TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM
TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG
KHOA CÔNG NGHỆ THÔNG TIN

ĐỒ ÁN CUỐI KÌ MÔN BẢO MẬT THÔNG TIN

Chữ ký điện tử và một số ứng dụng (Digital Signature and its applications)

Người hướng dẫn: **TS HUỲNH NGỌC TÚ**

Người thực hiện: **HUỲNH HỮU HIỆP – 51800677**

Lớp : **18050402**

Khoá : **22**

THÀNH PHỐ HỒ CHÍ MINH, NĂM 2020

TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM
TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG
KHOA CÔNG NGHỆ THÔNG TIN

ĐỒ ÁN CUỐI KÌ MÔN BẢO MẬT THÔNG TIN

Chữ ký điện tử và một số ứng dụng (Digital Signature and its applications)

Người hướng dẫn: **TS HUỲNH NGỌC TÚ**
Người thực hiện: **HUỲNH HỮU HIỆP**
Lớp **: 18050402**
Khoá **: 22**

THÀNH PHỐ HỒ CHÍ MINH, NĂM 2020

LỜI CẢM ƠN

Lời đầu tiên chúng tôi chân thành cảm ơn giảng viên hướng dẫn là cô Huỳnh Ngọc Tú. Người đã hướng dẫn trên lớp và truyền đạt khá nhiều kiến thức bổ ích cho chúng tôi trong suốt quá trình học tập cũng như giải đáp tất cả các thắc mắc mà chúng tôi gặp phải. Và hơn thế nữa cô còn là người cung cấp cho tôi nguồn tài liệu bổ ích cho chúng tôi. Từ đó, đó là nguồn kiến thức để tôi có thể nắm vững và đọc thêm một số tài liệu mà thầy cung cấp để có thể hoàn thành bài báo cáo như ngày hôm nay một cách hoàn thiện nhất. Do kiến thức còn hạn chế và cũng như không tránh khỏi những sai sót, qua đây chúng tôi mong cô có những ý kiến, đánh giá của thầy để bài báo cáo có thể hoàn thiện hơn.

Một lần nữa chúng tôi chân thành cảm ơn!

ĐỒ ÁN ĐƯỢC HOÀN THÀNH TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG

Tôi xin cam đoan đây là sản phẩm đồ án của riêng tôi và được sự hướng dẫn của TS Huỳnh Ngọc Tú. Các nội dung nghiên cứu, kết quả trong đề tài này là trung thực và chưa công bố dưới bất kỳ hình thức nào trước đây. Những số liệu trong các bảng biểu phục vụ cho việc phân tích, nhận xét, đánh giá được chính tác giả thu thập từ các nguồn khác nhau có ghi rõ trong phần tài liệu tham khảo.

Ngoài ra, trong đồ án còn sử dụng một số nhận xét, đánh giá cũng như số liệu của các tác giả khác, cơ quan tổ chức khác đều có trích dẫn và chú thích nguồn gốc.

Nếu phát hiện có bất kỳ sự gian lận nào tôi xin hoàn toàn chịu trách nhiệm về nội dung đồ án của mình. Trường đại học Tôn Đức Thắng không liên quan đến những vi phạm tác quyền, bản quyền do tôi gây ra trong quá trình thực hiện (nếu có).

TP. Hồ Chí Minh, ngày tháng năm

Tác giả

(ký tên và ghi rõ họ tên)

Huỳnh Hữu Hiệp

PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN

Phần xác nhận của GV hướng dẫn

_____

_____

_____

_____

_____

_____

_____

Tp. Hồ Chí Minh, ngày tháng năm
(kí và ghi họ tên)

Phần đánh giá của GV chấm bài

_____

_____

_____

_____

_____

_____

_____

Tp. Hồ Chí Minh, ngày tháng năm
(kí và ghi họ tên)

TÓM TẮT

Bài báo cáo cuối kỳ môn bảo mật thông tin sẽ trình bày sơ lược về chữ ký điện tử và một số ứng dụng của nó. Bài báo cáo gồm ba chương để khái quát toàn bộ nội dung trên. Chương đầu tiên là chương tổng quan sẽ giới thiệu khái quát về các khái niệm liên quan đến chữ ký điện tử, lịch sử hình thành, thành phần cấu tạo của nó và các thông tin pháp lý liên quan; cùng với đó là cách làm việc của chữ ký điện tử và ưu nhược điểm của nó so với chữ ký số. Chương thứ hai sẽ trình bày về các ứng dụng liên quan đến chữ ký điện tử và áp dụng chữ ký điện tử được sử dụng khá phổ biến hiện nay như: Smart Cards, Mitrenet, IDSN, Time Stamped Signatures, Blind Signatures, Data Storage,....vv. Và chương cuối cùng là mô phỏng chữ ký điện tử thông qua quá trình tạo chữ ký, ký chữ ký và xác nhận chữ ký cũng như thêm đó là phần tổng kết nội dung bao gồm những lợi ích và những hạn chế khi áp dụng chữ ký điện tử.

MỤC LỤC

DANH MỤC KÍ HIỆU VÀ CHỮ VIẾT TẮT

CÁC KÝ HIỆU

CÁC CHỮ VIẾT TẮT

ISDN	Integrated Services Digital Network (Mạng số tích hợp đa dịch vụ).
RSA	Rivest–Shamir–Adleman (Tên một thuật toán mã hóa).
RAM	Random Access Memory (Bộ nhớ truy xuất đọc ghi ngẫu nhiên).
ROM	Read Only Memory (Bộ nhớ chỉ đọc).
SHA	Secure Hash Algorithms (Giải thuật băm an toàn).

DANH MỤC CÁC BẢNG BIỂU, HÌNH VẼ, ĐỒ THỊ

DANH MỤC HÌNH

DANH MỤC BẢNG

CHƯƠNG 1 – TỔNG QUAN

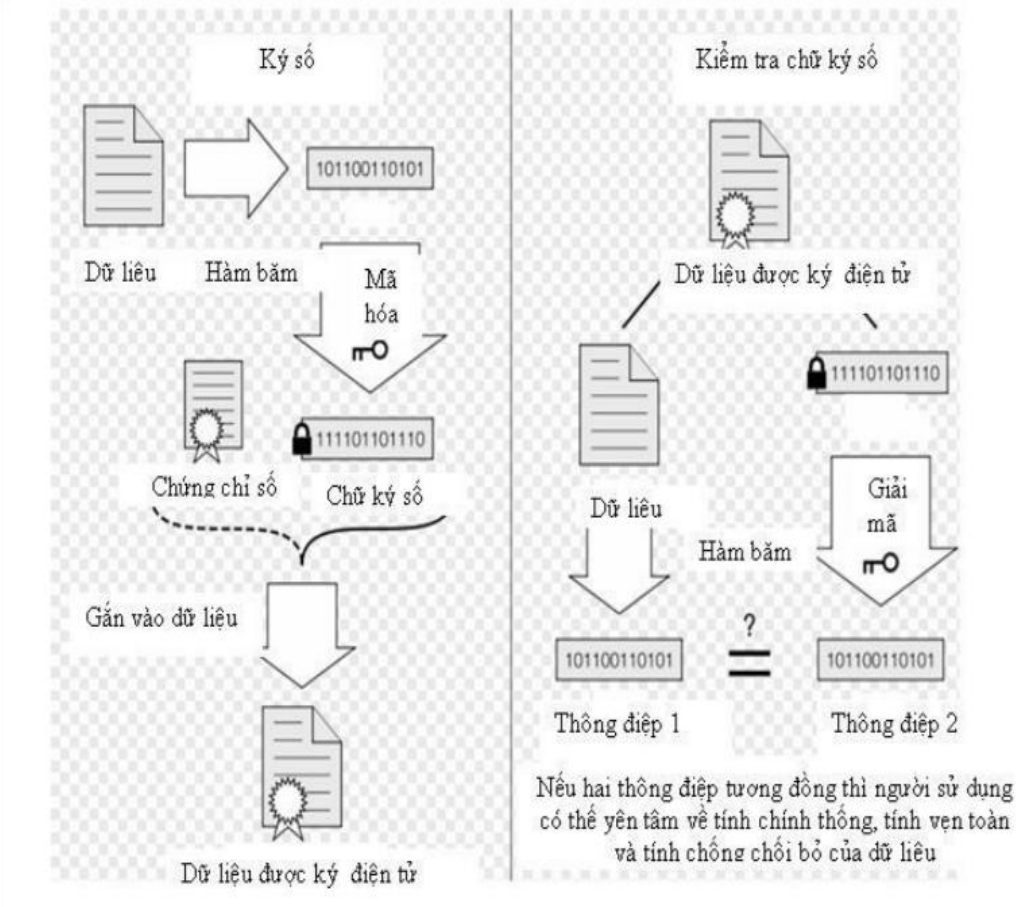
1.1 Các khái niệm về chữ ký điện tử

Hình 1-1: Mô phỏng chữ ký điện tử.

1.1.1 Chữ ký điện tử

- Chữ ký điện tử (Digital Signature) dựa trên kỹ thuật sử dụng mã hóa khóa công khai. Trong đó, cả người gửi và người nhận, mỗi người có một cặp khóa là khóa bí mật, hay riêng tư (Private Key) và khóa công khai (Public Key).
- Chữ ký điện tử (Digital Signature) là 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. Chữ ký điện tử được tạo ra bằng cách áp dụng thuật toán băm một chiều trên văn bản gốc để tạo ra bản phân tích văn bản (message digest) hay còn gọi là fingerprint, sau đó mã hóa bằng private key tạo ra chữ ký điện tử đính kèm với văn bản gốc để gửi đi. Khi nhận, văn bản được tách làm 2 phần, phần văn bản gốc được tính lại fingerprint để so sánh với fingerprint cũ cũng được phục hồi từ việc giải mã chữ ký điện tử.

- Chữ ký điện tử được sử dụng trong các giao dịch điện tử. Xuất phát từ thực tế, chữ ký điện tử cũng cần bảo đảm các chức năng: xác định được người chủ của một dữ liệu nào đó: văn bản, hình ảnh, video, ... dữ liệu đó có bị thay đổi hay không.



Hình 1-2: Mô hình chữ ký điện tử.

- Chữ ký điện tử hoạt động khi một người gửi một thông điệp, người đó dùng khóa riêng của mình để mã hóa thông điệp sang một dạng khó nhận dạng. Người nhận dùng khóa công khai của ngườ i gửi để mã hóa thông điệp. Tuy nhiên, để an toàn thật sự phải có các bước bổ sung. Do đó, thuật toán băm MD5 và thuật toán mã hóa RSA có thể được áp dụng để xây dựng ứng dụng chữ ký điện tử.

1.1.2 Chứng thư điện tử

Chứng thư điện tử là thông điệp dữ liệu do tổ chức cung cấp dịch vụ chứng thực chữ ký điện tử phát hành nhằm xác nhận cơ quan, tổ chức, cá nhân được chứng thực là người ký chữ ký điện tử.

