MỤC LỤC

LỜI NÓI ĐẦU 1

Chương 1. **MỘT SỐ KHÁI NIỆM CƠ BẢN** 2

1.1. TỔNG QUAN VỀ AN TOÀN THÔNG TIN 2

1.1.1. An toàn thông tin. 2

1.1.2. Tại sao cần bảo đảm an toàn thông tin ? 3

1.1.3. Nội dung của an toàn thông tin. 4

1.1.4.Các loại hành vi xâm phạm an toàn thông tin. 5

1.1.5. Các chiến lược an toàn hệ thống. 6

1.1.6. An toàn thông tin bằng mã hóa. 7

1.1.7. Vai trò của hệ mã hóa. 7

1.1.8. Tiêu chuẩn đánh giá hệ mật mã 9

1.2. MỘT SỐ KHÁI NIỆM TRONG SỐ HỌC 10

1.2.1. Ước chung lớn nhất, bội chung nhỏ nhất 10

1.2.1.1. Ước số và bội số 10

1.2.1.2. Ước chung lớn nhất, bội chung nhỏ nhất. 10

1.2.2.Quan hệ " Đồng dư " 11

1.2.2.1. Khái niệm 11

1.2.2.2. Các tính chất của quan hệ "Đồng dư" 11

1.2.3. Số nguyên tố 11

1.2.3.1. Khái niệm 11

1.2.3.2. Định lý về số nguyên tố 11

1.2.4.Khái niệm nhóm, nhóm con, nhóm Cyclic 12

1.2.5. Phần tử nghịch đảo 13

1.2.6. Các phép tính cơ bản trong không gian modulo 14

1.2.7. Độ phức tạp của thuật toán 15

1.3. CÁC HỆ MÃ HÓA 16

1.3.1. Tổng quan về mã hóa dữ liệu 16

1.3.1.1. Khái niệm mã hóa dữ liệu 16

1.3.1.2. Phân loại hệ mã hóa 17

1.3.2. Hệ mã hóa công khai 18
1.3.2.1. Hệ mã hóa RSA 18
1.3.2.2. Hệ mã hóa Elgamal 19
1.3.3. Hệ mã hóa đối xứng – cổ điển 20
1.3.4. Hệ mã hóa đối xứng DES 25
1.4. CHỮ KÝ SỐ 28
1.4.1. Giới thiệu 28
1.4.2. Phân loại Chữ ký số 30
1.4.3. Một số chữ ký số 32
1.4.3.1. Chữ ký RSA 32
1.4.3.2. Chữ ký ELGAMAL 33
1.4.3.3. Chữ ký Schnoor 34
1.4.3.4. Chữ ký mù 35
1.5. TỔNG QUAN VỀ TIỀN ĐIỆN TỬ 38
1.5.1. Tiền điện tử 38
1.5.1.1. Khái niệm 38
1.5.1.2. Cấu trúc tiền điện tử 39
1.5.1.3. Tính chất tiền điện tử 40
1.5.1.4. Mô hình giao dịch mua bán bằng Tiền Điện Tử 42
1.5.1.5. Quy trình thanh toán bằng Tiền Điện Tử 43
1.5.2. Qui Trình Sử Dụng Tiền Điện Tử 45
1.5.3. Vấn đề rút Tiền Điện Tử 45
Chương 2. **MỘT SỐ BÀI TOÁN AN TOÀN THÔNG TIN TRONG GIAI ĐOẠN RÚT TIỀN ĐIỆN TỬ** 46
2.1. MỘT SỐ BÀI TOÁN 46
2.1.1. Bài toán bảo vệ thông tin yêu cầu rút tiền 46
2.1.2. Bài toán thẩm tra hồ sơ rút tiền 46
2.1.3. Bài toán ẩn danh đồng tiền 46
2.1.4. Bài toán phòng tránh khai man giá trị đồng tiền 46
2.1.5. Bài toán bảo vệ đồng tiền trên đường truyền 46

2.2. PHƯƠNG PHÁP GIẢI QUYẾT 46
2.2.1. Giải quyết bài toán bảo vệ thông tin yêu cầu rút tiền 46
2.2.2. Giải quyết bài toán thẩm tra hồ sơ rút tiền.....47
2.2.3. Giải quyết bài toán ẩn danh đồng tiền.....47
2.2.4. Giải quyết bài toán phòng tránh khai man giá trị đồng tiền.....48
2.2.5. Giải quyết bài toán bảo vệ đồng tiền trên đường truyền.....49
Chương 3. **THỬ NGHIỆM CHƯƠNG TRÌNH CHỮ KÝ MÙ**..... 50
3.1. BÀI TOÁN LẬP TRÌNH 50
3.2. CẤU HÌNH HỆ THỐNG 50
3.3. CÁC THÀNH PHẦN CỦA CHƯƠNG TRÌNH..... 50
3.4. HƯỚNG DẪN SỬ DỤNG CHƯƠNG TRÌNH..... 52
KẾT LUẬN..... 55
PHỤ LỤC 56

LỜI CÁM ƠN

Em xin chân thành cám ơn PGS.TS Trịnh Nhật Tiến, đã hướng dẫn tận tình cho em trong quá trình thực hiện bản đồ án tốt nghiệp này. Đồng thời, em xin cảm ơn các thầy cô bộ môn công nghệ thông tin - trường Đại Học Dân Lập Hải Phòng đã trang bị cho em những kiến thức cơ bản, lam lền tảng để em có thể hoàn thành bản đồ án tốt nghiệp này.

Em xin cam đoan bản đồ án tốt nghiệp hoàn toàn do em tự viết dưới sự hướng dẫn của PGS.TS Trịnh Nhật Tiến.

LỜI NÓI ĐẦU

Ngày nay cùng với sự phát triển vượt bậc về khoa học công nghệ, sự mở rộng và phổ biến của Internet. Từ những nhu cầu thực tế đã thúc đẩy sự phát triển thương mại điện tử. Từ những hình thức thanh toán đơn giản đến nhu cầu thanh toán hiện đại, đòi hỏi phải có những hình thức thanh toán thông minh, an toàn. Điều đó dẫn đến công nghệ thanh toán điện tử ra đời và một trong những công nghệ đó là thanh toán **tiền điện tử**.

Trên toàn thế giới, **tiền điện tử** đã và đang được ứng dụng thành công, đem lại lợi ích cho người dùng.Tuy nhiên trong quá trình sử dụng tiền điện tử đã nảy sinh một số vấn đề đáng quan tâm như: người dùng gian lận giá trị đồng tiền, tiêu nhiều lần một đồng tiền hay xác định danh tính người sở hữu đồng tiền.

Đồ án đi vào nghiên cứu một số bài toán trong giai đoạn rút tiền điện tử và trình bày những cách giải quyết phù hợp cho bài toán đề trên.

Mục đích của luận văn là nghiên cứu một số giải pháp khoa học cho các bài toán phát sinh trong quá trình rút tiền điện tử, so sánh, đánh giá ưu nhược điểm của các giải pháp và chỉ rõ giải pháp nào phù hợp với từng loại tiền điện tử.

Do thời gian và kiến thức còn nhiều hạn chế, nên quyển đồ án này sẽ còn nhiều thiếu sót. Kính mong sự hướng dẫn, góp ý thêm của thầy cô và bạn bè.

Em xin chân thành cảm ơn!

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 nghê 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 được 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 được 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 dụng 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. Tại sao cần bảo đảm an toàn thông tin ?

Ngày nay, sự xuất hiện của internet và mạng máy tính đã giúp cho việc trao đổi thông tin trở lên nhanh gọn,dễ dàng. E-mail 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 trên mạng…

Tuy nhiên lại phát sinh những vấn đề mới. Thông tin quan trọng nằm ở kho giữ liệu hay đang trên đường truyền có thể bị trộm cắp, có thể bị làm sai lệch, có thể bị giả mạo. Điều đó có thể ảnh hưởng tới 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 tín tức về an ninh quốc gia là mục tiêu của các tổ chức tình báo trong và ngoài nước.

Theo số liệu CERT (Computer Emegency Response Team: Đội cấp cứu MT), số lượng các vụ tấn công trên Internet ngày một nhiều, quy mô của chúng mỗi ngày một lớn và phương pháp tấn công ngày càng hoàn thiện. Ví dụ cùng lúc tin tặc đã tấn công vào cả 100 000 máy tính có mặt trên mạng Internet, những máy tính của các công ty, các trường học, các cơ quan nhà nước, các tổ chức quân sự, các nhà băng, …cùng lúc ngưng hoạt động.

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 đã gửi cho họ. Khi họ 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 văn bản quan trọng phải ký dưới. Nhưng khi truyền trên mạng, văn bản hay giây 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 ký rất dễ giả mạo.

Để giải quyết tính hình trên, vấn đề bảo đảm An toàn thông tin đã được đặt ra trong lý luận cũng như trong 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 người ta quen 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.

