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

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

TÌM HIỂU, NGHIÊN CỨU MỘT SỐ TÌNH HUỐNG TRONG THỎA THUẬN HỢP ĐỒNG ĐIỆN TỬ

ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC HỆ CHÍNH QUY
NGÀNH CÔNG NGHỆ THÔNG TIN

Giáo viên hướng dẫn: PGS. TS Trịnh Nhật Tiến

Sinh viên: Phạm Thành Luân

Mã số sinh viên: 1013101014

Hải Phòng, 7/2012

LỜI CẢM ƠN

Em xin bày tỏ lòng biết ơn sâu sắc nhất tới PGS.TS Trịnh Nhật Tiến, thầy đã tận tình hướng dẫn và giúp đỡ em rất nhiều trong quá trình tìm hiểu và cài đặt chương trình để em hoàn thành tốt đồ án tốt nghiệp của mình.

Em xin chân thành cảm ơn sự dạy bảo của các thầy giáo, cô giáo Khoa Công Nghệ Thông Tin – Trường Đại Học Dân Lập Hải Phòng đã trang bị cho em những kiến thức cơ bản để em có thể hoàn thành đồ án tốt nghiệp.

Cuối cùng, em xin được bày tỏ lòng biết ơn tới những người thân trong gia đình bạn bè và đồng nghiệp đã dành cho em sự quan tâm, động viên trong suốt quá trình học tập và làm đề tài tốt nghiệp

MỤC LỤC

CÁC TỪ VIẾT TẮT

CPĐT	Chính phủ điện tử
CNTT	Công nghệ thông tin
CNTT-TT	Công nghệ thông tin – Truyền thông
G2C	Chính phủ với Công dân
G2B	Chính phủ với Doanh nghiệp
G2E	Chính phủ với người lao động
G2G	Chính phủ với Chính phủ
TMĐT	Thương mại điện tử
CERT	Computer Emegency Response Team: Đội cấp cứu máy tính
ATTT	An toàn thông tin

LỜI MỞ ĐẦU

Trong hoạt động của xã hội loài người, thông tin là một vấn đề không thể thiếu trong cuộc sống. Ngày nay thông tin càng trở thành một tài nguyên vô giá. Xã hội phát triển ngày càng cao nhu cầu trao đổi thông tin giữa các thành phần trong xã hội ngày càng lớn. Mạng máy tính ra đời mang lại cho con người nhiều lời ích trong việc trao đổi thông tin và xử lý thông tin một cách chính xác và nhanh chóng.

Với sự phát triển mạnh mẽ của mạng máy tính đặc biệt là sự ra đời của mạng toàn cầu(internet). Nó giúp cho mọi người khắp nơi trên thế giới có thể liên lạc và trao đổi thông tin với nhau một cách chính xác, dễ dàng trong một thời gian ngắn nhất.

Việc sử dụng internet để trao đổi thông tin, dữ liệu ngày càng nhiều, tạo điều kiện để các doanh nhân, cơ quan tổ chức, cá nhân trên khắp nơi biết đến nhau. Dẫn đến nhu cầu liên kết giữa các bên thông qua mạng internet ngày càng nhiều. Vấn đề đặt ra là trong môi trường mạng một lượng tin hay một khối dữ liệu khi được gửi đi từ người gửi đến người nhận thường phải qua nhiều nút, nhiều trạm vời nhiều sử dụng khác nhau, không ai đảm bảo rằng thông tin đến người nhận không bị sao chép, không bị đánh cắp hay không bị xuyên tạc . . . Chính vì lý do này mà vấn đề an toàn dữ liệu trên mạng nói riêng và an toàn dữ liệu nói chung là một vấn đề đang được quan tâm hàng đầu khi nghiên cứu truyền dữ liệu trên mạng. Việc để suất ra các phương pháp để giải quyết các vấn đề an toàn dữ liệu trên mạng là một điều cấp thiết.

Trong đồ án này, em nghiên cứu chủ yếu về một số tình huống xảy ra trong hợp đồng điện tử và hướng giải quyết đối với các tình huống đó. Đồ án bao gồm các phần sau:

Chương 1: Các khái niệm cơ bản.

Chương 2: Một số tình huống xảy ra trong thỏa thuận hợp đồng điện từ

và cách giải quyết

Chương 3: Thử nghiệm chương trình

Chương 1. CÁC KHÁI NIỆM CƠ BẢN

1.1. TỔNG QUAN VỀ CHÍNH PHỦ ĐIỆN TỬ

1.1.1. Khái niệm về 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 công nghệ thông tin và truyền thông. 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)

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, 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.

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, cách 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 24/7, 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 nhiều 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 vụ 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, trợ 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**

Hình 1. Các hình thức giao tiếp

1.2. TỔNG QUAN VỀ THƯƠNG MẠI ĐIỆN TỬ

1.2.1. Khái niệm thương mại điện tử

Có nhiều cách hiểu khác nhau về thương mại điện tử

- Theo luật mẫu về TMĐT của UNCITRAL: "TMĐT là tất cả các hoạt động thương mại thông thường được thực hiện thông qua các phương tiện điện tử và truyền thông đặc biệt là mạng Internet". Từ khái niệm trên ta thấy, TMĐT là sự đi lên một nấc cao mới của thương mại thông thường cùng với sự phát triển của thế giới số, chứ không phải là một lĩnh vực kinh doanh độc lập với thương mại thông thường

- Theo WTO TMĐT được hiểu như sau: "TMĐT bao gồm việc sản xuất, bán hàng, quảng cáo và phân phối sản phẩm được mua bán và thanh toán trên mạng Internet nhưng được giao nhận một cách hữu hình và tất cả các sản phẩm được giao nhận như những thông tin số hóa thông qua mạng Internet"

- Theo ỦY BAN CHÂU ÂU: "TMĐT được hiểu là việc thực hiện hoạt động kinh doanh qua các phương tiện điện tử. Nó dựa trên việc xử lý và truyền số liệu điện tử dưới dạng chữ, âm thanh và hình ảnh. TMĐT gồm nhiều hành vi trong đó có hoạt động mua bán hàng hóa qua phương tiện điện tử, giao nhận các nội dung kỹ thuật số trên mạng, chuyển tiền điện tử, mua bán cổ phiếu điện tử, vận đơn điện tử, đấu giá thương mại, hợp tác thiết kế, tài nguyên mạng, mua sắm công cộng, tiếp thị trực tiếp người tiêu dùng, và các dịch vụ sau bán hàng. TMĐT được thực hiện đối với cả thương mại hàng hóa (như hàng tiêu dùng, các thiết bị y tế chuyên dụng) và với cả thương mại dịch vụ (như dịch vụ cung cấp thông tin, dịch vụ tư vấn pháp lý, tài chính), các hoạt động truyền thông (như chăm sóc sức khỏe, giáo dục) và các hoạt động mới như siêu thị ảo"

Quan điểm về TMĐT theo cách hiểu của quốc tế được phân tích theo nghĩa rộng, phản ánh sự đi lên không ngừng của những ứng dụng CNTT và TMĐT trong mọi hoạt động của cuộc sống nói chung và hoạt động thương mại nói riêng.

Luật Giao dịch điện tử Việt Nam năm 2005 không đưa ra khái niệm thương mại điện tử. Luật chỉ quy định khái niệm về giao dịch điện tử, theo đó: "Giao dịch điện tử là giao dịch được thực hiện bằng phương tiện điện tử". Luật này cũng cụ thể hóa khái niệm phương tiện điện tử: "Phương tiện điện tử là phương tiện hoạt động dựa trên công nghệ điện, điện tử, kỹ thuật số, từ tính, truyền dẫn không dây, quang học, điện từ hoặc công nghệ tương tự". Qua khái niệm này, có thể thấy phạm vị điều chỉnh của Luật là rất rộng, bao trùm các giao dịch điện tử trong nhiều lĩnh vực, không chỉ rõ lĩnh vực kinh doanh, thương mại mà cả trong lĩnh vực dân sự, trong hoạt động quản lý của các cơ quan nhà nước. Được xây dựng dựa trên luật mẫu của UNCITRAL về TMĐT, Luật Giao dịch điện tử Việt Nam năm 2005 có cách tiếp cận tương tự với Luật mẫu, đó là cách tiếp cận theo nghĩa rộng. Đây là cách tiếp cận phù hợp. Việc coi TMĐT là hoạt động sử dụng các phương tiện điện tử theo nghĩa rộng và có tính mở sẽ ra trong tương lai, khả năng áp dụng TMĐT còn lớn hơn do nhiều phương tiện hiện đại mới sẽ ra đời. Hơn nữa, đối với các quốc gia đang phát triển trong đó có Việt Nam thì việc hiểu TMĐT theo nghĩa rộng sẽ khiến cả doanh nghiệp và người tiêu dùng giảm bớt lúng túng, bỡ ngỡ ban đầu. Khi chúng ta coi fax, telex, điện thoại xưa nay chúng ta vẫn quen sử dụng là những phương tiện thực hiện TMĐT thì việc áp dụng hình thức kinh doanh mới qua mạng Internet cũng chỉ là sự phát triển lên cao tất yếu trong cuộc cách mạng văn hóa thông tin.

1.2.2. Đặc điểm của thương mại điện tử

- TMĐT không thể hiện giao dịch trên giấy. Tất cả các văn bản đều thể hiện bằng các dữ liệu tin học, các băng ghi âm hoặc các phương tiện điện tử khác. Chính đặc điểm này làm thay đổi cơ bản văn hóa giao dịch bởi lẽ độ tin cậy không còn phụ thuộc vào các cam kết bằng giấy mà bằng niềm tin lẫn nhau giữa các đối tác. Giao dịch không dùng giấy tờ cũng làm giảm đáng kể chi phí và nhân lực để chu chuyển, lưu trữ và tìm kiếm văn bản khi cần thiết. Tuy nhiên, điều này cũng ẩn chứa rủi ro do không lưu trữ hợp đồng mà khi xảy ra các tranh chấp kiện tụng sẽ không có bằng chứng để tranh tụng.

- TMĐT phụ thuộc vào CNTT và trình độ của người sử dụng. Chính đặc điểm này tạo lên cách nhìn nhận về TMĐT của các quốc gia với các mức trình độ khoa học công nghệ khác nhau thì khác nhau. Nguồn nhân lực trong lĩnh vực TMĐT luôn phải được đào tạo để bắt kịp với thời đại của khoa học.

- TMĐT phụ thuộc vào mức độ số hóa

- TMĐT có tốc độ nhanh nhờ áp dụng kỹ thuật số nên tất cả các bước của quá trình giao dịch đều được tiến hành thông qua mạng máy tính

1.2.3. Ba hoạt động của thương mại điện tử

1.2.3.1. Giai đoạn Quảng cáo, Giới thiệu sản phẩm

Bước đầu tiên để tham gia Thương Mại Điện Tử là phải xây dựng một website cho riêng mình. Tùy theo đặc tính riêng của mỗi công việc, website này có thể từ rất đơn giản như là một vài trang web tĩnh (tức thông tin trên trang web này không thường xuyên thay đổi) đến phức tạp gồm các cơ sở dữ liệu và các trang web động (tức thông tin trên trang web này thường xuyên thay đổi) cho phép tương tác với người sử dụng. Nếu người chủ website chỉ muốn quảng cáo thông tin trên web của họ, người đó có thể xây dựng vài trang, bao gồm: trang chủ, trang giới thiệu về doanh nghiệp, trang giới thiệu về sản phẩm hay dịch vụ, và nên có ít nhất một địa chỉ email để người quan tâm có thể liên hệ người đó dễ dàng. Các trang web của người chủ website nên được viết bằng ngôn ngữ chung của đối tượng khách hàng, hiện giờ thông dụng nhất là tiếng Anh. Nếu đối tượng khách hàng là người Nhật, nên có một phiên bản tiếng Nhật song song với bản tiếng Anh hay tiếng Việt

Quảng bá website trên mạng:

Có được website cho doanh nghiệp rồi, bây giờ là lúc người chủ website phải quan tâm đến việc làm sao mọi người biết được địa chỉ website của mình? Chỉ xin nhấn mạnh rằng: hiện giờ khâu marketing (quảng bá hay tiếp thị) website của các doanh nghiệp ở Việt Nam còn chưa được chú trọng. Có rất nhiều website rất đẹp, xây dựng rất công phu, để rồi sau khi được online (trực tuyến), trong nhiều tháng nhiều năm liền chỉ có vài trăm hay vài nghìn người vào xem. Như vậy, hoàn toàn lãng phí chi phí và công sức xây dựng website.

