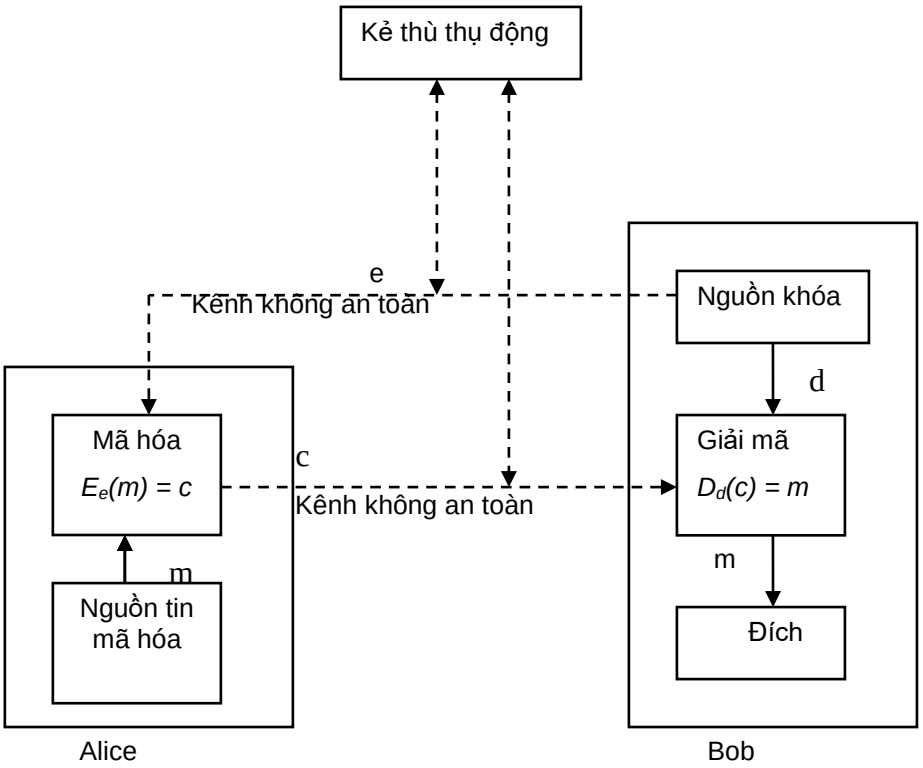
Trong đó (1) được sử dụng cho truyền tin mật: B, C, D muốn gửi tin cho A chỉ việc mã hóa thông tin với khóa công khai (Z_A) của A rồi gửi đi. Chỉ có A mới có thể có khóa riêng để giải mã (z_A) và đọc được tin, E dù nghe trộm cũng không thể giải mã để lấy được tin vì không có khóa z_A.

Còn (2) sẽ được sử dụng để xây dựng các hệ chữ ký điện tử (Ký bằng $E(Z_A)$ và kiểm định bằng $D(z_A)$).



Hình 2.0.9 Sơ đồ minh hoạ Public-key Cryptography

Một truyền thông hai phía sử dụng mã hóa khóa đối xứng có thể mô tả bằng sơ đồ khối như hình sau [1]:



Hình 2.0.10 Mô hình truyền thông hai phía sử dụng mã hóa khóa công khai

1.7.2 Nguyên tắc cấu tạo một hệ khóa công khai

Một hệ mã PKC có thể được tạo dựng trên cơ sở sử dụng một hàm kiểu one – way (một chiều). Một hàm f được gọi là one – way nếu:

a. Đối với mọi X tính ra Y = f(X) là dễ dàng;

b. Khi biết Y rất khó để tính ra X.

Cần một hàm one – way đặc biệt mà có trang bị một trap – door (cửa bẫy), sao cho nếu biết trap – door thì việc tính X khi biết f(X) là dễ dàng còn ngược lại sẽ khó khăn.

Một hàm one – way có trap – door như thế có thể dùng để tạo một hệ mã PKC. Lấy E_z (hàm sinh mã) là hàm one – way có trap – door. Trap – door chính là khóa bí mật, mà nếu biết nó thì có thể dễ dàng tính được nghịch đảo của E_z tức là biết D_z, còn nếu không biết thì rất khó tính được.

Những giải thuật khóa công khai dựa vào khóa công khai để mã hoá và khóa bí mật có liên quan để giải mã. Như vậy, mỗi người tham gia vào hệ thống đều có hai khóa: thuật toán mã hoá E và thuật toán giải mã D.

Những giải thuật này có những đặc tính quan trọng sau:

- ✔ D(E(P)) = P (Plaintext - bản tin mã hoá)
- ✔ Khối lượng tính toán không khả thi để xác định khóa giải mã d khi chỉ biết giải thuật mật mã và khóa mã hóa e.
- ✔ Không thể phát hiện khóa giải mã d từ bản tin P chọn sẵn
- ✔ Trong một số giải thuật như RSA còn có đặc điểm: hoặc một trong hai khóa liên quan có thể được sử dụng cho mã hóa còn khóa kia được dùng cho giải mã.
- ✔ Ngoài ra có một đặc tính khác, đó là việc tính toán cho các bên tạo cặp khóa mã hoá - giải mã, việc tính toán khi biết bản tin cần mã hoá và khóa công khai của bên kýa để tạo bản mã tương ứng, việc sử dụng bản tin đã được mã hoá và khóa bí mật của mình để khôi phục bản tin ban đầu phải dễ dàng thực hiện và với tốc độ cao.

Các bước cần thiết trong quá trình mã hóa khóa công khai:

- ✔ Mỗi hệ thống đầu cuối trong mạng tạo ra một cặp khóa để dùng cho mã hóa và giải mã bản tin mà nó sẽ nhận.
- ✔ Mỗi hệ thống công bố rộng rãi khóa mã hóa bằng cách đặt khóa vào một thanh ghi hay một file công khai. Đây là khóa công khai (*public key*), khóa bí mật d được giữ riêng (*private key*).
- ✔ Nếu A muốn gửi một bản tin P tới B thì A mã hóa P bằng khóa công khai e_B của B rồi gửi kết quả cho B.
- ✔ Khi B nhận bản mã, B giải mã bằng khóa bí mật d_B của mình. Không một người nào khác có thể giải được bản mã này bởi vì chỉ có mình B biết khóa bí mật đó thôi.

Với cách tiếp cận này, tất cả những người tham gia có thể truy xuất khóa công khai. khóa riêng được tạo ra bởi từng cá nhân, vì vậy không bao giờ được công bố. Ở bất kỳ thời điểm nào, hệ thống cũng có thể thay đổi khóa riêng của nó và công bố khóa công khai tương ứng để thay thế khóa công khai cũ.

1.7.3 Mã hóa khóa công khai RSA

a. Bài toán phân tích số nguyên

Bài toán phân tích số nguyên là một trong những bài toán được quan tâm đến những năm gần đây, độ an toàn của nhiều kỹ thuật mật mã phụ thuộc vào sự không giải nổi của bài toán này như hệ mật mã RSA, lược đồ chữ ký RSA…

Bài toán 1 (Bài toán phân tích số nguyên): Cho một số nguyên dương N, tìm các thừa số nguyên tố của N. Nghĩa là, $N = p_1^{e1}, p_2^{e2}, \ldots p_k^{ek}$, với p_i là những số nguyên tố phân biệt và $e_i \geq 1$ (với i = 1,..., k).

Bài toán này được tin tưởng là khó giải khi N là một số nguyên lớn, có nhiều thuật toán để giải bài toán này. Nhưng hiện nay vẫn chưa có thuật toán nào hiệu quả để phân tích số nguyên N có khoảng 232 chữ số thập phân (768-bits) trở lên.

Bài toán 2 (Bài toán RSA): Cho số nguyên dương N là tích của hai số nguyên tố phân biệt p và q (N = p * q), số nguyên e sao cho thỏa mãn gcd(e, (p – 1) * (q – 1)) = 1, và số nguyên c. Tìm một số nguyên m sao cho $m^e \equiv c \pmod N$.

Rõ ràng bài toán RSA cũng có độ khó tương tự như bài toán phân tích số nguyên, nhưng nó dễ dàng được giải nếu như biết được hai số nguyên tố p và q.

b. Mô tả các quá trình tạo khoá, mã hoá và giải mã

*** Tạo khóa**

Để sử dụng được hệ mật mã khóa công khai RSA, trước tiên mỗi người phải tạo riêng cho mình một cặp khóa gồm khóa công khai, và khóa riêng như sau:

- Tạo hai số nguyên tố phân biệt p và q lớn, sao cho bài toán phân tích thật sự là khó giải (kích cỡ mỗi số khoảng 512 bits → 1024 bits).
- Tính N = p* q và ϕ(N) = (p – 1) * (q – 1), (*ϕ(N) là Euluer Totient Function*)

- Chọn một số nguyên ngẫu nhiên e sao cho $1 < e < \phi(N)$ và gcd(e, $\phi(N)) = 1$
- Sử dụng thuật toán Euclide mở rộng, để tính số nguyên d duy nhất, sao cho $0 < d < \phi(N)$ và $e * d \equiv 1 \bmod \phi(N)$ (d là nghịch đảo của e modulo N)
- Công bố hai số (e, N) làm khóa công khai, còn (d, N) được giữ bí mật làm khóa riêng. Các số nguyên tố p, q sẽ bị xóa khi kết thúc quá trình tạo khóa.

- Mã hóa:

Hệ RSA là một hệ mật mã điển hình về kiểu mã hóa khối. Nghĩa là, thông điệp được chia thành nhiều khối (hoặc chuỗi) có chiều dài cố định, và mỗi khối sẽ được mã hóa riêng. Giả sử để gửi thông điệp bí mật M cho người B trong nhóm gửi thông tin an toàn, người A phải thực hiện các bước như sau:

- Lấy khóa công khai đích thực của người nhận B (e, N).
- Thực hiện một thuật toán để biến đổi thông điệp **m** thành những số nguyên M_i tương ứng sao cho $M_i < N$, (i = 1,…, k). ví dụ như phép biến đổi sau:

– Biến đổi các ký tự trong thông điệp **m** thành các số nguyên theo qui tắc: $\cup \leftrightarrow 00$, A $\leftrightarrow$ 01, B $\leftrightarrow$ 02,…, Z $\leftrightarrow$ 26 (với $\cup$ là khoảng trắng).

– Chia thông điệp vừa biến đổi thành k nhóm có chiều dài bằng nhau, mỗi nhóm biểu diễn một số nguyên $M_i \in \{0,\ldots, N-1\}$ (với $1 \le i \le k$).

- Thực hiện mã hóa lần lượt cho từng số $M_i \rightarrow C_i$ bằng cách tính:

$C_i = E_{ke}(M_i) = M_i^e \pmod N$.

Tập các số nguyên $\{C_1, C_2,...,C_k\}$ là bản mã để gửi đến người nhận B.

- Giải mã:

Để thực hiện quá trình giải mã, khôi phục lại nội dung của thông điệp M từ bản mã C nhận được, người nhận B sẽ thực hiện các bước như sau:

- Thực hiện giải mã lần lượt cho từng số nguyên $C_i \rightarrow M_i$ bằng cách tính:

$M_i = D(C_i) = C_i^d \pmod N$ với $0 \le M_i < N$, (d là khoá bí mật của B).

- Thực hiện phép biến đổi ngược lại từ các số M_i thành các chuỗi ký tự tương ứng, để khôi phục lại nội dung thông điệp M ban đầu.

Bảng 3: Bảng tóm tắt các bước tạo khoá, mã hoá, giải mã của hệ RSA

Tạo khoá:

- Tạo 2 số nguyên tố lớn p và q
- Tính N = p * q và
  Tính $\phi(N) = (p-1) * (q-1)$.
- Chọn $1<e<\phi(N)$: $gcd(\phi(N), e) = 1$.
- Tính $d = e^{-1} \bmod \phi(N)$

(dùng thuật toán Euclidean mở rộng).

