BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC DÂN LẬP HẢI PHÒNG
-------o0o-------

ĐỒ ÁN TỐT NGHIỆP

NGÀNH CÔNG NGHỆ THÔNG TIN

HẢI PHÒNG 2013

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC DÂN LẬP HẢI PHÒNG

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

VẤN ĐỀ CHIA SẺ BÍ MẬT VÀ ỨNG DỤNG TRONG BỎ PHIẾU ĐIỆN TỬ

ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC HỆ CHÍNH QUY

Ngành: CôngnghệThông tin

HẢI PHÒNG - 2013

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC DÂN LẬP HẢI PHÒNG

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

VẤN ĐỀ CHIA SẺ BÍ MẬT VÀ ỨNG DỤNG TRONG BỎ PHIẾU ĐIỆN TỬ

ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC HỆ CHÍNH QUY

Ngành: CôngnghệThông tin

Sinhviênthựchiện: BÙI VĂN TIẾN
Giáoviênhướngdẫn: PGS. TS TRỊNH NHẬT TIẾN
Mãsốsinhviên: 1351010003

HẢI PHÒNG - 2013

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC DÂN LẬP HẢI PHÒNG

CỘNG HÒA XA HỘI CHỦ NGHĨA VIỆT NAM
Độclập - Tự do - Hạnhphúc

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

NHIỆM VỤ THIẾT KẾ TỐT NGHIỆP

Sinhviên: BÙI VĂN TIẾNMã SV: 1351010003

Lớp: CT1301Ngành: CôngnghệThông tin

Tênđềtài:

VẤN ĐỀ CHIA SẺ BÍ MẬT
VÀ ỨNG DỤNG TRONG BỎ PHIẾU ĐIỆN TỬ

NHIỆM VỤ ĐỀ TÀI

1. Nội dung vàcácyêucầucầngiảiquyếttrongnhiệmvụđềtàitốtnghiệp

a. Nội dung

- Tìmhiểunghiêncứuvề Vấnđề Chia sẻBímật.
- Tìmhiểumộtsốbàitoán Antoànthông tin trongBỏphiếuđiệntử.
- ỨngdụngVấnđề chia sẻbímậttrongmộtsốbàitoántrên.

b. Cácyêucầucầngiảiquyết

- Tìmhiểuvàtrìnhbày 3 nội dung trên.
- Thửnghiệmítnhất 1 chươngtrìnhđểgiảiquyếtmộtbàitoán.

CÁN BỘ HƯỚNG DẪN ĐỀ TÀI TỐT NGHIỆP

Ngườihướngdẫnthứnhất:

Họvàtên:TrịnhNhậtTiến

Họchàm, họcvị: PhóGiáoSư, TiếnSĩ

Cơquancôngtác: TrườngĐạiHọcCôngNghệ, ĐạiHọcQuốcGiaHàNội

Nội dung hướngdẫn:

- TìmhiểunghiêncứuvềVấnđề Chia sẻBímật.
- TìmhiểumộtsốbàitoánAntoànthông tin trongBỏphiếuđiệntử.
- ỨngdụngVấnđề chia sẻbímậttrongmộtsốbàitoántrên.

Ngườihướngdẫnthứhai:

Họvàtên: …….

Họchàm, họcvị: …….

Cơquancôngtác: ……

Nội dung hướngdẫn: ……..

……

……

……

……

……...

Đềtàitốtnghiệpđượcgiaongàythángnăm 2013

Yêucầuphảihoànthànhtrướcngàythángnăm 2013

Đãnhậnnhiệmvụ: Đ.T.T.N	Đãnhậnnhiệmvụ: Đ.T.T.N
Sinhviên	Cánbộhướngdẫn Đ.T.T.N

PGS. TS TrịnhNhậtTiến

HảiPhòng, ngày .....tháng.....năm 2013

HIỆU TRƯỞNG

GS.TS.NGƯT TrầnHữuNghị

PHẦN NHẬN XÉT TÓM TẮT CỦA CÁN BỘ HƯỚNG DẪN

1. Tinhthầnthái độcủasinhviêntrongquátrìnhlàmđềtàitốtnghiệp:

.....
....
.....
....
.....
....
.....
....
.....
.....
.....
.....

2. Đánhgiáchấtlượngcủađềtàitốtnghiệp (so vớinội dung yêucầuđãđềratrongnhiệmvụđềtàitốtnghiệp)

.....
.....
.....
.....
.....
.....
.....
.....

3. Cho điểmcủacánbộhướngdẫn:

(Điểmghibằngsốvàchữ)

.....

.....

.....

Ngày.....tháng.....năm 2013

Cánbộhướngdẫnchính

(Ký, ghirõhọtên)

PHẦN NHẬN XÉT ĐÁNH GIÁ CỦA CÁN BỘ CHẤM PHẢN BIỆN ĐỀ TÀI TỐT NGHIỆP

1. Đánhgiáchấtlượngđềtàitốtnghiệp (vềcácmặtnhưcơsởlýluận, thuyết minh chươngtrình, giátrịthựctế, ...)

2. Cho điểmcủacánbộphảnbiện

(*Điểmghibằngsốvàchữ*)

.....

.....

.....

Ngày.....tháng.....năm 2013

Cánbộchấmphảnbiện

(Ký, ghirõhọtên)

MỤC LỤC

LỜI CẢM ƠN

Trước hết em xin được bày tỏ sự trân trọng và lòng biết ơn đối với thầy giáo PGS.TS. Trịnh Nhật Tiến - Khoa Công nghệ thông tin trường Đại học Công Nghệ, Đại học Quốc Gia Hà Nội. Trong suốt quá trình làm đồ án tốt nghiệp của em, thầy đã dành rất nhiều thời gian quí báu để tận tình chỉ bảo, hướng dẫn và định hướng cho em h đồ án tốttrong việc nghiên cứu và hoàn thàn nghiệp.

Em cũng xin cảm ơn các Thầy giáo, Cô giáo trong khoa Công nghệ thông tin – Trường Đại học dân lập Hải Phòng đã giúp đỡ, tạo điều kiện thuận lợi cho em trong suốt khóa học tại trường. Sự đóng góp quý báu của các Thầy Cô đã giúp cho em hoàn thành tốt đồ án tốt nghiệp.

LỜI MỞ ĐẦU

Trong suốt nhiều thế kỉ qua trên thế giới, các cuộc bầu cử đã giữ một vai trò quan trọng trong việc xác lập thể chế chính trị của các quốc gia.

Và trong xu hướng phát triển của khoa học công nghệ ngày nay, công nghệ thông tin đã ngày càng phổ biến và được áp dụng trong mọi lĩnh vực đời sống. Các cuộc bầu cử cũng không phải là ngoại lệ. Người ta đã bỏ rất nhiều công sức để nghiên cứu cải tiến các phương thức bầu cử để nó ngày càng trở nên tốt và tiện lợi hơn. Các phương thức thay đổi theo từng thời kỳ, theo sự tiến bộ của xã hội. Và với sự tiến bộ của xã hội ngày nay thì các dự án chính phủ điện tử để giúp nhà nước điều hành đất nước là một điều tất yếu, kèm theo đó thì sự phát triển của bỏ phiếu điện tử để thay thế cho bỏ phiếu thông thường là điều sẽ diễn ra trong tương lai.

Nắm được tầm quan trọng và tính tất yếu của bỏ phiếu điện tử, các nước, các tổ chức đã và đang xây dựng giải pháp cho bỏ phiếu điện tử.

Trong phạm vi của Đồ án tốt nghiệp này, để cho tập trung, Tôi sẽ trình bày vấn đề chia sẻ bí mật chủ yếu trong giai đoạn Đăng ký bỏ phiếu điện tử.

DANH MỤC HÌNH VẼ

DANH MỤC CÁC TỪ VIẾT TẮT

Các từ viết tắt	Viết đầy đủ
RSA	Tên 3 nhà khoa học: Ron Rivest, Adi Shamir, Leonard Adleman.
DES	Data Encryption Standard
ĐH	Ban điều hành
ĐK	Ban đăng ký
KP	Ban kiểm phiếu
CT	Cử tri
KT	Ban kiểm tra
ƯCLN	Ước chung lớn nhất
BCNN	Bội chung nhỏ nhất

Chương 1. MỘT SỐ KHÁI NIỆM CƠ BẢN

1.1. TỔNG QUAN VỀ AN TOÀN THÔNG TIN

1.1.1. An toàn thông tin

Khi nhu cầu trao đổi thông tin dữ liệu ngày càng lớn và đa dạng, các tiến bộ về điện tử - viễn thông và công nghệ thông tin không ngừng được phát triển ứng dụng để nâng cao chất lượng và lưu lượng truyền tin thì các quan niệm ý tưởng và biện pháp bảo vệ thông tin cũng đươc đổi mới. Bảo vệ an toàn thông tin là 1 chủ đề rộng, có liên quan đến nhiều lĩnh vực, trong thực tế có nhiều phương pháp đươc thực hiện để bảo vệ an toàn thông tin. Các phương pháp bảo vệ an toàn thông tin có thể được quy tụ vào ba nhóm sau:

- Bảo vệ an toàn thông tin bằng các biện pháp hành chính.
- Bảo vệ an toàn thông tin bằng các biện pháp kỹ thuật (phần cứng).
- Bảo vệ an toàn thông tin bằng các biện pháp thuật toán (phần mềm).

Ba nhóm trên có thể được ứng dung riêng rẽ hoặc phối kết hợp. Môi trường khó bảo vệ an toàn thông tin nhất cũng là môi trường đối phương dễ xâm nhập nhất đó là môi trường mạng và truyền tin. Biện pháp hiệu quả nhất và kinh tế nhất hiện nay trên mạng truyền tin và mạng máy tính là biện pháp thuật toán.

1.1.2. Nội dung của an toàn thông tin

An toàn thông tin bao gồm các nội dung sau:

1). Bảo mật : Tính kín đáo riêng tư của thông tin.

2). Bảo toàn : Bảo vệ thông tin không cho phép sửa đổi thông tin trái phép.

3). Xác thực : Xác thực đối tác, xác thực thông tin trao đổi, đảm bảo người gửi thông tin không thể thoái thác về trách nhiệm thông tin mình đã gửi.

4). Sẵn sàng : Luôn sẵn sàng thông tin cho người dùng hợp pháp.

Để đảm bảo thông tin trên đường truyền tin và trên mạng máy tính có hiệu quả, thì điều trước tiên là phải lường trước hoặc dự đoán trước các khả năng không an toàn, khả năng xâm phạm, các sự cố rủi ro có thể xảy ra đối với thông tin được lưu trữ và trao đổi trên đường truyền tin cũng như trên mạng. Xác định càng chính xác các nguy cơ nói trên thì càng quyết định được tốt các giải pháp để giảm thiểu các thiệt hại.

1.1.3. Hai loại hành vi xâm phạm an toàn thông tin

Có hai loại hành vi xâm phạm thông tin dữ liệu đó là: vi phạm thụ động và vi phạm chủ động.

Vi phạm thụ động chỉ nhằm mục đích cuối cùng là nắm bắt được thông tin (đánh cắp thông tin). Việc làm đó khi không biết được nội dung cụ thể nhưng có thể dò ra được người gửi, người nhận nhờ thông tin điều khiển giao thức chứa trong phần đầu các gói tin. Kẻ xâm nhập có thể kiểm tra được số lượng, độ dài và tần số trao đổi. Vì vậy vi phạm thụ động không làm sai lệch hoặc hủy hoại nội dung thông tin dữ liệu được trao đổi. Vi phạm thụ động thường khó phát hiện nhưng có thể có những biện pháp ngăn chặn hiệu quả.

Vi phạm thụ động là dạng vi phạm có thể làm thay đổi nội dung, xóa bỏ, xắp xếp lại thứ tự hoặc làm lặp lại gói tin tại thời điểm đó hoặc sau đó một thời gian. Vi phạm chủ động có thể thêm vào một số thông tin ngoại lai để làm sai lệch nội dung thông tin trao đổi. Vi phạm chủ động dễ phát hiện nhưng để ngăn chặn hiệu quả thì khó khăn hơn nhiều.

Có một thực tế là không có một biện pháp nào bảo vệ an toàn thông tin dữ liệu nào là an toàn tuyệt đối. Một hệ thống dù được bảo vệ chắc chắn đến đâu cũng không thể đảm bảo là an toàn tuyệt đối.

1.1.4. Các chiến lược an toàn hệ thống

1). Giới hạn quyền hạn tối thiểu

Đây là chiến lược cơ bản nhất theo nguyên tắc này bất kì mội đối tượng nào cũng chỉ có những quyền hạn nhất định đối với tài nguyên mạng, khi thâm nhập vào mạng đối tượng đó chỉ được sử dụng một số tài nguyên nhất định.

2). Bảo vệ theo chiều sâu

Nguyên tắc này nhắc nhở chúng ta: Không nên dựa vào mội chế độ an toàn nào dù cho chúng rất mạnh, mà nên tạo nhiều cơ chế an toàn để hỗ trợ lẫn nhau.

3). Nút thắt

Tạo ra một "cửa khẩu" hẹp, và chỉ cho phép thông tin đi vào hệ thống của mình bằng con đường duy nhất chính là "cửa khẩu" này => phải tổ chức một cơ cấu kiểm soát và điều khiển thông tin đi qua cửa này.

4). Điểm nối yếu nhất

Chiến lược này dựa trên nguyên tắc: "Một dây xích chỉ chắc tại mắt duy nhất, một bức tường chỉ cứng tại điểm yếu nhất".