Thực hiện marketing cho website đòi hỏi công sức, sự kiên trì và kiến thức. Người chủ cần phải dành khá nhiều thời gian trong ngày, trong tuần để lên mạng marketing cho website của mình. Nhưng không có nghĩa là người chủ website có thời gian lên mạng marketing cho website của mình thì bạn sẽ thực hiện marketing có hiệu quả.

Do đó, cách tốt nhất dành cho doanh nghiệp vừa và nhỏ là hãy khoán công việc này cho một dịch vụ xúc tiến Thương Mại Điện Tử bởi vì họ marketing chuyên nghiệp hơn và chi phí người chủ website bỏ ra sẽ ít hơn so với tự mình marketing. Tùy theo mức độ của dịch vụ, người chủ website có thể phải trả từ vài chục đến vài trăm đô-la Mỹ mỗi tháng để thuê dịch vụ marketing website cho riêng mình.

1.2.3.2. Giai đoạn Thoả thuận và Ký kết hợp đồng

Sau giai đoạn tìm hiểu, nghiên cứu các mặt hàng sản phẩm sẽ đến giai đoạn thỏa thuận và ký kết hợp đồng. Giai đoạn này là giai đoạn quan trong nhất trong ba giai đoạn, nó quyết định đến thành công của việc ký kết hợp đồng hay không.

Ở giai đoạn này, có một số tình huống hay xảy ra đối với một hợp đồng điện tử:

- Xem trộm nội dung hợp đồng.

- Sửa đổi trái phép nội dung hợp đồng.

- Phủ nhận chữ ký trên hợp đồng.

1.2.3.3. Giai đoạn Thực hiện hợp đồng

Các bên tham gia phải có trách nhiệm thực hiện hợp đồng đã ký kết. Việc chối bỏ hợp đồng là điều có thể xảy ra đối với một hợp đồng điện tử. Chính vì vậy, người đứng giữa (CA) các bên tham gia hợp đồng bây giờ có trách nhiệm như là người trọng tài bắt các bên tham gia phải thực hiện đúng những gì mà mình đã ký.

1.3. TỔNG QUAN VỀ AN TOÀN THÔNG TIN

1.3.1. Tại sao cần bảo đảm an toàn thông tin

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

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

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

Khi trao đổi thông tin trên mạng, những tình huống mới nảy sinh:

- Người ta nhận được một bản tin trên mạng, thì lấy gì làm đảm bảo rằng nó là của đối tác gửi cho họ. Khi nhận được tờ Sec điện tử hay tiền điện tử trên mạng, thì có cách nào xác nhận rằng nó là của đối tác đã thanh toán cho ta. Tiền đó là tiền thật hay tiền giả.

Thông thường người gửi 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 ký như cũ, chữ kỹ rất dễ bị giả mạo.

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

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

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

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

1.3.2. Khái niệm an toàn thông tin

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

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

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

1.3.3. Đặc điểm an toàn thông tin

1.3.3.1. 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 bổ sung, loại bỏ và sửa dữ liệu không được phép

- Bảo đảm xác thực (Chứng thực): Xác định đúng thực thể cần kết nối, giao dịch. Xác thực đúng thực thể có trách nhiệm về nội dung thông tin (xác định nguồn gốc thông tin).

- Bảo đảm sẵn sàng: Thông tin sẵn sàng cho người dùng hợp pháp

- Bảo đảm tính không thể chối bỏ: Thông tin và tài nguyên được xác nhận về mặt pháp luật của người cung cấp

1.3.3.2. Các nội dung an toàn thông tin

- Nội dung chính:

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

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

- Nội dung chuyên nghành

+ An toàn dữ liệu(data security)

+ An toàn cơ sở dữ liệu(database security)

+ An toàn hệ điều hành(operation system security)

+ An toàn mạng máy tính(network security)

1.3.3.3. Các chiến lược bảo đảm an toàn thông tin

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

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

1.3.4. Các phương pháp bảo vệ thông tin

1.3.4.1. Các giải pháp bảo đảm an toàn thông tin

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

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

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

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

Kỹ thuật: - Mã hóa, hàm băm, giấu tin, ký số. . .

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

2/. Phương pháp kiểm soát lỗi vào ra của thông tin

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

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

+ kiểm soát, tìm diệt "sâu bọ" vào trong hệ thống máy tính

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

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

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

+ Các "lỗ hổng" trong các giao thức.

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

+ Các "lỗ hổng" trong các ứng dụng.

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

+ Hạ tầng mật mã khóa công khai (PKI)

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

+ Kiểm soát và xử lý các lỗ hổng.

1.3.4.2. Các kỹ thuật bảo đảm an toàn thông tin

- Kỹ thuật diệt trừ: Virus máy tính, chương trình trái phép.

- Kỹ thuật tường lửa: Ngăn chặn truy cập trái phép, lọc thông tin không hợp pháp.

- Kỹ thuật mạng riêng ảo: Tạo ra hành lang riêng cho thông tin "đi lại".

- Kỹ thuật mật mã: Mã hóa, kỹ số, các giao thức mật mã, chống chối cãi.

- Kỹ thuật giấu tin: Che giấu thông tin trong môi trường dữ liệu khác.

- Kỹ thuật thủy ký: Bảo vệ bản quyền tài liệu số hóa.

- Kỹ thuật truy tìm "dấu vết" kẻ trộm tin.

1.3.4.3. Các công nghệ đảm bảo an toàn thông tin

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

1.4. TỔNG QUAN VỀ PHƯƠNG PHÁP MÃ HOÁ

1.4.1. Khái niệm mã hoá dữ liệu

Mã hóa là khái niệm đã được dùng lâu đời để đảm bảo an toàn thông tin. Hiện nay có nhiều phương pháp mã hóa khác nhau, mỗi phương pháp có ưu điểm và nhược điểm riêng. Tùy theo yêu cầu cụ thể để chọn phương pháp mã hóa. Sau đây là một số khái niệm dùng trong mật mã

Mã hóa: Là quá trình chuyển đổi thông tin từ dạng đọc được gọi là **bản rõ,** thành thông tin không thể đọc được (đối với những người không có quyền) theo cách thông thường được gọi là **bản mã**

Giải mã: là quá trình chuyển đổi thông tin ngược lại từ **bản mã** sang **bản rõ.**

Thuật toán mã hóa: là các thuật toán, các công thức tính toán để **mã hóa** và **giải mã** thông tin. Thuật toán càng phức tạp thì độ an toàn của bản mã càng cao.

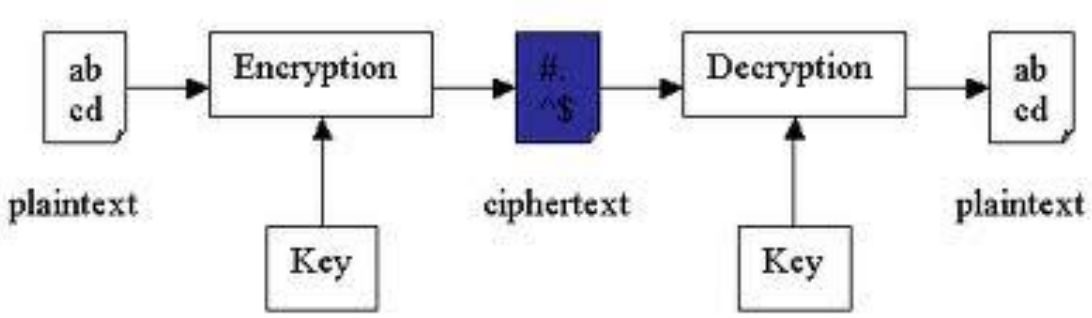
Khóa mã hóa: là các giá trị làm cho các thuật toán mã hóa chạy theo cách riêng để **mã hóa** và **giải mã**, khóa mật mã bao gồm có khóa lập mã và khóa giải mã. Phạm vi các giá trị có thể của khóa được gọi là không gian khóa. Không gian khóa càng cao thì độ an toàn của bản mã càng cao.

Hệ mã hóa: là tập hợp các thuật toán, các khóa nhằm mã hóa,

giải mã thông tin.

Mật mã học: là ngành nghiên cứu mật mã: tạo mã và phân tích mã.

Phân tích mã: là các kỹ thuật phân tích mã, kiểm tra tính toàn vẹn hoặc phá vỡ sự bí mật của bản mã. Phân tích mã còn gọi là **thám mã.**



Hình 2. Sơ đồ mã hóa

Có hai phương pháp mã hóa cơ bản là mã hóa công khai (mã hóa phi đối xứng) và mã hóa bí mật (mã hóa đối xứng).

1.4.2. Một số phương pháp mã hoá dữ liệu

1.4.2.1. Hệ mã hóa bí mật

Trong mã hóa bí mật, quá trình mã hóa và quá trình giải mã sử dụng cùng một thuật toán và khóa

Độ an toàn của mã khóa bí mật phụ thuộc vào một vài yếu tố như thuật toán mã hóa phải đủ mạnh (sao cho việc mã hóa thông báo chỉ dựa vào bản mã là không khả thi), sự bí mật của khóa (không phải là sự bí mật của thuật toán).

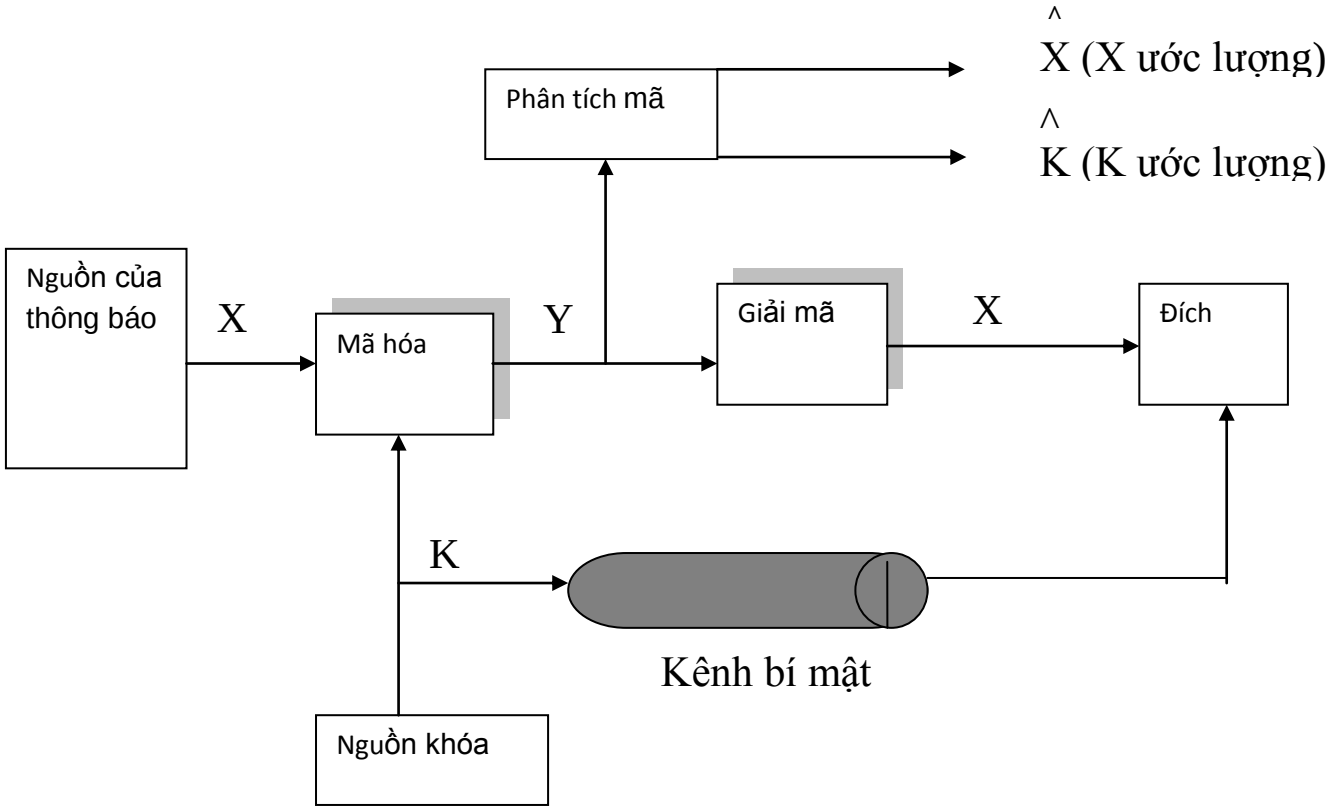
Nguồn A tạo ra một thông báo ở dạng rõ, X = {x1, x2, ..., xm}. Khóa được dùng khi mã hóa có dạng K = {k1, k2, ... , kl}. Nếu khóa do nguồn sinh ra, khóa phải được chuyển cho đích theo một kênh an toàn nào đó. Có thể dùng một thành viên thứ ba để sinh khóa và phân phối khóa an toàn cho cả nguồn và đích.

