MỤC LỤC

LỜI NÓI ĐẦU

Vấn đề an toàn bảo mật thông tin đang là một vấn đề nóng và bức xúc hiện nay.Có nhiều phương pháp bảo đảm an toàn thông tin nhưng phương pháp mật mã là một phương pháp tỏ ra có hiệu quả vàđáng chúý nhất.Độ an toàn mật mã nằmở khoá bí mật.Do đó vấn đề trao đổi phân phối khoá bí mật đóng vai trò quan trọng.

Đồánđi vào nghiên cứu các sơ đồ thoả thuận khoá bí mật vàứng dụng trong hành chính điện tử.

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

Em xin chân thành cảm ơn!

Chương 1. CÁC KHÁI NIỆM CƠ BẢN

1.1. TỔNG QUAN VỀ BẢO VỆ THÔNG TIN

1.1.1. Chức năng , Nhiệm vụ của Bảo vệ 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 dữ liệu cũng được đổi mới . Bảo vệ an toàn thông tin dữ liệu là một chủ đề rộng, có liên quan đến nhiều lĩnh vực và trong thực tế có rất nhiều phương pháp được thực hiện để bảo vệ an toàn thông tin dữ liệu:

+ Bảo vệ an toàn thông tin bằng các biện pháp hành chính

+ Bảo vệ an toàn thông tin bằng các biện pháp kĩ thuật (phần cứng)

+ Bảo vệ an toàn thông tin bằng các biện pháp thuật toán (phầm 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 và cũng là môi trường đối phương dễ xâm nhập nhất đó là môi trường mạng và quá trình truyền tin.

An toàn thông tin bao gồm các nội dung sau:

+ Bảo mật : Bảo vệ tính riêng tư của thông tin.

+ Bảo toàn : Bảo vệ thông tin , phòng tránh sửa đổi trái phép.

+ Xác thực : Bao gồm xác thực đối tác (bài toán nhận danh), xác thực thông tin trao đổi.

+ Trách nhiệm : Đảm bảo người gửi thông tin không thể thoái thác trách nhiệm về thông tin mà mình đã gửi.

Để đảm bảo an toàn thông tin dữ liệu 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 dữ liệu được lưu trữ và trao đổi trên đường truyền tin và cũng như trên mạng.

Có hai loại hành xi xâm phạm thông tin dữ liệu đó là : vi phạm chủ động và vi phạm thụ động. Vi phạm thụ động chỉ nhằm mục đích cuối cùng là nắm bắt được thông tin (đánh cắp thông tin). Việc làm đó có 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 sô 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 chủ 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 them 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.

Một thực tế là không có một biện pháp 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.

1.1.2. Các Phương pháp bảo vệ thông tin

1.1.2.1. Các chiến lược chính

***Giới hạn quyền tối thiểu (Last Privilege)**

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

***bảo vệ theo chiều sâu (Defence In Depth)**

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 lẫn nhau.

***Nút thắt (Choke Point)**

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 "của khẩu" này, nghĩa là phải tổ chức một cơ cấu kiểm soát và điều khiển thông tin đi qua cửa khẩu này.

***Điểm nối yếu nhất (Weakest Link)**

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 những chỗ yếu nhất của hệ thống để tấn công, do dó ta cần phải gia cố các điểm yếu của hệ thống. Thông thường chúng ta chỉ quan tâm đến kẻ tấn công trên mạng hơn là kẻ tiếp cận hệ thống , do đó an toàn vật lý được coi là yếu điểm nhất trong hệ thống của chúng ta.

***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 ra 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.

***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.

1.1.2.2 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 sever 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 vào mạng. Thông thường bao gồm các mức bảo vệ sau:

***Quyền truy nhập**

Lớp bảo vệ trong cùng là quyền truy nhập nhằm kiểm soát cac 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.

***Đăng ký tên/mật khẩu**

Thực ra đây cũng là kiểm soát quyền truy nhập, nhưng không truy nhập ở mức thông thường mà ở mức ở 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 tên đăng ký và mật khẩu trước. Người quản trị mạng có nhiệm vụ 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 (người sử dụng chị được truy nhập trong một thời gian nào đó tại một 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.

***Mã hóa dữ liệu**

Để đảm bảo thông tin trên đường truyền người ta thường sử dụng các phương pháp mã hóa. Dữ liệu bị biến đổi từ dạng nhân 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.

***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 trạm không có ổ lưu trữ ngoài như CD-ROM, USB disk…

***Tường lửa**

Ngăn chặn thâm 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 mạng nội bộ (intranet).

***Quản trị mạng**

Trong thời đại phát triển của công nghệ thông tin, mạng máy tính quyết định toàn bộ hoạt động của một 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 các sự cố là một công việc cấp thiết hàng đầu.

Mức độ bảo vệ

- *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.*
- *Backup dữ liệu quan trong định kì.*
- *Bảo dưỡng mạng theo định kì.*
- *Bảo mật dữ liệu, phân quyền truy cập, tổ chức nhóm làm việc trên mạng.*

1.1.2.3 An toàn thông tin bằng mật mã

Mật mã là một ngành khoa học chuyên nghiên cứu các phương pháp truyền tin bí mật. Mật mã bao gồm: lập mã và phá mã. Lập 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 đi trên mạng, quá trình này được gọi là mã hóa thông tin (encryption), ở trạm nhận phải thực hiện quá trình ngược lại, tưc là biến đổi thông tin từ dạng không nhận thức được (dữ liệu đã được mã hóa) về dạng nhận thức được (dạng gốc), quá trình này được gọi là giải mã. Đây là một lớp bảo vệ thông tin rất quan trọng và được sử dụng rộng rãi trong môi trường mạng

Để bảo vệ thông tin bằng mật mã người ta thường tiếp cận theo hai hướng:

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

Theo các thứ nhất thông tin được mã hóa để bảo vệ trên đường truyền giữa hai nút mà không quan tâm đến nguồn và địch 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 truyển đi tiếp, do đó các nút cần được bảo vệ tốt.

Ngược lại theo các 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 thỳ mới có thể mà hóa được còn dữ liệu điều khiển thỳ giữ nguyên để có thể xử lý tại các nút.

1.2. MỘT SỐ KHÁI NIỆM CƠ BẢN TRONG TOÁN HỌC

1.2.1. Khái niệm trong số học

Số nguyên tố và nguyên tố cùng nhau.

Số nguyên tố là số chỉ chia hết cho 1 và chính nó.

Ví dụ:2, 3, 5, 7, 17,… là những số nguyên tố.

Hai số m và n được gọi là nguyên tố cùng nhau nếu ước số chung lớn nhất của chúng bằng 1.

Ký hiệu : gcd(m,n)=1.

Ví dụ: 9 và 14 là nguyên tố cùng nhau.

Đồng dư thức.

Định nghĩa

Cho a và b là các số nguyên , n là số nguyên dương thì a được gọi là đồng dư với b theo mod n nếu n/(a-b) (tức (a - b) chia hết cho n, hay khi chia a và b cho n được cùng một số dư như nhau). Số nguyên n được gọi là mod của đồng dư.

Kí hiệu

$a \equiv b \pmod{n}$

Ví dụ:

$67 \equiv 11 \pmod 7$, bởi vì $67 \pmod 7 = 4$ và $11 \pmod 7 = 4$

Tính chất của đồng dư

Cho a , a1, b, b1, c € Z. Ta có các tính chất sau:

a ≡ b mod n khi và chỉ khi a và b có cùng số dư khi chia cho n.

Tính phản xạ: a ≡ a mod n.

Tính đối xứng : Nếu a ≡ b mod n thì b ≡ a mod n.

Tính giao hoán: Nếu a ≡ b mod n và b ≡ c mod n thì a ≡ c mod n.

a ≡ a1 mod n, b ≡ b1 mod n thì a + b = a1 + b1 mod n và ab = a1b1 mod n.

Lớp tương đương đồng dư

Lớp tương đương của một số nguyên a theo modulo n là tập hợp các số nguyên đồng dư với a theo mod n.

Mỗi lớp tương dương như vậy được đại điện bởi một số duy nhất trong tập hợp $Z_n = \{0, 1, 2, 3,\ldots,n-1\}$, là số dư chung khi chia các số đó cho n. Vì vậy, ta có thể đồng nhất Z_n với tập tất cả các lớp tương đương các số nguyên theo mod n, trên tập đó ta có thể xác định các phép tính cộng, trừ và nhân theo mod n.

Tập $Z_n = \{0, 1, 2, 3,\ldots,n-1\}$ được gọi là tập thặng dư đầy đủ theo mod n , vì mọi số nguyên bất kì đều có thể tìm đc trong Z_n một số đồng dư với mình (theo mod n).

Tập $Z_n^* = \{ a \in Z_n : \gcd(a, n) = 1\}$, tức Z_n^* là tập con của Z_n bao gồm tất cả các phần tử nguyên tố với n. Ta gọi tập đó là tập các thặng dư thu gọn theo mod n.

**Phần tử nghịch đảo*

Định nghĩa

Cho a $\in Z_n$. Nghịch đảo của a theo modulo n là một số nguyên x $\in Z_n$ sao cho ax ≡ 1 (mod n). Nếu tồn tại thì đó là giá trị duy nhất và a được gọi là khả nghịch, kí hiệu x là a^{-1}.