Chứng thư điện tử sử dụng để ký trên hóa đơn điện tử, đảm bảo:

+ Chống từ chối bởi người ký.

+ Đảm bảo tính toàn vẹn của HĐĐT trong qua trình lưu trữ, truyền nhận.

Chứng thư điện tử có thời hạn hiệu lực và có thể bị hủy bỏ hoặc thu hồi bởi nhà cung cấp dịch vụ chứng thư điện tử.

1.1.3 Chứng thực chữ ký điện tử

Chứng thực chữ ký điện tử là một loại hình dịch vụ chứng thực chữ ký điện tử do tổ chức cung cấp dịch vụ chứng thực chữ ký điện tử cung cấp cho thuê bao dễ xác thực việc thuê bao là người đã ký điện tử trên thông điệp dữ liệu. Dịch vụ chứng thực chữ ký điện tử bao gồm:

+ Tạo cặp khóa hoặc hỗ trợ tạo cặp khóa bao gồm khóa công khai và khóa bí mật cho thuê bao.

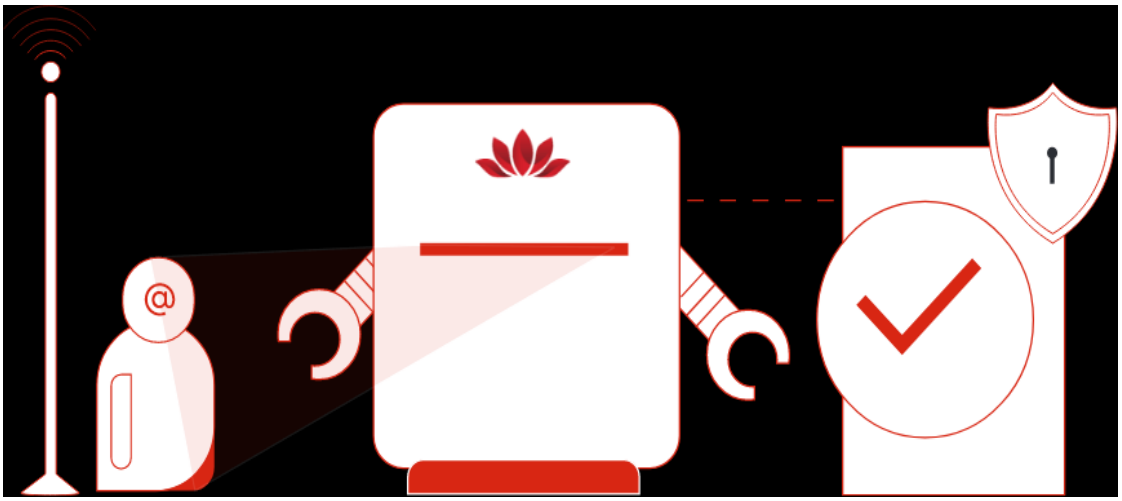
+ Cấp, gia hạn, tạm dừng, phục hồi và thu hồi chứng thư điện tử của thuê bao.

+ Duy trì trực tuyến cơ sở dữ liệu về chứng thư điện tử.

+ Cung cấp thông tin cần thiết để giúp chứng thực chữ ký số của thuê bao đã ký điện tử trên thông điệp dữ liệu.

+ Những dịch vụ khác có liên quan theo quy định.

Bản chất của chứng thực chữ ký điện tử tương tự như cấp con dấu và xác nhận con dấu của người đóng dấu, cung cấp bằng chứng cho sự nhận diện của một đối tượng. Chứng thực chữ ký điện tử giải quyết vấn đề mạo danh, giúp cho cho người nhận thông tin biết thông tin từ đâu cung cấp và tin tưởng vào bên cung cấp thông tin trong các giao dịch điện tử.



Hình 1-3: Chứng thực chữ ký điện tử.

1.1.4 Chương trình chữ ký điện tử

Chương trình ký điện tử là chương trình máy tính được thiết lập để hoạt động độc lập hoặc thông qua thiết bị, hệ thống thông tin, chương trình máy tính khác nhằm tạo ra một chữ ký điện tử đặc trưng cho người ký thông điệp dữ liệu.

1.2 Tổng quan chữ ký điện tử

1.2.1 Lịch sử ra đời

Con người đã sử dụng các hợp đồng dưới dạng điện tử từ hơn 100 năm nay với việc sử dụng mã Morse và điện tín. Vào năm 1889, tòa án tối cao bang New Hampshire (Hoa kỳ) đã phê chuẩn tính hiệu lực của chữ ký điện tử. Tuy nhiên, chỉ với những phát triển của khoa học kỹ thuật gần đây thì chữ ký điện tử mới đi vào cuộc sống một cách rộng rãi.

Vào thập niên 1980, các công ty và một số cá nhân bắt đầu sử dụng máy fax để truyền đi các tài liệu quan trọng. Mặc dù chữ ký trên các tài liệu này vẫn thể hiện trên giấy nhưng quá trình truyền và nhận chúng hoàn toàn dựa trên tín hiệu điện tử.

Hiện nay, chữ ký điện tử có thể bao hàm các cam kết gửi bằng email, nhập các số định dạng cá nhân (PIN) vào các máy ATM, ký bằng bút điện tử với thiết bị màn hình

cảm ứng tại các quầy tính tiền, chấp nhận các điều khoản người dùng (EULA) khi cài đặt phần mềm máy tính, ký các hợp đồng điện tử online.

1.2.2 Những thành phần tạo ra chữ ký điện tử

Chữ ký điện tử dựa trên công nghệ mã hoá khóa công khai (RSA): mỗi người dùng phải có 1 cặp khóa (key pair) bao gồm khóa công khai (public key) và khóa bí mật (private key).Cụ thể:

+ Private key: là một khóa trong cặp khóa thuộc hệ thống mật mã không đối xứng, được dùng để tạo chữ ký số.

+ Public key: là một khóa trong cặp khóa thuộc hệ thống mật mã không đối xứng, được sử dụng để giả mã kiểm tra chữ ký số được tạo bởi khóa bí mật tương ứng trong cặp khóa.

+ Digital Sign: là việc đưa khóa bí mật vào một chương trình phần mềm để tự động tạo và gắn chữ ký số vào thông điệp dữ liệu. Khi đọc các tài liệu chuyên ngành, bạn sẽ gặp nhiều cụm từ sign hoặc signed<object>, bạn hãy hiểu những nội dung đó có liên quan đến hoạt động của chữ kí số.

+ Signer (người ký): là đối tượng dùng đúng khóa bí mật của mình để tạo chữ ký số và ký vào một thông điệp dữ liệu dưới tên của mình.

+ Recipient (người nhận): là tổ chức, cá nhân nhận được thông điệp dữ liệu được ký số bởi người ký, sử dụng chứng thư số (digital certificate) của người ký đó để kiểm tra chữ ký số trong thông điệp dữ liệu nhận được và tiến hành các hoạt động, giao dịch có liên quan.

1.2.3 Tính pháp lý của chữ ký điện tử

- Các định nghĩa pháp lý

- Luật Giao dịch điện tử (Việt Nam), điều 4 định nghĩa:

(1) Chứng thư điện tử là thông điệp dữ liệu do tổ chức cung cấp dịch vụ chứng thực chữ ký điện tử phát hành nhằm xác nhận cơ quan, tổ chức, cá nhân được chứng thực là người ký chữ ký điện tử.

(2) Chứng thực chữ ký điện tử là việc xác nhận cơ quan, tổ chức, cá nhân được chứng thực là người ký chữ ký điện tử.

(5) Dữ liệu là thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự.

(12) Thông điệp dữ liệu là thông tin được tạo ra, được gửi đi, được nhận và được lưu trữ bằng phương tiện điện tử.

- Bộ luật ESIGN (Hoa Kỳ), điều 106 định nghĩa:

(2) Điện tử - chỉ các công nghệ liên quan tới điện, số, từ, không dây, quang, điện từ hoặc các khả năng tương tự.

(4) Văn bản điện tử - Các hợp đồng hoặc các văn bản khác được tạo ra, lưu trữ, trao đổi dưới dạng điện tử.

(5) Chữ ký điện tử - Các tín hiệu âm thanh, ký hiệu, quá trình gắn (vật lý hoặc logic) với hợp đồng hay văn bản và được thực hiện bởi người muốn ký vào hợp đồng hay văn bản đó.

- Bộ luật GPEA (Hoa Kỳ), điều 1710 định nghĩa:

(1) Chữ ký điện tử - là cách thức ký các văn bản điện tử đảm bảo:

(A) Nhận dạng và xác thực cá nhân đã tạo ra văn bản;

(B) Chỉ ra sự chấp thuận của người ký đối với nội dung trong văn bản.

- Bộ luật UETA (Hoa Kỳ), điều 2 định nghĩa:

(5) Điện tử - chỉ các công nghệ liên quan tới điện, số, từ, không dây, quang, điện từ hoặc các khả năng tương tự.

(6) Tác tử điện tử - là các chương trình máy tính hoặc các phương tiện tự động khác sử dụng độc lập để khởi đầu một hành động hoặc đáp lại các tín hiệu điện tử mà không cần sự giám sát của con người.

(7) Văn bản điện tử - Các văn bản được tạo ra, lưu trữ, trao đổi dưới dạng điện tử.

(8) Chữ ký điện tử - Các tín hiệu âm thanh, ký hiệu, quá trình gắn (vật lý hoặc logic) với hợp đồng hay văn bản và được thực hiện bởi người muốn ký vào hợp đồng hay văn bản đó.

- Kiểm tra tính pháp lý đối với chữ ký điện tử

Khi một chữ ký điện tử trên hợp đồng hay văn bản bị nghi ngờ thì chữ ký đó phải vượt qua một số kiểm tra trước khi có thể xử tại tòa án. Các điều kiện này có thể thay đổi tùy theo quy định của pháp luật, thậm chí trong một số trường hợp văn bản không có chữ ký (telex, fax...).

Tại Hoa Kỳ, các bước yêu cầu cho chữ ký điện tử bao gồm:

• Cung cấp thông tin cho người yêu cầu về tính pháp lý của chữ ký điện tử; các yêu cầu về phần cứng, phần mềm; các lựa chọn ký và chi phí (nếu có);

• Xác thực các bên để nhận diện rủi ro kinh doanh và yêu cầu;

• Đưa toàn bộ văn bản ra xem xét (các bên có thể phải điền số liệu);

• Yêu cầu các bên xác nhận sự tự nguyện ký vào văn bản;

• Đảm bảo các văn bản được xem xét không bị thay đổi từ khi ký;

• Cung cấp cho các bên các văn bản gốc pháp lý để lưu giữ.

• Vấn đề quan trọng cần được xem xét là sự giả mạo (giả mạo chữ ký và giả mạo sự chấp nhận). Tòa án phải giả định rằng sự giả mạo là không thể thực hiện. Tuy nhiên, đối với chữ ký điện tử thì việc làm giả là không quá khó khăn.