Kẻ phá hoại thường tìm chỗ yếu nhất của hệ thống để tấng công, do đó ta cần phải gia cố các yếu điểm của hệ thống. Thông thường chúng ta chỉ quan tâm đến kẻ tấn công trên mạng hơn là kẻ tiếp cận hệ thống của chúng ta.

5). Tính toàn cục

Các hệ thống an toàn đòi hỏi phải có tính toàn cục của các hệ thống cục bộ. Nếu có một kẻ nào đó có thể bẻ gãy một cơ chế an toàn thì chúng có thể thành công bằng cách tấn công hệ thống tự do của ai đó và sau đó tấn công hệ thống từ nội bộ bên trong.

6). Tính đa dạng bảo vệ

Cần phải sử dụng nhiều biện pháp bảo vệ khác nhau cho hệ thống khác nhau, nếu không có kẻ tấn công vào được một hệ thống, thì chúng cũng dễ dàng tấn công vào các hệ thống khác.

1.1.5. Các mức bảo vệ trên mạng

Vì không thể có một giải pháp an toàn tuyệt đối nên người ta thường phải sử dụng đồng thời nhiều mức bảo vệ khác nhau tạo thành nhiều hàng rào chắn đối với các hoạt động xâm phạm. Việc bảo vệ thông tin trên mạng chủ yếu là bảo vệ thông tin cất giữ trong máy tính, đặc biệt là các server trên mạng. Bởi thế ngoài một số biện pháp nhằm chống thất thoát thông tin trên đường truyền mọi cố gắng tập trung vào việc xây dựng các mức rào chắn từ ngoài vào trong cho các hệ thống kết nối mạng. Thông thường bao gồm các mức bảo vệ sau:

1). Quyền truy nhập

Lớp bảo vệ trong cùng là quyền truy nhập nhằm kiểm soát các tài nguyên của mạng và quyền hạn trên tài nguyên đó. Dĩ nhiên là kiểm soát được các cấu trúc dữ liệu càng chi tiết càng tốt. Hiện tại việc kiểm soát thường ở mức tệp.

2). Đăng kí tên, mật khẩu

Thực ra đây cũng là kiểm soát quyền truy nhập, nhưng không phải truy nhập ở mức thông tin mà ở mức hệ thống. Đây là phương pháp bảo vệ phổ biến nhất vì nó đơn giản ít phí tổn và cũng rất hiệu quả. Mỗi người sử dụng muốn được tham gia vào mạng để sử dụng tài nguyên đều phải có đăng kí tên và mật khẩu trước. Người quản trị mạng có trách nhiệm quản lý, kiểm soát mọi hoạt động của mạng và xác định quyền truy nhập của những người sử dụng khác theo thời gian và không gian(nghĩa là người sử dụng chỉ được truy nhập trong một khoảng thời gian nào đó tại mỗi vị trí nhất định nào đó).

Về lý thuyết nếu mọi người đều giữ kín được mật khẩu và tên đăng ký của mình thì sẽ không xảy ra các truy nhập trái phép. Song điều đó khó đảm bảo trong thực tế vì nhiều nguyên nhân rất đời thường làm giảm hiệu quả của lớp bảo vệ này. Có thể khắc phục bằng cách người quản trị mạng chịu trách nhiệm đặt mật khẩu hoặc thay đổi mật khẩu theo thời gian.

3). Mã hóa dữ liệu

Để bảo mật thông tin trên đường truyền người ta sử dụng các phương pháp mã hóa. Dữ liệu bị biến đổi từ dạng nhận thức được sang dạng không nhận thức được theo một thuật toán nào đó và sẽ được biến đổi ngược lại ở trạm nhận (giải mã). Đây là lớp bảo vệ thông tin rất quan trọng.

4). Bảo vệ vật lý

Ngăn cản các truy nhập vật lý vào hệ thống. Thường dùng các biện pháp truyền thống như ngăn cấm tuyệt đối người không phận sự vào phòng đặt máy mạng, dùng ổ khóa trên máy tính hoặc các máy trạm không có ổ mềm.

5). Tường lửa

Ngăn chặn xâm nhập trái phép và lọc bỏ các gói tin không muốn gửi hoặc nhận vì các lý do nào đó để bảo vệ một máy tính hoặc cả nội bộ (intranet).

6). Quản trị mạng

Trong thời đại phát triển của công nghệ thông tin, mạng máy tính quyết định toàn bộ hoạt động của cơ quan, hay một công ty xí nghiệp. Vì vậy việc bảo đảm cho hệ thống mạng máy tính hoạt động một cách an toàn, không xảy ra sự cố là một công việc cấp thiết hàng đầu. Công tác quản trị mạng máy tính được thực hiện một cách khoa học đảm vào các yêu cầu sau:

- Toàn bộ hệ thống hoạt động bình thường trong giờ làm việc.
- Có hệ thống dự phòng khi có sự cố về phần cứng hoặc phần mềm xảy ra.
- Sao lưu dữ liệu quan trọng theo định kỳ.
- Bảo dưỡng mạng theo định kỳ.
- Bảo mật dữ liệu, phân quyền truy cập, tổ chức nhóm làm việc trên mạng

1.1.6. An toàn thông tin bằng mã hóa

Để bảo vệ thông tin trên đường truyền người ta thường biến đổi nó từ dạng nhận thức được sang dạng không nhận thức được trước khi truyền trên mạng, quá trình này gọi được gọi là mã hóa thông tin (encryption). Ở trạm nhận phải thực hiện quá trình ngược lại, tức là biến đổi thông tin từ dạng không nhận thức được (dữ liệu đã được mà hóa) về dạng nhận thức được (dạng gốc), quá trình này gọi là giải mã.

Đây là một lớp bảo vệ thông tin rất quan trọng và được sủ dụng rộng rãi trong môi trường mạng. Để bảo vệ thông tin bằng mã hóa người ta thường tiếp cận theo hai hướng:

- Theo đường truyền (Link_Oriented_Security)
- Từ nút đến nút (End_to_End)

Theo cách thứ nhất, thông tin được mã hóa để bảo vệ trên đường truyền giữa hai nút mà không quan tâm đến nguồn và đích của thông tin đó. Ở đây ta lưu ý rằng thông tin chỉ được bảo vệ trên đường truyền, tức là ở mỗi nút đều có quá trình giải mã sau đó mã hóa để truyền đi tiếp, do đó các nút cần phải được bảo vệ tốt.

Theo cách thứ hai, thông tin trên mạng được bảo vệ trên toàn đường truyền từ nguồn đến đích. Thông tin sẽ được mã hóa ngay sau khi mới tạo ra và chỉ được giải mã khi về đến đích. Cách này mắc phải nhược điểm là chỉ có dữ liệu của người dùng thì mới có thể mã hóa được, còn dữ liệu điều khiển thì giữ nguyên để có thể xử lý tại các nút.

1.2. MỘT SỐ KHÁI NIỆM TOÁN HỌC

1.2.1. Ước chung lớn nhất, bội chung nhỏ nhất

1.2.1.1. Ước số và bội số

Cho hai số nguyên a và b, b ≠ 0. Nếu có một số nguyên q sao cho a = b*q, thì ta nói rằng a ***chia hết*** cho b, kí hiệu b\a. Ta nói b là ước của a, và a là bội của b.

Ví dụ:

Cho a = 6, b = 2, ta có 6 = 2*3, ký hiệu 2\6. Ở đây 2 là ước của 6 và 6 là bội của 2.

Cho các số nguyên a, b ≠ 0, tồn tại cặp số nguyên (q, r) (0≤ r ≤ /b/) duy nhất sao cho **a = b*q + r.** Khi đó q gọi là ***thương nguyên*****, r** gọi là *số dư* của phép chia a cho b. Nếu r = 0 thì ta có phép chia hết.

***Ví dụ*:**

Cho a = 13, b = 5, ta có 12 = 5*2 + 3. Ở đây thương q=2, số dư là r = 3.

1.2.1.2. Ước chung lớn nhất, bội chung nhỏ nhất.

Số nguyên d được gọi là *ước chung* của các số nguyên $a_1, a_2,\ldots,a_n$, nếu nó là *ước* của tất cả các số đó.

Số nguyên m được gọi là *bội chung* của các số nguyên $a_1, a_2,\ldots,a_n$, nếu nó là *bội* của tất cả các số đó.

Một ước chung d >0 của các số nguyên $a_1, a_2,\ldots,a_n$, trong đó mọi ước chung của $a_1, a_2,\ldots,a_n$, đều là ước của d, thì d được gọi là *ước chung lớn nhất* (UCLN) của $a_1, a_2,\ldots,a_n$. Ký hiệu d = gcd($a_1, a_2,\ldots,a_n$) hay d = UCLN($a_1, a_2,\ldots,a_n$). Nếu gcd($a_1, a_2,\ldots,a_n$) = 1, thì các số $a_1, a_2,\ldots,a_n$ được gọi là *nguyên tố cùng nhau.*

Một bội chung m >0 của các số nguyên $a_1, a_2,\ldots,a_n$, trong đó mọi bội chung của $a_1, a_2,\ldots,a_n$ đều là bội của m, thì m được gọi là *bội chung nhỏ nhất* (BCNN) của $a_1, a_2,\ldots,a_n$. Ký hiệu m = lcm($a_1, a_2,\ldots,a_n$) hay m = BCNN($a_1, a_2,\ldots,a_n$).

Ví dụ:

Cho a =12, b=15, gcd(12,15) = 3, lcm(12,15) = 60.

Hai số 8 và 13 là *nguyên tố cùng nhau*, vì gcd(8, 13) =1.

Ký hiệu :

Z_n = {0, 1, 2, … , n-1} là tập các số nguyên không âm < n.

Z_n^* = {e ∈ Z_n , e là nguyên tố cùng nhau với n}. Tức là e # 0.

1.2.2. Quan hệ " Đồng dư "

1.2.2.1. Khái niệm

Cho các số nguyên a, b, m (m >0). Ta nói rằng a và b ***"đồng dư" với nhau*** theo modulo m, nếu chia a và b cho m, ta nhận được cùng một số dư.

Ký hiệu : a ≡ b(mod m).

Ví dụ :

17 ≡ 5 (mod 3) vì 17 và 5 chia cho 3 được cùng số dư là 2.

1.2.2.2. Các tính chất của quan hệ "Đồng dư"

1). Quan hệ "đồng dư" là quan hệ tương đương trong Z.

Với mọi số nguyên dương m ta có :

a ≡ a (mod m) với mọi a ∈ Z;

a ≡ b (mod m) thì b ≡ a (mod m);

a ≡ b (mod m) và b ≡ c (mod m) thì a ≡ c (mod m);

2). Tổng hay hiệu các "đồng dư" :

(a + b) (mod n) = [(a mod n) + (b mod n)] (mod n)

(a - b) (mod n) = [(a mod n) - (b mod n)] (mod n)

3). Tích các "đồng dư":

(a * b) (mod n) = [(a mod n) * (b mod n)] (mod n)

1.2.3. Số nguyên tố

1.2.3.1. Khái niệm

Số nguyên tố là số tự nhiên lớn hơn 1 và chỉ có hai ước là 1 và chính nó.

Ví dụ :

Các số 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31 là các số nguyên tố.

1.2.3.2. Định lý về số nguyên tố

1). Định lý : Về số nguyên dương > 1.

Mọi số nguyên dương n >1 đều có thể biểu diễn được *duy nhất* dưới dạng :

$n=P_1^{n_1}. P_1^{n_2} \dots P_1^{n_k}$, trong đó :

k,n_i (i = 1,2,…,k) là các số tự nhiên, P_i là các số nguyên tố, từng đội một khác nhau.

2). Định lý : Mersenne.

Cho $p = 2^k -1$, nếu p là số nguyên tố, thì k phải là số nguyên tố.

3). Hàm Euler.

Cho số nguyên dương n, số lượng các số nguyên dương bé hơn n và *nguyên tố cùng nhau* với n được ký hiệu ø(n) và gọi là hàm *Euler.*

Nhận xét : Nếu p là số nguyên tố, thì ø(p) = p-1.

Định lý về Hàm Euler : Nếu n là tích của hai số nguyên tố n = p.q, thì

$$ø(n) = ø(p). ø(q) = (p-1)(q-1)$$

1.2.4. Khái niệm nhóm, nhóm con, nhóm Cyclic

a) Nhóm là bộ các phần tử (G, *) thỏa mãn các tính chất sau:

+ Tính chất kết hợp: (x * y) * z = x * (y * z)

+ Tính chất tồn tại phần tử trung gian e ∈ G: e * x = x * e = x, ∀x ∈ G

+ Tính chất tồn tại phần tử nghịch đảo x’ ∈ G: x’ * x = x * x’ = e

b) Nhóm con của G là tập S ⊂ G, S≠ ø, và thỏa mãn các tính chất sau:

+ Phần tử trung lập e của G nằm trong S.

+ S khép kín đối với phép tính (*) trong, tức là x * y ∈ S với mọi x, y ∈ S.

+ S khép kín đối với phép lấy nghịch đảo trong G, tức x^{-1}∈ S với mọi x∈ S.

c) Nhóm cyclic:

(G, *) là nhóm được sinh ra bởi một trong các phần tử của nó. Tức là có phần tử g ∈ G mà với mỗi a ∈ G, đều tồn tại số n ∈ N để g^n = a. Khi đó g là phần tử sinh hay phần tử nguyên thủy của nhóm G.