1.1.3. Nội dung của an toàn thông tin.

An toàn thông tin bao gồm các nội dung sau:

- Tính bí mật: Tính kín đáo riêng tư của thông tin.
- Tính toàn vẹn: Bảo vệ thông tin, không cho phép sửa đổi thông tin trái phép.
- Tính xác thực của thông tin, bao gồm xác thực đối tác (bài toán nhận danh), xác thực thông tin trao đổi.
- Tính trách nhiệm: Đảm bảo người gửi thông tin không thể thoái thác về trách nhiệm thông tin mình đã gửi.
- 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 đươc 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 điịnh được tốt các giải pháp để giảm thiểu các thiệt hại.

1.1.4.Các 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 khí 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 nhậm 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 nhưng biện pháp ngăn chặn hiệu quả.

Vi phạm thụ động là dạng vi phạm có thể làm thay đổi nội dung, xóa bỏ, làm trễ, 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.

1.1.5. 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 tàu nguyên nhất định.

2/. Bảo vệ theo chiều sâu

Nguyên tắc này nhắc nhở chúng ta: Không nên dựa vào một chế độ an toàn nào dù cho chúng rất mạnh, mà nên tạo nhiều cơ chế an toàn để tương hỗ lần 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 về 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.

1.1.6. An toàn thông tin bằng mã hóa.

Lạp mã bao gồm hai quá trình : mã hóa và giải mã. 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.

1.1.7. Vai trò của hệ mã hóa.

Các hệ mã hóa phải thực hiên được các vai trò sau:

-Hệ mật mã phải che dấu được nội dung của văn bản rõ để đàm bảo sao cho chỉ người chủ hợp pháp của thông tin mới có quyền truy cập thông tin, hay nói cách khác là chống truy cập không đúng quyền hạn.

- Tạo ra các yếu tố xác thực thông tin, đảm bảo thông tin lưu hành trong hệ thống đến người nhận hợp pháp là xác thực.

- Tổ chức các sơ đồ chữ ký điện tử, đảm bảo không có hiện tượng giả mạo, mạo danh để gửi thông tin trên mạng.

Ưu điểm lớn nhất của bất kỳ hệ mã hóa nào đó là có thể đánh giá được độ phức tạp tính toán mà "kẻ địch" phải giải quyết bài toán để có thế lấy được thông tin của dữ liệu đã được mã hóa. Tuy nhiên mỗi hệ khóa có một số ưu và nhược điểm khác nhau, nhưng nhờ đánh giá được độ phức tạp tính toán mà ta có thể áp dụng các thuật toán mã hóa khác nhau cho từng ứng dụng cụ thể tùy theo độ yêu cầu về độ an toàn.

Các thành phần của một hệ mã hóa:

Định nghĩa

Một hệ mã hóa là một bộ 5(P,C,K,E,D) thỏa mãn các điều kiện sau:

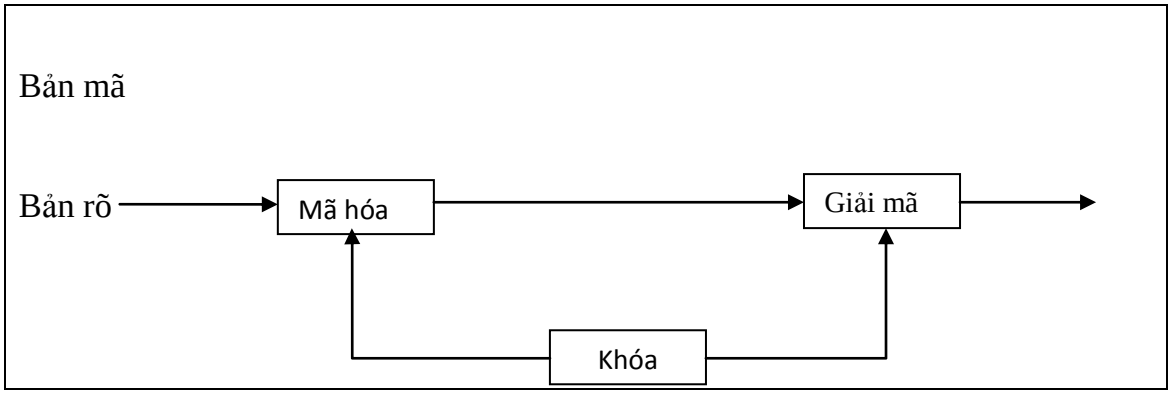
- P là một tập hợp hữu hạn các bản rõ(Plain Text), nó được gọi là không gian bản rõ.

- C là tập các hữu hạn các bản mã (Crypto), nó còn được gọi là không gian các bản mã. Mỗi phần tử của C có thể nhận được bằng cách áp dụng phép mã hóa E_k lên một phần tử của P, với k∈ K.

- K là tập hữu hạn các khóa hay còn gọi là không gian khóa. Đối với mỗi phần từ k của K được gọi là một khóa. Số lượng của không gian khóa phải đủ lớn để "kẻ địch" không có đủ thời gian thử mọi khóa có thể(phương pháp vét cạn).

- Đối với mỗi k∈ K có một quy tắc mã e_k: P→ C và một quy tắc giải mã tương ứng d_k∈ D. Mỗi e_k :P→ C và d_k :C→ P là những hàm mà:

$d_k(e_k(x)) = x$ với mọi bản rõ x ∈ P.



Hình 1: quá trình mã hóa.

1.1.8. Tiêu chuẩn đánh giá hệ mật mã.

Để đánh giá một hệ mã hóa người ta thường đánh giá thông qua các tính chất sau:

1/. Độ an toàn:

Một hệ mã hóa được đưa vào sử dụng, điều đầu tiên phải có độ an toàn cao. Ưu điểm của mã hóa là có thể đánh giá được độ an toàn thông qua độ an toàn tính toán mà không cần phải cài đặt. Một hệ mã hóa được coi là an toàn nếu để ohá hệ mã hóa này phải dùng **n** phép toán. Mà để giải quyết **n** phép toán cần thời gian vô cùng lớn, không thể chấp nhận được.

Một hệ mã hóa được gọi là tốt thì nó cần phải đảm bảo các tiêu chuẩn sau:

- Chúng phải có phương pháp bảo vệ mà chỉ dựa trên sự bí mật của các khóa, công khai thuật toán.
- Khi cho khóa công khai e_k và bản rõ P thì dễ dàng tính được ek(P) = C. Ngược lại khi cho d_k và bản mã C thì dễ dàng tính được $d_k(M)=P$. Khi không biết d_k thì không có khả năng tìm được M từ C, nghĩa là khi cho hàm $f:X \rightarrow Y$ thì việc tính $y = f(x)$ với mọi $x \in X$ là dễ còn việc tìm x khi biết y lại là vấn đề khó và nó được gọi là hàm một chiều.
- Bản mã C không được có các đặc điểm gây chú ý, nghi ngờ.

2/. Tốc độ mã và giải mã:

Khi đánh giá hệ mã hóa chúng ta phải chú ý đến tốc độ mã hóa và giải mã. Hệ mã hóa tốt thì thời gian mã hóa và giải mã nhanh.

3/. Phân phối khóa:

Một hệ mã hóa phụ thuộc vào khóa, khóa này được truyền công khai hay truyền khóa bí mật. Phân phối khóa bí mật thì chi phí sẽ cao hơn so với các hệ mã hóa có khóa công khai. Vì vậy đây cũng là một tiêu chí khi lựa chọn hệ mã hóa.

1.2. MỘT SỐ KHÁI NIỆM TRONG SỐ 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 :

$$n=P_1^{n_1}.P_1^{n_2}\ldots P_1^{n_k}$$

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 $\phi(n)$ và gọi là hàm *Euler*.

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

Định lý về Hàm Euler :

Nếu n là tích của hai số nguyên tố n = p.q, thì $\phi(n) = \phi(p).\ \phi(q) = (p-1)(q-1)$

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 $e \in G$: $e * x = x * e = x, \ \forall x \in G$

+ Tính chất tồn tại phần tử nghịch đảo $x' \in G$: $x' * x = x * x' = e$

b) Nhóm con của G là tập $S \subset G$, $S \neq \emptyset$, 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 $x * y \in S$ với mọi $x, y \in S$.

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

c) Nhóm cyclic:

(G, *) là nhóm được sinh ra bởi một trong các phần tử của nó. Tức là có phần tử $g \in G$ mà với mỗi $a \in G$, đều tồn tại số $n \in N$ 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.

Nhóm $(Z_n^*$, phép nhân mod n)

+ Kí hiệu $Z_n = \{0, 1, 2,\ldots, n-1\}$ là tập các số nguyên không âm < n.

Z_n và phép cộng (+) lập thành nhóm Cyclic có phần tử sinh là 1, phần tử trung lập e=0.

