BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC DÂN LẬP HẢI PHÒNG

-------o0o-------

MỘT SỐ BÀI TOÁN VỀ AN TOÀN THÔNG TIN TRONG GIAI ĐOẠN KIỂM PHIẾU ĐIỆN TỬ

ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC HỆ CHÍNH QUY

NGÀNH CÔNG NGHỆ THÔNG TIN

Giáo viên h- ớng dẫn: PGS. TS Trịnh Nhật Tiến

Sinh viên: Nguyễn Việt Thịnh

Mã số sinh viên: 1013101015

Hải Phòng, 7/2012

LỜI CẢM ƠN

Lời đầu tiên, em xin được gửi lời cảm ơn chân thành và sâu sắc nhất tới PGS.TS Trịnh Nhật Tiến – người Thầy luôn chỉ bảo, hướng dẫn hết sức nhiệt tình, giúp đỡ em trong suốt quá trình xây dựng đồ án.

Em xin chân thành cảm ơn các Thầy, Cô giáo đã dạy dỗ em trong suốt quá trình học tập tại trường Đại học Dân lập Hải Phòng. Những kiến thức các thầy cô truyền đạt sẽ mãi là hành trang để em vững bước trong tương lai.

Xin được cảm ơn tới các bạn lớp CTL401 đã cung cấp cho mình những tài liệu quý báu để mình hoàn thành đồ án. Cảm ơn tới tất cả các bạn bè của mình đã luôn sát vai, tin tưởng và giúp đỡ mình trong suốt những năm học qua.

Cuối cùng, con xin được gửi lời biết ơn sâu sắc nhất tới Bố mẹ và những người thân trong gia đình, những người luôn dành cho con tình yêu, niềm tin và động viên con trong suốt quá trình học tập.

Hải Phòng, tháng 7 năm 2012

Sinh viên: Nguyễn Việt Thịnh

GIỚI THIỆU ĐỀ TÀI

Đồ án tốt nghiệp này trình bày một số hiểu biết cơ bản về bỏ phiếu và bỏ phiếu điện tử, tình hình triển khai bỏ phiếu điện tử ở Việt Nam. Qua đó giúp người đọc hiểu thêm về quá trình kiểm phiếu, đồng thời cũng giúp hình dung được viễn cảnh bỏ phiếu điện tử ở Việt Nam.

Đồ án cũng trình bày những kiến thức tổng quát về phương pháp mã hóa khóa công khai, một phương pháp được sử dụng rộng rãi trong việc mã hóa văn bản và chữ ký số. Cùng với chữ ký số, hệ thống PKI (Cơ sở hạ tầng khóa công khai) cũng được giới thiệu giúp người đọc hiểu được phần nào cốt lõi của việc đảm bảo an toàn thông tin trong giai đoạn kiểm phiếu điện tử.

Phần chính của đồ án là nêu ra một số bài toán về an toàn thông tin trong giai đoạn kiểm phiếu điện tử. Phần này cũng phân tích kĩ các giải pháp và đưa ra những phương án có thể sử dụng để triển khai trong thực tế.

MỤC LỤC

CÁC KÝ HIỆU VIẾT TẮT

CT	Cử tri.
ĐH	Ban điều hành.
ĐK	Ban đăng ký.
KT	Ban kiểm tra
KP	Ban kiểm phiếu
TT	Thông tin
RSA	Tên 3 nhà khoa học: Ron Rivest, Adi Shamir, Leonard Adleman.
ID	Identify (Định danh)
SSL	Secure Sockets Layer
CA	Certificate Authority
HTTP	HyperText Transfer Protocol

CÁC KÝ HIỆU TOÁN HỌC

Z_n	Trường hữu hạn với n phần tử.
Sig_a	Thuật toán ký số
Ver	Thuật toán kiểm tra chữ ký
Blind(x)	Thuật toán làm mù
UnBlind(x)	Thuật toán xóa mù
Enc	Mã hóa
E_k	Thuật toán mã hóa

Chương 1. CÁC KHÁI NIỆM CƠ BẢN

1.1. TỔNG QUAN VỀ BỎ PHIẾU ĐIỆN TỬ

1.1.1. Khái niệm về bỏ phiếu

Bỏ phiếu là việc người dùng phiếu để bày tỏ sự lựa chọn hay thái độ của mình trong cuộc bầu cử hoặc biểu quyết.

Một cuộc bỏ phiếu thành công phải bảo đảm các tính chất:

Quyền bỏ phiếu: chỉ người có quyền bầu cử mới được bỏ phiếu. Mỗi cử tri chỉ được bỏ phiếu một lần.

Bí mật: không thể biết được lá phiếu nào đó là của ai, trừ cử tri của nó.

Kiểm soát kết quả: có thể phát hiện được những sai sót trong quá trình bỏ phiếu. Cho đến nay các cuộc bỏ phiếu vẫn được thực hiện theo cách truyền thống, tuy nhiên với tốc độ phát triển của ngành công nghệ thông tin, đặc biệt là xu thế thực hiện "Chính phủ điện tử" thì việc "bỏ phiếu điện tử" thay thế phương thức truyền thống là điều sẽ diễn ra trong tương lai gần.

1.1.2. Khái niệm bỏ phiếu điện tử

Người ta bỏ phiếu để bầu cử các chức vụ, chức danh hay để thăm dò dư luận về một kế hoạch, chính sách nào đó. Hiện nay có 2 loại bỏ phiếu chính. Bỏ phiếu trực tiếp tại hòm phiếu bằng các lá phiếu in trên giấy. ***Bỏ phiếu từ xa*** bằng các lá phiếu "số hóa" tạm gọi là các lá phiếu điện tử từ các máy tính cá nhân trên mạng, trên điện thoại di động…Nó cũng được gọi là ***bỏ phiếu điện tử.***

Bỏ phiếu điện tử là bỏ phiếu bằng các phương pháp điện tử. Các hệ thống bỏ phiếu điện tử cho phép cử tri sử dụng các kỹ thuật mã hóa, để giữ bí mật lá phiếu điện tử trước khi chuyển đến hòm phiếu qua các kênh công khai. Cử tri có thể bỏ phiếu qua Internet, các máy bỏ phiếu tự động.

1.1.3. Các thành phần trong hệ thống bỏ phiếu điện tử

1/. Cử tri:

Là người tham gia bỏ phiếu. Cử tri có quyền hợp lệ để bỏ phiếu, đồng thời là người giám sát cuộc bầu cử: kiểm tra xem lá phiếu của mình có được đếm không?.

2/. Ban điều hành (ĐH):

Quản lý các hoạt động bỏ phiếu, trong đó có thiết lập **danh sách cử tri** cùng các hồ sơ của mỗi cử tri, quy định cơ chế **định danh cử tri**.

3/. Ban đăng ký (ĐK):

Nhận dạng cử tri và cấp quyền bỏ phiếu cho cử tri, theo dõi cuộc bầu cử chống lại việc cử tri bỏ phiếu hai lần. Có hệ thống ký hỗ trợ.

4/. Ban kiểm tra (KT):

Kiểm tra cử tri có hợp lệ không? Nội dung lá phiếu có hợp lệ không?

(Vì là lá phiếu đã mã hóa nên ban kiểm phiếu không biết được lá phiếu có hợp lệ không, nên cần xác minh tính hợp lệ của lá phiếu trước khi nó chuyển đến hòm phiếu).

5/. Ban kiểm phiếu (KP):

Kiểm phiếu và thông báo kết quả bầu cử. Có hệ thống kiểm phiếu hỗ trợ.

6/. Hệ thống phân phối khóa tin cậy:

Cung cấp khóa ký của ban ĐK, quá trình mã hóa và giải mã lá phiếu.

7/. Hệ thống ký:

Giúp ban ĐK ký vào các định danh cử tri.

8/. Hệ thống kiểm phiếu:

Giúp ban KP tính kết quả cuộc bầu cử.

9/. Bảng niêm yết công khai (BB):

Giúp theo dõi quá trình bầu cử. Đây là kênh liên lạc công khai của tất cả các tành phần tham gia hệ thống bỏ phiếu điện tử.

1.1.4. Các giai đoạn bỏ phiếu điện tử

Bỏ phiếu điện tử gồm 3 giai đoạn chính:

Đăng ký, bỏ phiếu, kiểm phiếu và công bố kết quả.

1/. Giai đoạn đăng ký bỏ phiếu:

Chuẩn bị các thành phần kỹ thuật của hệ thống bỏ phiếu cũng như cơ cấu tổ chức. Ban KP, ban ĐK, ban KT được chỉ định. Danh sách các cử tri cũng được thiết lập. Trong bước này, quan trọng nhất là cơ chế định danh người gửi, dùng trong quá trình bỏ phiếu của cử tri.

2/. Giai đoạn bỏ phiếu:

Các cử tri thực hiện bỏ phiếu. Các cử tri phải có một hình thức định danh tính hợp lệ của lá phiếu. Thêm vào đó, một số kỹ thuật mã hóa cần được áp dụng để bảo đảm tính toàn vẹn của lá phiếu.

3/. Giai đoạn kiểm phiếu và công bố kết quả:

Ban KP sẽ tính toán kết quả dựa vào các lá phiếu đã thu thập, sau đó công bố kết quả.

1.1.5. Thực trạng bỏ phiếu điện tử ở Việt Nam và thế giới

Việt Nam:

Bỏ phiếu điện tử ở nước ta mới chỉ dừng ở mục đích bầu chọn, bình chọn (bầu chọn Vịnh Hạ Long là di sản Thiên nhiên thế giới, bình chọn bài hát hay trên sóng truyền hình..) song chưa thể triển khai vào bầu cử Quốc hội do còn nhiều hạn chế (vấn đề ngân sách, giáo dục ý thức cho người dân, quá trình phổ biến, huấn luyện phương thức thực hiện cho các cấp, các bộ phận liên quan..). Đây rõ ràng là một khoảng trống khá lớn, nhất là việc kinh phí lắp đặt hệ thống máy bầu cử hay trở ngại trong khoảng cách vùng miền.

Thế giới:

Khái niệm bỏ phiếu điện tử (e-voting) không còn xa lạ gì đối với các nước phát triển, nhất là ở Bắc Mỹ và Châu Âu. Tại Châu Á, chỉ có ba nước đã từng thử nghiệm hệ thống bầu cử điện tử, đó là Hàn Quốc, Nhật Bản và Ấn Độ, những nước có trình độ công nghệ phát triển cao. Tuy nhiên bầu cử điện tử tại ba nước này vẫn chưa được xem là thực sự thành công khi kết quả thu được từ những lá phiếu điện tử vẫn còn nhiều nghi vấn. Vấn đề lớn nhất chính là tính bảo mật của toàn hệ thống. Câu hỏi đặt ra là liệu có khả năng ai đó can thiệp vào những chiếc máy bầu cử hay chương trình bầu cử trên internet để làm thay đổi kết quả hay không.

Cần và Đủ:

Đề cập đến khả năng thực hiện bầu cử điện tử, ở một khía cạnh nào đó cần đáp ứng hai điều kiện. Thứ nhất, điều kiện cần là phải xây dựng một hệ cơ sở dữ liệu cho tất cả người dân. Một người dân cần phải có một con số nhận diện duy nhất, chẳng hạn như số giấy chứng minh nhân dân, để nhà nước có thể kiểm tra được số cử tri đi bầu. Hệ cơ sở dữ liệu này có thể ví như một cổng giao tiếp điện tử toàn quốc, là nơi có thể cung cấp thông tin của bất kì công dân nào khi truy xuất từ con số nhận diện của người đó.

Điều này cũng giúp cho cơ quan tiến hành việc bầu cử rà soát tính hợp pháp của cử tri, trong trường hợp có một số người bị tước quyền bầu cử. Ngoài ra, hệ cơ sở dữ liệu này sẽ là tiền đề cho tất cả các hoạt động khác của một quốc gia, chẳng hạn như chính phủ điện tử (e-government), quốc hội điện tử (e-parliament), chính trị điện tử (e-politics).. Thứ hai, điều kiện đủ là chính phủ phải định nghĩa được rõ ràng các quy trình trong bầu cử để có thể tin học hóa những quá trình đó. Không chỉ riêng trong bầu cử, các công ty quản lý hành chính khác cũng cần phải minh bạch trong quá trình thì mới có thể tiến hành tin học hóa - bước đầu tiên của điện tử hóa công tác quản lý. Riêng trong bầu cử điện tử, các quy trình đó có thể là phân công cho ai nắm giữ và chịu trách nhiệm về kết quả bầu cử, phân chia cấp độ bầu cử giữa các cấp quận, huyện, hội đồng nhân dân và địa biểu quốc hội.

1.2. TỔNG QUAN VỀ AN TOÀN THÔNG TIN

1.2.1. Sự cần thiết của bảo đảm an toàn thông tin

Ngày nay, sự suất hiện internet và mạng máy tính đã giúp cho việc trao đổi thông tin trở lên nhanh gọn, dễ dàng, Email cho phép người ta nhận hay gửi thư ngay trên máy tính của mình, E-business cho phép thực hiện các giao dịch buôn bán ngay trên mạng.

Tuy nhiên lại phát sinh những vấn đề mới. Thông tin quan trọng nằm ở kho dữ liệu hay đang trên đường truyền có thể bị trộm cắp, có thể bị làm sai lệch, có thể bị làm giả mạo. Điều đó làm ảnh hưởng đến các tổ chức, các công ty hay cả một quốc gia. Những bí mật kinh doanh, tài chính là mục tiêu của các đối thủ cạnh tranh. Những tin tức về an ninh quốc gia là mục tiêu của các tổ chức tình báo trong và ngoài nước.

Theo số liệu của CERT (Computer Emegency Response Team: đội cấp cứu máy tính) số lượng các vụ tấn công trên máy internet ngày càng nhiều, quy mô của chúng mỗi ngày một lớn và phương pháp tấn công ngày càng hoàn thiện.

Khi trao đổi thông tin trên mạng, những tình huống mới nảy sinh:
Người ta nhận được một bản tin trên mạng, thì lấy gì làm đảm bảo rằng nó là của đối tác gửi cho họ. Khi nhận được tờ Sec điện tử hay tiền điện tử trên mạng, thì có cách nào xác nhận rằng nó là của đối tác đã thanh toán cho ta. Tiền đó là tiền thật hay tiền giả. Thông thường người gửi vản bản quan trọng phải ký phía dưới. Nhưng khi truyền trên mạng, văn bản hay giấy thanh toán có thể bị trộm cắp và phía dưới nó có thể dán một chữ ký khác. Tóm lại với cách thức ký như cũ, chữ kỹ rất dễ bị giả mạo.

Để giải quyết tình hình trên, vấn đề đảm bảo an toàn thông tin (ATTT) đã được đặt ra trong lý luận cũng như thực tiễn.

Thực ra vấn đề này đã có từ ngàn xưa, khi đó nó chỉ có tên là "bảo mật", mà kỹ thuật rõ đơn giản, chẳng hạn trước khi truyền thông báo, người gửi và người nhận thỏa thuận một số từ ngữ mà ta quen thuộc gọi là "tiếng lóng"

Khi có điện tín điện thoại người ta dùng mật mã cổ điển, phương pháp chủ yếu là thay thế hay hoán vị các ký tự trong bản tin "gốc" để được bản tin "mật mã". Người khác khó có thể đọc được.

Với sự phát triển mạnh mẽ của công nghệ thông tin, an toàn thông tin đã trở thành một khoa học thực thụ vì có đất phát triển.

1.2.2. Khái niệm an toàn thông tin

1.2.1.1. Khái niệm

An toàn thông tin nghĩa là thông tin được bảo vệ, các hệ thống và dịch vụ có khả năng chống lại những sự can thiệp, lỗi và những tai họa không mong đợi, các thay đổi tác động đến độ an toàn của hệ thống là nhỏ nhất. Hệ thống không an toàn là hệ thống tồn tại những điểm: thông tin bị rò rỉ ra ngoài - thông tin dữ liệu trong hệ thống bị người không được quyền truy nhập lấy và sử dụng, thông tin bị thay đổi - các thông tin trong hệ thống bị thay thế hoặc sửa đổi làm sai lệch một phần hoặc hoàn toàn nội dung...

Giá trị thực sự của thông tin chỉ đạt được khi thông tin được cung cấp chính xác và kịp thời, hệ thống phải hoạt động chuẩn xác thì mới có thể đưa ra những thông tin có giá trị cao. Mục tiêu của an toàn bảo mật trong công nghệ thông tin là đưa ra một số tiêu chuẩn an toàn và áp dụng các tiêu chuẩn an toàn này vào chỗ thích hợp để giảm bớt và loại trừ những nguy hiểm có thể xảy ra. Ngày nay với kỹ thuật truyền nhận và xử lý thông tin ngày càng phát triển và phức tạp nên hệ thống chỉ có thể đạt tới một mức độ an toàn nào đó và không có một hệ thống an toàn tuyệt đối. Ngoài ra khi đánh giá còn phải cân đối giữa mức độ an toàn và chất lượng của dịch vụ được cung cấp.

Khi đánh giá độ an toàn thông tin cần phải dựa trên nội dung phân tích các rủi ro có thể gặp, từ đó tăng dần sự an toàn bằng cách giảm bớt những rủi ro. Các đánh giá cần hài hoà với đặc tính, cấu trúc hệ thống và quá trình kiểm tra chất lượng.

1.2.1.2. Các yêu cầu an toàn bảo mật thông tin.

Ngày nay, với sự phát triển rất nhanh của khoa học công nghệ, các biện pháp tấn công ngày càng tinh xảo hơn, độ an toàn của thông tin có thể bị đe dọa từ nhiều nơi, theo nhiều cách khác nhau, chúng ta cần phải đưa ra các chính sách đề phòng thích hợp. Các yêu cầu cần thiết của việc bảo vệ thông tin và tài nguyên:

• Đảm bảo bí mật (Bảo mật) thông tin không bị lộ đối với người không được phép.