Ví dụ:

(Z^+, *) gồm các số nguyên dương là một nhóm cyclic có phần tử sinh là 1.

1.2.5. Phần tử nghịch đảo

1). Khái niệm.

Cho a ∈ Z_n. Nếu tồn tại b ∈ Z_n sao cho a b ≡ 1 (mod n), ta nói b là phần tử nghịch đảo của a trong Z_n và ký hiệu a^{-1}. Một phần tử có phần tử nghịch đảo, gọi là khả nghịch.

2). Tính chất :

+ Cho a, b ∈ Z_n. Phép chia của a cho b theo modulo n là tích của a và b^{-1} theo modulo n và chỉ được xác định khi b khả nghịch theo modulo n.

+ Cho a ∈ Z_n, a khả nghịch khi và chỉ khi UCLN(a, n) = 1.

+ Giả sử d = UCLN (a, n). Phương trình đồng dư ax ≡ b mod n có nghiệm x nếu và chỉ nếu d chia hết cho b, trong trường hợp các nghiệm d nằm trong khoảng [0, n-1] thì các nghiệm đồng dư theo modulo $\frac{n}{d}$.

Ví dụ:

4^{-1}= 7 mod 9 vì 4 . 7 ≡ 1 mod 9

1.2.6. Các phép tính cơ bản trong không gian modulo

Cho n là số nguyên dương. Các phần tử trong Z_n được thể hiện bởi các số nguyên {0, 1, 2, ..., n-1}. Nếu a, b ∈ Z_n thì:

$$(a + b) \bmod n = \begin{cases} a + b \; nu \;\; a + b < n \\ a + b - n \; nu \; a + b \geq n \end{cases}$$

Vì vậy, phép cộng modulo (và phép trừ modulo) có thể được thực hiện mà không cần thực hiện các phép chia dài. Phép nhân modulo của a và b được thực hiện bằng phép nhân thông thường a với b như các số nguyên bình thường, sau đó lấy phần dư của kết quả sau khi chia cho n.

1.2.7. Độ phức tạp của thuật toán

1). Chi phí của thuật toán.

Chi phí phải trả cho một quá trình tính toán gồm chi phí thời gian và bộ nhớ.

+ Chi phí thời gian của một quá trình tính toán là thời gian cần thiết để thực hiện một quá trình tính toán.

+ Chi phí bộ nhớ của một quá trình tính toán là số ô nhớ cần thiết để thực hiện một quá trình tính toán.

Gọi A là một thuật toán, e là dữ liệu vào của bài toán đã được mã hóa. Thuật toán A tính trên dữ liệu vào e phải trả một giá nhất định.

Ký hiệu: $t_A(e)$ là giá thời gian và $l_A(e)$ là giá bộ nhớ.

2). Độ phức tạp về bộ nhớ:

$t_A(n) = \max \{ l_A(e)$, với $|e| \leq n\}$, n là "kích thước" đầu vào của thuật toán.

3). Độ phức tạp về thời gian: $l_A(n) = \max \{ t_A(e)$, với $|e| \leq n\}$.

4). Độ phức tạp tiệm cận:

Độ phức tạp PT(n) được gọi là tiệm cận tới hàm f(n), ký hiệu O(f(n)) nếu tồn tại các số n_0, c mà $PT(n) \leq c.f(n)$, $\forall n \leq n_0$.

5). Độ phức tạp đa thức:

Độ phức tạp PT(n) được gọi là đa thức, nếu nó tiệm cận tới đa thức p(n).

6). Thuật toán đa thức:

Thuật toán được gọi là đa thức, nếu độ phức tạp về thời gian là đa thức.

1.3. CÁC HỆ MÃ HÓA

1.3.1. Tổng quan về mã hóa dữ liệu

1.3.1.1. Khái niệm mã hóa dữ liệu

Để đảm bảo An toàn thông tin lưu trữ trong máy tính hay đảm bảo An toàn thông tin trên đường truyền tin người ta phải "***Che giấu***" các thông tin này.

"***Che***" thông tin (dữ liệu) hay "***Mã hóa***" thông tin là ***thay đổi hình dạng*** thông tin gốc, và người khách ***khó*** nhận ra.

"***Giấu***" thông tin (dữ liệu) là ***cất giấu*** thông tin trong bản tin khác, và người khác cũng ***khó*** nhận ra.

Thuật toán mã hóa 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 hóa thực hiện một cách riêng biệt và sinh bản rõ riêng.Thông thường khóa càng lớn thì bản mã càng an toàn, Phạm vi các giá trị có thể có của khóa gọi là ***không gian khóa.***

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

Hệ mã hóa:

Việc mã hóa phải theo các quy tắc nhất định, quy tắc đó gọi là ***Hệ mã hóa.***

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.

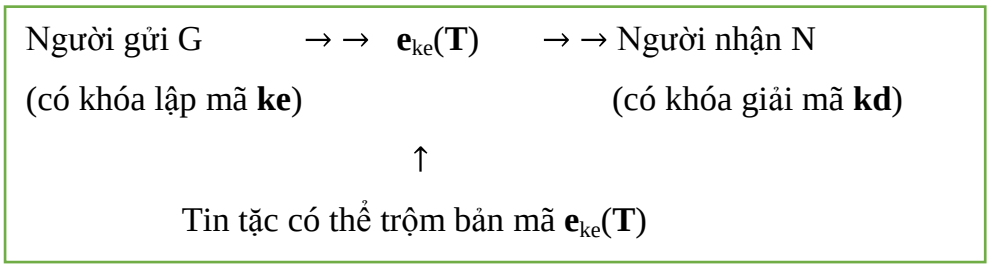
Với khóa lập mã **ke** $\in$ **K**, có hàm lập mã $\mathbf{e}_{ke} \in \mathbf{E}$, $\mathbf{e}_{ke}$: **P** $\rightarrow$ **C**,

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

sao cho $\mathbf{d}_{kd}$ ($\mathbf{e}_{ke}$ (x)) = **x**, $\forall \mathbf{x} \in$ **P**.

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

Mã hóa và giải mã:



1.3.1.2. Phân loại hệ mã hóa

Có nhiều cách để phân loại hệ mã hóa. Dựa vào tính chất đối xứng của khóa có thể phân các hệ mã hóa thành hai loại:

- Hệ mã hóa khóa đối xứng (hay còn gọi là mã hóa khóa bí mật): là những hệ mã hóa dùng chung một khóa cả trong quá trình mã hóa dữ liệu và giải mã dữ liệu. Do đó khóa phải được giữ bí mật tuyệt đối.

- Hệ mã hóa khóa bất đối xứng (hay còn gọi là mã khóa công khai): Hệ mật này dùng 1 khóa để mã hóa, dùng một khóa khác để giải mã, nghĩa là khóa để mã hóa và giải mã là khác nhau. Các khóa này tạo nên từng cặp chuyển đổi ngược nhau và không có khóa nào có thể "dễ" suy được từ khóa kia. Khóa để mã hóa có thể công khai, nhưng khóa để giải mã phải giữ bí mật.

Ngoài ra nếu dựa vào thời gian đưa ra hệ mã hóa, ta còn có thể phân làm hai loại: Mã hóa cổ điển (là hệ mật mã ra đời trước năm 1970) và mã hóa hiện đại(ra đời sau năm 1970).

Còn nếu dựa vào cách thức tiến hành mã hóa thì hệ mã hóa còn được chia làm hai loại là mã dòng (tiến hành mã từng khối dữ liệu, mỗi khối lại dựa vào các khóa khác nhau, các khóa này được sinh ra từ hàm sinh khóa, được gọi là dòng khóa) và mã khối (tiến hành mã từng khối dữ liệu với khóa như nhau).

1.3.2. Hệ mã hóa khóa công khai

1.3.2.1. Hệ mã hóa RSA

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 Ø(**n**) = (**p-1**).(**q-1**). Chọn khóa công khai b < Ø(n), nguyên tố với Ø(n).

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

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

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

Hàm Mã hoá: $y = \mathbf{e}_k(x) = x^b \bmod n$

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

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 Ø(n) = (p-1). (q-1) = 52 * 60 = 3120.

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

* ví dụ chọn b = 71.

+ Khóa bí mật a là phần tử nghịch đảo của b theo mod Ø(n): a*b ≡ 1(mod Ø(n)).

Từ a*b ≡ 1 (mod Ø(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: $\mathbf{c}_i = m_i^b \bmod n = m_i^{71} \bmod 3233$, 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: $m_i = c_i^a \bmod n = c_i^{791} \bmod 3233$, ta nhận lại bản rõ.

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, Ø(n).

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

Nếu biết được Ø(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.

1.3.2.2. Hệ mã hóa Elgamal

Sơ đồ: (Elgamal đề xuất năm 1985)

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

Chọn số nguyên tố **p** sao cho bài toán logarit rời rạc trong Z_p là "khó" giải.

Chọn phần tử nguyên thủy $\mathbf{g} \in Z_p^*$. Tính khóa công khai $h \equiv g^a \bmod \mathbf{p}$.

Định nghĩa tập khóa: $K = \{(p, g, a, h): h \equiv g^a \bmod \mathbf{p}\}$.

Các giá trị p, g, h được công khai, phải giữ bí mật **a**.

Với *bản rõ* $x \in P$ và *bản mã* $y \in \mathbf{C}$, với khóa $k \in K$ định nghĩa :

* ***Lập mã*** : Chọn ngẫu nhiên bí mật $r \in Z_{p-1}$, bản mã là $y = e_k(x, r) = (y_1, y_2)$

Trong đó : $y_1 = g^r \bmod p$ và $y_2 = x * h^r \bmod p$

**** Giải mã*** : $d_k(y_1, y_2) = y_2(y_1^a)^{-1} \bmod p$.

Ví dụ: * Bản rõ x = 1299.

Chọn p = 2579, g = 2, a = 765. Tính khóa công khai $h = 2^{765} \bmod 2579 = 949$.

* ***Lập mã*** : Chọn ngẫu nhiên r = 853. Bản mã là y = (435, 2369),

Trong đó: $y_1 = 2^{852} \bmod 2579 = 435$ và $y_2 = 1299 * 949^{853} \bmod 2579 = 2396$

**** Giải mã :*** $x = y_2(y_1^a)^{-1} \bmod p = 2369 * (435^{765})^{-1} \bmod 2579 = 1299$.

Độ an toàn :

- Hệ mã hóa Elgamal là không tất định, tức là với một bản rõ **x** và 1 khóa bí mật **a**, thì có thể có nhiều hơn một bản mã y, vì trong công thức lập mã còn có thành phần ngẫu nhiên r.
- Độ an toàn của Hệ mật mã Elgamal dựa vào khả năng giải bài toán logarit rời rạc trong Z_p. Theo giả thiết trong sơ đồ, thì bài toán này phải là "khó" giải.

Cụ thể là : Theo công thức lập mã : $y = e_k(x, r) = (y_1, y_2)$, trong đó $y_1 = g^r \bmod p$ và $y_2 = x * h^r \bmod p$.

Như vậy muốn xác định bản rõ **x** từ công thức y_2 , thám mã phải biết được **r**, Giá trị này có thể tính được từ công thức y_1 , nhưng lại gặp bài toán logarit rời rạc.

1.3.3. Hệ mã hóa khóa đối xứng – cổ điển

Khái niệm

Hệ mã hóa khóa 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 3: chuyển RÕ_SỐ ==> MÃ_SỐ.

Bước 2: chuyển RÕ_CHỮ ==> RÕ_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 3: chuyển MÃ_SỐ ==> RÕ_SỐ.

Bước 2: chuyển MÃ_CHỮ ==> MÃ_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".

1.3.3.1. 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.

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

Sơ đồ : Đặt P = C = Z_{26} . Bản mã y và bản rõ x ∈ Z_{26}.

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

Với khóa k = π ∈ 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.

1.3.3.3. Hệ mã hóa AFFINE

Sơ đồ :

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

Tập khóa K = {(a,b), với a,b ∈ Z_{26}, UCLN(a, 26) = 1}

Với khóa k = (a,b) ∈ 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 ∈ Z_{26} nguyên tố với 26 là Ø(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 ∈ Z_{26} là 26.
- Số các khóa (a,b) có thể là 12*26 = 312. Rất ít !
- Như vậy việc dò tìm khóa mật khá dễ dàng.

1.3.3.4. Hệ mã hóa VIGENERE

Sơ đồ:

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

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

Mã hóa Y = $(y_1, y_2, \ldots, y_m)=e_k(x_1, x_2, \ldots, x_m)=(x_1+ k1, x_2 + k_2, \ldots, x_m+ k_m)$ mod 26.

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

1.3.3.5. 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 ∈ Z_{26}.

- Tập khóa K là tập tất cả các hoán vị của {1, 2, …, m}
- Với mỗi khóa k = π ∈ 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 là:

1! + 2! + 3! + …+ m! trong đó m ≤ 26.

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

1.3.3.6. Hệ mã hóa HILL

Sơ đồ :

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

Tập khóa K={ k ∈ $(Z_{26})^{m*n}$ / det(K,26)=1}. (K phải có K^{-1})

Mỗi khóa K là một "***chùm chìa khóa***" :

Với mỗi k ∈ 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.