$(Z_n, +)$ gọi là nhóm cộng, đó là nhóm hữu hạn có cấp n.

+ Kí hiệu $Z_n^* = \{x \in Z_n$, x là nguyên tố cùng nhau với n$\}$. Tức là x phải $\neq 0$.

Z_n^* được gọi là Tập thặng dư thu gọn theo mod n, có phần tử là $\phi(n)$.

Z_n^* với phép nhân mod n, lập thành một nhóm (nhóm nhân), phần tử trung lập e = 1.

Tổng quát $(Z_n^*$, phép nhân mod n) không phải là nhóm Cyclic.

Nhóm nhân Z_n^* là Cyclic chỉ khi n có dạng: 2, 4, p^k, hay $2p^k$ với p là nguyên tố lẻ.

1.2.5. Phần tử nghịch đảo

1/. Khái niệm.

Cho $a \in Z_n$. Nếu tồn tại $b \in Z_n$sao cho $a*b \equiv 1 \pmod n$, 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 $\in Z_n$. 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 $\in Z_n$, 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 $\in Z_n$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 thựchiện 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 $\mathbf{ke} \in \mathbf{K}$, 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 $\mathbf{d}_{kd} \in \mathbf{D}$, $\mathbf{d}_{kd}$: $\mathbf{C} \rightarrow P$,

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

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

Mã hóa và giải mã

Người gửi G →→$\mathbf{e}_{ke}(\mathbf{T})$→→Người nhận N

(có khóa lập mã **ke**) (có khóa giải mã **kd**)

↑

Tin tặc có thể trộm bản mã $\mathbf{e}_{ke}(\mathbf{T})$

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 dung chung mội 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 dung 1 khóa để mã hóa, dung 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 đẻ 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 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 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 $\phi(\mathbf{n}) = (\mathbf{p-1}).(\mathbf{q-1})$. Chọn khóa công khai b <ϕ(n), nguyên tố với ϕ(n).

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

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

Với ***Bản rõ*** x ∈ P và ***Bản mã*** y ∈ C, định nghĩa:

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

Hàm Giải mã: $x = d_k(y) = y^a \mathrm{mod}\ n$

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 $\phi(n) = (p-1).\ (q-1) = 52 * 60 = 3120$.

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

Ví dụ chọn b = 71.

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

Từ $a*b \equiv 1\ (\mathrm{mod}\ \phi(n))$, 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: $\mathbf{c}_i = m_i^b \mathrm{mod}\ n = m_i^{71} \mathrm{mod}\ 3233$, 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: $m_i = c_i^{\ a} \bmod n = c_i^{\ 791} \bmod 3233$, 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, $\phi(n)$.

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.

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 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".

a. 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.

b. 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.

c. 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 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 các khóa (a,b) có thể là 12*26 = 312. Rất ít !

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

d. 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}).

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

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 mã 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.

e. 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, …,k_m) gồm m phần tử, ta định nghĩa:

* Mã hóa Y = (y_1,y_2, …,y_m) = e_k(x_1,x_2,…, x_m) = ($x_{k(1)}$, $x_{k(2)}$, …, $x_{k(m)}$)

* Giải mã X = (x_1,x_2,…, x_m) = d_k(y_1,y_2, …,y_m) =($y_{k(1)}^{-1}$,$y_{k(2)}^{-1}$,…, $y_{k(m)}^{-1}$)

- Trong đó k^{-1} =π^{-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! + …+ m! trong đó m ≤ 26.

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

f. 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, …,y_m) = e_k(x_1,x_2,…, x_m) = (x_1,x_2,…, x_m) * k

* Hàm giải mã: X = (x_1,x_2,…, x_m) = d_k(y_1,y_2, …,y_m) = (y_1,y_2, …,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 đối xứng DES

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.

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

b. 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**:

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

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}, …, k_1.

Xuất phát (đầu vào) từ bản mã y, kết quả (đầu ra) là bản rõ x.

c. 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 chữ ký

Với mỗi $k \in K$, 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 $x \in P$, $y \in A$:

$Ver_k(x, y)$ = 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 đặc trưng kiểm tra chữ ký

1). Chữ ký có thể khôi phục thông điệp:

Ví dụ: Chữ ký RSA

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

Ví dụ: Chữ ký Elgamal

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

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

- 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 $\phi(n)$ = (q-1)(p-1)= (3-1)(5-1) =8

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

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

Ký số: chữ ký trên x=2 ∈ P là $y = Sig_k(x)= x^a \pmod n = 2^3 \pmod{15} = 8$, y ∈ A.

Kiểm tra chữ ký :

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

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

$\gamma = g^r \bmod \mathbf{p}$ 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 $g \in \mathbf{G}$, 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 $h = g^a \bmod n$.

**** Ký số***:

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

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

Ví dụ: **m** = 0110, $g^s h^c$ = 01010, thì (**m**, $g^s h^c$) = 011001010.

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

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

**** Kiểm tra chữ ký:***

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

Vì $g^s h^c = g^{r - ca}(g^a)^c = g^r$ (mod n), do đó H(**m**, $g^s h^c$)= H(**m**, g^r)= c.

1.4.3.4. Chữ ký mù

a. Chữ ký mù theo Sơ đồ chữ ký RSA

* Mục đích là có chữ ký RSA trên **m**:

Theo sơ đồ chữ ký RSA, chữ ký trên **m** là giá trị **y** = $\mathbf{m}^{a}$ (mod n).

*Các bước thực hiện:

Người nhận chữ ký: Làm "mù" thông điệp **m**, (hay "che giấu" **m**).

Phần tử "làm mù" **r** được chọn ngẫu nhiên: **r** $\in Z_n^*$.

Giá trị "mù" của **m** là: **z** = Blind**(m)** = **m** . $\mathbf{r}^{b}$(mod n). (**z** là thông điệp "mù").

Người ký: Tạo chữ ký trên **z**, (hay chữ ký "mù" trên **m**).

y-mu = Sig(**z**)= $\mathbf{z}^{a}$ (mod n)=(**m**. $\mathbf{r}^{b}$)^{a} (mod n)= $\mathbf{m}^{a}$ * $\mathbf{r}^{b\,a}$ (mod n)= $\mathbf{m}^{a}$ * **r**(mod n).

Người nhận chữ ký: Xoá mù trên chữ ký **y**-mu, Nhận được chữ ký **y** trên **m**.

UnBlind (**y**-mu)= **y**-mu / **r** =$\mathbf{m}^{a}$ * **r**(mod n) / **r**=$\mathbf{m}^{a}$(mod n).

Vídụ :

* Chọn p = 3, q = 5 => n = 15, $\phi(n)$ = 8.

chọn b = 3 => a= 3.

* Mục đích là có chữ ký RSA trên **m** =**2**.

Theo ví dụ trên, đó là giá trị **y** =$\mathbf{m^a}$ (mod n) = $\mathbf{2^3}$(mod 15) = **8**.

*Các bước thực hiện:

Người nhận chữ ký: Làm "mù" thông điệp **m** = **2**.

Phần tử "làm mù" được chọn là **r** = **4**.

Giá trị "mù" của **m** là **z** = Blind(**m**) = **m** . $\mathbf{r^b}$(mod n) = **2** . $\mathbf{4^3}$(mod 15) = 8.

Người ký: Tạo chữ ký trên **z**, (hay chữ ký "mù" trên **m**).

y-mu = Sig(**z**) = $\mathbf{z^a}$ (mod n) = $\mathbf{8^3}$(mod 15) = **2**.

Người nhận chữ ký: Xoá mù trên chữ ký **y**-mu.

Nhận được chữ ký trên **m** là **y**= $\mathbf{m^a}$ (mod n) = **8**.

UnBlind (**y**-mu)= **y**-mu / **r** =**2** / **4**(mod 15)= **8**.

b. Chữ ký mù theo Sơ đồ chữ ký Schnorr

**** Chữ ký mù Schnorr:***

*** Vòng 1. Người ký thực hiện**:

+ Chọn ngẫu nhiên, bí mật **r'** $\in \mathbf{Z}_q^*$.

+ Tính **t'** $= g^{r'} \pmod n$, gửi **t'** cho Người nhận chữ ký.

*** Vòng 2. Người nhận chữ ký thực hiện**:

Làm "mù" thông điệp cần ký.

+ Chọn ngẫu nhiên, bí mật γ, $\delta \in \mathbf{Z}_q^*$.

+ Tính **t** = **t'** $g^{\gamma} h^{\delta} \pmod n$, **c = H(m, t)**.

+ Tính **c'= c** - **δ**(mod **q**), gửi **c'** cho Người ký.

(Thông điệp **m** đã được làm "mù", người ký khó thể nhận ra).

*** Vòng 3. Người ký thực hiện**:

+ Tính **s'** = **r'** - **c'** **a** (mod **q**), gửi **s'** cho Người nhận.