• Thông thường, các doanh nghiệp thường phải dựa trên các phương tiện khác để kiểm tra chữ ký điện tử chẳng hạn như gọi điện trực tiếp cho người ký trước khi giao dịch, dựa trên các quan hệ truyền thống hay không dựa hoàn toàn vào các văn bản dưới dạng điện tử. Đây là các thông lệ trong kinh doanh nên được áp dụng trong bất kỳ môi trường nào vì sự giả mạo cũng là một vấn đề thường xảy ra trong môi trường kinh doanh truyền thống. Chữ ký điện tử cũng như chữ ký truyền thống đều không đủ khả năng ngăn chặn hoàn toàn việc làm giả.

• Các ví dụ về chữ ký điện tử nêu ở trên chưa phải là chữ ký điện tử bởi vì chúng thiếu các đảm bảo mật mã học về nhận dạng người tạo ra và thiếu các kiểm tra tính toàn vẹn của dữ liệu. Các chữ ký này có tính chất pháp lý trên được gắn với văn bản trong một số trường hợp cụ thể.

- Giá trị pháp lý của chữ ký điện tử

- Chữ ký điện tử được tạo ra khi chứng thư số có hiệu lực và có thể kiểm tra được bằng khoá công khai ghi trên chứng thư số có hiệu lực đó.

- Chữ ký điện tử được tạo ra bằng khoá bí mật tương ứng với khoá công khai ghi trên chứng thư số do tổ chức có thẩm quyền cấp.

- Khóa bí mật chỉ thuộc sự kiểm soát của người ký tại thời điểm ký.

- Khóa bí mật và nội dung thông điệp dữ liệu chỉ gắn duy nhất với người ký khi người đó ký số thông điệp dữ liệu.

1.2.4 Những sử dụng giả luật của chữ ký điện tử

Một số trang web (đặc biệt là các trang khiêu dâm) và các điều khoản sử dụng phần mềm tuyên bố một số hành động gắn với chữ ký điện tử. Chẳng hạn, một trang web có thể tuyên bố rằng với việc truy cập vào trang web, bạn đã chấp nhận một số quy định. Một ví dụ khác là khi cài đặt phần mềm, trước khi cài sẽ xuất hiện một màn hình thông báo rằng với việc tiếp tục cài đặt thì bạn chấp nhận một số điều về bản quyền. Các điều khoản này có thể không được thông báo trước khi bán và không phải lúc nào cũng được hiển thị đầy đủ khi bạn cài đặt. Các điều kiện về bản quyền này thường bao gồm các điều cấm người sử dụng công bố các thông tin về sản phẩm nếu không được sự cho phép của nhà sản xuất, các điều hạn chế người sử dụng nghiên cứu sản phẩm (reverse engineering) kể cả cho mục đích hợp pháp như để tạo ra các tệp theo định dạng của phần mềm. Trong một số trường hợp, các điều khoản này có thể trái với quy định của pháp luật. Một số người cho rằng các điều trên là hợp lý để bảo vệ các bí mật công nghệ. Tuy nhiên một khi sản phẩm đã được bán rộng rãi thì lý do này cũng không thực sự thuyết phục.

Tính pháp lý của các điều khoản đề cập ở trên không rõ ràng. Tại Hoa Kỳ, chỉ có 2 tiểu bang chấp thuận bản sửa đổi của Luật thương mại thống nhất (Uniform Commercial Code) cho phép những hạn chế về bản quyền và thông báo sau bán hàng. Tại Anh, điều 9 của Quy chế thương mại điện tử năm 2002 (Electronic-Commerce (EC Directive) Regulations 2002 - SI 2002/2003) cho phép người mua có khả năng xác định trước các bước kỹ thuật khác nhau để kết thúc hợp đồng.

1.2.5 Chữ ký mật mã

- Nguyên tắc của hệ thống mã hóa công khai

Nếu ta mã hóa bằng khóa bí mật thì chỉ khóa công khai mới giải mã thông tin được, và ngược lại, nếu ta mã hóa bằng khóa công khai, thì chỉ có khóa bí mật mới giải mã được.

→ Gửi :

-Sau khi đăng ký một chứng chỉ số (với nhà cung cấp chứng chỉ số), ta được cấp một khóa riêng (khóa bí mật) lưu ở một chỗ 'kín' (ẩn) trên PC của chúng ta.

- Trước khi gửi văn bản, chúng ta áp dụng một thuật toán phần mềm để nhận giá trị băm của văn bản gốc.

- Chúng ta mã hóa giá trị băm đó bằng khóa riêng (hay gọi là 'ký' lên giá trị băm), và thu được cái gọi là chữ ký điện tử.

- Sau đó văn bản gốc được gửi đi cùng với chữ ký điện tử và khóa công khai của chúng ta.

→ Nhận:

- Khi nhận được thư, người nhận sử dụng khóa công khai của người gửi giải mã chữ ký điện tử để biết được người gửi có đúng là ta không, và đồng thời thu được giá trị băm của văn bản gốc.

- Người nhận cũng dùng thuật toán băm để thu được giá trị băm của văn bản nhận được.

- Nếu 2 giá trị băm bằng nhau thì văn bản được khẳng định là toàn vẹn (không bị thay đổi từ sau khi người gửi ký).

Một chữ ký điện tử sẽ là một chữ ký điện tử nếu nó sử dụng một phương pháp mã hóa nào đó để đảm bảo tính toàn vẹn (thông tin) và tính xác thực. Ví dụ như một bản dự thảo hợp đồng soạn bởi bên bán hàng gửi bằng email tới người mua sau khi được ký (điện tử).

Một điều cần lưu ý là cơ chế của chữ ký điện tử khác hoàn toàn với các cơ chế sửa lỗi (như giá trị kiểm tra - checksum...). Các cơ chế kiểm tra không đảm bảo rằng văn bản đã bị thay đổi hay chưa. Các cơ chế kiểm tra tính toàn vẹn thì không bao giờ bao gồm khả năng sửa lỗi.

Hiện nay, các tiêu chuẩn được sử dụng phổ biến cho chữ ký điện tử là OpenPGP, được hỗ trợ bởi PGP và GnuPG, và các tiêu chuẩn S/MIME (có trong Microsoft Outlook). Tất cả các mô hình về chữ ký điện tử đều giả định rằng người nhận có khả năng có được khóa công khai của chính người gửi và có khả năng kiểm tra tính toàn vẹn của văn bản nhận được. Ở đây không yêu cầu giữa 2 bên phải có một kênh thông tin an toàn.

Một văn bản được ký có thể được mã hóa khi gửi nhưng điều này không bắt buộc. Việc đảm bảo tính bí mật và tính toàn vẹn của dữ liệu có thể được tiến hành độc lập.

- Các bước mã hóa:

Có thể hình dung các bước tạo ra chữ ký điện tử khi gửi như sau:

1. Thay đổi origin content gửi đi bằng cách dùng giải băm, lúc này sẽ nhận được một chuỗi ký tự mới gọi là message digest.

2. Dùng private key của người gửi để mã hóa chuỗi kí tự message digest thu được ở bước 1. Sử dụng giải thuật RSA thu được chữ ký điện tử của message ban đầu.

3. Gộp chữ ký điện tử vào message ban đầu sau đó ký nhận vào message. Sau khi đã ký nhận mọi sự thay đổi trên message sẽ bị phát hiện trong giai đoạn kiểm tra, ngoài ra, quá trình này sẽ đảm bảo rằng người nhận sẽ hoàn toàn tin tưởng rằng thông tin nhận

được xuất phát từ chính người gửi mà họ mong muốn chứ không phải bị giả mạo, thay đổi.

- Các bước kiểm tra nội dung có bị thay đổi hay không như sau:

1. Sử dụng public key của người gửi sau đó giải mã chữ ký điện tử của message.
2. Sử dụng giải thuật để băm message đính kèm.
3. Kết quả thu được sẽ so sánh với message, nếu trùng hợp hoàn toàn thì sẽ kết luận message này không bị thay đổi, không bị đánh cắp dữ liệu và thông điệp được nhận từ chính người gửi.

1.2.6 Sử dụng chữ ký điện tử

Các ngành công nghiệp sử dụng công nghệ chữ ký số để hợp lý hóa các quy trình và cải thiện tính toàn vẹn của tài liệu. Các ngành sử dụng chữ ký số bao gồm:

+ Chính phủ - Văn phòng Xuất bản của Chính phủ Hoa Kỳ xuất bản các phiên bản điện tử của ngân sách, luật công và tư và các dự luật quốc hội có chữ ký số. Chữ ký điện tử được các chính phủ trên toàn thế giới sử dụng cho nhiều mục đích khác nhau, bao gồm xử lý tờ khai thuế, xác minh giao dịch giữa doanh nghiệp với chính phủ (B2G), phê chuẩn luật và quản lý hợp đồng. Hầu hết các cơ quan chính phủ phải tuân thủ luật pháp, quy định và tiêu chuẩn nghiêm ngặt khi sử dụng chữ ký điện tử.

+ Chăm sóc sức khỏe - Chữ ký điện tử được sử dụng trong ngành chăm sóc sức khỏe để nâng cao hiệu quả của quá trình điều trị và hành chính, tăng cường bảo mật dữ liệu, cho việc kê đơn điện tử và nhập viện. Việc sử dụng chữ ký điện tử trong chăm sóc sức khỏe phải tuân theo Đạo luật về trách nhiệm giải trình và cung cấp bảo hiểm y tế năm 1996 (HIPAA).

+ Các công ty Sản xuất - Sản xuất sử dụng chữ ký số để tăng tốc quy trình, bao gồm thiết kế sản phẩm, đảm bảo chất lượng (QA), cải tiến sản xuất, tiếp thị và bán hàng. Việc sử dụng chữ ký số trong sản xuất chịu sự điều chỉnh của Tổ chức Tiêu chuẩn hóa Quốc tế (ISO) và Chứng chỉ Sản xuất Kỹ thuật số của Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST) (DMC).

+ Dịch vụ tài chính - Khu vực tài chính Hoa Kỳ sử dụng chữ ký số cho các hợp đồng, ngân hàng không cần giấy tờ, xử lý khoản vay, tài liệu bảo hiểm, thế chấp, v.v. Lĩnh vực được quản lý chặt chẽ này sử dụng chữ ký điện tử với sự chú ý cẩn thận đến các quy định và hướng dẫn được đưa ra bởi Đạo luật chữ ký điện tử trong toàn cầu và thương mại quốc gia (Đạo luật về chữ ký điện tử), các quy định của UETA bang, Cục bảo vệ tài chính người tiêu dùng (CFPB) và Cơ quan tài chính liên bang Hội đồng Kiểm tra Định chế (FFIEC).

1.3 Cách làm việc của chữ ký điện tử

Digital Signature được tạo ra và kiểm tra bằng mật mã, đó là một phương pháp thuộc lĩnh vực toán học, nó chuyển toàn bộ message thành một dạng khó có thể nhận dạng và có thể được giải mã. Digital signature sử dụng hai khóa thông dụng, một khóa để tạo ra digital signature hoặc chuyển message thành dạng khó nhận dạng, một khóa dùng để kiểm tra digital signature hoặc để chuyển message đã mã hóa về dạng nguyên thủy của nó.

