NGHIÊN CỨU MỘT SỐ BÀI TOÁN VỀ AN TOÀN THÔNG TIN TRONG CHÍNH QUYỀN ĐIỆN TỬ

MỤC LỤC

BẢNG CÁC CHỮ VIẾT TẮT

Chữ viết tắt	Giải thích
CERT (Computer Emegency Respone Team)	Đội cấp cứu máy tính
PKI (Public Key Infrastructure)	Hạ tầng cơ sở mật mã khóa công khai
VNP (Virtual Private Network)	Mạng riêng ảo
CNTT	Công nghệ thông tin
CPĐT	Chính phủ điện tử
CNTT-TT	Công nghệ thông tin-Truyền thông
G2C (Government To Citizen)	Chính phủ với công dân
G2B (Government To Business)	Chính phủ với doanh nghiệp
G2E (Government To Employee)	Chính phủ với người lao động
G2G (Government To Goverment)	Chính phủ với Chính phủ
KV	Khu vực

LỜI CẢM ƠN

Người xưa có câu: "Uống nước nhớ nguồn, ăn quả nhớ kẻ trồng cây". Với em sinh viên khoá 11 của trường Đại Học Dân Lập Hải Phòng luôn luôn ghi nhớ những công lao to lớn của các thầy giáo, cô giáo. Những người đã dẫn dắt chúng em từ khi mới bước chân vào giảng đường đại học những kiến thức, năng lực và đạo đức chuẩn bị hành trang bước vào cuộc sống để xây dựng đất nước khi ra trường sau 4 năm học. Em xin hứa sẽ lao động hết mình đem những kiến thức học được phục vụ cho Tổ quốc. Em xin chân thành cảm ơn đến:

Cha, mẹ người đã sinh thành và dưỡng dục con, hỗ trợ mọi điều kiện về vật chất và tinh thần cho con trên con đường học tập lòng biết ơn sâu sắc nhất.

Thầy cô của trường và các thầy cô trong Ban giám hiệu, thầy cô trong Bộ môn CNTT của trường Đại học Dân lập Hải Phòng đã tận tình giảng dạy và tạo mọi điều kiện cho chúng em học tập trong suốt thời gian học tập tại trường.

Thầy Trịnh Nhật Tiến– Giáo viên hướng dẫn đồ án tốt nghiệp đã tận tình, hết lòng hướng dẫn em trong suốt quá trình nghiên cứu để hoàn thành đồ án tốt nghiệp này. Em mong thầy luôn luôn mạnh khoẻ để nghiên cứu và đào tạo nguồn nhân lực cho đất nước.

Một lần nữa em xin chân thành cảm ơn.

Hải Phòng, ngày ..... tháng ..... năm 2011

Sinh viên thực hiện

Ngô Thị Loan

GIỚI THIỆU

Ứng dụng công nghệ thông tin (CNTT) đang là xu thế tất yếu hiện nay. Để thúc đẩy hoạt động này, Chính phủ đã ban hành nhiều cơ chế, chính sách nhằm tạo môi trường và điều kiện thuận lợi cho các Bộ, ngành, địa phương và toàn xã hội triển khai có hiệu quả các hoạt động ứng dụng CNTT.

Hướng tới "Chính phủ điện tử" (CPĐT), càng trở nên cần thiết xuất phát từ các yếu tố sau:

Thứ nhất là: Đối tượng quản lý của Bộ, ngành rộng, số lượng các đối tượng đều rất lớn, và thuộc nhiều lĩnh vực.

Tất cả đối tượng này đều rải rác từ cơ sở. Để làm tốt công tác tham mưu cho chính phủ và đưa ra định hướng, những quyết định đúng đắn và nhanh nhất……

Bộ phải nắm bắt được các con số đầy đủ, kịp thời và chính xác. Vì vậy việc triển khai ứng dụng mạnh mẽ CNTT là đòi hỏi tất yếu và khách quan.

Cơ chế, chính sách do Bộ xây dựng, tham mưu, đề xuất với Chính phủ thường có liên quan mật thiết đến người dân, người lao động và toàn xã hội do vậy, cần phải có một hệ thống dữ liệu kịp thời, đầy đủ và chính xác. Để có được hệ thống dữ liệu như vậy, cần ứng dụng tối đa CNTT trong các khâu thu thập, cập nhật, xử lý, cung cấp thông tin….

Thứ hai là: Khối lượng công việc cần xử lý của Bộ, ngành ngày càng nhiều, việc ứng dụng CNTT sẽ mang lại hiểu quả thiết thực trong quản lý tiến độ công việc, góp phần cải cách hành chính, giảm bớt chi phí về nhân lực, tài lực, đồng thời nâng cao chất lượng công tác chuyên môn.

Thứ ba là: Ứng dụng CNTT giúp công tác truyền tải văn bản, thông tin chỉ đạo điều hành, dữ liệu… của Bộ đến cơ sở được kịp thời, thông suốt.

Không những thế, ứng dụng CNTT cũng giúp Bộ, ngành chuyển tải được nhiều nội dung thông tin hơn, hình thức cung cấp thông tin cũng phong phú hơn, ngoài thông tin dưới dạng chữ còn có thông tin hình ảnh và âm thanh…Hình thức cung cấp thông tin như vậy sẽ giúp người dân ngày càng hiểu rõ hơn chính sách liên quan đến lĩnh vực quản lý của Bộ, ngành.

Để có được các thông tin chính xác nhất, thì An toàn thông tin là vấn đề rất quan trọng cần được chú trọng quan tâm. Và cần áp dụng các công nghệ phù hợp để đảm bảo được thông tin truyền/ nhận là đúng đắn nhất có thể.

Theo quan niệm của chúng tôi, khái niệm "chính quyền điện tử" có nghĩa rộng hơn khái niệm "chính phủ điện tử".

Với "chính quyền điện tử", sẽ dễ hiểu rằng không chỉ có giao dịch với chính phủ trung ương, mà còn có giao dịch với chính quyền địa phương (ở mọi cấp).

Chương1. CÁC KHÁI NIỆM CƠ BẢN

1.1.TỔNG QUAN VỀ "CHÍNH PHỦ ĐIỆN TỬ"

1.1.1. Khái niệm "Chính phủ điện tử"

"Chính phủ điện tử" (CPĐT) là Chính phủ ứng dụng Công nghệ thông tin - truyền thông để các cơ quan Chính phủ đổi mới tổ chức, đổi mới các quy trình hoạt động, tăng cường năng lực của Chính phủ, làm cho Chính phủ làm việc hiệu lực, hiệu quả và minh bạch hơn, cung cấp thông tin, dịch vụ tốt hơn cho người dân, doanh nghiệp và các tổ chức, tạo điều kiện thuận lợi cho người dân thực hiện quyền dân chủ và tham gia quản lý Nhà nước.

Nói một cách ngắn gọn: CPĐT là Chính phủ hoạt động hiệu lực, hiệu quả hơn, cung cấp dịch vụ tốt hơn trên cơ sở ứng dụng CNTT – TT. CPĐT là một hệ thống thông tin hỗ trợ công tác quản lý, điều hành của Chính phủ một cách hiệu quả.

Có nhiều cách tiếp cận khác nhau nên có nhiều định nghĩa về CPĐT**:**

Cách tiếp cận 1: Theo định nghĩa của Ngân hàng thế giới (World Bank)

"CPĐT là việc các cơ quan Chính phủ sử dụng một cách có hệ thống công nghệ thông tin và viễn thông để thực hiện các quan hệ với công dân, với doanh nghiệp và các tổ chức xã hội. Nhờ đó, giao dịch của các cơ quan Chính phủ 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, tăng cường tính công khai, sự tiện lợi, góp phần vào sự tăng trưởng giảm chi phí ".

Với cách tiếp cận này, CPĐT bao hàm 3 yếu tố:

- Ứng dụng CNTT và truyền thông
- Nhằm cải thiện giao dịch giữa Nhà nước với công dân và doanh nghiệp
- Giảm chi phí và bớt tham nhũng thông qua tăng cường công khai, minh bạch.

Cách tiếp cận 2 :

CPĐT là sự tối ưu hóa liên tục việc chuyển giao các dịch vụ, sự tham gia của các thành phần và quản lý của Nhà nước bớt việc chuyển đổi các quan hệ bên trong và bên ngoài thông qua công nghệ, Internet và các phương tiện mới.

Các thành phần bên ngoài ở đây chỉ các dịch vụ trực tuyến (Online Service) đối với công dân hay doanh nghiệp, còn quan hệ bên trong để chỉ các hoạt động của Chính phủ (Government Operations) từ các công thức của bộ máy nhà nước.

CPĐT là một "Chính phủ vận hành trực tuyến" (Government OnLine-GOL)

Hay Chính phủ 24x7 , thậm chí 24x365.

Một điểm cơ bản của CPĐT là khả năng sử dụng các công nghệ mới như hạ tầng cơ sở công nghệ thông tin, mạng máy tính và cao nhất là Internet làm nền tảng cho việc quản lý và vận hành của bộ máy Nhà nước nhằm cung cấp các "dịch vụ" cho toàn xã hội.

Trong xã hội thông tin hiện nay, quá trình hoạt động và quản lý từ cấp cao nhất đến cơ sở cần phải được dựa trên các hệ thống tập hợp, lưu trữ, xử lý, sử dụng và khai thác thông tin có hiệu quả để cai quản và điều hành vĩ mô mọi hoạt động của nền kinh tế toàn xã hội. Tốc độ phát triển mạnh mẽ như vũ bão của Internet hiện nay (đặc biệt tại các nước phát triển) đã và đang là động lực làm thay đổi cách thức kinh doanh và vận hành doanh nghiệp và cũng là nhân tố tích cực cho việc hình thành và phát triển CPĐT, để trở thành một hệ thống hiệu quả hơn và phục vụ tốt hơn.

Cách tiếp cận 3: CPĐT là hệ thống thông tin đặc biệt nhằm

Kết nối các cơ quan của Chính phủ trong các hoạt động, cung cấp, cung cấp, chia sẻ thông tin và phối hợp cung cấp giá trị tốt nhất trong việc cung ứng các dịch công với chất lượng tốt nhất, phương thức mới nhất trên môi trường điện tử.

Xây dựng và hình thành cổng điện tử của các cơ quan hành chính địa phương, cung cấp thông tin cho mọi người dân về những công việc của cơ quan hành chính, các quy định và thủ tục, dịch vụ mà cơ quan hành chính cung cấp cho nhu cầu của người dân.

Coi "công dân" là "khách hàng": thay đổi cách tiếp cận về quan hệ giữa công dân với Chính phủ, 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 mới đã được chuyển thành các "Trung tâm kết nối", giúp cho mọi người có thể tự lựa chọn phương án, cánh thức để giải quyết những vấn đề của cá 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.