*** Vòng 4. Người nhận chữ ký thực hiện:**

Xóa mù chữ ký.

+ Tính **s** = **s'** + $\gamma \pmod q$ và **c = H(m, t)**. Chữ ký là (**c, s**).

Chú ý:

- Người ký không biết **c**, **s**, vì chúng được làm mù bởi các tham số ngẫu nhiên γ, δ.

- Chữ ký là hợp lệ vì:

$$\mathbf{g^s h^c} = g^{s'+\gamma} h^{c'+\delta} = g^{r'-c'a+\gamma+c'a} h^{\delta} = t' g^{\gamma} h^{\delta} = \mathbf{t} \bmod n.$$

Như vậy **c = H(m, t) = H(m, $\mathbf{g^s h^c}$)**, tức là thỏa mãn điều kiện về chữ ký Schnorr.

1.5. TỔNG QUAN VỀ TIỀN ĐIỆN TỬ

1.5.1. Tiền điện tử

1.5.1.1. Khái niệm

Tiền điện tử (E-money, E-currency, Internet money, Digital money, Digital cash) là thuật từ vẫn còn mơ hồ và chưa được định nghĩa đầy đủ. Tuy nhiên có thể hiểu Tiền điện tử là loại tiền trao đổi theo phương pháp "điện tử", liên quan đến mạng máy tính và những hệ thống chứa giá trị ở dạng số (Digital stored value Systems).

Tiền điện tử cho phép người dùng thanh toán khi mua hàng, hay sử dụng các dịch vụ, nhờ truyền đi các "dãy số" từ máy tính (hay thiết bị lưu trữ như Smart Card) này với máy tính khác (Smart Card).

Cũng như dãy số (Serial) trên tiền dấy, dãy số của tiền điện tử là duy nhất. Mỗi "đồng tiền điện tử" được phát hành bở một tổ chức (ngân hàng) và biểu diễn một lượng tiền thật nào đó.

Tiền điện tử có loại ẩn danh (identified e-money), có loại định danh (anonymous identified e-money).

Tiền ẩn danh không tiết lộ thông tin định danh người sử dụng. Tính ẩn danh của tiền điện tử tương tự như tiền mặt thông thường. Tiền điện tử ẩn danh được rút từ một tài khoản, có thể được tiêu xài hay chuyển cho người khác mà không để lại dấu vết.

Có nhiều loại tiền ẩn danh, có loại ẩn danh đối với người bán, nhưng không ẩn danh với ngân hàng. Có loại ẩn danh hoàn toàn, ẩn danh với tất cả mọi người.

Tiền điện tử định danh tiết lộ thông tin định danh của người dùng. Nó tương tự như thẻ tín dụng, cho phép ngân hàng lưu dấu vết tiền khi luân chuyển.

Mỗi loại tiền chia thành hai dạng: trực tuyến (online) và không trực tuyến (offline).

Trực tuyến: nghĩa là cần phải tương tác với phía thứ ba để thực hiện giao dịch.

Không trực tuyến: nghĩa là có thể kiểm soát đc giao dịch, mà không cần liên quan trực tiếp đến phía thứ ba (ngân hàng).

Hiện nay có 2 hệ thống tiền điện tử chính: Thẻ thông minh(Smart card) hay phần mềm. Tuy nhiên chúng có chung đặc điểm cơ bản sau: tính an toàn, tính riêng tư, tính độc lập, tính chuyển nhượng, tính phân chia.

1.5.1.2. Cấu trúc tiền điện tử

Với mỗi hệ thống thanh toán điện tử, tiền điện tử có cấu trúc và định dạng khác nhau nhưng đều bao gồm các thông tin chính như sau:

Số seri của đồng tiền: giống như tiền mặt, số seri dùng để phân biệt các đồng tiền khác nhau. Mỗi đồng tiền điện tử sẽ có một seri duy nhất. Tuy nhiên, khác với tiền mặt, số seri trên tiền điện tử thường là mội dãy số được sinh ngẫu nhiên. Điều này có liên quan tới tính ẩn danh của người sử dụng.

Giá trị của đồng tiền: Mỗi đồng tiền điện tử sẽ có giá trị tương đương vớimột lượng tiền nào đó. Trong tiền mặt thông thường , mỗi tờ tiền có một giá trị nhất định(1$, 10$...), trong tiền điện tử, giá trị này có thể là một con số bất kì (7$,19$...).

Hạn định của đồng tiền: Để đảo bảo tính an toàn của đồng tiền và tính hiệu quả của hệ thống, các hệ thống thường giới hạn ngày hết hạn của đồng tiền. Một đòng tiền điện tử sau khi phát hành sẽ phải gửi lại ngận hàng trước thời điểm hết hạn.

Các thông tin khác: đây là các thông tin thêm nhằm phục vụ cho mục đích đảm bảo an toàm vào tính tin cậy của đồng tiền điện tử, ngăn chặn việc giả majo tiền điện tử và phát hiện các vi phạm (nếu có). Trong nhiều hệ thống các thông tin này giúp truy vết định danh người sử dụng có hành vi gian lận trong thanh toán điện tử.

Các thồn tin trên tiền điện tử được ngân hàng kí khóa bằng bí mật của mình. Bất kì người sử dụng nào cũng có thể kiểm tra tính hợp lệ của đồng tiền bằng các sử dụng khóa công khai của ngân hàng.

1.5.1.3. Tính chất tiền điện tử

Tiền điện tử cũng có một số đặc điểm tương tự tiền giấy: dùng để biểu diễn một lượng tiền nào đó, có thể chuyển nhượng được, không để lại dấu vết, có tính ẩn danh, có thể mang đi mang lại và đặc biệt có thể đổi được.

1/. Tính an toàn (Security)

* Đảm bảo đồng tiền điện tử không bị sao chép, không bị dử dụng lại.

* Sự giả mạo(forgery)

Các gian lận thường gặp trong hệ thống thanh toán là sự giả mạo. Tương tự như tiền giấy, có hai loại giả mạo đối với tiền điện tử.

- Giả mạo đồng tiền: tạo ra đồng tiền giả giống như thật, nhưng không có xác nhận rút tiền của ngân hàng.

- Tiêu một đồng tiền nhiều lần: là sử dụng cùng một đồng tiền nhiều lần (thuật ngữ tương đương như double spending, hay multiple spending, hay repeat spending).

2/.Tính xác thực

Do luôn có sự giả mạo, nên ta cần phải xác lập được các mức khác nhau về cách đánh giá tính xác thực.

- Nhận dạng người dùng: người dùng cần phải biết mình đang giao dịch với ai.

- Xác thực tính toàn vẹn thông điệp: đảo bảo bản copy của thông điệp hoàn toàn giống bản ban đầu.

3/.Tính riêng tư (Privacy)

Chưa thể định nghĩa một cách rõ ràng tính chất này của tiền điện tử. Đối với môt số người, tính riêng tư có nghĩa là sự bảo vệ chống lại "eavesdropping". Đối với một số người khác như David Chaum, "tính riêng tư" có nghĩa là trong quá trình thanh toán, người trả tiền phải được ẩn danh, không để lại dấu vết, ngân hàng không nói được tiền giao dịch là của ai.

Tính chất này nhằm bảo vệ người dùng, khó có thể truy vết, chấp nối mới quan hệ giữa người dùng với các giao dịch hay chi tiêu mà người đó thực hiện. Tính chất này cũng có thể thấy rõ trong các giao dịch bằng tiền mặt. Sau khi thanh toán, việc chứng minh người nào đã sở hữu số tiền đó trước đây là rất khó.

4/. Tính độc lập (Portability)

Tính chất này có nghĩa là sự an toàn của tiền điện tử không phụ thuộc vào vị trí địa lý. Tiền có thể được chuyển qua mạng máy tính hoặc lưu trữ vào các thiết bị nhớ khác nhau.

5/. Tính chuyển nhượng được (Transferrability)

Người dùng Tiền điện tử có thể chuyển giao quyền sở hữu đồng tiên điện tử cho nhau. Tính chuyển nhượng được là một tính chất rất quan trọng cho việc tiêu tiền điện tử, thực sự giống với tiêu tiền mặt thông thường.

Tuy vậy, có một số vấn đề nảy sinh mà hệ thống vẫn cần giải quyết:

- Kích thước dữ liệu tăng lên sau mỗi lần chuyển nhượng. Vì vậy, cần giới hạn số lần chuyển nhượng tối đa cho phép.

- Phát hiện giả mạo và tiêu một đồng tiền nhiều lần có thể quá trễ, khi đồng tiền đã được chuyển nhượng nhiều lần.

- Người dùng có thể nhận ra đồng tiền của mình, nếu nó lại xuất hiện trong một lần giao dịch khác.