Với nguồn đầu vào là thông báo X và khóa mã K, đầu ra là của thuật toán mã hóa là một bản mã Y = {y1, y2, ..., yn}. Chúng ta có thể viết như sau:

$$Y = E_K(X).$$

Khi nhận được bản mã, người nhận có thể giải mã bằng cách dùng cùng một khóa và thuật toán (dùng khi giải mã như sau):

$$X = D_K(Y).$$



Hình 3. Mô hình mã hóa đối xứng

Việc mã hóa và giải mã thông báo nhanh và hiệu quả. Tuy nhiên, khóa phải được giữ cẩn thận. Nếu bị lộ khóa, tất cả các thông báo trước đó đều bị lộ và cả người gửi và người nhận phải dùng khóa mới cho các cuộc truyền thông tiếp theo.

Quá trình phân phối khóa mới cho các thành viên rất khó khăn. Một vấn đề nảy sinh đối với mã hóa khóa đối xứng là chúng không thích hợp với môi trường lớn, chẳng hạn trên internet. Do đó mỗi cặp thành viên truyền thông trên internet phải có khóa bí mật khi họ muốn trao đổi thông tin với nhau một cách an toàn, dẫn đến số lượng khóa sẽ rất lớn giống như hệ thống đường dây điện thoại riêng không có các chạm truyền mạch, chẳng hạn với 12 người muốn truyền thông, chúng ta cần có 66 khóa bí mật.

1.4.2.2. Hệ mã hóa khóa công khai

Mã hóa khóa công khai có ưu điểm là số lượng khóa không lớn, nếu có N người muốn trao đổi thông tin với người khác an toàn thì chỉ cần duy nhất N cặp khóa, ít hơn rất nhiều so với mã hóa đối xứng. Ưu điểm thứ hai là việc phân phối khóa không phải là một vấn đề khó. Khóa công khai của mỗi người có thể được gửi đi theo kênh an toàn nếu cần thiết và không yêu cầu bất kỳ sự kiểm soát đặc biệt nào khi phân phối. Mã hóa công khai có khả năng thực thi chữ ký số, có nghĩa là một tài liệu có thể được ký và gửi cho người nhận bất kỳ cùng với chống chối bỏ. Thực tế khó có một người nào đó khác ngoài người ký - sinh ra chữ ký điện tử, thêm vào đó, người ký không thể chối bỏ việc ký vào tài liệu sau khi ký.

Mã hóa công khai có một số khó khăn đó là: Quá trình mã hóa và giải mã chậm so với mã hóa đối xứng. Khoảng thời gian này tăng lên một cách nhanh chóng nếu bạn và khách hàng của bạn tiến hành thương mại trên internet. Người ta không có ý định thay thế mã hóa khóa đối xứng bằng mã hóa công khai. Chúng bổ sung lẫn nhau.

Các thuật toán khóa công khai dùng một thuật toán để mã hóa và khóa khác để giải mã. Chúng có tính chất quan trọng là không thể xác địch được khóa giải mã nếu chỉ căn cứ vào thuật toán và khóa mã hóa.

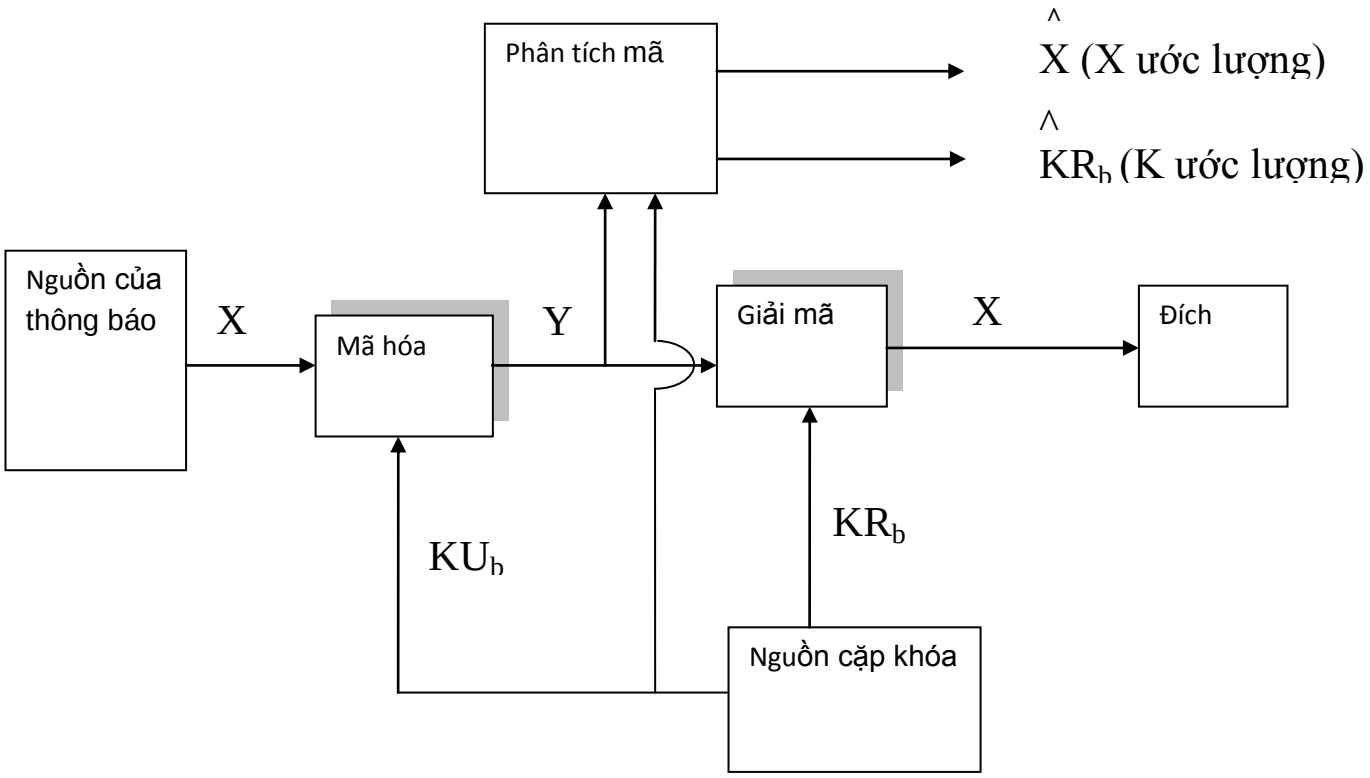
Quá trình mã hóa khóa công khai gồm các bước cơ bản sau:

- Mỗi thành viên sinh ra một cặp khóa, cặp khóa này dùng để mã hóa và giải mã.

- Mỗi thành viên công bố khóa mã hóa của mình bằng cách đặt khóa này vào một địa chỉ được công bố công khai. Đây chính là khóa công khai. Khóa cùng cặp được giữ bí mật, đó là khóa riêng.

- Nếu A muốn gửi cho B một thông báo, A mã hóa thông báo này với khóa công khai của B.

- Nếu B nhận được thông báo, B giải mã thông báo bằng khóa riêng của B. Không một người nhận nào khác có thể giải mã thông báo, bởi chỉ có B mới biết khóa riêng của mình.



Hình 4. Lược đồ mã hóa khóa công khai: Bí mật

Với cách giải quyết này, tất cả các thành viên tham gia truyền thông đều có thể có được khóa công khai. Khóa riêng của mỗi thành viên được giữ bí mật. Mỗi thành viên có thể thay đổi các khóa riêng của mình bắt cứ lúc nào, đồng thời công bố khóa công khai cùng cặp để thay thế cặp khóa cũ.

Ta sẽ xem xét các yếu tố cần thiết trong lược đồ mã hóa khóa công khai(hình trên).

Nguồn A đưa ra một thông báo rõ và bản rõ của thông báo là

$$X = [x1, x2, ... , xm]$$

A dự định gửi thông báo cho đích B, B sinh ra một cặp khóa công khai KU_b

và khóa riêng KR_b. Chỉ có B mới biết KR_b, còn KU_b được công bố công khai, do đó A có thế có được khóa công khai này.

Với đầu vào là thông báo X và khóa mã hóa Kub, A tạo ra một bản mã

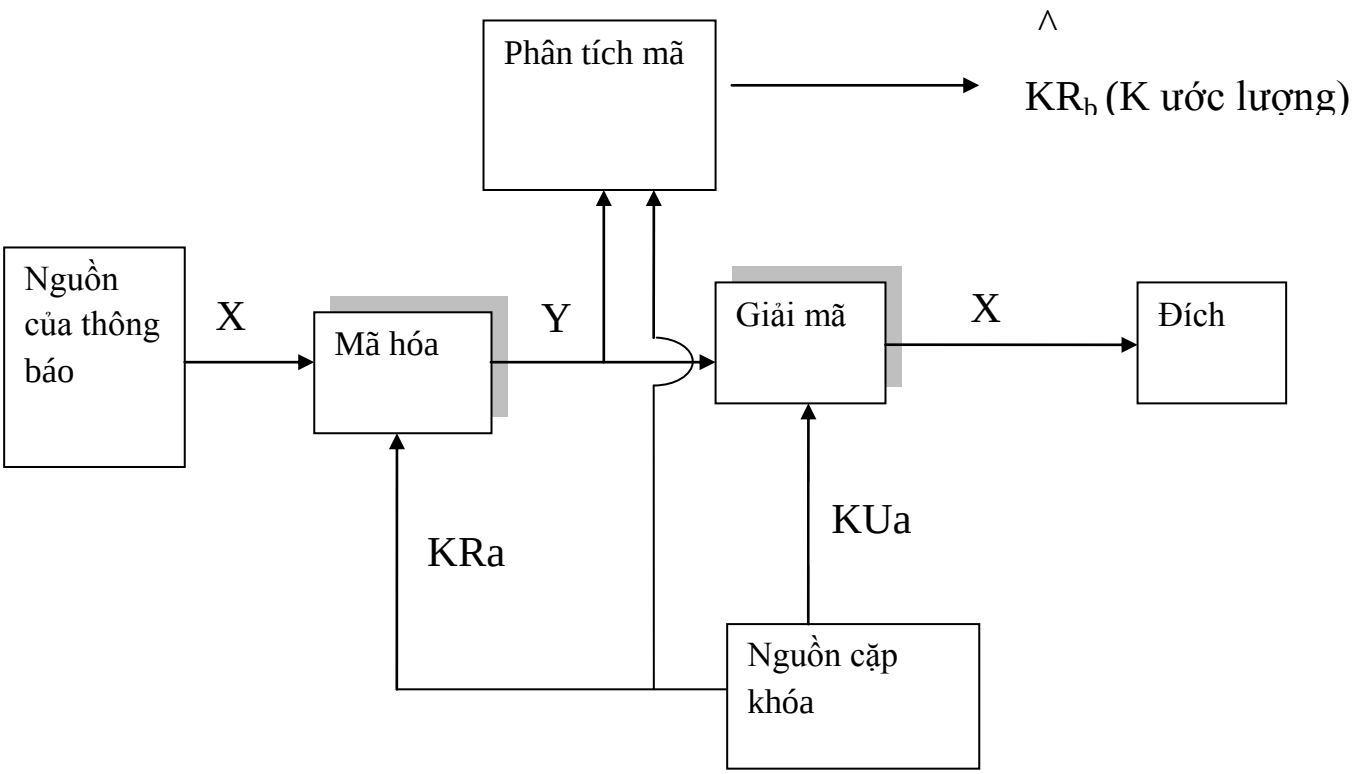
$$Y = [y1, y2, ... , yn]. \text{ Với } Y = EK_{Ub}(X).$$

Người nhận hợp lệ (người có khóa riêng) thu được X qua phép biến đổi ngược

$$X = D_{KRb}(Y).$$

Chúng ta đã biết, một trong hai khóa trong cặp khóa có thê được dùng để mã hóa, khóa còn lại được dùng để giải mã. Điều này cho phép thực hiện một lược đồ hơi khác một chút. Lược đồ được minh họa trong hình trên cung cấp tính bí mật. Hình dưới minh họa việc mã hóa khóa công khai cho xác thực:

$$Y = E_{KUa(}X) \text{ và } X = D_{KRa}(Y)$$



Hình 5. Lược đồ mã hóa khóa công khai: Xác thực

Trong trường hợp này, A chuẩn bị một thông báo gửi cho B và thông báo với khóa riêng của A trước khi truyền đi, B có thể giải mã bằng khóa công khai của A. Thông báo được mã hóa bằng khóa riêng của A nên chỉ có A mới là người tạo ra thông báo. Do vậy, toàn bộ thông báo mã hóa được dùng như là một chữ ký số. Hơn nữa, không thể sửa đổi thông báo nếu không có khóa riêng của A, chính vì vậy thông báo được xác thực cả nguồn gốc lẫn tính toàn vẹn dữ liệu.