Tính chất

Cho a, b $\in Z_n$. Phép chia của a cho b theo mod n là tích của a và b^{-1} theo mod n, và chỉ được xác định khi b có nghịch đảo theo mod n.

Cho a $\in Z_n$, a khả nghịch khi và chỉ khi gcd(a, n) = 1.

Giả sử d = gcd(a, n). Phương trình đồng dư ax ≡ b mod n có nghiệm x khi và chỉ khi d chia hết cho b , trong trường hợp các nghiệm d nằm trong khoảng 0 đến n – 1 thì các nghiệm đồng dư theo modulo n/d.

Ví dụ:

4^{-1} = 7 (mod 9) vì 4.7 ≡ 1 (mod 9)

1.2.2. khái niệm trong đại số

*** *Khái niệm nhóm***

Khái niệm

Nhóm là bộ phận 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:

$x' \in G: x' * x = x * x' = e$

Cấp của nhóm

Ta gọi số các phần tử trong 1 nhóm là *cấp của nhóm đó*.

Ta kí hiệu $\emptyset(n)$ là các số nguyên dương bé hơn n và nguyên tố cùng với n. Như vậy, nhóm Z_n^* có cấp $\emptyset(n)$ và nếu p là số nguyên tố thì nhóm Z_p^* có cấp p – 1 .

Cấp của phần tử

Ta nói một phần tử $g \in Z_n^*$ có cấp m, nếu m là số nguyên dương bé nhất sao cho $g^m \equiv 1 \bmod n$.

Khái niệm nhóm con

Nhóm con là bộ phận các phần tử (S, *) thỏa mãn các tính chất sau:

S ∈ G, Phần tử trung gian e ∈ S

x, y ∈ S => x * y ∈S

Khái niệm nhóm Cyclic

Nhóm Cyclic là nhóm mà mọi phần tử x của nó được sinh ra từ một phần tử đặc biệt g ∈ G. Phần tử này được gọi là phần tử sinh (nguyên thủy) , tức là :

Với ∀x ∈ G:∃n ∈ N mà g^n = x.

Ví dụ: (Z^+ , +) là một nhóm cyclic có phần tử sinh là 1.

1.2 MÃ HÓA

1.2.1 Khái niệm mã hóa

Mã hóa là phương pháp biến đổi thông tin (phim , ảnh, văn bản,…) từ dạng bình thường sang dạng thông tin "khó" có thể hiểu được, nếu không có phương tiện giải mã. Giải mã là phương pháp chuyển thông tin đã được mã hóa về dạng thông tin ban đầu (quá trình ngược của mã hóa).

Mã hóa tuân theo quy tắc nhất định gọi là hệ mã hóa. Có hai loại:

-*Mã hóa đối xứng.*

-*Mã hóa công khai (phi đối xứng).*

Sau đây là định nghĩa hình thức về sơ đồ mã hóa và cách thức thực hiện để lập mã và giải mã:

Một sơ đồ hệ thống mã hóa là một bộ năm δ = (P, C, K, E, D) thỏa mãn:

P là một tập hữu hạn các ký tự bản rõ,

C là một tập hữu hạn các ký tự bản mã,

K là một tập hữu hạn các khóa,

E là một ánh xạ từ P x K vào C được gọi là phép lập mã

P là một ánh xạ từ K x C vào P, được gọi là phép giải mã

Với mỗi k ∈ K ta định nghĩa $e_k \in$ E; e_k : P $\rightarrow$ C là hàm lập mã và d_k : C $\rightarrow$ P là hàm giải mã sao cho:

$\forall x \in$ P: e_k (x) = E (K, x)

$\forall y \in$ C: d_k (x) = D (K, y)

e_k và d_k được gọi là hàm lập mã và hàm giải mã ứng với khóa mật mã K. Các hàm đó phải thỏa mãn hệ thức:

$\forall x \in$ P: d_k (e_k (x)) = x

Hệ mã hóa công khai sử dụng một cặp khóa. Một trong hai khóa được gọi là khóa riêng (Private Key) và phải được giữ bí mật bởi người sở hữu. Khóa còn lại được gọi là công khai (Public Key), nó được phổ biến cho tất cả những ai muốn giao dịch với người riêng tương ứng. Cặp khóa này có liên quan về mặt toán học, và không thể sử dụng các thông tin của khóa công khai để tìm ra khóa riêng.

Theo lý thuyết bất kì ai cũng có thể gửi cho giữ khóa riêng một thông điệp được mã hóa bằng khóa công khai, và như vậy chỉ có người nào sở hữu mã công riêng mới có thể giãi mã được. Đồng thời, người sở hữu khóa riêng cũng chứng minh được tính toàn vẹn của dữ liệu mà anh ta gửi cho người khác bằng chữ kí điện tử thông qua việc sử dụng khóa riêng để mã hóa. Bất kì ai nhận được dữ liệu đó đều có thể sử dụng khóa công khai tương ứng để kiểm tra xem nó do ai gửi và có toàn vẹn hay không.

1.2.2 Hệ mã hóa khóa công khai RSA

RSA là hệ mã hóa công khai, độ an toàn của hệ dựa vào bài toán khó:" Phân tích số nguyên thành thừa số nguyên tố".

Sơ đồ

- Chọn ngẫu nhiên và độc lập hai số nguyên tố lớn p và q với p≠q
- Tính : $n = p.q$
- Tính giá trị hàm số Ơle: $\Phi(n) = (p-1)(q-1)$
- Chọn số tự nhiên b, $1 < b < \Phi(n)$ và là số nguyên tố cùng nhau với $\Phi(n)$
- Tính a là nghịch đảo của b : $ab \equiv 1 (mod \Phi(n))$

Khi đó, b là khóa lập mã, công khai ; a là khóa giải mã, bí mật.

Lập mã

Chọn P = C = Z_n với $n = p.q$, $Z_n = \{0, 1, 2, ..., n-1\}$

$x \in Z_n \rightarrow y = x^b \bmod n \in Z_n$

Giải mã

$y \in Z_n \rightarrow x = y^a \bmod n \in Z_n$

1.3 CHỮ KÝ SỐ

Ký số là phương pháp ký một thông điệp lưu dưới dạng "số" (điện tử).Thông điệp được ký và chữ ký cùng truyền trên mạng tới người nhận.

Với chữ ký truyền thống , khi ký lên tài liệu thì chữ kí gắn kết với tài liệu được ký. Chữ ký số không được gắn một cách vật lý với thông điệp được ký.

Đối với chữ ký trên giấy, ta kiểm tra bằng cách so sánh nó với chữ ký gốc đã đăng ký. Tất nhiên, phương pháp này không an toàn vì có thể bị đánh lừa bởi chữ ký của người khác. Trong khi chữ ký số được kiểm tra bằng thuật toán kiểm tra công khai, " người bất kì" có thể kiểm tra chữ ký số. Việc sử dụng lược đồ ký an toàn sẽ ngăn chặn khả năng đánh lừa (giả mạo chữ ký).

Sơ đồ chữ ký số là bộ năm **(P, A, K, S, V)** trong đó:

P: tập hữu hạn các thông điệp **A:** tập hữu hạn các chữ ký.

K: tập hữu hạn các khóa (không gian khóa).

Với mỗi $k \in K$ tồn tại thuật toán kí $sig_k \in$**S** và một thuật toán xác minh ver_k $\in$**V.**

Mỗi sig_k :P→ A và ver_k : P x A → $\{true, false\}$ là những hàm sao cho mỗi thông điệp x $\in$**P** và mỗi chữ ký y thỏa mãn phường trình dưới đây:

$$ver(x.y) = ver(x.y) = \begin{cases} truekhiy = sig\ (x) \\ falsekhiy \neq sig(x) \end{cases}$$

1.3.1 Một số sơ đồ ký số

1.3.1.1 Sơ đồ ký số RSA

Sơ đồ ký số RSA được cho bởi bộ năm : S = **(P, A, K, S, V).**

1./ Phần chuẩn bị

P = **A** = Z_n , với n = p.q và q là các số nguyên tố lớn.

Φ(n) = (p – 1)(q – 1) K = (n, p, q, a, b)

Chọn b $\in Z_n$ nguyên tố cùng nhau với Φ(n)

Chọn a $\in Z_n$ là nghịch đảo của b thep module Φ(n)

Các giá trị n và b công khai; các giá trị p, q, a bí mật.

2./ Phần Ký

Với mỗi K = (n, p, q, a, b) và x $\in Z_n$ ta định nghĩa chữ ký là:

y = $sig_k(x) = x^a \bmod n$,y$\in$ A

3./Kiểm tra chữ ký

$Ver_k(x, y)$= true $\Leftrightarrow \Leftrightarrow x \equiv y^b \pmod n$

1.3.1.2 Sơ đồ ký số Schnorr

1./Phần chuẩn bị

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

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

Chọn $x \neq 0$ làm khóa bít mật Tính $y = g^x$ làm khóa công khai

Lấy H là hàm băm không va chạm.

2./Phần ký:

Giả sử cần ký trên văn bản m.