Mã hóa: khối bản rõ M < N

- Tính: $\mathbf{C = M^e \bmod N}$

Gửi khối bản mã (số nguyên) C đến người nhận

Giải mã: khối bản mã C < N

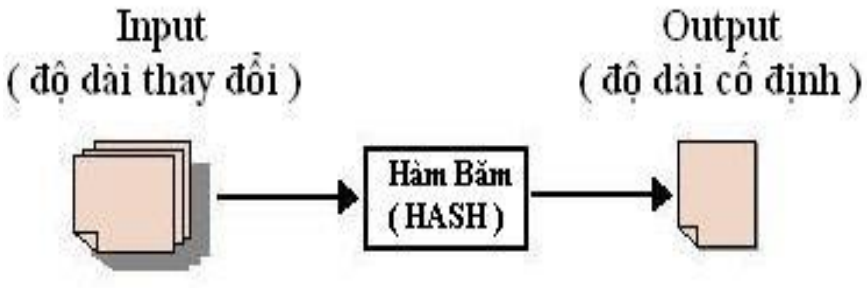
- Tính: $\mathbf{M = C^d \bmod N}$

khôi phục lại khối bản rõ (số nguyên) M ban đầu

- **Khóa công khai:** $k_e = (e, N)$
- **Khóa riêng:** $k_d = (d, N)$

*** Hàm băm**

Hàm băm (hash), là một thuật toán dùng để biến một thông điệp **M** ở đầu vào (input) có chiều dài thay đổi bất kỳ, thành một giá trị **h** ở đầu ra (output) có chiều dài cố định, **h** được gọi là giá trị **hash**. Hàm băm được sử dụng trong rất nhiều lĩnh vực tính toán, mật mã là một trong số đó.



Hình 2.5: Sơ đồ minh họa hàm băm (HASH)

◆ Hai ứng dụng phổ biến nhất của hàm hash trong lĩnh vực mật mã là:

- Nén thông điệp thành một khối nhỏ có chiều dài xác định, phục vụ cho các lược đồ chữ ký điện tử, khối dữ liệu nhỏ này gọi là thông điệp thu gọn

(Message Digest). Ví dụ như chữ ký điện tử DSA (Digital Signature Algorithm) dùng hàm băm SHA-1 để tạo thông điệp thu gọn dài 160-bits.

- Kiểm tra tính toàn vẹn dữ liệu (Data Integrity), nghĩa là kiểm tra xem dữ liệu có bị thay đổi trên đường truyền hay không, bằng cách tạo mã chứng thực thông điệp MAC (Message Authentication Code).

* Yêu cầu của một hàm băm

◆ Hàm hash dùng trong lĩnh vực mật mã phải thỏa các tiêu chuẩn sau:

- Thông điệp (Message) ở đầu vào có chiều dài bất kỳ.
- Thông điệp thu gọn (Message digest) đầu ra có chiều dài cố định (đủ nhỏ).
- Hàm băm H(x) dễ dàng tính toán cho mọi thông điệp x
- Hàm băm H(x) là hàm một chiều (one-way-function): cho trước một giá trị hash **h** thì khó tính toán để tìm ra thông điệp ở đầu vào x sao cho H(x) = h.
- Đụng độ (collision-free): hàm băm H(x) có hai cấp đụng độ là:
- Đụng độ cấp độ yếu (Weakly collision-free): cho trước thông điệp **x**, không thể tính toán tìm ra một thông điệp **y** khác **x** mà H(x) = H(y).
- Đụng độ cấp độ mạnh (Strongly collision-free): không thể tính toán để tìm ra hai thông điệp bất kỳ **x** và **y** khác nhau, mà có cùng giá trị **hash**, nghĩa là H(x) = H(y).

*** Ứng dụng hàm băm**

Các hàm băm được ứng dụng trong nhiều lĩnh vực, chúng thường được thiết kế phù hợp với từng ứng dụng. Ví dụ, các hàm băm mật mã học giả thiết sự tồn tại của một đối phương – người có thể cố tình tìm các dữ liệu vào với cùng một giá trị băm. Một hàm băm tốt là một phép biến đổi "một chiều", nghĩa là không có một phương pháp thực tiễn để tính toán được dữ liệu vào nào đó tương ứng với giá trị băm mong muốn, khi đó việc giả mạo sẽ rất khó khăn. Một hàm một chiều mật mã học điển hình không có tính chất hàm đơn ánh và tạo nên một hàm băm hiệu quả; một hàm trapdoor mật mã học điển hình là hàm đơn ánh và tạo nên một hàm ngẫu nhiên hiệu quả.

Bảng băm, một ứng dụng quan trọng của các hàm băm, cho phép tra cứu nhanh một bản ghi dữ liệu nếu cho trước khóa của bản ghi đó (Lưu ý: các khóa này thường không bí mật như trong mật mã học, nhưng cả hai đều được dùng để "mở khóa" hoặc để truy nhập thông tin.) Ví dụ, các khóa trong một từ điển điện tử Anh-Anh có thể là các từ tiếng Anh, các bản ghi tương ứng với chúng chứa các định nghĩa. Trong trường hợp này, hàm băm phải ánh xạ các xâu chữ cái tới các chỉ mục của mảng nội bộ của bảng băm.

Các hàm băm dành cho việc phát hiện và sửa lỗi tập trung phân biệt các trường hợp mà dữ liệu đã bị làm nhiễu bởi các quá trình ngẫu nhiên. Khi các hàm băm được dùng cho các giá trị tổng kiểm, giá trị băm tương đối nhỏ có thể được dùng để kiểm chứng rằng một file dữ liệu có kích thước tùy ý chưa bị sửa đổi. Hàm băm được dùng để phát hiện lỗi truyền dữ liệu. Tại nơi gửi, hàm băm được tính cho dữ liệu được gửi, giá trị băm này được gửi cùng dữ liệu. Tại đầu nhận, hàm băm lại được tính lần nữa, nếu các giá trị băm không trùng nhau thì lỗi đã xảy ra ở đâu đó trong quá trình truyền. Việc này được gọi là kiểm tra dư (redundancy check).

Các hàm băm còn được ứng dụng trong việc nhận dạng âm thanh, chẳng hạn như xác định xem một file MP3 có khớp với một file trong danh sách một loại các file khác hay không.

c. Chữ ký số

Trong giao dịch điện tử nói chung và thương mại điện tử nói riêng, quá trình trao đổi thông tin tương tác giữa các thành viên, đòi hỏi phải có một cơ chế hay hệ thống xác định nguồn gốc chủ sở hữu của thông tin. Giống như trong lĩnh vực tài liệu thông thường, nếu như chữ ký viết tay là để chứng minh tác giả hay người công nhận nội dung của tài liệu, thì lĩnh vực tài liệu điện tử cũng có một tiêu chuẩn như vậy về "chữ ký", gọi là chữ ký điện tử (digital signature).

Chữ ký điện tử là một đoạn dữ liệu ngắn đính kèm với văn bản gốc để chứng thực tác giả của văn bản và giúp người nhận kiểm tra tính toàn vẹn của nội dung văn bản gốc. Về nguyên tắc của chữ ký điện tử cũng gần như chữ ký

thông thường, ví dụ như nếu người A muốn gửi thông điệp cho người B, thì A sẽ gửi chữ ký cùng với thông điệp của mình cho B. Khi nhận được thông điệp và chữ ký, bằng cách nào đó để B có thể xác định chữ ký kèm theo thông điệp có phải của người A hay không. Điểm khác biệt giữa chữ ký điện tử và chữ ký thông thường là: chữ ký thông thường thì nằm bên trong thông điệp, và chữ ký của một người là luôn giống nhau ở mọi thông điệp, còn chữ ký điện tử thì được gửi kèm với thông điệp nhưng tách biệt, và chữ ký của một người cho các thông điệp khác nhau là hoàn toàn khác nhau.

** Yêu cầu của một hệ thống chữ ký điện tử*

- Hệ thống chữ ký điện tử cần thỏa mãn các yêu cầu sau :

• Tính an toàn (security): chữ ký không thể làm giả được nếu không biết thông tin bí mật (private key) để tạo ra chữ ký.

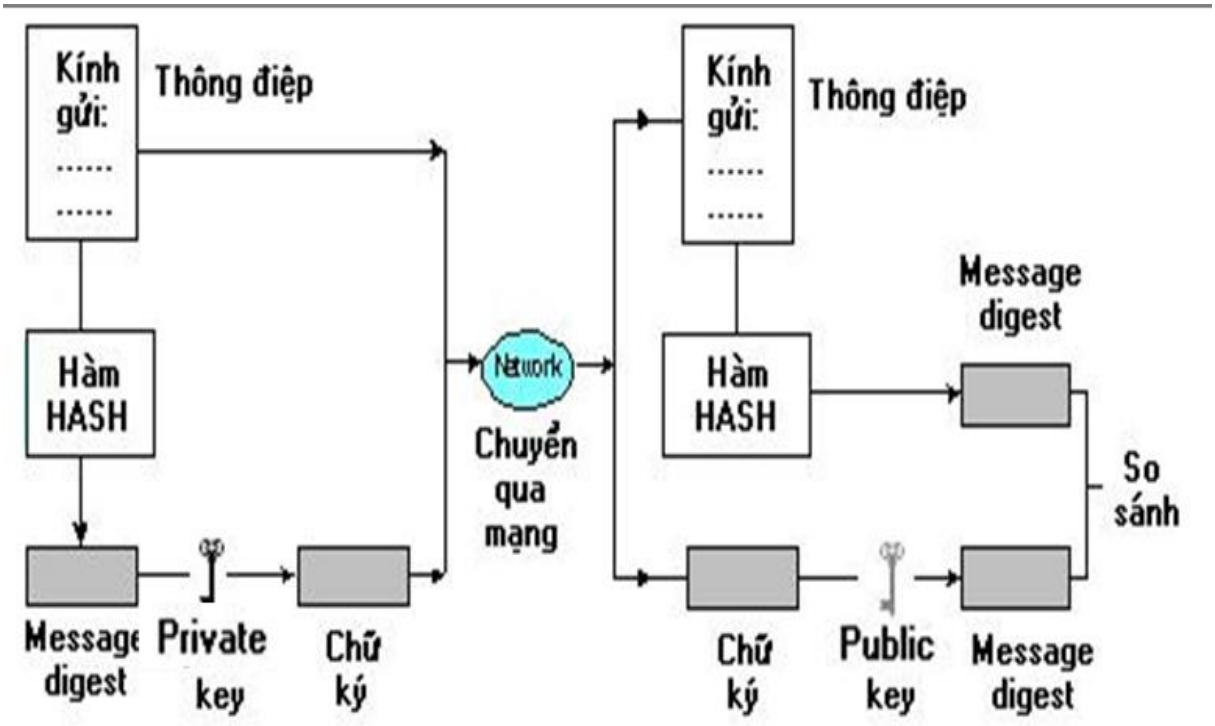
• Tính hiệu quả (performance): ký và xác nhận chữ ký nhanh, dễ dàng.

• Chống nhân bản chữ ký: chữ ký không thể sao chép để dùng lại sau này. Ví dụ A ký chứng nhận cho phép B rút một số tiền, cần phải có cách nào đó để B không thể dùng chứng nhận này lại lần thứ hai.

• Tính không thể phủ nhận (non-repudiation): người ký không thể phủ nhận chữ ký của mình khi đã ký vào tài liệu.