Cách tiếp cận 4: CPĐT là Chính phủ

Sử dụng CNTT nhằm giải phóng các hoạt động thông tin, vượt qua các rào cản vật lý của hệ thống giấy tờ truyền thống và các hệ thống cơ sở khác.

Sử dụng công nghệ để tăng cường khả năng tiếp cận cho công dân, doanh nghiệp, các đối tác và người lao động đến các dịch vụ của Chính phủ.

Theo khái niệm này, CPĐT là việc tự động hóa, máy tính hóa các quy trình giấy tờ nhằm thúc đẩy:

- Phong cách lãnh đạo mới
- Phương pháp mới trong việc thiết lập chiến lược
- Phương thức mới trong giao dịch và kinh doanh
- Phương thức mới trong việc lắng nghe công dân và cộng đồng
- Phương thức mới trong tổ chức và cung cấp thông tin

Các dịch vụ CPĐT tập trung vào 4 đối tượng khách hàng chính:

- Người dân
- Cộng đồng doanh nghiệp
- Các công chức Chính phủ
- Các cơ quan Chính phủ.

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

1.1.2. Các giao dịch trong " Chính phủ điện tử"

CPĐT bao gồm 3 thành tố chính:

1.1.2.1. Các dịch vụ công:

Chính phủ tập trung vào việc nâng cao chất lượng và hiệu quả dịch vụ, cung cấp cho các đối tác liên quan như doanh nghiệp, người dân, các tổ chức phi Chính phủ. Điều đó được thực hiện thông qua các kênh khác nhau. Đây là một hình thức giao dịch khác ngoài những 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 hàng có thể sử dụng các dịch vụ của Chính phủ mọi lúc, mọi nơi. Ví dụ, một công dân có thể đăng ký làm hộ chiếu và gửi ảnh qua Internet.

1.1.2.2. Tiếp cận thông tin

Chính phủ phải mở rộng việc kết nối với các đối tác liên quan. Họ có thể kết nối vào cổng thông tin của Chính phủ thông qua Internet và qua các ki-ốt. Mọi người không phải tới các cơ quan quản lý nhà nước để lấy thông tin. Thay vào đó, người ta sẽ tiếp cận thông tin theo phương thức tự phục vụ. CPĐT giúp những người quản lý có trách nhiệm hơn vì tính minh bạch cao hơn, giảm thiểu những gì không hiệu quả và tệ quan liêu. Một trong những thách thức lớn nhất đối với các Chính phủ là tổ chức lại quy trình hoạt động, hiện tại để khai thác các lợi ích của CNTT-TT. Đồng thời, Chính phủ phải xem xét và cải tổ lại chính sách hành chính, đào tạo lại cán bộ Nhà nước về CNTT và kỹ năng hành chính công mới.

1.1.2.3. Sự tương tác giữa Chính phủ và công chúng:

CNTT sẽ làm cho Chính phủ quản lý cởi mở và dễ tiếp cận hơn bằng việc cho phép công chúng cùng tham gia vào các công việc của các cơ quan Nhà nước.

CPĐT cũng tạo thêm cơ hội phát triển cho các đối tác liên quan, đặc biệt là cộng đồng người nghèo ở những nước kém phát triển hay những người ở nông thôn.

Nhờ hiệu quả của CNTT-TT, Chính phủ có thể vươn tới cả những đối tượng ở khu vực nông thôn, vùng sâu, vùng xa.

Trong một hệ thống CPĐT, từng cá nhân có khả năng đưa ra yêu cầu đối với một dịch vụ cụ thể của Chính phủ và nhận được dịch vụ đó thông qua Internet hoặc một số cơ chế được vi tính hóa. Trong một số trường hợp, các dịch vụ Chính phủ được cung cấp thông qua một văn phòng Chính phủ thay vì nhiều văn phòng Chính phủ. Trong một số trường hợp khác, các giao dịch Chính phủ được hoàn tất mà không phải liên lạc trực tiếp với các nhân viên Chính phủ

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

- Chính phủ với Công dân (G2C)
- Chính phủ với Doanh nghiệp (G2B)
- Chính phủ với người lao động (G2E)
- Chính phủ với Chính phủ (G2G)

1/. G2C (Government To Citizen)

Giao dịch và cung cấp các dịch vụ của Chính phủ 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 thuế thu nhập cũng như hỗ trợ người dân đối với các dịch vụ cơ bản như 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 phủ đối với các doanh nghiệp, các tổ chức phi Chính phủ, nhà sản xuất như 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 như là khách thể đại diện cho lực lượng sản xuất trực tiếp ra của cải vật chất của nền kinh tế.

Các giao dịch G2B bao gồm nhiều dịch vụ khác nhau được trao đổi giữa Chính phủ 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.

Ở mức cao hơn, các dịch G2B bao gồm việc mua sắm điện tử và trao đổi trực tiếp giữa Chính phủ với các nhà cung cấp để mua sắm hàng hóa và dịch vụ cho

Chính phủ. 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 phủ. Hệ thống này cũng giúp cho Chính phủ 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 phủ đối với người 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 phủ như việc cung cấp đào tạo và phát triển nguồn nhân lực qua đó cải tiến các chức năng hành chính hàng ngày cũng như cách 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 phủ 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 phủ 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 phủ 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 phủ 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.

Ngoài 4 mô hình giao dịch chủ yếu trên, bảng dưới đây cho thấy những hình thức giao tiếp khác trong Chính phủ điện tử.

Hình thức giao tiếp				
CPĐT	Nhân dân Công dân	CQ hành chính Nhà nước	Khu vực II Kinh tế	Khu vực III NPO/NGO
Nhân dân, Công dân	**C2C**	**C2G**	**C2B**	**C2N**
CQ hành chính, NN	**G2C**	**G2G**	**G2B**	**G2N**
KV II, Kinh tế	**B2C**	**B2G**	**B2B**	**B2N**
KV III, NPO/NGO	**N2C**	**N2G**	**N2B**	**N2N**

1.2. TỔNG QUAN VỀ AN TOÀN THÔNG TIN

1.2.1. Một số khái niệm trong an toàn thông tin

1.2.1.1. Mật mã (Cryptography)

1/. Khái niệm Mật mã

"***Mật mã***" là kỹ thuật được dùng lâu đời nhất trong việc bảo đảm An toàn thông tin. Trước đây "mật mã" chỉ dùng trong ngành an ninh quốc phòng, ngày nay việc bảo đảm . An toàn thông tin là nhu cầu của mọi ngành, mọi người (do các thông tin chủ yếu được truyền trên mạng công khai), vì vậy kỹ thuật "mật mã" là công khai cho mọi người dùng. Điều bí mật nằm ở "***khóa***" mật mã.

Hiện nay có nhiều kỹ thuật mật mã khác nhau, mỗi kỹ thuật có những ưu, nhược điểm riêng. Tuỳ theo yêu cầu của môi trường ứng dụng mà người ta dùng kỹ thuật này hay kỹ thuật kia. Có những môi trường cần phải an toàn tuyệt đối bất kể thời gian và chi phí. Có những môi trường lại cần giải pháp dung hoà giữa bảo mật và chi phí thực hiện.

Mật mã cổ điển chủ yếu dùng để "che giấu" dữ liệu. Mật mã hiện đại còn dùng để thực hiện: Ký số (ký điện tử), tạo đại diện thông điệp, giao thức bảo toàn dữ liệu, giao thức xác thực thực thể, giao thức xác thực tài liệu, giao thức chứng minh "không tiết lộ thông tin", giao thức thỏa thuận hay phân phối khóa, chống chối cãi trong giao dịch điện tử, chia sẻ bí mật, ...

Theo nghĩa hẹp, mật mã chủ yếu dùng để bảo mật dữ liệu. Khi đó người ta quan niệm:

Mật mã học là Khoa học nghiên cứu mật mã: ***Tạo mã*** và ***Phân tích mã.***

Phân tích mã là kỹ thuật, nghệ thuật phân tích mật mã, kiểm tra tính bảo mật của nó hoặc phá vỡ sự bí mật của nó. Phân tích mã còn gọi là ***Thám mã.***

Theo nghĩa rộng, kỹ thuật mật mã là một trong những công cụ hiệu quả bảo đảm An toàn thông tin nói chung: bảo mật, bảo toàn, xác thực, chống chối cãi, ...

2/. Khái niệm mã hóa (Encryption)

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

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

- ***Giải mã*** là quá trình chuyển thông tin ngược lại từ ***Bản mã*** thành ***Bản rõ***.
- ***Thuật toán mã hoá*** hay ***giải mã*** là thủ tục để thực hiện mã hóa hay giải mã.
- ***Khóa mã hóa*** là một giá trị làm cho thuật toán mã hoá thực hiện theo cách riêng biệt và sinh ra bản rõ riêng. Thông thường khoá càng lớn thì bản mã càng an toàn. Phạm vi các giá trị có thể có của khoá được gọi là ***Không gian khoá.***
- ***Hệ mã hóa*** là tập hợp các thuật toán, các khóa nhằm che dấu thông tin cũng như làm cho rõ nó.

3/. Khái niệm ký số (Digital Signature)

Thông thường sau khi thỏa thuận một văn bản hợp tác, hợp đồng hay thừa nhận trách nhiệm về nội dung một tài liệu, người ta phải xác nhận sự đồng ý của mình bằng cách "***ký tay***" vào cuối văn bản hay tài liệu.

Bằng cách nào đó người ta phải thể hiện đó là "***chữ ký***" của họ (***chữ ký*** bằng "***tay***", **một dấu hiệu riêng** của họ), người khác ***không thể*** giả mạo (bắt chước) được.

Mọi cách sao chép ***chữ ký*** trên tài liệu thường dễ bị phát hiện, vì bản sao có thể phân biệt được với bản gốc.

Nhưng "**ký**" trên tài liệu trong máy tính hay truyền qua mạng máy tính như thế nào, khi nội dung tài liệu đều được biểu diễn dưới dạng số hoá (chỉ dùng hai số 0 và 1, ta gọi là **tài liệu số**).

Việc giả mạo và sao chép lại đối với tài liệu số là hoàn toàn dễ dàng, không thể phân biệt được bản gốc với bản sao. Hơn nữa, một tài liệu số có thể bị cắt dán, lắp ghép là hoàn toàn có thể và ta không thể phân biệt được bản gốc với bản sao.

Vậy một chữ ký như ***chữ ký*** bằng "***tay***" thông thường **ở cuối tài liệu số**, ***không thể*** chịu trách nhiệm đối với toàn bộ nội dung tài liệu.

Chữ ký như thế nào thì mới thể hiện được trách nhiệm đối với toàn bộ tài liệu**?**

Chắc chắn chữ ký đó phải được "***ký***" trên ***từng bít*** của tài liệu**.**

Vậy "***ký***" trên tài liệu số được thực hiện như thế nào ?