6/. Tính phân chia được (Divisibility)

Người dùng có thể phân chia đồng tiền của mình thanh những mảnh có giá trị nhỏ hơn, với điều kiện tổng giá trị các mảnh nhỏ bằng giá trị đồng tiền ban đầu. Tiền điện tử thực chất là một dãy số bị mã khóa, nên không phải hệ thống nào cũng thực hiện được việc chia dãy số này thành các đồng tiền có giá trị nhỏ hơn.

1.5.1.4. Mô hình giao dịch mua bán bằng Tiền Điện Tử

Mô hình giao dịch mua bán bằng tiền điên tử có 3 giao dịch với 3 đối tượng:

* Rút tiền: Ông A chuyển tiền tử tài khoản ở ngân hàng vào "túi" của mình ("túi " có thể là Smart Card hay máy tính).

* Thanh toán: Ông A chuyển tiền từ "túi" của mình đến "túi " ông B.

* Gửi tiền: Ông B huyển tiền nhận được vào tài khoản của mình ở ngân hàng. Mô hình này có thể thực hiện bằng 2 cách: trực tuyến, không trực tuyết.

Trực tuyến:

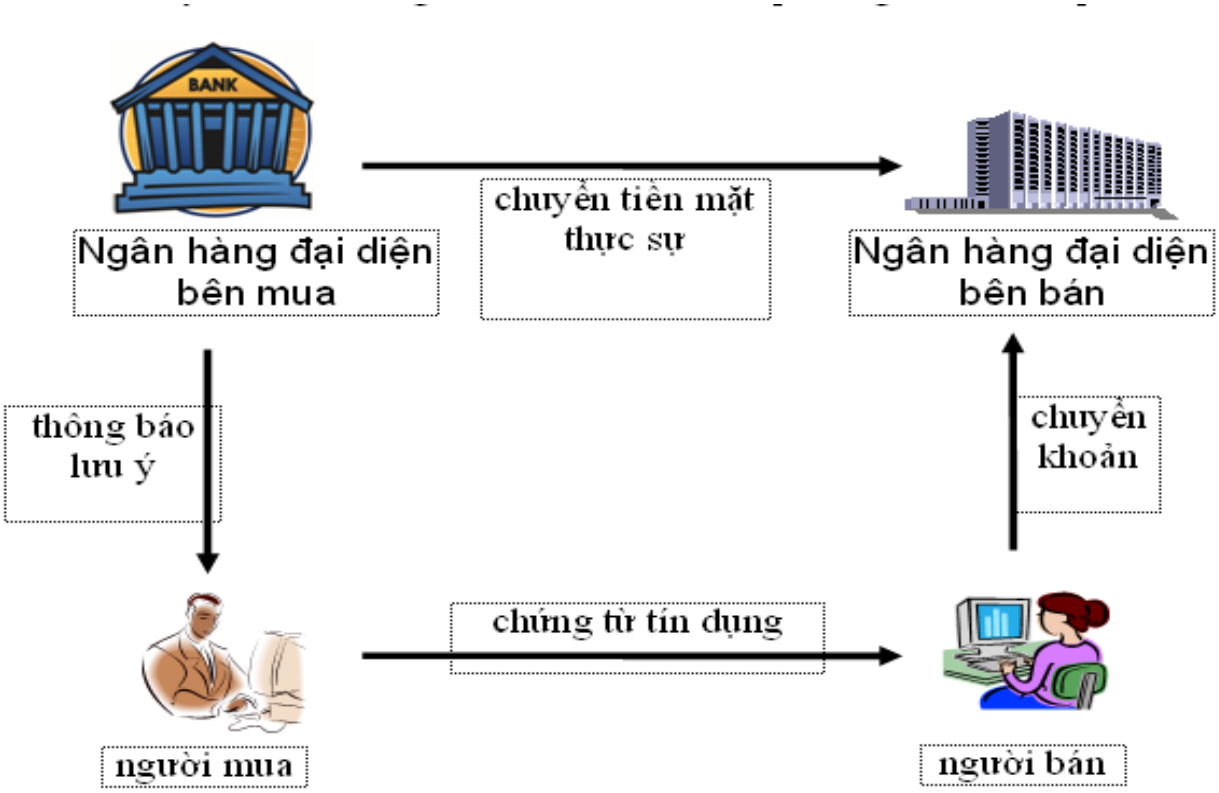
Ông B liên lạc với ngân hàng để kiểm tra tính hợp lệ của đồng tiền trước khi thanh toán và phân phối hàng. Thanh toán và gửi tiền được tiến hành đồng thời.

Thanh toán trực tuyến cần thiết cho gaio dịch có giá trị lớn. Hệ thống yêu cầu phải liên lạc với ngân hàng trong suốt mỗi lần giao dịch, vì thế chi phí nhiều hơn (tiền và thời gian).

1.5.1.5. Quy trình thanh toán bằng Tiền Điện Tử

1/. Mô hình trả tiền sau.

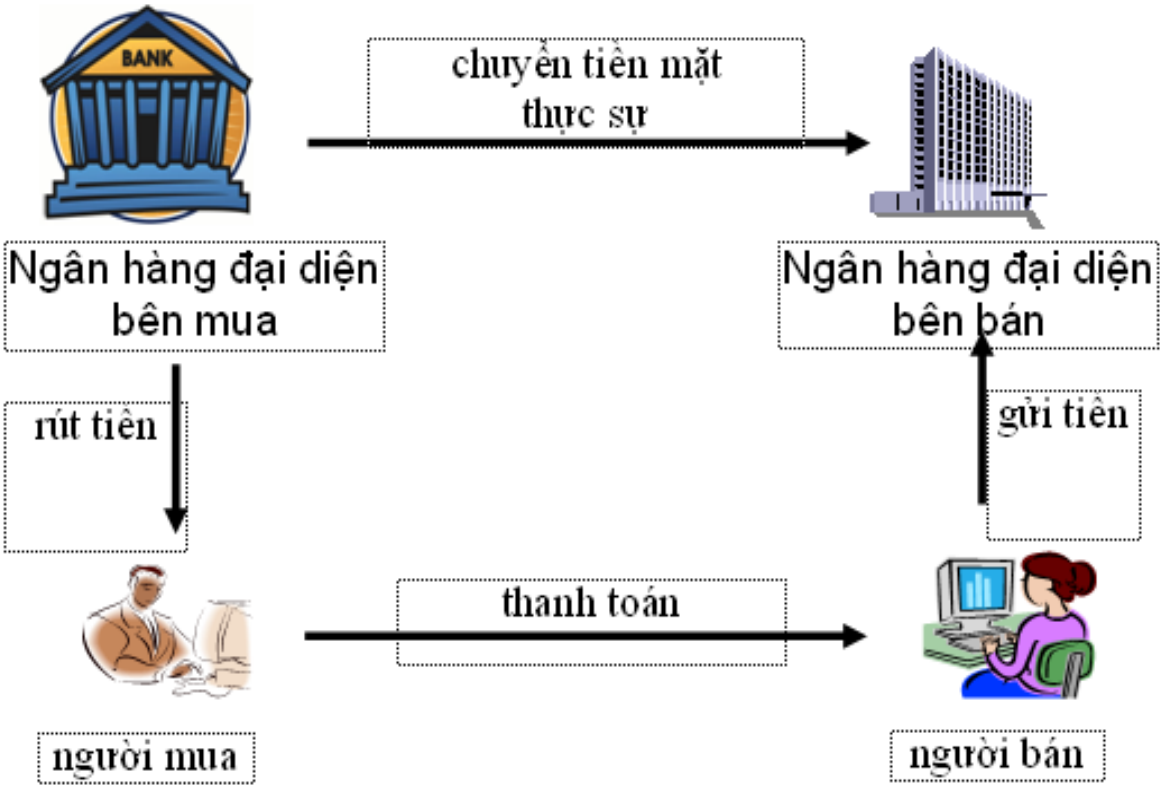
Thời điểm tiền mặt được rút ra khỏi tài khoản bên mua để chuyển sang bên bán, xảy ra ngay (pay-now) hoặc sau (pay-later) giao dịch mua bán. Hoạt động của hệ thống dựa trên nguyên tắc tín dụng (Credit crendental). Nó còn được gọi là *mô hình mô phỏng Séc* (Cheque-like model).



Hình 2: Mô hình trả tiền sau

2/.Mô hình trả tiền trước

Khách hàng liên hệ với ngân hàng (hay công ty môi giới - Broker) để có được chứng từ do ngân hàng phát hành. Chứng từ hay Đồng tiền số này mang dấu ấn của ngân hàng, được đảm bảo bởi ngân hàng và do đó có thể dùng ở bất cứ nơi nào đã có xác lập hệ thống thanh toán với ngân hàng này.



Hình 2: Mô hình trả tiền trước

1.5.2. Qui Trình Sử Dụng Tiền Điện Tử

1/. Giai đoạn 1: Rút tiền

Người có tiền cần sử dụng đến tiền, rút tiền từ ngân hàng.