Digital signature là cách cơ bản để bảo mật cho một tài liệu điện tử (e-mail, spreaDigital Signatureheet_bảng tính, text file,..) đáng tin cậy. Đáng tin nghĩa là ta biết ai đã tạo ra tài liệu và ta biết nó không bị thay đổi trong bất cứ cách nào từ người tạo ra nó. Digital signature dựa vào thuật toán mã hoá để bảo đảm độ tin cậy. Mã hoá là quá trình mang tất cả dữ liệu từ một máy tính gửi sang máy tính khác và mã hóa nó thành một dạng mà chỉ có máy tính được gửi mới có thể giải mã. Độ tin cậy là quá trình kiểm tra xác nhận được thông tin đến từ một nguồn tin cậy. Hai quá trình này liên quan chặt chẽ đến digital signature.

Một Digital Signature có thể được xem như một giá trị số, được biểu diễn như một dãy các ký tự, và được sử dụng trong tin học như một biểu thức toán học. Biểu thức phụ thuộc vào hai đầu vào: dãy các ký tự biểu diễn dòng dữ liệu điện tử được ký và số bảo mật được tham chiếu đến như một signature public key, điều này có nghĩa là với mỗi chữ ký thì chỉ duy nhất người đã ký mới có thể truy xuất đến public key. Public key là

khoá công khai cho tất cả mọi người, nó giống như số điện thoại trong danh bạ điện thoại, cho phép việc kiểm tra chữ ký. Kết quả cho thấy việc biểu diễn chữ ký số gắn vào dữ liệu điện tử giống như sử dụng chữ ký tay trên giấy trong tài liệu văn bản.

Digital signature làm việc dựa trên hai khoá là public key và private key và thực hiện qua hai giai đoạn là việc hình thành chữ ký trên tài liệu ở phía người gửi và việc xác nhận tài liệu nhận được chính xác và nguyên vẹn hay không ở phía người nhận. Vấn đề bảo mật ở digital signature không giống với các phương pháp mã hoá cổ điển là chỉ dùng một khoá cho cả việc mã hoá ở người gửi và giải mã ở người nhận mà sử dụng hai khoá: private key để mã hoá và public key để giải mã kiểm tra.

1.3.1 Quá trình ký trong Message

- Bước 1:

Băm tài liệu gửi thành các hash-value hay còn được gọi là Message Digest, các Message Digest này sẽ được tính toán để đưa vào quá trình mã hoá chữ ký.

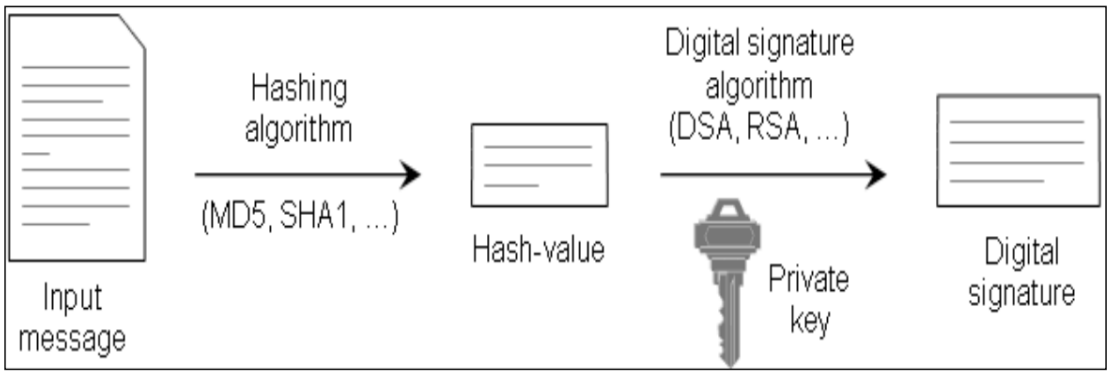
- Bước 2: Tính Message Digest

Trong bước hai của tiến trình, một hash-value (giá trị băm) của một message thường được gọi là Message Digest được tính toán bằng cách áp dụng các thuật toán băm mã hoá cryptographic hashing arthgorithm như MD2, MD4, MD5, SHA1,…Một hash-value đã tính của message là một dãy bit liên tục, có độ dài cố định, được trích rút từ message theo cách nào đó. Tất cả các thuật toán chính xác cho việc tính toán message digest được cung cấp như một phép biến đổi toán học, trong đó cứ một bit đơn từ input message được biến đổi thì một digest khác được gửi đến. Với cách làm việc như vậy các thuật toán là rất bảo đảm độ tin cậy trước các cuộc tấn công

- Bước 3: Tính Digital Signature

Trong bước hai của việc ký message, thông tin nhận được trong bước băm message (Message Digest) đã mã hoá với khoá private key của người ký vào message, vì thế một giá trị băm giải mã cũng được gọi là Digital Signature được gửi đến. Vì mục đích này, các thuật toán mã hoá cho việc tính chữ ký số từ message digest được dùng.

Thuật toán thường được sử dụng là RSA, DIGITAL SIGNATUREA, ECDIGITAL SIGNATUREA. Thông thường, chữ ký số gắn vào message trong định dạng đặc biệt để kiểm tra khi cần thiết.



Hình 1-4: Quá trình ký trong Message.

1.3.2 Quá trình kiểm tra xác nhận chữ ký trên tài liệu

- Bước 1: Tính Current Hash – Value

Trong bước một, một hash-value của message đã ký được tính. Với việc tính này thì vẫn sử dụng thuật toán băm như đã dùng trong suốt quá trình ký. Hash-value nhận được được gọi là current hash-value bởi vì nó được tính từ trạng thái hiện thời của message.

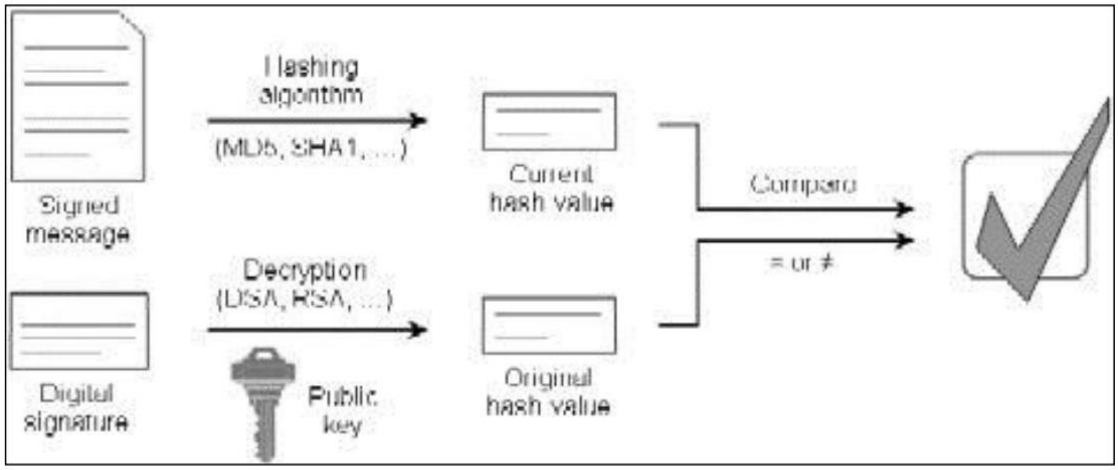
- Bước 2: Tính Original Hash – Value

Trong bước hai của quá trình kiểm tra digital signature, digital signature được giải mã với cũng với thuật toán mã hoá đã được sử dụng trong suốt quá trình ký. Việc giải mã được thực hiện bằng khoá public key tương ứng với khoá private key được dùng trong suốt quá trình ký của message. Kết quả là, chúng ta nhận được original hash-value mà đã được tính từ message gốc trong suốt bước một của quá trình ký (original message digest).

- Bước 3: So sánh Current với Original Hash – Value

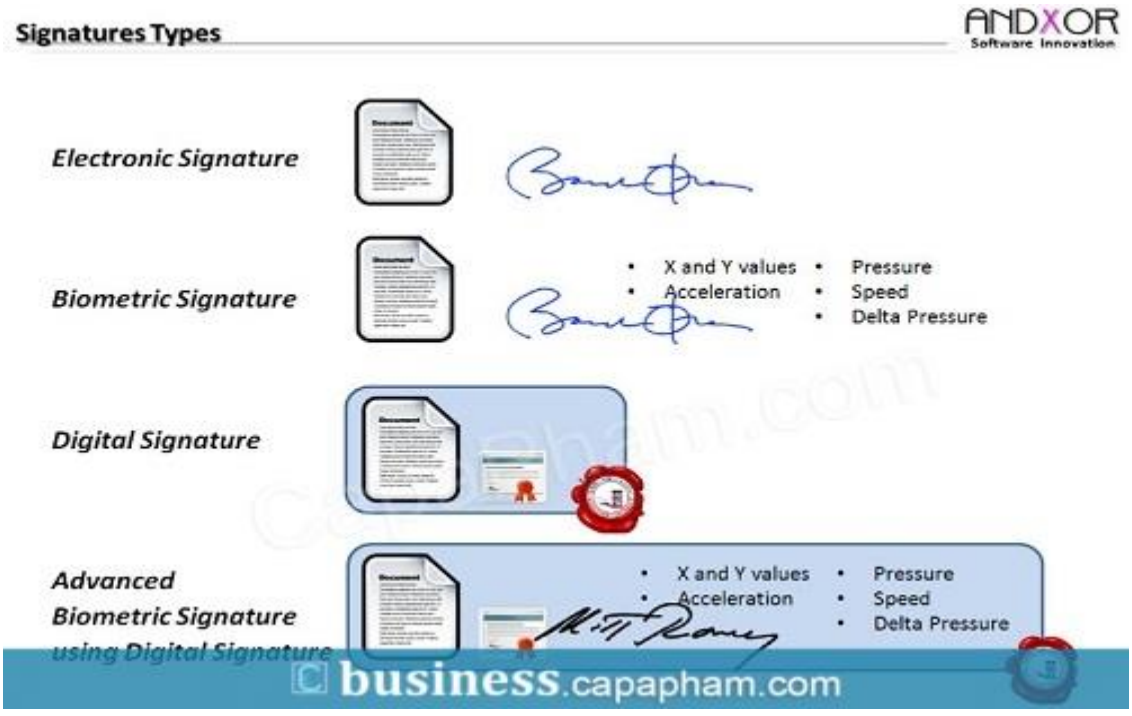
Trong bước ba, chúng ta đối chiếu current hash-value nhận được trong bước một với original hash-value nhận được trong bước hai. Nếu hai giá trị này giống hệt nhau thì

việc kiểm tra sẽ thành công nếu chứng minh được message đã được ký với khoá private key đúng với khoá public key đã được dùng trong quá trình kiểm tra. Nếu hai giá trị này khác nhau thì nghĩa là digital signature là sai và việc kiểm tra là thất bại.