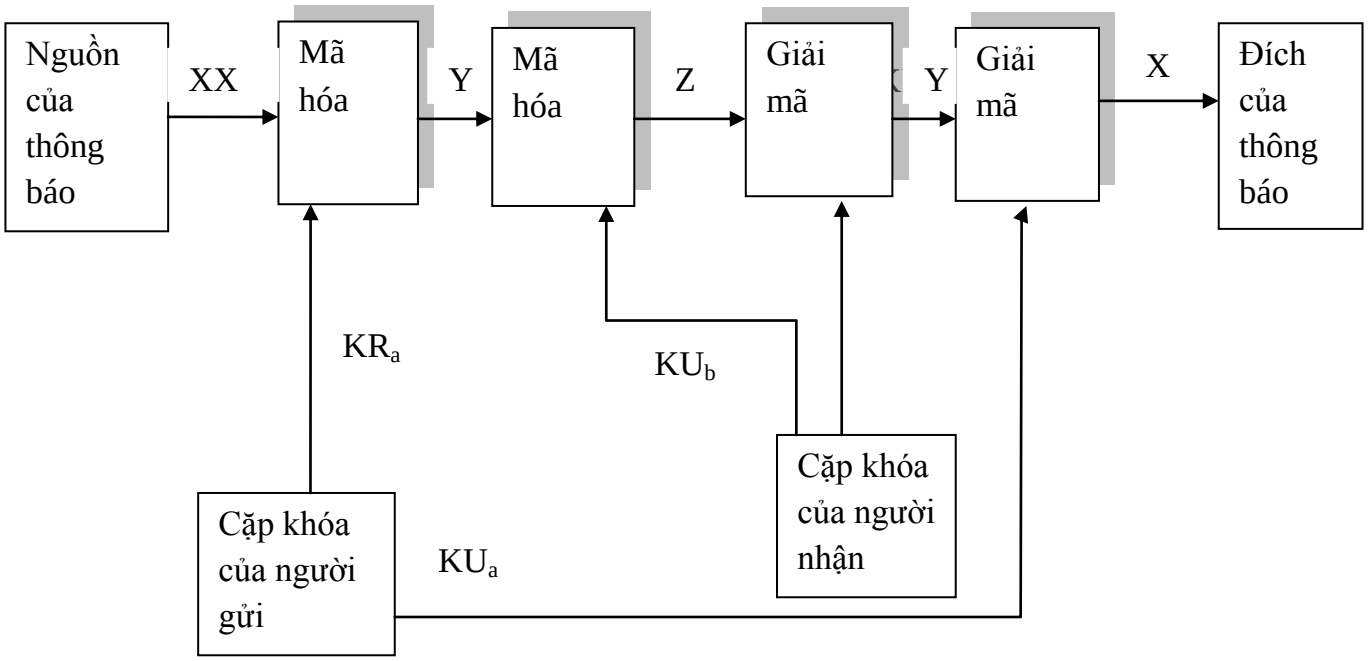
Trong lược đồ trước, toàn bộ thông báo được mã hóa, nó đòi hỏi khả năng lưu trữ lớn. Mỗi tài liệu phải được lưu trữ ở dạng bản rõ. Bản sao được lưu trữ dưới dạng bản mã, do vậy chúng ta có thể kiểm tra được nguồn gốc và các nội dung trong trường hợp xảy ra tranh chấp. Một cách hiệu quả hơn để có được kết quả như trên là mã hóa một khối nhỏ các bit. Khối này được gọi là dấu xác thực. Nó phải có tích chất là mọi thay đổi trên tài liệu đều dẫn tới sự thay đổi của dấu xác thực. Nếu dấu xác thực được mã hóa bằng khóa riêng của người gửi, nó được dùng như một chữ ký. Chữ ký được dùng để kiểm tra nguồn gốc và nội dung thông báo.

Việc dùng lược đồ mã hóa khóa công khai có thể đảm bảo cho tính xác thực và tính bí mật được trình bày trong hình dưới.

$$Z = E_{KUb}[E_{kra}(X)].$$

$$X = D_{KUa}[D_{kra}(Z)].$$

Trước hết, chúng ta mã hóa bằng khóa riêng của người gửi, đưa ra một chữ ký số. Tiếp theo, mã hóa một lần nữa bằng khóa công khai của người nhận. Chỉ có người nhận hợp pháp mới giải được bản mã cuối cùng này vì anh ta có khóa riêng cùng cặp. Như vậy sẽ đảm bảo tính bí mật. Khó khăn của biện pháp này là thuật toán khóa công khai, nó thực sự phức tạp, phải tiến hành bốn lần (chứ không phải hai lần) cho mỗi cuộc truyền thông.



Hình 6. Lược đồ mã hóa khóa công khai: Bí mật và xác thực

Như đã trình bày ở trên, một đặc điểm của mã hóa khóa công khai là khóa công khai được công bố công khai và khóa riêng cùng cặp được chủ sở hữu giữ bí mật. Do vậy, vấn đề đặt ra là khóa công khai được phân bố như thế nào? Tuy nói rằng nó được công bố công khai, bất kỳ người dùng nào cũng có thể lấy được khóa công khai khi muốn dùng nó, nhưng phải dùng một cơ chế nào đó để xác thực rằng, khóa công khai đó là chính người gửi thông báo hoặc người nhận thông báo chủ định và khóa công khai này cùng cặp với khóa riêng của họ.

Vấn đề phân phối khóa công khai được giải quyết qua nhiều kỹ thuật phân phối khóa công khai như khai báo công khai, thư mục công khai, trung tâm quản lý khóa công khai và chứng chỉ khóa công khai.

Hiện nay người ta chủ yếu dùng hệ thống chứng chỉ khóa công khai để phân phối khóa công khai. Mỗi chứng chỉ có chứa một khóa công khai và các thông tin khác. Nó được cơ quan quản lý chứng chỉ tạo ra và phát hành cho các thành viên. Mỗi thành viên chuyển thông tin khóa công khai của mình cho các thành viên khác thông qua chứng chỉ. Các thành viên khác có thể kiểm tra chứng chỉ do cơ quan quản lý tạo ra.

1.4.3. Một số hệ mã hóa

1.4.3.1. Hệ mã hóa đối xứng DES

1/. Giới thiệu

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

+ Hệ mã hóa phải có độ an toàn cao.

+ Hệ mã hóa phải được định nghĩa đầy đủ và dễ hiểu.

+ Độ an toàn của hệ mã hóa phải nằm ở khóa, không nằm ở thuật toán.

+ Hệ mã hóa phải sẵn sàng cho mọi người dùng ở các lĩnh vực khác nhau.

+ Hệ mã hóa phải xuất khẩu được.

- DES được IBM phát triển, là một cải biên của hệ mật LUCIPHER DES, nó được công bố lần đầu tiên vào ngày 17/03/1975. Sau nhiều cuộc tranh luận công khai, cuối cùng DES được công nhận như một chuẩn liên bang vào ngày 23/11/1976 và được công bố vào ngày15/01/1977.

- Năm 1980, "cách dùng DES" được công bố. Từ đó chu kỳ 5 năm DES được xem xét lại một lần bởi Ủy ban tiêu chuẩn quốc gia Mỹ.

2/. Quy trình mã hóa theo DES

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

Chia thành

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

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

Kết nối

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

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

3/. Lập mã và giải mã

a/. Lập mã: - Bản rõ là xâu x, bản mã là xâu y, khóa là xâu K, đều có độ dài 64 bit

- Thuật toán mã hóa DES thực hiện qua 3 bước chính như sau:

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

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

(IP(x) tách thành $L_0 R_0$).

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

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

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

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

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

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

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

b/. Quy trình giải mã

- Quy trình giải mã của DES tương tự như quy trình lập mã, nhưng theo dùng các khóa thứ tự ngược lại: $k_{16,}$ k_{15}, …, k_1.

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

4/. Độ an toàn của hệ mã hóa DES

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

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

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

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

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

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

1.4.3.2. Hệ mã hóa khóa công khai RSA

Sơ đồ

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

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

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

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

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

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

- Hàm mã hóa: $y = e_k(x) = x^b \bmod n$

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

Độ an toàn

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

- Hệ mật RSA an toàn, khi giữ được bí mật khóa giải mã a, p, q, $\phi(n)$. Nếu biết được p và q, thì thám mã dễ dàng tính được $\phi(n) = (q-1) * (p-1)$. Nếu biết được $\phi(n)$, thì thám mã sẽ tính được a theo thuật toán Euclide mở rộng. Nhưng phân tích n thành tích của p và q là bài toán "khó".

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

Ví dụ:

Giả sử A chọn p = 101 và q = 113. Khi đó n = p.q = 11431 và $\phi(n) = 100.112 = 11200$. Vì $11200 = 2^6 5^2 7$, nên ta có thể dùng một số nguyên b như một số mũ mã hóa khi và chỉ khi b không chia hết cho 2, 5, 7. Vì thế trong thực tế A sẽ không phân tích $\phi(n)$, A kiểm tra điều kiện UCLN($\phi(n)$, b) = 1 bằng thuật toán Euclide. Giả sử A chọn
b = 3533, khi đó theo thuật toán Euclide mở rộng

$$b^{-1} = 6597 \bmod 11200$$

Vì vậy, số mũ mật để giải mã là a = 6597.

A sẽ công bố n = 11413 và b = 3533 trong một danh bạ. Bây giờ, Giả sử B muốn gửi bản rõ 9726 cho A. B sẽ tính:

$$9726^{3533} \bmod 11413 = 5761$$

Và gửi bản mã 5761 trên kênh truyền. Khi A nhận được bản mã 5761 A sẽ dùng số mũ bí mật a để tính

$$5761^{6597} \bmod 11413 = 9726.$$

1.5. TỔNG QUAN VỀ PHƯƠNG PHÁP KÝ ĐIỆN TỬ

1.5.1. Chữ ký số

1.5.1.1. Khái niệm chữ ký số

Digital signature – Chữ ký điện tử là thông tin đi kèm dữ liệu (văn bản, hình ảnh, video . . .) nhằm xác định người chủ của dữ liệu đó. Chữ ký số là nền tảng bảo đảm an ninh cho nền kinh tế tri thức, đồng thời là cơ sở pháp lý để giải quyết tranh chấp trong thương mại điện tử.

Lược đồ chữ ký số là phương pháp ký một thông điệp lưu dưới dạng điện tử. Và thông điệp được ký này có thể được truyền trên mạng.

Với chữ ký truyền thống, khi ký lên một tài liệu thì chữ ký là bộ phận vật lý của tài liệu được ký. Tuy nhiên, chữ ký số không được gắn một cách vật lý với thông điệp được ký.

Để kiểm tra chữ ký đối với chữ ký truyền thống việc kiểm tra bằng cách so sánh nó với những chữ ký gốc đã đăng ký. Tất nhiên, phương pháp này không được an toàn lắm vì nó tương đối dễ dàng đánh lừa bởi chữ ký của người khác. Trong khi chữ ký số thì được kiểm tra bằng cách dùng thuật toán kiểm tra đã biết công khai. Như vậy "người bất kỳ" 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).

Chữ ký điện tử phải đáp ứng được yêu cầu:

- **Chứng thực:** Chữ ký thuyết phục được người nhận rằng văn bản chứa nó là do người ký gửi đến.

- **Chống giả mạo:** Chữ ký là bằng chứng cho việc người ký đã ký lên, bởi không ai có thể giả mạo chữ ký của người ký.

- **Chống tái sử dụng:** Chữ không chỉ đặc trưng cho người ký mà còn cả văn bản chứa nó, người ta không thể di chuyển chữ ký vào một tài liệu khác với vai trò như chữ ký hợp pháp của văn bản ấy.

- **Chống thay đổi văn bản:** Sau khi văn bản được ký, nó không thể bị sửa đổi vì mọi sự sửa đổi đều dẫn đến chữ ký không hợp lệ.

- **Chống phủ nhận:** Người ký không thể phủ nhận chữ ký của mình trên văn bản.

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

- P là tập hữu hạn các văn bản có thể.