1.3.4. Hệ mã hóa khóa đối xứng DES

1.3.4.1. Hệ mã hóa DES

Giới thiệu :

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

Quy trình mã hóa theo DES :

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

Chia thành

Giai doạn 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

1.3.4.2. Lập mã và giải mã

Lập mã DES :

* 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_0R_0, trong đó L_0 là 32 bit đầu (Left), R_0là 32 bit cuối (Right).

(IP(x) tách thành L_0R_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 2).

$k_1, k_2, \ldots, k_{16}$ 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 được bản mã y.

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

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.

1.3.4.3. 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 $e_K(x) = y$.

1.4. CHỮ KÝ SỐ

1.4.1. Giới thiệu

Để chứng thực nguồn gốc hay hiệu lực của một tài liệu (ví dụ: đơn xin nhập học, giấy báo nhập học,…) lâu nay người ta dùng chữ ký "tay", ghi vào phía dưới của mỗi tài liệu. Như vậy người ký phải trực tiếp "ký tay" vào tài liệu.

Ngày nay các tài liệu được số hóa, người ta cũng có nhu cầu chứng thực nguồn gốc tài liệu. Rõ ràng không thể "ký tay" vào tài liệu vì chúng không được in ấn trên giấy. Tài liệu "số" là một xâu các bit (0 hay 1), xâu bít có thể rất dài, "Chữ ký" để chứng thực một xâu bít tài liệu cũng không thể là một xâu bit nhỏ đặt phía dưới xâu bit tài liệu. Một "Chữ ký" như vậy chắc chắn sẽ bị kẻ gian sao chép để đặt dưới một tài liệu khác một cách bất hợp pháp.

Những năm 80 của thế kỷ 20, các nhà khoa học đã phát minh ra "chữ ký số" để chứng thực một "tài liệu số" . Đó chính là bản mã của xâu bit tài liệu.

Người ta tạo ra "chữ ký số" trên "tài liệu số" giống như tạo ra "bản mã" của tài liệu với "khóa lập mã".

Như vậy "ký số" trên "tài liệu số" là "ký" trên từng bit tài liệu. Kẻ gian khó có thể giả mạo "chữ ký số" nếu nó không biết "khóa lập mã".

Để kiểm tra một "chữ ký số" thuộc về một "tài liệu số", người ta giải mã "chữ ký số" bằng "khóa giải mã", và so sánh với tài liệu gốc.

Ngoài ý nghĩa để chứng thực nguồn gốc hay hiêu lực của các tài liệu số hóa, Mặt mạnh của "Chữ ký số" hơn "Chữ ký tay" là ở chỗ người ta có thể "ký" vào tài liệu từ rất xa trên mạng công khai. Hơn thế nữa, có thể "ký" bằng các thiết bị cầm tay như Điện thoại di động, laptop,.. tại khắp mọi nơi miễn là kết nối được vào mạng. Đỡ tốn thời gian, công sức, chi phí…

"Ký số" thực hiện trên từng bit tài liệu, nên độ dài của "chữ ký số" ít nhất cũng bằng độ dài của tài liệu. Do đó thay vì ký trên tài liệu dài, người ta thường dùng "hàm băm" để tạo "đại diện" cho tài liệu, sau đó mới "ký số" lên "đại diện" này.

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 ∈ K, tồn tại một thuật toán ký $Sig_k \in S$, $Sig_k : P \rightarrow A$, có thuật toán kiểm tra chữ ký $Ver_k \in V$, $Ver_k : P \times A \rightarrow$ {đúng, sai}, thỏa mãn điều kiện sau với mọi x ∈ P, y ∈ A :

$Ver_k (x, y)$ = Đúng, nếu $y = Sig_k (x)$ hoặc Sai, nếu $y \neq Sig_k (x)$.

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.

1.4.2. Phân loại "Chữ ký số"

Có nhiều loại chữ ký tùy theo cách phân loại, sau đây xin giới thiệu một số cách.

Cách 1: Phân loại chữ ký theo khả năng khôi phục thông điệp gốc 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.

Ví dụ : Chữ ký RSA

2). Chữ ký không thể khôi phục thông điệp gốc :

Ví dụ: Chữ ký Elgamal 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).

1.4.3. Một số loại chữ ký số

1.4.3.1. Chữ ký RSA

Sơ đồ : (đề xuất năm 1978)

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

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

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

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

Ký số: chữ ký trên x ∈ P là $y = Sig_k(x) = x^a \pmod n$, y ∈ A (R1).

Kiểm tra chữ ký: $Ver_k(x,y)$ = đúng ⇔ $x = y^b \pmod n$ (R2).

Chú ý:

Việc "ký số" vào x tương ứng với việc "mã hóa" tài liệu x.

Kiểm thử chính là việc giải mã "chữ ký", để kiểm tra xem tài liệu đã giải mã có đúng với tài liệu trước khi ký hay không. Thuật toán và kiểm thử "chữ ký" là công khai, ai cũng có thể kiểm thử chữ ký được.

Ví dụ: chữ ký trên x = 2

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

Chọn bí mật số nguyên tố p=3, q=5, tính n=p*q=3*5=15, công khai n.

Đặt P=C=Z_n. tính bí mật $\emptyset(n)$ = (q-1)(p-1)= (3-1)(5-1) =8

Chọn khóa công khai b= 3<$\emptyset(n)$, nguyên tố cùng nhau với $\emptyset(n)$ =8.

Khóa bí mật a =3, là phần tử nghịch đảo của b theo mod $\emptyset(n)$: a*b=1(mod$\emptyset(n)$)

* *Ký số*: chữ ký trên x=2 $\in$ P là :

$y = Sig_k(x) = x^a \pmod n = 2^3 \pmod{15} = 8$, $y \in A$.

* *Kiểm tra chữ ký* :

$Ver_k(x,y)$ = đúng $\leftrightarrow x = y^b \pmod n \leftrightarrow 2 = 8^b \pmod{15}$

1.4.3.2. Chữ ký ELGAMAL

Sơ đồ : (Elgamal đề xuất năm 1985)

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

Chọn số nguyên tố **p** sao cho bài toán logarit rời rạc trong Z_p là "khó" giải.

Chọn phần tử nguyên thủy $g \in Z_p^*$. Đặt $P = Z_p^*$, $A = Z_p^* \times Z_{p-1}$.

Chọn khóa bí mật là $a \in Z_p^*$. Tính khóa công khai $h \equiv g^a \bmod \mathbf{p}$.

Định nghĩa tập khóa : $K = \{(p, g, a, h): h \equiv g^a \bmod \mathbf{p}\}$.

Các giá trị p, g, h được công khai, phải giữ bí mật a.

* ***Ký số***: Dùng 2 khóa ký: khóa **a** và khóa ngẫu nhiên bí mật $r \in Z_{p-1}^*$.

(Vì $r \in Z_{p-1}^*$, nên nguyên tố cung p-1, do đó tồn tại $r^{-1} \bmod(p-1)$).

Chữ ký trên $x \in P$ là $y = Sig_k(x, r) = (\gamma, \delta)$, $y \in A$ (E1)

Trong đó $\gamma \in Z_p^*$, $\delta \in Z_{p-1}$:

$$\gamma = g^r \bmod \mathbf{p} \text{ và } \delta = (x - a * \gamma) * r^{-1} \bmod (p-1)$$

**** Kiểm tra chữ ký :***

$Ver_k(x, \gamma, \delta)$ = đúng $\leftrightarrow h^{\gamma} * \gamma^{\delta} \equiv g^x \bmod p$. (E2)

Chú ý: Nếu chữ ký được tính đúng, kiểm thử sẽ thành công vì

$h^{\gamma} * \gamma^{\delta} \equiv g^{a\gamma} * g^{r*\delta} \bmod p \equiv g^{(a\gamma + r*\delta)} \bmod p \equiv g^x \bmod p.$

Do $\delta = (x - a * \gamma) * r^{-1} \bmod (p - 1)$ nên $(a * \gamma + r * \delta) \equiv x \bmod (p-1)$

1.4.3.3. Chữ ký Schnoor

**** Sinh khóa***:

Cho $\mathbf{Z}_n^*$, **q** là số nguyên tố, cho **G** là nhóm con cấp **q** của $\mathbf{Z}_n^*$.

Chọn phần tử sinh $\mathbf{g} \in \mathbf{G}$, sao cho bài toán logarit rời rạc trên **G** là "khó giải".

Chọn hàm băm H: $\{0, 1\}^* \rightarrow \mathbf{Z}_q$.

Chọn khóa bí mật là $a \in \mathbf{Z}_n^*$, khóa công khai là $\mathbf{h} = \mathbf{g}^a \mod n$.

**** Ký số***:

Chữ ký Schnorr trên $\mathbf{m} \in \{0, 1\}^*$ được định nghĩa là cặp (**c**, **s**), nếu thỏa mãn điều kiện $c = H(\mathbf{m}, \mathbf{g}^s \mathbf{h}^c)$.

Chú ý: Ký hiệu $(\mathbf{m}, \mathbf{g}^s \mathbf{h}^c)$ là phép "ghép nối" **m** và $\mathbf{g}^s \mathbf{h}^c$.

Ví dụ: $\mathbf{m} = 0110$, $\mathbf{g}^s \mathbf{h}^c = 01010$, thì $(\mathbf{m}, \mathbf{g}^s \mathbf{h}^c) = 011001010$.

Tạo chữ ký Schnorr: Chữ ký là cặp (**c**, **s**).

+ Chọn ngẫu nhiên $\mathbf{r} \in \mathbf{Z}_q^*$. Tính $\mathbf{c} = H(\mathbf{m}, \mathbf{g}^r)$, $\mathbf{s} = \mathbf{r} - \mathbf{c}\,\mathbf{a} \pmod{\mathbf{q}}$.

**** Kiểm tra chữ ký:***

Cặp (**c**, **s**) là chữ ký Schnorr, vì thỏa mãn điều kiện $c = H(\mathbf{m}, \mathbf{g}^s \mathbf{h}^c)$.

Vì $\mathbf{g}^s \mathbf{h}^c = \mathbf{g}^{r - c\,a} (\mathbf{g}^a)^c = \mathbf{g}^r \pmod n$, do đó $H(\mathbf{m}, \mathbf{g}^s \mathbf{h}^c) = H(\mathbf{m}, \mathbf{g}^r) = c$.

Chương 2.

ỨNG DỤNG VẤN ĐỀ CHIA SẺ BÍ MẬT TRONG BỎ PHIẾU ĐIỆN TỬ

2.1. TỔNG QUAN VỀ BỎ PHIẾU ĐIỆN TỬ.

2.1.1. Vấn đề bỏ phiếu từ xa.

2.1.1.1. Khái niệm bỏ phiếu từ xa.

Xã hội dân chủ có nhiều việc cần đến " bỏ phiếu ": để thăm dò các kế hoạch, để bầu các chức vị, chức danh… Nhưng quĩ thời gian của người ta không nhiều, mặt khác một người có thể làm việc tại nhiều nơi, như vậy người ta khó có thể thực hiện được nhiều cuộc bỏ phiếu theo phương pháp truyền thống. Rõ ràng "bỏ phiếu từ xa " đang và sẽ là nhu cầu cấp thiết, vấn đề trên chỉ còn là thời gian và kỹ thuật cho phép. Đó là cuộc " bỏ phiếu " được thực hiện từ xa trên mạng máy tính qua các phương tiện " điện tử " như máy tính cá nhân, điện thoại di động…Như vậy mọi người trong cuộc "không thể nhìn thấy mặt nhau" và các "lá phiếu" (lá phiếu "số ") được chuyển từ xa trên mạng máy tính tới " hòm phiếu".

Cũng như cuộc bỏ phiếu truyền thống, cuộc bỏ phiếu từ xa phải đảm bảo yêu cầu: " bí mật " " toàn vẹn " và " xác thực " của lá phiếu , mỗi cử tri chỉ được bỏ phiếu một lần, mọi người đều có thể kiểm tra tính đúng đắn của cuộc bỏ phiếu, cử tri không thể chỉ ra mình đã bỏ phiếu cho ai (để có cơ hội mua bán phiếu bầu),…

Yêu cầu " bí mật " của lá phiếu là : ngoài cử tri, chỉ có ban kiểm phiếu mới biết được biết nội dung lá phiếu, nhưng họ lại không thể biết ai là chủ nhân của nó.

Yêu cầu " toàn vẹn " của lá phiếu là : trên đường truyền tin, nội dung lá phiếu không thể bị thay đổi, tất cả lá phiếu đều được chuyển tới hòm phiếu an toàn, đúng thời gian, chúng được kiểm phiếu đầy đủ.

Yêu cầu " xác thực " của lá phiếu là : lá phiếu gửi tới hòm phiếu phải hợp lệ, đúng là của người có quyền bỏ phiếu, cử tri có thể nhận ra lá phiếu của họ.

2.1.1.2. Tổ chức hệ thống bỏ phiếu từ xa.

a). Các thành phần trong Ban tổ chức bỏ phiếu gồm có :

- 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, qui định cơ chế ***định danh cử tri.***

- Ban đăng ký (ĐK) ***nhận dạng cử tri*** và ký ***cấp quyền*** bỏ phiếu cho họ. Có hệ thống " ký " hỗ trợ.

- Ban kiểm tra (KT) ***xác minh tính hợp lệ*** của lá phiếu. (Vì lá phiếu đã mã hóa nên ban KP không thể biết được lá phiếu có hợp lệ không, nên cần phải xác minh tính hợp lệ của lá phiếu trước khi nó đến hòm phiếu).