Hình 1-5: Quá trình kiểm tra xác nhận chữ ký trên tài liệu.

1.4 Chữ ký điện tử và chữ ký số



Hình 1-6: Chữ ký điện tử và một số chữ ký khác.

- Giống nhau

Tính duy nhất của cả hai loại chữ ký này đó là đều thay thế cho chữ ký viết tay truyền thống và được sử dụng trong các giao dịch trực tuyến.

- Khác nhau

Yếu tố so sánh	Chữ ký điện tử	Chữ ký số
Tính chất	Chữ ký điện tử có thể là bất kỳ biểu tượng, hình ảnh, quy trình nào được đính kèm với tin nhắn hoặc tài liệu biểu thị danh tính của người ký và hành động đồng ý với nó.	Chữ ký số có thể được hình dung như một "dấu vân tay" điện tử, được mã hóa và xác định danh tính người thực sự ký nó.
Tiêu chuẩn	Không phụ thuộc vào các tiêu chuẩn. Không sử dụng mã hóa.	Sử dụng các phương thức mã hóa mật mã.
Cơ chế xác thực	Xác minh danh tính người ký thông qua email, mã PIN điện thoại, vv.	ID kỹ thuật số dựa trên chứng chỉ - Digital Signature Certificate (DSC).
Tính năng	Xác minh một tài liệu.	Bảo mật một tài liệu.
Xác nhận	Không có quá trình xác nhận cụ thể.	Được thực hiện bởi các cơ quan chứng nhận tin cậy hoặc nhà cung cấp dịch vụ ủy thác.
Bảo mật	Dễ bị giả mạo.	Độ an toàn tương đối cao.

Phần mềm độc quyền	Có thể được xác nhận bởi bất cứ ai mà không cần phần mềm xác minh độc quyền.	Trong nhiều trường hợp, chữ ký số không được ràng buộc về mặt pháp lý và sẽ yêu cầu phần mềm độc quyền để xác nhận chữ ký số.

CHƯƠNG 2 – MỘT SỐ ỨNG DỤNG

Chữ ký điện tử thường được sử dụng trong các hoạt động thương mại điện tử. Ví dụ trong các trong các trường hợp sau:

1. 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.

2. Các giao dịch thanh toán trực tuyến của ngân hàng.

3. Ký xác nhận khi mua hàng online.

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 …

→ Phạm vi của chữ ký điện tử không chỉ giới hạn trong việc trao đổi tin nhắn. Chữ ký viết tay được sử dụng phổ biến trong các loại đơn xin chứng minh nhân thân của người ký. Tương tự như vậy, chữ ký điện tử có thể được sử dụng cho tất cả các loại hồ sơ điện tử. Bất kỳ lĩnh vực nào mà tính toàn vẹn và hợp lệ của dữ liệu là quan trọng, có thể sử dụng Chữ ký điện tử. Ở đây chúng tôi thảo luận về một số ứng dụng này:

2.1 Smart Cards (Thẻ thông minh)

Hình 2-7: Thẻ thông minh hiện nay.

Thẻ thông minh là một thẻ nhựa, kích thước và hình dạng của thẻ tín dụng, với một chip máy tính nhúng. Một ý tưởng cũ của nó các bằng sáng chế đầu tiên đã được nộp 20 năm trước đây nhưng những hạn chế thực tế làm cho họ khả thi chỉ có năm hoặc lâu hơn năm trước đây. Kể từ đó họ đã cất cánh, chủ yếu là ở châu Âu. Nhiều quốc gia sử dụng thẻ thông minh để thanh toán điện thoại. Ngoài ra còn có thẻ tín dụng thông minh, thẻ tiền mặt thông minh, tất cả mọi thứ thông minh thẻ. Các công ty thẻ tín dụng Mỹ đang nhìn vào công nghệ này, và trong vòng một vài năm thậm chí ngược người Mỹ sẽ có thẻ thông minh trong ví của họ

Một thẻ thông minh có chứa một máy tính nhỏ (thường là một bộ vi xử lý 8-bit), RAM (khoảng một quarterkilobyte), ROM (khoảng 6 hoặc 8 kilobyte), và hoặc EPROM hoặc EEPROM (một vài kilobyte). Thẻ thông minh thế hệ tương lai chắc chắn sẽ có nhiều dung lượng hơn, nhưng một số hạn chế về vật lý trên thẻ thông minh khiến việc mở rộng trở nên khó khăn. Thẻ có hệ điều hành, chương trình và dữ liệu riêng. (Những

gì nó không có là sức mạnh; mà đến khi thẻ được cắm vào một người đọc.) Và nó được an toàn. Trong một thế giới mà bạn có thể không tin tưởng người khác máy tính hoặc điện thoại hoặc bất cứ điều gì, bạn vẫn có thể tin tưởng một thẻ mà bạn giữ với bạn trong ví của bạn. Thẻ thông minh có thể có các giao thức mật mã và thuật toán khác nhau được lập trình vào chúng. Họ có thể được cấu hình như một ví điện tử, và có thể chi tiêu và nhận tiền mặt kỹ thuật số. Họ có thể thực hiện giao thức xác thực không kiến thức;họ có thể có khóa mã hóa riêng của họ. Họ có thể ký tài liệu hoặc mở khóa ứng dụng trên máy tính. Một số thẻ thông minh được giả định là chống giả mạo; điều này thường bảo vệ các tổ chức mà vấn đề thẻ. Một ngân hàng sẽ không muốn bạn có thể hack thẻ thông minh của họ để cung cấp cho mình nhiều tiền hơn

2.2 Mitrenet

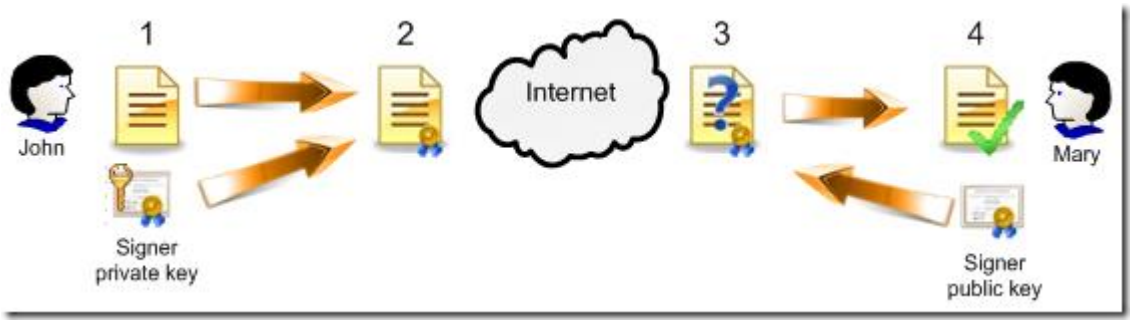
Một trong những triển khai sớm nhất của mật mã khóa công khai là hệ thống thử nghiệm MEMO (MITRE Encrypted Mail Office). MITRE là một nhà thầu DoD, một chính phủ nghĩ rằng xe tăng, và một bó tất cả các xung quanh của guys thông minh. MEMO là một hệ thống thư điện tử an toàn cho người dùng trong mạng MITRENET, sử dụng mật mã khóa công khai để trao đổi khóa và DES để mã hóa tệp. Trong hệ thống MEMO, tất cả các khóa công khai được lưu trữ trong một trung tâm phân phối khóa công cộng, đó là một nút chọn một riêng biệt trên mạng. Chúng được lưu trữ trong EPROM để ngăn chặn bất cứ ai thay đổi chúng. Khóa riêng được tạo ra bởi người dùng hoặc bởi hệ thống. Đối với người dùng để gửi tin nhắn an toàn, hệ thống đầu tiên thiết lập một đường dẫn liên lạc an toàn với Trung tâm phân phối khóa công khai. Người dùng yêu cầum một tập tin của tất cả các phím công cộng từ trung tâm. Nếu người dùng vượt qua một bài kiểm tra nhận dạng bằng cách sử dụng khóa riêng của mình, Trung tâm sẽ gửi danh sách này cho máy trạm người dùng. Danh sách được mã hóa bằng DES để đảm bảo tính toàn vẹn của tệp.

2.3 ISDN

Bell-Northern Research đã phát triển một nguyên mẫu thiết bị đầu cuối điện thoại điện thoại từ xa Mạng lưới Dịch vụ Kỹ thuật số Tích hợp (ISDN) an toàn. Là một chiếc điện thoại, nó không bao giờ được phát triển ngoài nguyên mẫu mà sản phẩm kết quả là Lớp phủ bảo mật dữ liệu gói. Thiết bị đầu cuối sử dụng trao đổi khóa Dif fi e-Hellman, chữ ký số RSA và mã hóa dữ liệu DES; nó có thể truyền và nhận giọng nói và dữ liệu ở tốc độ 64 kilobitsper giây

2.4 Time Stamped Signatures (Chữ ký đóng dấu thời gian)

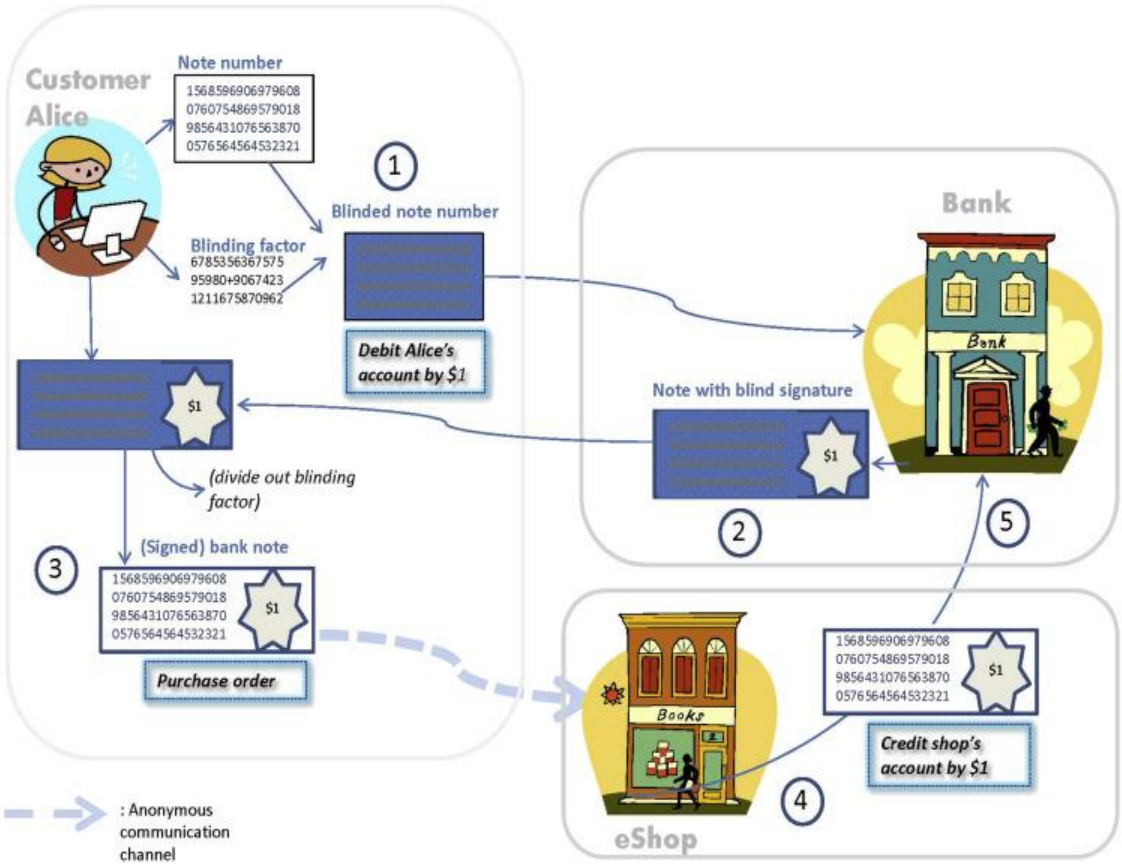
Đôi khi, một tài liệu đã ký cần được đóng dấu thời gian để ngăn nó bị thay thế bằng một câu quảng cáo. Đây được gọi là lược đồ chữ ký điện tử có dấu thời gian.