Thực chất của việc ***ký*** "***điện tử***" là ***mã hoá***.

"***Xác nhận chữ ký***" là ***kiểm tra*** việc mã hoá trên có đúng không.

Như vậy khi gửi 1 file tài liệu số có chữ ký trên đó, người ta phải gửi cả 2 file: một file tài liệu và một file chữ ký. Nhờ đó mới kiểm tra được có đúng chữ ký đó ký trên tài liệu đi kèm hay không.

1.2.1.2. Giấu tin (Steganography)

1/. Khái niệm giấu tin

Mã hoá thông tin là biến đổi thông tin "dễ hiểu" (hiển thị rõ ràng, có thể đọc được, ecó thể hiểu được) thành thông tin dưới dạng "bí mật" (khó thể hiểu được vì chỉ nhìn thấy những kí hiệu rời rạc vô nghĩa).

Thông tin mã hóa dễ bị phát hiện, vì chúng có hình dạng đặc biệt. Khi đó tin tặc sẽ tìm mọi cách để xác định bản rõ.

Giấu thông tin (Steganography) là che giấu thông tin này vào trong một thông tin khác.

Thông tin được giấu (nhúng) vào bên trong một thông tin khác, sẽ khó bị phát hiện, vì người ta khó nhận biết được là đã có một thông tin được ***giấu*** (nhúng) vào bên trong một thông tin khác (gọi là ***môi trường giấu tin***).

Nói cách khác, giấu tin giống như "***ngụy trang***" cho thông tin, không gây ra cho tin tặc sự nghi ngờ. Ví dụ một thông tin ***giấu*** vào bên trong một bức tranh, thì **sự vô hình** của thông tin chứa trong bức tranh sẽ "***đánh lừa***" được chú ý của tin tặc.

Theo nghĩa rộng, ***giấu tin*** cũng là ***hệ mật mã***, nhằm đảm bảo tính bí mật của thông tin.

Tóm lại, giải pháp hữu hiệu để "**che giấu**" thông tin là kết hợp cả hai phương pháp:

Mã hóa thông tin trước, sau đó ***giấu*** **bản mã** vào bên trong một thông tin khác.

Có thể kết hợp cả ba giải pháp: ***Nén*** thông tin, ***Mã hóa*** thông tin, ***Giấu*** thông tin.

2/. Khái niệm Thủy ký (WaterMarking)

Theo nghĩa rộng, "***Giấu tin***" nhằm thực hiện hai việc:

- ***Bảo vệ thông tin cần giấu.***

- ***Bảo vệ chính môi trường giấu tin.***

Giấu (nhúng) thông tin mật vào một thông tin khác, sao cho người ta khó phát hiện ra thông tin mật đó. Đó là bảo vệ thông tin cần giấu.

Loại giấu tin này được gọi là "Steganography".

Giấu (nhúng) thông tin vào một thông tin khác, nhằm bảo vệ chính đối tượng được dùng để giấu tin vào. Tức là giấu tin để bảo vệ chính môi trường giấu tin.

Tin được giấu có vai trò như ***chữ ký*** hay ***con dấu*** dùng để xác thực (chứng nhận) thông tin (là môi trường giấu tin). Loại"giấu tin"này được gọi là thủy ký (***Watermarking***).

Ví dụ:

Giấu một thông tin sở hữu của người chủ vào trong tác phẩm (tài liệu số) của họ, nếu ai sử dụng trái phép tác phẩm đó, thì ***thông tin giấu*** sẽ là ***vật chứng*** để chứng minh quyền hợp pháp của người chủ. Đó là ứng dụng để bảo vệ bản quyền tác phẩm "số".

Ví dụ:

Khi giấu một thông tin vào trong một tác phẩm (tài liệu số), ta có thể dùng chính thông tin giấu để kiểm xem tác phẩm có bị thay đổi nội dung hay không. Vì nếu tác phẩm bị thay đổi nội dung, thì không thể lọc ra được thông tin giấu nguyên vẹn như lúc ban đầu.

Đó là ứng dụng: Dùng thông tin giấu để kiểm tính toàn vẹn của môi trường giấu tin.

1.2.1.3. Nén thông tin

1/. Khái niệm "Nén tin" (Nén dữ liệu)

Nén dữ liệu (Data Compression) là **kỹ thuật** chuyển dữ liệu dạng "dư thừa" sang dạng "ít dư thừa", dữ liệu thu được sau khi nén ***nhỏ hơn*** dữ liệu gốc rất nhiều. Như vậy đỡ tốn bộ nhớ để lưu trữ dữ liệu, mặt khác tiết kiệm thời gian và chi phí truyền dữ liệu.

Như vậy việc nghiên cứu các kỹ thuật nén dữ liệu là điều rất cần thiết, góp phần nâng cao hiệu quả sử dụng các tài nguyên của các hệ thống máy tính.

Song song với việc nén dữ liệu, phải có kỹ thuật giải nén, nhằm chuyển dữ liệu được nén sang dữ liệu ban đầu.

Ngoài thuật ngữ "nén dữ liệu", do bản chất của kỹ thuật, nó còn có tên gọi là: "Giảm độ dư thừa", "Mã hóa ảnh gốc".

Hầu hết các máy tính hiện nay được trang bị "Modem", nhằm nén và giải nén các thông tin truyền và nhận thông qua đường điện thoại.

Hiện nay có nhiều kỹ thuật nén dữ liệu, nhưng chưa có phương pháp nén nào được coi là vạn năng, vì nó phụ thuộc vào nhiều yếu tố và bản chất của dữ liệu gốc. Kỹ thuật nén dữ liệu thường chỉ dùng cho một lớp dữ liệu có chung đặc tính nào đó.

Một số kỹ thuật nén dữ liệu hiện nay: Mã độ dài loạt (Run length coding), Mã hoá độ dài biến động (Variable length coding), Mã Huffman, …

Tỷ lệ nén dữ liệu (Compression rate).

Tỷ lệ nén là một trong các đặc trưng quan trọng nhất của phương pháp nén. Người ta định nghĩa tỷ lệ nén là:

Tỷ lệ nén = **(1/ r)** %

Với **r** là ***Tỷ số nén*** = kích thước dữ liệu gốc **/** kích thước dữ liệu thu được sau nén.

Tỷ số nén **r** = 10 / 1, nghĩa là dữ liệu gốc là 10 phần, sau khi nén chỉ còn 1 phần.

Với dữ liệu ảnh, kết quả "nén" thường là **10 :1**. Theo kết quả nghiên cứu gần đây tại Viện kỹ thuật Georgie, kỹ thuật nén "***Fractal***" cho tỷ số nén là **30 : 1.**

2/. Các phương pháp "Nén tin".

Hiện nay có nhiều kỹ thuật nén dữ liệu, nhưng chưa có phương pháp nén nào được coi là vạn năng, vì nó phụ thuộc vào nhiều yếu tố và bản chất của dữ liệu gốc. Kỹ thuật nén dữ liệu thường chỉ dùng cho một lớp dữ liệu có chung đặc tính nào đó.

Một số kỹ thuật nén dữ liệu hiện nay:

- Mã độ dài loạt (Run length coding)
- Mã hóa độ dài biến động (Variable length coding)
- Mã Huffman

1.2.1.4. Tường lửa (Firewall)

1/. Khái niệm Tường lửa

"**Tường lửa**" trong công nghệ mạng thông tin được hiểu là một hệ thống phần cứng, phần mềm hay hỗn hợp phần cứng - phần mềm, có tác dụng như một ***tấm ngăn cách*** giữa các tài nguyên thông tin của mạng nội bộ và thế giới Internet bên ngoài.

Phạm vi hẹp hơn như trong một mạng nội bộ, người ta cũng bố trí "**Tường lửa**" để ***ngăn cách*** các miền an toàn khác nhau (Security Domain).

Thuật ngữ "Tường lửa" có nguồn gốc trong kỹ thuật xây dựng để ngăn chặn, hạn chế hỏa hoạn. Trong CNTT, "Tường lửa" là kỹ thuật được tích hợp vào hệ thống mạng để chống lại sự truy cập trái phép. Kỹ thuật nhằm ***bảo vệ thông tin nội bộ***, mặt khác ***hạn chế sự xâm nhập của thông tin trái phép*** vào hệ thống.

Kỹ thuật này phục vụ cho An toàn Hệ thống máy tính là chính, nhưng cũng hỗ trợ bảo đảm An toàn truyền tin, ví dụ ***chống trộm cắp, sửa đổi thông tin*** (chẳng hạn làm sai lệch tin tức hay giả mạo chữ ký) trước khi đến tay người nhận.

Nhiệm vụ của Tường lửa:

Quyết định người nào, dịch vụ nào bên ngoài được truy cập vào bên trong Hệ thống máy tính. Quyết định người nào, dịch vụ nào bên trong được truy cập ra bên ngoài Hệ thống máy tính.

Để bảo đảm An toàn thông tin, tất cả các trao đổi thông tin từ ngoài vào trong hay ngược lại đều phải thực hiện thông qua "Tường lửa".

2/. Các thành phần của Tường lửa

a/. Về mặt vật lý: "***Tường lửa***" gồm có:

+ Một hay nhiều máy chủ kết nối với bộ định tuyến (Router) hoặc có chức năng như vậy.

+ Các phần mềm quản lý an ninh trên hệ thống máy chủ, Ví dụ Hệ quản trị xác thực (Athentication), Hệ cấp quyền (Authorization), Hệ kế toán (Accounting), ..

b/. Về mặt chức năng: "***Tường lửa***" có các thành phần:

+ Bộ lọc Packet (Packet - Filtering Router).

+ Cổng ứng dụng (Application - level Gateway hay Proxy Server).

+ Cổng mạch (Circuite - level Gateway).

1.2.1.5. Mạng riêng ảo (VPN: Virtual Private Network)

Khái niệm Mạng riêng ảo

Mạng riêng ảo (Virtual Private Networks: **VPN**) không phải là giao thức, cũng không phải là một phần mềm máy tính. Đó là một **chuẩn công nghệ** cung cấp sự ***liên lạc an toàn*** giữa hai thực thể bằng cách ***mã hóa các giao dịch*** trên mạng công khai (không an toàn, ví dụ như Internet).

Qua mạng công khai, một thông điệp được chuyển qua một số máy tính, Router, switch, … trước khi đến đích. Trên đường truyền tin, thông điệp có thể bị chặn lại, bị sửa đổi hoặc bị đánh cắp.

Người quản trị an ninh cần bảo đảm những điều kiện như sau:

- Tính riêng tư (Privacy): Người ngoài cuộc không thể hiểu được liên lạc đó.
- Tính toàn vẹn (Intergrity): Người ngoài cuộc không thể thay đổi được liên lạc đó.
- Tính xác thực (Authenticity): Người ngoài cuộc không thể tham gia vào liên lạc đó.