- Ban kiểm phiếu (KP) tính toán và thông báo kết quả bỏ phiếu. Có hệ thống "kiểm phiếu " hỗ trợ.

b). Các thành phần kỹ thuật trong Hệ thống bỏ phiếu gồm có:

- Hệ thống máy tính và các phần mềm phục vụ quy trình bỏ phiếu từ xa.

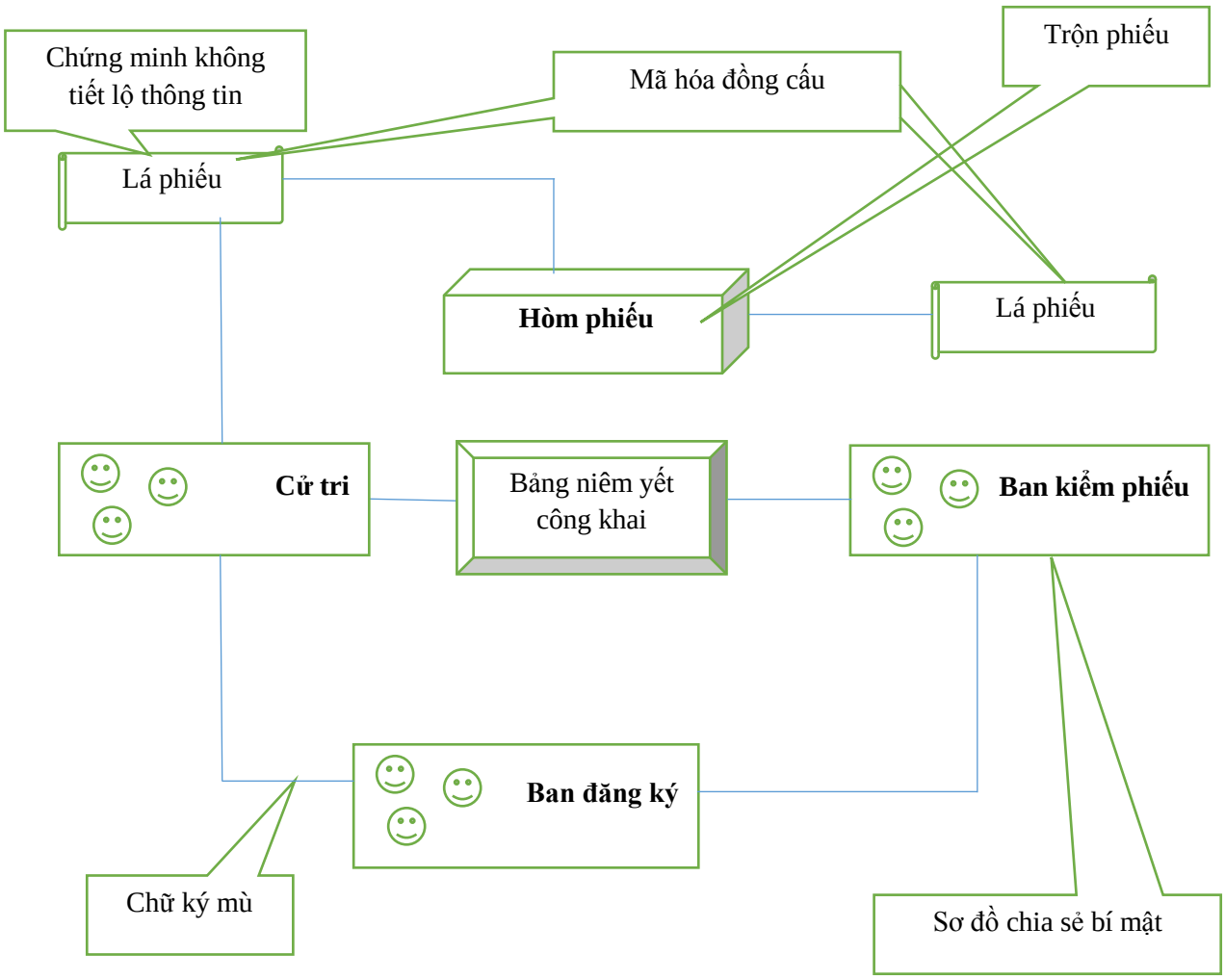
- Người trung thực ***kiểm soát Server*** đảm bảo yêu cầu bảo mật và toàn vẹn kết quả bỏ phiếu.

- Một số kỹ thuật đảm bảo an toàn thông tin : chữ ký mù, mã hóa đồng cấu, chia sẻ bí mật, " chứng minh không tiết lộ thông tin ".

- Hệ thống phân phối khóa tin cậy sẵn sàng cung cấp khóa cho công việc mã hóa hay ký " số ".

2.1.2. Quy trình bỏ phiếu từ xa.

Hiện nay người ta đã nghiên cứu và thử nghiệm một số quy trình bỏ phiếu từ xa, mỗi quy trình có những ưu nhược điểm riêng. Quy trình bỏ phiếu từ xa gồm có 3 giai đoạn : đăng ký, bỏ phiếu, kiểm phiếu.



Hình 2.1. Quy trình bỏ phiếu từ xa

2.1.2.1. Giai đoạn đăng ký.

a). Công việc

* **Cử tri :**

1). Cử tri chọn bí mật số định danh **x,** giấy chứng minh thư điện tử (CMT), thông tin nhận dạng (ví dụ như "vân tay"). Cử tri làm mù **x** thành **y** = Blind(**x**).

2). Cử tri gửi tới Ban đăng ký (ĐK) thông tin nhận dạng của mình, CMT, số **y** (định danh **x** đã được họ làm mù thành **y**).

* **Ban đăng ký :**

3). Ban đăng ký nhận dạng cử tri, Kiểm tra CMT của cử tri. Nếu hồ sơ của cử tri hợp lệ, khớp với danh sách cử tri của Ban điều hành (ĐH), Cử tri chưa xin cấp chữ ký lần nào, thì ra lệnh cho Hệ thống "ký" lên **y**. Đó là chữ ký **z** = sign(**y**) .

4). Ban đăng ký ghi số CMT của cử tri vào danh sách các cử tri đã được cấp chữ ký để tránh việc cử tri đăng ký bỏ phiếu nhiều lần.

5). Ban đăng ký gửi chữ ký **z** về cho cử tri.

*** Cử tri :**

6). Khi nhận được chữ ký này, cử tri "xóa mù" trên **z**, họ sẽ nhận được chữ ký sign(**x**) trên định danh thật **x** . Lá phiếu có gắn chữ ký sign(**x**) được xem như đã có chữ ký của Ban đăng ký. Đó là lá phiếu hợp lệ để cử tri ghi ý kiến của mình.

7). Cử tri có thể kiểm tra chữ ký của Ban đăng ký trên lá phiếu của mình có hợp lệ hay không bằng cách dùng hàm kiểm tra chữ ký và khóa công khai của Ban đăng ký

Chú ý rằng **khóa ký** trên định danh của cử tri được chia sẻ cho mọi thành viên của Ban đăng ký và Ban kiểm tra, nhờ đó sau này Ban kiểm tra có thể phát hiện những cử tri giả mạo chữ ký của Ban đăng ký.

b). Kỹ thuật sử dụng

* Kỹ thuật " Chia sẻ khóa bí mật " (Secret Sharing):

- Hệ thống phân phối khóa tin cậy (PP khóa) đã chia sẻ khóa ký cho các thành viên Ban đăng ký trước đó. Sau khi xét duyệt hồ sơ xin chữ ký của cử tri, nếu mọi thành viên của Ban đăng ký đều nhất trí cho ký thì họ sẽ khớp các mảnh khóa riêng để nhận được khóa ký.

- Mục đích kỹ thuật : Từng thành viên của Ban đăng ký không thể tùy tiện cấp chữ ký.

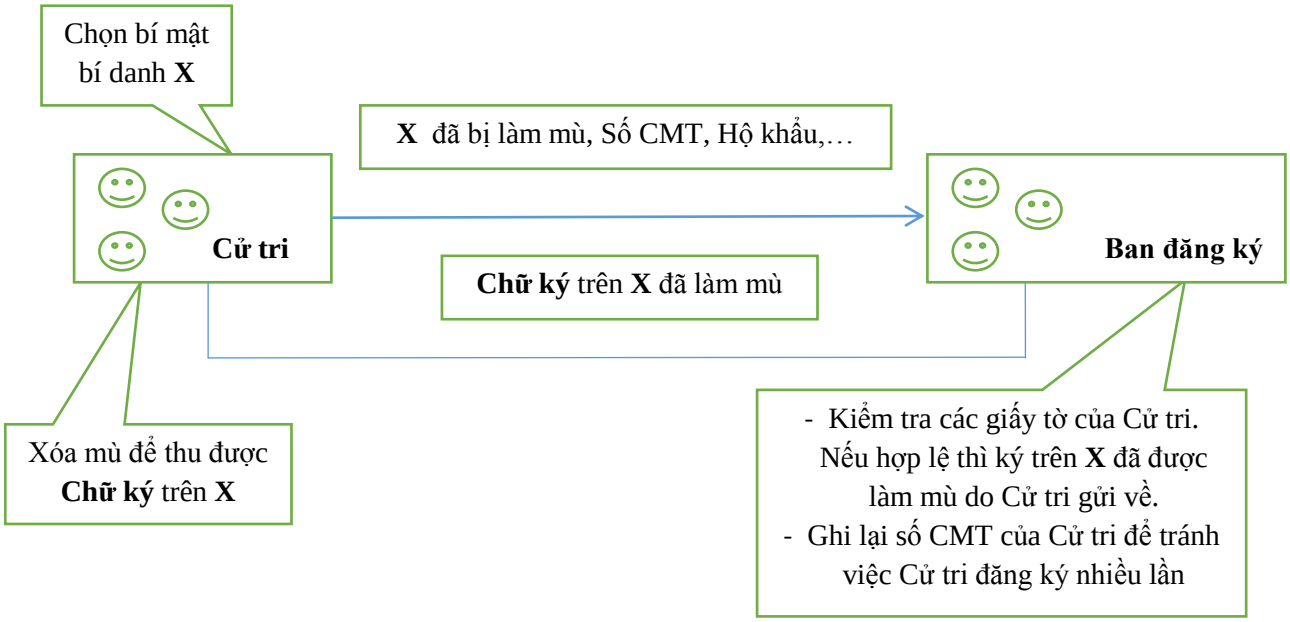
* Kỹ thuật " Chữ ký mù " (Blind Signature):

- Ban đăng ký sử dụng kỹ thuật ký "mù" để ký lên định danh " mù " của cử tri.

- Mục đích của kỹ thuật : Ban đăng ký không thể biết được ai đã ghi ý kiến vào lá phiếu, tức là bảo đảm không lộ danh tính cử tri.

c). Sơ đồ Giai đoạn đăng ký

Để được quyền bầu cử, Cử tri phải có chữ ký của Ban đăng ký



Hình 2.2. Sơ đồ giai đoạn đăng ký.

2.1.2.2 . Giai đoạn bỏ phiếu.

a). Công việc

*** Cử tri :**

1). Sau khi lá phiếu có chữ ký của Ban đăng ký, cử tri ghi ý kiến vào lá phiếu.

2). Cử tri mã hóa lá phiếu bằng khóa công khai của Ban kiểm phiếu.

3). Cử tri gửi tới Ban kiểm tra : lá phiếu đã mã hóa, Định danh **x** (không bị làm mù) của họ, Chữ ký của Ban đăng ký trên lá phiếu, "Chứng minh không tiết lộ thông tin" về lá phiếu.

Lá phiếu không được chuyển thẳng tới hòm phiếu mà trước đó phải chuyển tới Ban kiểm tra. Tại đây họ kiểm tra chữ ký cấp quyền bỏ phiếu có bị giả mạo không, xác minh tính hợp lệ của lá phiếu.

*** Ban kiểm tra :**

4). Kiểm tra chữ ký cấp quyền bỏ phiếu trên lá phiếu. (Liên hệ với Ban đăng ký)

5). Kiểm tra tính hợp lệ của lá phiếu. (tương tác với cử tri)

6). Mã hóa lại lá phiếu, gửi về hòm phiếu.

Khi lá phiếu (đã mã hóa) về Ban kiểm tra, cử tri phải gửi kèm theo định danh thật **x** (không bị làm mù). Như vậy Ban kiểm tra biết được chữ ký thật sign(**x**) của Ban đăn ký trên lá phiếu và định danh thật **x** của cử tri, nhưng không biết danh tính thật của cử tri (họ tên, số CMT,...). Ngược lại, Ban đăng ký biết các thông tin này nhưng lại không biết được định danh thật **x** của cử tri (vì nó đã bị làm mù trước khi gửi tới họ).

Khóa ký vào định danh của cử tri được chia sẻ cho mọi thành viên của Ban đăng ký và Ban kiểm tra. Vì vậy trong giai đoạn này, Ban kiểm tra dùng khóa ký đó để ký lên định danh thật **x** của cử tri, kiểm tra xem có giống như chữ ký Sign(**x**) mà cử tri đã gửi tới họ. Nếu hai chữ ký trong lá phiếu trêm là giả mạo, lá phiếu này sẽ không được gửi tiếp đến hòm phiếu.

Ban kiểm tra thực hiện các giao thức tương tác với cử tri để kiểm tra tính hợp lệ của lá phiếu. Sau khi xác minh tính hợp lệ của lá phiếu, Ban kiểm tra gửi nó về hòm phiếu.