• Đảm bảo tính tin cậy (Confidentiality): Thông tin và tài nguyên không thể bị truy cập trái phép bởi những người không có quyền hạn.

• Đảm bảo tính toàn vẹn (Integrity): Thông tin và tài nguyên không thể bị sửa đổi, bị thay thế bởi những người không có quyền hạn.

• Đảm bảo tính sẵn sàng (Availability): Thông tin và tài nguyên luôn sẵn sàng để đáp ứng sử dụng cho người có quyền hạn.

• Đảm bảo tính không thể chối bỏ (Non-repudiation): Thông tin và tài nguyên được xác nhận về mặt pháp luật của người cung cấp.

1.2.1.3. Các nội dung an toàn thông tin

Nội dung chính:

• An toàn máy tính: là sự bảo vệ các thông tin cố định bên trong máy tính, là khoa học về bảo đảm an toàn thông tin trong máy tính

• An toàn truyền tin: là sự bảo vệ thông tin trên đường truyền tin(thông tin được truyền từ hệ thống này sang hệ thống khác), là khoa học bảo đảm an toàn thông tin trên đường truyền tin.

Nội dung chuyên ngành:

• An toàn dữ liệu (data security)

• An toàn cơ sở dữ liệu (database security)

• An toàn hệ điều hành (operation system security)

• An toàn mạng máy tính (network security)

1.2.1.4. Các chiến lược bảo đảm an toàn thông tin.

Cấp quyền hạn tối thiểu: Nguyên tắc cơ bản trong an toàn nói chung là "hạn chế sự ưu tiên". Mỗi đối tượng sử dụng hệ thống (người quản trị mạng, người sử dụng..) chỉ được cấp phát một số quyền hạn nhất định đủ dùng cho công việc của mình.

Phòng thủ theo chiều sâu: Nguyên tắc tiếp theo trong an toàn nói chung là "bảo vệ theo chiều sâu". Cụ thể là tạo lập nhiều lớp bảo vệ khác nhau cho hệ thống.

1.3. CÁC PHƯƠNG PHÁP BẢO VỆ THÔNG TIN

Các giải pháp bảo đảm an toàn thông tin

Phương pháp che giấu, bảo đảm toàn vẹn và xác thực thông tin.

• "Che" dữ liệu (mã hóa): thay đổi hình dạng dữ liệu gốc, người khác khó nhận ra.

• "Giấu" dữ liệu: Cất giấu dữ liệu này trong môi trường dữ liệu khác.

• Bảo đảm toàn vẹn và xác thực thông tin(đánh giấu thông tin)

Kỹ thuật:

Mã hóa, hàm băm, giấu tin, ký số. . .

Giao thức bảo toàn thông tin, giao thức xác thực thông tin, . . .

Phương pháp kiểm soát lỗi vào ra của thông tin.

• Kiểm soát, ngăn chặn các thông tin vào ra hệ thống máy tính.

• Kiểm soát, cấp quyền sử dụng các thông tin trong hệ thống máy tính.

• Kiểm soát, tìm diệt "sâu bọ" vào trong hệ thống máy tính

Kỹ thuật: Mật khẩu, tường lửa, mạng riêng ảo, nhận dạng, xác định thực thể, cấp quyền hạn.

Phát hiện và xử lý các lỗ hổng trong an toàn thông tin.

• Các "lỗ hổng" trong các thuật toán hay giao thức mật mã, giấu tin.

• Các "lỗ hổng" trong các giao thức.

• Các "lỗ hổng" trong các hệ điều hành.

• Các "lỗ hổng" trong các ứng dụng.

Phối hợp các phương pháp: Xây dựng các "hành lang", "đường đi" an toàn cho thông tin gồm 3 phần:

• Hạ tầng mật mã khóa công khai(PKI)

• Kiểm soát nối vào – ra: Mật khẩu, tưởng lửa, mạng riêng ảo, cấp quyền hạn.

• Kiểm soát và xử lý các lỗ hổng.

Các kỹ thuật bảo đảm an toàn thông tin

- Kỹ thuật diệt trừ: Virus máy tính, chương trình trái phép.
- Kỹ thuật tường lửa: Ngăn chặn truy cập trái phép, lọc thông tin không hợp pháp.
- Kỹ thuật mạng riêng ảo: Tạo ra hành lang riêng cho thông tin "đi lại".
- Kỹ thuật mật mã: Mã hóa, kỹ số, các giao thức mật mã, chống chối cãi.
- Kỹ thuật giấu tin: Che giấu thông tin trong môi trường dữ liệu khác.
- Kỹ thuật thủy ký: Bảo vệ bản quyền tài liệu số hóa.
- Kỹ thuật truy tìm "dấu vết" kẻ trộm tin.

Các công nghệ đảm bảo an toàn thông tin

- Công nghệ chung: Tường lửa, mạng riêng ảo, PKI(khóa côngkhai),
thẻ thông minh. . .
- Công nghệ cụ thể: SSL, TLS, PGP, SMINE . . .

1.4. PHƯƠNG PHÁP MÃ HÓA

1.4.1. Tổng quan về mã hóa dữ liệu

Khái niệm về mã hóa.

• ***Mã hóa*** là quá trình chuyển thông tin có thể đọc được (gọi là ***Bản rõ***) thành thông tin "**khó"** thể đọc được theo cách thông thường (gọi là ***Bản mã***).

Đó là một trong những kỹ thuật để bảo mật thông tin.

• ***Giải mã*** là quá trình chuyển thông tin ngược lạI: từ ***Bản mã*** thành ***Bản rõ***.

• ***Thuật toán mã hoá*** hay ***giải mã*** là thủ tục tính toán để thực hiện mã hóa hay giải mã

• ***Khóa mã hóa*** là một giá trị làm cho thuật toán mã hoá thực hiện theo cách riêng biệt và sinh ra bản rõ riêng. Thông thường khoá càng lớn thì bản mã càng an toàn. Phạm vi các giá trị có thể có của khoá được gọi là ***Không gian khoá.***

• ***Hệ mã hóa*** là tập các thuật toán, các khóa nhằm che giấu thông tin, cũng như làm cho rõ nó.

Phân loại: Phân loại mã hóa theo đặc trưng của khóa

Có 2 loại:

+ Hệ mã hóa khóa bí mật.

+ Hệ mã hóa khóa công khai.

a). Giới thiệu về mã hóa:

Chúng ta biết rằng thông tin truyền đi trên mạng rất dễ bị trộm cắp. Để đảm bảo việc truyền tin an toàn, người ta thường mã hóa thông tin trước khi truyền đi. Việc mã hóa cần theo quy tắc nhất định. Hiện nay có 2 loại mật mã: hệ mật mã khoá bí mật và hệ mật mã khóa công khai . Hệ mật mã khóa bí mật (còn gọi là hệ mật mã đối xứng hay hệ mật mã cổ điển) dễ hiểu, dễ thực thi nhưng độ an toàn không cao. Với các hệ mật mã khóa bí mật, nếu biết khóa lập mã hay thuật toán lập mã, người ta có thể tìm thấy ngay được bản rõ.

Ngược lại, các hệ mật mã khóa công khai (còn gọi là hệ mật mã phi đói xứng) cho biết khóa lập mã K và hàm lập mã $e_{k,}$ thì cũng rất khó tìm được cách giải mã. Và việc thám mã là rất khó khăn do độ phức tạp tính toán lớn.

Hệ mã hóa được định nghĩa là bộ năm (**P**, **C**, **K**, **E**, **D**), trong đó:

P là tập hữu hạn các ***bản rõ*** có thể.

C là tập hữu hạn các ***bản mã*** có thể.

K là tập hữu hạn các ***khoá*** có thể.

E là tập các hàm lập mã.

D là tập các hàm giải mã.

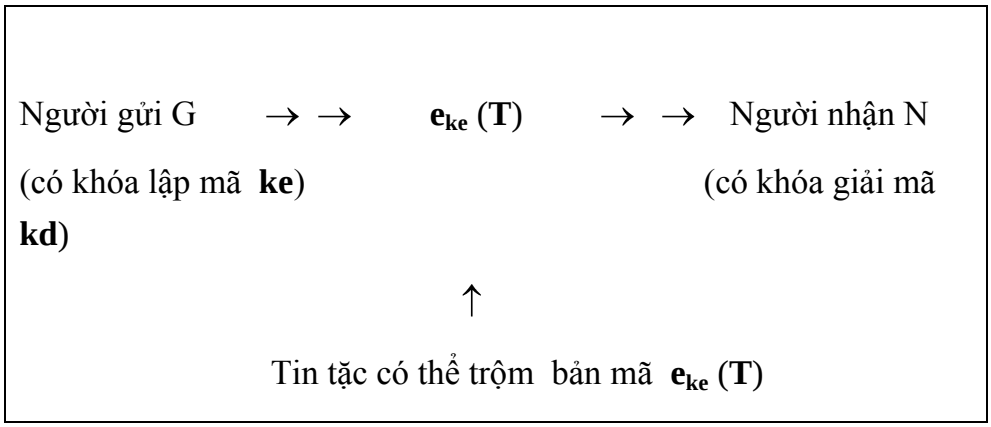
Với khóa lập mã $\mathbf{ke} \in \mathbf{K}$, có hàm lập mã $\mathbf{e_{ke}} \in \mathbf{E}$, $\mathbf{e_{ke}}: \mathbf{P} \rightarrow \mathbf{C}$,

Với khóa giải mã $\mathbf{kd} \in \mathbf{K}$, có hàm giải mã $\mathbf{d_{kd}} \in \mathbf{D}$, $\mathbf{d_{kd}}: \mathbf{C} \rightarrow \mathbf{P}$,

sao cho $\mathbf{d_{kd}(e_{ke}(x)) = x}$, $\forall \mathbf{x} \in \mathbf{P}$.

Ở đây **x** được gọi là ***bản rõ***, $\mathbf{e_{ke}(x)}$ được gọi là ***bản mã***.

Mã hóa và giải mã.



b). Hệ mật mã khóa bí mật:

Hệ mật mã khóa bí mật là hệ mật mã mà khóa mã hóa có thể dễ dàng tìm được từ khóa giải mã và ngược lại. Trong rất nhiều trường hợp, khoá mã hoá và khoá giải mã là giống nhau. Hệ mật mã khóa bí mật yêu cầu người gửi và người nhận phải thoả thuận một khoá trước khi tin tức được gửi đi, khoá này phải được cất giữ bí mật. Độ an toàn của hệ này phụ thuộc vào khoá, nếu để lộ ra khoá này nghĩa là bất kỳ người nào cũng có thể mã hoá và giải mã thông báo.

Các đặc điểm của hệ mật mã khóa bí mật:

- Các phương pháp mã hóa cổ điển đòi hỏi người mã hóa và người giải mã phải có cùng chung một khóa.
- Khóa phải được giữ bí mật tuyệt đối, khóa phải được gửi đi trên kênh an toàn.

Vì dễ dàng xác định một khóa nếu biết khóa kia.

Phạm vi ứng dụng:

Hệ mật mã đối xứng thường được sử dụng trong môi trường mà khóa có thể dễ dàng trao chuyển bí mật, chẳng hạn trong cùng một văn phòng. Nó cũng được dùng để mã hóa thông tin khi lưu trên đĩa.

Một số thuật toán mã hóa khóa đối xứng:

- Hệ mã hóa dịch chuyển.
- Hệ mã hóa thay thế.
- Hệ mã hóa Affine.
- Hệ mã hóa Vigenere.
- Hệ mã hóa hoán vị.

c). Hệ mật mã khóa công khai.

Trong hệ mật mã khóa công khai, khóa mã hõa khác với khóa giải mã. Mặt khác, biết được khóa này không thể dễ dàng tìm được khóa kia, do vật khóa mã hóa có thể công khai. Một người bất kì có thể sử dụng khóa công khai để mã hóa tin tức, nhưng chỉ người nào có đúng khóa giải mã thì mới có khả năng xem được bản rõ.

Khóa mã hóa còn gọi là khóa công khai (public key), khóa giải mã là khóa bí mật (private key).

Các đặc điểm của hệ mật mã khóa công khai:

- Khi biết các điều kiện ban đầu, việc tìm ra cặp khóa công khai và bí mật phải được thực hiện một cách dễ dàng, tức là trong thời gian đa thức.
- Người gửi G có khóa công khai, có bản tin P thì có thể tạo ra bản mã C nhanh gọn, nghĩa là cũng trong thời gian đa thức.
- Người nhận N khi nhận được bản mã hóa C với khóa bí mật có thể giải mã bản tin dễ dàng trong thời gian đa thức.
- Nếu kẻ phá hoại biết khóa công khai, và hơn nữa cả bản mã C thì việc tìm ra bản rõ P là bài toán khó, số phép thử là vô cùng lớn, không khả thi.
- Hệ mật mã khóa công khai tiện lợi hơn hệ mật mã đối xứng ở chỗ thuật toán được viết một lần nhưng có thể được sử dụng nhiều lần và cho nhiều người. Chỉ cần bí mật khóa riêng.

- Nhược điểm: Tốc độ mã hóa chậm. Tốc độ nhanh nhất của loại mật mã khóa công khai chậm hơn nhiều so với hệ mật mã khóa bí mật. Do đó người ta thường kết hợp hai loại mã hóa để nâng cao tốc độ mã hóa và độ an toàn.

Phạm vi ứng dụng:

Hệ mật mã khóa công khai được sử dụng chủ yếu trên các mạng công khai như Internet, khi mà việc trao đổi khóa bí mật tương đói khó khăn. Đặc trưng nổi bật của hệ mã hóa khóa công khai là cả khóa công khai và bản mã C đều có thể gửi đi trên một kênh thông tin không an toàn.

1.4.2. Mã hóa

Mã hóa là một trong những phương pháp được sử dụng nhằm bảo vệ lá phiếu, phòng tránh sửa đổi

Một số thuật toán mã hóa khóa công khai:

- Mã hóa RSA.
- Mã hóa Elgamal.

Ví dụ về Hệ mã hóa khóa công khai RSA:

1). Sơ đồ (Rivest, Shamir, Adleman đề xuất năm 1977)

- *Tạo cặp khóa* (*bí mật, công khai*) (a, b) :

Chọn bí mật số nguyên tố lớn p, q, tính n = p * q, công khai n, đặt $P = C = Z_n$

Tính bí mật $\phi(n) = (p-1).(q-1)$. Chọn khóa công khai $b < \phi(n)$, nguyên tố với $\phi(n)$.

Khóa bí mật **a** là phần tử nghịch đảo của b theo mod $\phi(n)$: $a*b \equiv 1 \bmod \phi(n)$.

Tập cặp khóa (bí mật, công khai) $K = \{(a, b)/\ a, b \in Z_n,\ a*b \equiv 1 \bmod \phi(n)\}$.

Với *Bản rõ* $x \in P$ và *Bản mã* $y \in C$, định nghĩa:

Hàm Mã hoá: $y = e_k(x) = x^b \bmod n$

Hàm Giải mã: $x = d_k(y) = y^a \bmod n$

2). Ví dụ .

Bản rõ chữ: R E N A I S S A N C E

****Sinh khóa***:

Chọn bí mật số nguyên tố p= 53, q= 61, tính n = p * q = 3233, công khai n.

Đặt $P = C = Z_n$, tính bí mật $\phi(n) = (p-1).(q-1) = 52 * 60 = 3120$.

+ Chọn khóa công khai b là nguyên tố với $\phi(n)$, tức là ƯCLN(b, $\phi(n)$) = 1,

ví dụ chọn b = 71.

+ Khóa bí mật a là phần tử nghịch đảo của b theo mod $\phi(n)$: $a*b \equiv 1(\text{mod } \phi(n))$.

Từ $a*b \equiv 1 (\text{mod } \phi(n))$, ta nhận được khóa bí mật a = 791.

* **Bản rõ số:**

R	E	N	A	I	S	S	A	N	C	E	(Dấu cách)
17	04	13	00	08	18	18	00	13	02	04	26
m_1		m_2		m_3		m_4		m_5		m_6	

Theo phép lập mã: $c_i = m_i^{\ b} \text{ mod } n = m_i^{\ 71} \text{ mod } 3233$, ta nhận được:

* **Bản mã số**:

c_1	c_2	c_3	c_4	c_5	c_6
3106	0100	0931	2691	1984	2927

Theo phép giải mã: $m_i = c_i^{\ a} \text{ mod } n = c_i^{\ 791} \text{ mod } 3233$, ta nhận lại bản rõ.

3). Độ an toàn

- Hệ mã hóa RSA là tất định, tức là với một bản rõ x và một khóa bí mật a, thì chỉ có một bản mã **y**.

- Hệ mật RSA an toàn, khi giữ được bí mật khoá giải mã a, p, q, $\phi(n)$.

Nếu biết được p và q, thì thám mã dễ dàng tính được $\phi(n) = (q-1)*(p-1)$.

Nếu biết được $\phi(n)$, thì thám mã sẽ tính được **a** theo thuật toán Euclide mở rộng.

Nhưng phân tích n thành tích của p và q là bài toán "khó".

Độ an toàn của Hệ mật RSA dựa vào khả năng giải bài toán phân tích số nguyên dương n thành tích của 2 số nguyên tố lớn p và q.

Mã hóa đồng cấu.

Khái niệm mã hóa đồng cấu:

Giả sử cho trước (G_1, +) và (G_2,*) là hai nhóm với các toán tử + và * lần lượt trong G_1 và G_2. Một ánh xạ f: $G_1 \rightarrow G_2$ được gọi là một phép đồng cấu (đồng cấu nhóm) nếu thỏa mãn điều kiện:

f(g1+g2+…+gn) = f(g1)*f(g2)*….*f(gn). (với n≥2)

Hệ mã hóa Elgamal có tính chất đồng cấu.