Hình 2-8: Chữ ký đóng dấu thời gian.

2.5 Blind Signatures (Chữ ký mù)

Đôi khi chúng tôi có một tài liệu mà chúng tôi muốn ký mà không tiết lộ nội dung của tài liệu đó cho người ký



Hình 2-9: Mô phỏng chữ ký mù.

2.6 Electronic Mail (Thư điện tử)

Hình 2-10: Thư điện tử sử dụng hiện nay.

Khi chúng ta gửi e-mail đến một hộp thư, chủ nhân của hộp thư phải nhận e-mail đó ở dạng ban đầu. Nếu trong quá trình vận chuyển, nội dung thay đổi do vô tình hoặc do sự xâm nhập của bên thứ ba, thì đầu nhận sẽ có thể nhận ra sự thay đổi này trong nội dung. Ngoài ra, không ai có thể gửi e-mail giả dạng người khác. Cả hai yếu tố này đều được Chữ ký số đảm nhận. Bất kỳ thay đổi nào trong e-mail sẽ ảnh hưởng đến thông báo thư do SHA tạo ra và do đó chữ ký điện tử sẽ được đánh dấu là chưa được xác minh. Vì vậy người nhận sẽ từ chối tin nhắn đó.

2.7 Data Storage (Lưu trữ dữ liệu)

Đây là một ứng dụng thú vị nữa của chữ ký điện tử. Giả sử một lượng lớn dữ liệu được lưu trữ trên máy tính. Chỉ những người được ủy quyền mới được phép thực hiện các thay đổi đối với dữ liệu. Trong trường hợp đó, cùng với dữ liệu, chữ ký cũng có thể được lưu trữ dưới dạng tệp đính kèm. Chữ ký này được tạo từ bản tóm tắt dữ liệu và khóa riêng tư. Vì vậy, nếu bất kỳ thay đổi nào trong dữ liệu được thực hiện bởi một số

người không được phép, thì chúng sẽ dễ dàng được nhận ra tại thời điểm xác minh chữ ký và do đó, bản sao dữ liệu đó sẽ bị loại bỏ.

2.8 Electronic Funds Transfer (Chuyển thư điện tử)

Hình 2-11: Xu thế chuyển thư điện tử.

Các ứng dụng như ngân hàng trực tuyến, thương mại điện tử đều có thể loại. Trong các ứng dụng này, thông tin được trao đổi bởi hai bên là rất quan trọng và do đó phải duy trì tính bí mật và tính xác thực cao. Chữ ký điện tử có thể đảm bảo việc xác thực thông tin của chúng, nhưng cần duy trì tính bí mật bằng cách sử dụng một số kỹ thuật mã hóa. Vì vậy, trước khi tạo thông báo tóm tắt, thông báo phải được mã hóa. Sau đó, chữ ký điện tử được tạo và đính kèm vào tin nhắn. Ở đầu nhận sau khi xác minh chữ ký, tin nhắn được giải mã để khôi phục lại tin nhắn ban đầu

2.9 Software Distribution (Nhà phân phối phần mềm)

Các nhà phát triển phần mềm thường phân phối phần mềm của họ bằng một số phương tiện điện tử, ví dụ, internet. Trong trường hợp này, để đảm bảo rằng phần mềm vẫn chưa bị sửa đổi và nguồn của phần mềm là chính hãng, bạn có thể sử dụng Chữ ký số. Nhà phát triển ký vào phần mềm và người dùng xác minh chữ ký trước khi sử dụng. Nếu chữ ký được xác minh, thì chỉ người dùng mới có thể chắc chắn về tính hợp lệ của phần mềm đó.

CHƯƠNG 3 – MÔ PHỎNG CHỮ KÝ ĐIỆN TỬ VÀ KẾT LUẬN

3.1 Chương trình mô phỏng chữ ký điện tử

3.1.1 Kịch bản Demo

Bài báo cáo đồ án cuối ký được thực hiện nhằm mô phỏng chữ ký điện tử được áp dụng một cách rộng rãi hiện nay thông qua việc áp dụng thuật toán RSA. RSA là một hệ mã hóa bất đối xứng được phát triển bởi Ron Rivest, Adi Shamir và Leonard Adleman và được sử dụng rộng rãi trong công tác mã hoá và công nghệ chữ ký điện tử. Trong hệ mã hóa này, khóa công khai có thể chia sẻ công khai cho tất cả mọi người. Hoạt động của RSA dựa trên 4 bước chính: sinh khóa, chia sẻ key, mã hóa và giải mã. Để chứng minh tính thông dụng của thuật toán nhóm chúng tôi đã tạo chương trình viết bằng lập trình JavaSwing để làm mô phỏng. Trong đó nhóm chúng tôi thực hiện chương trình gồm các bước chính thông qua thuật toán RSA: Đầu tiên chúng tôi xây dựng chương trình cho phép tạo khóa công khai (Public Key) cũng như khóa bí mật (Private Key) và lựa chọn độ dài của khóa. Sau đó chúng tôi cho phép người gửi lựa chọn file sử dụng khóa bí mật để mã hóa hàm băm cũng như ký chữ ký trên đó. Người dùng sử dụng một file bất kỳ để nhận dạng có phù hợp hay không thông qua sử dụng khóa công khai để giải mã và kiểm tra chữ ký; cuối cùng chương trình thông báo kết quả chữ ký có toàn vẹn hay bị thay đổi cho người nhận biết kết quả.

3.1.2 Lợi ích của chương trình

- Giải quyết bài toán gì?

Chữ ký điện tử sử dụng RSA giải quyết cho bài toán về mã hóa bất đối xứng. Có thể sử dụng mã hóa bất đối xứng cho các hệ thống mà trong đó nhiều người dùng có thể cần mã hóa và giải mã tệp hoặc bộ dữ liệu, đặc biệt trong trường hợp không có giới hạn về tốc độ và sức mạnh tính toán. Ví dụ, có thể sử dụng phương thức mã hóa này trong hệ thống email được mã hóa, trong đó khóa công khai được sử dụng để mã hóa các email và khóa cá nhân được sử dụng để giải mã chúng. Khóa được sử dụng để mã hóa được

gọi là khóa công khai và có thể được chia sẻ với người khác. Còn khóa được sử dụng để giải mã là khóa cá nhân và cần được giữ bí mật.

→ Giá trị chữ ký điện tử:

+ Xác định nguồn gốc

+ Dữ liệu được gửi một cách toàn vẹn

+ Chữ ký số không thể phủ nhận

+ Phương thức mã hóa bất đối xứng cung cấp mức độ bảo mật cao hơn, bởi vì ngay cả khi ai đó lấy được tin nhắn và tìm thấy khóa công khai, họ cũng không thể giải mã tin nhắn.

- Thực hiện ra sao?

Việc ký tên và xác thực chữ ký số sử dụng hệ mã hóa RSA tương tự như quá trình mã hóa mà giải mã ở trên. Tuy nhiên vai trò của khóa công khai và khóa bí mật thì có thay đổi. Để tạo chữ ký, người gửi sẽ dùng khóa bí mật và người nhận sẽ dùng khóa công khai để xác thực chữ ký đó.

Chữ ký điện tử thường sử dụng phương pháp mã hóa giá trị băm của bản tin.

→Tác dụng của hàm băm:

+ Các hàm băm là hàm 1 chiều, vì vậy dù có được băm cũng không thể biết được bản tin gốc như thế nào.

+ Độ dài băm là cố định và thường rất nhỏ, vì vậy chữ số sẽ không chiếm quá nhiều dung lượng.

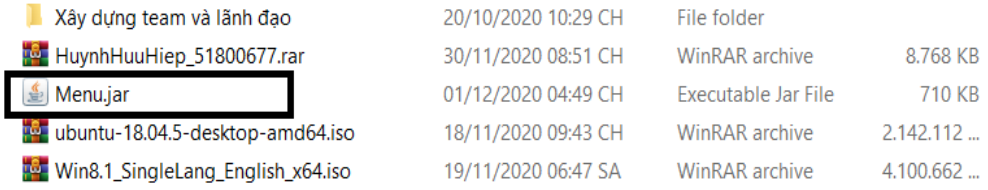
+ Giá trị băm còn có thể dùng để kiểm tra lại bản tin nhận được có nguyên vẹn hay không.

+ Hệ mã hóa bất đối xứng cho phép tạo chữ ký với khóa bí mật mà chỉ người chủ mới biết. Khi nhận gói tin, người nhận xác thực chữ ký bằng cách dùng khóa công khai giải mã, sau đó tính giá trị băm của bản tin gốc và so sánh với băm trong gói tin nhận được. Hai chuỗi này phải trùng khớp với nhau.