Để có khái niệm rõ hơn về VPN, ta cần hiểu về một số khái niệm sau:

- ***Định đường hầm*** (Tunneling):

Đó là một cơ chế dùng để ***đóng gói*** một giao thức vào trong một giao thức khác.

Trên Internet, "định đường hầm" cho phép những giao thức như IPX, ppleTalk,.. được mã hóa, sau đó đóng gói trong IP.

Trong VPN, "định đường hầm" che giấu giao thức lớp mạng nguyên thủy bằng cách mã hóa gói dữ liệu này vào trong một vỏ bọc IP.

Vỏ bọc IP thực chất là một gói IP, được truyền một cách an toàn qua mạng Internet. Tại bên nhận, khi nhận được gói trên, sẽ tiến hành gỡ bỏ vỏ bọc bên ngoài, giải mã thông tin dữ liệu trong gói này, và phân phối nó đến thiết bị truy cập thích hợp.

Đường hầm cũng là một ***đặc tính ảo*** trong VPN. Các công nghệ đường hầm được dùng phổ biến hiện nay cho truy cập VPN gồm có: giao thức định đường hầm điểm, PPTN, L2F, L2TP hoặc IP Sec, GRE (Generic Route Encapsulation).

-Bảo mật (***Mã hóa-*** Encryption): là việc chuyển các dữ liệu có thể đọc được (Clear text), vào trong một định dạng "khó" thể đọc được (Cipher text).

Mã hóa đối xứng là cùng một khóa và một thuật toán vừa dùng để mã hóa dữ liệu và cũng vừa để giải mã dữ liệu. Nói chính xác là: Từ khóa lập mã có thể tính được "dễ dàng" khóa giải mã và ngược lại.

Mã hóa phi đối xứng là mã hóa dữ liệu bằng một khóa và một thuật toán, giải mã bằng một khóa và thuật toán khác.

- ***Thỏa thuận về chất lượng dịch vụ*** (***QoS:*** Service Quality):

Thỏa thuận về ***Chất lượng dịch vụ*** thường định ra giới hạn cho phép về ***độ trễ trung bình*** của gói trong mạng. goài ra, các thỏa thuận này được phát triển thông qua các dịch vụ với nhà cung cấp.

Mạng riêng ảo là sự kết hợp của ***Định đường hầm + Bảo mật + Thỏa thuận QoS***.

1.2.2. Các phương pháp bảo đảm an toàn thông tin

1.2.2.1. Vấn đề bảo đảm An toàn thông tin

1/. Tại sao cần Bảo đảm An toàn thông tin

Ngày nay, sự xuất hiện Internet và mạng máy tính đã giúp cho việc trao đổi thông tin trở nên 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 dữ 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 tin tức về an ninh quốc gia là mục tiêu của tổ chức tình báo trong và ngoài nước.

Theo dữ liệu của CERT (Computer Emegency Respone Team: đội cấp cứu máy tính) số lượng vụ tấn công trên Internet ngày càng 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, 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 đảm bảo rằng nó là của đối tác đã gửi cho họ. Khi nhận được tờ Sec điện tử hay Tiền điện tử trên mạng, thì có cách nào để xác nhận xem nó là của đối tác thanh toán cho ta. Tiền đó là tiền thật hay tiền giả?

Thông thường, người gửi văn bản quan trọng phải ký phía dưới. Nhưng khi truyền trên mạng, văn bản hay giấy thanh toán có thể bị trộm cắp và phía dưới nó có thể dán một chữ ký khác. Tóm lại với cách thức như cũ, chữ ký rất dễ bị giả mạo.

Để giải quyết tình 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 có tên là "bảo mật" mà kỹ thuật rõ đơn giản, chẳng hạn trước khi truyền thông báo người gửi và người nhận thỏa thuận một số từ ngữ mà ta quen gọi là tiếng "lóng".

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

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 nhu cầu cần phát triển.

2/. Nội dung lý thuyết về An toàn thông tin

Mục tiêu của An toàn thông tin

- ***Bảo đảm bí mật (Bảo mật)***

Thông tin không bị lộ đối với người không được phép

- ***Bảo đảm toàn vẹn (Bảo toàn)***

Ngăn chặn hay hạn chế việc bổ sung, loại bỏ và sửa chữa dữ liệu không được phép.

- ***Bảo đảm xác thực (Chứng thực)***

Xác thực đúng thực thể cần kết nối, giao dịch.

Xác thực đúng thực thể có trách nhiệm về nội dung thông tin (Xác thực nguồn gốc thông tin)

- ***Bảo đảm sẵn sàng***

Thông tin sẵn sàng cho người dùng hợp pháp

3/. Các nội dung An toàn thông tin

a/. Nội dung chính

Để bảo vệ thông tin bên trong máy tính hay đang trên đường truyền tin, phải nghiên cứu về An toàn máy tính và An toàn truyền tin.

- ***An toàn thông tin trong máy tính*** (Computer Security)

Là sự bảo vệ các thông số cố định bên trong máy tính (Static Information).

Là khoa học về bảo đảm an toàn thông tin trong máy tính.

- ***An toàn thông tin trên đường truyền tin*** (Communication Security)

Là sự bảo vệ thông tin trên đường truyền tin (Dynamic Information)

(thông tin đang được truyền từ hệ thống này sang hệ thống khác).

b/. Hệ quả từ nội dung chính

Để bảo vệ thông tin bên trong máy tính hay đang trên đường truyền tin, phải nghiên cứu các nội dung sau:

- An toàn dữ liệu (Data Security)
- An toàn Cơ sở dữ liệu (CSDL) (Data base Security)
- An toàn hệ điều hành (Operaton system Security)
- An toàn mạng máy tính (Network Security)

1.2.2.2. Phương pháp bảo đảm An toàn thông tin

1/. Các chiến lược bảo đảm An toàn thông tin

a/. Cấp quyền hạn tối thiểu (Least Privilege)

Nguyên tắc cơ bản trong an toàn nói chung là "Hạn chế ưu tiên".

Mỗi đối tượng sử dụng hệ thống (người quản trị mạng, người sử dụng…) chỉ được cấp phát một số quyền hạn nhất định đủ dùng cho công việc của mình.

b/. Phòng thủ theo chiều sâu (Defense in Depth)

Nguyên tắc tiếp theo trong an toàn nói chung là "Bảo vệ theo chiều sâu".

Cụ thể là tạo lập nhiều lớp bảo vệ khác nhau cho hệ thống:

Thông tin / / / / /

Access right Login/Password Data Encription Physical Protection Firewall

2/. Các giải pháp bảo đảm An toàn thông tin

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

- "Che" dữ liệu (Mã hóa): thay đổi hình dạng dữ liệu gốc, người khác khó nhận ra.
- "Giấu" dữ liệu : cất giấu dữ liệu này trong môi trường dữ liệu khác.
- Bảo đảm toàn vẹn và xác thực thông tin.

Kỹ thuật:

+ Mã hóa, hàm băm, giấu tin, ký số, thủy ký….

+ Giao thức bảo toàn thông tin, giao thức xác thực thông tin…

b/. Phương pháp kiểm soát lối vào ra của thông tin

- Kiểm soát, ngăn chặn các thông tin vào ra hệ thống máy tính.
- Kiểm soát, cấp quyền sử dụng các thông tin trong hệ thống máy tính
- Kiểm soát, tìm diệt "sâu bọ" (Virus, ,…) vào ra hệ thống máy tính.

Kỹ thuật:

+ Mật khẩu (Password), Tường lửa (Firewall)

+ Mạng riêng ảo (Vitrual Private Network)

+ Nhận dạng, Xác thực thực thể, Cấp quyền hạn.

c/. Kiểm soát và xử lý các lỗ hổng trong An toàn thông tin

Khái niệm** "lỗ hổng***"

+Lỗ hổng thiếu an ninh trong hệ thống thông tin là một điểm yếu có thể tạo ra sự ngưng trệ của dịch vụ, thêm quyền đối với người dùng, hoặc cho phép truy nhập không hợp pháp vào hệ thống.

+Ví dụ:

Lỗ hổng có thể nằm ngay trong các dịch vụ như: sendmail, web, ftp,…

Lỗ hổng tồn tại trong hệ điều hành như windows NT, unix,…

Lỗ hổng có thể trong mạng máy tính, trong các kỹ thuật bảo vệ thông tin.

***Phân loại lỗ hổng theo mức nguy hiểm:**

Theo cách phân loại của bộ quốc phòng Mỹ, các lỗ hổng thiếu an ninh trên một hệ thống thông tin được phân loại như sau:

+*Lỗ hổng mức C* (Mức trung bình):

Lỗ hổng loại này có mức độ nguy hại trung bình, chỉ ảnh hưởng đến chất lượng dịch vụ, có thể làm ngưng trệ, gián đoạn hệ thống. Không phá hỏng dữ liệu, hay đạt được quyền truy nhập hợp pháp.

Ví dụ: Lỗ hổng loại này cho phép thực hiện tấn công "Từ chối dịch vụ" (DoS: Dinal of Server).

+*Lỗ hổng mức B* (Mức nguy hiểm):

Lỗ hổng loại này cho phép người dùng có thêm quyền trên hệ thống mà không cần kiểm tra tính hợp lệ. Lỗ hổng loại này thường có trong các ứng dụng của hệ thống thông tin, có thể dẫn đến mất hoặc lộ thông tin yêu cầu bảo vệ.

+*Lỗ hổng mức A* (Mức rất nguy hiểm):

Lỗ hổng loại này cho phép người dùng ở ngoài có thể truy nhập vào hệ thống bất hợp pháp. Lỗ hổng này rất nguy hiểm, có thể phá hủy hệ thống.

***Phân loại lỗ hổng theo các thành phần của hệ thống thông tin:**

Theo cách phân loại này, các lỗ hổng thiếu an ninh trên một hệ thống thông tin được phân loại như sau:

+Lỗ hổng trong mạng máy tính:

Ví dụ: Lỗ hổng trong giao thức ARP.

+Lỗ hổng trong các kỹ thuật bảo vệ thông tin:

Ví dụ: Lỗ hổng trong các kỹ thuật mã hóa, ký số,…

+Các "lỗ hổng" trong các Thuật toán hay giao thức mật mã, giấu tin

+Các "lỗ hổng" trong các Giao thức mạng

+Các "lỗ hổng" trong các Hệ điều hành mạng

+ Các "lỗ hổng" trong các Ứng dụng

***Kiểm soát và xử lý các "Lỗ hổng" thiếu an ninh:**

+Việc đầu tiên cần phải xác định loại lỗ hổng, từ đó xác định rõ nguồn gốc điểm yếu này, sau đó tìm cách xử lý thích hợp.