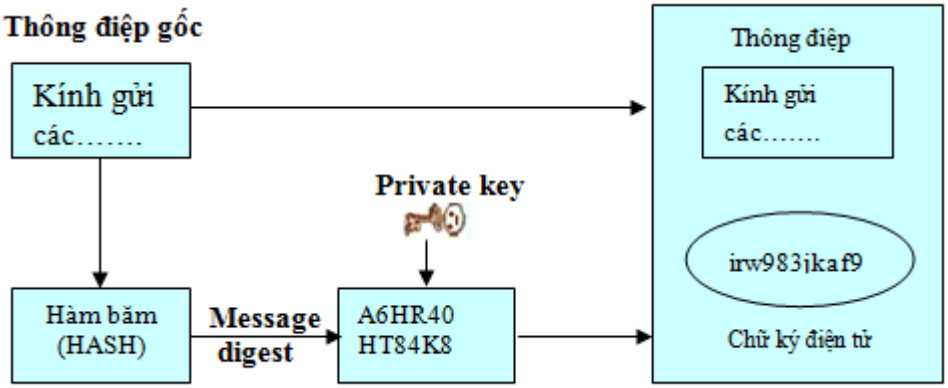
** Lược đồ chung của chữ ký điện tử*

Một lược đồ chữ ký điện tử bao gồm 2 thành phần: thuật toán ký, và thuật toán xác nhận chữ ký. Nghĩa là, nếu người A muốn gửi cho người B một thông điệp x, thì A dùng một thuật toán và khoá bí mật của mình để tạo chữ ký $y = sign_{kdA}(x)$, rồi gửi cả thông điệp x lẫn chữ ký y cho B. Sau khi nhận được thông điệp x và chữ ký y. B sẽ dùng thuật toán cùng với khóa công khai của A để xác nhận chữ ký y có phải là chữ ký của A cho thông điệp x này hay không $verify_{keA}(x, y) = \{true, false\}$.



Hình 2.6: Mô hình tổng quát của chữ ký điện tử

- Các bước thực hiện tạo chữ ký điện tử:
  - Người gửi sử dụng một hàm băm, để biến đổi thông điệp x thành một thông điệp thu gọn (message digest) **h** có chiều dài cố định: **h** = Hash(x).
  - Người gửi dùng khoá riêng k_d của mình mã hóa chuỗi **h**: y = E_{kd}(h), kết quả y thu được chính là chữ ký điện tử (digital signature) đối với thông điệp x.
  - Cuối cùng chữ ký **y** có thể được nối vào cuối thông điệp **x** hoặc lưu vào một file gửi kèm với thông điệp. Sau khi đã ký nhận mọi sự thay đổi của thông điệp sẽ được phát hiện trong quá trình kiểm tra xác nhận chữ ký. Điều này đảm bảo cho người nhận tin rằng thông điệp họ nhận được đích thực là của người gửi và nội dung thông điệp hoàn toàn không bị thay đổi.



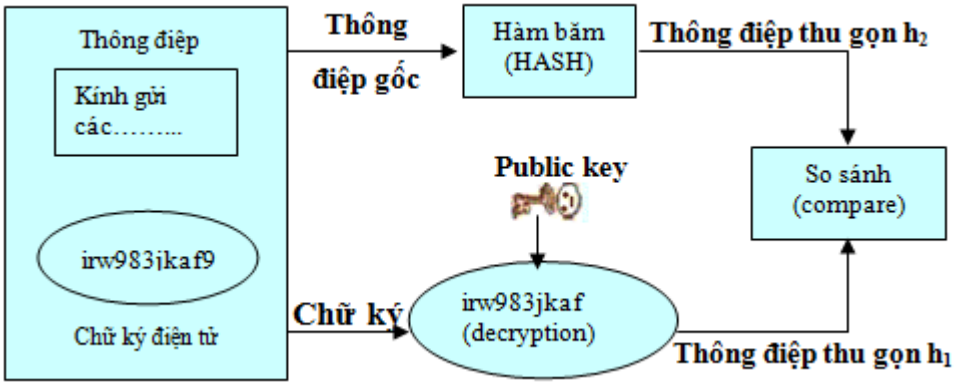
Hình 2.7: Sơ đồ minh họa các bước tạo chữ ký điện tử

◆ Các bước thực hiện kiểm tra tính đúng của chữ ký điện tử:

– Người nhận dùng khoá công khai (key public) k_e của người gửi để giải mã chữ ký điện tử y vừa nhận, khôi phục lại thông điệp thu gọn: $\mathbf{h_1} = D_{ke}(y)$.

– Người nhận sử dụng hàm băm giống như người gửi để biến đổi thông điệp x nhận được thành thông điệp thu gọn: $\mathbf{h_2}$ = Hash(x).

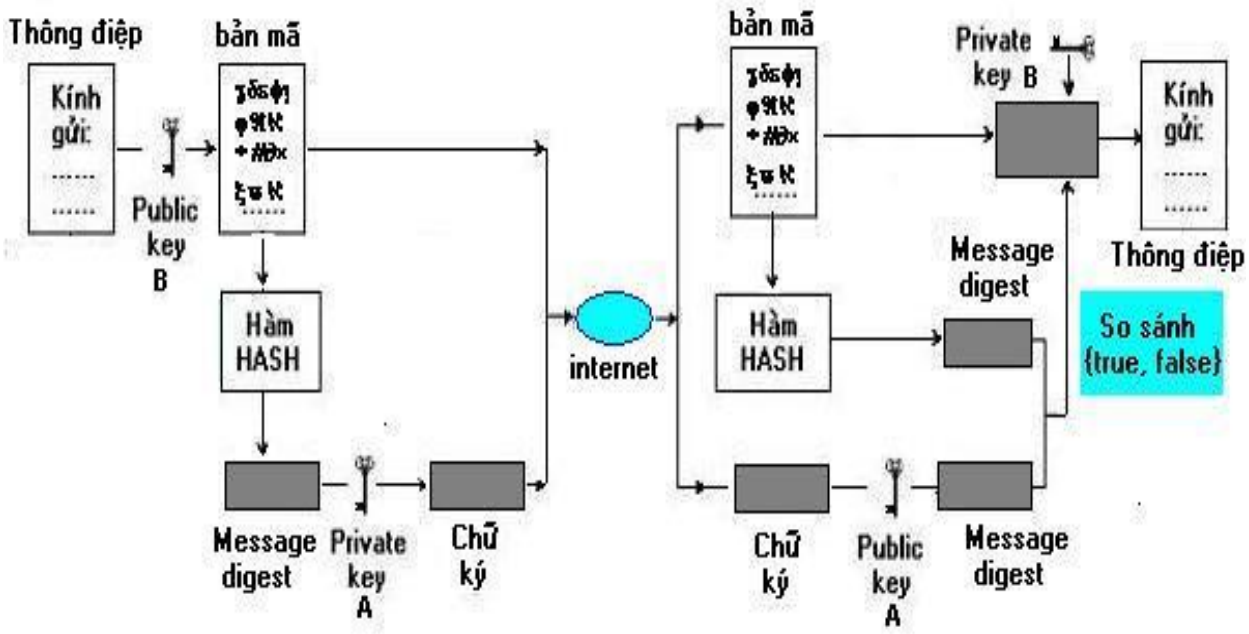
– So sánh kết quả, nếu $h_1 = h_2$ thì chấp nhận chữ ký là của người gửi. Ngược lại, chữ ký trên thông điệp không được chấp nhận.



Hình 2.8: Sơ đồ minh họa các bước kiểm tra chữ ký điện tử

Nhận xét: Lược đồ chữ ký điện tử theo kiểu này, cho phép xác định được chủ nhân đích thực của thông điệp, đồng thời đảm bảo nội dung của thông điệp không bị sửa đổi hay làm giả mạo bởi người khác trong quá trình truyền đi trên mạng. Nhưng nội dung của thông điệp có thể đọc được, do trong lược đồ này chỉ thực hiện mã hóa một khối dữ liệu nhỏ đặt trưng cho thông điệp mà không

mã hoá toàn bộ thông điệp, điều này không phù hợp với nhu cầu trao đổi các thông tin bí mật thông qua internet. Vì vậy để có thể đảm bảo được bí mật của nội dung, người gửi cần thực hiện quá trình mã hóa thông điệp bằng khóa công khai của người nhận, trước khi thực hiện ký xác nhận vào tài liệu, và người nhận phải thực hiện thêm một bước giải mã thông điệp bằng khoá riêng của mình sau khi kiểm tra đúng chữ ký của người gửi.



Hình 2.9: Mô hình chữ ký điện tử dùng quá trình mã hóa và giải mã

- Các bước thực hiện mã hoá và tạo chữ ký cho thông điệp

• Người gửi A mã hóa thông điệp x bằng khóa công khai của người nhận B: $C = E_{keB}(x)$. (k_{eB} là khoá công khai của người nhận B)

• Người gửi A thực hiện bước tạo chữ ký để xác nhận bản mã C với khóa riêng của mình: $y = Sig_{kdA}(C)$.

• Gửi chữ ký **y** và bản mã C đến người nhận B.

- Mô tả các bước kiểm tra chữ ký và giải mã thông điệp

• Người nhận kiểm tra chữ ký trên thông điệp bằng khóa công khai của người gửi A: $ver_{keA}(C, y) = \{true, false\}$.

- Nếu bước kiểm tra ở trên là đúng (true), thì người nhận tiếp tục thực hiện quá trình giải mã C với khóa riêng của mình: $x = D_{kdB}(C)$, để khôi phục lại thông điệp x. Ngược lại chữ ký của A đối với tài liệu x là không hợp lệ.

** Ứng dụng chữ ký điện tử*

Một e-mail có thể được ký bằng chữ ký điện tử và đảm bảo người nhận có thể chắc chắn rằng email đó đúng là của người gửi, chứ không phải e-mail giả mạo. Để đảm bảo được yếu tố này, người gửi và người nhận đều phải sử dụng cùng một hệ thống chứng thư số.

Vậy vai trò trong **chữ ký điện tử** của chứng thư số là gì? Dịch vụ chứng thư số thường được sử dụng nhiều trong các hoạt động giao dịch thương mại điện tử, đặc biệt trong thanh toán trực tuyến của ngân hàng.

Người dùng, ngoài cách bảo mật thông thường bằng mật khẩu, cũng cần dùng một chứng thư số cá nhân để xác định danh tính của mình, xác nhận các hoạt động giao dịch của mình tại ngân hàng. Chứng thực số sẽ giúp ngân hàng đảm bảo các khách hàng không thể chối bỏ các giao dịch của mình.

Các hoạt động liên ngân hàng như thanh toán, chuyển khoản…trong giao dịch điện tử cũng đều phải sử dụng chứng thực số để xác định rõ danh tính của các bên tham gia, trách nhiệm của các bên trong từng loại giao dịch. Đây là quy trình bảo mật quan trọng, là cơ sở pháp lý để căn cứ khi thực hiện các hoạt động giao dịch trực tuyến.

Không chỉ nằm trong lĩnh vực thương mại điện tử, chứng thư số hiện còn được sử dụng như một dạng của chứng minh thư nhân dân. Tại các nước phát triển, chứng thư số (CA) được tích hợp vào các con chíp nhớ nằm trong thẻ tín dụng để tăng khả năng bảo mật, chống giả mạo, cho phép chủ thẻ xác minh danh tính của mình trên các hệ thống khác nhau như xe bus, thẻ rút tiền ATM, hộ chiếu điện tử tại các cửa khẩu, kiểm soát hải quan …

Chữ ký điện tử dường như đã là một phần không thể thiếu của các doanh nghiệp hiện đại, muốn phát triển nhanh và xa hơn

** Lược đồ chữ ký điện tử RSA*

Hệ mật mã khóa công khai RSA cũng có thể được sử dụng để cung cấp một hệ thống chữ ký điện tử bằng cách đảo ngược vai trò của quá trình mã hóa và giải mã. Muốn thực hiện lược đồ chữ ký điện tử RSA, mỗi người sử dụng phải tạo một cặp khóa, bao gồm khóa công khai và khóa riêng giống như trong lược đồ mã hóa và giải mã RSA, đồng thời thống nhất sử dụng cùng một hàm băm H(x). Giả sử để tạo chữ ký cho thông điệp (tài liệu) **m** người sử dụng A thực hiện như sau :

- Tính thông điệp thu gọn M = H(**m**) (M là duy nhất đối với thông điệp **m**).
- Tính S = $Sign_{Kd}$ (M) = M^d mod N (với d là khóa bí mật của người ký A).
- Kết quả S thu được chính là chữ ký của A đối với thông điệp **m**.