- A là tập hữu hạn các chữ ký có thể.

- K là tập hữu hạn các khóa có thể.

- S là tập các thuật toán ký.

- V là tập các thuật toán kiểm thử.

- Với mỗi khóa $k \in K$, có thuật toán ký $Sig_k \in S$, $Sig_k: P \rightarrow A$, có thuật toán kiểm tra chữ ký $Ver_k \in V$, $Ver_k: P \times A \rightarrow$ {đúng, sai}, thỏa mãn điều kiện sau $\forall x \in P$, $y \in A$:

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

1.5.1.2. Các ưu điểm của chữ ký số

1/. Khả năng xác định nguồn gốc

Các hệ thống mật mã hóa khóa công khai cho phép mật mã hóa văn bản với khóa bí mật mà chỉ có người chủ của khóa biết. Để sử dụng chữ ký số thì văn bản cần phải được mã hóa bằng hàm băm (văn bản được "băm" ra thành chuỗi, thường có độ dài cố định và ngắn hơn văn bản) sau đó dùng khóa bí mật của người chủ khóa để mã hóa, khi đó ta được chữ ký số. Khi cần kiểm tra, bên nhận giải mã (với khóa công khai) để lấy lại chuỗi gốc (được sinh ra qua hàm băm ban đầu) và kiểm tra với hàm băm của văn bản nhận được. Nếu 2 giá trị (chuỗi) này khớp nhau thì bên nhận có thể tin tưởng rằng văn bản xuất phát từ người sở hữu khóa bí mật. Tất nhiên là chúng ta không thể đảm bảo 100% là văn bản không bị giả mạo vì hệ thống vẫn có thể bị phá vỡ.

Vấn đề nhận thức đặc biệt quan trọng đối với các giao dịch tài chính. Chẳng hạn một chi nhánh ngân hàng gửi một gói tin về trung tâm dưới dạng *(a,b)*, trong đó *a* là số tài khoản và *b* là số tiền chuyển vào tài khoản đó. Một kẻ lừa đảo có thể gửi một số tiền nào đó để lấy nội dung gói tin và truyền lại gói tin thu được nhiều lần để thu lợi (tấn công truyền lại gói tin).

2/. Tính toàn vẹn

Cả hai bên tham gia vào quá trình thông tin đều có thể tin tưởng là văn bản không bị sửa đổi trong khi truyền vì nếu văn bản bị thay đổi thì hàm băm cũng sẽ thay đổi và lập tức bị phát hiện. Quá trình mã hóa sẽ ẩn nội dung của gói tin đối với bên thứ 3 nhưng không ngăn cản được việc thay đổi nội dung của nó. Một ví dụ cho trường hợp này là tấn công đồng hình (homomorphism attack): tiếp tục ví dụ như ở trên, một kẻ lừa đảo gửi 1.000.000 đồng vào tài khoản của a, chặn gói tin *(a,b)* mà chi nhánh gửi về trung tâm rồi gửi gói tin (a,b^3) thay thế để lập tức trở thành triệu phú!

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

3/. Tính không thể phủ nhận

Trong giao dịch, một bên có thể từ chối nhận một văn bản nào đó là do mình gửi. Để ngăn ngừa khả năng này, bên nhận có thể yêu cầu bên gửi phải gửi kèm chữ ký số với văn bản. Khi có tranh chấp, bên nhận sẽ dùng chữ ký này như một chứng cứ để bên thứ ba giải quyết. Tuy nhiên, khóa bí mật vẫn có thể bị lộ và tính không thể phủ nhận cũng không thể đạt được hoàn toàn.

1.5.2. Chữ ký điện tử

1.5.2.1. Thế nào là chữ ký điện tử

Một trong những điều kiện quan trọng để dựa vào đó có thể xác định tính hiệu lực của hợp đồng điện tử là quy định về chữ ký điện tử.

Chữ ký điện tử là chữ ký được tạo lập dưới dạng từ, chữ số, ký hiệu, âm thanh, hoặc các hình thức khác bằng phương tiện điện tử, gắn liền, hoặc kết hợp một cách logic với thông điệp dữ liệu, có khả năng xác nhận người ký thông điệp dữ liệu và xác nhận sự chấp thuận của người đó đối với nội dung thông điệp dữ liệu được ký.

Chữ ký điện tử trên thực tế tồn tại ở nhiều dạng. Ví dụ, ở Anh, con dấu của một công ty đã được coi là chữ ký, hoặc bản fax của một chữ ký cũng có giá trị như bản chính. Nhiều phương pháp để "áp" các dấu trên giấy đã được công nhận như là một chữ ký, ví dụ như là một bức thư được in trên giấy tiêu đề của một công ty cũng có thể được coi là được "ký". Như vậy, để phát triển việc giao kết hợp đồng điện tử, người ta đã "mềm hoá" các quy định về chữ ký điện tử và công nhận nhiều hình thức của chữ ký này.

Chỉ cần tồn tại một sự xác nhận nào đó là đã đủ điều kiện để chữ ký điện tử trở thành một chữ ký có hiệu lực. Đối với các thư điện tử, người viết thường tạo một dữ liệu chữ ký ở cuối thư và hình thức này cũng được pháp luật nhiều nước, đặc biệt là các nước theo hệ thống pháp luật Common law chấp nhận có giá trị như một chữ ký. Tuy nhiên, trên thực tế cách thức này không an toàn và dễ bị ăn cắp (chỉ bằng một thao tác cắt-dán đơn giản). Vì vậy, các nước thường đưa ra những quy định liên quan đến chữ ký điện tử nhằm chống lại các hành vi ăn cắp hay hành vi mạo danh chữ ký điện tử. Giao kết hợp đồng điện tử mà không tìm hiểu kỹ các quy định của pháp luật hiện hành về chữ ký điện tử sẽ đặt các doanh nghiệp vào những rủi ro khôn lường.

So sánh chữ ký thông thường với chữ ký điện tử

Chữ ký thông thường	**Chữ ký điện tử**
Vấn đề ký một tài liệu Chữ ký chỉ là một phần vật lý của tài liệu	Vấn đề ký một tài liệu Chữ ký điện tử không gắn kiểu vật lý vào bức thông điệp nên thuật toán được dùng phải « không nhìn thấy »theo một cách nào đó trên thông điệp
Vấn đề về kiểm tra Chữ ký được xác nhận bằng cách so sánh nó với chữ ký xác thực khác. Tuy nhiên, đây không phải là một cách an toàn vì nó rễ bị giả mạo	Vấn đề về kiểm tra Chữ ký điện tử có thể kiểm tra được nhờ dùng một thuật toán « kiểm tra công khai ». Như vậy, bất cứ ai cũng có thể kiểm tra được chữ ký điện tử. Việc dùng chữ ký điện tử an toàn có thể chặn được giả mạo
Bản copy thông điệp được ký bằng chữ ký thông thường lại có thể khác với bản gốc	Bản copy thông điệp được ký bằng chữ ký điện tử thì đồng nhất với bản gốc, điều này có nghĩa là cần phải ngăn chặn một bức thông điệp ký số không bị dừng lại

1.5.2.2. Bảo mật chữ ký điện tử

Pháp luật các nước thường quy định về bảo mật chữ ký điện tử. Một trong những phương pháp tiên tiến đang được nhiều nước áp dụng để bảo mật chữ ký điện tử là mã hoá chữ ký điện tử.

Mã hoá là khoa học về an ninh thông tin, nó gắn liền với các hệ thống xáo trộn thông tin và sau đó sắp xếp lại các thông tin này. Các chuyên gia an ninh thông tin hiện nay nghiêng về sử dụng phương pháp mã hoá chữ ký có tên là hạ tầng mã hoá công khai (Public Key Infrastructure - PKI). Đây là một một trong những phương pháp an toàn và sử dụng một thuật toán để mã hoá các văn bản trực tuyến, theo đó, chỉ có các bên có thẩm quyền truy cập được vào các văn bản này. Các bên này có chìa khoá để đọc và ký vào các văn bản, bởi vậy nó có khả năng đảm bảo không có ai mạo danh chữ ký. Mặc dù các tiêu chuẩn kỹ thuật cho phương pháp này đang trong quá trình nghiên cứu và xây dựng công nghệ PKI được mong chờ chắc chắn sẽ được chấp nhận rộng rãi trong tương lai và các doanh nghiệp, những người tiêu dùng sẽ có khả năng sở hữu và sử dụng chữ ký điện tử mã hoá này.

1.5.3. Một số phương pháp Ký số

1.5.3.1. Chữ ký RSA

Tạo khóa:

Sơ đồ chữ ký cho bởi bộ năm (P, A, K, S, V)

Cho n = p.q; với mỗi p, q là các số nguyên tố lớn khác nhau $\phi(n) = (p-1).(q-1)$.

Cho $P = A = Z_n$ và định nghĩa:

K là tập các khóa, K = (K', K''); với K' = a; K'' = (n,b)

$a, b \in Z_n$, thỏa mãn $ab = 1 \bmod \phi(n)$.

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

Tạo chữ ký:

Với mỗi K = (n.p, q, a, b) xác định:

$Sig_{K'}(x) = x^a \bmod n$

Kiểm tra chữ ký:

$Ver_{K''}(x, y) = true \Leftrightarrow x \equiv y^b \bmod n$; $x, y \in Z_n$

Giả sử A muốn gửi thông báo x, A sẽ tính chữ ký y bằng cách:

$y = Sig_{K'}(x) = x^a \bmod n$ (a là tham số bí mật của A)

A gửi cặp (x, y) cho B. Nhận được thông báo x, chữ ký y, B bắt đầu tiến hành kiểm tra đẳng thức:

$x = y^b \bmod n$ (b là khóa công khai của A)

Nếu đúng, B công nhận y là chữ ký trên x của A. Ngược lại, B sẽ coi x không phải của A gửi cho mình (chữ ký không tin cậy)

Người ta có thể giả mạo chữ ký của A như sau: Chọn y sau đó tính

$x = Ver_{K''}(y)$, khi đó $y = Sig_{K'}(x)$. Một cách khắc phục khó khăn này là việc yêu cầu x phải có nghĩa. Do đó, chữ ký giả mạo thành công với xác suất rất nhỏ. Ta có thể kết hợp chứ ký với mã hóa làm cho độ an toàn tăng lên.

Giả sử trên mạng truyền thông tin công cộng, ta có hai hệ mật mã hóa công khai δ_1 và hệ xác nhận chữ ký δ_2. Giả sử B có bộ khóa mật mã $K = (K', K'')$ với $K' = (n, e)$ và $K'' = d$ trong hệ δ_1 và A có bộ khóa chữ ký $K_s = (K_s', K_s'')$ với $K_s' = a$, $K_s'' = (n, b)$ trong hệ δ_2. A có thể gửi đến cho B một thông báo vừa bảo mật vừa có chữ ký xác nhận như sau: A tính chữ ký của mình là: $y = Sig_A(x)$ và sau đó mã hóa cả x và y bằng cách sử dụng mật mã công khai e_B của B, khi đó A nhận được $z = e_B(x, y)$, bản mã z sẽ được gửi tới B, khi nhận được z việc trước tiên B phải giải mã bằng hàm d_B để nhận được (x, y). Sau đó B sử dụng hàm kiểm tra công khai của A để kiểm tra xem $Ver_A(x, y) = true$? Tức là kiểm tra xem chữ ký đó có đúng là của A không.

Ví dụ

A dùng lược đồ chữ ký RSA với n = 247, với p = 13, q = 19;

$\phi(n) = 12. 18 = 216$. Khóa công khai của A là b = 7

$=> a = 7^{-1} \mod 216 = 31$.

A công khai (n, b) = (247, 7)

A ký trên thông báo x = 100 với chữ ký :

$$y = x^a \mod n = 100^{31} \mod 247 = 74$$

A gửi cặp (x, y) = (100, 74) cho B, B kiểm tra bằng cách sử dụng khóa công khai của A như sau:

$x = y^b \mod n = 74^7 \mod 247 = 100 = x$.

B chấp nhận y = 74 là chữ ký đáng tin

1.5.3.2. Chữ ký ElGamal

Lược đồ chữ ký ElGamal được giới thiệu năm 1985 và được viện tiêu chuẩn và Công nghệ quốc gia Mỹ sửa đổi thành chuẩn chữ ký số. Lược đồ chữ ký ElGamal không tất định phải giống như hệ mã hóa ElGamal. Điều này có nghĩa là có nhiều chữ ký hợp lệ cho một thông báo bất kỳ. Thuật toán kiểm tra phải có khả năng chấp nhận bấy kỳ một chữ ký hợp lệ nào khi xác minh.