Ví dụ: lỗ hổng trong giao thức ARP. Một cách xử lý là trước khi giao dịch với một nút mạng, phải xác thực nút mạng này.

d/. Phòng tránh các dạng tấn công Hệ thống thông tin

Xây dựng "hành lang", "đường đi" An toàn cho thông tin gồm 3 phần:

- Hạ tầng mật mã khóa công khai (Public Key Infrastructure - PKI)
- Kiểm soát lối vào – ra : Mật khẩu, Tường lửa, Mạng riêng ảo, Cấp quyền hạn
- Kiểm soát và Xử lý các lỗ hổng

e/. Phương pháp phòng chống "Tấn công" hệ thống thông tin

***Phát hiện hệ thống bị tấn công:**

Không có hệ thống nào có thể đảm bảo được an toàn tuyệt đối. Người quản trị hệ thống phải có các biện pháp kiểm tra hệ thống xem có dấu hiệu bị tấn công hay không. Các biện pháp gồm có:

-Kiểm tra các dấu hiệu hệ thống bị tấn công: Hệ thống thường bị "treo" hoặc bị "Crash" bằng những thông báo lỗi không rõ ràng. Khó xác định nguyên nhân do thiếu thông tin liên quan.

Trước tiên hãy xác định lỗi có phải do phần cứng hay không. Nếu không phải do phần cứng, hãy nghĩ đến khả năng máy tính bị tấn công.

-Kiểm tra các tài khoản người dùng mới trong hệ thống: Một số tài khoản lạ, nhất là UID của tài khoản đó bằng 0.

-Kiểm tra xuất hiện các tập tin lạ: Thường phát hiện thông qua cách đặt tên các tập tin. Mỗi người quản trị hệ thống nên có thói quen đặt tên tập tin theo một mẫu nhất định để dễ dàng phát hiện tập tin lạ.

-Kiểm tra thời gian thay đổi trên hệ thống, đặc biệt là chương trình login, sh, hoặc các scripts khởi động trong /etc/init.d, etc/rc.d…

-Kiểm tra hiệu năng của hệ thống. Sử dụng các tiện ích theo dõi tài nguyeenvaf các tiến trình đang hoạt động trên hệ thống như pas hoặc top…

-Kiểm tra hoạt động của các dịch vụ mà hệ thống cung cấp. Ta đã biết mục đích tấn công là làm tê liệt hệ thống.

-Kiểm tra truy nhập bằng các Acount thông thường, đề phòng các Acount này bị truy nhập trái phép và thay đổi quyền hạn mà các người dùng hợp pháp không kiểm soát được.

-Kiểm tra các file liên quan đến cấu hình mạng và dịch vụ như /etc/ineted.còn, bỏ các dịch vụ không cần thiết. Đối với dịch vụ không cần thiết chạy dưới quyền root thì không chạy bằng các quyền yếu hơn.

-Kiểm tra các phiên bản của Sendmail, /bin/mail, ftp, fingerd, tham gia các nhóm tin về bảo mật để cá thông tin về lỗ hổng của dịch vụ sử dụng.

***Phòng chống tấn công hệ thống mật mã bảo đảm thông tin:**

Tùy theo từng hệ thống mật mã, người ta có phương pháp riêng để phòng chống tấn công.

+Ví dụ khi tấn công bản mã, kẻ gian có hai phiwowng pháp chính:

Dùng thống kê ngôn ngữ học, để xác định bản rõ của bản mã.

Tính ra khóa bí mật để giải mã, xác định bản rõ.

+Ví dụ khi tấn công để giả mạo chữ ký số, kẻ gian có các phương pháp:

Giả mạo đồng thời cả tài liệu cùng chữ ký số.

Tính ra khóa bí mật để ký vào tài liệu giả mạo

+Ví dụ khi tấn công tin giấu, kẻ gian có các phương pháp:

Nghiên cứu môi trường hay giấu tin, để xác định có giấu tin không;

Từ đó bằng các kỹ thuật để xác định độ dài tin giấu, hay tách tin giấu.

Khi nghi vấn có tin giấu, kẻ gian phá hoại môi trường giấu tin

f/. Phương pháp bảo vệ thông tin bằng nhiều lớp

Vì không có giải pháp an toàn tuyệt đối, nên người ta thường sử dụng đồng thời nhiều mức bảo vệ khác nhau, tạo thành nhiều lớp rào chắn đối với các hoạt động xâm phạm.

-Lớp 1: sử dụng các phương pháp mã hóa (Encryption).

-Lớp 2: Xác định quyền truy nhập và quyền hạn truy nhập.

-Lớp 3: Hạn chế tài khoản truy nhập (đăng ký tên và mật khẩu).

-Lớp 4: Hệ thống tường lửa (Firewall):

Tự động ngăn chặn các xâm nhập trái phép và cho lọc các gói tin không mong muốn gửi đi.

-Lớp 5: bảo vệ vật lý, ngăn chặn các truy nhập bất hợp pháp vào hệ thống.

Ví dụ: Các biện pháp ngăn chặn người không có trách nhiệm vào phòng máy, dùng hệ thống khóa trên máy tính, cài đặt hệ thống báo động khi có truy nhập trái phép.

3/. Các kỹ thuật bảo đảm An toàn thông tin

- Kỹ thuật Diệt trừ: Virus máy tính, Chương trình trái phép ("Ngựa Troire")…
- Kỹ thuật Tường lửa: Ngăn chặn truy cập trái phép, lọc thông tin không hợp pháp.
- Kỹ thuật Mạng riêng ảo: Tạo ra hành lang riêng cho các thông tin "đi lại".
- Kỹ thuật Mật mã: Mã hóa, ký số, các giao thức mật mã, chống chối cãi…
- Kỹ thuật Giấu tin: Che giấu thông tin trong môi trường dữ liệu khác.
- Kỹ thuật Thủy ký: Bảo vệ bản quyền tài liệu số hóa.
- Kỹ thuật Truy tìm dấu vết kẻ trộm tin.

4/. Các công nghệ bảo đảm An toàn thông tin

- Các công nghệ chung:

  Tường lửa, Mạng riêng ảo, PKI (Public Key Infrastructure: hạ tầng cơ sở mật mã khóa công khai), Thẻ thông minh.

- Công nghệ cụ thể:

  SSL, TLS, PGP, SMINE…

1.2.3.Công cụ bảo đảm An toàn thông tin

+ Nén dữ liệu.

+ Mã hóa dữ liệu.

+ Giấu tin.

+ Chữ ký số.

+ Hàm băm.

Chương2. MỘT SỐ BÀI TOÁN VỀ AN TOÀN THÔNG TIN TRONG GIAO DỊCH TRỰC TUYẾN

2.1. TỔNG QUAN VỀ GIAO DỊCH TRỰC TUYẾN

Các tiêu chí về dịch vụ hành chính công trực tuyến, được đề cập trong công văn số 1448/BBCVT-KHTC.

2.1.1. Giao dịch trực tuyến cấp độ 1

Một dịch vụ hành chính công trực tuyến được xem là đạt mức 1, nếu như dịch vụ hành chính công đó có đầy đủ hoặc phần lớn các thông tin sau:

+Quy trình thực hiện dịch vụ hành chính công đó.

Ví dụ như sở cứ, cơ quan thực hiện, địa chỉ,

+Thủ tục thực hiện dịch vụ, các giấy tờ cần thiết.

+Các bước tiến hành, thời gian thực hiện, chi phí thực hiện dịch vụ.

Chú ý: với mức 1, chưa yêu cầu sử dụng mạng máy tính.

2.1.2. Giao dịch trực tuyến cấp độ 2

Một dịch vụ hành chính công trực tuyến được xem là đạt mức 2, nếu như:

a/. Đạt được tiêu chí mức 1.

b/. Cho phép người dùng chuyển về các mẫu đơn, hồ sơ (qua mạng máy tính) để họ có thể in ra giấy, hoặc điền vào các mẫu đơn.

Việc nộp lại hồ sơ sau khi hoàn thành được thực hiện qua bưu điện, hoặc người dùng trực tiếp mang đến cơ quan thụ lý hồ sơ.

Nếu một dịch vụ hành chính công trực tuyến được đăng ký mức 2, tuy có cung cấp các mẫu đơn hồ sơ để người dùng dịch vụ tải về, nhưng không cần đầy đủ các thông tin cần thiết đối với dịch vụ hành chính công trực tuyến mức 1, cũng không được xem là dịch vụ hành chính công trực tuyến mức 2 cũng như mức 1.

2.1.3. Giao dịch trực tuyến cấp độ 3

Một dịch vụ hành chính công trực tuyến được xem là đạt mức 3, nếu như:

a/. Đạt được các tiêu chí mức 1.

b/. Đạt được các tiêu chí mức 2.

c/. Cho phép người dùng điền trực tuyến vào các mẫu đơn, hồ sơ và ***gửi lại trực tuyến*** các mẫu đơn, hồ sơ tới cơ quan và người thụ lý hồ sơ.

Các giao dịch trong quá trình thụ lý hồ sơ và cung cấp dịch vụ được thực hiện qua mạng máy tính. Tuy nhiên, việc thanh toán chi phí và trả kết quả sẽ thực hiện khi người dùng dịch vụ đến trực tiếp cơ quan cung cấp dịch vụ.

Ghi chú:

Nếu một dịch vụ hành chính công trực tuyến được đăng ký mức 3, có cung cấp cơ chế điền biểu mẫu và xử lý trực tuyến, nhưng không cung cấp đầy đủ các thông tin cần thiết đối với dịch vụ hành chính công trực tuyến mức 1, thì cũng không được xếp mức cho dịch vụ hành chính công.

2.1.4. Giao dịch trực tuyến cấp độ 4

Một dịch vụ hành chính công trực tuyến được xem là đạt mức 4, nếu như :

a/. Đạt được các tiêu chí mức 1.

b/. Đạt được các tiêu chí mức 2.

c/. Đạt được các tiêu chí mức 3.

d/. Việc thanh toán chi phí được thực hiện trực tuyến, việc trả kết quả có thể thực hiện trực tuyến, hoặc qua đường bưu điện.

Ghi chú:

Nếu một dịch vụ hành chính công trực tuyến được đăng ký mức 4, có cung cấp cơ chế điền biểu mẫu và xử lý trực tuyến, nhưng không cung cấp đầy đủ các thông tin cần thiết đối với dịch vụ hành chính công trực tuyến mức 1, thì cũng không được xếp mức cho dịch vụ hành chính công .

2.2. BÀI TOÁN BẢO MẬT THÔNG TIN

2.2.1. Bài toán bảo mật thông tin

Thực thể không được cấp quyền không thể xem trộm bản tin.

Ví dụ: kẻ gian không được xem trộm tài liệu mật.