Chọn r ngẫu nhiên thuộc Z_q, Tính c = H(m, x^r), Tính s = (r+xc)mod q

Chữ ký Schnorr là cặp (c, s)

3./ Phần kiểm tra chữ ký

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

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

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

Khâu quan trọng nhất của Thương mại điện tử là việc thanh toán, bởi vì mục tiêu cuối cùng của cuộc trao đổi thương mại là người mua nhận được những cái gì cần mua và người bán nhận được số tiền thanh toán.

Thanh toán là một trong những vấn đề phức tạp nhất của Thương mại điện tử.Hoạt động Thương mại điện tử chỉ phát huy được tính ưu việt khi áp dụng được hính thức thanh toán điện tử.

Thanh toán điện tử là việc thanh toán tiền thông qua các thông điệp điện tử (Electronic message) thay cho việc thanh toán bằng tiền Sec hay tiền mặt.Bản chất của mô hình thanh toán Thanh toán điện tử cũng là mô phỏng lại mô hình thanh toán truyền thống, nhưng các thủ tục giao dịch, các thao tác xử lý dữ liệu, quá trình chuyển tiền…tất cả đều được thực hiện thông qua mạng máy tính, được bối bằng các giao thức chuyên dụng.

Chương 2: TỔNG QUAN VỀ HÀNH CHÍNH ĐIỆN TỬ

2.1 KHÁI QUÁT VỀ HỆ THỐNG HÀNH CHÍNH NHÀ NƯỚC VIỆT NAM

Tổ chức Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam bao gồm 4 cấp là trung ương, tỉnh, huyện và xã.

Ở cấp Trung ương có Quốc hội, Chủ tịnh nước, Chính quyền, Tòa án nhân dân tối cao, Viện kiểm sát nhân dân tối cao.

Quốc hội là cơ quan đại biểu cao nhất của nhân dân, cơ quan quyền lực nhà nước cao nhất của nước Cộng hòa xã hội chủ nghĩa Việt Nam, do nhân dân trực tiếp bầu ra với nhiệm kỳ là 5 năm.

Quốc hội bầu ra chủ tịch nước, Thủ thướng Chính quyền, Chánh án Tòa án nhân dân tối cao, Viện trưởng Viện Kiểm sát nhân dân tối cao.

Chính quyền địa phương (cấp tỉnh , huyện và xã) có Hội đồng nhân dân do nhân dân bầu ra trực tiếp với nhiệm kỳ là 5 năm. Hội đồng nhân dân bầu ra Ủy ban nhân dân là cơ quan hành chính nhà nước ở địa phương.

Chính quyền và Ủy ban nhân dân các cấp hợp thành hệ thong cơ quan hành chính nhà nước ở Việt Nam.Chính quyền là cơ quan chấp hành của Quốc hội, cơ quan hành chính nhà nước cao nhất của nước Cộng hòa xã hội chủ nghĩa Việt Nam.

2.1.1 Chính quyền

Chính quyền thống nhất quản lý việc thực hiện các nhiệm vụ chính trị, kinh tế, văn hóa, xã hội, quốc phòng , an ninh và đối ngoại của Nhà nước; bảo đảm hiệu lực của bộ máy Nhà nước từ trung ương đến cơ sở; bảo đảm việc tôn trọng và chấp hành Hiên pháp và pháp luật; phát huy quyền làm chủ cảu nhân dân trong sự nghiệp xây dựng và bảo vệ Tổ quốc, bảo đảm ổn định và nâng cao đời sống vật chất và văn hóa của nhân dân.Chính quyền chịu trách nhiệm trước Quốc hội và báo cáo công tác với Quốc hội, Ủy ban thường vụ Quốc hội, Chủ tịch nước.

Cơ cấu tổ chức Của chính quyền gồm có:

Các bộ;

Các cơ quan ngang bộ;

Quốc hội quyết định thành lập hoặc bãi bỏ các bộ và cơ quan ngang bộ theo đề nghị của Thủ Tướng Chính quyền. [21]

2.1.2 Cơ quan thuộc Chính quyền

Cơ quan thuộc Chính quyền do Chính quyền thành lập, bao gồm: Cơ quan thuộc Chính quyền thực hiện một số nhiệm vụ, quyền hạn quản lý nhà nước về nghành, lĩnh vực, quản lý nhà nước các dịch vụ công thuộc nghành, lĩnh vực và thực hiện một số nhiệm vụ, quyền hạn cụ thể về đại diện chủ sở hữu phần vốn của nhà nước tại doanh nghiệp có vốn nhà nước theo quy định cảu pháp luật.

Cơ quan thuộc Chính quyền hoạt đọng sự nghiệp để phục vụ nhiệm vụquản lý nhà nước của Chính quyền hoặc thực hiện một số dịch vụ công có đặc điểm, tính chất quan trọng mà Chính quyền phải trực tiếp chỉ đạo; thực hận một số nhiệm vụ quyền hạn cụ thể về đại diện chủ sở hữu phần vốn của nhà nước tại doanh nghiệp có vốn nhà nước theo quy định cảu pháp luật. (Nghị định số 30/2003/NĐ-CP ngày 01/04/2003 của Chính quyền quy định chức năng, nhiệm vụ quyền hạn và cơ cấu tổ chức của cơ quan thuộc Chính quyền)

Thủ trưởng cơ quan thuộc Chính quyền là người đứng đầu và lãnh đạomột cơ quan thuộc Chính quyền; chịu trách nhiệm trước Thủ Tướng Chính quyền, trước Chính quyền về việc thực hiện chức năng, nhiệm vụ quyền hạncủa cơ quan mình; Thủ trưởng cơ quan thuộc Chính quyền không ban hành văn bản quy phạm pháp luật để thực hiện quản lý nhà nước đối với những vấn đề thuộc nghành, lĩnh vực mà cơ quan thuộc Chính quyền đang quản lý do Thủ Tướng Chính quyền Quyết định. [21]

2.1.3 Các bộ, Các cơ quan ngang bộ

Lãnh đạo công tác của các bộ, các cơ quan ngang bộ và các cơ quan thuộc Chính quyền, Ủy ban nhân dân các cấp, xây dựng và kiện toàn hệ thống bộ máy hành chính nhà nước thống nhấttừ trung ương đến cơ sở; hướng dẫn kiểm traHội đồng nhân dân thực hiện các văn bản cảu cơ quan nhà nước cấp trên tạo điều kiện để Hội đồng nhân dân thực hiện nhiệm vụ và quyền hạn theo luật định, đào tạo bồi dưỡng, sắp xếp và sử dụng đội ngủ cán bộ, công chức viên chức nhà nước.

Bảo đảm việc thi hành Hiến pháp và pháp luật trong các cơ quan nhà nước, tổ chức chính trị- xã hội , tổ chức xã hội, tổ chức kinh tế, đơn vị vũ trang nhân dân và công dân; tổ chức và lãnh đạo công tác tuyên truyền, giáo dục Hiến pháp và pháp luật trong nhân dân.

Trình dự án pháp luật, pháp lệnh và các dự án khác trước Quốc hội và Ủy ban thường vụ Quốc hội .

Thống nhất quản lý việc xây dựng, phát triển nền kinh tế quốc dân, phát triển văn hóa, giáo dục, y tế, khoa học và công nghệ, các dịch vụ công; quản lý và bảo đảm sử dụng có hiệu quảtài sản thuộc sở hữu toàn dân; thực hiện kế hoạch phát triển kinh tế- xã hội và ngân sách nhà nước, chính sách tài chính, tiền tệ quốc gia.Thi hành những biện pháp bảo vệ quyền và lợi ích hợp pháp của công dân, tạo điều kiện cho công dân sử dụng quyền và làm tròn nghĩa vụ của mình; bảo về tài sản và lợi ích của Nhà nước và của xã hội; bảo vệ môi trường.

Củng cố và tang cường nền quốc phòng toàn dân, an ninh nhân dân; bảo đảm an ninh quốc gia và trật tự, ân toàn xã hội xây dựng lực lượng vũ trang nhân dân; thi hành lệnh động viên, lệnh ban bố tình trạng khẩn cấp và mọi biện pháp cần thiết khác để bảo vệ nhà nước.Tổ chức và lãnh đạo công tác kiểm kê, thống kê của nhà nước, công tác thanh tra và kiểm tra nhà nước, chống tham nhũng lãng phí vàmọi biểu hiện quan liêu hách dịch, cửa quyền trong bộ máy nhà nước, giải quyết khiều nại tố cáo của công dân.

Thực hiện chính sách xã hội chính sách dân tộc, chính sách tôn giáo; thống nhất quản lý công tác thi đua khen thưởng.

Quyết định điều chỉnh địa giới các đơn vị hành chính dưới cấp tỉnh , thành phố trực thuộc trung ương.

Phối hợp với Ủy ban trung ương Mặt trận Tổ quốc Việt Nam, Bna chấp hành Tổng Liên đoàn lao động Việt Nam, ban chấp hành trung ương của đoàn thể nhân dân trong khi thực hiện nhiệm vụ , quyền hạn của mình; tạo điều kiện để các tổ chức đó hoạt động hiệu quả. [21]

2.1.4 Ủy ban nhân dân các cấp

Ủy ban nhân dân do hội đồng nhân dân bầu là cơ quan chấp hành của hội đồng nhân dân, cơ quan hành chính nhà nước ở địa phương, chịu trách nhiệm trước hội đồng nhân dancing cấp và cơ quan nhà nước cấp trên.