Trong Hệ Elgamal P = Zp , chọn tập bản mã C ={(a, b) / a, b ∈ Zp }.

Chọn khóa bí mật là a ∈ Zp* , khóa công khai là $h = g^a$.

Để mã hóa m, ta chọn số ngẫu nhiên bí mật k,

bản mã là $(x, y) = E_k(m) = (g^k, h^K m)$.

Tài liệu được giải mã là $m = y/x^a$

Vì $y/x^a = h^k m/(g^k)^a = h^k m/(g^a)^k = h^k m/h^k = m$.

Nhận xét:

1/. Hệ mã hóa Elgamal có tính chất đồng cấu vì:

$E_{k1}(m_1) = (g^{k1}, h^{k1}m_1)$, $E_{k2}(m_2) = (g^{k2}, h^{k2}m_2)$.

Thỏa mãn tính chất đồng cấu:

$E_{k1}(m_1) * E_{k2}(m_2) = (g^{k1} g^{k2}, h^{k1}h^{k2} m_1m_2) = (g^k, h^k m_1m_2) = E^k(m_1 * m_2)$.

Với $k = k_1 + k_2$.

2/. Trong bài toán Elgamal trên thì hàm f chính là hàm Encrypt ($E^k(m)$).

G1 chính là tập hợp các bản rõ, tạo thành nhóm với phép tính +.

G2 chính là tập hợp các bản mã, tạo thành nhóm với phép tính *.

+, * là phép cộng và nhân theo không gian modulo ().

Ví dụ về Ứng dụng hệ mã hóa đồng cấu Elgamal cho loại bỏ phiếu có/ không

Bài toán:

Cần lấy ý kiến về một việc nào đó, cử tri phải ghi vào lá phiếu: đồng ý (1) hay không đồng ý (0). Nội dung lá phiếu được mã hoá và gửi về Ban kiểm phiếu. Vấn đề là Ban kiểm phiếu tính kết quả bỏ phiếu như thế nào, trong khi không biết nội dung từng lá phiếu ? (Vì chúng đã được mã hoá).

Giải quyết:

Cho dễ hiểu, chúng tôi trình bày cách giải quyết thông qua một ví dụ cụ thể.

B1: Cử tri ghi ý kiến vào lá phiếu

Giả sử có 4 cử tri tham gia bỏ phiếu là V_1, V_2, V_3, V_4.

Lá phiếu tương ứng của họ ghi:

v1 = 0 (không đồng ý), v2 = 1 (đồng ý), v3 = 1, v4 = 0.

Chọn phần tử sinh g =3, hệ mã hoá Elgamal được sử dụng với các khoá như sau:

Khóa bí mật a = 2, khóa công khai $h = g^a = 3^2 = 9$.

Mỗi cử tri V_i, chọn khóa ngẫu nhiên bí mật k đề mã hóa lá phiếu m của mình thành $(x, y) = (g^k, h^k m)$

B2: Cử tri mã hoá lá phiếu

V_1 mã hóa lá phiếu của mình như sau và gửi tới Ban kiểm phiếu:

V_1 chọn ngẫu nhiên $k_1 = 5$, mã hóa $v_1 = 0$

thành $(x_1, y_1) = (3^5, 9^5 * 3^0) = (3^5, 9^5)$.

V_2 mã hóa lá phiếu của mình như sau và gửi tới Ban kiểm phiếu:

V_2 chọn ngẫu nhiên $k_2 = 3$, mã hóa $v_2 = 1$

thành $(x_2, y_2) = (3^3, 9^3 * 3^1) = (3^3, 9^3 * 3)$.

V_3 mã hóa lá phiếu của mình như sau và gửi tới Ban kiểm phiếu:

V_3 chọn ngẫu nhiên $k_3 = 3$, mã hóa $v_3 = 1$

thành $(x_3, y_3) = (3^3, 9^3 * 3^1) = (3^3, 9^3 * 3)$.

V_4 mã hóa lá phiếu của mình như sau và gửi tới Ban kiểm phiếu:

V_4 chọn ngẫu nhiên $k_4 = 7$, mã hóa $v_4 = 0$

thành $(x_4, y_4) = (3^7, 9^7 * 3^0) = (3^7, 9^7)$.

Bước 3: Ban kiểm phiếu tính kết quả

Ban KP không cần giải mã từng lá phiếu, vẫn có thể tính được kết quả bỏ phiếu bằng cách tính nhân các lá phiếu đã được mã hóa:

$(x_1, y_1) * (x_2, y_2) = (x_1x_2, y_1y_2) = (g^{k1+k2} h^{k1+k2}, g^{v1+v2})$.

Theo tính chất đồng cấu thì tích của phép nhân trên chính là kết quả bỏ phiếu.

Cụ thể tích của 4 giá trị lá phiếu đã được mã hóa là:

$(X, Y) = (\prod_i x_i , \prod_i y_i) = (g^{k1+k2+k3+k4} , h^{k1+k2+k3+k4} g^{v1+v2+v3+v4}) = (3^{18}, 9^{18} * 3^2)$.

Giải mã (X, Y) bằng cách tính:

$\mathbf{m} = g^v = \mathbf{Y/X^a} = 9^{18} * 3^2/(318)^2 = \mathbf{3^2}$

Như vậy số phiếu đồng ý (ghi 1) là **2**.

1.4.3. Hệ mã hóa đối xứng – cổ điển

Khái niệm

- Hệ mã hóa đối xứng đã được dùng từ rất sớm, nên còn được gọi là Hệ mã hóa đối xứng – cổ điển. Bản mã hay bản rõ là dãy các ký tự Lantin.

- Lập mã: thực hiện theo các bước sau:

Bước 1: nhập bản rõ ký tự: RÕ_CHỮ.

Bước 2: chuyển RÕ_CHỮ ==> RÕ_SỐ.

Bước 3: chuyển RÕ_SỐ ==> MÃ_SỐ.

Bước 4: chuyển MÃ _SỐ ==> MÃ_CHỮ

- Giải mã: thực hiện theo các bước sau.

Bước 1: nhập bản mã ký tự: MÃ_CHỮ.

Bước 2: chuyển MÃ_CHỮ ==> MÃ_SỐ

Bước 3: chuyển MÃ_SỐ ==> RÕ_SỐ.

Bước 4: chuyển RÕ_SỐ ==> RÕ_CHỮ

Các hệ mã hóa cổ điển

- Hệ mã hóa dịch chuyển: khóa có 1 chìa.
- Hệ mã hóa Affine: khóa có 2 chìa.
- Hệ mã hóa thay thế: khóa có 26 chìa.
- Hệ mã hóa VIGENERE: khóa có m chìa
- Hệ mã hóa HILL: khóa có ma trận chìa

1/. Hệ mã hóa dịch chuyển

Sơ đồ

Đặt P = C = K = Z_{26}. Bản mã y và bản rõ x $\in$ Z_{26}.

Với khóa k $\in$ K, ta định nghĩa:

Hàm mã hóa: $y=e_k(x) = (x+k) \bmod 26$

Hàm giải mã: $x=d_k(y) = (y-k) \bmod 26$

Độ an toàn

Độ an toàn của mã dịch chuyển là rất thấp

Tập khóa K chỉ có 26 khóa, nên việc phá khóa có thể thực hiện dễ dàng bằng cách thử kiểm tra từng khóa: k=1,2,3, …,26.

2/. Hệ mã hóa thay thế (Hoán vị toàn cục)

Sơ đồ

Đặt P = C = Z_{26}. Bản mã y và bản rõ x $\in$ Z_{26}.

Tập khóa K là tập mọi hoán vị trên Z_{26}.

Với khóa k = $\pi \in$ K, tức là 1 hoán vị trên Z_{26}, ta định nghĩa:

- Mã hóa: $y=e_\pi(x)=\pi(x)$
- Giải mã: $x=d_\pi(y)=\pi^{-1}(y)$

Độ an toàn

Độ an toàn của mã thay thế thuộc loại cao

- Tập khóa K có 26! Khóa ($>4.10^{26}$), nên việc phá khóa cố thể thực hiện bằng cách duyệt tuần tự 26! Hoán vị của 26 chữ cái.
- Để kiểm tra tất cả 26! Khóa, tốn rất nhiều thời gian.

Hiện nay với hệ mã này, người ta có phương pháp thám mã khác nhanh hơn.

3/. Hệ mã hóa AFFINE

Sơ đồ

- Đặt P = C = Z_{26}. Bản mã y và bản rõ x $\in$ Z_{26}.

- Tập khóa K = {(a,b), với a,b$\in$ Z_{26}, UCLN(a,26)=1}

- Với khóa k=(a,b)$\in$K, ta định nghĩa:

- Phép mã hóa $y=e_k(x)= (ax + b) \bmod 26$
- Phép giải mã $x=d_k(y)= a^{-1}(y-b) \bmod 26$

Độ an toàn:

Độ an toàn của Hệ mã hóa Affine: Rất thấp

- Điều kiện UCLN(a,26)=1 để bảo đảm a có phần tử nghịch đảo $a^{-1} \bmod 26$, tức là thuật toán giải mã d_k luôn thực hiện được.

- Số lượng a$\in$ Z_{26} nguyên tố với 26 là $\phi(26)=12$, đó là

1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25

- Các số nghịch đảo theo (mod 26) tương ứng là:

1, 9, 21, 15, 3, 19, 7, 23, 11, 5, 17, 25

- Số lượng b $\in$ Z_{26} là 26

- Số khóa (a,b) có thể là 12*26 = 312. Rất ít

- Như vậy việc dò tìm khóa mật khá dễ dàng.

4/. Hệ mã hóa VIGENRE

Sơ đồ:

- Đặt P =C=K=$(Z_{26})^m$, m là số nguyên dương, các phép toán thực hiện trong $(Z_{26})^m$.

- Bản mã Y và bản rõ X $\in$ $(Z_{26})^m$. Khóa k = $(k_1, k_2, \ldots, k_m)$ gồm m phầm tử.

Mã hóa $Y = (y_1, y_2, \ldots, y_m) = e_k(x_1, x_2, \ldots, x_m)$

$= (x_1 + k_1, x_2 + k_2, \ldots, x_m + k_m) \bmod 26$

Giải mã $X= (x_1, x_2, \ldots, x_m) = d_k(y_1, y_2, \ldots, y_m) = (y_1 - k_1, y_2 - k_2, \ldots, y_m - k_m) \bmod 26$

Độ an toàn:

Độ an toàn của mã VIGENERE là tương đối cao

Nếu khóa gồm m ký tự khác nhau, mỗi ký tự có thể được ánh xạ vào trong m ký tự có thể, do đó hệ mật này được gọi là thay thế đa biểu. Như vậy số khóa có thể có trong mật Vigenere là 26^m. Nếu dùng phương pháp "tấn công vét cạn", thám mã phải kiểm tra 26^m khóa. Hiện nay với hệ mã này, người ta có phương pháp thám mã khác nhanh hơn.

5/. Hệ mã hóa hoán vị cục bộ

Sơ đồ

Đặt $P = C = K = (Z_{26})^m$, m là số nguyên dương. Bản mã Y và bản rõ $X \in Z_{26}$.

- Tập khóa K là tập tất cả các hoán vị của {1, 2, …, m}
- Với mỗi khóa $k = \pi \in K$, $k = (k_1, k_2, \ldots, k_m)$ gồm m phần tử, ta định nghĩa:
  - Mã hóa $Y = (y_1, y_2, \ldots, y_m) = e_k(x_1, x_2, \ldots, x_m) = (x_{k(1)}, x_{k(2)}, \ldots, x_{k(m)})$
  - Giải mã $X = (x_1, x_2, \ldots, x_m) = d_k(y_1, y_2, \ldots, y_m) = (y_{k(1)}^{-1}, y_{k(2)}^{-1}, \ldots, y_{k(m)}^{-1})$
- Trong đó $k^{-1} = \pi^{-1}$ là hoán vị ngược của π.

Độ an toàn

- Nếu dùng phương pháp "tấn công vét cạn", thám mã phải kiểm tra số khóa có thể là: $1! + 2! + 3! + \ldots + m!$ trong đó $m \leq 26$.
- Hiện nay với hệ mã này, người ta có phương pháp thám mã khác nhanh hơn.

6/. Hệ mã hóa HILL

Sơ đồ

- Đặt P = C = $(Z_{26})^m$,m là số nguyên dương. Bản mã Y và bản rõ X $\in$ $(Z_{26})^m$.
- Tập khóa K={ k $\in$$(Z_{26})^{m*n}$/det(k,26)=1}. (k phải có k^{-1})
- Mỗi khóa K là một chùm chìa khóa
- Với mỗi k $\in$ K, định nghĩa:

- Hàm lập mã: $Y = (y_1, y_2, \ldots, y_m) = e_k(x_1, x_2, \ldots, x_m) = (x_1, x_2, \ldots, x_m) * k$
- Hàm giải mã: $X = (x_1, x_2, \ldots, x_m) = d_k(y_1, y_2, \ldots, y_m) = (y_1, y_2, \ldots, y_m) * k^{-1}$

Độ an toàn

Nếu dùng phương pháp "tấn công vét cạn", thám mã phải kiểm tra số khóa có thể với m lần lượt là 2, 3, 4, …, trong đó m lớn nhất là bằng độ dài bản rõ.

1.4.4. Hệ mã hóa đối xứng DES

1/. Hệ mã hóa đối xứng DES

a/. Giới thiệu

- 15/05/1973, Ủy ban tiêu chuẩn quốc gia Mỹ đã công bố một khuyến nghị về hệ mã hóa chuẩn.

- Hệ mã hóa phải có độ an toàn cao.
- Hệ mã hóa phải được định nghĩa đầy đủ và dễ hiểu.
- Độ an toàn của hệ mã hóa phải nằm ở khóa, không nằm ở thuật toán.
- Hệ mã hóa phải sẵn sàng cho mọi người dùng ở các lĩnh vực khác nhau.
- Hệ mã hóa phải xuất khẩu được.

- DES được IBM phát triển, là một cải biên của hệ mật LUCIPHER DES, nó được công bố lần đầu tiên vào ngày 17/03/1975. Sau nhiều cuộc tranh luận công khai, cuối cùng DES được công nhận như một chuẩn liên bang vào ngày 23/11/1976 và được công bố vào ngày15/01/1977.
- Năm 1980, "cách dùng DES" được công bố. Từ đó chu kỳ 5 năm DES được xem xét lại một lần bởi Ủy ban tiêu chuẩn quốc gia Mỹ.

b/. Quy trình mã hóa theo DES

Giai đoạn 1: Bản rõ chữ =====➔ Bản rõ số (Dạng nhị phân)

Chia thành

Giai đoạn 2: Bản rõ số =====➔ Các đoạn 64 bit rõ số

Giai đoạn 3: 64 bit rõ số =====➔ 64 bit mã số

Kết nối

Giai đoạn 4: Các đoạn 64 bit mã số =====➔ Bản mã số (Dạng nhị phân)

Giai đoạn 5: Bản mã số =====➔ Bản mã chữ

2/. Lập mã và giải mã

a/. Lập mã

- Bản rõ là xâu x, bản mã là xâu y, khóa là xâu K, đều cố đọ dài 64 bit
- Thuật toán mã hóa DES thực hiện qua 3 bước chính như sau:

Bước 1: Bản rõ x được hoán vị theo phép hoán vị IP, thành IP (x).

IP(x) = $L_0 R_0$, trong đó L_0 là 32 bit đầu (Left), R_0 là 32 bit cuối (Right).

(IP(x) tách thành $L_0 R_0$).

Bước 2 : Thực hiện 16 vòng mã hóa với những phép toán giống nhau

Dữ liệu được kết hợp với khóa thông qua hàm f:

$L_l = R_{l-1}$, $R_l = L_{l-1} \oplus f(R_{l-1},k_1)$ trong đó:

$\oplus$ là phép toán hoặc loại trừ của hai xâu bit (cộng theo modulo 26)

$k_1, k_2, \ldots, k_{16}$ là các khóa con (48 bit) được tính từ khóa gốc K.

Bước 3: Thực hiện phép hoán vị ngược IP^{-1} cho xâu $L_{16}R_{16}$, thu dược bản mã y.

$$y = IP^{-1} (L_{16}, R_{16})$$

b/. Quy trình giải mã

- Quy trình giải mã của DES tương tự như quy trình lập mã, nhưng theo dùng các khóa thứ tự ngược lại: $k_{16}, k_{15}, \ldots, k_1$.
- Xuất phát (đầu vào) từ bản mã y, kết quả (đầu ra) là bản rõ x.

3/. Độ an toàn của hệ mã hóa DES

- Độ an toàn của hệ mã hóa DES có liên quan đến các bảng S_j:

• Ngoại trừ các bảng S, mọi tính toán trong DES đều tuyến tính, tức là việc tính phép hoặc loại trừ của hai đầu ra cũng giống như phép hoặc loại trừ của hai đầu vào, rồi tính toán đầu ra.

• Các bảng S chứa đựng nhiều thành phần phi tuyến của hệ mật, là yếu tố quan trọng nhất đối với độ mật của hệ thống.

Khi mới xây dựng hệ mật DES, thì tiêu chuẩn xây dựng các hộp S không được biết đầy đủ. Và có thể các hộp S này có thể chứa các "cửa sập" được giấu kín. Và đó cũng là một điểm đảm bảo tính bảo mật của hệ DES

- Hạn chế của DES chính là kích thước không gian khóa:

Số khóa có thể là 2^{56}, không gian này là nhỏ để đảm bảo an toàn thực sự. Nhiều thiết bị chuyên dụng đã được đề xuất nhằm phục vụ cho phép tấn công với bản rõ đã biết. Phép tấn công này chủ yếu thực hiện theo phương pháp "vét cạn". Tức là với bản rõ x và bản mã y tương ứng (64 bit), mỗi khóa có thể đều được kiểm tra cho tới khi tìm được một khóa K thỏa mãn $e_K(x) = y$.