Khi kiểm tra chữ ký của tài liệu nhận được người sử dụng B thực hiện như sau:

- Lấy khóa công khai đích thực của người ký A (N, e) (ở tại thư mục chung).
- Kiểm tra chữ ký S ≤ N; nếu không thì từ chối chữ ký.
- Tính M’ = S^e mod N.
- Tính M = H(m).
- Chấp nhận chữ ký là đúng của người gửi, nếu và chỉ nếu M □ M’.

Nếu quá trình kiểm tra chữ ký đúng (Ver_K(**m**, S) = true) thì người nhận B chắc chắn rằng thông điệp **m** đích thực là của người A gửi và nội dung thông điệp không bị thay đổi hay bị làm giả mạo bởi người khác khi truyền đi trên mạng.

** Tóm tắt và kết luận ứng dụng*

Lược đồ chữ ký RSA là lược đồ được dùng phổ biến nhất trong các ứng dụng bảo mật do có độ an toàn và hiệu quả thực hiện tốt nhất hiện nay. Các thuật toán cũng đơn giản, và dễ hiện thực.

Lược đồ chữ ký điện tử RSA được chọn để tích hợp vào hệ thống bảo vệ an toàn thư điện tử của đề tài. Kèm theo với lược đồ chữ ký RSA là thuật băm MD5 cũng được chọn để phù hợp cho yêu cầu tạo thông điệp thu gọn (message

digest) dài 128-bits từ thông điệp đầu vào có chiều dài bất kỳ, phục vụ cho hệ thống chữ ký.

1.7.4 Giải thuật băm bảo mật SHA

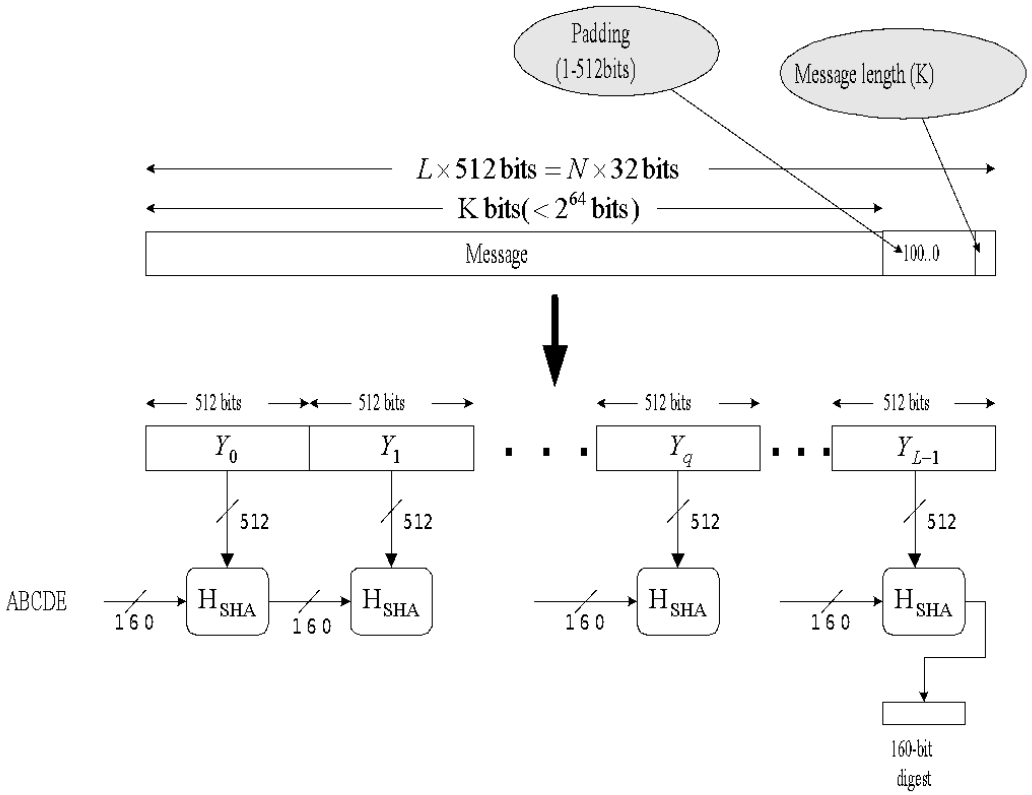
Chuẩn DSS cũng yêu cầu sử dụng thuật toán băm bảo mật SHA (*Secure hash algorithm*) trong thuật toán chữ ký số DSA [5].

Hàm băm (*Hash function*) thực hiện ánh xạ một bức điện có độ dài tuỳ ý đến một miếng băm có kích thước cố định. Thuật toán băm (*hash algorithm*) thông thường không có khóa đi kèm cho nên cũng giống như cách gọi khác của thuật toán mã đối xứng (là *thuật toán 1 khóa*) và thuật toán mã khóa công khai (là *thuật toán 2 khóa*), thuật toán băm còn có tên gọi là *thuật toán không khóa* (*no-key algorithm* hay *zero-key algorithm*).

Có nhiều hàm băm khác nhau như MD2, MD4, MD5. SHA do National Institute of Standart and Technology (NIST) phát triển được công bố năm 1993. SHA -1 là một phiên bản nâng cấp của SHA được đưa ra năm 1995[6].

Nội dung của thuật toán SHA – 1 như sau:

Giải thuật lấy một bản tin (*message*) là đầu vào với chiều dài tối đa nhỏ hơn 2^{64} bits và đầu ra là một *message digest* dài 160 bits. Đầu vào được xử lý theo những khối 512 bits. *Message digest*, ban đầu được thiết kế để sử dụng trong thuật toán DSA, cũng có thể là đầu vào cho RSA để tạo hoặc kiểm tra chữ ký cho đoạn tin trong hệ thống. Việc ký một *message digest* thường hiệu quả hơn việc ký trực tiếp vào bản thân *message* do kích thước của *message digest* thường nhỏ hơn rất nhiều so với kích thức của đoạn tin. Bên ký và bên kiểm tra chữ ký phải sử dụng cùng một giải thuật băm.

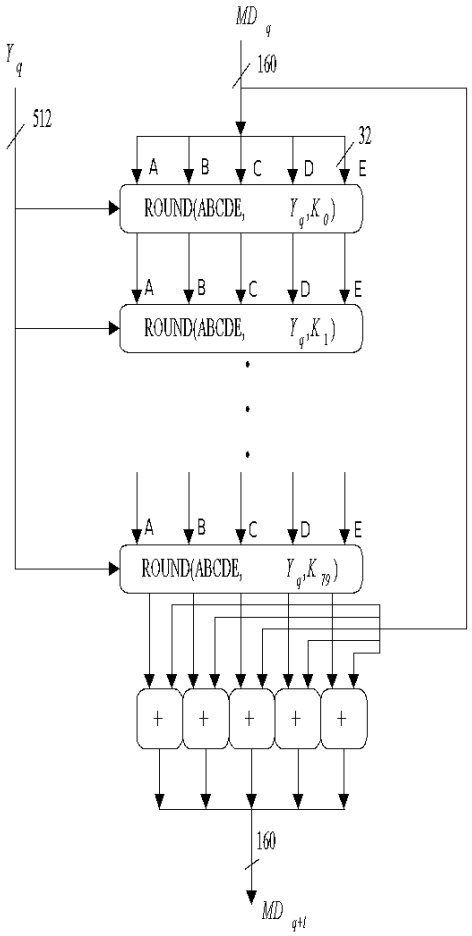


Hình 3.10: Quá trình tạo message của SHA-1

Quá trình xử lý bao gồm các bước sau:

- **Bước 1 (*Append padding bits*):** Đoạn tin được thêm vào sao cho chiều dài của nó đồng dư với 448 theo module 512 (chiều dài ≡ 448 mod 512). Phần đệm (padding) luôn được thêm vào thậm chí cả khi đoạn tin có độ dài cần thiết. Do đó, số lượng bit thêm vào nằm trong khóa ng 1 đến 512. Phần đệm bao gồm một bit 1 và một số các bit 0 cần thiết phía sau.
- **Bước 2 (*Append length*):** Một khối 64 bits được thêm vào đoạn tin. Khối này được coi như một số tự nhiên không dấu và chứa độ dài của đoạn tin ban đầu (trước khi thêm bit)
- **Bước 3 (*Initialize MD buffer*):** Một buffer 160 bits được sử dụng để lưu những giá trị trung gian và kết quả của hàm băm. Buffer có thể được thể hiện như 5 register 32-bit (A,B,C,D,E), tổng cộng là 160 bits.

- **Bước 4 (*Process message in 512-bits (16-word) block*):** Phần trọng yếu của giải thuật là một phần gồm 4 vòng, mỗi vòng có 20 bước. Đó là một module bao gồm 80 bước xử lý, module này được ký hiệu là H_{SHA} trong *Hình 3.11*. Mỗi vòng lấy đầu vào là khối 512-bit hiện tại đang được xử lý (Y_q) và buffer 160-bit chứa giá trị *ABCDE*, và cập nhật nội dung của buffer. Mỗi vòng cũng sử dụng một hằng số phụ K_t.



Hình 3.11: Quá trình xử lý SHA-1 cho một khối 512-bit (H_{SHA})

Giải thuật lấy Y_q và một giá trị băm trung gian MD_q làm đầu vào. MD_q được đặt vào trong buffer *ABCDE*. Đầu ra của bước thứ 80 được cộng với MD_q để tạo ra MD_{q+1}. Phép cộng được thực hiện độc lập đối với mỗi 5 word trong buffer với những word tương ứng trong MD_q , sử dụng phép cộng module 2^{32}.

- **Bước 5:** Sau khi tất cả L khối 512-bit được xử lý, đầu ra của giai đoạn thứ L là một *message digest* 160-bit.

Giải thuật SHA-1 có nhiều ưu điểm nổi trội hơn so với giải thuật MD5 dựa trên những phương diện quan trọng sau đây:

- ✔ *An toàn đối với tấn công dạng brute-force:* Sự khác biệt quan trọng nhất là *digest* của SHA-1(160 bits) dài hơn 32-bit so với *digest* của MD5(128 bits). Sử dụng công nghệ *brute-force*, độ khó khăn để tính toán ra một đoạn tin nào đó có *message digest* cho trước cần 2^{128} phép tính cho MD5 và 2^{160} cho SHA-1. Hơn nữa, sử dụng công nghệ *brute-force*, độ khó khăn để tạo ra 2 đoạn tin có cùng *message digest* cần 2^{64} phép tính cho MD5 và 2^{80} phép tính cho SHA-1. Do đó, SHA-1 được coi như mạnh hơn đối với những tấn công dạng *brute-force.*
- ✔ *An toàn đối với thám mã:* Người ta đã chứng minh được MD5 có thể bị tổn thương đối với tấn công dạng thám mã còn SHA-1 thì khó khăn hơn.