Ủy ban nhân dân chịu trách nhiệm chấp hành Hiến pháp, luật, các văn bản của cơ quan nhà nước cấp trên và nghị quyết của hội đồng nhân dân cùng cấp nhằm đảm bảo thực hiện chủ trương, biện pháp phát triển kinh tế - xã hội, củng cố quốc phòng an ninh và thực hiện các chính sách khác trên địa bàn.

Ủy ban nhân dân thực hiện chức năng quản lý nhà nước ở địa phương, góp phần bảo đảm sự chỉ đạo, quản lý thống nhất trong bộ máy hành chính nhà nước từ trung ương tới cơ sở.

Các cơ quan chuyên môn thuộc Ủy ban nhân dân là cơ quant ham mưu, giúp Ủy ban nhân dân cùng cấp thực hiện chức năng quản lý nhà nước ở địa phương và thực hiện một số nhiệm vụ,quyền hạn theo sự ủy quyền của Ủy ban nhân dân cùng cấp và theo quy định của pháp luật; góp phần bảo đảm sự thống nhấtquản lý của ngành hoặc lĩnh vực công tác từ trung ương đến cơ sở.

Các cơ quan chuyên môn thuộc Ủy ban nhân dân là cơ quan tham mưu, giúp Ủy ban nhân dân cùng cấp thực hiện chức năng quản lý quản lý nhà nước ở địa phương và thực hiện một số nhiệm vụ,quyền hạn theo sự ủy quyền của Ủy ban nhân dân cùng cấp và theo quy định của pháp luật; góp phần bảo đảm sự thống nhấtquản lý của ngành hoặc lĩnh vực công tác từ trung ương đến cơ sở.[21]

2.2 GIỚI THIỆU CHUNG VỀ HÀNH CHÍNH ĐIỆN TỬ

2.2.1 Công tác hành chính

2.2.1.1. Nhiệm vụ chính của Cơ quan nhà nước

Mối tổ chức hay cơ quan có các nhiệm vụ, kế hoạch chính như sau:

1/. Nhiệm vụ trọng tâm của cơ quan: đó là nhiệm vụ số một của cơ quan.

2/. Nhiệm vụ đối nội, đối ngoại, hợp tác, phát triển: Đó là các nhiệm vụ chính tiếp theo góp phần thực

hiệnnhiệm vụ trọng tâm.

2.2.1.2. Công tác hành chính

Trong một tổ chức hay cơ quan, công tác hành chính bao gồm các công việc thường xuyên hàng ngày, để dẫn dắt thực hiện các nhiệm vụ theo đúng kế hoạch.

2.2.1.3. Nhiệm vụ giao dịch hành chính

Giao dịch hành chính bao gồm các công việc như: Soạn thảo công văn, xin chữ ký cấp trên, nhận công văn đến cơ quan, chuyển công văn đi đên cơ quan khác, tổng hợp thông tin phân loại tài liệu đi đến,….

Giao dịch hành chính thông thương như trước là bằng phương pháp ” thủ công”. Ngày nay giao dịch hành chính bằng phương pháp điện tử, hay còn gọi là giao dịch hành chính “trực tuyến”

2.2.2. Giao dịch hành chính trực tuyến

2.2.2.1. Giao dịch hành chính thông thường

Giao dịch hành chính thông thường : là giao dịch giữa hai hay nhiều đối tác là họ trực tiếp gặp nhau tại một địa điểm, và trao đổi thỏa thuận với nhhau về một vấn đề nào đó.

Giao dịch hành chính thông thường trong các hoạt động hành chính hay các hoạt động kinh tế xã hội khác cũng tương tự, có thế gọi là giao dịch thủ công.

Giao dịch hành chính bao gồm các công việc cụ thể : Soạn thảo công văn, xin chữ ký cấp trên, nhận công văn đến cơ quan, chuyển công văn đi đên cơ quan khác, tổng hợp thông tin phân loại tài liệu đi đến,….

Với giao dịch hành chính thông thường các công văn hay tài liệu ghi trên giấy, chúng được chuyển từ cơ quan (hay cá nhân) này đến cơ quan (hay cá nhân) khác qua bộ phận văn thư hay bằng đường bưu điện,..

2.2.2.2. Giao dịch hành chính trực tuyến:

Giao dịch điện tử (Electronic Transaction) hay giao dịch trực tuyến online Transaction là hình thái hoạt động giao dịch bằng phương pháp ‘’điện tử ‘’. Tức là việc trao đổi thông tin thông qua các phương tiện công nghệ điện tử, thông tin giao dịchkhông cần phải in ra giấy, vì thông tin giao dịch dưới dạng ‘’ số ’’ có giá trị pháp lý như thông tin trên giấy. (Do đó giao dịch loại này còn được gọi là ‘’ giao dịch không giấy tờ’’).

Giao dịch hành chính trực tuyến: các công văn hay tài liệuđều dưới dạng số (không ghi trên giấy), chúng được chuyển từ cơ quan (hay cá nhân) này đến cơ quan (hay cá nhân) khác trên mạng máy tính (không qua bộ phận văn thư hay bằng đường bưu điện như giao dịch thông thường). Giao dịch loại này còn được gọi là ‘’giao dịch không giấy tờ’’.

2.2.3. Khái niệm về hành chính điện tử

‘’Hành chính điện tử’’ là việc các cơ quan trong Chính quyền nhà nước sử dụng hệ thống công nghệ thông tin và viễn thông thực hiện giao dịch hành chính trực tuyến để cung cấp các dịch vụ công trực tuyến cho người dân, doanh nghiệp, các tổ chức xã hội và nội bộ cơ quan nhà nước. Nhờ đó, giao dịch của các cơ quan Chính quyền với công dân và các tổ chức sẽ được cải thiện, nâng cao chất lượng. Lợi ích thu được sẽ là giảm thiểu tham nhũng, tang cường tính công khai, sự tiện lợi góp phần vào sự tăng trưởng giảm chi phí.

Giao dịch hành chính điện tử sử dụng các công nghệ mới như hạ tầng công nghệ thông tin, mạng máy tính và cao nhất la Internet làm nền tảng cho quản lý và vận hành bộ máy Nhà nước nhằm cung cấp các dịch vụ cho toàn xã hội.

Giao dịch hành chính điện tử kết nối các cơ quan của chính quyền trong các hoạt động , cung cấp, chia sẻ thông tin và phối hợp cung cấp giá trị tốt nhất trong việc cung ứng các dịch vụ công với chất lượng tốt nhất, phương thức mới nhất trên môi trường điện tử. Coi ‘’công dân’’ là ‘’khách hàng’’ thay đổi cách tiếp cận về quan hệ giữa công dân với chính quyền, từ quan hệ ‘’xin - cho’’ thành quan hệ ‘’phục vụ, cung ứng dịch vụ’’. Khách hàng là công dân có nhiều khả năng lựa chọn dịch vụ tốt nhất cho cuộc sống. Việc cung ứng các sản phẩm dịch vụ tư vấn bằng công nghệ mớigiúp cho con người có thể tự lựa chọn phương án, cách thức để giải quyết các vấn đề các nhân trong cuộc sống. Cơ quan hành chính biến thành các trung tâm kết nối thông tin, giúp đỡ, hướng dẫn, hỗ trợ người dân lựa chọn và thực hiện các dịch vụ hành chính.\

Các giao dịchhành chính điện tử trong chính quyền điện tử tập chung vào 4 đôií tượng khách hàng chính: Người dân, Cộng đồng doanh nghiệp, Các công chức Chính quyền, Các cơ quan Chính quyền.

Mục đích của hành chính điện tử là làm cho mối tác động qua lại giữa chính quyền với người dân, doanh nghiệp, nhân viên Chính quyền, các cơ quan chính quyền trở nên thuận tiện, than thiện, minh bạch, đỡ tốn kém và hiệu quả hơn.

2.2.4 Các giao dịch hành chính điện tử trong cơ quan nhà nước

2.2.4.1 Các dịch vụ công

Nhà nước tập trung vào việc nâng cao chất lượng và hiệu quả dịch vụ, cung cấp cho các đối tác lien quan như doanh nghiệp, người dân, các tổ chức phi Chính quyền. Điều đó được thực hiện thông qua các kênh khác nhau.Đây là một hình thức giao dịch khác ngoài hình thức đang tồn tại hiện nay là gặp trực tiếp (face to face), chẳng hạn qua Internet, các ki-ốt (trạm giao dịch điện tử) và thậm chí qua điện thoại di động.Mục đích là để tạo thuận lợi cho khách hàngcó thể sử dụng các dịch vụ của chính quyền mọi lúc, mọi nơi.Ví dụ, một công dân có thể đăng ký làm hộ chiếu và gửi ảnh qua internet.

1/. Các đặc điểm của dịch vụ công

Nghị định 86/2002/NĐ-CP quy định chức năng nhiệm vụ, tổ chức bộ máy của bộ, cơ quan ngang bộ quy định tại điều 9 về quản lý nhà nước các tổ chức thực hiện dịch vụ công thuộc ngành lĩnh vực.