2.2.2. Phương pháp giải quyết bài toán bảo mật thông tin

Để bảo mật thông tin, hiện nay có nhiều phương pháp kỹ thuật, nhưng người ta thường dùng phương pháp mã hóa thông tin.

***Mã hóa thông tin:** (Thực tế dùng hệ mã hóa khóa đối xứng).

+Đầu vào: Chọn tài liệu cần mã hóa (bản rõ): **X.**

-Chon thuật toán mã hóa **E**. Chọn khóa mã hóa **k.**

-Ấn nút "mã hóa".

+Đầu ra: bản mã **Y** của bản rõ **X** : $\mathbf{Y= E_k (X).}$

Ví dụ:

Nhân viên hành chính chuyển thư mời họp **X**, cần bảo mật thư mời, họ phải thực hiện các bước sau, sẽ nhận được bản mã **Y** của bản rõ **X.**

+Bước 1: Mã hóa giấy mời. (Thực hiện các thao tác mã hóa như trên).

Cho đơn giản, giả thiết rằng các thành viên tham dự họp đã thống nhất một khóa giải mã chung duy nhất. Nếu cần an toàn hơn, người ta sử dụng một hệ mã hóa "quảng bá", mỗi người có khóa giải mã riêng, nhưng khóa lập mã vẫn chung do nhân viên hành chính quy định.

+Bước 2: chuyển thư mời đã mã hóa **Y** cho các thành viên dự họp.

Ghi địa chỉ E-mail các thành viên dự họp, chuyển bản mã Y qua mạng máy tính

Khi nhận được bản mã tài liệu, trong hệ thống giao dịch trực tuyến, người nhận chọn chức năng giải mã và thực hiện các thao tác sau:

+Đầu vào: Chọn tài liệu cần giải mã (bản mã): **Y.**

-Chọn thuật toán giải mã **D**. Chọn khóa giải mã **k.**

-Ấn nút "giải mã".

+Đầu ra: Tài liệu gốc (bản rõ): : $\mathbf{X= D_k (Y).}$

2.3. BÀI TOÁN BẢO TOÀN THÔNG TIN

2.3.1. Bài toán bảo toàn thông tin

Thực thể không được cấp quyền không có thể sửa đổi bản tin.

Ví dụ: kẻ gian không được sửa đổi nội dung công văn

2.3.2. Phương pháp giải quyết bài toán bảo toàn thông tin

Để bảo toàn thông tin, hiện nay có nhiều phương pháp, kỹ thuật, nhưng người ta thường dùng phương pháp tạo đại diện thông điệp, hay chữ kí số.

***Tạo đại diện thông điệp:**

+Đầu vào: Chọn tài liệu cần tạo đại diện: **X.**

-Chọn hàm băm **H.** (Thực tế dùng hàm băm dòng MD hay SHA).

-Ấn nút "Tạo đại diện": Nhận được đại diện **Y** của **X** (với độ dài cố định).

+Đầu ra: Kết quả là cặp **(X,Y), Y = H(X).**

Ví dụ:

Nhân viên hành chính chuyển thư mời họp **X** các thành viên dự họp, cần bảo toàn thư mời, họ cần thực hiện các bước sau:

+Bước 1: tạo đại diện thư mời**: Y = H(X)**

Để cho đơn giản, giả thiết rằng các thành viên tham dự họp đã thống nhất dùng một hàm băm chung duy nhất **H.**

+Bước 2: Ghi địa chỉ E-mail các thành viên dự họp, chuyển thư mời họp kèm theo đại diện thư mời: **(X,Y).**

***Kiểm tra sự bảo toàn thông tin:**

Khi nhận được tài liệu (kèm đại diện tài liệu): **(X,Y),** người nhận chọn chức năng tạo đại diện tài liệu và so sánh hai đại diện tài liệu.

-Chọn tài liệu **X** cần tạo đại diện.

-Chọn hàm băm (Dùng hàm băm H như của người gửi đại diện tài liệu).

-**Ấn nút** "Tạo đại diện": Nhận được đại diện $\mathbf{Y^+}$ của **X:** $\mathbf{Y^+ = H(X).}$

-So sánh hai đại diện: đại diện cũ **Y** (của người gửi) và đại diện mới $\mathbf{Y^+}$ (người nhận tạo ra). Nếu hai đại diện trùng nhau, thì tài liệu đã được bảo toàn.

Ví dụ:

Khi nhận được thư mời họp kèm đại diện thư mời**: (X,Y),** để kiểm tra thư mời có bị sửa đổi khi truyền tin, họ phải thực hiện hai bước như trên:

+Bước 1: Tạo đại diện của thư mời họp vừa nhận: $\mathbf{Y^+ = H(X).}$

+Bước 2: So sánh hai đại diện của thư mời họp: **Y** và $\mathbf{Y^+}$.

Nếu hai đại diện trùng nhau, thì thư mời họp đã được bảo toàn.

Nếu hai đại diện không trùng nhau, thì thư mời họp đã bị sửa đổi.

2.4. BÀI TOÁN XÁC THỰC THÔNG TIN

2.4.1. Bài toán xác thực thông tin

Thực thể nhận tin có thể định danh được thực thể gửi tin và ngược lại.

Ví dụ: Kẻ gian không thể giả mạo chữ ký trong tài liệu.

2.4.2. Phương pháp giải quyết bài toán xác thực thông tin

Để xác thực thông tin, hiện nay có nhiều phương pháp, kỹ thuật, nhưng người ta thường dùng "Chữ ký số".

***Tạo chữ ký số trên tài liệu:** (Tạo chữ ký **Z** trên tài liệu **X**)

+Đầu vào: Chọn tài liệu cần ký: **X.**

-Chọn thuật toán ký số: **Sig.** Chọn khóa ký số **k.**

-**Ấn nút** "Ký số". Nhận được chữ ký **Z** trên tài liệu **X.**

+Đầu ra: Kết quả là cặp **(X, Z), $Z = Sig_k (X)$.**

***Kiểm tra chữ ký số trên tài liệu:** (Kiểm tra chữ ký **Z** trên tài liệu **X**)

+Đầu vào: Chọn tài liệu có chữ ký và chữ ký cần kiểm tra: **(X, Z).**

-Chọn thuật toán kiểm tra chữ ký số: **Ver.** Chọn khóa kiểm tra chữ ký **k**.

-**Ấn nút** "kiểm tra chữ ký". (Thuật toán tương ứng với thuật toán ký).

+Đầu ra: Kết quả **$Ver_k (Z)$ = (T or F).**

Chú ý:

Chữ ký số có dung lượng lớn (độ dài) ít nhất cũng bằng tài liệu cần ký (tài liệu gốc), như vậy tốn nhiều thời gian ký, thời gian truyền chữ ký, tốn bộ nhớ lưu chữ ký, tốn băng thông truyền chữ ký,… Do đó trên thực tế người ta ký số trên đại diện tài liệu, vì nó có dung lượng nhỏ nhỏ.

***Tạo chữ ký số trên đại diện tài liệu:**

+Đầu vào: Chọn tài liệu cần ký**: X.**

-Tạo đại diện của tài liệu cần ký: **Y = H(X).**

-Chọn thuật toán ký số: **Sig.** Chọn khóa ký số **k.**

-Ấn nút "ký số". Nhận được chữ ký **Z** trên đại diện **Y: $Z = Sig_k (Y)$.**

Z cũng được xem là chữ ký trên tài liệu cần ký **X.**

+Đầu ra: Kết quả là cặp **(X, Z)**, trong đó **$Z = Sig_k (Y)$, $Y = H(X)$.**

Ví dụ:

Nhân viên hành chính xin chữ ký người quản lý trên thư mời họp **X,** sau đó chuyển thư **X** kèm chữ ký **Z** cho các thành viên dự họp, họ thực hiện:

+Bước 1: Người quản lý "ký" trên thư mời họp X, bằng việc "ký" trên thư mời **$Y = H(X)$.** Chữ ký là **$Z = Sig_k (Y)$.**

+Bước 2: Ghi địa chỉ E-mail các thành viên dự họp, chuyển thư mời họp kèm theo chữ ký trên đại diện thư mời**: (X,Z).**

***Kiểm tra chữ ký số trên đại diện tài liệu:**

(Kiểm tra chữ ký **Z** trên đại diện **Y** của tài liệu **X**)

+Đầu vào: Cặp **(X, Z),** trong đó **$Z = Sig_k (Y)$, $Y = H(X)$.**

-Tạo đại diện **Y** của tài liệu **X**. Sẽ nhận được **$Y = H(X)$.**

(Dùng hàm băm H như của người gửi đại diện tài liệu).

-Chọn tài liệu có chữ ký và chữ ký cần kiểm tra**: (Y,Z).**

-Chọn thuật toán kiểm tra chữ ký số: **Ver**. Chọn khóa kiểm tra chữ ký **k**.

-**Ấn nút** "kiểm tra chữ ký". (Thuật toán tương ứng với thuật toán ký).

+Đầu ra: Kết quả **$Ver_k (Z) = (T \text{ or } F)$.**

Chú ý:

Khi nhận được chữ ký Z trên đại diện tài liệu X, tức là cặp (X,Z), người nhận sẽ kiểm tra chữ ký Z trên đại diện tài liệu X.

Nếu không có đại diện tài kiệu đi kèm, thì người nhận phải tạo ra đại diện tài liệu này là Y = H(X). Kiểm tra chữ ký Z trên đại diện Y

Chương 3. THỬ NGHIỆM CHƯƠNG TRÌNH BẢO ĐẢM ATTT

Trong chương 3, đồ án tốt nghiệp thử nghiệm chữ ký Elgamal.

3.1. CẤU HÌNH HỆ THỐNG

3.1.1. Phần cứng

Yêu cầu phần cứng của chương trình: chiếm dung lượng nhỏ (khoảng 4,3 MB), có thể chạy trên mọi thế hệ của máy tính có hệ điều hành DOS.th

3.1.2. Phần mềm

Yêu cầu phần mềm của chương trình:

+Máy phải cài đặt và sử dụng một trong các hệ điều hành sau: window 2000, window XP (pack 1, 2, 3), window server, window 7

.+ Phần mềm:Tubo C++ 3.0

-Ưu điểm: miễn phí, không cần cài đặt, biên dịch và chạy chương trình nhanh, môi trường tích hợp thuận tiện.