3.2 Chương trình Demo

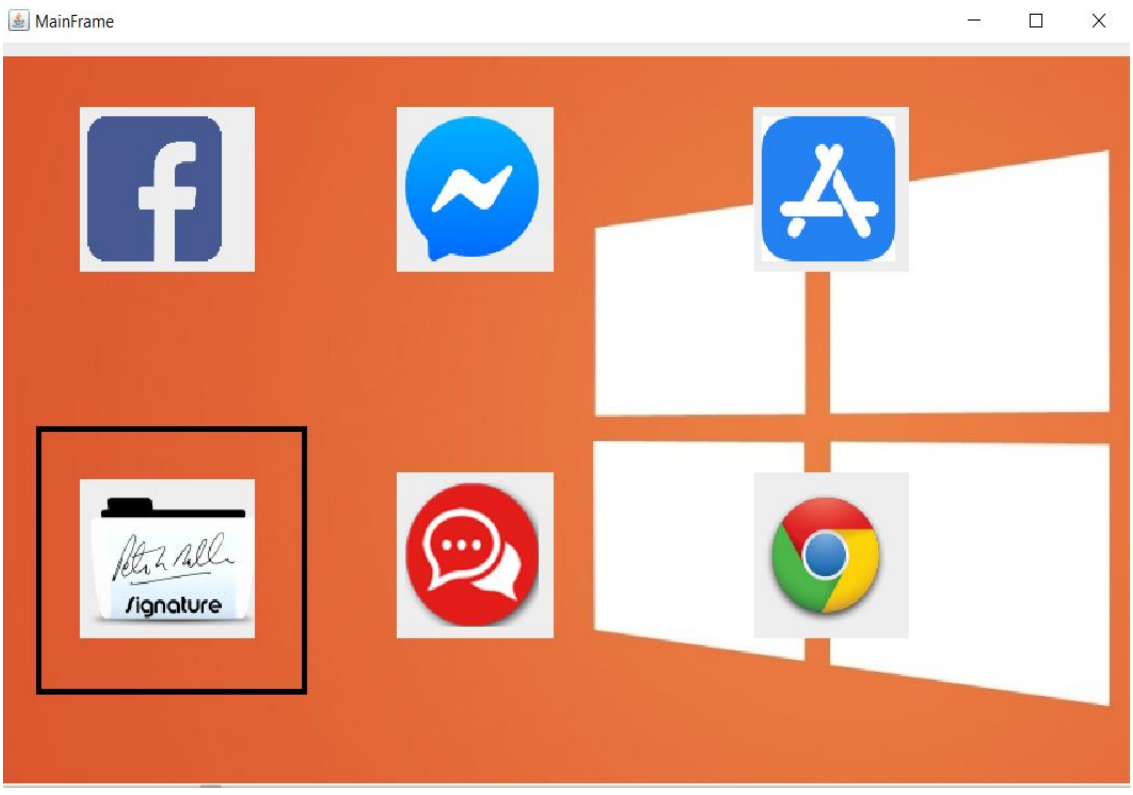
Dưới đây là hướng dẫn chạy chương trình cũng như các hình ảnh minh họa kết quả:

- Đầu tiên để chạy chương trình ta mở file Menu.jar do nhóm chúng tôi đã xuất ra file.jar để chạy nhanh hơn:



Hình 3-12: Giao diện chính cần chọn để chạy ứng dụng.

- Khi nó một màn hình Menu xuất hiện ta chọn biểu tượng "Signatures" để mở ứng dụng :



Hình 3-13: Giao diện chính của Menu.

- Khi Click xong một giao diện chữ ký điện tử sẽ xuất hiện như hình:

Hình 3-14: Giao diện chính của chương trình.

→ Giải thích:

Giao diện gồm 3 khung:

+ Khung đầu tiên là các bước chọn độ dài khóa, tạo khóa công khai và khóa bí mật

+ Khung thứ hai là quá trình ký chữ ký thông qua khóa bí mật từ người gửi

+ Khung thứ ba là quá trình kiểm tra chữ ký thông qua khóa công khai đến từ người nhận

+ Ngoài ra còn có cách sử dụng ứng dụng bằng cách Click vào icon “Guides” trên màn hình và nút “Back” để trở lại màn hình chính:

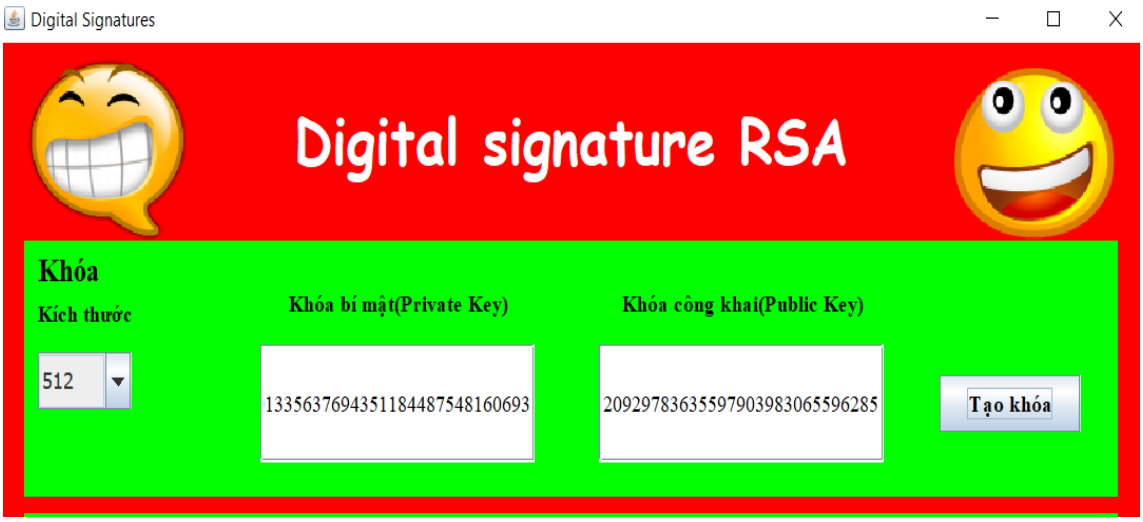
Hình 3-15: Click để mở hướng dẫn sử dụng.

- Khi nó sẽ xuất hiện giao diện hướng dẫn sử dụng ứng dụng khá chi tiết:

Hình 3-16: Giao diện hướng dẫn sử dụng chương trình.

- Tiếp theo ta sẽ thực hiện tạo và ký cũng như xác nhận trên ứng dụng:

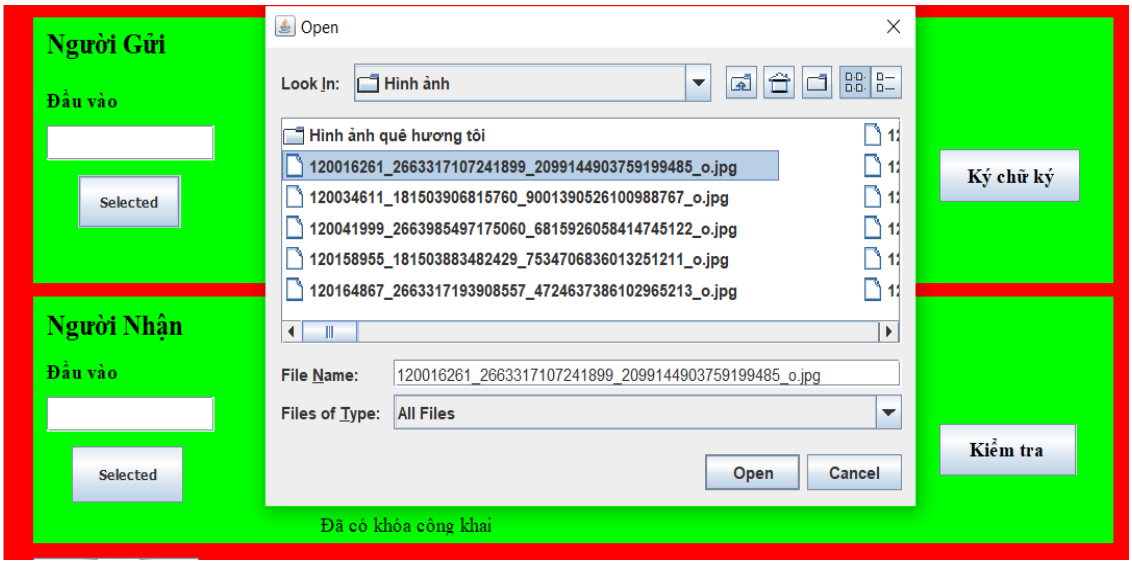
- Đầu tiên ta sẽ chọn một độ dài khóa bất kỳ ở đây mình chọn 512bit và Click nút tạo khóa để khóa công khai và khóa bí mật được tạo:



Hình 3-6: Giao diện tạo khóa công khai và bí mật.

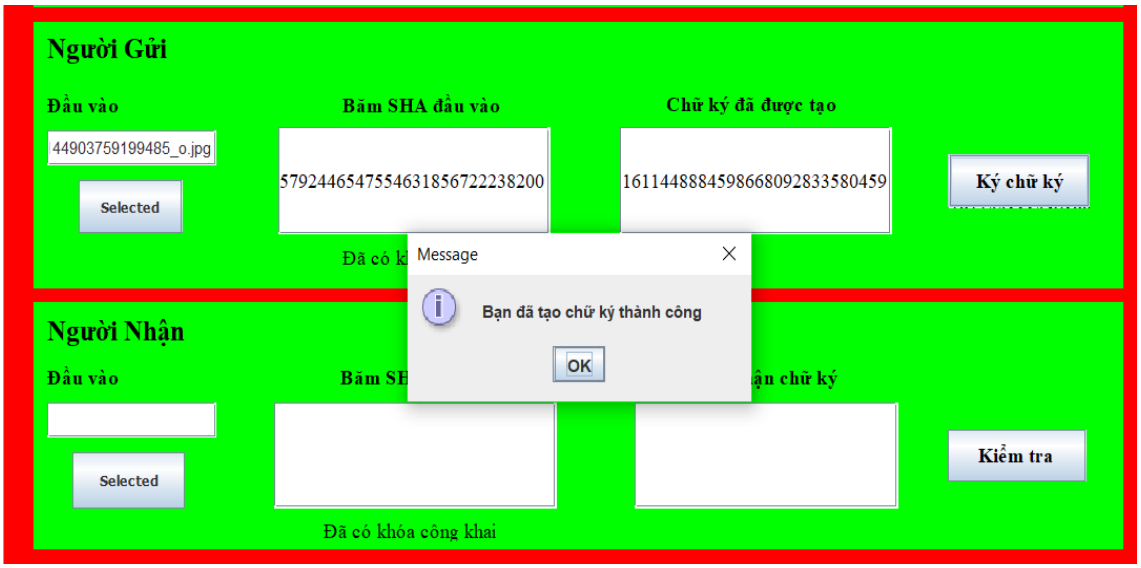
- Sau đó đến bước ký chữ ký:

- Đầu tiên ta Click vào Selected để chọn một file bất kỳ ở đây mình chọn một hình ảnh:



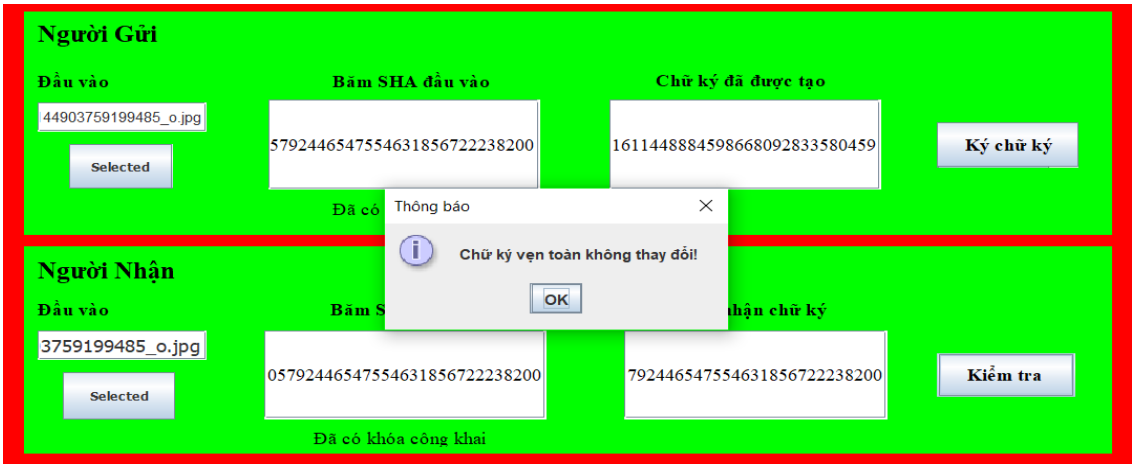
Hình 3-17: Giao diện chọn file bất kỳ.