1.5. CHỮ KÝ SỐ

Trong các giao dịch truyền thống, chúng ta vẫn sử dụng giấy tờ, công văn cùng với chữ ký và con dấu. Việc giao dịch, trao đổi thông tin trên môi trường internet cũng cần có một cơ chế tương tự và chữ ký số được sử dụng để phục vụ cho môi trường này. Khác với chữ ký thường có thể phải mất nhiều thời gian để giám định khi cần thiết, chữ ký số có thể được giám định, xác nhận nhanh với các công cụ điện tử. Cũng thế, chứng thực số là một dịch vụ trên internet tương tự như việc công chứng trên giấy tờ, văn bản thông thường. Cụ thể, chữ ký số là một giải pháp công nghệ đảm bảo tính duy nhất cho một người khi giao dịch thông tin trên mạng đảm bảo các thông tin cung cấp là của người đó.

Chữ ký số do người sử dụng tạo ra sau khi được nhà cung cấp dịch vụ cung cấp chứng thư số. Chứng thực số được sử dụng để các đối tác của người sử dụng biết và xác định được chữ ký, chứng thư của mình là đúng.

1.5.1. Định nghĩa

Chữ ký số (một dạng chữ ký điện tử) là thông tin được mã hóa bằng khóa riêng (tương ứng với một khóa công khai) của người gửi, được đính kèm theo văn bản nhằm đảm bảo cho người nhận định danh và xác thực đúng nguồn gốc, tính toàn vẹn của dữ liệu nhận được.

Chữ ký số ra đời để khắc phục các thiếu sót của những hệ thống xác thực ra đời trước đó. Cùng với sự phát triển của thương mại điện tử, ngoài nhu cầu xác thực, các nhu cầu khác về bảo mật như toàn vẹn dữ liệu và chống từ chối cũng đều hết sức cấp thiết.

Chữ ký số đóng một vai trò rất quan trọng trong trường hợp xảy ra tranh chấp vì chữ ký số được cung cấp bởi hệ thống CA công cộng như FPT có giá trị pháp lý tương đương như chữ ký tay trong các giao dịch phi điện tử.

Chữ kí số là một tập con của chữ kí điện tử. Khái niệm chữ kí điện tử- mặc dù thường được sử dụng cùng nghĩa với *chữ ký số* nhưng thực sự có nghĩa rộng hơn. *Chữ ký điện tử* chỉ đến bất kỳ phương pháp nào (không nhất thiết là mật mã) để xác định người chủ của văn bản điện tử. Chữ ký điện tử bao gồm cả địa chỉ telex và chữ ký trên giấy được truyền bằng fax.

Chữ ký số được phát triển dựa trên lý thuyết mật mã, cụ thể là kỹ thuật mật mã hoá công khai. Trong mô hình này, một hệ mã khoá công khai sẽ có hai chìa khoá: Một chìa khoá công khai (public key) và một chìa khoá bí mật (private key), mỗi chìa khoá là một số cố định được sử dụng trong quá trình mã hoá và giải mã; trong đó, khoá công khai được công bố rộng rãi cho mọi người và được sử dụng để mã hoá, còn khoá bí mật thì được giữ kín và được sử dụng để giải mã.

Chữ ký số, tương tự như chữ ký bằng tay, nó phải có một số tính chất sau:

- Có khả năng xác thực tác giả và thời gian ký.

- Có khả năng xác thực nội dung tại thời điểm ký.

- Các thành viên thứ ba có thể kiểm tra để xác thực khi xảy ra tranh chấp.

Vì chức năng ký số bao hàm cả chức năng xác thực, dựa vào tính chất cơ bản này ta đưa một số yêu cầu sau cho chữ ký số:

- Chữ ký số phải là một mẫu bit phụ thuộc vào thông báo được ký.

- Chữ ký phải dùng thông tin duy nhất nào đó từ người gửi, nhằm ngăn chặn tình trạng giả mạo và chối bỏ.

- Tạo ra chữ ký số dễ dàng.

- Dễ nhận ra và dễ kiểm tra chữ ký.

- Khó làm giả chữ ký số bằng cách tạo ra một thông báo mới cho một chữ ký số hiện có, hoặc tạo ra một chữ ký giả cho một thông báo có trước.

- Trong thực tế cần phải sao lưu bản sao của chữ ký số.

Bảng so sánh chữ ký thông thường và chữ ký số:

	Chữ ký thông thường	**Chữ ký số**
Vấn đề ký 1 tài liệu	Chữ ký chỉ là một phần vật lý của tài liệu	Chữ ký số không gắn kiểu vật lý vào bức thông điệp nên thuật toán được dùng phải "không nhìn thấy" theo một cách nào đó trên bức thông điệp.
Vấn đề kiểm tra	Chữ ký được kiểm tra bằng cách só sánh nó với chữ ký xác thực khác. Tuy nhiên, đây không phải là một phương pháp an toàn vì nó dễ bị giả mạo.	Chữ ký số có thể kiểm tra nhờ dùng một thuật toán kiểm tra công khai. Như vậy, bất kỳ ai cũng có thể kiểm tra được chữ ký số. Việc dùng chữ ký số an toàn có thể chặn được giả mạo.

Một điểm khác biệt cơ bản nữa giữa chữ ký thông thường và chữ ký số, đó là việc sử dụng lại. Bản copy thông điệp được ký bằng chữ ký số thì đồng nhất với bản gốc, còn bản copy thông điệp được ký bằng chữ ký thông thường lại có thể khác với bản gốc. Điều này có nghĩa là cần phải ngăn chặn một bức thông điệp ký số không bị dùng lại.

Ví dụ: A ký một bức thông điệp xác nhận B rút 1000$ trong tài khoản của A, A chỉ muốn B làm điều đó một lần, do đó bản thân bức điện cần chứa thông tin thêm để ngăn nó bị dùng lại.

Đối với các hoạt động trên môi trường mạng ngày càng phát triển như hiện nay, chữ ký số là một hình thức đảm bảo tính pháp lý của các cam kết. Nó phải đáp ứng được các yêu cầu:

- Người nhận có thể xác thực được đặc điểm nhận dạng của người gửi.
- Người gửi sau này không thể chối bỏ nội dung của bản tin đã gửi.
- Người gửi không thể bịa đặt thay đổi bản tin sau khi đã gửi.

Sơ đồ chữ ký số

Một sơ đồ chữ ký số thường bao gồm hai thành phần chủ chốt là thuật toán ký và thuật toán xác minh.

Một sơ đồ chữ ký số là một bộ 5 (P, A, K, S, V) thỏa mãn các điều kiện sau :

- P là một tập hợp các bản rõ có thể
- A là tập hữu hạn các chữ ký có thể
- K là tập hữu hạn các khóa có thể
- S là tập các thuật toán ký
- V là tập các thuật toán xác minh

Với mỗi k thuộc K, tồn tại một thuật toán ký sigk thuộc S và một thuật toán xác minh verk thuộc V, trong đó sigk và verk là các ánh xạ :

sigk là một ánh xạ từ P sang A và Verk là một ánh xạ từ A sang tập biểu diễn {True, False} thỏa mãn với mọi x thuộc P, y thuộc A, ver (x,y)= true nếu y=sig(x) và ver(x,y) = false nếu y khác sig(x).

Chú ý:

Người ta thường dùng hệ mã hóa khóa công khai để lập: "*Sơ đồ chữ ký số*".

Ở đây khóa bí mật a dùng làm khóa "*ký*", khóa công khai b dùng làm khóa kiểm tra "*chữ ký*".

Ngược lại với việc mã hóa, dùng khóa công khai b để lập mã, dùng khóa bí mật a để giải mã.

Điều này là hoàn toàn tự nhiên, vì "*ký*" cần giữ bí mật nên phải dùng khóa bí mật a để "*ký*". Còn "chữ ký" là công khai cho mọi người biết, nên họ dùng khóa công khai b để kiểm tra.

1.5.2. Phân loại "Chữ ký số"

Cách 1: Phân loại chữ ký theo đặc trưng kiểm tra chữ ký

1). Chữ ký khôi phục thông điệp:

Là loại chữ ký, trong đó người gửi chỉ cần gửi "chữ ký", người nhận có thể khôi phục lại được thông điệp, đã được "ký" bởi "chữ ký" này.

2). Chữ ký đi kèm thông điệp:

Là loại chữ ký, trong đó người gửi cần gửi "chữ ký", phải gửi kèm cả thông điệp đã được "ký" bởi "chữ ký" này. Ngược lại, người nhận sẽ không có được thông điệp gốc.

Ví dụ: Chữ ký Elgaman là chữ ký đi kèm thông điệp.

Cách 2: Phân loại chữ ký theo mức an toàn.

1). Chữ ký "không thể phủ nhận":

Nhằm tránh việc nhân bản chữ ký để sử dụng nhiều lần, tốt nhất là người gửi tham gia trực tiếp vào việc kiểm thử chữ ký. Điều đó được thực hiện bằng một giao thức kiểm thử, dưới dạng một giao thức mời hỏi và trả lời.

Ví dụ: Chữ ký không phủ định (Chaum-van Antverpen).

2). Chữ ký "một lần":

Chữ ký dùng một lần (one-time signature) là một khái niệm vẫn còn khá mới mẻ song rất quan trọng, đặc biệt là trong một số mô hình về bỏ phiếu điện tử và tiền điện tử.

Để đảm bảo an toàn, "khóa ký" chỉ dùng 1 lần (one-time) trên 1 tài liệu.

Ví dụ: Chữ ký một lần Lamport. Chữ ký Fail-Stop (Van Heyst & Pedersen).

Cách 3: Phân loại chữ ký theo ứng dụng đặc trưng.

Chữ ký "mù" (Blind Signature).

Chữ ký "nhóm" (Group Signature).

Chữ ký "bội" (Multy Signature).

Chữ ký "mù nhóm" (Blind Group Signature).

Chữ ký "mù bội" (Blind Multy Signature).

1.5.3. Lịch sử

Con người đã sử dụng các hợp đồng dưới dạng điện tử từ hàng trăm 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 vượt bậc của khoa học kỹ thuật nói chung và công nghệ thông tin nói riêng gần đây thì chữ ký điện tử mới đi vào cuộc sống một cách rộng rãi.

Vào thập kỷ 1980, các công ty, tổ chức và một số cá nhân bắt đầu sử dụng máy fax để trao đổi các tài liệu quan trọng. Mặc dù chữ ký trên các tài liệu này vẫn thể hiện trên giấy tờ 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 thư điện tử, nhập các số định danh 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 trực tuyến...

1.5.4. Các ưu điểm của chữ ký số

Việc sử dụng chữ ký số mang lại một số lợi điểm sau:

1/. Khả năng xác định nguồn gốc

Các hệ thống mật mã hóa khóa công khai cho phép mật mã hóa văn bản với khóa bí mật mà chỉ có người chủ của khóa có. Để sử dụng chữ ký số thì văn bản cần phải được mã hóa hàm băm (thường có độ dài cố định và ngắn hơn nhiều so với văn bản) sau đó dùng khóa bí mật của người chủ khóa để mã hóa, khi đó ta được chữ ký số. Khi cần kiểm tra, bên nhận sử dụng khóa công khai của bên gửi thực hiện giải mã để lấy lại hàm băm và kiểm tra với hàm băm của văn bản nhận được. Nếu hai giá trị này khớp nhau thì bên nhận có thể tin tưởng rằng văn bản được gửi đi từ người sở hữu khóa bí mật. Tất nhiên chúng ta không thể đảm bảo 100% là văn bản không bị giả mạo vì hệ thống vẫn có thể bị truy cập và giả mạo.

Vấn đề là hàm băm thực đặc biệt quan trọng đối với các giao dịch tài chính. Chẳng hạn một chi nhánh ngân hàng gửi một gói tin A về trung tâm trong đó chứa thông tin về số tài khoản và số tiền gửi. Kẻ gian có thể thực hiện một giao dịch, sau đó bắt lấy nội dung gói tin A và truyền lại gói tin thu được nhiều lần hoặc thay đổi nội dung gói tin để thu lợi (tấn công truyền lại gói tin).

2/. Tính toàn vẹn

Cả hai bên tham gia vào quá trình trao đổi thông tin đều có thể tin tưởng là văn bản không bị sửa đổi trong quá trình truyền truyền vì nếu văn bản bị thay đổi dù là cực nhỏ thì giá trị hàm băm cũng sẽ thay đổi theo và việc này sẽ bị phát hiện. Nếu chỉ có quá trình mã hóa thì chỉ có thể ẩn nội dung của gói tin nhưng không thể ngăn cản được việc thay đổi nội dung của nó. Một ví dụ cho trường hợp này là tấn công đồng hình (homomorphism attack): tiếp tục ví dụ như ở trên, một kẻ lừa đảo gửi 500.000 Đồng vào tài khoản Z, sau đó bắt gói tin A mà chi nhánh gửi về trung tâm sau đó gửi gói tin B có giá trị hơn để sinh lợi.

Đây là vấn đề bảo mật của chi nhánh đối với trung tâm ngân hàng không hẳn liên quan đến tính toàn vẹn của thông tin từ người gửi tới chi nhánh, bởi thông tin đã được băm và mã hóa để gửi đến đúng đích của nó tức chi nhánh ngân hàng, vấn đề còn lại vấn đề bảo mật của chi nhánh ngân hàng tới trung tâm của nó.

3/. Tính không thể chối bỏ

Trong khi trao đổi thông tin, một bên có thể không nhận thông tin là do mình gửi đi. Để chống lại khả năng này, bên nhận có thể yêu cầu bên gửi phải gửi kèm chữ ký số với thông tin. Khi có tranh chấp xảy ra, bên nhận sẽ dùng chữ ký này như một chứng cứ để bên thứ ba giải quyết. Tuy nhiên, bằng cách nào đó khóa bí mật vẫn có thể bị lộ và tính không thể chối bỏ cũng không phải là hoàn toàn.

4/. Thực hiện chữ ký số khóa công khai

Chữ ký số khóa công khai dựa trên nền tảng mật mã hóa khóa công khai. Để có thể trao đổi thông tin trong môi trường này, mỗi người sử dụng cần tạo, hoặc đăng ký cho mình cặp khóa: một khóa bí mật và một khóa công khai. Khóa bí mật phải được bảo quản kĩ lưỡng, không được để lộ, khóa công khai sẽ được công bố rộng rãi qua nhà phân phối chứng thực khóa công khai hoặc qua được riêng. Nếu chỉ biết khóa công khai thì không thể dò ngược lại được để tìm khóa bí mật.

Quá trình này gồm ba thuật toán:

• Thuật toán tạo khóa.

• Thuật toán tạo chữ ký số.

• Thuật toán thẩm tra chữ ký số.

Xét ví dụ sau: Bob muốn gửi thông tin cho Alice và muốn Alice biết thông tin đó thực sự do chính Bob gửi. Bob gửi cho Alice bản tin kèm với chữ ký số. Chữ ký này được tạo ra với khóa bí mật của Bob. Khi nhận được bản tin, Alice sử dụng khóa công khai của Bob để kiểm tra nguồn gốc của văn bản. Bản chất của thuật toán tạo chữ ký đảm bảo nếu chỉ cho trước bản tin, rất khó (gần như không thể) tạo ra được chữ ký của Bob nếu không biết khóa bí mật của Bob.

Nếu quá trình kiểm tra cho kết quả đúng thì Alice có thể tin tưởng rằng bản tin thực sự do Bob gửi. Thông thường, Bob không mật mã hóa toàn bộ bản tin với khóa bí mật mà chỉ thực hiện với giá trị băm của bản tin đó. Điều này khiến việc ký trở nên đơn giản, thực hiện nhanh hơn và chữ ký ngắn hơn. Tuy nhiên nó cũng làm nảy sinh vấn đề khi hai bản tin khác nhau lại cho ra cùng một giá trị băm. Đây là điều có thể xảy ra khi sử dụng các thuật toán hàm băm mặc dù xác suất rất thấp.

1.5.5. Tình trạng hiện tại – luật pháp và thực tế.

Tất cả các mô hình chữ ký số cần phải đạt được một số yêu cầu để có thể được chấp nhận trong thực tế:

- Chất lượng của thuật toán: một số thuật toán không đảm bảo an toàn.

- Chất lượng của phần mềm/ phần cứng thực hiện thuật toán.

- Khóa bí mật phải được giữ an toàn.

- Quá trình phân phối khóa công cộng phải đảm bảo mối liên hệ giữa khóa và thực tế sở hữu khóa là chính xác. Việc này thường được thực hiện bởi hạ tầng khóa công cộng (PKI) và mối liên hệ khóa với người sở hữu được chứng thực bởi những người điều hành PKI. Đối với hệ thống PKI mở, nơi mà tất cả mọi người đều có thể yêu cầu sự chứng thực trên thì khả năng sai sót là rất thấp. Tuy nhiên các PKI thương mại cũng đã gặp phải rất nhiều vấn đề có thể dẫn đến những văn bản bị ký sai.

- Những người sử dụng (và phần mềm) phải thực hiện các quá trình đúng thủ tục (giao thức).

Chỉ khi các điều kiện trên được thỏa mãn thì chữ ký số mới là bằng chứng xác định người chủ (người có thẩm quyền) của văn bản.

Một số cơ quan lập pháp, dưới sự tác động của các doanh nghiệp hy vọng thu lợi từ PKI hoặc với mong muốn là người đi tiên phong trong lĩnh vực mới, đã ban hành các điều luật cho phép, xác nhận hay khuyến khích việc sử dụng chữ ký số. Nơi đầu tiên thực hiện điều này là bang Utah (Hoa Kỳ). Tiếp theo sau là các bang Massachusetts và California. Các nước khác cũng thông qua những đạo luật và quy định và cả Liên hợp quóc cũng có những dự án đưa ra những bộ luật mẫu trong vấn đề này.