Chương 2
TÌM HIỂU VỀ HÀNH CHÍNH ĐIỆN TỬ

- Tìm hiểu về hành chính điện tử

Nội dung của chương 2 trình bày về lý thuyết mã hóa và giải mã, hai kỹ thuật dùng trong mật mã hóa là Mã khóa bí mật và Mã khóa công khai. Đối với mỗi phương pháp, chương này sẽ đi vào cụ thể thuật toán được sử dụng phổ biến nhất. Đó là thuật toán mã hóa khóa bí mật dùng chuẩn DES và thuật toán mã hóa khóa công khai RSA.

2.1 Tìm hiểu về chính phủ điện tử và hành chính điện tử

2.1.1. Chính phủ điện tử là gì?

Chính phủ điện tử (Electronic government – e-gov) hiện nay còn được hiểu theo nhiều nghĩa, điều đó phụ thuộc vào mức độ ứng dụng công nghệ thông tin vào hoạt động quản lý công, khả năng ưu tiên về chính sách, và khả năng ứng dụng công nghệ thông tin của từng chính phủ cụ thể. Theo nghĩa rộng thì e-gov là việc sử dụng Internet (online-trực tuyến) trong các hoạt động tương tác giữa chính phủ với các bộ phận khác nhau trong xã hội hoặc chỉ đơn giản là nâng cao năng lực ứng dụng công nghệ thông tin của nhân viên hành chính thuộc bộ máy công. Theo nghĩa cụ thể hơn thì "Chính phủ điện tử là việc sử dụng công nghệ thông tin, mà đặc biệt là Internet, như là một công cụ để hỗ trợ nhằm đạt đến một chính phủ hoạt động hiệu quả nhất".

Sự ra đời của chính phủ điện tử là một cuộc cách mạng trong tiến trình phát triển hành chính công. Chính phủ điện tử sẽ làm thay đổi phương thức sản xuất và cung ứng dịch vụ công nhằm phục vụ người dân tốt hơn. Chính phủ điện tử cũng đặt ra những thách thức lớn hơn bao giờ hết, đặc biệt là sự biến đổi không ngừng với tốc độ nhanh về công nghệ khiến các dự án công nghệ trong khu vực công luôn đứng trước nguy cơ lạc hậu.

Nhìn chung, các khái niệm về chính phủ điện tử đều coi đó là việc ứng dụng thành tựu khoa học công nghệ thông tin vào điều hành của chính phủ và tương tác của chính phủ đối với các thành tố khác trong xã hội như công dân, doanh nghiệp… nhằm phân phối dịch vụ trực tiếp tới khách hàng không giới hạn thời gian. Có thể rút ra một số đặc điểm chung về chính phủ điện tử như sau: Chính phủ điện tử là chính phủ sử dụng công nghệ thông tin và viễn thông để tự động hóa và triển khai các thủ tục hành chính. Chính phủ điện tử cho phép công dân có thể truy cập các thủ tục hành chính thông qua các phương tiện điện tử như internet, điện thoại di động, truyền hình tương tác… Chính phủ điện tử là chính

phủ làm việc với người dân 24/24 giờ, 7 ngày mỗi tuần, 365 ngày mỗi năm và người dân có thể thụ hưởng các dịch vụ công dù họ ở bất cứ đâu.

2.1.2. Hành chính điện tử

a. Hành chính điện tử là gì?

Hành chính điện tử là hình thức hành chính nhà nước sử dụng công nghệ thông tin và truyền thông (ICT) để thực hiện các hoạt động của mình, tập trung vào 3 mặt: quan hệ với người dân, hoạt động nội bộ và quan hệ với các hội đồng địa phương khác.

***Các nguyên tắc của quản trị điện tử**

Quản trị điện tử dựa trên các nguyên tắc sau:

- **Đa kênh** : quảng bá dịch vụ bằng cách cung cấp thông qua tất cả các kênh có sẵn cho người dân.
- **Công khai, minh bạch** về thủ tục hành chính: việc thông tin về thủ tục hành chính hiệu quả hơn.
- **Khả năng tiếp cận** : đảm bảo rằng mọi công dân có thể truy cập các dịch vụ và thông tin thông qua các thiết bị điện tử.
- **Hợp tác giữa các cơ quan hành chính nhà nước** : cho phép tương tác giữa các cơ quan hành chính và cung cấp các dịch vụ kết hợp cho công dân. Công nhận lẫn nhau của các tài liệu điện tử và hệ thống nhận dạng và xác thực.
- **Bảo mật** : yêu cầu việc cung cấp dịch vụ điện tử ít nhất phải có cùng mức độ bảo mật với các dịch vụ không được cung cấp dưới dạng điện tử. Mức độ bảo mật nên cho phép gia tăng các giao dịch điện tử với các lĩnh vực đặc biệt nhạy cảm với vấn đề này (công nhân chuyên nghiệp, các công ty).
- **Tính tương** xứng: chỉ yêu cầu các bảo đảm và các biện pháp an ninh thích hợp cho thủ tục được thực hiện. Công dân sẽ không được yêu cầu cung cấp thêm thông tin quá mức cần thiết.

- **Trách nhiệm và chất lượng** : tôn trọng những gì mà các cơ quan hành chính nhà nước cung cấp thông qua các thiết bị điện tử. Điều này có thể đòi hỏi phải xem xét lại các chính sách thông tin và truyền thông địa phương.
- **Tính trung lập về công nghệ** : tiến bộ trong việc sử dụng các tiêu chuẩn mở hoặc những tiêu chuẩn thường được công chúng sử dụng, tránh phụ thuộc vào các công cụ phần mềm với chi phí giấy phép trong quan hệ với người dân.

***Ưu điểm của quản trị điện tử**

Hành chính điện tử mang lại những lợi thế quan trọng, cho cả người dân và cho chính nền hành chính.

Đối với công dân:

- Tiếp cận các dịch vụ công 24 giờ, bảy ngày một tuần.
- Thủ tục đơn giản, nhanh chóng.
- Không cần phải đến cơ quan quản lý.

Đối với các cơ quan hành chính nhà nước:

- Cải thiện các dịch vụ và do đó hình ảnh của chính quyền.
- Cải thiện hiệu quả nội bộ.
- Tích hợp các kênh cung cấp dịch vụ khác nhau.
- Khuyến khích sử dụng chung các công nghệ mới.

b. Vai trò của hành chính điện tử

- Quản trị toàn diện: hành chính điện tử giúp xây dựng lòng tin giữa chính phủ và người dân, một yếu tố cần thiết trong quản trị tốt bằng cách sử dụng các chiến lược dựa trên internet để người dân tham gia vào quá trình chính sách, minh họa cho sự minh bạch và trách nhiệm giải trình của chính phủ.

- Thực hiện dễ dàng và nhanh chóng: Với chính phủ điện tử, thủ tục giấy tờ đã được thực hiện rất đơn giản và trực quan. Điều này tạo điều kiện thuận lợi cho việc chia sẻ thông tin và ý tưởng giữa tất cả các cơ quan chính phủ và các bộ để xây dựng một cơ sở dữ liệu lớn. Việc đưa các quyết định và chính sách của chính phủ tới người dân cũng rất dễ dàng, vì chính phủ điện tử cho phép mọi người dân tiếp cận thông tin.

- Hiệu quả hoạt động cao: Điều quan trọng đối với người dân là hiệu quả của các dịch vụ được cung cấp. Hiệu quả của chính phủ được đo lường bằng chất lượng của các tương tác của chính phủ với người dân. Việc xử lý các thủ tục giấy tờ trong hệ thống chính quyền truyền thống là một công việc khó khăn, tiêu tốn nhiều nguồn lực; thời gian dành cho các thủ tục giấy tờ không tạo ra nhiều giá trị cho công dân. Vấn đề này càng trở nên phù hợp hơn khi chúng ta xem xét thực tế là người dân đang đòi hỏi nhiều hơn từ các dịch vụ công. Bằng cách thiết lập một điểm giao tiếp tập trung thông qua chính phủ điện tử, các chính phủ có thể đạt được hiệu quả hoạt động cao

- Tăng mức độ tin cậy cao vào chính phủ: Đối với bất kỳ chính phủ nào để tồn tại, duy trì chính phủ đó phải giành được sự tin tưởng của đa số người dân. Chính phủ điện tử luôn có đủ khả năng đó cho bất kỳ chính phủ nào chấp nhận nó. Nó cải thiện các dịch vụ thông qua sự hiểu biết tốt hơn về các yêu cầu của công dân, do đó hướng đến các dịch vụ trực tuyến liền mạch. Điều đó đạt được thông qua việc cải thiện tính minh bạch, độ chính xác và tạo điều kiện thuận lợi cho việc chuyển đổi thông tin giữa chính phủ và công dân.

- Giảm chi phí điều hành chính phủ: Chính phủ điện tử rất hiệu quả về chi phí. Ví dụ, chính phủ muốn lấy ý kiến của công chúng về một vấn đề nào đó, với hệ thống chính phủ điện tử, chính phủ có thể thực hiện một cuộc khảo sát và lấy ý kiến rất nhanh với chi phí cực thấp. Điều đó cũng áp dụng khi chính phủ muốn nắm bắt một số dữ liệu. Nhờ một cải tiến mới được gọi là giải pháp đám mây, giúp các chính phủ tiết kiệm đáng kể từ chi phí cơ sở hạ tầng CNTT và chi phí bảo trì.

Rõ ràng là việc triển khai chính phủ điện tử không chỉ tiết kiệm nguồn lực, công sức và tiền bạc mà còn có thể nâng cao chất lượng dịch vụ một cách sâu rộng và giảm thời gian dành cho các cơ quan ban ngành của Chính phủ**.**

2.1.3 Mục tiêu của Chính phủ điện tử

2.1.3.1. Các mục tiêu của CPĐT

Mục tiêu chung là tăng cường năng lực, nâng cao hiệu quả điều hành nhà nước của chính phủ, mang lại thuận lợi cho dân chúng, tăng cường sự công khai minh bạch (transparency), giảm chi tiêu chính phủ. Mục tiêu cụ thể là:

– Nâng cao năng lực quản lý điều hành của Chính phủ và các cơ quan chính quyền các cấp (trao đổi văn bản điện tử, thu thập thông tin chính xác và kịp thời ra quyết định, giao ban điện tử …)

– Cung cấp cho người dân và doanh nghiệp các dịch vụ công tạo điều kiện cho người dân dễ dàng truy nhập ở khắp mọi nơi

– Người dân có thể tham gia xây dựng chính sách, đóng góp vào quá trình xây dựng luật pháp, quá trình điều hành của chính phủ một cách tích cực.

– Giảm được chi phí cho bộ máy chính phủ

– Thực hiện một chính phủ hiện đại, hiệu quả và minh bạch

Chính phủ điện tử sẽ tạo ra phong cách lãnh dạo mới, phương thức mới, cung cấp dịch vụ cho người dân và nâng cao được năng lực quản lý điều hành đất nước.

Do vậy mà trong thời gian qua, các nước đều cố gắng đầu tư xây dựng CPĐT. Xây dựng CPĐT ở Việt Nam là một yêu cầu cấp thiết, nó là một phần quan trọng trong tiến trình cải cách nền hành chính quốc gia.

Những khó khăn, trở ngại trong quá trình xây dựng CPĐT tại Việt Nam còn rất nhiều:

– Bất cập từ các dự án CNTT -Cơ sở hạ tầng CNTT – TT còn yếu kém.

– Trình độ dân trí thấp

– Trình độ nhận thức và kỹ năng của cán bộ viên chức bị hạn chế

– Quy trình nghiệp vụ chưa ổn định (đang trong quá trình cải cách).