- Sau đó Click vào nút "Ký chữ ký" để ký chữ ký thông qua người gửi sử dụng khóa bí mật để mã hóa hàm băm SHA thì khóa bí mật và chữ ký được ký cùng thông báo chữ ký được ký thành công:



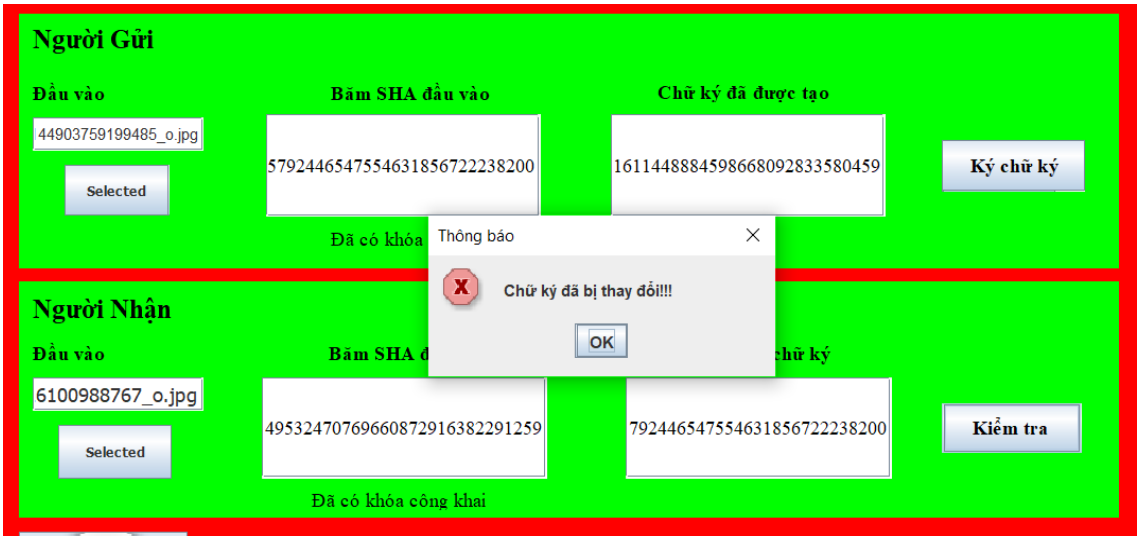
Hình 3-18: Giao diện ký chữ ký.

- Sau đó chúng ta sẽ kiểm tra chữ ký từ người nhận thông qua khóa công khai để kiểm tra chữ ký. Tương tự chúng ta chọn một file bất kỳ để kiểm tra nó ở đây mình chọn hình ảnh đúng hình ảnh trên và Click nút Kiểm tra thì thông báo chữ ký hợp lệ sẽ tạo ra do đúng với hình ảnh ban đầu:



Hình 3-19: Giao diện kiểm tra chữ ký.

- Ngược lại chúng tối chọn một hình ảnh khác kết quả sẽ thông báo chữ ký bị thay đổi:



Hình 3-20: Giao diện thông báo chữ ký bị thay đổi.

→ Đó là những gì mà nhóm mình đã thực hiện được tuy còn khá nhiều sai sót mong nhận được những góp ý đánh giá đến từ mọi người.

3.3 Kết luận

- Những lợi ích

Đây là những lý do phổ biến để áp dụng chữ ký điện tử trong truyền thông:

→ Xác thực

Mặc dù thông báo có thể thường bao gồm thông tin về thực thể gửi tin nhắn, thông tin đó có thể không chính xác. Chữ ký điện tử có thể được sử dụng để xác thực nguồn tin nhắn. Quyền sở hữu của một khóa bí mật chữ ký điện tử được ràng buộc với một người dùng cụ thể, một chữ ký hợp lệ cho thấy rằng thông tin đó đã được gửi bởi người dùng đó. Tầm quan trọng của tính xác thực cao trong tính xác thực của người gửi đặc biệt rõ ràng trong bối cảnh tài chính. Ví dụ: giả sử chi nhánh của ngân hàng gửi hướng dẫn đến trung tâm của ngân hàng yêu cầu thay đổi số dư của tài khoản. Nếu trung tâm không tin rằng một thông điệp như vậy thực sự được gửi từ một nguồn được ủy quyền, thì hành động theo yêu cầu như vậy có thể là một hành động nghiêm trọng.

→ Tính toàn vẹn

Trong nhiều trường hợp, người gửi và người nhận tin nhắn có thể có nhu cầu đảm bảo rằng nội dung của chúng không bị thay đổi trong quá trình truyền. Mặc dù mã hóa ẩn nội dung của một tin nhắn, nhưng có thể thay đổi một tin nhắn được mã hóa mà không hiểu nó. (Một số nhịp thuật toán mã hóa, được gọi là nhịp không thể xử lý, ngăn chặn điều này, nhưng một số khác thì không.) Tuy nhiên, nếu một thư được ký điện tử, bất kỳ thay đổi nào trong thư sẽ làm mất hiệu lực của chữ ký. Hơn nữa, không có cách nào hợp lý để sửa đổi một thông điệp và chữ ký của nó để tạo ra một thông điệp mới với chữ ký hợp lệ, vì điều này vẫn được coi là không khả thi về mặt tính toán đối với hầu hết các hàm băm mật mã

Một số lợi ích khác:

- ✓ Tiết kiệm được thời gian và chi phí trong quá trình hoạt động giao dịch điện tử.

- ✓ Linh hoạt trong cách thức ký kết các văn bản hợp đồng, buôn bán,… có thể diễn ra ở bất kỳ nơi đâu, ở bất kỳ thời gian nào.
- ✓ Đơn giản hóa quy trình chuyển, gửi tài liệu, hồ sơ cho đối tác khách hàng, cơ quan tổ chức.
- ✓ Bảo mật danh tính của cá nhân, doanh nghiệp an toàn.
- ✓ Thuận lợi trong việc nộp hồ sơ thuế, kê khai thuế cho doanh nghiệp khi chỉ cần sử dụng chữ ký điện tử thực hiện các giao dịch điện tử là có thể hoàn thành xong các quá trình đó.
- ✓ Bảo mật danh tính của cá nhân, doanh nghiệp một cách an toàn.

Những hạn chế

Mặc dù kỹ thuật chữ ký số là một phương pháp rất hiệu quả để duy trì tính toàn vẹn và tính toàn vẹn của dữ liệu, nhưng có một số nhược điểm liên quan đến phương pháp này:

- Khóa cá nhân phải được giữ một cách an toàn. Việc mất khóa cá nhân có thể gây ra thiệt hại nghiêm trọng vì bất kỳ ai có được khóa cá nhân đều có thể sử dụng nó để gửi tin nhắn đã ký cho chủ sở hữu khóa công khai và khóa công khai sẽ nhận ra những tin nhắn này là hợp lệ và do đó người nhận sẽ cảm thấy rằng tin nhắn đã được xác thực. chính chủ.
- Quá trình tạo và xác minh chữ ký điện tử đòi hỏi một lượng thời gian đáng kể, vì vậy, đối với việc trao đổi thông điệp thường xuyên, tốc độ truyền thông sẽ giảm.
- Khi chữ ký điện tử không được khóa công khai xác minh, thì người nhận chỉ cần đánh dấu các tin nhắn là không hợp lệ nhưng anh ta không biết liệu tin nhắn đó bị hỏng hay khóa cá nhân giả đã được sử dụng.
- Để sử dụng chữ ký điện tử, người dùng phải lấy khóa cá nhân và khóa công khai, người nhận cũng phải có chứng chỉ chữ ký số. Điều này đòi hỏi họ phải trả thêm số tiền.

- Nếu người dùng thay đổi khóa riêng tư của mình sau mỗi khoảng thời gian đã định, thì hồ sơ của tất cả những thay đổi này phải được lưu giữ. Nếu tranh chấp nảy sinh về một tin nhắn đã gửi trước đó thì cặp khóa cũ cần được chuyển đến. Do đó việc lưu trữ tất cả các khóa trước đó là một khoản phí khác.
- Mặc dù chữ ký số cung cấp tính xác thực nhưng nó không đảm bảo tính bí mật của dữ liệu. Để đảm bảo bí mật, một số kỹ thuật khác như mã hóa và giải mã cần được sử dụng

Mở rộng

Chữ ký điện tử là một quá trình đảm bảo rằng nội dung của thư đã không được thay đổi khi truyền đi. Khi các máy chủ, kỹ thuật số ký một tài liệu, ta thêm một băm một chiều (mã hóa) của các tin nhắn nội dung bằng cách sử dụng cặp khóa công cộng và riêng tư của mình. Khách hàng của ta vẫn có thể đọc nó, nhưng quá trình tạo ra một "chữ ký" mà chỉ có khóa công khai của máy chủ có thể giải mã. Khách hàng, bằng cách sử dụng khóa công khai của máy chủ, sau đó có thể xác nhận người gửi cũng như tính toàn vẹn của nội dung thư. Cho dù đó là:

• Một email

• Một đơn đặt hàng trực tuyến

• Hoặc một bức ảnh có hình mờ trên eBay

Nếu quá trình truyền đến nhưng chữ ký điện tử không khớp với khóa công khai trong chứng chỉ số, thì khách hàng biết rằng thông điệp chưa bị thay đổi.

TÀI LIỆU THAM KHẢO

Tiếng Việt

1. https://business.capapham.com/chu-ky-dien-tu-chu-ky-so-la-gi/#Chu_ky_so_la_gi_What_is_a_Digital_Signature. [Accessed 10 11 2020].
2. https://tincoinviet.net/digital-signature-la-gi/. [Accessed 12 10 2020].

Tiếng Anh

3. https://en.wikipedia.org/wiki/Digital_signature. [Accessed 10 10 2020].
4. https://searchsecurity.techtarget.com/definition/digital-signature. [Accessed 1 10 2020].
5. https://www.slideshare.net/jolly9293/seminar-ppt-on-digital-signature. [Accessed 11 10 2020].
6. http://computerfun4u.blogspot.com/2009/02/applications-of-digital-signature.html. [Accessed 1 10 2020].