Tuy nhiên, các quy định này lại thay đổi theo từng nước tùy theo điều kiện và trình độ khoa học (mật mã học). Chính sự khác nhau này làm bối rối những người sử dụng tiềm năng, gây khó khăn cho việc kết nối giữa các quốc gia và do đó làm chậm lại tiến trình phổ biến chữ ký số.

1.5.6. Đăng ký, sử dụng và thẩm tra chữ ký số.

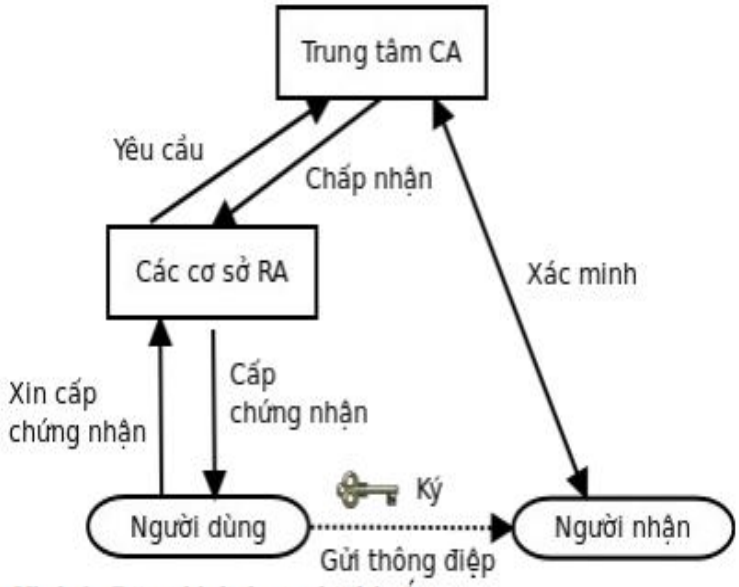
1/. Các bước mã hoá và ký

Bước 1: Ở bước này, sử dụng hàm băm để đảm bảo tính toàn vẹn của thông điệp. Các thuật toán hàm băm không làm thay đổi thông điệp mà chỉ dùng để tạo ra một chuỗi băm riêng của thông điệp. Sau đó bước 3 sẽ sử dụng thông điệp và chuỗi băm của thông điệp để thực hiện mã hóa. Bước này có thể dùng SHA hoặc MD5.

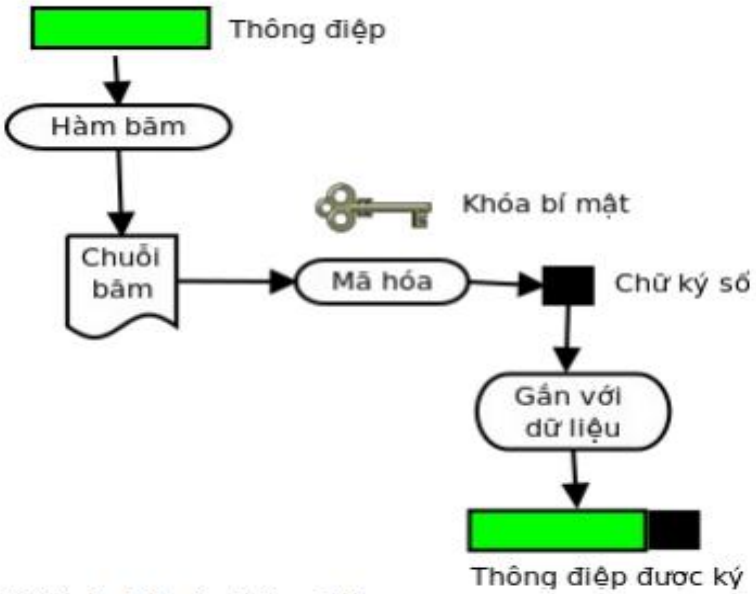
Bước 2: Mã hóa chuỗi băm của thông điệp bằng khóa bí mật của người gửi ở bước 1. Quá trình này thường dùng các thuật toán như RSA, DSA, 3DES,... Kết quả thu được chính là chữ ký số của thông điệp ban đầu.

Bước 3: Sử dụng khóa công khai của người nhận để mã hoá thông tin cần gửi đi.

Bước 4: Gộp chữ ký số vào thông điệp đã được mã hoá và gửi đi. Như vậy sau khi đã ký nhận chữ ký số vào thông điệp đã được mã hoá, mọi sự thay đổi trên thông điệp sẽ bị phát hiện trong giai đoạn thẩm tra. Ngoài ra, việc ký nhận này cho phép người nhận xác định được chính xác người gửi tin.



Hình 1: Đăng kí dịch vụ chữ ký số



Hình 2: Ký vào thông điệp

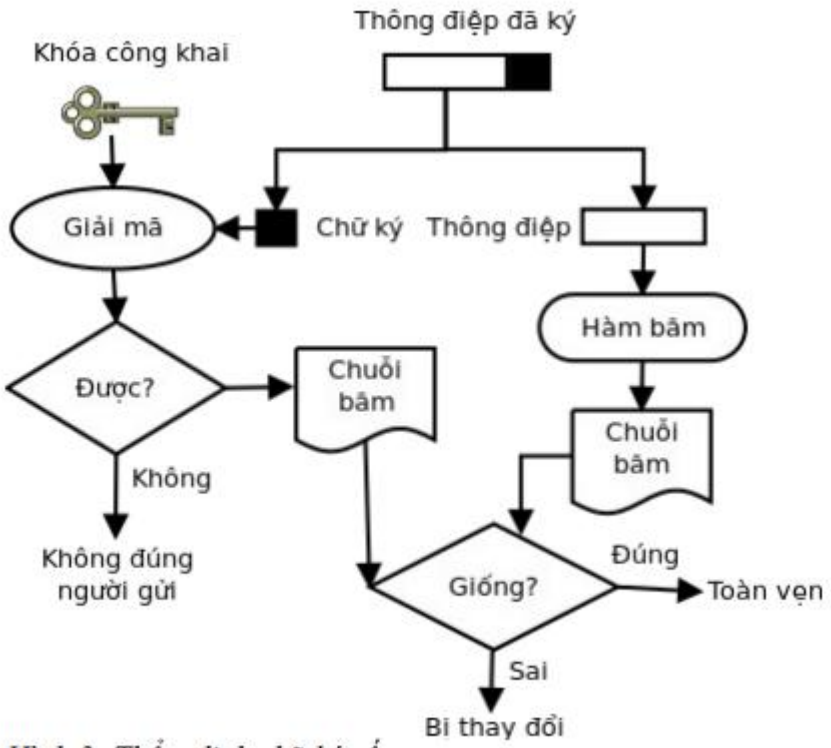
2/. Các bước kiểm tra

Bước 1: Người nhận dùng khóa bí mật của mình để giải mã thông tin nhận được gồm hai phần: phần thông điệp và phần chữ ký người gửi.

Bước 2: Dùng khóa công khai của người gửi (khoá này được phát hành qua một nhà chứng nhận khóa công khai) để giải mã chữ ký số của thông điệp, ta được chuỗi băm của thông điệp.

Bước 3: Dùng giải thuật MD5 (hoặc SHA) băm thông điệp đính kèm ta có chuỗi băm của thông điệp nữa.

Bước 4: So sánh kết quả thu được ở bước 2 và 3 nếu trùng nhau, ta kết luận thông điệp này không bị thay đổi trong quá trình truyền và thông điệp này là của người gửi.



Hình 3: Thẩm định chữ ký số

1.5.7. Một vài thuật toán dùng trong chữ ký số.

1/. Chữ ký số RSA

Trong mật mã học, RSA là một thuật toán mật mã hóa khóa công khai. Đây là thuật toán đầu tiên phù hợp với việc tạo ra chữ ký điện tử đồng thời với việc mã hóa.

Nó đánh dấu một sự tiến bộ vượt bậc của lĩnh vực mật mã học trong việc sử dụng khóa công khai. RSA đang được sử dụng phổ biến trong thương mại điện tử và được cho là đảm bảo an toàn với điều kiện độ dài khóa đủ lớn.

Thuật toán được Ron Rivest, Adi Shamir và Len Adleman mô tả lần đầu tiên vào năm 1977 tại Học viện Công nghệ Massachusetts (MIT). Tên của thuật toán lấy từ ba chữ cái đầu của tên ba tác giả.

Trước đó, vào năm 1973, Clifford Cocks, một nhà toán học người Anh, đã mô tả một thuật toán tương tự. Với khả năng tính toán tại thời điểm đó thì thuật toán này không khả thi và chưa bao giờ được thực nghiệm. Tuy nhiên, phát minh này chỉ được công bố vào năm 1997 vì được xếp vào loại tuyệt mật.

Thuật toán RSA được MIT đăng ký bằng sáng chế tại Hoa Kỳ vào năm 1983 (Số đăng ký 4.405.829). Bằng sáng chế này hết hạn vào ngày 21 tháng 9 năm 2000. Tuy nhiên, do thuật toán đã được công bố trước khi có đăng ký bảo hộ nên sự bảo hộ hầu như không có giá trị bên ngoài Hoa Kỳ. Ngoài ra, nếu như công trình của Clifford Cocks đã được công bố trước đó thì bằng sáng chế RSA đã không thể được đăng ký.

Thuật toán RSA có hai khóa: khóa công khai và khóa bí mật. Mỗi khóa là những số cố định sử dụng trong quá trình mã hóa và giải mã. Khóa công khai được công bố rộng rãi cho mọi người và được dùng để mã hóa. Những thông tin được mã hóa bằng khóa công khai chỉ có thể được giải mã bằng khóa bí mật tương ứng. Nói cách khác, mọi người đều có thể mã hóa nhưng chỉ có người biết khóa bí mật mới có thể giải mã được.

a). Tạo khóa

Giả sử Alice và Bob cần trao đổi thông tin bí mật thông qua một kênh không an toàn (ví dụ như Internet). Với thuật toán RSA, Alice đầu tiên cần tạo ra cho mình cặp khóa gồm khóa công khai và khóa bí mật theo các bước sau:

• Chọn 2 số nguyên tố lớn p và q với $p \neq q$, lựa chọn ngẫu nhiên và độc lập.

• Tính: $n = pq$.

• Tính: giá trị hàm số Ơle $\varphi(n)=(p-1)(q-1)$.

• Chọn một số tự nhiên e sao cho $1< e < \varphi(n)$ và là số nguyên tố cùng nhau với $\varphi(n)$.

• Tính: d sao cho $de \equiv 1 (\mathrm{mod}\ \varphi(n))$.

Khóa công khai bao gồm:

• *n*, môđun

• *e*, số mũ công khai (cũng gọi là số mũ mã hóa).

Khóa bí mật bao gồm:

• *n*, môđun, xuất hiện cả trong khóa công khai và khóa bí mật

• *d*, số mũ bí mật (cũng gọi là số mũ giải mã).

Một dạng khác của khóa bí mật bao gồm:

• *p* and *q*, hai số nguyên tố chọn ban đầu

• *d mod (p-1)* và *d mod (q-1)* (thường được gọi là *dmp1* và *dmq1*)

• *(1/q) mod p* (thường được gọi là *iqmp*)

Dạng này cho phép thực hiện giải mã và ký nhanh hơn với việc sử dụng định lý số dư Trung Quốc. Ở dạng này, tất cả thành phần của khóa bí mật phải được giữ bí mật.

Alice gửi khóa công khai cho Bob, và giữ bí mật khóa cá nhân của mình. Ở đây, *p* và *q* giữ vai trò rất quan trọng. Chúng là các phân tố của n và cho phép tính *d* khi biết *e*. Nếu không sử dụng dạng sau của khóa bí mật (dạng CRT) thì *p* và *q* sẽ được xóa ngay sau khi thực hiện xong quá trình tạo khóa.

b). Mã hóa

Giả sử Bob muốn gửi đoạn thông tin M cho Alice. Đầu tiên Bob chuyển *M* thành một số $m < n$ theo một hàm có thể đảo ngược (từ *m* có thể xác định lại *M*) được thỏa thuận trước.

Lúc này Bob có *m* và biết *n* cũng như *e* do Alice gửi. Bob sẽ tính *c* là bản mã hóa của *m* theo công thức: $c = m^e \bmod n$

Hàm trên có thể tính dễ dàng sử dụng phương pháp tính hàm mũ (theo môđun) bằng (thuật toán bình phương và nhân). Cuối cùng Bob gửi *c* cho Alice.

c). Giải mã

Alice nhận *c* từ Bob và biết khóa bí mật *d*. Alice có thể tìm được m từ c theo công thức sau:

$$m=c^d \bmod n$$

Biết *m*, Alice tìm lại M theo phương pháp đã thỏa thuận trước. Quá trình giải mã hoạt động vì ta có:

$$c^d \equiv (m^e)^d \equiv m^{ed} \bmod n.$$

Do $ed \equiv 1 \pmod{p-1}$ và $ed \equiv 1 \pmod{q-1}$, (theo Định lý Fermat nhỏ) nên:

$$m^{ed} \equiv m \bmod p \text{ và } m^{ed} \equiv m \bmod q$$

Do *p* và *q* là hai số nguyên tố cùng nhau, áp dụng định lý số dư Trung Quốc, ta có:

$$m^{ed} \equiv m \bmod pq. \text{ hay } c^d \equiv m \bmod n.$$

d). Ví dụ

Sau đây là một ví dụ với những số cụ thể. Ở đây chúng ta sử dụng những số nhỏ để tiện tính toán còn trong thực tế phải dùng các số có giá trị đủ lớn.

Lấy:

p = 61 - số nguyên tố thứ nhất (giữ bí mật hoặc hủy sau khi tạo khóa)

q = 53 - số nguyên tố thứ hai (giữ bí mật hoặc hủy sau khi tạo khóa)

n = pq = 3233 - môđun (công bố công khai)

e = 17 - số mũ công khai

d = 2753 - số mũ bí mật

Khóa công khai là cặp (e, n). Khóa bí mật là d. Hàm mã hóa là:

$$encrypt(m) = m^e \bmod n = m^{17} \bmod 3233$$

với *m* là văn bản rõ. Hàm giải mã là:

$$decrypt(c) = c^d \bmod n = c^{2753} \bmod 3233$$

với *c* là văn bản mã.

Để mã hóa văn bản có giá trị 123, ta thực hiện phép tính:

$$encrypt(123) = 123^{17} \bmod 3233 = 855$$

Để giải mã văn bản có giá trị 855, ta thực hiện phép tính:

$$decrypt(855) = 855^{2753} \bmod 3233 = 123$$

Cả hai phép tính trên đều có thể được thực hiện hiệu quả nhờ giải thuật bình phương và nhân.

e). Chuyển đổi văn bản rõ

Trước khi thực hiện mã hóa, ta phải thực hiện việc chuyển đổi văn bản rõ (chuyển đổi từ *M* sang *m*) sao cho không có giá trị nào của M tạo ra văn bản mã không an toàn. Nếu không có quá trình này, RSA sẽ gặp phải một số vấn đề sau:

• Nếu *m* = 0 hoặc *m* = 1 sẽ tạo ra các bản mã có giá trị là 0 và 1 tương ứng

• Khi mã hóa với số mũ nhỏ (chẳng hạn *e* = 3) và m cũng có giá trị nhỏ, giá trị *m^e* cũng nhận giá trị nhỏ (so với *n*). Như vậy phép môđun không có tác dụng và có thể dễ dàng tìm được *m* bằng cách khai căn bậc *e* của *c* (bỏ qua môđun).

• RSA là phương pháp mã hóa xác định (không có thành phần ngẫu nhiên) nên kẻ tấn công có thể thực hiện tấn công lựa chọn bản rõ bằng cách tạo ra một bảng tra giữa bản rõ và bản mã. Khi gặp một bản mã, kẻ tấn công sử dụng bảng tra để tìm ra bản rõ tương ứng.

Trên thực tế, ta thường gặp 2 vấn đề đầu khi gửi các bản tin ASCII ngắn với m là nhóm vài ký tự ASCII. Một đoạn tin chỉ có 1 ký tự NUL sẽ được gán giá trị *m* = 0 và cho ra bản mã là 0 bất kể giá trị của *e* và *N*. Tương tự, một ký tự ASCII khác, SOH, có giá trị 1 sẽ luôn cho ra bản mã là 1. Với các hệ thống dùng giá trị *e* nhỏ thì tất cả ký tự ASCII đều cho kết quả mã hóa không an toàn vì giá trị lớn nhất của *m* chỉ là 255 và 255^3 nhỏ hơn giá trị *n* chấp nhận được. Những bản mã này sẽ dễ dàng bị phá mã.

Để tránh gặp phải những vấn đề trên, RSA trên thực tế thường bao gồm một hình thức chuyển đổi ngẫu nhiên hóa *m* trước khi mã hóa. Quá trình chuyển đổi này phải đảm bảo rằng *m* không rơi vào các giá trị không an toàn. Sau khi chuyển đổi, mỗi bản rõ khi mã hóa sẽ cho ra một trong số khả năng trong tập hợp bản mã.

Điều này làm giảm tính khả thi của phương pháp tấn công lựa chọn bản rõ (một bản rõ sẽ có thể tương ứng với nhiều bản mã tuỳ thuộc vào cách chuyển đổi).