-Nhược điểm: không thể biên dịch chương trình chạy trên window, không hỗ trợ các công nghệ mới như nhắc nhở người dùng các từ khoá, hàm và kiểu dữ liệu, thao tác soạn thảo của Tubo C++3.0 cũng không tiện lợi vì đòi hỏi sử dụng các tổ hợp phím khá phức tạp…

3.2. CÁC THÀNH PHẦN CỦA CHƯƠNG TRÌNH

***Khái niệm chữ kí số**

Một sơ đồ chữ ký gồm bộ 5 (P, A, K, S, V) thoả mãn các điều kiện dưới đây:

P là tập hữu hạn các bức điện (thông điệp) có thể

A là tập hữu hạn các chữ kí có thể

K không gian khoá là tập hữu hạn các khoá có thể

Sig_k là thuật toán ký $P \rightarrow A$

$x \in P \rightarrow y = Sig_k(x)$

Ver_k là thuật toán kiểm thử: (P, A) $\rightarrow$ (Đúng, sai)

$$Ver_k(x, y) = \begin{cases} \text{Đúng} & \text{Nếu } y = Sig_k(x) \\ \text{Sai} & \text{Nếu } y \neq Sig_k(x) \end{cases}$$

***Phân loại sơ đồ chữ ký số**

Có nhiều loại chữ kí tuỳ theo cách phân loại sau đây là một số cách:

Cách 1: Phân loại chữ kí theo đặc trưng kiểm tra chữ kí gồm có:

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

Ví dụ: Chữ kí RSA là chữ kí khôi phục thông điệp.

2/. Chữ kí không khôi phục thông điệp: Là loại chữ kí, trong đó người gửi chỉ cần gửi "chữ ki", phải gửi kèm cả thông điệp đã được "kí" bởi chữ kí này. Ngược lại người nhận sẽ không có được thông điệp gốc.

Ví dụ: Chữ kí Elgamal là chữ kí không khôi phục thông điệp

Cách 2: Phân loại chữ kí theo mức an toàn gồm có:

1/. Chữ kí "không thể phủ nhận": Nhằm tránh việc nhân bản chữ kí để sử dụng nhiều lần, tốt nhất là người gửi tham gia trực tiếp vào việc kiểm thủ chữ kí. điều đó được thực hiện bằng một giao thức kiểm thủ, dưới dạng một giao thúc mời hỏi và trả lời.

Ví dụ: Chữ kí không phủ định (Chaum – van Antverpen).

2/. Chữ kí "một lần":

Để đảm bảo an toàn, "Khoá kí" chỉ dùng một lần (one time) trên một tài liệu.

Ví dụ: Chữ kí một lần Lamport, chữ kí Fail – stop (Van Heyst & Pedersen).

Cách 3: Phân loại chữ kí theo ứng dụng đặc trưng gồm có:

Chữ kí "mù" (Blind Signature)

Chữ kí "nhóm" (Group Signature)

Chữ kí "bội" (Multy Signature)

Chữ kí "mù nhóm" (Blind Group Signature)

Chữ kí "mù bội" (Blind Multy Signature)

* **Sơ đồ chữ kí Elgamal:**

+Tạo cặp khoá (bí mật, công khai) (a,h):

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

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

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

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

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

+Kí số:

Dùng 2 khoá kí: khoá **a** và khoá ngẫu nhiên bí mật $\mathbf{r} \in \mathbf{Z_{p-1}^*}$

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

Chữ kí trên $\mathbf{x} \in \mathbf{P}$ là $\mathbf{y} = \mathbf{Sig_k}\ \mathbf{(x,r)} = \mathbf{(\gamma, \delta)}$, $\mathbf{y} \in \mathbf{A}$ (E_1)

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

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

+Kiểm tra chữ kí:

$Ver_k(x, y, \delta)$ = đúng $\leftrightarrow$ $\mathbf{h^{\gamma} * \gamma^{\delta}} \equiv \mathbf{g^x} \mod \mathbf{p}$ (E_2)

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

$\mathbf{h^{\gamma} * \gamma^{\delta}} \equiv \mathbf{g^{a\,\gamma}} * \mathbf{g^{r*\delta}} \mod \mathbf{p} \equiv \mathbf{g^{(a\,\gamma + r*\delta)}} \mod \mathbf{p} \equiv \mathbf{g^x} \mod \mathbf{p}$

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

Ví dụ: Chữ ký Elgamal trên dữ liệu **x= 112**.

+Tạo cặp khoá (bí mật, công khai) (a,h):

Chọn số nguyên tố **p** = 463 . Đặt $\mathbf{P = Z_p^*}$, $\mathbf{A = Z_p^* \times Z_{p-1}^*}$

Chọn phần tử nguyên thuỷ **g**= 2 $\in \mathbf{Z_p^*}$.

Chọn khoá bí mật là **a**=211 $\in \mathbf{Z_p^*}$.

Tính khoá công khai $\mathbf{h \equiv g^a} \mod \mathbf{p} = \mathbf{2^{211}} \mod 463 = 249$.

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

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

+Kí số: Chọn ngẫu nhiên khóa bí mật r = 235 $\in \mathbf{Z_{p-1}^*}$**.** Khoá ký là (a, r).

Vì $\mathbf{r} \in \mathbf{Z_{p-1}^*}$, nên nguyên tố cùng **p-1**, do đó tồn tại $\mathbf{r^{-1}} \mod \mathbf{(p-1).}$ Cụ thể:

UCLN (r, p-1) = UCLN (235, 462) = 1

nên $r^{-1} \mod (p-1) = 235^{-1} \mod 462 = 289$.

Chữ kí trên dữ liệu **x** = 112 là **(γ,δ)** = (16,18).

Trong đó

$\gamma = \mathbf{g^r} \mod \mathbf{p} = 2^{235} \mod 463 = 16$

$\boldsymbol{\delta = (x - a*\gamma)*r^{-1}} \mod \mathbf{(p-1)} = (\mathbf{112}\text{-}211*16)* 289 \mod 462 = \mathbf{108}$

+Kiểm tra chữ kí:

Ver_k (x, y, δ) = đúng $\leftrightarrow$ $h^{\gamma}*\gamma^{\delta} \equiv g^{x} \mod p$

$h^{\gamma} * \gamma^{\delta} = 249^{16} * 16^{108} \mod 463 = \mathbf{132}$

$g^{x} \mod p = 2^{112} \mod 463 = \mathbf{132}$.

Hai giá trị đó bằng nhau, như vậy chữ ký là đúng.

*** Các thành phần của chương trình:** Gồm 3 phần

- Sinh khoá:

Input: hai số nguyên tố p, g

Output: Cặp khóa (bí mật, công khai)

- Ký số:

Input: Bản rõ x, dùng 2 khoá kí: khoá **a** và khoá ngẫu nhiên bí mật $r \in Z_{p-1}^{*}$

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

Chữ kí trên $x \in P$ là $y = Sig_k(x,r) = (\gamma,\delta)$, $y \in A$ (E_1)

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

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

Out put: Chữ ký số

- Kiểm tra chữ ký số

Input: bản rõ x,

Output: Xác thực chữ ký đúng hoặc sai chữ ký:

3.3. CHƯƠNG TRÌNH

```
#include<stdio.h>
#include<conio.h>
#include<math.h>
#include <stdlib.h>
#include<string.h>
//=========================================
int roso(char s);
char rochu(int s);
void kyvb(char *tep);
int Kiemthu();
long int kha_nghich(long int b, long int n);
void output();
void Elgamal();
long exp_mod(long x, long b, long n);
//=========================================
long int p,a,alpha,k,beta,k1;
long int delta,gamma;
int chuky[500],sl;
//=========================================
int roso(char s)
{
  return s;
}
char rochu(int s)
{
  return s;
```

```
}
//================ky cao van ban==============
void kyvb(char *tep)
{
  clrscr();
  char c,c1;
  long int so;
  int so1,so2,l,i;
  FILE *f,*f1;
  char *tep1;
  char *s;
  sl=1;
  chuky[0]=gamma;
  f=fopen(tep,"a+t");
  if(f==NULL)
     {
     printf("Loi mo tep!!!");
     getch();
     exit(0);
     }
  while(!feof(f))
  {
      fscanf(f,"%c",&c);      //doc tung ky tu trong tep.
      if(c!=10)
           {
              so=roso(c);     //lay gia tri so cua tung ky tu c.
              delta=((so-a*gamma)*k1)%(p-1);   //tinh gia tri ky la gamma.
```

```
            delta=delta+(p-1);     //vi delta<0
            chuky[sl]=delta;      //gia tri ky tren tung ky tu.
            sl++;
        }
  }
  fclose(f);
 }
//============Ham kiem thu chu ky================
int Kiemthu()
{
  char *tep,*tep1;
  char c;
  int d;
  long int so;
  FILE *f,*f1;
  printf("Nhap ten tep can kiem thu:");fflush(stdin);
  gets(tep);
  printf("Nhap ten tep chua chu ky can kiem thu:");fflush(stdin);
  gets(tep1);
  f=fopen(tep,"rt");
  f1=fopen(tep1,"rt");
  int kt=1;
  fscanf(f1,"%2d",&sl);
  fscanf(f1,"%2d\n",&gamma);
  int i=1;
  while(i<sl-1)
  {
```

```
            fscanf(f,"%c",&c);
            so=roso(c);
            fscanf(f1,"%3d",&d);
            if((a*gamma+k*d)%(p-1)!=so)
             { kt=0;
              return kt;}
          i++;
   }
  fclose(f1);
  fclose(f);
  return kt;
}
//===========Tinh Kha nghich ================
long int kha_nghich(long int b, long int n)
    {
          long int n0, b0;
          long int t, t0, temp, q, r;
          n0=n;  b0=b;  t0=0;   t=1;
          q=floor(n0/b0);
          r=n0-q*b0;
          while(r>0){
                              temp=t0-q*t;
                              if (temp < 0)
                                        temp = n- ((-temp) % n);
                              else
                                        temp = temp % n;
                              t0=t;
```

```
                    t=temp;
                    n0=b0;
                    b0=r;
                    q=floor(n0/b0);
                    r=n0-q*b0;
                }
        if(b0!=1)
        {
           printf("Khong co a"); return 0;}
        else return(t%n);
   }
//=================================================
void output()
{
 char c;
 char *tep;
 FILE *f;
 printf("Nhap ten tep can luu chu ky:");fflush(stdin);
 gets(tep);
 f=fopen(tep,"wt");
 if(f==NULL)
  {
  printf("\nLoi mo tep!!!!!!");
  getch();
  exit(0);
  }
   fprintf(f,"%d",sl);
```

```
    fprintf(f," %d\n",chuky[0]);
    for(int i=1;i<sl;i++)
            {
              fprintf(f," %2d",chuky[i]);
            }
    fclose(f);
 }
//=============Ham chinh==============================
void Elgamal()
{
     printf("\n\n =====* CHU KY ELGAMAL *======");
   long int x,y;
   int ch;
   char *tep,*tep1;
     FILE *f,*f1;
   char c;
     printf("\n\nNhap so nguyen to p:");scanf("%ld",&p);
     printf("Nhap a:");scanf("%ld",&a);
     printf("Nhap alpha:");scanf("%ld",&alpha);
     printf("Nhap khoa k:");scanf("%ld",&k);
     beta=exp_mod(a,alpha,p);
     gamma=exp_mod(k,alpha,p);
     k1=kha_nghich(k,p-1);
   while(1)
     {
          printf("\n\nCAC LUA CHON CHO CHU KY SO ELGAMAL\n");
          printf("[1].Ky \n");
```

```
printf("[2].Hien thi \n");
printf("[3].Kiem thu\n");
printf("[0].Thoat!!\n");
printf("\n\nMoi ban chon:");scanf("%d",&ch);
switch(ch)
 {
    case 1:{
            printf("Nhap ten tep:");fflush(stdin);
            gets(tep);
            kyvb(tep);
            output();
            }break;
    case 2:{
            printf("Nhap ten can hien thi:");fflush(stdin);
            gets(tep);
            printf("Nhap tep ten chua chu ky tuong ung:");fflush(stdin);
            gets(tep1);
            f=fopen(tep,"r+t");
            int d;
            printf("\n\n  VAN BAN\n\n");
            while(!feof(f))
            {
                fscanf(f,"%c",&c);
                printf("%c",c);
            }
            f1=fopen(tep1,"r+t");
            printf("\n\n CHU KY\n\n");
```

```
                    fscanf(f1,"%d",&sl);
                    fscanf(f1,"%d",&gamma);
                    printf("do dai xau:%2d" "gia tri gamma:%2d\n",sl,gamma);
                    for(int i=0;i<sl-1;i++)
                        {
                          fscanf(f1,"%d",&d);
                          printf(" %2d",d);
                        }
                    fclose(f1);
                    fclose(f1);
                   }break;
               case 3:{
                        if(Kiemthu()==1)printf("Chu ky dung!!");
                        else printf("Chu ky gia!!");
                         }
               case 0:break;
             }
           if(ch==0) break;
   }
   getch();
}
//=========== Tinh Mod ============
long exp_mod(long x, long b, long n)
{
          long a = 1l, s = x;
   while (b != 0) {
    if (b & 1l) a = (a * s) % n;
```

```
            b >>= 1;
        if (b != 0) s = (s * s) % n;
}
        if (a < 0) a += n;
  return a;
}
//============================================================
void menu()
{
    int c;
    while(
  {
        clrscr();
        printf("\n\n=====* CHUONG TRINH CHU KY SO *=======");
        printf("\n[1].CHU KY ELGAMAL");
        printf("\n[2].Thoat khoi chuong trinh");
        printf("\n\n Moi ban chon:");scanf("%d",&c);
     switch(c)
        {
        case 2:
              return;
        case 1 :
                 Elgamal();
                 break;
        }

  }
```