2.1.3.2 Lợi ích của CPĐT

CPĐT là chính phủ đảm bảo được cung cấp đầy đủ thông tin cần thiết và đúng lúc cho việc ra quyết định. CPĐT lý tưởng là một chính phủ cung cấp đầy đủ thông tin, đúng thời điểm cho những người quyết định, đó là lợi thế lớn nhất của CNTT.

CPĐT sử dụng CNTT để tự động hoá các thủ tục hành chính của chính phủ, áp dụng CNTT vào các quy trình quản lý, hoạt động của chính phủ do vậy tốc độ xử lý các thủ tục hành chính nhanh hơn rất nhiều lần.

CPĐT cho phép công dân có thể truy cập tới các thủ tục hành chính nà thông qua phương tiện điện tử, ví dụ như: Internet, điện thoại di động, truyền hình tương tác.

CPĐT giúp cho các doanh nghiệp làm việc với chính phủ một cách dễ dàng bởi mọi thủ tục đều được hiểu, hướng dẫn và mỗi bước công việc đều được đảm bảo thực hiện tốt, tin cậy. Mọi thông tin kinh tế mà chính phủ có đều được cung cấp đầy đủ cho các doanh nghiệp để hoạt động hiệu quả hơn.

Đối với công chức, CNTT dùng trong CPĐT là một công cụ giúp họ hoạt động hiệu quả hơn, có khả năng dáp ứng nhu cầu của công chúng về thông tin truy cập và xử lý chúng.

2.1.4 Ưu điểm và nhược điểm của chính phủ điện tử

*** Ưu điểm**

– Những ưu điểm chính của chính phủ điện tử bao gồm tăng tính hiệu quả, cải thiện dịch vụ, tăng khả năng tiếp cận dịch vụ công và tính minh bạch, trách nhiệm cao hơn:

– Tăng độ minh bạch của chính phủ vì người dân sẽ được thông báo về những hoạt động mà chính phủ đang thực hiện cũng như những chính sách mà họ đề ra.

– Cải thiện được hiệu quả so với hệ thống hành chính làm việc trên bàn giấy, giúp tiết kiệm thời gian, đồng thời rút gọn khoảng cách giao tiếp giữa chính phủ và doanh nghiệp

– Giảm được phần chi phí dành cho việc phục vụ các hoạt động của công chức và mua sắm công.Cho phép người dân có thể truy cập và thu thập thông tin liên quan đến bất kỳ bộ phận nào của chính phủ và người dân có quyền tham gia vào quá trình ra quyết định của chính phủ.

***Nhược điểm**

– **Thời gian**: để xây dựng được chính phủ điện tử cần đồng bộ hóa được các bộ phận hành chính với nhiều thủ tục khác nhau, nhiều hoạt động khác nhau. Điều này dẫn tới việc sẽ mất một thời gian dài để có thể hoàn thành,

– **Bảo mật**: Việc lưu trữ dữ liệu cá nhân của công dân có thể bị xem là kiểm soát quyền riêng tư hoặc lạm dụng cho những mục đích khác. Còn có nguy cơ việc dữ liệu bị mất cắp, hoặc bị rò rỉ thông tin hoặc bị bán, sử dụng cho các mục đích thương mại.

– **Chi phí**: Tốn nhiều chi phí để có thể hoàn thành được chính phủ điện tử. Và còn có các chi phí tiếp tục phát sinh như chi phí dùng để bảo trì, nâng cấp trang web. Đồng thời cũng phải trả một khoản phí lớn để bảo vệ được quyền riêng tư, tránh bị hack dữ liệu.

– **Chế độ chính trị** tùy vào các chế độ chính trị khác nhau mà sẽ có nhiều vấn đề phát sinh liên quan, ví dụ với các nước theo chế độ xem trọng quyền tự do và riêng tư của người dân thì việc nắm giữ thông tin cá nhân của người dân sẽ bị nhiều sự phản đối.

Với những nước còn nghèo, chưa phổ cập internet toàn dân thì sẽ có những bộ phận người dân không thể tiếp cận được chính phủ điện tử, họ là những người có thể bị cập nhật thông tin chậm trễ, chính phủ không tiếp cận được nhóm đối tượng này thông qua chính phủ điện tử.

2.2. Vai trò của Chính phủ điện tử với phát triển kinh tế số ở Việt Nam

- Tạo môi trường pháp lý minh bạch cho quá trình phát triển kinh tế số.

- Hỗ trợ đẩy nhanh quá trình xây dựng hạ tầng công nghệ thông tin, nền tảng của cho phát triển nền kinh tế số.

- Đổi mới, nâng cao hiệu quả đào tạo nguồn nhân lực số, chuẩn bị sẵn sàng nền kinh tế số.

- Đẩy nhanh việc số hoá các thủ tục hành chính, cung cấp các dịch vụ công, đẩy mạnh cải cách hành chính, tạo môi trường số giữa Chính phủ với các doanh nghiệp.

2.3. Hồ sơ hành chính điện tử

Theo Thông tư số 32/2017/TT-BTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông, quy định tại điều 3 như sau: Hồ sơ hành chính điện tử là hồ sơ được tạo ra, được gửi đi, được nhận, được lưu trữ bằng phương tiện điện tử.

Hồ sơ hành chính điện tử được sắp xếp, tổ chức, lưu trữ trong cơ sở dữ liệu của ứng dụng dịch vụ công trực tuyến để bảo đảm khả năng xử lý, tra cứu, thống kê, tổng hợp, kết nối, chia sẻ với các cơ sở dữ liệu của các hệ thống ứng dụng liên quan;

2.4 Kết luận

Hai kỹ thuật cơ bản trong lý thuyết mã hóa là Mã hóa khóa bí mật (*secret-key crytography*) và Mã hóa khóa công khai (*public-key crytography*). Hệ mã khóa bí mật giống như việc sử dụng khóa chìa, hai bên A và đều phải có chìa giống nhau để đóng hay mở, chỉ có hai người này mới sử dụng được khóa đó, còn hệ mã khóa công khai giống như việc dùng thùng thư riêng cho mỗi người, B hay người nào đó muốn gửi gì cho A thì bỏ vào thùng, sau đó A sẽ dùng chìa riêng để mở.

Người ta sẽ dùng phương pháp mã khóa bí mật hay mã khóa công khai tuỳ theo yêu cầu về bảo mật để giữ bí mật thông tin. Ứng dụng được xây dựng trong phần sau của đồ án sẽ sử dụng thuật toán mã hóa khóa công khai RSA để ký số lên các thông điệp truyền đi giữa các đối tác trong hệ thống.

Chương 3
XÂY DỰNG ỨNG DỤNG CỔNG DỊCH VỤ CÔNG QUỐC GIA.

3.1. Lược đồ chữ ký số áp dụng trong xây dựng ứng dụng

Người dùng phải đăng ký tài khoản máy chủ. Khi đăng ký thành công, khách hàng sẽ được tự động chọn ngẫu nhiên khóa (bao gồm các cặp khóa công khai và bí mật). Khi thực hiện các dịch vụ trên cổng thông tin dịch vụ công quốc gia, người dùng sẽ thao tác và điền các thông tin được cung cấp. Khách hàng gửi xác nhận tới máy chủ để tiến hàng khai báo. Quá trình truyền thông giữa các bên tham gia được bảo đảm bằng cách sử dụng chữ ký số trên các thông điệp truyền đi. Cụ thể, lược đồ chữ ký số được sử dụng trong hệ thống như sau:

- User sau khi đăng ký tài khoản thành công, sẽ được cặp khóa công khai **(e_1, N_1)** và khóa bí mật **(d_1, N_1)** đã được mã hóa và lưu trong cơ sở dữ liệu của mỗi người dùng.

- Server sử dụng hàm băm **SHA-1** để băm thông điệp **X**. **X** ở đây là thông tin đăng ký khai báo của **User** bao gồm: thông tin cá nhân (Họ tên, số chứng minh nhân dân,...).

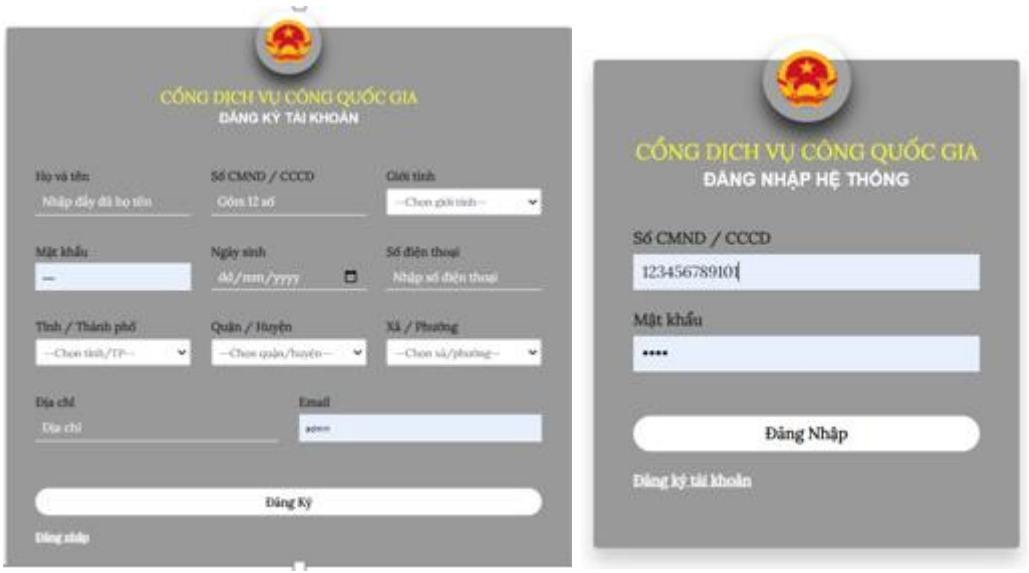
Khi hoàn tất các thao tác điền các thông tin được yêu cầu. Hệ thống sẽ tự động thực hiện các công việc sau:

1. Thu gọn thông điệp **X** bởi hàm băm: **Y = H(X)**
2. **User** giải mã khóa bí mật và dùng nó để ký lên thông điệp đã băm **Y** (thông điệp rút gọn) để tạo ra chữ ký số trên **Y** bằng cách tính **S = modN_1**
3. **User** gửi cặp **(X, S)** là chữ ký **S** cho **Server**. Sau khi nhận được chữ ký **(X, S)**, **server** tiến hàng kiểm tra chữ ký như sau:

- Dùng hàm băm **H** để rút gọn thông điệp **X** thành **Y = H(X)**
- **Server** sử dụng cặp khóa công khai **(e_1, N_1)** của User để tính $\mathbf{Y^1 = modN_1}$. Nếu $\mathbf{Y^1 = Y}$ thì **Server** chấp nhập chữ ký **S** trên thông điệp **X** của **User** là đúng. Ngược lại $\mathbf{Y^1 \neq Y}$ thì **Server** không thừa nhận **S** là chữ ký của **User** trên thông điệp **X** vì cho đây là chữ ký giả mạo hoặc thông điệp đã bị thay đổi.