Ban kiểm tra đứng trung gian giữa Cử tri và Ban kiểm phiếu để ngăn chặn một số tình huống thiếu an toàn hay vi phạm luật bỏ phiếu, ví dụ trường hợp mua bán phiếu bầu cử. (Phương pháp bỏ phiếu truyền thống không cần giai đoạn này)

b). Kỹ thuật sử dụng.

* Kỹ thuật "Mã hóa đông cấu" (Homomorphism Cryptography)

Mã hóa đồng cấu có tính chất đặc biệt: tích của các "bản tin" (messenge) được mã hóa bằng tổng các "bản tin" được mã hóa. Điều này rất thích hợp cho loại bỏ phiếu điện tử khi mà các "bản tin" được mã hóa thành 0 hay 1.

Mục đích của kỹ thuật : Ban kiểm phiếu không cần giải mã từng lá phiếu, vẫn có thể kiểm phiếu được.

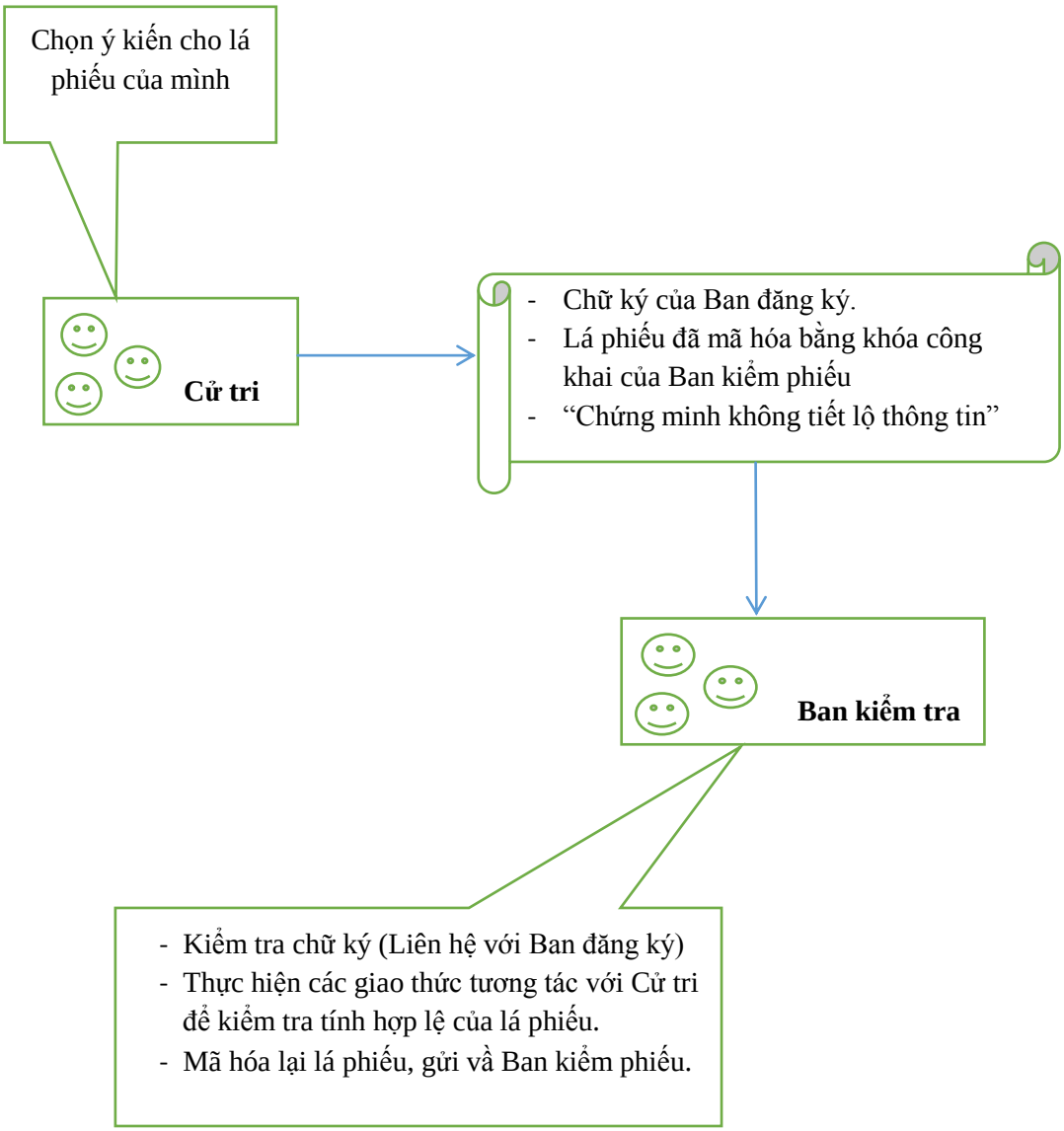
* Kỹ thuật "Chứng minh không tiết lộ thông tin" (Zero_knowlwage proof)

Mục đích của kỹ thuật : Ban kiểm tra có cơ sở để xác minh tính hợp lệ của lá phiếu. (Vì dưới dạng mã hóa, nên không thể biết lá phiếu có hợp lệ không).

* Kỹ thuật "Ký số" (Digital Signature) : kiểm tra chữ ký cấp quyền trên lá phiếu.

* Kỹ thuật "Mã hóa" (Cryptography) : Mã hóa lại lá phiếu, gửi về hòm phiếu.

c). Sơ đồ giai đoạn bỏ phiếu



Hình 2.3. Sơ đồ giai đoạn bỏ phiếu.

2.1.2.3 . Giai đoạn kiểm phiếu.

a. Công việc

1). Các lá phiếu sẽ được "trộn" nhờ kỹ thuật "trộn" trước khi chúng được chuyển về Ban kiểm phiếu, nhằm giữ bí mật danh tính cho các cử tri.

2). Ban kiểm phiếu tính kết quả dựa vào các lá phiếu (đã má hóa) gửi về.

Theo phương pháp mã hóa đồng cấu, Ban kiểm phiếu không cần giải mã từng lá phiếu, vẫn có thể kiểm phiếu được.

Khi kiểm phiếu, các thành viên trong Ban kiểm phiếu dùng các mảnh khóa riêng của mình để khôi phục khóa bí mật và dùng khóa bí mật này để tính kết quả.

3). Ban kiểm phiếu thông báo kết quả trên bảng niêm yết công khai.

b. Kỹ thuật sử dụng.

* Kỹ thuật "Trộn" (Mixing).

Ban kiểm phiếu gồm m thành viên, để họ không thể biết được lá phiếu nào là của ai, người ta xây dựng hệ thống mã hóa m tầng và giải mã m lần mới biết được nội dung của các lá phiếu.

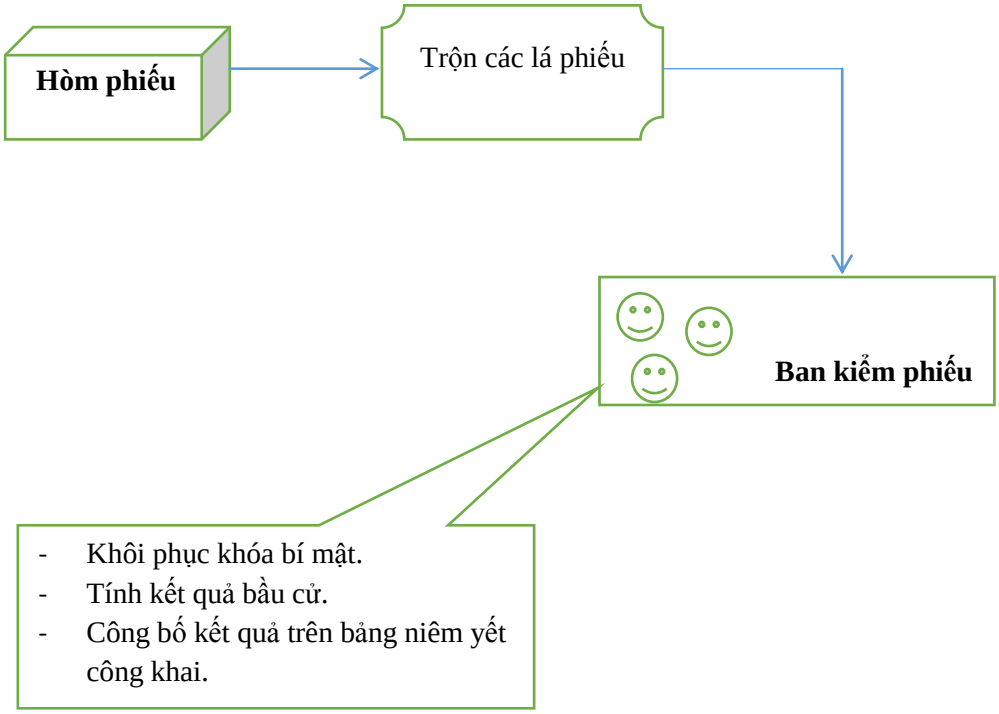
Đầu tiên người thứ nhất trong Ban kiểm phiếu biết được từng lá phiếu là của ai, nhưng lại không biết nội dung của chúng. Anh ta giải mã lần 1, vẫn không biết nội dung của chúng, người này trộn theo trật tự khác. Mọi người tiếp theo trong Ban kiểm phiếu thực hiện các công việc như người thứ nhất. Sau khi người cuối cùng giải mã lần thứ m thì nội dung các lá phiếu đã rõ ràng, nhưng các thành viên trong Ban kiểm phiếu không thể biết được "tác giả" của từng lá phiếu vì chúng được "trộn" m-1 lần.

* Kỹ thuật "Chia sẻ khóa bí mật " (Secret Sharing).

Chia sẻ khóa bí mật để giải mã lá phiếu, mỗi người trong ban kiểm phiếm chỉ giữ một mảnh khóa nên không thể tự ý giải mã lá phiểu để sửa lại nội dung lá phiếu.

* Kỹ thuật "Mã hóa đồng cấu" (Homomorphism Cryptography).

c). Sơ đồ giai đoạn kiểm phiếu.



Hình 2.4. Sơ đồ giai đoạn kiểm phiếu.

2.2. VẤN ĐỀ CHIA SẺ BÍ MẬT

2.2.1. Khái niệm chia sẻ bí mật.

Khái niệm:

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 mảnh.

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

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 dấu 1 mảnh.

2.2.2. Các sở đồ chia sẻ bí mật.

2.2.2.1 . Sơ đồ ngưỡng Shamir.

a). 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 khoá không đọc nằm trong số m thành viên trên.

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

Sơ đồ ngưỡng Shamir 1979.

Bài toán

- Chia khoá bí mật K trong Z_p thành t mảnh, phân cho mỗi người giữ 1 mảnh, $t \leq m$. t thành viên "khớp t mảnh" sẽ nhận được K.

b). Chia mảnh khoá K (Chủ khóa D)

Khởi tạo: Chọn số nguyên tố p.

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

$1 \leq i \leq m$ ($m < p$, 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 .

Ví dụ 1 *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 $\mathbf{y_i} = P(\mathbf{x_i})$, $1 \leq i \leq m$, trong đó:

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

$y1 = P(x1) = P(1) = 13 + a_1 .1 + a_2 .1^2 = 13 + 10 .1 + 2 .1^2 = 8$

$y3 = P(x3) = P(3) = 13 + a_1 .3 + a_2 .3^2 = 13 + 10 .3 + 2 .3^2 = 10$

$y5 = P(x5) = P(5) = 13 + a_1 .5 + a_2 .5^2 = 13 + 10 .5 + 2 .5^2 = 11$

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

c). Cách khôi phục khóa K từ t thành viên

Phương pháp: 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 2 Khôi phục khoá K

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

y1 =8, y3 = 10, y5 = 11, để khôi phục lại khoá K.

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

Thay x1 = 1, x3 = 3, x5 = 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 a0 , a1, a2.

$y1 = P(x1) = P(1) = a_0 + a1 .1 + a2 .1^2 = 8 \pmod{17}$.

$y3 = P(x3) = P(3) = a_0 + a1 .3 + a2 .3^2 = 10 \pmod{17}$.

$y5 = P(x5) = P(5) = a_0 + a1 .5 + a2 .5^2 = 11 \pmod{17}$.

Giải hệ 3 phương trình tuyến tính trong Z_{17}, nghiệm duy nhất là: a_0 =13, a1=10, a2=2.

Khoá được khôi phục là: K= a_0 =13.

2.2.2.2. Cấu trúc mạch đơn điệu.

Giả sử ta không muốn tất cả các tập con t thành viên bất kỳ đều có khả năng mở khoá như trong sơ đồ ngưỡng Shamir, mà chỉ một số các tập con thành viên chỉ định trước có thể làm được điều đó.