Lược đồ chữ ký ElGamal được định nghĩa như sau:

Tạo khóa:

Cho p là số nguyên tố sao cho bài toán logarit rời rạc trong Z_p là khó giải

và giả sử

$\alpha \in Z_p^*$ là phần tử nguyên thủy

Cho p = Z_p^*, A = Z_p^*. Z_{p-1} và định nghĩa

$$K = \{(p, a, \alpha, \beta): \beta = \alpha^a \bmod p\}.$$

Các giá trị p, α, β là công khai, a là bí mật.

Tạo chữ ký

Với K = (p, a, α, β) và với số ngẫu nhiên Z_{p-1}^*

Định nghĩa $Sig_K(\gamma, \delta)$ trong đó:

$\gamma = \alpha^k \bmod p$ và $\delta = (x - a^*\gamma) * k^{-1} \bmod (p-1)$

Kiểm tra chữ ký:

Với x, y $\in Z_p^*$ và $\delta \in Z_{p-1}^*$, ta định nghĩa

$Ver_k(x, \gamma, \delta)$ = TRUE $\Leftrightarrow \beta^\gamma \gamma^\delta \equiv \alpha^x \bmod p$.

Chứng minh:

Nếu chứ ký được thiết lập đúng thì hàm kiểm tra sẽ thành công vì:

$$\beta^{\gamma}\gamma^{\delta} \equiv \alpha^{a\gamma}.\ \alpha^{e\delta} \bmod p$$

$$\equiv \alpha^{x} \bmod p \ (\text{vì } \alpha\gamma + r\delta \equiv x \bmod (p-1))$$

A tính chữ ký bằng cách dùng cả giá trị bí mật a (là một phần của khóa) lẫn số ngẫu nhiên bí mật k (dùng để ký trên x). Việc kiểm tra có thể được thực hiện duy nhất bằng thông tin công khai.

Ví dụ: Giả sử p = 467, α = 2, a = 127

Khi đó: $\beta = \alpha^{k} \bmod p = 2^{127} \bmod 467 = 132$.

Giả sử A có thong báo x = 100 và A chọn ngẫu nhiên k = 213 vì (213, 466) = 1 và

$\delta = (x - a\gamma)k^{-1} \bmod (p-1) = (100 - 127.\ 29).\ 431 \bmod 466 = 51$

Chứ ký của A trên x = 100 là (29, 51)

Bất kỳ người nào cũng có thể kiểm tra chữ ký bằng cách:

$132^{29}.\ 29^{51} = 189 \bmod 467$

$2^{100} = 189 \bmod 467$

Do đó, chữ ký là tin cậy.

1.5.3.3.Chữ ký số Schnorr (Chữ ký một lần)

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

Với sơ đồ chữ ký dùng một lần của Schnorr, những người dùng trong cùng hệ thống có thể chia sẻ một số ngẫu nhiên g và hai số nguyên tố p và q sao cho q|(p-1), q#1 và $g^q \equiv 1 \bmod q$. Sơ đồ ký như sau:

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 khác 0 làm khóa bí mật.

Tính $y = g^x$ làm khóa công khai.

Lấy H là hàm băm không va chạm.

Ký: Chọn r ngẫu nhiên thuộc Zq,

Tính $c = H(m, g^r)$

Tính $s = (r - c.x) \bmod q$

Chữ ký Schnorr là cặp (c, s).

Kiểm tra chữ ký:

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

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

Để ý rằng ở đây, c xuất hiện ở cả hai vế của phương trình

1.5.3.4. Chữ ký không thể phủ nhận (Chống chối bỏ)

Chữ ký không thể phủ nhận do David Chaum và Hans Van Antwerpen phát minh năm 1989. Ở đây, thuật toán kiểm định đòi hỏi phải có sự tham gia của người ký. Thực chất đây là chữ ký có tính chất không thể chuyển giao được (Untranferable). Chỉ có ý nghĩa với người nhận là người có trao đổi làm ăn với người ký, khi chuyển nó cho một người khác thì không còn tác dụng nữa (không thể kiểm định được chữ ký nữa). Các văn bản có chữ ký này không nhằm vào mục đích đem đi công bố ở nơi khác mà chỉ có tính chất giấy phép. Vì thế nếu sao chép là mất ý nghĩa.

Thuật toán

❖ **Chuẩn bị các tham số**

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

  p = 2*q+1, q cũng là số nguyên tố.
- Gọi P là nhóm nhân con của Zp* theo q (P gồm các thặng dư bậc 2 theo mod p).
- Chọn phần tử sinh g của nhóm P cấp q.

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

❖ **Thuật toán ký**

- Dùng khóa bí mật k’ = a để ký lên x:

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

❖ **Giao thức kiểm thử**

- Dùng khóa công khai k’’ = (p, g, h)
- Với x, y $\in$ P người nhận N cùng người gửi G thực hiện giao thức kiểm thử:

  B1: N chọn ngẫu nhiên e_1 , $e_2 \in Z_q^*$

  B2: N tính $c = y^{e1} h^{e2} \bmod p$, và gửi cho G.

  B3: G tính $d = c^{a-1 \bmod q} \bmod p$ và gửi cho N.

  B4: N chấp nhận y là chữ ký đúng nếu $d \equiv y^{e1} g^{e2} \bmod p$

❖ **Giao thức chối bỏ**

B1: N chọn ngẫu nhiên e_1 , $e_2 \in Z_q^*$

B2: N tính $c = y^{e1} h^{e2} \bmod p$, và gửi cho G.

B3: G tính $d = c^{a-1 \bmod q} \bmod p$ và gửi cho N.

B4: N thử điều kiện $d \neq x^{e1} g^{e2} \bmod p$.

B5: N chọn ngẫu nhiên f_1 , $f_2 \in Z_q^*$

B6: N tính $C = \gamma^{f1} \beta^{f2} \bmod p$, và gửi cho G.

B7: G tính $D = C^{a-1 \bmod q} \bmod p$ và gửi cho N.

B8: N thử điều kiện $D \neq x^{f1} g^{f2} \bmod p$.

B9: N kết luận y là chữ ký giả mạo nếu:

$(d * \alpha^{-e}{}_2)^{f}{}_1 \equiv (D * \alpha^{-f}{}_2)^{e}{}_1 \bmod p$ (thay α bằng g)

1.5.3.5. Các loại chữ ký khác

1/. Chữ ký đồng thời

Ở đây, chữ ký không phải là của một người mà là của một nhóm người. Muốn tạo được chữ ký, tất cả những người này phải tham gia vào một giao thức (protocal). Tuy nhiên chữ ký có thể được kiểm định bởi bất cứ ai. Đây là trường hợp dành cho thực tế của việc đưa ra những quyết định của nhiều người.

2/. Chữ ký ủy nhiệm

Hệ chữ ký này dành cho các trường hợp mà người chủ chữ ký bị ốm không có khả năng làm việc hay đã đi vắng đến một nơi không có phương tiện mạng máy tính cần thiết để ký. Vì vậy chữ ký ủy nhiệm được tạo ra để người ký có thể ủy nhiệm cho một người nào đó ký thay. Tất nhiên chữ ký ủy nhiệm phải có các thuộc tính riêng thêm vào:

- Chữ ký ủy nhiệm là phần phân biệt với chữ ký thường và người được ủy nhiệm không thể tạo được chữ ký chủ (chữ ký của người chủ).

- Chữ ký ủy nhiệm cũng có chức năng chứng thực như chữ ký chủ, chỉ có người được ủy nhiệm và người chủ mới có thể tạo được chữ ký này. Người nhận được văn bản có thể hoàn toàn tin tưởng vào chữ ký đó như chữ ký chủ.

- Người chủ có thể xác định được danh tính của người ký từ một chữ ký ủy nhiệm.

- Người được ủy nhiệm không thể chối cãi được nếu đã ký vào một văn bản ủy nhiệm hợp lệ (tức là anh ta không thể chối đổ cho ai khác hay chính người chủ đã ký mà lại nói là anh ta ký).

3/. Chữ ký nhóm

Tình huống thực tế minh họa cho chữ ký này như sau: Một công ty có nhiều máy tính nối với nhau trong một mạng cục bộ, các máy tính này được đặt trong một số phòng ban bộ phận. Mỗi phòng chỉ có một máy in mà chỉ các cán bộ của phòng mới được in ra. Vì vậy người ta muốn một cơ chế để việc in này có thể thực hiện mà việc kiểm soát không cho người ngoài phòng in được, trong khi mỗi yêu cầu in lại không cần nêu rõ tên người yêu cầu để tránh xâm phạm tính riêng tư của từng công việc.

Như vậy, một hệ chữ ký sẽ được thiết lập sao cho chỉ có những người nằm trong một nhóm người nào đó - trong cùng phòng - là có thể tạo ra được chữ ký mà người kiểm định - trong ví dụ trên là máy in hay chương trình quản lý máy in - kiểm tra và chấp nhận. Chữ ký này chỉ nói lên người ký nằm trong nhóm đó mà thôi chứ không nói lên đích xác đó là người nào lên giữ được tính riêng tư của từng người ký. Tuy nhiên hệ chữ ký đặc biệt này còn có một tính chất đặc biệt khác nữa là: nếu cần thiết, một người thẩm quyền có thể "mở" được một chữ ký ra để xem ai cụ thể trong nhóm đã ký.

Ứng dụng của nó là nếu chương trình quản lý máy in cho thấy có người đã quá lạm dụng thì trưởng phòng có thể dùng quyền giới hạn của mình để "cảnh báo" những chữ ký lên những yêu cầu in tốn kém đó, sau đó có biện pháp phạt người lạm dụng đó. Khả năng nay làm cho tất cả mọi người phải biết điều độ với máy in của công ty, nếu không muốn bị nêu tên cảnh báo.

1.6. THỎA THUẬN HỢP ĐỒNG ĐIỆN TỬ

1.6.1. Khái niệm về giao kết hợp đồng điện tử

Khái niệm giao kết hợp đồng điện tử

Giao kết hợp đồng là thuật ngữ được Bộ luật dân sự Việt Nam năm 2005 sử dụng để chỉ việc ký kết hợp đồng. Vì vậy, giao kết hợp đồng điện tử là quá trình đàm phán, thương thảo, tạo lập và ký kết hợp đồng thông qua trao đổi các dữ liệu điện tử. Các hợp đồng như vậy sẽ được lưu trữ hoàn toàn ở dạng dữ liệu điện tử.

Luật Giao dịch điện tử Việt Nam năm 2005 định nghĩa: "Giao kết hợp đồng điện tử là việc sử dụng thông điệp dữ liệu để tiến hành một phần hay toàn bộ giao dịch trong quá trình giao kết hợp đồng". Quá trình giao kết hợp đồng có thể được thực hiện qua nhiều giao dịch, từ việc quảng cáo hàng hóa (dịch vụ), chào bán, chào mua hàng hóa (dịch vụ) đến chấp nhận mua hay bán hàng hóa, dịch vụ đó. Khi một số các giao dịch này hay toàn bộ các giao dịch này được thực hiện thông qua việc trao đổi dữ liệu (như trao đổi dưới dạng điện tín, điện báo, fax, thư điện tử…) thì quá trình đó được gọi là quá trình giao kết hợp đồng điện tử.

Trên thực tế việc giao kết hợp đồng điện tử có thể đơn giản là việc người tiêu dùng thực hiện một giao dịch nhỏ, đơn giản thông qua các phương tiện điện tử như đặt mua vé máy bay, vé tàu qua điện thoại hoặc Internet; đặt mua sách, mua hàng hóa tiêu dùng thông qua chào hàng hoặc đặt hàng thông qua website bán hàng của doanh nghiệp kinh doanh hàng hóa trên mạng, thanh toán thông qua thẻ ngân hàng…Hợp đồng điện tử cũng có thể được giao kết giữa 2 hay nhiều công ty để thực hiện giao dịch, trao đổi nhằm bán hoặc mua hàng hóa,dịch vụ nhằm mục đích thương mại. Quá trình giao kết này có thể dẫn đến giá trị một hợp đồng lớn và tính chất phức tạp, trong thực tiễn TMĐT, phương thức này được gọi là B2B (BUSINESS TO BUSINESS).