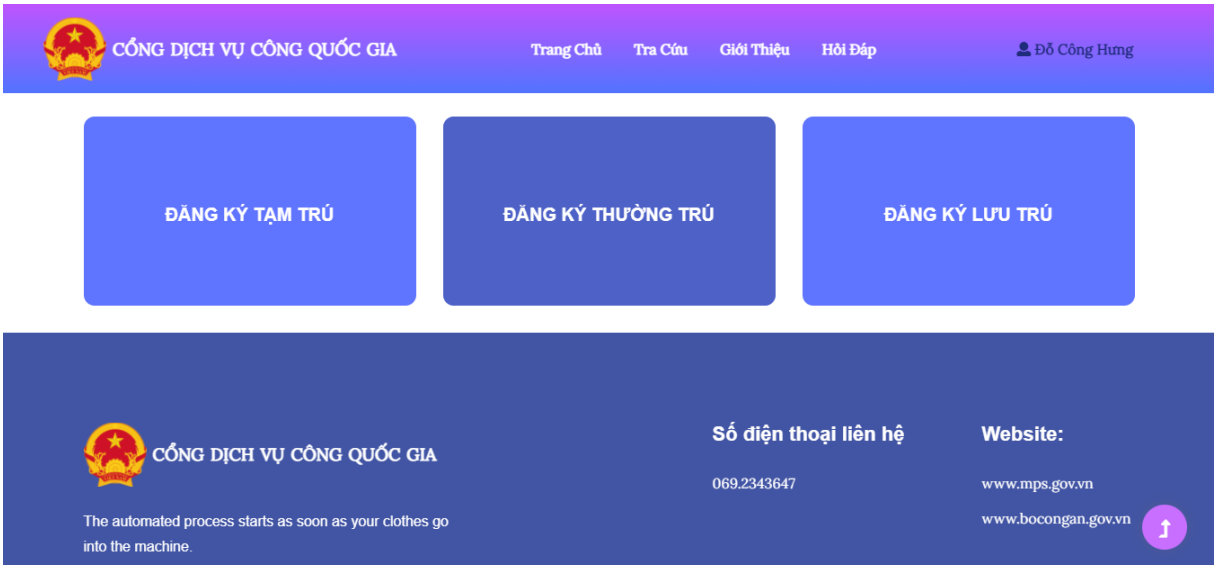
3.2 Một số hình ảnh ứng dụng cổng thông tin dịch vụ quốc gia

Đăng ký tài khoản. Sau khi đăng ký thành công, tiến hành đăng nhập hệ thống



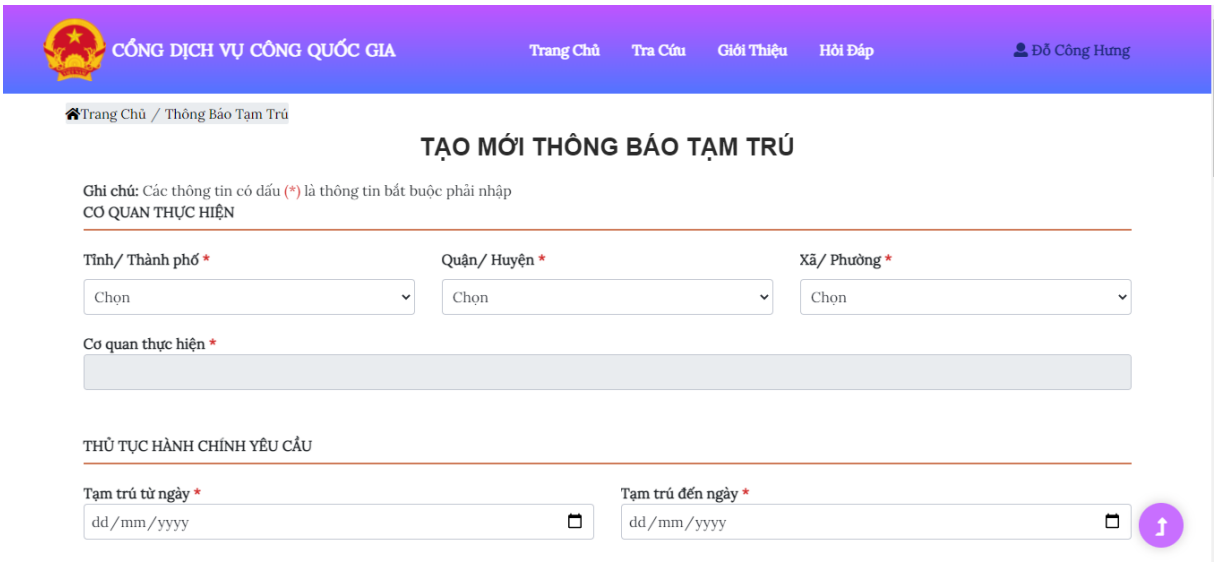
Hình 3.0.1 Đăng ký tài khoản và đăng nhập hệ thống

Đăng nhập thành công, người dùng sẽ thấy giao diện trang chủ với 3 thủ tục hành chính, gồm: Đăng ký tạm trú, thường trú và lưu trú.



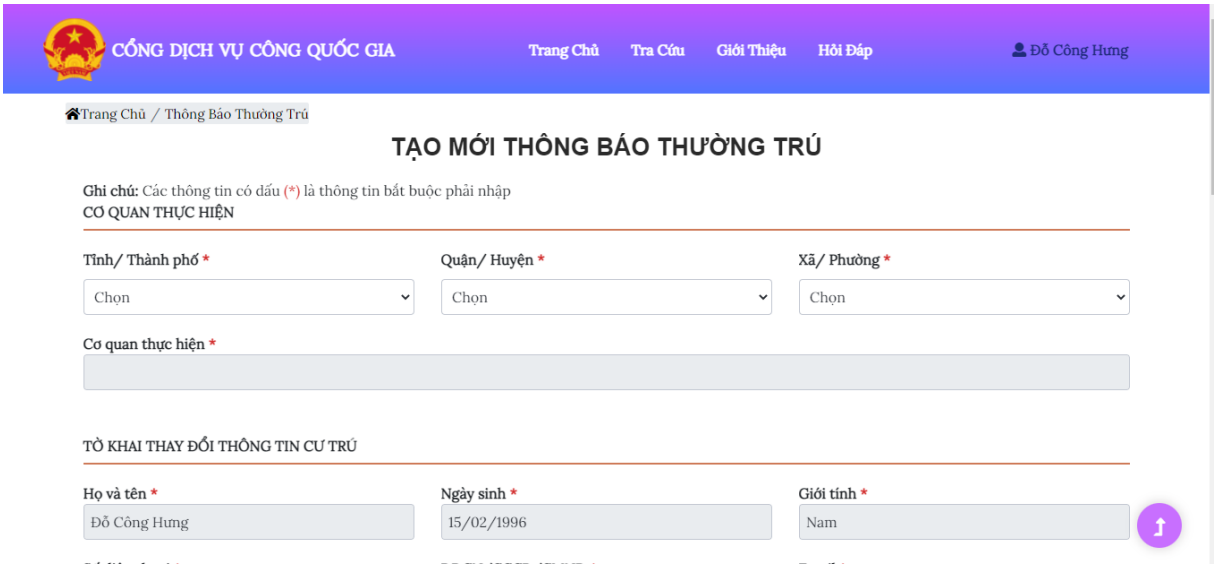
Hình 3.0.2 Giao diện trang chủ

Giao diện thủ tục thông báo tạm trú, với các cơ quan thực hiện được hiển thị tự động. Khi người dùng chọn tỉnh, thành phố, quận/huyện sẽ hiển thị địa bàn hành chính của tỉnh thành phố đó, tương tự với xã phường.



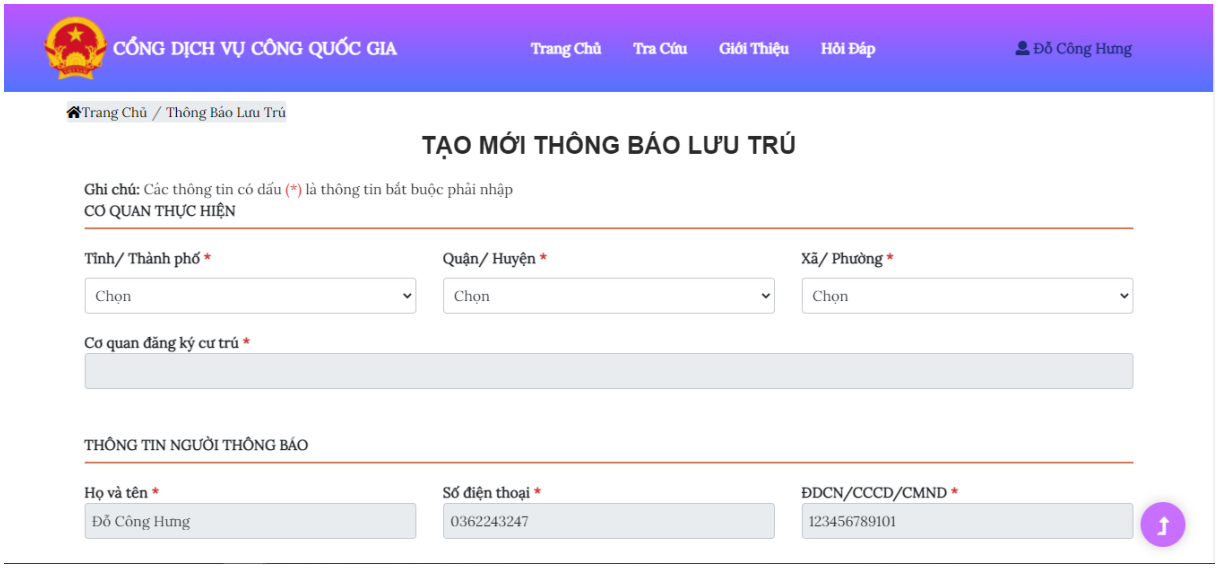
Hình 3.0.3 Giao diện thủ tục thông báo tạm trú

Tương tự với thông báo thường trú. Các thông tin của người thay đổi nơi thường trú sẽ tự động hiển thị cho người dùng. Giúp người dùng nhanh chóng thực hiện thủ tục hành chính.



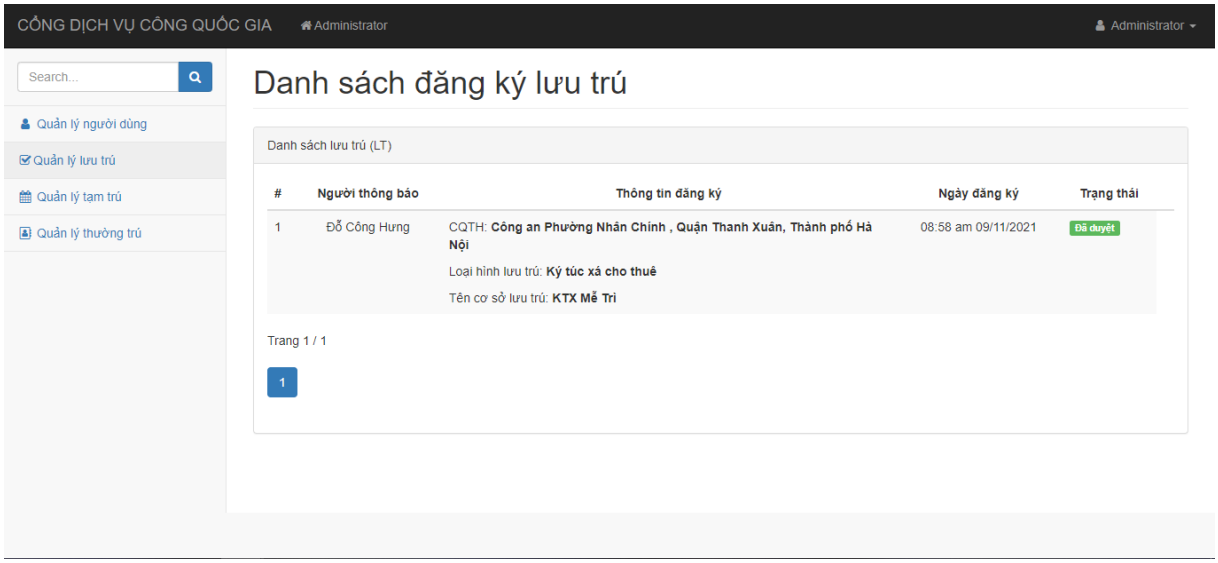
Hình 3.0.4 Giao diện thủ tục thông báo thường trú