Theo nghị định trên, dịch vụ công là một hoạt động thuộc phạm vi chức năng, nhiệm vụ của bộ máy hành chính nhà nước. Mặc dù có nhiều cách tiếp cận khái niệm, thuật ngữ dịch vụ công dưới các góc độ khác nhau, nhưng về cơ bản đều thống nhất tương đối ở các đặc điểm sau của dịch vụ công:

+ Dịch vụ công là một loại dịch vụ do Nhà nước (cơ quan hành chính, đơn vị sự nghiệp của Nhà nước) trực tiếp thực hiện hoặc ủy quyền cho các tổ chức, đơn vị ngoài Nhà nước thực hiện dưới sự giám sát của Nhà nước.

+ Nhằm đáp ứng các nhu cầu của xã hội (nhu cầu tối thiểu, thiết yếu).

+ Nhà nước là người chịu trách nhiệm đến cùng trước nhân dân, xã hội về chất lượng dịch vụ cũng như số lượng dịch vụ. Trách nhiệm ở đây thể hiện qua việc hoạch định chính sách, thể chế pháp luật, quy định tiêu chuẩn chất lượng, thanh tra kiểm tra giám sát việc thực hiện…

+ Không nhằm mục tiêu lợi nhuận.

+ Đối tượng thụ hưởng Dịch vụ công không trực tiếp trả tiền

> *Tóm lại: Có thể hiểu Dịch vụ công là dịch vụ do Nhà nước chịu ttrách nhiệm, phục vụ các nhu cầu cơ bản, thiết yếu chung của người dân và cộng đồng, bảo đảm ổn định và công bằng xã hội, không vì mục tiêu lợi nhuận.

2/. Các loại dịch vụ công ở nước ta hiện nay

***Loại 1: Dịch vụ sự nghiệp công(hay hoạt động sự nghiệp công)**

Các hoạt động phục vụ những nhu cầu thiết yếu cho xã hội, quyền và lợi ích công dân. Nhà nước thực hiện thông qua các tổ chức,đơn vị sự nghiệp của Nhà nước hoặc ủy quyền cho các tổ chức ngoài nhà nước thực hiện.

Ví dụ như chăm sóc sức khỏe, giáo dục, đào tạo, văn hóa, thể dục thể thao, khoa học, bảo hiểm an sinh xã hội, phòng cháy chữa cháy, bão lụt, thiên tai, dịch vụ tư vấn, hỗ trợ pháp lý cho người nghèo…

***Loại 2: Dịch vụ công ích.**

Các hoạt động có một phần mang tính chất kinh tế hàng hóa.

Ví dụ như cung cấp điện, cấp nước sạch, vệ sinh môi trường, giao thông vận tải công cộng, xây dựng kết cấu hạ tầng, khuyến nông, khuyến ngư….

***Loại 3: Dịch vụ hành chính công**

Theo Nghị định 64/2007/NĐ-CP (10/04/2007), Dịch vụ hành chính conglà dịch vụ liên quan đến hoạt động thực thi pháp luật, không nhằm mục tiêu lợi nhuận, do cơ quan nhà nước(hoặc tổ chức, doanh nghiệp được ủy quyền) có thẩm quyền cấp cho tổ chức, cá nhân dưới hình thức các loại giấy tờcó giá trị pháp lý trong các lĩnh vực mà cơ quannhà nước đó quản lý.Tóm lại, đó là các hoạt động thực thi pháp luật của các cơ quan nhà nước.

2.2.4.2.Các loại hình giao dịch hành chính điện tử của cơ quan nhà nước:

Về tổng thể có thể phân loại CPĐT thành 4 loại, tương ứng với bốn dạng dịch vụ Chính quyền bao gồm:

Chính quyền với Công dân (G4C)

Chính quyền với Doanh nghiệp (G2B)

Chính quyền với người lao động (G2E)

Chính quyền với Chính quyền (G2G)

1/. G4C (Government To Citizen)

Giao dịch và cung cấp các dịch vụ của Chính quyền trực tiếp cho cộng đồng, thí dụ tổ chức bầu cử của công dân, thăm dò dư luận, quản lý quy hoạch xây dựng đô thị, tư vấn, khiếu nại, giám sát và thanh toán thuế, hóa đơn của các nghành với người thuê bao, dịch vụ thông tin trực tiếp 24x7, phục vụ công cộng, môi trường giáo dục.

G2C bao gồm phổ biến thông tin tới công chúng, các dịch vụ công dân cơ bản như gia hạn giấy phép, cấp giấy khai sinh/ khai tử/đăng ký kết hôn và kê khai các biểu mẫu nộp thuể thu nhập cũng như hỗ trợ ngσηời dân đối với các dịch vụ cơ bản giáo dục, chăm sóc y tế, thông tin bệnh viện, thư viện và rất nhìu dịch vụ khác.

2/. G2B (Government To Business)

Dịch vụ và quan hệ của Chính quyền đối với các doanh nghiệp, các tổ chức phi Chính quyền, nhà sản xuất dịch vụ mua sắm, thanh tra, giám sát doanh nghiệp (về đóng thuế, tuân thủ luật pháp,…); thông tin về phát triển đất đai, đấu thầu, xây dựng; cung cấp thông tin dạng văn bản, hướng dẫn sử dụng, quy định, thi hành chính sách… cho các doanh nghiệp.

Đây là thành phần quan hệ cơ bản trong mô hình nhà nước là chủ thể quản lý vĩ mô nền kinh tế, xã hội thông qua chính sách, cơ chế và luật pháp doanh nghiệp là khách thể đại diện cho lực lượng sản xuất trực tiếp ra của cải vật chất của nền kinh tế.

1. Các giao dịch G2B bao gồm nhiều dịch vụ khác nhau được trao đổi giữa Chính quyền và cộng đồng doanh nghiệp bao gồm cả việc phổ biến các chính sách, biên bản ghi nhớ, các quy định và thể chế.Các dịch vụ được cung cấp bao gồm truy xuất các thông tin về kinh doanh, tải các mẫu đơn , gia hạn giấy phép, đăng ký kinh doanh, xin cấp giấp phép, nộp thuế. Các dịch vụ được cung cấp thông qua các giao dịch G2B cũng hỗ trợ việc phát triển kinh doanh, đặc biệt là phát triển các doanh nghiệp vừa và nhỏ. Việc đơn giản hóa các thủ tục xin cấp phép, hỗ trợ quá trình phê duyệt đối với các yêu cầu của các doanh nghiệp vừa và nhỏ sẽ thúc đẩy kinh doanh phát triển.
2. Ở mức cao hơn, các dịch G2B bao gồm việc mua sắm điện tử và trao đổi trực tiếp giữa Chính quyền với các nhà cung cấp để mua sắm hàng hóa và dịch vụ cho
3. Chính quyền.Một dịch vụ điển hình là các web-site mua sắm điện tử sẽ cho phép những người sử dụng đã đăng ký và được chấp nhận có thể tìm kiếm các người mua và người bán hàng hóa và dịch vụ. Tùy theo từng phương pháp, người mua hoặc người bán có thể xác định giá cả hoặc mở thầu. Việc mua sắm điện tử làm cho quá trình đấu thầu trở nên minh bạch và cho phép các doanh nghiệp nhỏ có thể thể tham gia đấu thầu đối với các dự án lớn của Chính quyền. Hệ thống này cũng giúp cho Chính quyền có thể tiết kiệm chi tiêu nhiều hơn thông qua việc cắt giảm chi phí cho môi giới trung gian và giảm chi phí hành chính của các đại lý mua bán.

3/. G2E (Government To Employee)

Dịch vụ, giao dịch trong mối quan hệ giữa Chính quyền đối với ngơi làm công lao động như bảo hiểm, dịch vụ việc làm, trơ cấp thất nghiệp, y tế nhà ở….

G2E bao gồm các dịch vụ G2C và các dịch vụ chuyên nghành khác dành riêng cho các công chức Chính quyền việc cung cấp đào tạo và phát triển nguồn nhân lực qua đó cải tiến các chức năng hành chính hàng ngày cũng nhưcách thức giải quyết công việc với người dân.

4./ G2G (Government To Goverment)

Triển khai ở hai cấp độ trong nước và quốc tế.Các giao dịch G2G là các giao dịch giữa Chính quyền trung ương / quốc gia và các chính quyền địa phương, giữa các vụ và công ty, cơ quan có liên quan.Đồng thời, các dịch vụ G2G là các giao dịch giữa các Chính quyền và có thể sử dụng như một công cụ của các mối quan hệ quốc tế và ngoại giao.

G2G được hiểu như khả năng phối hợp , chuyển giao và cung cấp các dịch vụ một cách có hiệu quả giữa các ngành, các cấp , các tổ chức, bộ máy của nhà nước trong việc điều hành và quản lý nhà nước, trong đó chính bản thân bộ máy của Chính quyền vừa đóng vai trò là chủ thể và khách thể trong mối quan hệ này.

Toàn bộ hệ thống quan hệ, giao dịch của Chính quyền như G2C, G2E, G2B và G2G phải được đặt trên một hạ tầng vững chắc của hệ thống: độ tin cậy(Strust), khả năng đảm bảo tính riêng tư (privacy) và bảo mật an toàn (security) và cuối cùng tất cả đều dựa trên hạ tầng công nghệ, và truyền thông với các quy mô khác nhau: mạng máy tính, mạng Internet. Extranet và Internet.