1.6.2. Chủ thể của hợp đồng điện tử

Chủ thể tham gia giao kết hợp đồng điện tử gồm các bên - người bán và người mua hàng hoá (hoặc cung ứng dịch vụ) qua mạng. Để hợp đồng có hiệu lực, chủ thể phải có năng lực pháp lý và năng lực hành vi. Tuy nhiên, việc xác định năng lực chủ thể của các chủ thể trong giao kết hợp đồng điện tử sẽ trở nên khó khăn hơn rất nhiều so với trong hợp đồng truyền thống. Những khó khăn đó là:

- Người bán trên mạng chắc chắn không muốn và không thể bán hàng hoá và dịch vụ cho mọi đối tượng vào mạng Internet. Họ bị ràng buộc và chi phối bởi các quy định pháp lý của nước mình cũng như nước ngoài tham gia giao kết với họ. Chẳng hạn lệnh cấm vận của Mỹ với Irap, Libya, Cuba sẽ làm vô hiệu hoá các hợp đồng điện tử được giao kết giữa các cá nhân và tổ chức của các nước này với nhau. Hoặc theo quy định của pháp luật mỗi nước, một mặt hàng hoá hay dịch vụ đối với nước này là hợp pháp nhưng ở nước khác lại bị cấm lưu thông cũng làm cho hợp đồng điện tử được giao kết để mua hàng hay dịch vụ không thực hiện được dù đã giao kết. Vì vậy, chỉ một sơ suất nhỏ trong việc xác định năng lực của các chủ thể sẽ có thể dẫn đến hợp đồng điện tử vô hiệu và gây ra nhiều tổn thất thiệt hại cho người bán.

- Khó khăn nhất trong việc xác định năng lực chủ thể đối với các doanh nghiệp cung cấp hàng hoá (dịch vụ) qua mạng là khó xác định được xem liệu khách hàng có đủ năng lực hành vi hay chưa. Vấn đề rắc rối phát sinh khi khách hàng ở tuổi vị thành niên.

Một là, theo quy định của pháp luật ở một số nước, có một số loại hàng hoá cấm bán cho đối tượng là vị thành niên như thuốc lá, rượu, sách báo khiêu dâm v.v…Theo pháp luật của những nước này, người bán trong trường hợp này có thể bị buộc vào tội hình sự hoặc phải chịu trách nhiệm dân sự nếu không biết chắc khách hàng của mình đã đủ tuổi hành vi hay chưa. Rất khó xác định được điều này khi mua hàng qua mạng.

Hai là, các hợp đồng giao kết với tuổi vị thành niên mà không nhằm phục vụ nhu cầu sinh hoạt thiết yếu của chúng cũng sẽ bị vô hiệu. Vấn đề là hợp đồng sẽ bị vô hiệu với vị thành niên nhưng vị thành niên sẽ được miễn trách nhiệm và sẽ gây ra nhiều hậu quả pháp lý cho người bán.

- Sự xuất hiện của người thứ ba trong giao kết hợp đồng điện tử. Có thể thấy vai trò của người thứ ba trong việc giao kết hợp đồng điện tử, vai trò của bên thứ ba là nhà cung cấp dịch vụ mạng, các cơ quan chứng thực là rất quan trọng vì họ có thể đảm bảo giá trị pháp lý và tính hiệu lực của hợp đồng điện tử. Chính họ là người chuyển, lưu giữ các thông tin điện tử, các thông điệp số, cung cấp chứng thực xác nhận độ chính xác và tin cậy của các thông tin điện tử và các thông điệp số đó. Vì vậy, để các hoạt động TMĐT phát huy hết vai trò của nó một cách có hiệu quả thì pháp luật về TMĐT cần phải có các quy định về trách nhiệm và giới hạn trách nhiệm của các nhà cung cấp dịch vụ mạng với các thông tin mà họ gửi, nhận và lưu trữ trong máy chủ. Đồng thời cũng cần phải ban hành các quy định pháp lý cụ thể điều chỉnh hoạt động của các cơ quan chứng thực trên mạng. Những quy định này chính là cơ sở pháp lý hướng dẫn việc giao kết hợp đồng điện tử mà các chủ thể giao kết hợp đồng điện tử, đặc biệt là các doanh nghiệp kinh doanh trên mạng phải nghiên cứu để tuân thủ trước khi thực hiện giao kết hợp đồng điện tử nói chung và giao kết hợp đồng thương mại điện tử nói riêng, nếu họ muốn thành công trong lĩnh vực kinh doanh đặc biệt này.

Tóm lại, việc xác định năng lực của chủ thể trong giao kết hợp đồng điện tử là vô cùng quan trọng, với tính đặc thù của loại hình kinh doanh này mang tính phi biên giới nên nó mang trong mình những rủi ro pháp lý về chủ thể giao kết hợp đồng mà những nhà kinh doanh cần hết sức cẩn trọng trong việc giao kết hợp đồng điện tử. Chỉ cần một chút thiếu cẩn trọng trong việc xác định năng lực của chủ thể giao kết hợp đồng điện tử có thể đem lại cho những nhà cung cấp hàng hoá (dịch vụ) những tổn thất và hậu quả pháp lý nghiêm trọng.

1.6.3. Hình thức hợp đồng điện tử

Hợp đồng điện tử được thiết lập dưới dạng thông điệp dữ liệu, hay nói cách khác, là hợp đồng điện tử không sử dụng các hình thức hợp đồng truyền thống như hợp đồng bằng lời nói, bằng hành vi hay bằng văn bản. Hợp đồng điện tử có thể là hợp đồng được thảo và gửi qua thư điện tử hoặc là hợp đồng nhấn nút đồng ý qua các trang web bán hàng, theo đó khi người mua nhấn vào nút "tôi đồng ý" trên trang web bán hàng (có chứa các điều kiện mua bán trước khi giao dịch hoàn thành) thì hợp đồng được coi là giao kết và các bên phải thực hiện các cam kết của mình.

Một trong những vấn đề khó khăn của hợp đồng điện tử là các thoả thuận như vậy thường được thực hiện trong môi trường hoàn toàn trực tuyến. Một môi trường như vậy liệu có mang tính ràng buộc pháp lý hay không?

Câu hỏi này cũng như những khó khăn nêu trên được lý giải rõ hơn nếu điểm qua một số dạng, một số biểu hiện của hình thức hợp đồng điện tử mà chúng được sử dụng phổ biến hiện nay trong giao kết hợp đồng điện tử. Các dạng biểu hiện về hình thức của giao kết hợp đồng điện tử là:

- **Hình thức trao đổi dữ liệu điện tử**

Trao đổi dữ liệu điện tử (Electronic Data Interchange viết tắt là EDI) là việc trao đổi các dữ liệu dưới dạng "có cấu trúc". Có cấu trúc nghĩa là các thông tin trao đổi được các đối tác thoả thuận với nhau sẽ tuân thủ theo một khuôn dạng nào đó từ máy tính điện tử này sang máy tính điện tử khác, giữa các công ty hoặc giữa các đơn vị đã thoả thuận buôn bán với nhau. Theo cách này, sẽ tự động hoá hoàn toàn không cần đến sự can thiệp của con người. Theo uỷ ban của Liên Hiệp Quốc về Luật Thương mại Quốc Tế (UNCITRAL), việc trao đổi dữ liệu điện tử được quy định như sau: "*Trao đổi dữ liệu điện tử (EDI) là việc chuyển giao thông tin từ máy tính điện tử này sang máy tính điện tử khác bằng phương tiện điện tử, có sử dụng một tiêu chuẩn đã được thoả thuận để cấu trúc thông tin*"

- **Hình thức thanh toán điện tử**

Một trong những dạng biểu hiện của hình thức hợp đồng điện tử là thanh toán điện tử. Thanh toán điện tử (electronic payment) là việc thanh toán tiền thông qua bản tin điện tử (electronic message) thay cho việc dùng tiền mặt. Ví dụ, trả lương bằng cách chuyển tiền trực tiếp vào tài khoản, trả tiền mua hàng bằng thẻ mua hàng, thẻ tín dụng v.v…Ngày nay, với sự phát triển của TMĐT, thanh toán điện tử đã mở rộng và được thực hiện dưới các hình thức khác nhau như:

- *Trao đổi dữ liệu điện tử tài chính* (Financial Electronic Data Interchange, gọi tắt là FEDI) chuyên phục vụ cho việc thanh toán điện tử giữa các công ty giao dịch với nhau bằng điện tử.

- *Tiền mặt Internet* (Internet Cash) là tiền mặt được mua từ một nơi phát hành (ngân hàng hoặc một tổ chức tín dụng nào đó), sau đó được chuyển đổi tự do sang các đồng tiền khác thông qua Internet, áp dụng trong phạm vi một nước cũng như giữa các quốc gia với nhau; tất cả đều được thực hiện bằng kỹ thuật số hoá, vì thế tiền mặt này còn có tên gọi là "tiền mặt số hoá" (digital cash).

- *Túi tiền điện tử* (electronic purse), còn gọi là "ví điện tử" là nơi để tiền mặt Internet, chủ yếu là thẻ thông minh (smart card), còn gọi là thẻ giữ tiền (stored value card), tiền được trả cho bất kỳ ai đọc được thẻ đó.

- **Hình thức thư điện tử**

Hình thức phổ biến của hợp đồng điện tử là thư điện tử. Luật giao dịch điện tử Việt Nam năm 2005 quy định: "*Hình thức hợp đồng điện tử là hợp đồng được thiết lập dưới dạng thông điệp dữ liệu*"(Điều 33). Điều 10 của Luật này giải thích rõ: "*Thông điệp dữ liệu được thể hiện dưới hình thức trao đổi dữ liệu điện tử, chứng từ điện tử, thư điện tử, điện tín, điện báo, fax*…".

Các doanh nghiệp, các cơ quan nhà nước…sử dụng thư điện tử để gửi cho nhau một cách "trực tuyến" thông qua mạng, gọi là thư điện tử (electronic mail, viết tắt là e-mail). Thông tin trong thư điện tử không phải tuân theo một cấu trúc định trước nào.

Trên đây liệt kê ba dạng biểu hiện về hình thức của hợp đồng điện tử. Về mặt kỹ thuật công nghệ thông tin, các dạng biểu hiện về hình thức của hợp đồng điện tử này còn được gọi là thông điệp dữ liệu điện tử. Vậy hình thức hợp đồng dưới dạng thông điệp dữ liệu điện tử này có giá trị pháp lý như thế nào? Luật pháp các nước khác nhau quy định không giống nhau về vấn đề này. Các nước theo hệ thống luật Anh-Mỹ (Comon law) thừa nhận dữ liệu máy tính là một tài liệu vì nó chứa "những thông tin có thể đọc được, có thể lưu trữ trong máy tính hoặc các file dữ liệu". Mặc dù vậy, dữ liệu máy tính chưa thoả mãn đầy đủ các yêu cầu được coi là dạng văn bản. Theo điều 1 Luật năm 1978 của Anh thì: "Văn bản được hiểu là bản đánh máy, bản in, bản ảnh và các hình thức thể hiện từ ngữ ở dạng hữu hình". Dữ liệu máy tính không được coi là hữu hình.

Giá trị pháp lý của các tài liệu điện tử được Luật mẫu của UNCITRAL thừa nhận, theo Điều 5; Điều 6 của Luật này quy định không có sự khác nhau về giá trị pháp lý giữa tài liệu điện tử và tài liệu trên giấy. Tuy nhiên, Luật mẫu chỉ có giá trị khi các bên dẫn chiếu trong hợp đồng thì nó mới có giá trị thực sự.

Luật thương mại Việt Nam năm 1997 khẳng định thư điện tử và các hình thức thông tin điện tử khác cũng được coi là hình thức văn bản (Điều 49). Luật thương mại năm 2005, Điều 15 đã có quy định rõ hơn: "*Trong hoạt động thương mại, các thông điệp dữ liệu đáp ứng điều kiện, tiêu chuẩn kỹ thuật theo quy định của pháp luật thì được thừa nhận có giá trị pháp lý tương đương văn bản*". Luật giao dịch điện tử Việt Nam năm 2005 cụ thể: "thông điệp dữ liệu được thể hiện dưới hình thức trao đổi dữ liệu điện tử, chứng từ điện tử, thư điện tử, điện tín, fax và các hình thức tương tự khác" (Điều 10). Luật giao dịch điện tử năm 2005 khẳng định giá trị pháp lý của các thông điệp dữ liệu điện tử trên là: "Thông tin trong thông điệp dữ liệu không bị phủ nhận giá trị pháp lý chỉ vì thông tin đó được thể hiện dưới dạng thông điệp dữ liệu" (Điều 11).