Một số tiêu chuẩn, chẳng hạn như PKCS, đã được thiết kế để chuyển đổi bản rõ trước khi mã hóa bằng RSA. Các phương pháp chuyển đổi này bổ sung thêm bít vào *M*. Các phương pháp chuyển đổi cần được thiết kế cẩn thận để tránh những dạng tấn công phức tạp tận dụng khả năng biết trước được cấu trúc của bản rõ. Phiên bản ban đầu của PKCS dùng một phương pháp đặc ứng (ad-hoc) mà về sau được biết là không an toàn trước tấn công lựa chọn bản rõ thích ứng (adaptive chosen ciphertext attack). Các phương pháp chuyển đổi hiện đại sử dụng các kỹ thuật như chuyển đổi mã hóa bất đối xứng tối ưu (Optimal Asymmetric Encryption Padding - OAEP) để chống lại tấn công dạng này. Tiêu chuẩn PKCS còn được bổ sung các tính năng khác để đảm bảo an toàn cho chữ ký RSA (Probabilistic Signature Scheme for RSA – RSA-PSS).

2/. Chữ ký số DSA

Giải thuật ký số (Digital Signature Algorithm, viết tắt DSA) là chuẩn của chính phủ Mỹ hoặc FIPS cho các chữ ký số.

a). Tạo khoá

• Chọn số nguyên tố 160 bit q.

• Chọn 1 số nguyên tố L bit p, sao cho p=qz+1 với số nguyên z nào đó,

$512 \leq L \leq 1024$, L chia hết cho 64.

• Chọn h, với $1 < h < p - 1$ sao cho $g = h^z \bmod p > 1$. ($z = (p-1) / q$)

• Chọn x ngẫu nhiên, thoả mãn $0 < x < q$.

• Tính giá trị $y = g^x \bmod p$.

• Khoá công là (p, q, g, y). Khoá riêng là x.

Hầu hết các số h đều thoả mãn yêu cầu, vì vậy giá trị 2 thông thường được sử dụng.

b). Ký

• Tạo 1 số ngẫu nhiên với mỗi thông điệp, giá trị k thỏa mãn 0 < k < q

• Tính $r = (g^k \bmod p) \bmod q$

• Tính $s = (k^{-1} (\text{SHA-1}(m) + x*r)) \bmod q$, ở đây SHA-1*(m)* là hàm băm mã hoá SHA-1 áp dụng cho thông điệp *m*

• Tính toán lại chữ ký trong trường hợp không chắc chắn khi *r=0* hoặc *s=0*

• Chữ ký là *(r,s)*

Giải thuật Euclid mở rộng có thể được sử dụng để tính toán biểu thức $k^{-1} \bmod q$.

c). Xác nhận

• Loại bỏ chữ ký nếu hoặc 0< *r* <q hoặc 0< *s* <q không thỏa mãn.

• Tính $w = (s)^{-1} \bmod q$

• Tính $u1 = (\text{SHA-1}(m)*w) \bmod q$

• Tính $u2 = (r*w) \bmod q$

• Tính $v = ((g^{u1}*y^{u2}) \bmod p) \bmod q$

• Chữ ký là có hiệu lực nếu v = r

d). Sự đúng đắn của giải thuật

Lược đồ ký số là đúng đắn có ý nghĩa khi người xác nhận luôn chấp nhận các chữ ký thật. Điều này có thể được chỉ ra như sau:

Từ $g = h^z \bmod p$ suy ra $g^q \equiv h^{qz} \equiv h^{p-1} \equiv 1 \pmod p$ bởi định lý Fermat nhỏ. Bởi vì $g>1$ và q là số nguyên tố suy ra g có bậc q.

Người ký tính

$$s=k^{-1}(SHA-1(m)+xr) \bmod q$$

Như vậy: $k \equiv SHA-1(m)s^{-1} + xrs^{-1} \equiv SHA-1(m)w+xrw \pmod q$.

Bởi vì g có bậc q chúng ta có

$$g^k \equiv g^{SHA-1(m)w}\, g^{xrw} \equiv g^{SHA-1(m)w}\, y^{rw} \equiv g^{u1}\, y^{u2} \pmod p.$$

Cuối cùng, tính đúng đắn của DSA suy ra từ

$$r=(g^k \bmod p) \bmod q = (g^{u1}\, y^{u2} \bmod p) \bmod q = v.$$

3/. Ký số Schnoor

Sơ đồ:

Lấy G là nhóm con cấp q của **Z_n* với q là số nguyên tố.**

Chọn phần tử sinh g $\in$ G sao cho bài toán logarit trên G là khó giải.

Chọn x $\neq$ 0 làm khóa bí mật

Tính y = g^x làm khóa công khai

Lấy H làm hàm băm không va chạm.

*** Ký:**

Giả sử cần ký trên văn bản m

Chọn r ngẫu nhiên thuộc Z_q

Tính c = H (m,x^r)

Tính s = (r+xc) mod q

Chữ ký Schorr là cặp (c,s)

*** Kiểm tra chữ ký:**

Với một văn bản m cho trước, một cặp (c, s) được gọi là một chữ ký Schnorr hợp lệ nếu thỏa mãn phương trình.

c = H (m, g^s * y^s)

4/. Chữ ký dùng một lần.

Sơ đồ chữ ký dùng một lần có nhiều ứng dụng, đặc biệt là một số ứng dụng trong các mô hình tiền điện tử. Sau đây là sơ đồ chữ ký dùng một lần của Schorr.

Với sơ đồ này, người dùng trong cùng một hệ thống có thể chia sẻ một số ngẫu nhiên và 2 số nguyên tố p và q sao cho: $q \mid (p-1)$, $q \neq 1$ và $g^q = 1 \bmod q$

Chuẩn bị:

Người dùng, giả sử Alice chọn $S_k \in Z_q$ ngẫu nhiên làm khóa bí mật.

Tính $P_t = g^{-sk} \bmod p$ làm khóa công khai.

Ký:

Giả sử Alice cần ký trên thông điệp m

Alice lấy ngẫu nhiên $r \in Z_q^*$

Tính $x = g^r \bmod p$, $c = H(m||x)$, $y = (r + cS_k) \bmod q$

Chữ ký trên thông điệp m là (c, y)

Kiểm tra:

Ver = true $\Leftrightarrow$ $x = g^r \bmod p$ và $c = H(m \,||\, x)$

Nhận xét:

Số r không được dùng quá một lần để tạo ra các chữ ký khác nhau.

Alice sử dụng r để ký hai lân thông điệp m và m', tạo ra hai chữ ký khác nhau là (c, y) và (c', y'). Khi đó ta có:

$(y - y') = [(r + cS_k) - (r + c'S_k)] = S_k * (c - c')$

Như vậy, nếu Alice sử dụng r quá một lần để ký cho hai thông điệp khác nhau, thì bất kỳ ai có hai thông điệp trên, đều có thể giải mã được khóa bí mật S_k.

Vì vậy, sơ đồ chữ ký này được gọi là sơ đồ chữ ký dùng một lần.

5/. Chữ ký không thể phủ định

Trong các sơ đồ chữ ký điện tử ta đã trình bày ở trên, việc kiểm thử tính đúng đắn của chữ ký là do người nhận tiến hành. Như vậy, cả văn bản cùng chữ ký có thể được sao chép và phát tán cho nhiều người mà không được phép của người gửi. Để tránh khả năng đó, người ta đưa ra sơ đồ Chữ ký không thể phủ định được với một yêu cầu là chữ ký không thể được kiểm thử nếu không có sự hợp tác của người ký. Sự hợp tác đó được thể hiện qua giao thức kiểm thử (hay xác nhận).

Khi chữ ký đòi hỏi được xác nhận bằng một giao thức kiểm thử thì một vấn đề nảy sinh là làm sao có thể ngăn cản người ký chối bỏ một chữ ký mà anh ta đã ký? Để đáp ứng yêu cầu đó, cần có thêm một giao thức chối bỏ, thông qua giao thức này, người ký có thể chứng minh một chữ ký không phải là chữ ký của mình.
Nếu anh ta từ chối không tham gia giao thức đó thì có bằng chứng là anh ta không chứng minh được chữ ký đó là giả mạo, tức là anh ta không chối bỏ được chữ ký của mình.
Một sơ đồ Chữ ký không thể phủ định có 3 phần:

- Một thuật toán ký.
- Một giao thức kiểm thử (giao thức xác nhận).
- Một giao thức chối bỏ.

1.6. HẠ TẦNG MẬT MÃ KHÓA CÔNG KHAI (PKI)

Để triển khai được chữ ký số, việc cần thiết nhất là phải xây dựng được hệ thống PKI hoàn chỉnh, thuận tiện với người sử dụng.

1.6.1. Tổng quan về PKI

Public Key Infrastructure (PKI) là một cơ chế để cho một bên thứ ba (thường là nhà cung cấp chứng thực số) cung cấp và xác thực thông tin định danh các bên tham gia vào quá trình trao đổi thông tin. Cơ chế này cho phép gán cho mỗi người sử dụng trong hệ thống một cặp khóa bí mật/khóa công khai. Hệ thống này thường bao gồm một phần mềm ở trung tâm, và các chi nhánh ở những địa điểm khác nhau của người dùng. Khoá công khai thường được phân phối dựa trên cơ sở hạ tầng khóa công khai – hay Public Key Infrastructure.

Khái niệm hạ tầng khoá công khai thường được dùng chỉ toàn bộ hệ thống bao gồm cả nhà cung cấp chứng thực số (CA) cùng các cơ chế liên quan đồng thời với toàn bộ việc sử dụng các thuật toán mã hoá công khai trong trao đổi thông tin. Trên thực tế một hệ thông PKI không nhất thiết phải sử dụng phương pháp mã hóa khóa công khai.

1.6.2. Các thành phần của PKI

PKIs thông thường bao gồm các thành phần chính sau:

• Chứng thực và đăng ký mật mã đầu cuối.

• Kiểm tra tính toàn vẹn của khoá công khai.

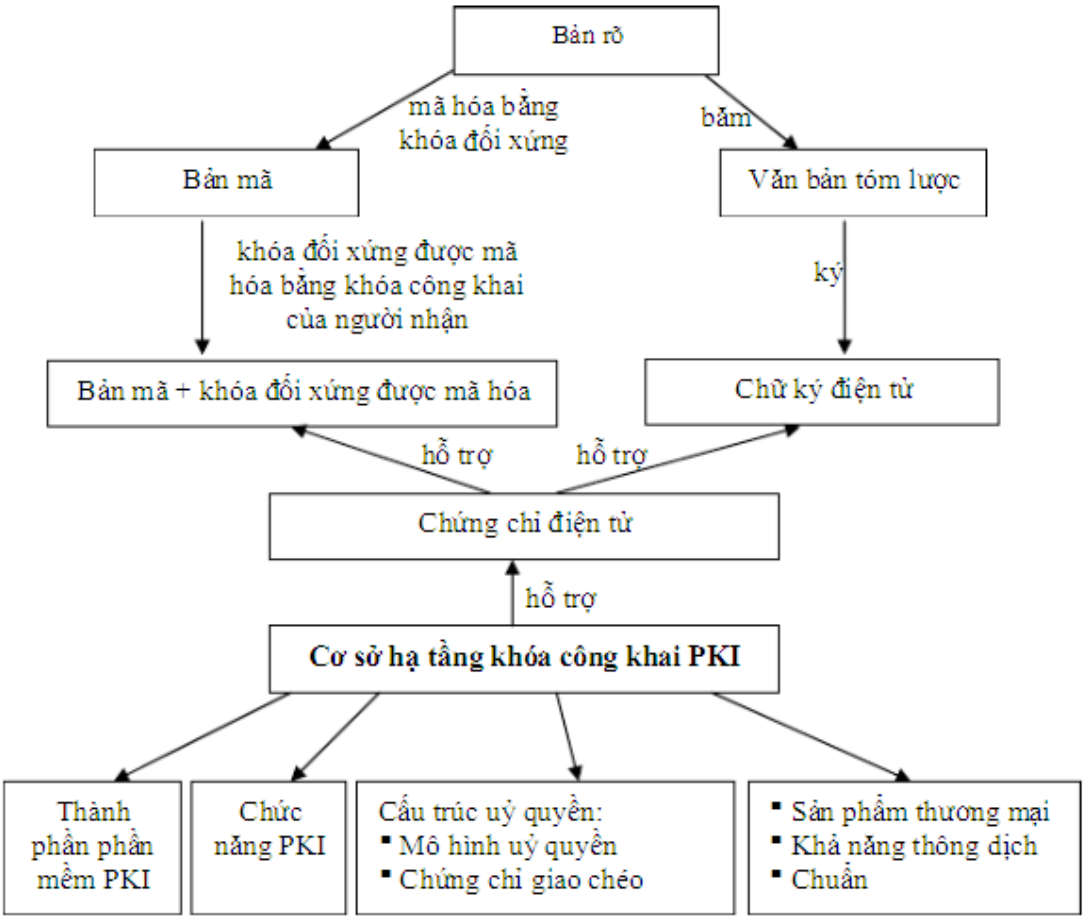
• Chứng thực yêu cầu trong quá trình bảo quản các khoá công khai.

• Phát hành khoá công khai.

• Huỷ bỏ khoá công khai.

• Duy trì việc thu hồi các thông tin về khoá công khai (CRL).

• Đảm bảo an toàn về độ lớn của khoá.



Kỹ thuật kết nối an toàn gói tin trên Internet

1/. Chứng nhận khóa công khai

Mục tiêu của việc trao đổi khoá bất đối xứng là phát một cách an toàn khoá công khai từ người gửi (mã hoá) đến người nhận (giải mã). PKI hỗ trợ tạo điều kiện cho việc trao đổi khoá an toàn để đảm bảo xác thực các bên trao đổi với nhau. Chứng nhận khóa công khai được phát bởi nhà cung cấp chứng nhận số (CA). Để nhà cung cấp chứng nhận số cấp phát chứng nhận cho người dùng thì việc đầu tiên là phải đăng ký. Quá trình đăng ký gồm: đăng ký, kích hoạt, và chứng nhận của người dùng với PKI (CAs và RAs).

Quá trình đăng ký như sau:

• Người dùng đăng ký với CA hoặc RA. Trong quá trình đăng ký, người dùng đưa ra cách nhận biết đến CA. CA sẽ xác thực đầu cuối, phát khóa công khai đến người sử dụng.

• Các đầu cuối bắt đầu khởi tạo phase bằng cách tạo ra một cặp khóa và khóa công khai của cặp khóa được chuyển đến CA.

• CA viết mật hiệu lên chứng nhận khóa công khai cùng với khóa bí mật để tạo một chứng nhận khóa công khai cho mật mã đầu cuối.

Lúc này các người dùng có thể yêu cầu và nhận chứng thực khóa công khai từ người sử dụng khác. Chúng có thể sử dụng khóa công khai của CAs để giải mã chứng nhận khóa công khai để thu được khoá tương ứng.

Trong nhiều trường hợp, CA sẽ cung cấp tất cả các dịch vụ cần thiết của PKI để quản lý các khóa công khai bên trong mạng. Tuy nhiên có nhiều trường hợp CA có thể uỷ nhiệm làm công việc của RA. một số chức năng mà CA có thể uỷ nhiệm thay thế cho RA như:

• Kiểm tra mật mã đầu cuối đã đăng ký khóa công khai với CA để có khóa bí mật mà được dùng để kết hợp với khóa công khai.

• Phát cặp khóa được dùng để khởi tạo phase của quá trình đăng ký.

• Xác nhận các thông số của khóa công khai.

• Phát gián tiếp các danh sách thu hồi chứng nhận (CRL).

2/. Phát hành chứng nhận số

CA dùng để cấp phát chứng nhận, xác thực PKI khách, và khi cần thiết thu hồi lại chứng nhận. CA đại diện cho nguồn tin cậy chính của PKI. Vì CA là yếu tố duy nhất trong PKI mà có thể phát chứng thực khóa công khai đến những người sử dụng. CA cũng luôn đáp ứng cho việc duy trì CRL. PKI không phải chỉ có một CA mà PKI có thể thiết lập nhiều CAs khác nhau.

Các CA giúp dễ dàng xác nhận và lấy thông tin của những người thực hiện trao đổi thông tin với nhau. Các CA không chỉ chứng nhận cho những người dùng mà còn có thể chứng nhận những CA khác bằng cách cấp phát chứng nhận cho chúng. Những CA đã được chứng nhận lại có thể chứng nhận tiếp cho những CA khác, cứ như vậy cho đến khi các thực thể có thể ủy nhiệm cho nhau trong quá trình giao dịch.

1.6.3. Mục tiêu và các chức năng của PKI

PKI cho phép những người tham gia xác thực lẫn nhau và sử dụng các thông tin từ các chứng thực khoá công khai để mã hoá và giải mã thông tin trong quá trình trao đổi.

PKI cho phép các giao dịch điện tử được diễn ra đảm bảo tính bí mật, toàn vẹn và xác thực lẫn nhau mà không cần trao đổi các thông tin bảo mật từ trước.

Mục tiêu chính của PKI là cung cấp khoá công khai và xác định mối liên hệ giữa khoá và định dạng người dùng. Nhờ vậy, người dùng có thể sử dụng trong một số ứng dụng như :

• Mã hoá Email hoặc xác thực người gửi Email.

• Mã hoá hoặc chứng thực văn bản.

• Xác thực người dùng ứng dụng.

• Các giao thức truyền thông an toàn.

1.6.4. Các dịch vụ PKI

PKI chủ yếu cung cấp dịch vụ xuất bản chứng chỉ và làm sao có thể truy nhập và sử dụng chúng. Giống như danh bạ điện thoại vậy, thư mục PKI liệt kê khóa công khai của tổ chức hay cá nhân. Các PKI giải quyết các bài toán quản lý khóa: tạo sinh, phân phối, xác thực và lưu giữ. Một cơ sở hạ tầng khóa công khai PKI gồm:

- Một ủy quyền chứng chỉ (CA) sinh và kiểm thử các chứng chỉ.
- Một ủy quyền đăng ký (RA) thực hiện kiểm thử ủy quyền chứng chỉ trước khi xuất bản chứng chỉ cho bên yêu cầu.
- Dịch vụ thư mục (DS) trong đó các chứng chỉ (cùng với khóa công khaic ủa chúng) được lưu giữ và có sẵn dùng (thường là trong thư mục chuẩn ITU X.500)
- Thực thể cuối (EE) giữ chứng chỉ: người dùng, tổ chức, ứng dụng..
- Các client dùng PKI để nhận chứng chỉ, hợp lệ chứng chỉ và chữ ký

Một hệ thống quản lý chứng chỉ.