CHƯƠNG 3.MỘT SỐ SƠ ĐỒ THỎA THUẬN KHÓA BÍ MẬT DÙNG TRONG HÀNH CHÍNH ĐIỆN TỬ

3.1 VẤN ĐỀ THOẢ THUẬN KHOÁ BÍ MẬT

Nếu không muốn dùng dịch vụ phân phối khoá qua trung tâm được uỷ quyền TT, cặp người dùng phải tự thoả thuận khoá (trao đổi) khoá bí mật.Thoả thuận khoá mật là giao thức để cặp người dùng (hoặc nhiều hơn) liên kết với nhau cùng thiết lập khoá mật, bằng cách liên lạc trên kênh công khai. Phương pháp thiết lập khoá chung kiểu này không nhờ Tổ chức tin cậy TT điều phối, cặp người dùng tự "Thoả thuận khoá mật". Hiện nay có hai phương pháp chính để "Thoả thuận khoá mật":

+ ***Phương pháp thông thường*** Khi cặp người dùng thông nhất có một khoá mật chung, thì một trong hai người chọn khoá ngẫu nhiên K, sau đó truyền nó một cách an toàn đến người kia bằng phương pháp nào đó, ví dụ bằng mã khoá công khai hay phương pháp "giấu tin". Phương pháp này phải dùng nhiều thông tin truyền đi và cất giữ, mặt khác độ an toàn thấp vì phải truyền đi "trọn vẹn " một khoá trên mạng công khai.

+ ***Phương pháp hiệu quả*** Phương pháp hiệu quả để thoả thuận khoá phải đạt được hai tiêu chí sau: + Bảo đảm an toàn các thông tin về khoá mật . Tức là bảo đảm rằng thám mã khó có thể khám phá hay tráo đổi khoá mật. + Giảm được thông tin cần truyền đi và cất giữ, trong khi vẫn cho phép mỗi cặp người dùng tính toán được khoá mật. Theo phương pháp hiệu quả, người dùng không truyền cho nhau trên mạng "trọn vẹn" một khoá K, mà chỉ truyền vật liệu công khai và cách thức tạo khoá K đến cặp người dùng U và V. Phương pháp này không phải dùng nhiều thông tin truyền đi và cất giữ, mặt khác độ an toàn cao, vì người dùng chỉ truyền trên mạng vật liệu công khai và cách thức tạo khoá mật, chứ không truyền trực tiếp khoá mật. Thám mã có trộm được tin trên đường truyền, cũng khó tính được khoá mật vì không biết vật liệu bí mật của từng người dùng.

3.2. SƠ ĐỒ THỎA THUẬN KHÓA BÍ MẬT DIFFE HELLMAN

Hệ phân phối khoá Diffie-Hellman không đòi hỏi TA phải biết và chuyển bất kỳ thôngtin bí mật nào về khoá của các người tham gia trong mạng để họ thiết lập được khoáchung bí mật cho việc truyền tin với nhau.

Trong một hệ phân phối khoá Diffie-Hellman, TA chỉ việc chọn một số nguyên tố lớn pvà một phần tử nguyên thuỷ α theo mod p, sao cho bài toán tính logα trong p Zp* là rấtkhó. Các số p và α được công bố công khai cho mọi người tham gia trong mạng.Ngoàira, TA có một sơ đồ chữ ký với thuật toán ký (bí mật) sigTA và thuật toán kiểm chứng(công khai) verTA.

Một thành viên bất kỳ A với danh tính ID(A) tuỳ ý chọn một số $aA(0 \le aA \le p - 2)$ và tính$bA = \alpha aA \bmod p$. A giữ bí mật *aA* và đăng ký các thông tin (ID(A), *bA*) với TA. TA cấp choA chứng chỉ:

C(A) = (ID(A), *bA*, sigTA(ID(A), *bA*)).

Các chứng chỉ của các thành viên trong mạng có thể được lưu giữ trong một cơ sở dữliệu công khai hoặc uỷ thác cho TA lưu giữ và cung cấp công khai cho các thành viênmỗi khi cần đến.

Khi hai thành viên A và B trong mạng cần có một khoá bí mật chung để truyền tin bảomật cho nhau thì A dùng thông tin công khai *bB* có trong C(B) kết hợp với số bí mật củamình là *aA* để tạo nên khoá:

$KA,B = bB$

$aA \bmod p = \alpha aBaA \bmod p$

Khoá chung đó B cũng tạo ra được từ các thông tin công khai *bA*của A và số bí mật củamình:

$KA,B = bA$

$aB \bmod p = \alpha aAaB \bmod p$

Để bảo đảm được các thông tin về và *bB* và *bA* là chính xác, A và B có thể dùng thuậttoán verTA để kiểm chứng chữ ký xác thực của TA trong các chứng chỉ C(B) và C(A)tương ứng.

Độ an toàn của hệ phân phối khoá Diffie-Hellman được bảo đảm bởi yếu tố sau đây:

Biết *bA* và *bB* để tính KA,B chính là bài toán Diffie-Hellman tương đương: biết α*a*mod*p*

Phân phối khóa và thỏa thuận khóa

và α*b*mod*p*, tính α*ab*mod*p*. Đây là một bài toán khó tương đương bài toán tính lôgarit rờirạc hay bài toán phá mật mã ElGamal.

Giao thức trao đổi khoá Diffie-Hellman

Hệ phân phối khoá Diffie-Hellman nói trong mục trước có thể dễ dàng biến đổi thànhmột giao thức trao đổi (hay thoả thuận) khoá trực tiếp giữa những người sử dụng màkhông cần có sự can thiệp của một TA làm nhiệm vụ điều hành hoặc phân phối khoá.

Một nhóm bất kỳ người sử dụng có thể thoả thuận cùng dùng chung một số nguyên tốlớn p và một phần tử nguyên thuỷ α theo mod p, hai người bất kỳ trong nhóm A và Bmỗi khi muốn truyền tin bảo mật cho nhau có thể cùng thực hiện giao thức sau đây đểtrao đổi khoá:

1. A chọn ngẫu nhiên số aA (0 aA p -2), giữ bí mật aA, tính *bA* = α*aA*mod*p*

và gửi bA cho B.

2. Tương tự, B chọn ngẫu nhiên số aB (0 aB p -2), giữ bí mật aB, tính *bB* = α*aB*mod*p* vàgửi bB cho A.

3. A và B cùng tính được khoá chung:

KA,B= *bB*

*aA*mod*p*= *bA*

*aB*mod*p*(= α*aAaB*mod*p*)

Giao thức trao đổi khoá Diffie-Hellman có các tính chất sau:

3.2.1. Giao thức là an toàn đối với việc tấn công thụ động

nghĩa là một người thứ ba, dùbiết bA và bB sẽ khó mà biết được KA,B.Ta biết rằng bài toán "biết bA và bB tìm KA,B" chính là bài toán Diffie-Hellman và nói rằng bài toán đó tương đương với bài toán phá mật mã El Gamal.

Bây giờ ta chứng minh điều này. Phép mật mã El Gamal với khoá K = (p,α,a,β), trongđó β = α$a$mod$p$, cho ta từ một bản rõ x và một số ngẫu nhiên $k \in Zp - 11$ lập được mật mã:

$eK(x,k) = (y1,y2)$

Trong đó: $y1 = \alpha k \mathrm{mod} p, y2 = x\beta k \mathrm{mod} p$

Và phép giải mã được cho bởi:

$dK(y1,y2) = y1(y2\ a\ ) - 1 \mathrm{mod} p$

Phân phối khóa và thỏa thuận khóa

Giả sử ta có thuật toán A giải bài toán Diffie-Hellman. Ta sẽ dùng A để phá mã El

Gamal như sau: Cho mật mã ($y1$,$y2$). Trước hết, dùng A cho $y1 = \alpha k \mathrm{mod} p$ và β = α$a$mod$p$,ta được:

A(y1, β) = αka = β$k$mod$p$

và sau đó ta thu được bản rõ x từ βk và y2 như sau:

$x = y2(\beta k) - 1 \mathrm{mod} p$

Ngược lại, giả sử có thuật toán B phá mã El Gamal, tức là:

B (p,α,a,β,$y1$,$y2$) = $x = y2(y1\ a\ ) - 1 \mathrm{mod} p$

Áp dụng B cho β = bA,$y1 = bB$,$y2 = 1$, ta được

B (p,α,bA,bB,1) − 1 = (1.(bB

aA) − 1) − 1 = α$aAaB$mod$p$ tức là giải được bài toán Diffie-Hellman.

3.2.2Giao thức là không an toàn đối với việc tấn công chủ động bằng cách đánh tráo

Nghĩa là một người thứ ba C có thể đánh tráo các thông tin trao đổi giữa A vàB, chẳng hạn, C thay $\alpha^{a}A$mà A định gửi cho B bởi $\alpha^{a'}A$,và thay $\alpha^{a}B$mà B định gửi cho Abởi $\alpha^{a'}B$, như vậy, sau khi thực hiện giao thức trao đổi khoá, A đa lập một khoá chung$\alpha^{aAa'B}$với C mà vẫn tưởng là với B, đồng thời B đa lập một khoá chung $\alpha^{a'AaB}$với C màvẫn tưởng là với A; C có thể giải mã mọi thông báo mà A tưởng nhầm là mình gửi đếnB, cũng như mọi thông báo mà B tưởng nhầm là mình gửi đến A!