Tương tự, với giao diện thông báo lưu trú, hiển thị thông tin cũng hoàn toàn tự động



Hình 3.0.5 Giao diện thủ tục thông báo lưu trú

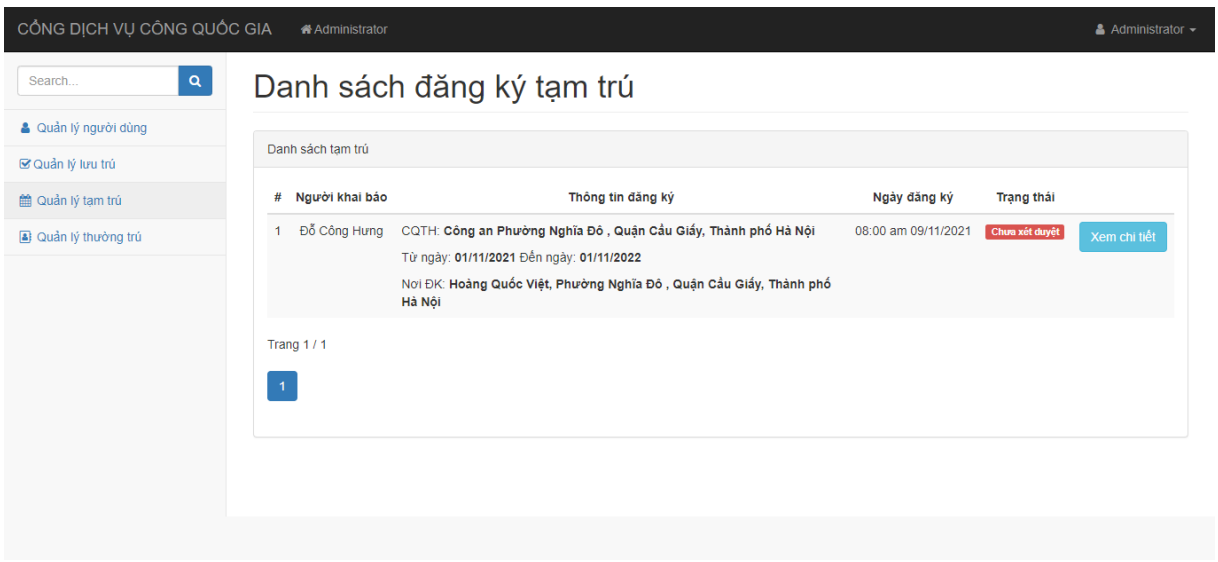
Sau khi người dùng ấn gửi các thông tin, hệ thống sẽ tự động xác thực người dùng và tính toàn vẹn của thông tin bằng chữ ký điện tử và lưu vào trong hệ thống. Bên dưới là giao diện dành cho quản trị viên hệ thống. Gồm: Danh sách đăng ký lưu trú.



Hình 3.0.6 Giao diện quản trị viên: danh sách đăng ký lưu trú

Danh sách đăng ký tạm trú.

Đối với các thủ tục hành chính chưa được xét duyệt, quản trị viên sẽ được thông báo dưới cột trạng thái, bao gồm cả 3 thủ tục hành chính. Để xét duyệt thủ tục, quản trị viên sẽ ấn vào nút xem chi tiết để xem chi tiết các thông tin của người dùng đã thực hiện.

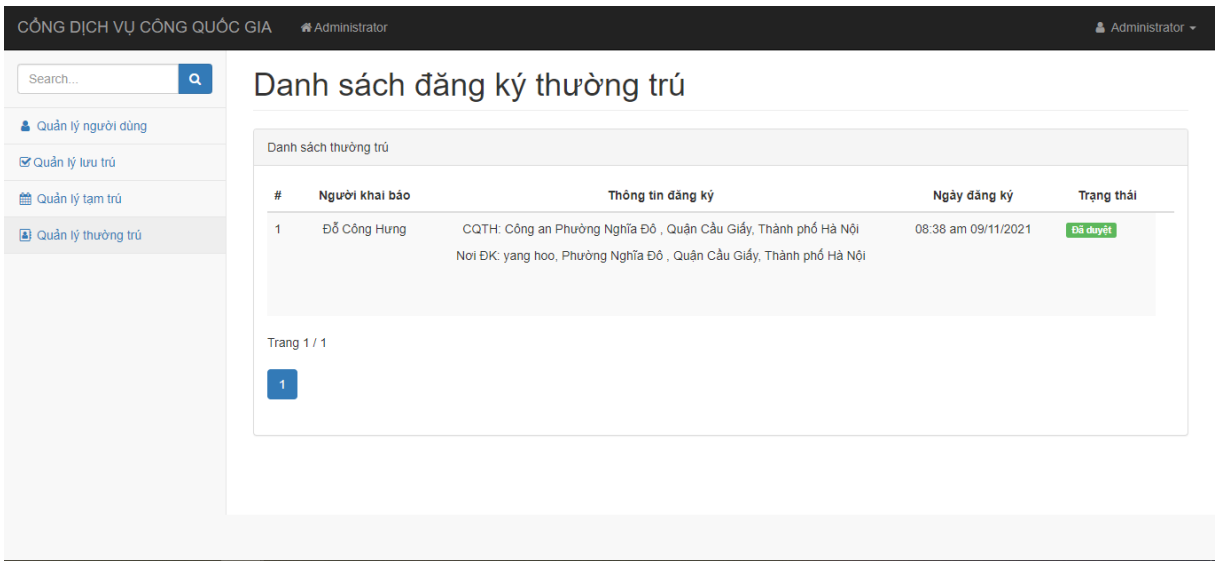


Hình 3.0.7 Giao diện quản trị viên: đăng ký tạm trú

Khi ấn vào xem chi tiết, hệ thống sẽ chuyển về giao diện như hình. Hiển thị tất cả các thông tin mà người dùng đã cung cấp.

Hình 3.0.8 Giao diện quản trị viên: chi tiết thủ tục

Danh sách đăng ký thường trú



Hình 3.0.9 Giao diện quản trị viên: danh sách đăng ký thường trú

3.3 Kết luận

Hệ thống được xây dựng nhằm mục đích ứng dụng chữ ký điện tử trong quá trình truyền thông giữa các đối tác tham gia thực hiện một thủ tục hành chính qua mạng. Giao thức dùng trong chương trình đã được đơn giản hóa so với giao thức đang được dùng trong các hệ thống dịch vụ công quốc gia. Điểm mấu chốt trong giao thức này đó là việc sử dụng một chứng thực điện tử - Receipt làm bằng chứng cho một quá trình truyền nhận thông tin. Đây là cơ sở để các cơ quan có thẩm quyền xác thực người dùng và tính toàn vẹn thông tin nhằm thực hiện các thủ tục hành chính mà người dùng yêu cầu. Chương trình được xây dựng bằng ngôn ngữ C#, sử dụng các thư viện mã hóa có sẵn và ký số lên các thông điệp.

KẾT LUẬN

Hiện nay, Đảng và Chính phủ Việt Nam rất quan tâm và đã có nhiều việc làm thiết thực nhằm thiết lập cơ sở hạ tầng cho Chính phủ điện tử như chữ ký điện tử. Ngày nay, với sự phát triển mạnh mẽ của khoa học công nghệ, nhất là công nghệ thông tin - truyền thông, hoạt động giao dịch trực tiếp giữa các cơ quan, tổ chức, cá nhân đã được chuyển dần sang phương thức giao dịch mới - giao dịch điện tử. Khi sử dụng phương thức giao dịch điện tử, các giới hạn về khoảng cách địa lý hay chênh lệch về thời gian của giao dịch truyền thống dần được loại bỏ, thay vào đó là các giao dịch được diễn ra theo thời gian thực. Tuy nhiên, vấn đề đặt ra đối với giao dịch điện tử là việc xác định chính xác người tham gia giao dịch, văn bản sau khi ký có bị chỉnh sửa hay không và người ký trên dữ liệu số thừa nhận chữ ký đó không... Tất cả những băn khoăn, thắc mắc trên đều được khẳng định thông qua "Chữ ký số".

Với tầm quan trọng như vậy của việc xây dựng cơ sở hạ tầng cho Chính phủ điện tử, hành chính điện tử, đồ án này đã trình bày về:

- Vấn đề an toàn thông tin trên mạng Internet và vai trò của mật mã hóa trong việc bảo mật thông tin
- Các kỹ thuật mã hóa cơ bản là mã hóa khóa bí mật, mã hóa khóa công khai, các thuật toán phổ biến của mỗi kỹ thuật, so sánh và đánh giá các phương pháp, áp dụng trong thực tế.
- Khái niệm về chữ ký điện tử, các bước trong hoạt động của một hệ chữ ký điện tử và việc áp dụng chữ ký điện tử để giải quyết vấn đề xác thực. Tài liệu cũng trình bày hai loại chữ ký điện tử, thuật toán chữ ký điện tử DSA theo chuẩn của Viện tiêu chuẩn và công nghệ quốc gia Mỹ (NIST).
- Xây dựng thuật toán mã hóa công khai RSA trong thực hiện thủ tục hành chính điện tử.
- Xây dựng ứng dụng cổng dịch vụ công quốc gia dựa trên thuật toán mã hóa công khai RSA.

Một số vấn đề tiếp tục nghiên cứu và đề xuất:

- Mở rộng chức năng của chứng thực, ngoài xác nhận thanh toán còn xác định một số quyền cho chủ sở hữu chứng thực như quyền truy nhập tới một tài nguyên...v.v.
- Số hóa thêm nhiều các thủ tục hành chính, giảm bớt các thủ tục, thông tin không cần thiết.
- Không ngừng cải thiện và phát triển khả năng mã hóa thông tin, nghiên cứu thêm các thuật toán chữ ký số mới.

TÀI LIỆU THAM KHẢO

[1] *"Java Security"*, O'Reilly 2nd Edition, 1998

[2] Choi, Stahl & Whinston (2003), "*The Economics of Electronic Commerce*" , chapter 10 "*Electronic Payment Systems***"**

[3] Donal O'Mahony, Michael Peirce, and Hitesh Tewari (June 1997), "*Electronic Payment Systems*.", Artech House Computer Science Library.

Dr. Andreas Schöter, Rachel Willmer (1997), *"Digital Money Online A Review of Some Existing Technologies"*

[5] European Central Bank (16/9/2002), "*E-Payments in Europe – The EuroSystem's Perspectivee"*

[6] Federal Information Processing Standards Publication 180 (1995), *"Secure Hash Standard (SHA)"*

[7] Federal Information Processing Standards Publication 186 (1994), *"Digital Signature Standard (DSS)"*

[8] Feng Bao, Robert Deng, Jianying Zhou, "*Electronic Payment Systems with Fair On-line Verification (Extended Version)*"

[9] IAIK (2005), "*IAIK JCE 3.1.3Documentation*"

Information Security Committe Electronic Commerce and Information Technology Division Section of Science and Technology American Bar Association (1996), *"Legal Infrastructure forCertification Authorities and Secure Electronic Commerce"*

[11] Jonathan B. Knudsen (1998), *"Java Cryptography"*

[12] M. Bellare, J. Garay, C. Jutla, M. Yung (1998), *"VarietyCash: a Multi-Purpose Electronic Payment System"*

[13] Prof. F. Bodart (2004), "*Electronic Payment Systems*"

[14] Svetlin Nakov (2005), "*How Digital Signatures Work: Digitally Signing Messages"*

[15] Thông tư số **32/2017/**TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và truyền thông

[16] https://luatduonggia.vn/chinh-phu-dien-tu-la-gi-khai-niem-vai-tro-va-muc-tieu-cua-chinh-phu-dien-tu/