2/. Giai đoạn 2: Trả tiền (chuyển tiền)

Người mua hàng chuyển tiền trả cho người bán.

3/. Giai đoạn 3: Gửi tiền

Người bán hàng gửi tiền vừa nhận được vào ngân hàng

1.5.3. Vấn đề rút Tiền Điện Tử

Các bước rút tiền:

B1: Người có tiền gửi yêu cầu rút tiền đến ngân hàng.

B2: Ngân hàng tiến hành kiểm tra thông tin tài khoản.

- Nếu tài khoản không đủ hoặc không có thì từ chối yêu cầu rút tiền.

- Nếu tài khoản thỏa mãn thì thực hiện bước 3.

B3: Cho phép rút tiền

- Người rút tiền tạo đồng tiền, và làm mù đồng tiền.

- Ngân hàng kí vào đồng tiền đã được làm mù và gửi trả lại cho người rút tiền.

- Người rút tiền nhận được đồng tiền và kiểm tra chữ kí trên đồng tiền, xóa mù trên đồng tiền người rút tiền sẽ nhận được chữ ký thật trên đồng tiền thật.

Chú ý:khi rút tiền cần đảm bảo "Ẩn danh" đồng tiền.

Chương 2. MỘT SỐ BÀI TOÁN AN TOÀN THÔNG TIN TRONG GIAI ĐOẠN RÚT TIỀN ĐIỆN TỬ

2.1. MỘT SỐ BÀI TOÁN

2.1.1. Bài toán bảo vệ thông tin yêu cầu rút tiền

Thông tin yêu cầu rút tiền trên đường truyền có thể bị lộ và bị sửa đổi trái phép

2.1.2. Bài toán thẩm tra hồ sơ rút tiền

Ngân hàng khi nhận được yêu cầu rút tiền cần thẩm tra yêu cầu đó

2.1.3. Bài toán ẩn danh đồng tiền

Thông tin về đồng tiền cần phải được giữ bí mật với ngân hàng.

2.1.4. Bài toán phòng tránh khai man giá trị đồng tiền

Vì đồng tiền đã được làm mù nên người rút tiền có thể gian trá khai man giá trị đồng tiền, đồng tiền được gửi đến để nhận chữ ký từ ngân hàng không đúng với giá trị trong yêu cầu gửi đến trước đó.

2.1.5. Bài toán bảo vệ đồng tiền trên đường truyền

Đồng tiền trên đường truyền có thể bị lộ và sửa đổi trái phép

2.2. PHƯƠNG PHÁP GIẢI QUYẾT

2.2.1. Giải quyết bài toán bảo vệ thông tin yêu cầu rút tiền

Thông tin yêu cầu rút tiền rất quan trọng vì vậy yêu cầu cần

- Bảo mật: bảo đảm thông tin không bị lộ.

- Bảo toàn để thông tin không bị sửa đổi trái phép trên đường truyền

- Xác thực: yêu cầu rú tiền phải có chữ ký xác thực của người rút.

1/. Bảo mật, bảo toàn thông tin trên đường truyền

Ta dùng phương pháp mã hóa

2/. Xác thực

Khi gửi đi yêu cầu rút tiền, người có tiền xác thực yêu cầu bằng chữ ký vào bản mã, ngân hàng sẽ dựa vào đó để xác thực yêu cầu.

2.2.2. Giải quyết bài toán thẩm tra hồ sơ rút tiền

Khi nhận được yêu cầu rút tiền ngân hàng cần kiểm tra thông tin yêu cầu rút tiền (thông tin tài khoản của người dùng)

2.2.3. Giải quyết bài toán ẩn danh đồng tiền

Sau khi người có tiền gửi yêu cầu rút tiền đến ngân hàng và được ngân hàng chấp nhận, người có tiền tạo một đồng tiền như trong yêu cầu rồi gửi tới ngân hàng. Vì thông tin về đồng tiền cần đảm bảo bí mật nên đồng tiền khi gửi tới ngân hàng cần được "Ẩn danh" ở đây ta sử dụng chữ ký mù.

1/. Dùng chữ ký mù : bao gồm 3 bước

- Bước 1: Người có tiền làm mù đồng tiền

- Bước 2: Người có tiền gửi đồng tiền (đã bị làm mù) cho ngân hàng. Ngân hàng ký vào đồng tiền đã bị làm mù (ký mù), sau đó gửi đồng tiền lại cho người rút tiền.

-Bước 3: Người rút tiền sau khi nhận được đồng tiền thì xóa mù trên đồng tiền và sẽ nhận được chứ ký thật trên đồng tiền thật.

2/. Ứng dụng chữ ký mù RSA trong dùng tiền điện tử

- ***Người có tiền***: Làm "mù" đồng tiền **m**, (hay "che giấu" **m**).

Phần tử "làm mù" **r** được chọn ngẫu nhiên: $\mathbf{r} \in Z_n^*$.

Giá trị "mù" của **m** là:**z** = Blind**(m)** = **m** . $\mathbf{r}^{\mathbf{b}}$(mod n). (**z** là thông điệp "mù").

- ***Ngân hàng***: Tạo chữ ký trên **z**, (hay chữ ký "mù" trên **m**).

y-mu = Sig(**z**)= $\mathbf{z}^{\mathbf{a}}$ (mod n)=(**m**. $\mathbf{r}^{\mathbf{b}}$)$^{\mathbf{a}}$ (mod n)= $\mathbf{m}^{\mathbf{a}}$ * $\mathbf{r}^{\mathbf{b}\,\mathbf{a}}$ (mod n)= $\mathbf{m}^{\mathbf{a}}$ * **r** (mod n).

- ***Người có tiền*** : Xoá mù trên chữ ký **y**-mu, Nhận được chữ ký **y** trên **m**.

UnBlind (**y**-mu)= **y**-mu / **r** =$\mathbf{m}^{\mathbf{a}}$ * **r**(mod n) / **r**=$\mathbf{m}^{\mathbf{a}}$(mod n).

2.2.4. Giải quyết bài toán phòng tránh khai man giá trị đồng tiền

Để tránh bị người rút tiền khai man giá trị đồng tiền ngân hàng có một số biện pháp sau:

*** Cách 1**: Ngân hàng sử dụng một số chìa khóa ký, cụ thể là cho mỗi giá trị đồng tiền sẽ có một loại khóa ký riêng.

Ví dụ: Đồng tiền 1 triệu sẽ dùng khóa k_1 để ký

Đồng tiền 2 triệu sẽ dùng khóa k_2 để ký

...

Đồng tiền 10 triệu sẽ dùng khóa k_{10} để ký

…

- Người rút tiền yêu cầu rút 10 triệu và gửi đồng tiền đến ngân hàng, ngân hàng sẽ dùng khóa k10 để ký mù trên đồng tiền.

- Người rút tiền nhận được đồng tiền và xóa mù sẽ nhận được chữ ký thật trên đồng tiền thật.

- Khi người rút tiền tiêu tiền, người nhận được đồng tiền sẽ dùng khóa công khai của ngân hàng tương ứng với giá trị trên đồng tiền để kiểm tra.

Ví dụ: Giá trị trên đồng tiền là 100 triệu => dùng q_{100}.

- Nếu người rút tiền khai man giá trị đồng tiền, sẽ bị lộ

Ví Dụ: Người rút tiền xin rút 10 triệu nhưng lại tạo đồng tiền có giá trị 100 triệu, ngân hàng dùng khóa k_{10} để ký. Vì trên giá trị đồng tiền ghi 100 triệu nên người nhận được đông tiền sẽ dùng q_{100} để kiểm tra => không đúng với khóa ký => đồng tiền sai.

*** Cách 2:** Người có tiền và ngân hàng có thể thực hiện một giao thức dựa vào xác xuất.

- Người có tiền tạo 10 tờ tiền (c1, c2, …c10) các tờ tiền này có mệnh giá giống nhau chỉ khác nhau về số seri.

- Người có tiền sẽ làm mù cả 10 đồng tiền và gửi về cho ngân hàng.

- Ngân hàng sẽ chọn ngẫu nhiên 9 trong số 10 đồng tiền đó để yêu cầu người có tiền tiết lộ thông tin để xóa mù chúng.

- Nếu cả 9 đồng tiền đều hợp lệ về mặt giá trị, thì ngân hàng sẽ ký mù lên đồng tiền còn lại và gửi về cho người rút tiền.

2.2.5. Giải quyết bài toán bảo vệ đồng tiền trên đường truyền

Đồng tiền trên đường truyền cần được :

- Bảo mật : đảm bảo thông tin không bị lộ

- Bảo toàn : để thông tin về đồng tiền không bị sửa đổi trái phép trên đường truyền

Giống như bài toán 1 ở đây chúng ta cũng dùng phương pháp mã hóa để đảm bảo bảo mật vào bảo toàn đồng tiền trên đường truyền.