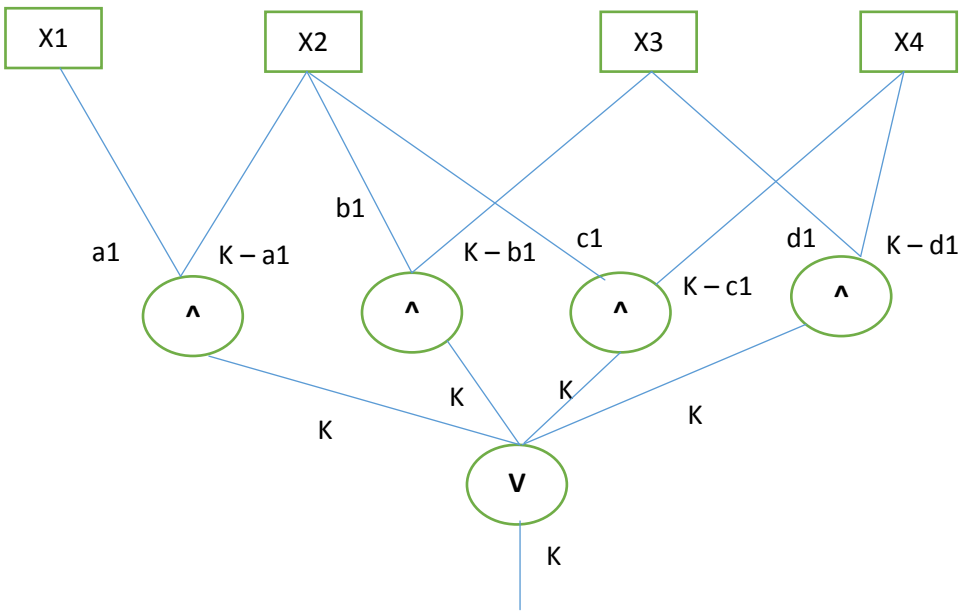
Cấu trúc đơn điệu là một giải pháp cho yêu cầu trên. Tập con các thành viên có thể mở được khoá gọi là tập con hợp thức. Tập các tập con hợp thức gọi là cấu trúc truy nhập.

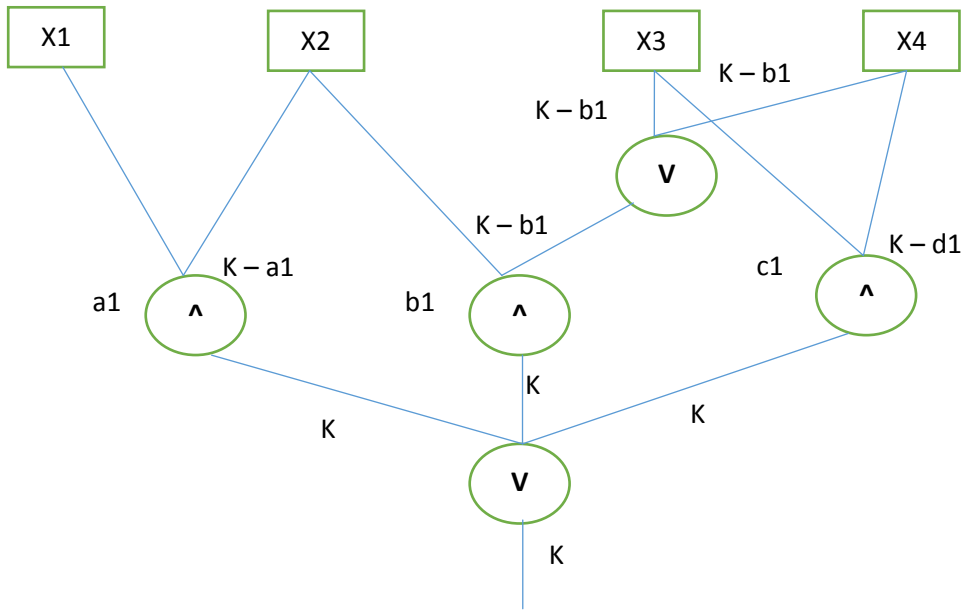
Ví dụ:

Nếu có một tập gồm các thành viên $\{P_1, P_2, P_3, P_4\}$ trong đó các tập con có thể mở khoá là: $\{P_1, P_2, P_4\}$, $\{P_1, P_3, P_4\}$, $\{P_2, P_3\}$

Khi đó ta sẽ thu được công thức Boolean sau:

$$(P_1 \wedge P_2 \wedge P_4) \vee (P_1 \wedge P_3 \wedge P_4) \vee (P_2 \wedge P_3)$$





2.2.2.3 . Cấu trúc không gian vectơ Brickell.

Giai đoạn khởi đầu:

1. Với $1 \leq i \leq w$, D sẽ trao vectơ (P_i) $(Z_p)^d$ cho P_i. Các vectơ này được công khai.

Phân phối mảnh:

2. Giả sử D muốn chia sẻ một khóa $K \in Z_p$, D sẽ chọn một cách bí mật (ngẫu nhiên, độc lập) d-1 phần tử của Z_p là $a_2, \ldots, a_d$

3. Với $1 \leq i \leq w$, D tính: $y_i = (P_i)$ trong đó $= (K, a_2, \ldots, a_d)$

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

2.3. ỨNG DỤNG CHIA SẺ BÍ MẬT TRONG ĐĂNG KÝ BỎ PHIẾU ĐIỆN TỬ.

2.3.1. Một số bài toán trong đăng ký bỏ phiếu điện tử.

1/. Bài toán bảo vệ hồ sơ Đăng ký bỏ phiếu điện tử.

Cử tri gửi hồ sơ đăng ký về cho Ban đăng ký thẩm định.

Vấn đề nảy sinh :

Trên đường truyền, Hồ sơ Đăng ký của Cử tri có thể bị kẻ gian thay đổi thông tin, hoặc đánh cắp hồ sơ Đăng ký.

Phương pháp giải quyết :

Sử dụng các kỹ thuật mã hóa.

2/. Bài toán thẩm định hồ sơ đăng ký.

Trong quá trình đăng ký bỏ phiếu điện tử, để Ban đăng ký có thể cấp quyền bầu cử cho Cử tri thì Ban đăng ký phải xác thực được thông tin của Cử tri có đáp ứng được yêu cầu của cuộc bầu cử hay không. (Ví dụ : Cử tri phải là công dân của nước Việt Nam, Cử tri đủ tuổi để bầu cử….).

Vấn đề nảy sinh :

Cử tri có thể cấu kết với thành viên trong ban kiểm phiếu để duyệt hồ sơ cho mình trong khi hồ sơ không đủ điều kiện bỏ phiếu.

Phương pháp giải quyết :

Sử dụng kỹ thuật chia sẻ khóa bí mật để giải mã hồ sơ.

3/. Bài toán Ban đăng ký ký vào lá phiếu (Đã ẩn danh).

Sau khi thẩm định hồ sơ Đăng ký của Cử tri, nếu hồ sơ hợp lệ thì Ban đăn ký sẽ ký lên lá phiếu và gửi về cho Cử tri.

Vấn đề nảy sinh :

Cử tri có thể cấu kết với thành viên trong Ban đăng ký để xin cấp chữ ký cho mình nhiều lần. Như vậy sẽ xảy ra tình trạng bán chữ ký.

Phương pháp giải quyết :

Sử dụng kỹ thuật chia sẻ khóa bí mật, để ký.

2.3.2. Ứng dụng chia sẻ bí mật.

1/. Ứng dụng chia sẻ bí mật vào bài toán Thẩm định hồ sơ đăng ký.

Khóa giải mã từng hồ sơ đăng ký bỏ phiếu điện tử sẽ được chia thành nhiều mảnh, mỗi người trong ban Đăng ký sẽ giữ một mảnh. Khi tất cả mọi người trong ban Đăng ký đồng ý giải mã hồ sơ thì sẽ ghép các mảnh khóa lại để được khóa giải mã hồ sơ.

Như vậy một người trong ban Đăng ký không thể tự ý sửa đổi hồ sơ đăng ký của cử tri để phù hợp với điều kiện đăng ký.

2/. Ứng dụng chia sẻ bí mật vào bài toán Ký vào lá phiếu.

Khóa ký mù vào lá phiếu sẽ được chia thành nhiều mảnh, mỗi người trong ban Đăng ký sẽ giữ một mảnh khóa. Khi tất cả mọi người trong ban Đăng ký đồng ý ký thì sẽ ghép các mảnh khóa lại để được khóa ký và ký lên lá phiếu.

Như vậy một người trong ban Đăng ký không thể tùy tiện cấp chữ ký được, mà phải có sự đồng thuận nhất chí của tất cả thành viên trong Ban đăng ký.

Chương 3. THỬ NGHIỆM CHƯƠNG TRÌNH.

3.1. THỬ NGHIỆM CHƯƠNG TRÌNH CHIA SẺ KHÓA BÍ MẬT.

*** Thử nghiệm chương trình chia sẻ khóa bí mật theo sơ đồ ngưỡng Shamir :**

Bài toán

Chia khoá bí mật K trong Zp thành t mảnh, phân cho mỗi người giữ 1 mảnh, $t \leq m$. t thành viên "khớp t mảnh" sẽ nhận được K.

3.1.1. Chia sẻ khoá bí mật K

Khởi tạo: Chọn số nguyên tố p.

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

$1 \leq i \leq m$ ($m < p$, 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 .

3.1.2. Khôi phục khóa K từ t thành viên

Phương pháp: 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.

3.2. CẤU HÌNH HỆ THỐNG.

1/. Cấu hình phần cứng.

RAM : tối thiểu 512 MB

CPU : Intel core i3-540 @ 3.06GHz

2/. Phần mềm.

Hệ điều hành (OS) : Windows 7 : 32bit hoặc 64bit.

Chương trình chạy trên nền .NET framework 4.

3.3. CÁC THÀNH PHẦN CHƯƠNG TRÌNH.

Chương trình có 2 thành phần chính :

a). Chia sẻ khóa bí mật.

Phần chia sẻ khóa bí mật bao gồm các ô :

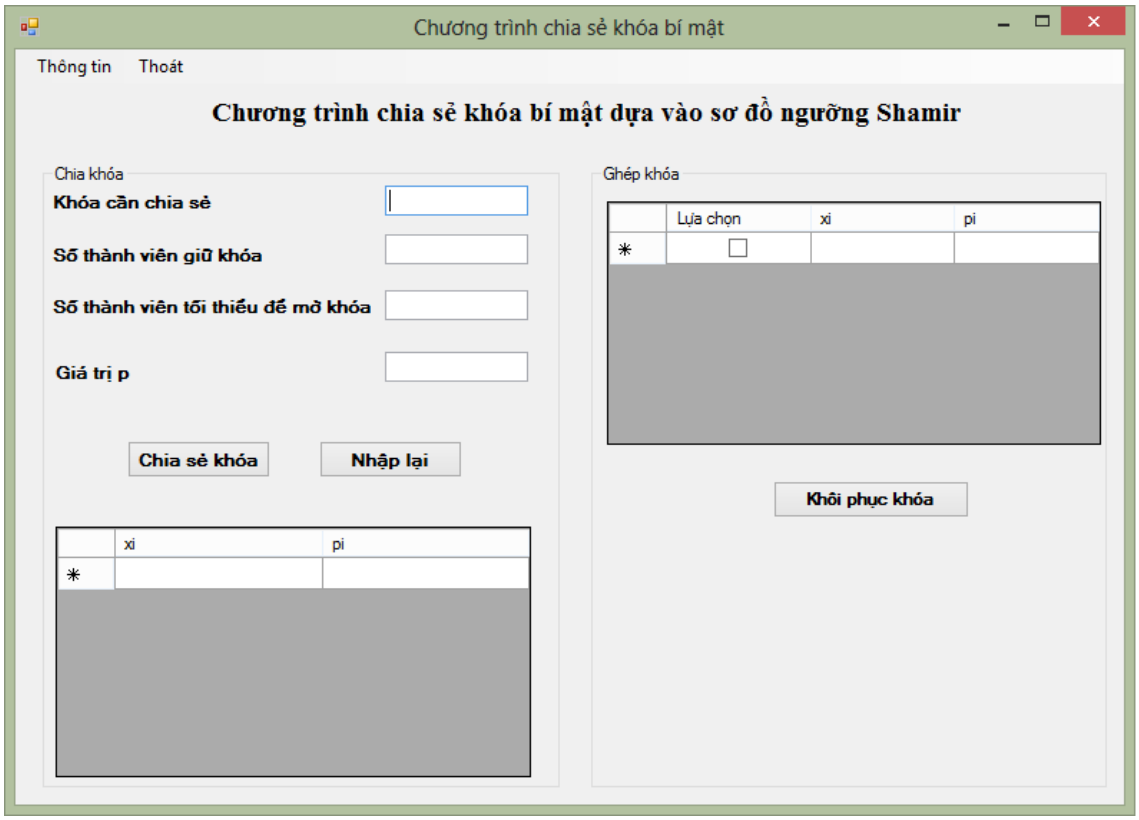
- Khóa cần chia sẻ.
- Số thành viên giữ khóa.
- Số thành viên tối thiểu để mở khóa.
- Giá trị p.
- Nút "Chia sẻ khóa".
- Nút "Nhập lại"
- Bảng kết quả sau khi chia khóa.

b). Khôi phục khóa bí mật.