Hệ thống quản lý chứng chỉ thường có các dịch vụ sau:

- Hủy bỏ chứng chỉ: hủy chứng chỉ đã xuất bản, tạo và công khai danh sách chứng chỉ thu hồi
- Hết hạn chứng chỉ và cập nhật
- Dịch vụ bảo đảm có thể giải mã được các văn bản đã mã hóa trước đó
- Sao lưu và phục hồi chứng chỉ: bảo đảm không bị mất thông tin
- Dịch vụ hỗ trợ không thể thoái thác: việc sao lưu và phục hồi khóa gây ra một kẽ hở cho hệ thống. Ai đó có thể lợi dụng điều này cho rằng đã có người khác truy nhập tới khóa đăng ký của họ, vì thế họ không hoàn toàn chịu trách nhiệm cho những giao dịch kiểu như thế, mặc dù những giao dịch này rõ ràng là do họ ký. Do đó cần thiết phải duy trì hai cặp khóa cho mỗi người dùng. Cặp khóa mã hóa có thể sao lưu và phục hồi, ngược lại thì cặp khóa ký không nên để cho người dùng sở hữu hoàn toàn.
- Dịch vụ tem thời gian
- Hợp lệ chứng chỉ thông qua chính sách.

Chương 2. MỘT SỐ BÀI TOÁN VỀ AN TOÀN THÔNG TIN TRONG GIAI ĐOẠN KIỂM PHIẾU ĐIỆN TỬ

2.1. MỘT SỐ BÀI TOÁN

2.1.1. Bài toán thông gian giữa người kiểm phiếu và ứng viên

Tình huống: Ứng viên "tác động" đến Người của Ban kiểm phiếu để họ sửa thông tin lá phiếu, nhằm có lợi cho ứng viên. Ở đây là sửa những lá *phiếu không bầu* cho ứng viên thành lá *phiếu bầu* cho ứng viên.

2.1.2. Bài toán thông gian giữa ứng viên và cử tri

Tình huống: "Cử tri Bán phiếu bầu"

Cử tri cho Ứng viên "Xem" lá phiếu của họ

(Chiếu trên màn hình khi kiểm phiếu công khai).

Ứng viên nhìn thấy lá phiếu Bầu cho mình, nên phải "Cám ơn" cử tri.

2.2. CÁCH GIẢI QUYẾT

2.2.2. Bảo vệ nội dung lá phiếu, phòng tránh sửa đổi trái phép

Dùng "người trung thực" đứng giữa.

Cử tri gửi lá phiếu, phải qua "người trung thực".

"người trung thực" mã hoá lá phiếu lần 2, sau đó gửi vào hòm phiếu.

Khi kiểm phiếu, chiếu lên màn hình.

Cử tri không nhận ra lá phiếu của mình, nhằm tránh "Cử tri Bán phiếu bầu".

Sau đây là các cách dùng để bảo vệ nội dung lá phiếu nhằm phòng tránh sửa đổi trái phép:

1). Chữ ký không thể phủ định

Trong phần trước ta đã trình bày một số sơ đồ chữ ký điện tử. Trong các sơ đồ đó, việc kiểm thử tính đúng đắn của chữ ký là do người nhận thực hiện. Nhằm tránh việc nhân bản chữ ký để sử dụng nhiều lần, tốt nhất là để người gửi tham gia trực tiếp vào việc kiểm thử chữ ký. Điều đó được thực hiện bằng một giao thức kiểm thử, dưới dạng một giao thức mời hỏi và trả lời.

Giả sử tài liệu cùng chữ ký từ G gửi đến N. Khi N yêu cầu G cùng kiểm thử chữ ký, thì một vấn đề nảy sinh là làm sao để ngăn cản G chối bỏ một chữ ký mà anh ta đã ký, G có thể tuyên bố rằng chữ ký đó là giả mạo ?

Để giải quyết tình huống trên, cần có thêm giao thức chối bỏ, bằng giao thức này, G có thể chứng minh một chữ ký là giả mạo. Nếu G từ chối tham gia vào giao thức đó, thì có thể xem rằng G không chứng minh được chữ ký đó là giả mạo.

Như vậy sơ đồ chữ ký không phủ định được gồm 3 phần: một thuật toán ký, một giao thức kiểm thử, và một giao thức chối bỏ.

Sơ đồ. (Chaum - van Antverpen).

Chuẩn bị các tham số:

Chọn số nguyên tố p sao cho bài toán log rời rạc trong Z_p là khó.

p = 2*q+1, q cũng là số nguyên tố.

Gọi P là nhóm nhân con của Z_p* theo q (P gồm các thặng dư bậc hai theo mod p).

Chọn phần tử sinh g của nhóm P cấp q.

Đặt P = A = P, K = {(p, g, a, h): $a \in Z_q^*$, $h \equiv g^a \bmod p$ }

Thuật toán ký:

Dùng khoá bí mật k' = a để ký lên x:

Chữ ký là $y = Sig_{k'}(x) = x^a \bmod p$.

Giao thức kiểm thử:

Dùng khoá công khai k" = (**p**, **g**, **h**).

Với **x**, **y** ∈ **P**, người nhận N cùng người gửi G thực hiện giao thức kiểm thử:

1/. N chọn ngẫu nhiên e_1, $e_2 \in Z_q^*$

2/. N tính $c = y^{e1} h^{e2} \bmod p$, và gửi cho G.

3/. G tính $d = c^{a^{-1} \bmod q} \bmod p$ và gửi cho N.

4/. N chấp nhận **y** là chữ ký đúng, nếu $d \equiv x^{e1} g^{e2} \bmod p$

Giao thức chối bỏ:

1/. N chọn ngẫu nhiên e_1, $e_2 \in Z_q^*$

2/. N tính $c = y^{e1} h^{e2} \bmod p$, và gửi cho G.

3/. G tính $d = c^{a^{-1} \bmod q} \bmod p$ và gửi cho N.

4/. N thử điều kiện $d \neq x^{e1} g^{e2} \pmod p$.

5/. N chọn ngẫu nhiên $f_1, f_2 \in Z_q^*$.

6/. N tính $C = y^{f_1} * \beta^{f_2} \bmod p$ và gửi cho G.

7/. G tính $D = C^{a^{-1} \bmod q} \bmod p$ và gửi cho N.

8/. N thử điều kiện $D \neq x^{f1} g^{f2} \pmod p$.

9/. N kết luận **y** là chữ ký *giả mạo* nếu:

$(d * \alpha^{-e_2})^{f_1} \equiv (D * \alpha^{-f_2})^{e_1} \pmod p$ (thay α bằng g).

Ví dụ Ký trên **x** = 229

Chuẩn bị các tham số:

Chọn số nguyên tố p = 467 = 2 * q + 1, q = 233 cũng là số nguyên tố.

Chọn phần tử sinh của nhóm P là g = 4, (P là nhóm nhân con cấp q của Z_p*).

Đặt P = A = P, K = {(p, g, a, h): $a \in Z_q^*$, $h \equiv g^a \bmod p$ }

Chọn khóa mật a = 121. Khóa công khai $h \equiv g^a \bmod p = 4^{121} \bmod 467 = 422$.

Thuật toán ký:

Dùng khoá bí mật k' = **a** để ký lên **x** = 229:

Chữ ký là $\mathbf{y} = \mathbf{Sig}_{k'}(\mathbf{x}) = \mathbf{x}^{\mathbf{a}} \bmod \mathbf{p} = 229^{121} \bmod 467 = \mathbf{9}$.

Giao thức kiểm thử:

Dùng khoá công khai k" = (p, g, h) = (467, 4, 422).

1/. N chọn ngẫu nhiên $e_1 = 48$, $e_2 = 213 \in Z_q^*$

2/. N tính $\mathbf{c} = y^{e1} h^{e2} \bmod p = 116$ và gửi cho G.

3/. G tính $d = c^{a^{-1} \bmod q} \bmod p = 235$ và gửi cho N.

4/. N chấp nhận **y** là chữ ký đúng, nếu $d \equiv x^{e1} g^{e2} \bmod p$

N thử điều kiện $d \equiv x^{e1} g^{e2} \bmod p$.

Rõ ràng $235 \equiv 229^{48} * 4^{213} \pmod{467}$.

N chấp nhận **y** = **9** đúng là chữ ký của G trên **x** = 229.

Giao thức chối bỏ:

Giả sử G gửi tài liệu **x** = 226 với chữ ký **y** = 183. Giao thức chối bỏ thực hiện:

1/. N chọn ngẫu nhiên $e_1 = 47$, $e_2 = 137 \in Z_q^*$

2/. N tính $c = y^{e1} h^{e2} \bmod p = 306$, và gửi cho G.

3/. G tính $d = c^{a^{-1} \bmod q} \bmod p = 184$, và gửi cho N.

4/. N thử điều kiện $d \neq x^{e1} g^{e2} \pmod p$.

Điều kiện trên không đúng vì $184 \neq 226^{47} * 4^{137} \equiv 145 \bmod 467$.

N lại tiếp tục thực hiện bước 5 của giao thức.

5/. N chọn ngẫu nhiên $f_1 = 225$, $f_2 = 19 \in Z_q^*$.

6/. N tính $C = y^{f_1} * \beta^{f_2} \bmod p = 348$, và gửi cho G.

7/. G tính $D = C^{a^{-1} \bmod q} \bmod p = 426$, và gửi cho N.

8/. N thử điều kiện $D \neq x^{f1} g^{f2} \pmod p$.

$D = 426$ trong khi $x^{f1} g^{f2} \pmod p = 226^{225} * 4^{19} \equiv 295 \bmod 467$.

Điều kiện 8 là đúng, nên N thực hiện bước 9:

9/. N kết luận **y** là chữ ký ***giả mạo*** nếu:

$(d * \alpha^{-e_2})^{f_1} \equiv (D * \alpha^{-f_2})^{e_1} \pmod p$ (thay α bằng g).

N tính giá trị của 2 vế đồng dư ≡

$(d * \alpha^{-e2})^{f1} \equiv (184 * 4^{-137})^{225} \equiv 79 \bmod 467$

$D * \alpha^{-f2})^{e1} \equiv (426 * 4^{-19})^{47} \equiv 79 \bmod 467$

Hai giá trị đó bằng nhau. Kết luận chữ ký y là *giả mạo*

2). Chữ ký nhóm

Chữ ký nhóm là chữ ký điện tử đại diện cho một nhóm người hay một tổ chức. Các thành viên của một nhóm người được phép ký trên thông điệp với tư cách là người đại diện cho nhóm.

a). Đặc điểm của chữ ký nhóm:

Chỉ có thành viên trong nhóm mới có thể ký tên vào bản thông báo đó.

Người nhận thông điệp có thể kiểm tra xem chữ ký đó có đúng là của nhóm đó hay không, nhưng người nhận không thể biết được người nào trong nhóm đã ký vào thông điệp đó.

Trong trường hợp cần thiết chữ ký nhóm có thể được "mở" (có hoặc không có sự giúp đỡ của thành viên trong nhóm) để xác định người nào đã ký vào thông điệp đó.

b). Một sơ đồ chữ ký nhóm gồm 3 thành phần cơ bản:

• Người quản lý nhóm.

• Các thành viên trong nhóm.

• Người không thuộc nhóm.

c). Một sơ đồ chữ ký nhóm thường bao gồm 5 thủ tục:

KeyGen: Là thuật toán sinh khóa công khai của nhóm, khóa bí mật của người quản lý nhóm : KeyGen() → (pk,gmsk) trong đó pk là khóa công khai của nhóm (dùng để xác minh chữ ký của nhóm), gmsk là khóa bí mật của nhóm. Nếu số người trong nhóm là cố định thì KeyGen()→ (pk,gmsk,sk_i) trong đó sk_i là khóa bí mật của thành viên thứ i trong nhóm

Join : Cho phép một người không phải là thành viên nhóm gia nhập nhóm. Khi gia nhập nhóm, thành viên i sẽ nhận được khóa bí mật của mình là sk_i, người quản lý nhóm sẽ lưu thông tin của thành viên mới này.

Sig : Khi thành viên i muốn ký thông điệp m đại diện cho nhóm, anh ta sẽ sử dụng thủ tục Sig: Sig(m, sk_i)→. Chữ ký trên thông điệp m là δ.

Verify : Khi muốn kiểm tra chữ ký δ có phải là chữ ký đại diện cho nhóm trên thông điệp m sử dụng thủ tục Verify(m, δ,pk) = [False True]

Open : Với mỗi chữ ký trên thông điệp m, người quản lý nhóm có thể xác định được thành viên nào đã ký vào thông điệp bằng việc sử dụng thủ tục Open(gmsk,m, δ), đầu ra của thủ tục là thông tin về thành viên đã ký.

d). Hiệu quả của chữ ký nhóm:

Khi đánh giá hiệu quả của một sơ đồ chữ ký nhóm ta cần quan tâm đến các thông số sau:

• Độ lớn của khóa công khai nhóm γ (số bit)

• Độ lớn của chữ ký trên một thông điệp (số bit)

• Hiệu quả của các thủ tục Setup, Join, Sign, Verify, Open

Tính ưu việt của chữ ký nhóm chính là khả năng cho phép những nhóm người, những tổ chức giao tiếp với nhau, mà trong đó việc xác thực các thông tin gửi cho nhau thông qua các khóa công khai của mỗi nhóm. Nhờ đó các thành viên của nhóm có thể ký nặc danh đại diện cho nhóm của mình mà không thể để lộ thông tin cá nhân của mình, và chỉ có người quản trị mới có thể xác định được người ký.

e). Việc đảm bảo an ninh với chữ ký nhóm:

Không thể giả mạo: Chỉ có các thành viên trong nhóm mới có thể địa diện cho nhóm ký trên thông điệp của nhóm.

Người ký nặc danh có thể tính toán được: Bất kỳ ai cũng có thể xác thực chữ ký một cách dễ dàng nhưng không thể biết được ai là ngời ký (trừ người quản lý nhóm).

Không thể chối bỏ: Một thành viên ký trên một thông điệp thì không thể chối bỏ chữ ký đó được. Người quản lý nhóm có thể xác định được ai đã ký vào thông điệp đó.

Không thể phân tích quan hệ: Việc phân tích xem hai chữ ký của một thành viên trong nhóm khác nhau như thế nào là khó đối với các thành viên của nhóm trừ người quản lý nhóm.

Ngăn chặn framing Attacks: Khi một số thành viên liên kết với nhau cũng không thể gải mạo chữ ký của thành viên khác trong nhóm.

Ngăn chặn sự liên minh: Khi một số thành viên liên kết với nhau cũng không thể tạo ra một chữ ký hợp lệ mà không xác định được người ký.

3). Kỹ thuật trộn phiếu bầu

Khi Bỏ phiếu từ xa, để đảm bảo bí mật, cử tri mã hóa nội dung lá phiếu. Ban KP phải giải mã mới biết được lá phiếu ghi gì. Có thể có một người hay một nhóm người trong Ban KP muốn biết nội dung cũng như tác giả của lá phiếu, điều đó có thể dẫn đến rắc rối cho cử tri sau này. Để tránh tình huống trên người ta dùng kỹ thuật trộn phiếu. Theo kỹ thuật này, danh tính của cử tri không cần phải ẩn đi.

Do trộn các lá phiếu, người ta không thể biết được ai đã bỏ phiếu nào, vì liên kết giữa các cử tri và lá phiếu đã bị xáo trộn.

Quy trình trộn phiếu:

1/. Có n cử tri với n lá phiếu $B_1, B_2, \ldots, B_n$.

2/. Mỗi cử tri mã hóa lá phiếu của mình, đạt được mã hóa ở mức 0 là:

$C_{10}, C_{20}, \ldots, C_{n0}$.

3/. Có t máy trộn $S_1, S_2, \ldots, S_t$.

4/. Máy trộn thứ i với đầu vào $(C_{1(i-1)}, C_{2(i-1)}, \ldots, C_{n(i-1)})$ sẽ hoán vị ngẫu nhiên bí mật thứ tự của chúng, sau đó mã hóa thêm một bước để được $(C_{1i}, C_{2i} \ldots, C_{ni})$.

5/. Bước mã hóa cuối cùng sẽ đạt được $(C_{1t}, C_{2t}, \ldots, C_{nt})$.

6/. Kết quả của mỗi bước được công bố trên bảng niêm yết công khai.

Những vấn đề cần lưu ý khi sử dụng kỹ thuật trộn theo sơ đồ trên:

- Việc mã hóa lá phiếu ở bước 2: Cần có chứng minh không tiết lộ thông tin để chứng minh cho tính hợp lệ của lá phiếu nhằm đảm bảo rằng C_{i0} quả thực là bản mã của B_i ở bước 0.
- Các máy trộn phải đảm bảo tính trung thực, không được tráo đổi các lá phiếu hoặc nhân đúp các lá phiếu. Để thực hiện điều này phải thiết kế các mạng trộn có thể xác minh.