Chương 3. THỬ NGHIỆM CHƯƠNG TRÌNH CHỮ KÝ MÙ

3.1. BÀI TOÁN LẬP TRÌNH

Chữ ký mù RSA

3.2. CẤU HÌNH HỆ THỐNG

Phần cứng: - CPU E5200 2.50GHz

- RAM 2G

- Dung lượng ổ đĩa cứng tối thiểu 20G

- Bàn phím và chuột tương thích.

Phần mềm: - Hệ điều hành windows xp hoặc win7.

- Microsoft Visual Studio 2010.

3.3. CÁC THÀNH PHẦN CỦA CHƯƠNG TRÌNH

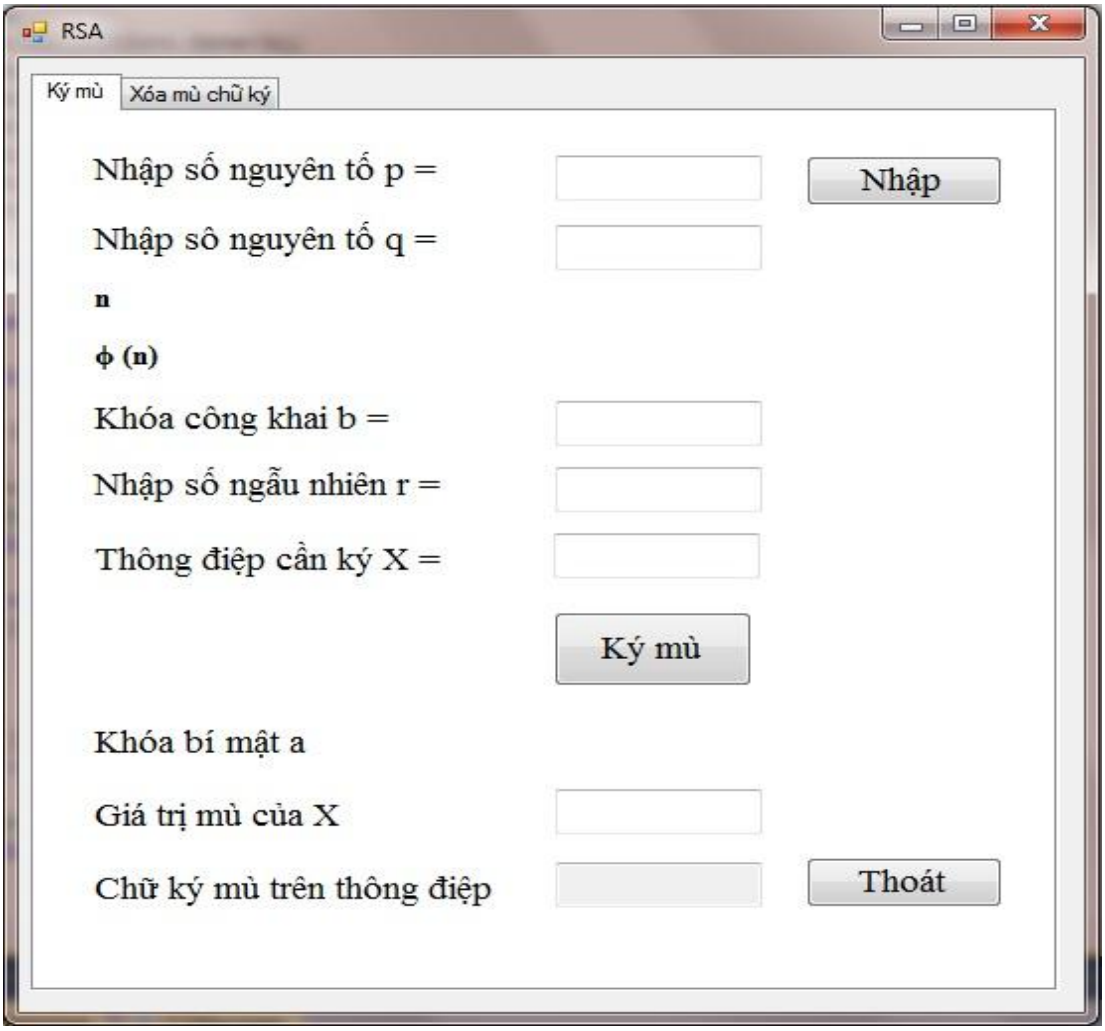
Chương trình mô phỏng thuật toán mã hóa RSA, viết bằng ngôn ngữ C# trên Visual Studio 2010.

Chương trình gồm có 2 phần:

- Ký mù: Ký mù trên một số nguyên.

- Xóa mù: Xóa mù chữ ký.

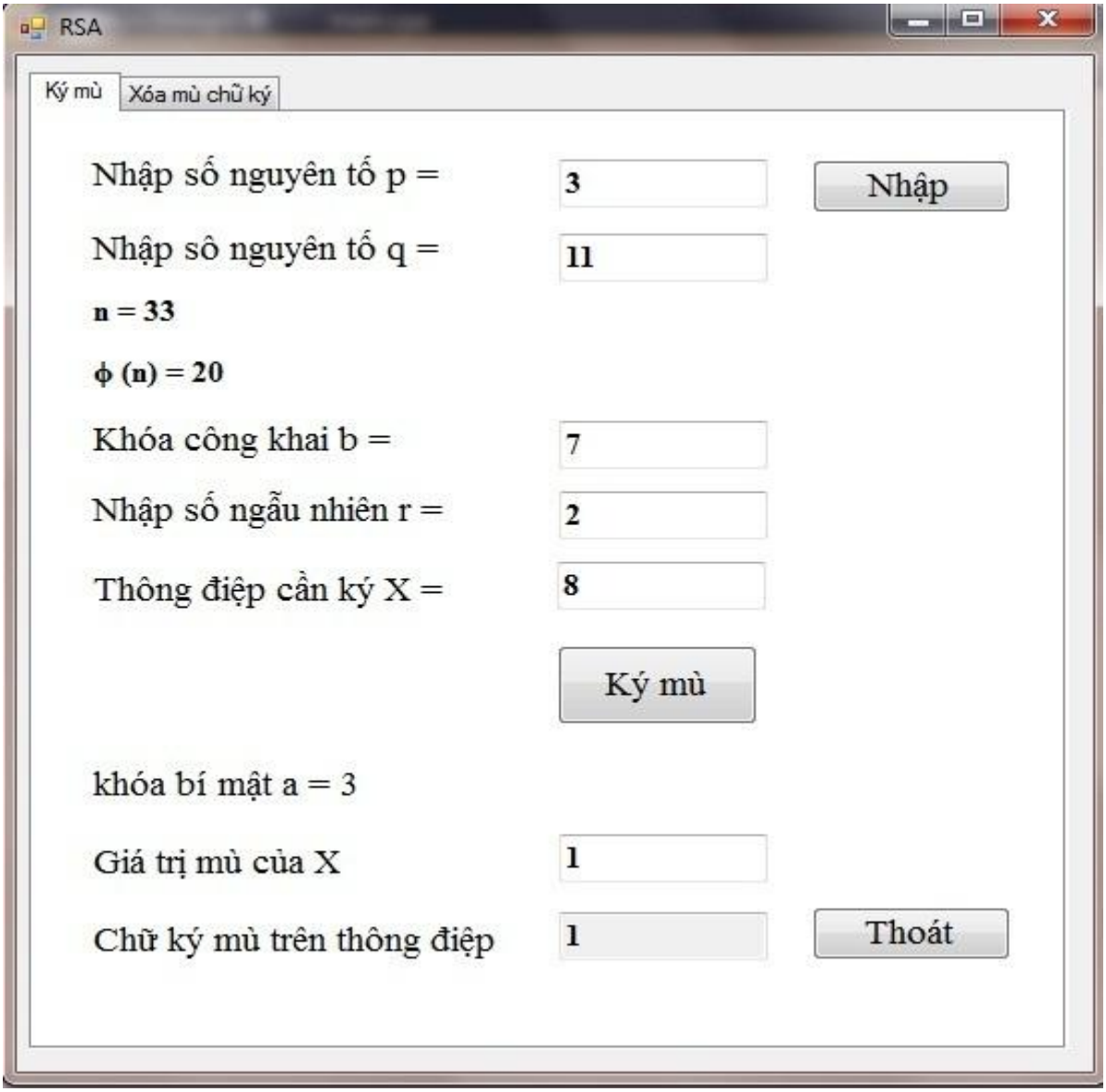
Dưới đây là giao diện của trương trình:



Hình 4: Giao diện trương trình

3.4. HƯỚNG DẪN SỬ DỤNG CHƯƠNG TRÌNH

1/. Chức năng ký mù:



Hình 5 : Giao diện chức năng ký mù

- Thông tin đầu vào:

+ Người dùng chọn số nguyên tố p, q ->bấmNhập để tính **n** và **ϕn.**

+ Nhập khóa công khai b (b là số nguyên tố cùng nhau với **ϕ n**), nhập số ngẫu nhiên r (r là số nguyên tố cùng nhau với **n**), nhập thông điệp cần ký X là một số nguyên.