Phần khôi phục khóa của chương trình bao gồm :

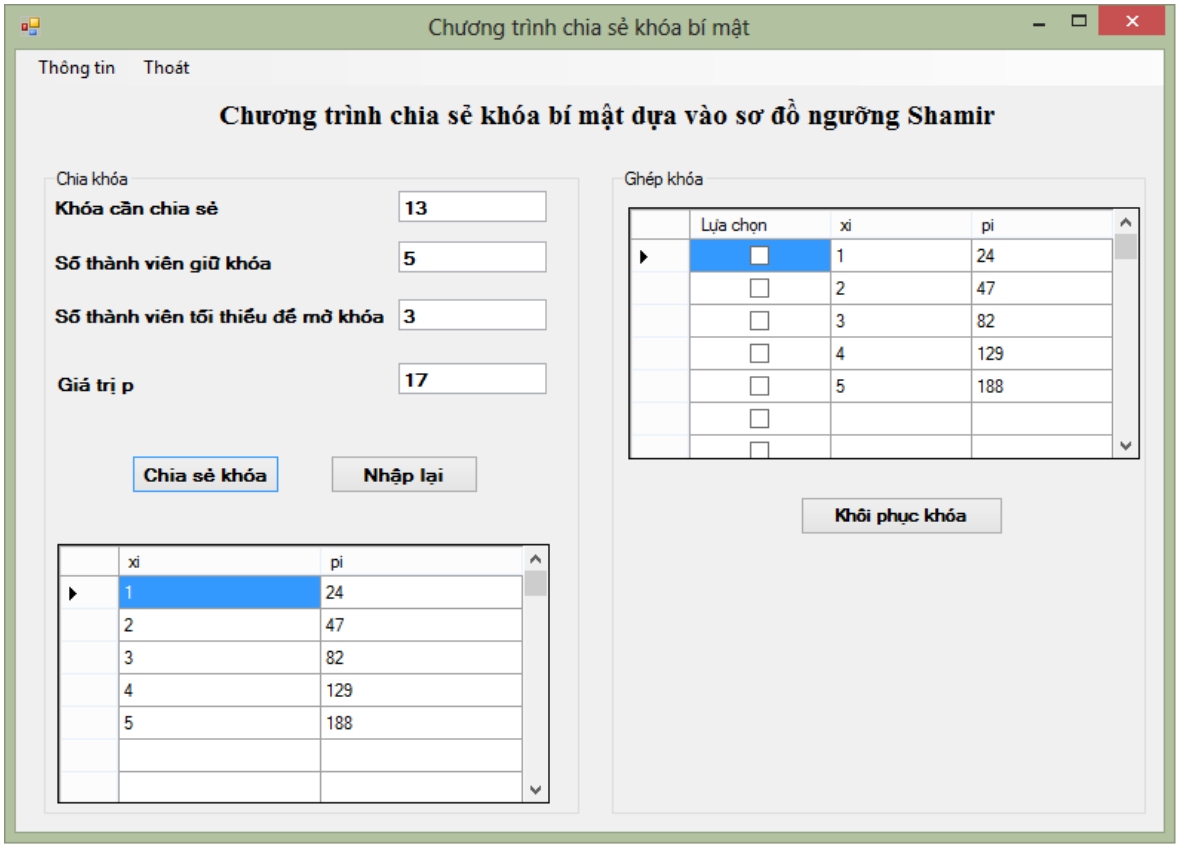
- Bảng chứa các giá trị khóa đã chia sẻ.
- Nút "Khôi phục khóa".
- Hộp thông báo kết quả khóa sau khi khôi phục khóa.

3.4. HƯỚNG DẪN SỬ DỤNG CHƯƠNG TRÌNH.



Hình 3.1. Giao diện chương trình chia sẻ khóa bí mật

3.4.1. Chia sẻ khóa bí mật.



Hình 3.2. Hướng dẫn chia khóa bí mật

Các bước thực hiện :

- Bước đầu tiên ta nhập giá trị khóa cần chia sẻ.
- Nhập số lượng thành viên cần chia sẻ : Chính là số lượng thành viên giữ khóa.
- Nhập số lượng thành viên tối thiểu để có thể mở khóa.
- Nhập giá trị p (p ở đây là một số nguyên tố).
- Click vào nút "Chia sẻ khóa", và kết quả sẽ được hiện thị ra bảng kết quả. Ta đem trao giá trị P_i cho người thứ X_i tương ứng.
- Click vào nút "Nhập lại" nếu muốn nhập lại các giá trị từ đầu.

Ví dụ :

Nhập các thông tin cần thiết ban đầu như hình 3.2 thì ta sẽ được kết quả trong bảng phía dưới như sau :

Người thứ 1 giữ mảnh khóa có giá trị : 24

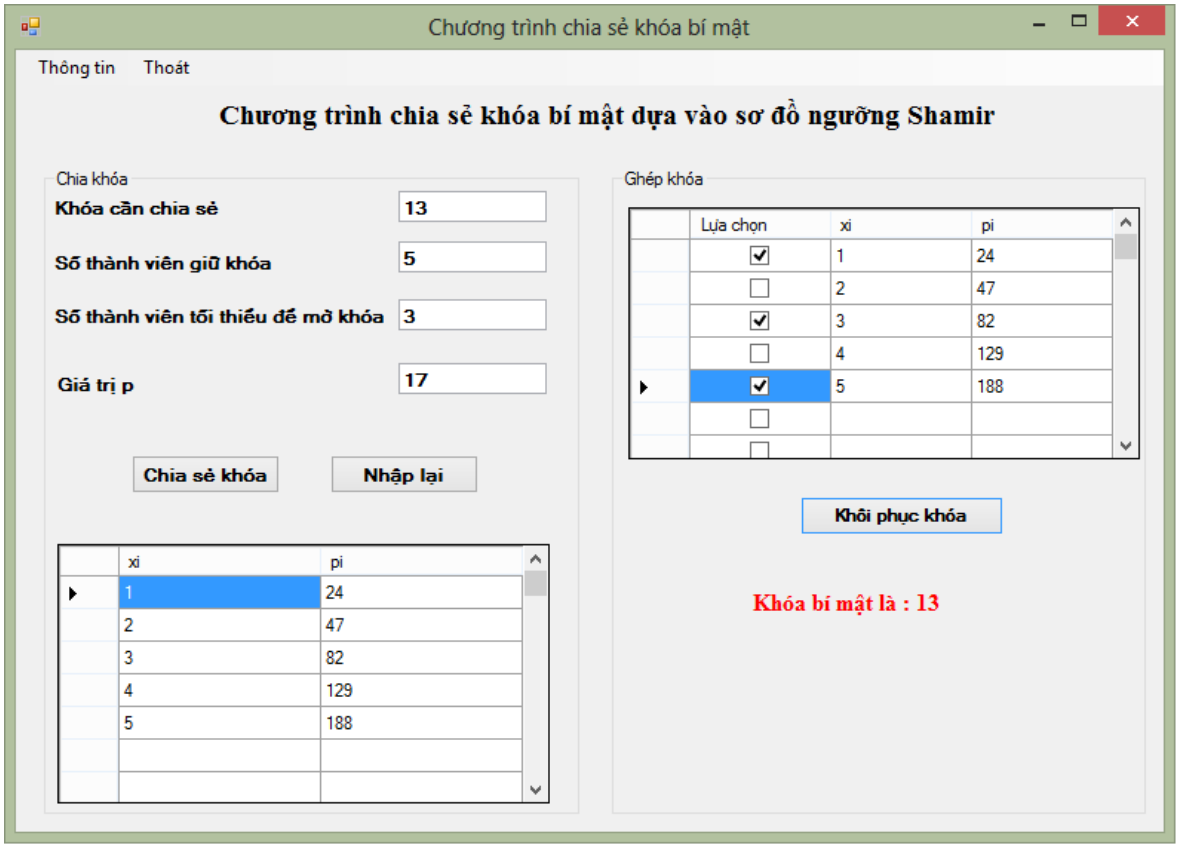
Người thứ 2 giữ mảnh khóa có giá trị : 47

Người thứ 3 giữ mảnh khóa có giá trị : 82

Người thứ 4 giữ mảnh khóa có giá trị : 129

Người thứ 5 giữ mảnh khóa có giá trị : 188

3.4.2. Khôi phục khóa bí mật.



Hình 3.3. Hướng dẫn ghép các mảnh khóa bí mật

Các bước thực hiện :

- Tại bảng chứa các mảnh khóa đã chia, ta tích chọn vào cột "Lựa chọn" để chọn các mảnh khóa đem đi khôi phục (Số lượng lựa chọn phải lớn hơn hoặc bằng số lượng tối thiểu thành viên có thể ghép khóa.).
- Click vào nút "Khôi phục khóa". Kết quả sẽ được hiển thị ra phía bên dưới.

KẾT LUẬN

Đồ án tốt nghiệp có 2 kết quả chính :

1. Về mặt lý thuyết, Đồ án tốt nghiệp đã trình bày :

- Tổng quan về An Toàn Thông Tin.
- Tổng quan về bỏ phiếu điện tử.
- Vấn đề chia sẻ bí mật và ứng dụng trong bỏ phiếu điện tử.

2. Về mặt thực hành, Đồ án tốt nghiệp đã thử nghiệm chương trình : Chia sẻ khóa bí mật dựa vào sơ đồ ngưỡng Shamir.

Chương trình chia sẻ khóa bí mật dựa vào sơ đồ ngưỡng Shamir bao gồm 2 phần chính là :

- Chia sẻ khóa bí mật.
- Khôi phục khóa bí mật.

TÀI LIỆU THAM KHẢO

1. ***" Giáo trình An toàn dữ liệu "*** – PGS. TS Trịnh Nhật Tiến, Đại học Công Nghệ, Đại học Quốc Gia Hà Nội.

2. ***"Về một quy trình bỏ phiếu từ xa"*** -Trịnh Nhật Tiến, Trương Thị Thu Hiền, Đại học Công Nghệ, Đại học Quốc Gia Hà Nội.

3. Website ***: www.tailieu.vn***

PHỤ LỤC

1). Code chương trình chia sẻ khóa (ngôn ngữ lập trình vb.net) :

```
Dim p As Integer
   Dim k As Double
   Dim m As Integer
   Dim t As Integer
   Dim kt As Integer
   Dim a() As Double
   Private Sub bt_chia_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles bt_chia.Click

      If txt_k.Text = "" Or txt_m.Text = "" Or txt_p.Text = "" Or txt_t.Text = ""
Then
         MessageBox.Show("Bạn phải điền đầy đủ thông tin vào các ô !")
      Else
         p = Convert.ToDouble(txt_p.Text)
         k = Convert.ToDouble(txt_k.Text)
         m = Convert.ToDouble(txt_m.Text)
         t = Convert.ToDouble(txt_t.Text)

         ReDim a(0 To p)
         Dim y(0 To p) As Double
         Dim tg(0 To p) As Double
         Dim GetNumber As New Random
         DataGridView1.Rows.Add(100)
         DataGridView2.Rows.Add(100)
         kt = 0
         For i = 2 To p - 1 Step 1
            If p Mod i = 0 Then
               kt = 1
```

```
            End If
        Next
        If kt = 1 Then
            MessageBox.Show("Giá trị p phải là số nguyên tố !")
        Else
            For i = 1 To (t - 1) Step 1
                a(i) = GetNumber.Next(1, p)
            Next
            For j = 1 To m Step 1
                tg(j) = 0
                For i = 1 To (t - 1) Step 1
                    tg(j) = tg(j) + (a(i) * j ^ (i))
                Next
                y(j) = (k + tg(j))
                DataGridView1.Item(0, j - 1).Value() = j.ToString
                DataGridView1.Item(1, j - 1).Value() = y(j).ToString
                DataGridView2.Item(1, j - 1).Value() = j.ToString
                DataGridView2.Item(2, j - 1).Value() = y(j).ToString

            Next
        End If
    End If
End Sub
```

2). Code chương trình khôi phục khóa (ngôn ngữ lập trình vb.net) :

```
Private Sub bt_ghep_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles bt_ghep.Click
    Dim pt(100, 100) As Integer
    Dim b(100) As Integer
    Dim y(0 To p) As Integer
    Dim tg(0 To p) As Integer
    Dim n As Integer, aa As Integer, s As Integer, jj As Integer, kk As Integer
```

```
        Dim i1, i2 As Integer, ii As Integer
        n = t
        Dim c(n, n + 1)
        jj = 0
        i1 = 0
        i2 = 0
        For j = 0 To m Step 1
            If DataGridView2.Item(0, j).Value <> Nothing Or DataGridView2.Item(0,
j).Value = 1 Then
                i2 = i2 + 1
            End If
        Next
        If i2 < t Then
            MessageBox.Show("Bạn phải chọn số người ghép khóa tối thiểu bằng " +
txt_t.Text.ToString)
            For j = 0 To m Step 1
                DataGridView2.Item(0, j).Value = 0
            Next
        Else
            If i2 > t Then
                MessageBox.Show("Bạn nên chọn số người ghép khóa bằng " +
txt_t.Text.ToString)
                For j = 0 To m Step 1
                    DataGridView2.Item(0, j).Value = 0
                Next
            Else
                For j = 0 To m Step 1
                    If DataGridView2.Item(0, j).Value <> Nothing Or
DataGridView2.Item(0, j).Value = 1 Then
                        i1 = i1 + 1
```

```
                b(i1) = DataGridView2.Item(2, j).Value()
                c(i1, 1) = 1
                For ii = 2 To n
                    c(i1, ii) = (j + 1) ^ (ii - 1)
                Next
                c(i1, n + 1) = b(i1)
            End If
        Next

        For i = 1 To n
            s = c(i, i)
            For j = 1 To n + 1
                c(i, j) = c(i, j) / s
            Next j
            For j = 1 To n
                If j <> i Then
                    aa = c(j, i)
                    For kk = 1 To n + 1
                        c(j, kk) = c(j, kk) - aa * c(i, kk)
                    Next kk
                End If
            Next j
        Next
        For i = 1 To n
            a(i - 1) = c(i, n + 1)
        Next i
        lb_k.Text = "Khóa bí mật là : " + a(0).ToString
    End If
  End If
End Sub
```