Có 2 kiểu mạng trộn:

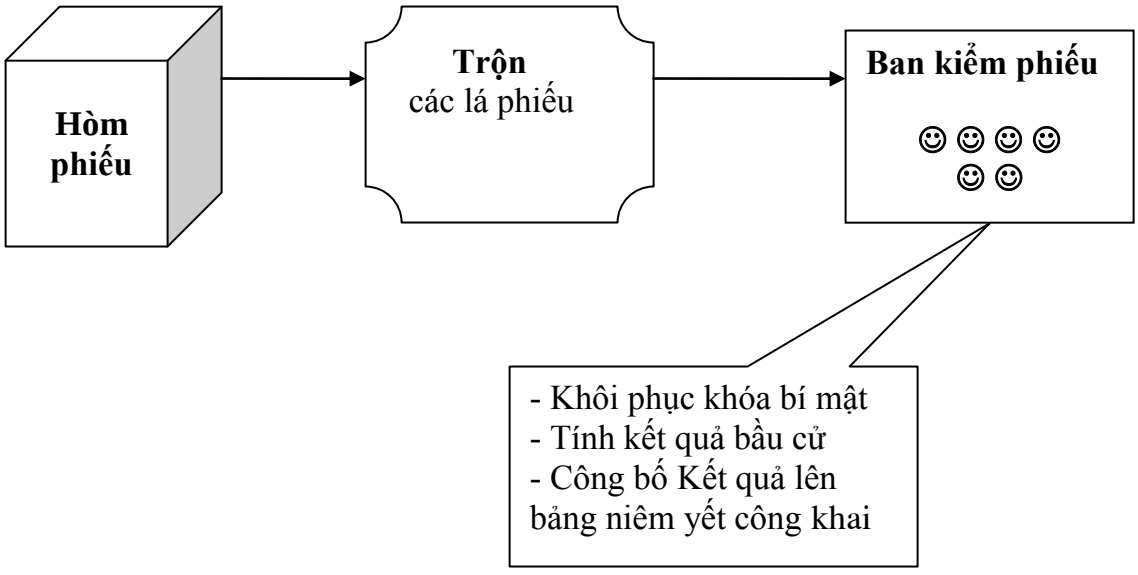
- Mạng trộn giải mã từng bước, mỗi máy trộn sẽ tiến hành giải mã từng bậc một. Đến máy trộn cuối cùng, ta thu được bản rõ, tức nội dung lá phiếu. Mỗi máy trộn S_j có một cặp khóa bí mật, công khai (PK_j, SK_j) và một sơ đồ mã hóa công khai tùy chọn. Vì vậy mỗi bản mã hóa sẽ là:

$C_{i0} = E(PK_1, E(PK_2,\ldots, E(PK_t, B_t)\ldots))$.

Với $E(PK_t, B_t)$ là hàm mã hóa. B_t là lá phiếu của người thứ t.

- Mạng trộn mã hóa sử dụng mã hóa Elgamal.

Sơ đồ giai đoạn kiểm phiếu



Chương 3. VẤN ĐỀ CHIA SẺ KHÓA BÍ MẬT

Kỹ thuật Chia sẻ khóa bí mật (Secret Sharing)

Sơ đồ chia sẻ bí mật không phải là một lĩnh vực mới mẻ của an toàn bảo mật thông tin, nhưng hứa hẹn sẽ mang đến những ứng dụng rộng khắp, quan trọng nhất là ứng dụng bỏ phiếu điện tử.

Sơ đồ chia sẻ bí mật chính là phương thức dùng để chia một bí mật ra làm nhiều phần riêng biệt sau đó phân phối tới những người tham gia. Trong đó chỉ những người được chỉ định trước mới có khả năng khôi phục bí mật bằng cách gộp những phần thông tin của họ, những người không được chỉ định sẽ không thu được bất kỳ thông tin gì về bí mật.

Ý tưởng: thông tin quan trọng cần bí mật, không nên trao cho một người nắm giữ, mà phải chia thông tin đó thành nhiều mảnh và trao cho mỗi người một hay một số mảnh.

Thông tin gốc chỉ có thể được xem lại, khi mọi người giữ các mảnh TT đều nhất trí. Các mảnh TT được khớp lại để được TT gốc.

Yêu cầu: để thực hiện công việc trên, phải sử dụng một sơ đồ gọi là **Sơ đồ chia sẻ bí mật.**

Khái niệm chia sẻ bí mật:

Sơ đồ chia sẻ bí mật dùng để chia sẻ một thông tin cho **m** thành viên, sao cho chỉ những tập con hợp thức các thành viên mới có thể khôi phục lại thông tin bí mật, còn lại không ai có thể làm được điều đó.

Ứng dụng:

- Chia sẻ Thông tin mật thành nhiều mảnh.
- Chia sẻ PassWord, Khoá mật thành nhiều mảnh.

Mỗi nơi, mỗi người hay mỗi máy tính cất giấu 1 mảnh.

Các thành phần của sơ đồ chia sẻ bí mật :

Người phân phối bí mật (Dealer): Là người trực tiếp chia bí mật ra thành nhiều phần.

Những người tham gia nhận dữ liệu từ Dealer (Participant) ký hiệu P

Nhóm có khả năng khôi phục bí mật (Acess structure): Là tập con của P trong đó có các tập con có khả năng khôi phục bí mật.

Các sơ đồ chia sẻ bí mật:

1/. Sơ đồ chia sẻ bí mật sơ khai

Một sơ đồ chia sẻ bí mật đảm bảo tính bảo mật là sơ đồ trong đó bất kỳ người nào có ít hơn t phần dữ liệu (là số lượng đủ để khôi phục bí mật) không có nhiều thông tin hơn một người không có dữ liệu. Xem xét sơ đồ chia sẻ bí mật sơ khai trong đó cụm từ bí mật "password" được chia thành các phần "pa…","ss…","wo…" và "rd…". Một người không có một trong các phần bí mật đó chỉ biết mật khẩu có 8 chữ cái. Anh ta sẽ phải đoán mật khẩu đó từ 226 = 8 tỷ khả năng có thể xảy ra. Một người có một phần trong số 6 phần của mật khẩu đó sẽ phải đoán 6 chữ cái tương đương với 226 khả năng. Hệ thống này không phải là một sơ đồ chia sẻ bí mật bảo mật bởi vì một người tham gia có ít hơn t phần dữ liệu thu được một phần đáng kể thông tin về bí mật.Trong một sơ đồ bảo mật, mặc dù một người tham gia chỉ thiếu một phần dữ liệu cũng có thể sẽ đối mặt với 268 = 208 tỷ khả năng.

2/. Sơ đồ chia sẻ bí mật tầm thường

Có một vài sơ đồ chia sẻ bí mật trong đó yêu cầu tất cả những người tham gia phải cùng nhau khôi phục lại bí mật :

Mã hóa bí mật thành một số nguyên S. Đưa cho mỗi người tham gia i một số ngẫu nhiên r_i (trừ một người).

Đưa cho người cuối cùng một số (S- r_1 - r_2 -…- r_{n-1}).

Bí mật chính là tổng của các số của tất cả những người tham gia vào sơ đồ.

Mã hóa bí mật bằng 1 byte S. Đưa cho mỗi người tham gia i một byte bi (trừ một người), đưa cho người cuối cùng byte (S XOR b_1XOR b_2 …XOR b_{n-1})

3/. Sơ đồ chia sẻ bí mật có ngưỡng giới hạn (Threshold secret sharing schemes)

Mục tiêu của sơ đồ dạng này là chia một ít dữ liệu D ra thành nhiều phần D_1, D_2,…,D_n sao cho :

Nếu biết k hoặc nhiều hơn các phần D_i có thể dễ dàng suy ngược lại D

Nếu biết k-1 hoặc ít hơn các phần D_i không thể suy ngược lại D

Sơ đồ này được gọi là sơ đồ ngưỡng giới hạn (k,n). Nếu k = n thì tất cả mọi thành viên phải cùng nhau mới có thể suy ngược lại bí mật.

Dưới đây là 2 sơ đồ bí mật dạng (k, n)

Sơ đồ chia sẻ bí mật Blakley

Hai đường thẳng không song song nằm trong cùng một mặt phẳng cắt nhau tại một điểm duy nhất. Ba mặt phẳng không song song trong không gian cắt nhau tại một điểm duy nhất. Tổng quát hơn, bất kỳ n mặt siêu phẳng nào cũng cắt nhau tại một điểm cụ thể.

Bí mật có thể được mã hóa là một đơn tọa độ của giao điểm đó. Nếu bí mật được mã hóa bằng cách sử dụng tất cả các tọa độ, mặc dù chúng là ngẫu nhiên, khi đó một người tham gia (ai đó sở hữu một hoặc nhiều các siêu mặt n chiều) thu được thông tin về bí mật do anh ta biết nó nhất định phải nằm trên mặt mà anh ta sở hữu. Nếu một người trong cuộc mà thu được nhiều thông tin hơn một người ngoài cuộc về bí mật, khi đó hệ thống này không còn bảo mật nữa. Nếu chỉ có một trong số các tọa độ được sử dụng, khi đó một người trong cuộc không biết về bí mật hơn một người ngoài cuộc (thí dụ:Bí mật phải nằm trên trục x trong hệ trục tọa đồ Decac). Mỗi người tham gia được đưa đủ thông tin để định nghĩa một siêu mặt; bí mật được khôi phục bằng cách tính toán điểm giao nhau của các mặt và lấy một tọa độ cố định của giao điểm đó.

Sơ đồ của Blakley trong hệ tọa độ không gian 3 chiều: Thông tin của mỗi người tham gia là một mặt phẳng và bí mật chính là giao điểm của 3 mặt phẳng đó. Thông tin của 2 người không đủ để chỉ ra được bí mật mặc dù chúng đã thu hẹp được phạm vi của bí mật là 1 điểm nằm trên giao tuyến của 2 mặt phẳng đã biết. Sơ đồ của Blakley có hiệu quả không gian ít hơn sơ đồ của Shamir dưới đây; trong khi với sơ đồ của Shamir, mỗi một phần chia chỉ lớn bằng bí mật ban đầu. Các phần chia của Blakley lớn hơn t lần, với t là số người tham gia vừa đủ thu được bí mật. Sơ đồ của Blakley có thể được thu gọn bằng cách giới hạn mặt nào có thể sử dụng làm phần chia.
Kết quả thu được sẽ là một sơ đồ tương đương với sơ đồ của Shamir.

Sơ đồ ngưỡng Shamir

Ý tưởng về sơ đồ ngưỡng giới hạn của Shamir dựa trên tính chất: Hai điểm có thể định nghĩa một đường thẳng, 3 điểm định nghĩa được 1 parabol, 4 điểm định nghĩa được một hình lập phương, cứ như thế một cách tổng quát cần n+1 điểm để định nghĩa một đa thức bậc n.

Sơ đồ chia sẻ ngưỡng A(t, m)

Cho t, m nguyên dương, **t ≤ m.** Sơ đồ ngưỡng A (t, m) là *Phương pháp phân chia bí mật K* cho một tập gồm m thành viên, sao cho t thành viên bất kỳ có thể tính được K, nhưng không một nhóm gồm (t-1) thành viên nào có thể làm được điều đó. Người phân chia các mảnh khóa không được nằm trong số m thành viên trên.

Ví dụ : có m = 3 thủ quỹ giữ két bạc. Hãy xây dựng hệ thống sao cho bất kì t = 2 thủ quỹ nào cũng có thể mở được két bạc, nhưng từng người một riêng rẽ thì không thể. Đó là sơ đồ ngưỡng A (2,3).

Sơ đồ ngưỡng Shamir 1979 :

Bài toán:

Chia khóa bí mật K trong Z_p thành t mảnh, phân cho mỗi người giữ 1 mảnh, t ≤ m

T thành viên "khớp t mảnh" sẽ nhận được K

Khởi tạo: Chọn số nguyên tố p.

1. D chọn m phần tử x_i khác nhau, $\neq 0$ trong Z_p,

   $1 \leq i \leq m$ (yêu cầu: m < p,Tl: x_i khác nhau, $\neq 0$ trong Z_p).

   D trao x_i cho thành viên P_i . Giá trị x_i là công khai.

Phân phối mảnh khoá $K \in Z_p$

2. D chọn bí mật (ngẫu nhiên,độc lập) t-1 phần tử $\in Z_p$

   là $a_1, \ldots, a_{t-1}$.

3. Với $1 \leq i \leq m$, D tính: $y_i = P(x_i)$,

   $P(x) = \mathbf{K} + \sum_{j=1}^{t-1} a_j x^j \bmod p$

4. Với $1 \leq i \leq m$, D sẽ trao mảnh y_i cho P_i .

Khôi phục khoá K từ t thành viên

Giải hệ phương trình tuyến tính t ẩn, t phương trình

Vì P(x) có bậc lớn nhất là (t-1) nên ta có thể viết:

$P(x) = K + a_1 x^1 + a_2 x^2 + \ldots + a_{t-1} x^{t-1}$

Các hệ số K, $a_1, \ldots, a_{t-1}$ là các phần tử chưa biết của Z_p, $a_0 = K$ là khoá.

Vì $y_{ij} = P(x_{ij})$, nên có thể thu được t phương trình tuyến tính t ẩn $a_0, a_1, \ldots, a_{t-1}$,

Nếu các phương trình độc lập tuyến tính thì sẽ có một nghiệm duy nhất và ta được giá trị khoá $a_0 = K$.

Chú ý: các phép tính số học đều thực hiện trên Z_p.

Ví dụ:

Chia mảnh khóa K

Khoá K = 13 cần chia thành 3 mảnh cho 3 người P1, P3, P5.

1. Chọn số nguyên tố p =17, chọn m = 5 phần tử $\mathbf{x_i = i}$

   trong Z_p , i =1, 2, 3, 4, 5.

   D trao giá trị công khai $\mathbf{x_i}$ cho P_i .

2. D chọn bí mật, ngẫu nhiên t -1 = 2 phần tử trong Z_p

   a_1 =10, a_2 = 2.

3. D tính $\mathbf{y_i} = P(\mathbf{x_i})$, $1 \le i \le m$, trong đó:

   $P(x)=K + \sum^{t-1}_{j=1} a_j x_j^{\ j} \pmod p = 13 + a_1 x + a_2 x^2 \pmod{17}$.

   $y_1 = P(x_1) = P(1) = 13 + a_1.1 + a_2.1^2 \pmod{17} = 13 + 10.1 + 2 .1^2 \pmod{17} = 8$

   $y_3 = P(x_3) = P(3) = 13 + a_1.3 + a_2.3^2 \pmod{17} = 13 + 10.3 + 2 .3^2 \pmod{17} = 10$

   $y_5 = P(x_5) = P(5) = 13 + a_1.5 + a_2.5^2 \pmod{17} = 13 + 10.5 + 2 .5^2 \pmod{17} = 11$

4. D trao mảnh $\mathbf{y_i}$ cho P_i .

Khôi phục khoá K

B ={P1, P3, P5} cần kết hợp các mảnh khóa của họ:

y_1 =8, y_3 = 10, y_5 = 11, để khôi phục lại khóa K.

Theo sơ đồ khôi phục khóa K, $\mathbf{y_{ij} = P(x_{ij})}$, $1 \le j \le t$.

Thay $x_1 = 1$, $x_3 = 3$, $x_5 = 5$ vào

$P(x) = a_0 + a_1 x + a_2 x^2 \pmod{17}$, $a_0 = K$.

ta nhận được 3 phương trình với 3 ẩn số a_0 , a_1, a_2.

$y_1 = P(x_1) = P(1) = a_0 + a_1.1 + a_2.1^2 = 8 \pmod{17}$.

$y_3 = P(x_3) = P(3) = a_0 + a_1.3 + a_2.3^2 = 10 \pmod{17}$.

$y_5 = P(x_5) = P(5) = a_0 + a_1.5 + a_2.5^2 = 11 \pmod{17}$.

Giải hệ 3 phương trình tuyến tính trong Z_{17}, nghiệm duy nhất là:

a_0 =13, a_1=10, a_2=2.

Khoá được khôi phục là: K= a_0 =13.

Ứng dụng

Trong việc giữ khóa két bạc:

Không nên trao khoá két bạc cho một người duy nhất.

Khoá phải được chia nhỏ thành nhiều mảnh và trao cho mỗi thành viên một mảnh.

Trong bỏ phiếu điện tử:

Không thể tin hoàn toàn vào tất cả các thành viên Ban kiểm phiếu.

Vì vậy, lá phiếu nên chia thành nhiều mảnh và trao cho mỗi Kiểm phiếu viên một mảnh của lá phiếu.

Trong lưu trữ các khóa bí mật:

Khoá bí mật và quan trọng không nên lưu trữ tại một Server. Nó phải được chia nhỏ và lưu trữ tại nhiều máy trạm.

KẾT LUẬN:

Đồ án tốt nghiệp đã thực hiện được những nội dung chính sau:

1. Tìm hiểu một số phương pháp bảo vệ thông tin:
   - Mã hóa dữ liệu
   - Chữ ký số
   - Hạ tầng mật mã khóa công khai (PKI)
2. Tìm hiểu một số bài toán về an toàn thông tin
   trong giai đoạn kiểm phiếu điện tử.
3. Tìm hiểu về vấn đề "Chia sẻ bí mật".

DANH MỤC TÀI LIỆU THAM KHẢO

Tiếng Việt.

1. GS Phan Đình Diệu, *Giáo trình Lý thuyết Mật Mã & An toàn thông tin*, NXB Đại học quốc gia Hà nội 2006.
2. PGS.TS Trịnh Nhật Tiến, *Giáo trình An toàn dữ liệu*, 2008.
3. PGS.TS Trịnh Nhật Tiến, ThS. Trương thị Thu Hiền, *"Mã hóa đồng cấu và ứng dụng"*, ĐHQG Hà Nội, 10/2003.
4. http://www.vi.wikipedia.org/wiki/Chữ_ký_số
   http://www.vi.wikipedia.org/wiki/Mã_hóa

Tiếng Anh.

1. Zuzana Rjaskova, *Electronic Voting Schemes*, 2002.
2. Adi Shamir, "How to share a secret", Communications of the ACM, 1979.