+ Sau khi nhập xong thông tin bấm Ký mù để ký.

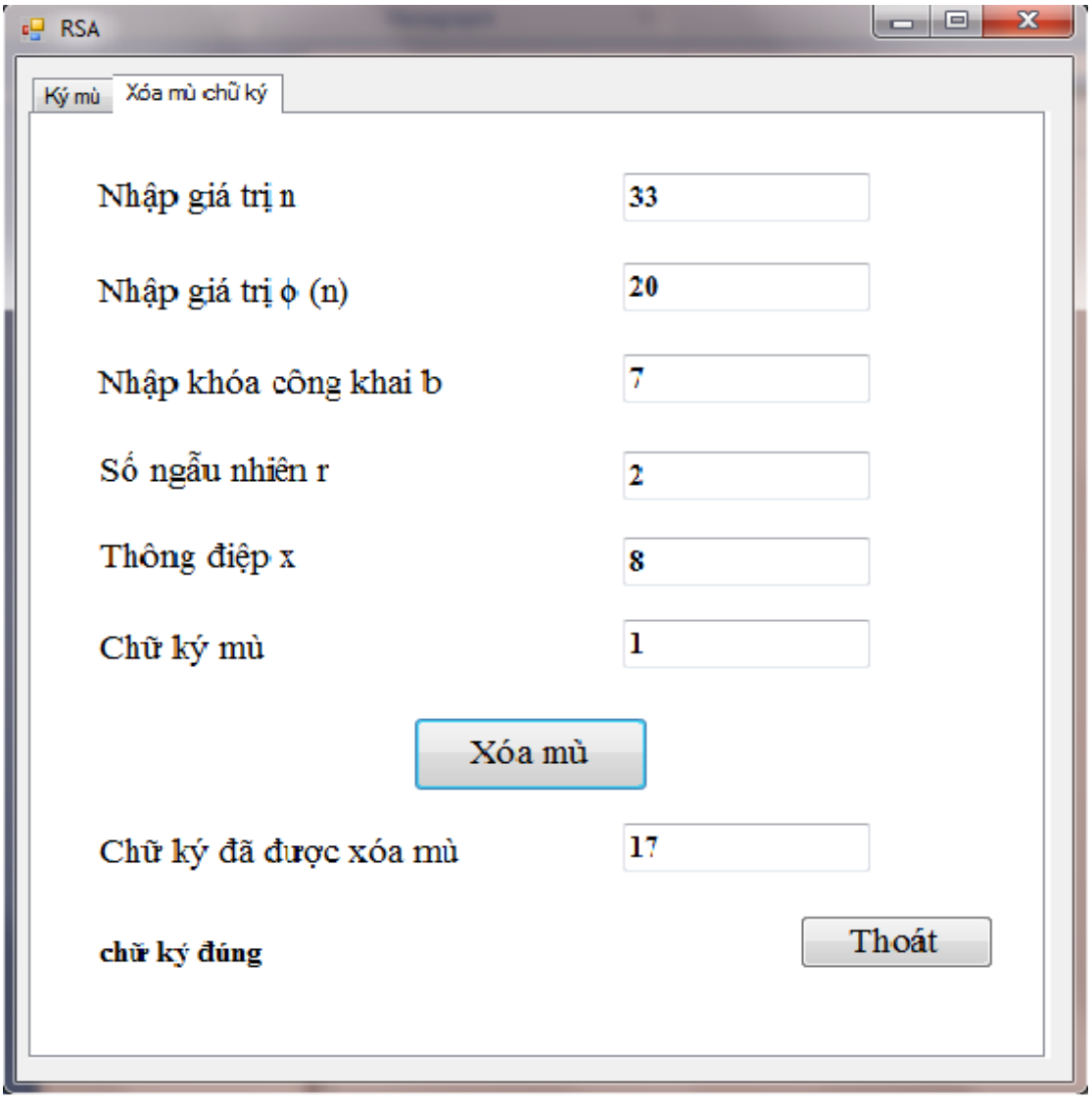
- Thông tin đầu ra:

+ Giá trị thông điệp X sau khi làm mù.

+ Chữ ký mù trên thông điệp.

- Nhấn Thoát để thoát khỏi chương trình.

2/. Chức năng xóa mù chữ ký



Hình 6: Giao diện chức năng xóa mù chữ ký

- Thông tin đầu vào:

+ Số n, giá trị ϕn**,** khóa công khai b, thông điệp X, chứ ký mù trên thông điệp

+ Sau khi nhập xong thông tin thì nhấn Xóa mù để thực hiện chức năng xóa mù

- Thông tin đầu ra:

+ Giá trị chữ ký sau khi xóa mù.

+ Xác thực đúng sai của chữ ký.

- Nhấn Thoát để thoát khỏi chương trình

KẾT LUẬN

Sau một thời gian làm việc, với sự nỗ lực của bản thân và sự tận tình chỉ bảo của thầy giáo PGS.TS.Trịnh Nhật Tiến em đã hoàn thành đồ án tốt nghiệp của mình.

Đồ án đã trình bày những kiến thức tổng quát về tiền điện tử, nghiên cứu và phân tích giải pháp cho các bài toán này sinh khi rút tiền điện tử.

Đồ án tốt nghiệp có 2 kết quả chính:

1/. Về mặt lý thuyết

Đồ án tốt nghiệp đã trình bày các vấn đề sau:

+ Tổng quan về An toàn thông tin.

+ Tổng quan về Tiền Điện Tử và Rút tiền điện tử

+ Một số bài toán về An toàn thông tin trong giai đoạn rút tiền điện tử

2/. Về mặt thực hành

Đồ án tốt nghiệp đã thực hiện được chương trình : ký "mù" RSA.

PHỤ LỤC

Code chương trình ký mù RSA

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Windows.Forms;

namespace chu_ky_RSA
{
publicpartialclassF_RSA : Form
    {
public F_RSA()
        {
            InitializeComponent();
        }
//=====================================================

//tinh nghich dao
publicint nghichdao(int A, int B)
        {

for (int i = 1; i < B; i++)
            {
```

```
if ((i * A) % B == 1)
                {
                    A = i;
break;
                }
            }
return (A);
        }
//=====================================================
int p, q, pi_n, pi_n2, n, a, a2, b, b2, r, r2;
Int64 x, z, u, v;

privatevoid tabPage1_Click(object sender, EventArgs e)
        {

        }

privatevoid btkyso_Click_1(object sender, EventArgs e)
        {
            p = Convert.ToInt16(txtp.Text);
            q = Convert.ToInt16(txtq.Text);
            x = Convert.ToInt16(txtx.Text);
            r = Convert.ToInt16(txtr.Text);
            b = Convert.ToInt16(txtb.Text);
            n = p * q;
            pi_n = (p - 1) * (q - 1);
```

```
//tao khoa a
            a = nghichdao(b, pi_n);
//làm mù thông điệp
            u = Convert.ToInt64(x * Math.Pow(r, b)) % n;

//ký mù trên u
            v = Convert.ToInt64(Math.Pow(u, a)) % n;
            txtv.Text = v.ToString();
            txtxm.Text = u.ToString();

            lba.Text = "khóa bí mật a = " + a.ToString();
        }

privatevoid bt_nhap_Click(object sender, EventArgs e)
        {
            p = Convert.ToInt16(txtp.Text);
            q = Convert.ToInt16(txtq.Text);
            n = p * q;
            pi_n = (p - 1) * (q - 1);
            lbn.Text = "n = " + n.ToString();
            lbpi_n.Text = "ϕ (n) = " + pi_n.ToString();
        }

privatevoid button1_Click(object sender, EventArgs e)
        {
this.Close();
        }
```

```
privatevoid button2_Click(object sender, EventArgs e)
        {
this.Close();
        }

privatevoid button3_Click(object sender, EventArgs e)
        {
            r2 = Convert.ToInt16(txtr2.Text);
            n = Convert.ToInt16(txtn2.Text);
            b2 = Convert.ToInt16(txtb2.Text);
            pi_n2 = Convert.ToInt16(txtpi_n2.Text);
            v = Convert.ToInt16(txtv2.Text);
            x = Convert.ToInt16(txtx2.Text);
            a2 = nghichdao(b2, pi_n2);
            r = nghichdao(r2, n);
            z = (r * v) % n;
            txtz.Text = z.ToString();
            kt = Convert.ToInt64(Math.Pow(z, b2)) % n;
            if (x == kt)
            {
                lbkt.Text = "Chữ ký đúng ";
            }
            else
            {
                lbkt.Text = "Chữ ký sai ";
            }
        }

    }
}
```