Một cách khắc phục kiểu tấn công chủ động nói trên là làm sao để A và B có thể kiểmchứng để xác thực tính đúng đắn của các khoá công khai bA và bB. Đưa vào giao thứctrao đổi khoá Diffie-Hellman thêm vai trò điều phối của một TA để được một hệ phânphối khoá Diffie-Hellman như ở mục 7.2.1 là một cách khắc phục như vậy. Trong hệphân phối khoá Diffie-Hellman, sự can thiệp của TA là rất yếu, thực ra TA chỉ làm mỗimột việc là cấp chứng chỉ xác nhực khoá công khai cho từng người dùng chứ không đoihỏi biết thêm bất cứ một bí mật nào của người dùng. Tuy nhiên, nếu chưa thoả mãn vớivai trò hạn chế đó của TA, thì có thể cho TA một vai trò xác nhận yếu hơn, không liênquan gì đến khoá, chẳng hạn như xác nhận thuật toán kiểm thử chữ ký của người dùng,còn bản thân các thông tin về khoá (cả bí mật và công khai) thì do những người dùngtrao đổi trực tiếp với nhau. Với cách khắc phục có vai trò rất hạn chế đó của TA, ta cóđược giao thức ở phần sau.

Phân phối khóa và thỏa thuận khóa

Giao thức trao đổi khoá D-H có chứng chỉ xác thực

Mỗi người dùng A có một danh tính ID(A) và một sơ đồ chữ ký với thuật toán ký sigAvà thuật toán kiểm chứng verA. TA cũng có một vai trò xác thực, nhưng không phải xácthực bất kỳ thông tin nào liên quan đến việc tạo khoá mật mã của người dùng (dù làkhoá bí mật hay là khoá công khai), mà chỉ là xác thực một thông tin ít quan hệ khácnhư thuật toán kiểm chứng chữ ký của người dùng. Còn bản thân các thông tin liên quanđến việc tạo khoá mật mã thì các người dùng sẽ trao đổi trực tiếp với nhau. TA cũng cómột sơ đồ chữ ký của mình, gồm một thuật toán ký sigTA và một thuật toán kiểm chứng(công khai) verTA. Chứng chỉ mà TA cấp cho mỗi người dùng A sẽ là:

C(A) = (ID(A), verA , sigTA(ID(A), verA)).

Rõ ràng trong chứng chỉ đó TA không xác thực bất kỳ điều gì liên quan đến việc tạo

khoá của A cả. Việc trao đổi khoá giữa hai người dùng A và B được thực hiện theo giaothức sau đây:

1. A chọn ngẫu nhiên số aA (0 aA p -2), tính *bA* = α*aA*mod*p*

và gửi bA cho B.

2. B chọn ngẫu nhiên số aB (0 aB p -2), giữ bí mật aB, tính *bB* = α*aB*mod*p*, tính tiếp

K = *bB*

*aB*mod*p*

yB= *sigB*(*bB*,*bA*) và gửi (C(B), bB, yB) cho A.

3. A tính: *K* = *bB*

*aB*mod*p*dùng verB để kiểm chứng yB, dùng verTA để kiểm chứng C(B),

sau đó tính *yA* = *sigA*(*bA*,*bB*), và gửi (C(A), yA) cho B.

4. B dùng verA để kiểm chứng yA ,và dùng verTA để kiểm chứng C(A).

Nếu tất cả các bước đó được thực hiện và các phép kiểm chứng đều cho kết quả đúngđắn, thì giao thức kết thúc, cả A và B đều có được khoá chung K. Do việc dùng các thuậttoán kiểm chứng nên A biết chắc giá trị bB là của B và B biết chắc giá trị bA là của A,loại trừ khả năng một người C nào khác đánh tráo các giá trị đó giữa đường.

Phân phối khóa và thỏa thuận khóa

Ví dụ:Giả sử p=25307, còn $\alpha = 2$ là phần tử nguyên thủy của trường GF(p), những tham số công khai. Giả sử U chọn a_U=3578. Sau đó U tính giá trị công khai:

$$b_U = \alpha^{a_U} \bmod p = 2^{3578} (\text{mod} 25307) = 6113,$$

đặt trên dấu xác nhận của U. Giả sử V chọn a_V=19956. Và V cũng tính giá trị công khai:

$$b_V = \alpha^{a_V} \bmod p = 2^{19956} (\text{mod} 25307) = 7984,$$

đặt trên dấu xác thực của V.Bây giờ U và V muốn liên lạc với nhau thi U và V tính ra khóa mật:

U tính: $K_{U,V} = (b_V)^{a_U} (\text{mod}\, p) = 7984^{3578} (\text{mod} 25307) = 3694.$

V tính: $K_{V,U} = (b_U)^{a_V} (\text{mod}\, p) = 6113^{19956} (\text{mod} 24307) = 3694.$

3.3. SƠ ĐỒ THỎA THUẬN KHÓA BÍ MẬT BLOM :

Ý tưởng chính Ta giả thiết rằng có một mạng gồm n người sử dụng.Giả sử rằng các khoá được chọn trên trường hữu hạn *pZ*, trong đó p là số nguyên tố (p n).Cho k là số nguyên, 1 k n-2.Giá trị k để hạn chế kích thước lớn nhất mà sơ đồ vẫn duy trì được độ mật. TT sẽ truyền đi k+1 phần tử của *p Z* , cho người sử dụng trên kênh an toàn (so với n-1 trong sơ đồ phân phối trước cơ bản). Mỗi cặp người sử dụng U và V sẽ có khả năng tính khoá Ku, v = Kv, u như trước đây. Điều kiện an toàn như sau: tập bất kì gồm nhiều nhất k người sử dụng không liên kết từ U, V phải không có khả năng xác định bất kì thông tin nào về Ku, v.

3.3.1. Giao thức khoá Blom với k =1

1/. Số nguyên tố p công khai, với người sử dụng U, phần tử ru*p Z* là công khai, khác nhau. 2/. TT chọn 3 phần tử ngẫu nhiên bí mật a, b, c *p Z* (không cần khác biệt) và thiết lập đa thức: f(x, y) = (a + b*(x + y) + c*x*y) mod p.

3/. Với người sử dụng U, TT tính đa thức: gu(x) = f(x, ru) mod p và truyền gu(x) đến U trên kênh an toàn. gu(x) là đa thức tuyến tính theo x, có thể viết: gu(x) = f(x, ru) mod p = (a+b.(x+ ru) + c.x. ru mod p) mod p hay gu(x) = au + bu*x, trong đó: au = a + b*ru mod p bu = b + c*ru mod p

4/. Nếu U và V muốn liên lạc với nhau, họ sẽ dùng khoá chung: Ku, v = Kv, u = f(ru, rv) = (a + b*(ru+ rv) + c.ru.rv) mod p. U tính Ku, v = f(ru, rv) = gu(rv) =(a+b.(rv+ ru) + c.rv. ru) mod p. V tính Ku, v = f(ru,rv) = gv(ru) =(a+b.(ru+ rv) + c.ru.rv) mod p. Do tính chất đối xứng của đa thức f(x,y), nên Ku,v= Kv,u.

Ví dụ 1

1/. Giả sử có 3 người sử dụng là U,V và W. Chọn số nguyên tố p =17, Các phần tử công khai của họ là ru = 12, rv = 7, rw = 1.

2/. TT chọn ngẫu nhiên, bí mật a = 8, b = 7, c = 2. Khi đó đa thức f như sau:

f(x, y) = (8 + 7*(x + y) + 2*x*y) mod 17.

3/. TT tính các đa thức và gửi cho U, V, W tương ứng là: gu(x) = f(x, 12) = (8 + 7*(x + 12) + 12*2*x) mod 17 = 7 + 14*x. gv(x) = f(x, 7) = (8 + 7*(x + 7) + 7*2*x) mod 17 = 6 + 4*x. gw(x) = f(x, 1) = (8 + 7*(x + 1) + 12*2*x) mod 17 = 15 + 9*x.

4/. Khi U và V muốn liên lạc với nhau, người dùng tự tính khoá chung: U tính Ku, v= gu(rv) = f(ru,rv) =(a+b.(rv+ ru) + c.rv. ru) mod p =7 + 14*7 mod 17 = 3. V tính Ku, v = gv(ru) = f(ru,rv) =(a+b.(ru+ rv) + c.ru.rv) mod p = 6 + 4*12 mod 17 =3. * 3 khoá tương ứng với 3 cặp người dùng là: Ku, v = f(ru,rv) = (8 + 7*(12 + 7) + 2*12*7) mod 17 = 3. Ku, w = f(ru,rw) =(8 + 7*(12 + 1) + 2*12*71) mod 17 = 4. Kv, w = f(rv,rw) = (8 + 7*(7 + 1) + 2*7*71) mod 17 = 10.

Mức an toàn

a). Sơ đồ Blom với k = 1 an toàn với 1 đối thủ.

Định lý: Theo sơ đồ Blom với k =1

khoá của một cặp đối tác là an toàn không điều kiện trước bất kì người sử dụng thứ ba. TT: Không một người sử dụng nào có thể xác định được thông tin về khoá của 2 người sử dụng khác.