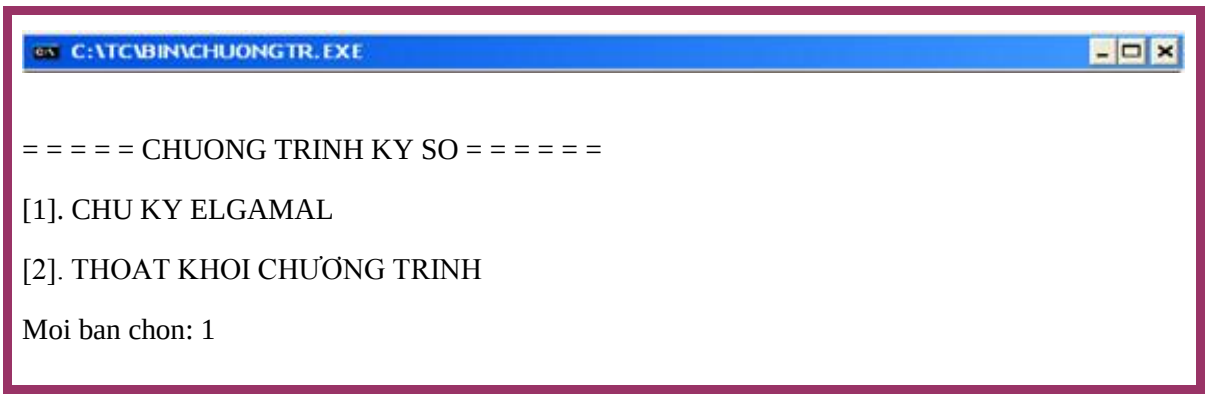
```
}
//=========================================
void main()
{clrscr();
  menu();}
//================== Ket thuc ===============
```

3.4. HƯỚNG DẪN SỬ DỤNG CHƯƠNG TRÌNH

+Khởi động TC để vào chương trình.

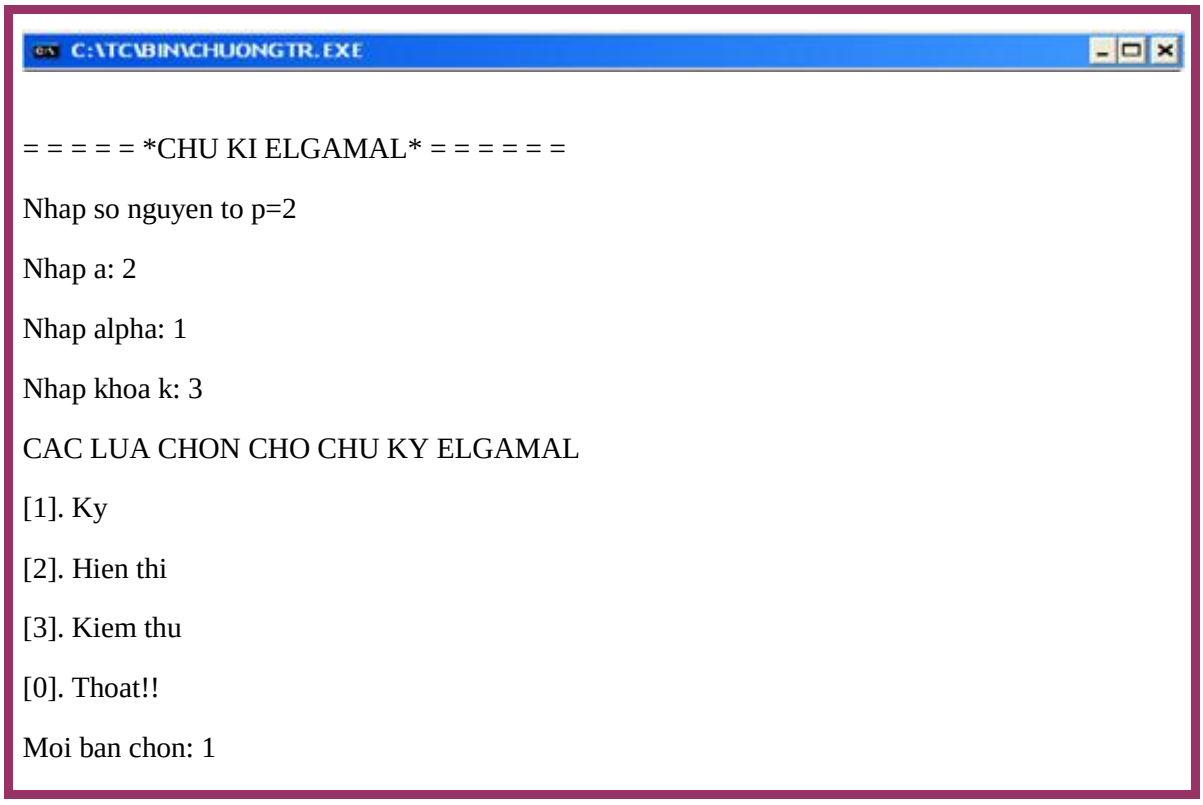
+Trước khi chạy chương trình nhấn phím F9 để kiểm tra lỗi.

+Nếu không báo lỗi nhấn tổ hợp phím Ctrl + F9 để chạy chương trình, xuất hiện giao diện như sau:



+ Nhấn phím 1 để vào chương trình, phím 2 để thoát khỏi chương trình

+ Kết quả thử nghiệm chương trình



KẾT LUẬN

Công nghệ thông tin và truyền thông đóng vai trò ngày càng quan trọng trong cuộc sống hàng ngày của con người, làm biến đổi sâu sắc cách thức làm việc, giải trí, các nguyên tắc tiến hành kinh doanh…

Cuộc cách mạng của CNTT trong những năm qua đã khởi xướng cho một trào lưu trong lĩnh vực quản lý–điều hành đất nước gọi là ‘‘ Chính phủ điện tử’’.

‘‘Chính phủ điện tử’’ hướng tới việc cung cấp hàng hóa và dịch vụ công cho người dân sẽ trở nên tốt hơn không chỉ thông qua việc cải tiến các thủ tục và cách thức quản lý của Chính phủ, tăng cường tính hiệu quả của Chính phủ đối với xã hội và cộng đồng.

Cũng chính vì vậy vấn đề đảm bảo an toàn thông tin trong ‘‘Chính phủ điện tử’’ là rất cần thiết .

Khóa luận gồm hai phần chính :

1/. Tìm hiểu và nghiên cứu qua tài liệu để hệ thống lại các vấn đề sau

- Tổng quan về ‘‘ Chính phủ điện tử’’.
- Tổng quan về An toàn thông tin.
- Một số bài toán trong giao dịch trực tuyến.

2./ Thử nghiệm xây dựng chương trình chữ ký số

-Xây dựng chương trình chữ kí Elgamal

TÀI LIỆU THAM KHẢO

Tiếng Việt:

[1] Phan Đình Diệu : *Lý thuyết mật mã và An toàn thông tin*, 2004

[2] Trịnh Nhật Tiến: *Bài giảng môn An toàn dữ liệu* , 2005

[3] TS. Trần Minh Tiến, TS. Nguyễn Thành Phúc, " *Chính phủ điện tử* " , Nhà xuất bản bưu điện năm 2004.

[4] http://www.pcworld.com.vn , "*Quản lý - Nhà nước*" , Tạp chí Thế giới Vi tính.

Tiếng Anh:

[5] D.Stinson. Cryptography: *Theory and Practicce, CRT Press* 1995

[6] Danley Harrisson. "*An Introduction to Steganography*" , 2000

[7] N.F.Johnson (2002), *" Steganography* ", George Mason University

[8] Onur Mutlu (December 2001) "*An Overview ofImage Watermarking Algorithms*", Project Report EE 731R Digital Image Processing, pp 1.

[9] S.Castano, M.Fugini, G.martella, P.Samarati : *Database Security*, 1994

[10] W.Bender, D.Gruhl, N.Morimoto, A.Lu (2000), " *Tecniques for Data Hiding* " *IBM Systems Journal*, Vol. 35 Nos 3 1996, pp 20-30.

[11] Jalal Feghhi, jalil Feghhi, Peter Williams. Digital Certificates: *Applied Internet Security*, 1999

[12] Các tài nguyên khác trên Internet