***Chứng minh*:** Giả sử người sử dụng thứ ba là W muốn thử tính khoá. Ku, v = (a + b*(ru + rv) + c*ru*rv) mod p Trong đó các giá trị ru, rv là công khai, còn a, b, c không được biết. W tìm biết được các giá trị: aw = a + b*rw mod p. bw = b + c*rw mod p. Vì chúng là hệ số của đa thức gw(x) được TT gửi đến cho W. Ta sẽ chỉ ra rằng thông tin mà W biết phù hợp với giá trị tùy ý t *p Z* của khoá Ku,v.

Xét phương trình ma trận sau:

1 ru+rv rurv a t

1 rw 0 b = aw

0 1 rw c bw

(2) Tức là hệ các phương trình: Ku,v = (a+b *(ru + rv) + c *ru *rv) mod p = t (1) a+b *rw mod p = aw b+c *rw mod p = bw (3) (1) thể hiện giả thiết rằng Ku,v = t, (2),(3) cho thấy W biết a, b và c từ gw(x).

Định thức của ma trận hệ số là: { (1*rw *rw) + (1 *1 *rurv) +(0 *(ru + rv) *0) }- { 0*rw *rurv) + (1 *1 *0) +(1 *(ru + rv) *rw)}= = {rw2 + rurv} – {(ru + rv)*rw} = (rw - ru)(rw - rv).

Vì rw ru và rw rv nên định thức ma trận hệ số khác không. Do đó phương trình ma trận có nghiệm duy nhất cho a, b, c. Nói cách khác, bất kì giá trị t nào thuộc *p Z* cũng có thể nhận là khoá Ku,v.

b). Sơ đồ không an toàn với liên minh 2 đối thủ Định lý

Liên minh của 2 người sử dụng W, X, (không phải là cặp người dùng U, V) sẽ có khả năng xác định khoá Ku,v bất kì U và V.

Chứng minh Hai người W và X cùng biết rằng các đẳng thức sau: aw = a + b*rw. bw = b + c*rw. ax = a + b*rx. bx = b + c*rx. Như vậy, họ có bốn phương trình trong đó ba ẩn chưa biết và dễ dàng tính ra nghiệm duy nhất cho a, b, c. Một khi đã biết a, b, và c, họ có thể thiết lập đa thức f(x, y) và tính khoá bất kì mà họ muốn .

CHƯƠNG 4:THỬ NGHIỆM CHƯƠNG TRÌNH

4.1. CHƯƠNG TRÌNH PHÂN PHỐI KHÓA BLOM VỚI K > 1

4.1.1. Cấu hình hệ thống.

+Phần cứng Yêu cầu phần cứng của chương trình: CPU Khoảng 15- 20M.

+ Phần mềm Yêu cầu phần mềm của chương trình: Tubo C++ phiên bản 4.9.9.2, Hệ điều hành Windown XP.

4.1.2. Các thành phần của chương trình.

Thành phần của chương trình gồm :

+ Input: - Số lượng người dùng, hệ số k, số nguyên tố p.

- Các phần tử công khai và hệ số a ngẫu nhiên bí mật.

+ Output: - Khóa tương ứng giữa những cặp người dùng.

4.1.3. Chương trình.

```
#include <iostream>
#include <cmath>
#include <stdlib.h>
using namespace std;
  //------------------------------------------------
int a[1000][1000];
//cac so ngau nhien bi mat ma TT chon
int k;
//he so k
int p;
//so nguyen to p
int n;
 //so luong nguoi dung
int r[1000];
```

```
  //phan tu cong khai cua n nguoi dung //-----------------------------------------------
--------------------
void gx(int y)
   {
         int heso_x[100] = {0};
         for(int i=0;i<=k;i++)
          {
         for(int j=0;j<=k;j++)
           {
            heso_x[i] += (int)(a[i][j]*pow((double)y,j));
                  }

heso_x[i] %= p;
if(i>1)
cout<< " + " << heso_x[i] << "*x^" << i;
else if(i==1)
cout<< " + " << heso_x[i] << "*x";
         else if(i==0)
         cout<< heso_x[i];
           }
            }
                  //-------------------------------------------------------------------------
int f(int x, int y)
 {
int kq = 0;
for(int i=0;i<=k;i++)
   {
         for(int j=0;j<=k;j++)
```

```
            {
             kq += a[i][j]*pow((double)x,i)*pow((double)y,j);
              }
                    }
                   kq %= p; return kq;
                     }

//---------------------------------------------------------------------------
void nhapdulieu()
{ cout<< "So luong nguoi dung = ";
cin>> n;
cout<< "k = ";
cin>> k;
cout<< "p = ";
          cin>> p;
          cout<< "Cac phan tu cong khai cua " << n << " nguoi dung lan luot la:\n";
          for(int i=0;i<n;i++)
             {
                   cout<< "r["<< i+1 <<"] = ";
                   cin>> r[i];
                     }
                   cout<< "Cac he so a[i][j] do TT chon ngau nhien bi mat la:\n";
                            for(int i=0;i<=k;i++)
                            for(int j=0;j<=i;j++)
                               {
                            cout<< "a[" << j << "][" << i << "] = ";
                            cin>> a[i][j]; a[j][i] = a[i][j];
```

```
                    }
                    }


int main()
{ nhapdulieu();
  cout << "\nDa thuc gui cho "<< n <<" nguoi dung lan luot la:\n";
for(int i=0;i<n;i++)
   {
        cout<< "G" << i+1 << "(x) = ";
        gx(r[i]);
        cout<< "\n";
           }
              cout<< "\nKhoa tuong ung giua nhung cap nguoi dung la:\n";
              for(int i=0;i<n;i++)
                {
              for(int j=0;j<=i;j++)
                       {
                      if(i!=j)
                        {
              cout<< "K["<< j+1 <<"]["<< i+1 <<"] = " << f(r[i],r[j]) << "\n";
                          }
                                }
                                 }
                               cout<< "\n";
                               system("pause");
                                       }
```

4.1.4. Hướng dẫn sử dụng chương trình.

+ Khởi động TC để vào chương trình.

- Sinh khóa
- Khai báo hệ số k.
- Khai báo số nguyên tố p.
- Khai báo số lượng người dùng.
- Khai báo các phần tử công khai.

+ Trước khi chạy chương trình nhấn F9 để kiểm tra lỗi + Nếu không báo lỗi nhấn tổ hợp phím CTRL+ F9 để chạy chương trình.

Kết quả thử nghiệm của chương trình: Số lượng người dùng = 3 k = 4 p = 83 Các phần tử công khaicủa 3 ngườidùnglầnlượtlà:

r[1] = 3 r[2] = 6 r[3] = 9

Các hệ số a[i][j] do TT chọn ngẫu nhiên số bí mật:

a[0][0] = 3 a[0][1] = 3 a[1][1] = 3 a[1][2] = 3 a[2][2] = 3 a[0][3] = 3 a[1][3] = 3 a[2][3] = 3 a[3][3] = 3 a[0][4] = 3 a[0][4] = 3 a[2][4] = 3 a[3][4] = 3 a[4][4] = 3

Đa thức gửi cho 3 người dùng là:

G1(x) = 35+ 45*x+ 82*x^2+ 50*x^3 + 12*x^4

G2(x) = 72+ 57*x+ 73*x^2+ 34*x^3 + 7*x^4

G1(x) = 17+ 13*x+ 19*x^2+ 57*x^3 + 9*x^4

Khoá tương ứng giữa các cặp người dùng là:

K[1][2] = 61 K[1][3] = 5 K[2][3] = 21

Pess any key to continue...

KẾT LUẬN

Sau 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 các sơđồ thoả thuận khoá bí mật vàứng dụng trong hành chính điện tử.

Đồ án tốt nghiệp gồm có hai kết quả chính:

1./Nghiên cứu và hệ thống lại các vấn đề sau:

- Tổng quan về an toàn thông tin.
- Một số phương pháp mã hóa, ký số.
- Tổng quan về hành chínhđiện tử.
- Vấn đề thoả thuận khoá bí mật.
- Một số sơ đồ thoả thuận khoá bí mật.

2./Thử nghiệm một số ứng dụng.

-Thử nghiệm chương trình phân phối khoá Blom.

TÀI LIỆU THAM KHẢO

Tiếng việt.

1.Trịnh Nhật Tiến PGS.TS (2008), *Giáo trình An toàn dữ liệu.*

2.Trịnh Nhật Tiến PGS.TS (2007), *Bài giảng môn An toàn và bảo mật dữ liệu.*

3.Trịnh Nhật Tiến PGS.TS (2007), *Bài giảng môn Phân tích đánh giá thuật toán.*

4.Nguyễn Văn Vỵ PGS.TS (2002), *Phân tích thiết kế Hệ thống thông tin*, Nhà xuất bản thống kê Hà Nội.

5. NguyễnĐăng Khoa :*Nghiên cứu một số bài toán về an toàn thông tin trong hành chính điện tử*

Tiếng Anh

6.ByeongKon Kim, School of Enginerring, Information and Communications University (2004).

7.[Ebook- C] *Applied Cryptography Second Edition* – John Wiley & Sons Inc.pdf

8.Pretince Hall – *Modern Cryptography- Theory And Practice* -2003.pdf

9.http://ntrd.cs.tcd.ie/meipeice/Project/Mlists/brands.html