Nhằm hướng dẫn các doanh nghiệp về vấn đề này, đặc biệt, nhằm làm yên lòng các doanh nghiệp cũng như các chủ thể tham gia giao kết hợp đồng điện tử, Điều 12 luật Giao dịch điện tử năm 2005 quy định:

"Trong trường hợp pháp luật yêu cầu thông tin phải được thể hiện bằng văn bản thì thông điệp dữ liệu được xem là đáp ứng yêu cầu này nếu thông tin chứa trong thông điệp dữ liệu đó có thể truy cập và sử dụng được để tham chiếu khi cần thiết". Những quy định này sẽ là cơ sở pháp lý quan trọng thừa nhận giá trị pháp lý các hình thức khác nhau của hợp đồng điện tử nếu những thông điệp hình thức này có chứa những thông tin có thể truy cập và sử dụng được để tham chiếu khi cần thiết. Như vậy, trong những năm gần đây thực tiễn pháp lý nhiều nước trên thế giới cũng như Việt Nam đã có sự thừa nhận là hình thức hợp pháp của hợp đồng điện tử, có giá trị pháp lý như văn bản, có giá trị làm chứng cứ (nếu đáp ứng các điều kiện do luật định). Vấn đề còn lại là phải làm sao để những thông tin chứa trong thông điệp dữ liệu đó có thể truy cập được và sử dụng được để tham chiếu khi cần thiết.

1.6.4. Thời gian và địa điểm giao kết hợp đồng điện tử

Về trình tự giao kết hợp đồng điện tử, các bên giao kết vẫn phải tuân theo những quy định về đề nghị giao kết hợp đồng (chào hàng) và chấp nhận chào hàng như đối với việc giao kết hợp đồng truyền thống. Tuy vậy, việc "gửi" và "nhận" một chào hàng hay một chấp nhận chào hàng được thể hiện dưới hình thức một thông điệp dữ liệu có tính chất khác với việc gửi và nhận một hình thức "vật chất" thông thường. Vấn đề được đặt ra khi giao kết hợp đồng điện tử là: Khi nào chào hàng bắt đầu có hiệu lực, khi nào chấp nhận chào hàng được coi là đã được gửi đi hay đã nhận bởi người chào hàng?

Vì chào hàng và chấp nhận chào hàng là những thông tin được tạo ra, được gửi đi, được nhận và được lưu trữ bằng phương tiện điện tử cho nên quá trình này thường không cần có sự can thiệp trực tiếp của con người. Điều này dẫn đến một khó khăn trong việc xác định thời gian và địa điểm giao kết hợp đồng. Thời gian giao kết hợp đồng là yếu tố quan trọng xác định thời điểm có hiệu lực của hợp đồng khi không có một thoả thuận nào khác của các bên. Còn địa điểm giao kết hợp đồng là một trong những căn cứ để xác định luật điều chỉnh các giao dịch trong hợp đồng quốc tế.

Câu hỏi đầu tiên được đặt ra là, khi nào hợp đồng được coi là giao kết. Dù áp dụng thuyết tiếp thu hay thuyết tống phát thì cũng cần phải xác định thời điểm một thông điệp dữ liệu (ví dụ, một chấp nhận chào hàng được "gửi" bởi người khởi tạo - người được chào hàng) được "nhận" bởi người nhận (người chào hàng). Thời điểm được chuyển ra ngoài hệ thống thông tin của người gửi, hay thời điểm thông điệp dữ liệu được nhập vào một hệ thống thông tin ngoài tầm kiểm soát của người gửi. Còn thời gian nhận được thông điệp số là thời điểm thông điệp đó nhập vào hệ thống thông tin của người nhận, khi nó đến máy chủ của người chào hàng, khi nó được tải về máy tính của người này, hay khi người chào hàng đọc nó? Các thời điểm này có thể khác nhau tuỳ thuộc vào thời điểm người chào hàng nối mạng. Trong các án lệ về giao kết hợp đồng điện tử, trọng tài, toà án thường xét đến thời gian tiếp nhận dự kiến, thường được xác định bằng cách giả định rằng người chào hàng phải liên tục, một cách hợp lý, kết nối để nhận các thông điệp (e-mail văn bản chẳng hạn) gửi đến mình và khi nhận được thì phải đọc ngay khi đã tải về. Vấn đề sẽ còn phức tạp hơn khi phải dự tính đến chênh lệch múi giờ giữa các nước, giờ mở văn phòng … Ví dụ, nếu một thông điệp chấp nhận chào hàng được gửi ngày 30/09/2007 lúc 18h30, hợp đồng sẽ được coi là giao kết vào ngày làm việc kế tiếp, tức ngày 01/10/2007 khi văn phòng của người chào hàng bắt đầu mở cửa. Luật mẫu về TMĐT của UNCITRAL, Điều 15 quy định: *" việc gửi một thông tin số hóa được coi là hoàn thành khi thông tin đó vào hệ thông thông tin không phụ thuộc vào người gửi, trừ trường hợp có thỏa thuận khác giữa người gửi và người nhận"*.

Trong Luật giao dịch điện tử Việt Nam năm 2005, Điều 17 quy định rõ:

"*Trong trường hợp các bên tham gia giao dịch không có thỏa thuận khác thì thời điểm gửi thông điệp dữ liệu được quy định như sau: thời điểm gửi một thông điệp dữ liệu là thời điểm thông điệp dữ liệu này vào hệ thống thông tin nằm ngoài tầm kiểm soát của người khởi tạo*"

Về thời điểm nhận dữ liệu, Điều 19 của Luật giao dịch điện tử Việt Nam năm 2005 quy định như sau: "*Nếu người nhận đã chỉ định một hệ thống thông tin để nhận thông điệp dữ liệu , thời điểm nhận được thông điệp dữ liệu là thời điểm thông điệp nhập vào hệ thống thông tin đã được chỉ định. Nếu người nhận không chỉ định một hệ thống thông tin thì thời điểm nhận là thời điểm thông điệp dữ liệu nhập vào bất kỳ hệ thống thông tin nào của người nhận*"

Như vậy, nếu Luật mẫu của UNCITRAL chủ yếu nhấn vào thời điểm người nhận truy cập vào hệ thống thông tin thì luật giao dịch điện tử của Việt Nam lại nhấn mạnh vào thời điểm thông điệp dữ liệu đi vào hệ thống thông tin.

Tuy nhiên, có thể nhận thấy cả 2 nguồn luật trên đều đã gián tiếp gắn kết giao dịch điện tử vào với một mạng truyền nhất định, thông qua việc đề cập tới các khái niệm về hệ thống thông tin nằm ngoài tầm kiểm soát của người nhận. Vậy nếu như theo cách hiểu giao dịch điện tử thực hiện bằng các phương tiện điện tử và không gắn với một mạng truyền tin thì khái niệm hệ thống thông tin của người gửi và người nhận sẽ được hiểu như thế nào? Đây vẫn là câu hỏi bỏ ngỏ cho các nhà làm luật của Việt Nam và quốc tế

Khó khăn tương tự cũng sẽ phát sinh khi xác định địa điểm giao kết hợp đồng. Người chào hàng có thể thực hiện việc trao đổi dữ liệu để giao kết hợp đồng điện tử ở khắp nơi, không nhất thiết phải là trụ sở, hay tại nơi cư trú của mình. Các bên trong giao dịch TMĐT tiếp xúc với nhau trong môi trường ảo, một môi trường "số hoá", mọi lúc, mọi nơi đề có thể truy cập vào mạng để gửi và nhận thông điệp dữ liệu.

Vậy địa điểm gửi và nhận thông điệp dữ liệu (nhằm xác định địa điểm giao kết hợp đồng) có phải là địa điểm các bên có mặt, một cách thực tế, khi gửi/nhận hay không? Một địa điểm như vậy sẽ được xác minh và chứng minh như thế nào? Điều này dường như là khó có thể thực hiện được do tính phi biên giới và tính ảo của môi trường điện tử.

Và khi đã xác định được một địa điểm như vậy thì sẽ xảy ra những trường hợp địa điểm này lại không có mối liên hệ với các chủ thể tham gia, với nơi phát sinh nghĩa vụ hay nơi thực hiện nghĩa vụ. Trong bối cảnh đó, vấn đề đặt ra sẽ là cần phải xác định địa điểm gửi và nhận thông điệp dữ liệu như thế nào và theo nguyên tắc nào?

Luật mẫu của UNCITRAL Điều 15, khoản 4 quy định như sau: "Thông điệp dữ liệu được suy đoán là đã được gửi đi từ người gửi đặt tại cơ sở và được nhận tại nơi người nhận đặt tại cơ sở, trừ trường hợp có thỏa thuận khác giữa người gửi và người nhận". Nếu người gửi và người nhận có nhiều hơn một cơ sở thì cơ sở nhận tin hoặc gửi tin là cơ sở có liên quan chặt chẽ nhất với hoạt động diễn ra tại đó, hoặc nếu không có hoạt động diễn ra tại đó thì là cơ sở chính. Nếu người gửi hoặc người nhận không có cơ sở nào thì đó là nơi người nhận hoặc người gửi thường trú. Nơi liên quan chặt chẽ đến hoạt động diễn ra tại đó có thể được hiểu là nơi diễn ra hoặc liên quan nhiều nhất tới giao dịch đối tượng của hợp đồng. Tuy nhiên, lại không có quy định rõ thế nào là chặt chẽ, do đó vấn đề này có lẽ sẽ được quyết định bởi từng cơ quan giải quyết cụ thể.

Theo Luật giao dịch điện tử của Việt Nam 2005 thì địa điểm gửi nhận các thông điểm dữ liệu được quy định tai Điều 17,119 như sau : "*địa điểm gửi, nhận thông điệp dữ liệu là " trụ sở của người khởi tạo, người nhận nếu người khởi tạo là cá nhân. Nếu người khởi tạo/người nhận có nhiều trụ sở thì địa điểm gửi/ nhận thông điệp dữ liệu là trụ sở có mối liên hệ mật thiết với giao dịch*". Tuy nhiên, vấn đề còn bỏ ngỏ là nếu người gửi/nhận giao dịch tại 1 cửa hàng internet hoặc tại một nơi mình đang đi công tác thì sao?

1.6.5. Nội dung hợp đồng điện tử

Nội dung của một hợp đồng điện tử bao gồm các điều khoản thoả thuận giữa các chủ thể. Đối với hợp đồng điện tử, các điều khoản này mang tính kỹ thuật điện tử rất cao và thường do người bán (hoặc người cung ứng dịch vụ) làm sẵn và hiển thị trên web của mình.

Vì vậy, khi nói đến nội dung của hợp đồng điện tử, khác với hợp đồng truyền thống- hợp đồng mà khi đàm phán để tiến tới giao kết, các bên thường chỉ chú ý đến các điều khoản chủ yếu làm thành nội dung của hợp đồng như đối tượng của hợp đồng, giá cả, điều kiện thanh toán, điều kiện cơ sở giao hàng v.v…Ở hợp đồng điện tử, các bên giao kết hợp đồng bắt buộc và trước hết phải chú ý đến những quy định có tính kỹ thuật của công nghệ tin học. Đó là cách hiển thị nội dung của hợp đồng điện tử. Nếu không thao tác tốt, chính xác quy trình kỹ thuật này thì việc giao kết hợp đồng điện tử về mặt nội dung cũng không thể đạt được. Vì vậy, khía cạnh pháp lý của quy trình giao kết liên quan đến nội dung của hợp đồng điện tử. Từ đó, có thể khẳng định, các yêu cầu về mặt kỹ thuật của cách hiển thị nội dung của hợp đồng điện tử cũng chính là cơ sở pháp lý mà các bên phải tuân thủ khi giao kết hợp đồng điện tử, đặc biệt là hợp đồng TMĐT.

1.6.5.1. Cách hiển thị nội dung của hợp đồng điện tử

Để những nội dung này có hiệu lực thì trước hết phải thu hút được sự chú ý của người truy cập. Các cách hiển thị hiện nay là:

- Hiển thị không có đường dẫn "without hyperlink":

Theo cách này, người bán thường ghi chú ở cuối mỗi đơn hàng rằng: "Hợp đồng này tuân theo các điều khoản tiêu chuẩn của công ty". Tuy nhiên, cách thức này có nhược điểm là chưa đủ mạnh để thu hút sự chú ý của khách hàng và nếu khách hàng có để ý tới đi nữa thì họ cũng không biết tìm các điều khoản tiêu chuẩn của công ty ở đâu.

- Hiển thị có đường dẫn "with hyperlink":

Ở trường hợp này, cũng có sự ghi chú giống như trường hợp trên nhưng có đường dẫn đến trang web chứa các điều khoản tiêu chuẩn của công ty. Cách thức này được phần lớn người bán trực tiếp sử dụng.

Nhược điểm của phương pháp này là chưa chắc khách hàng đã vào trang web để đọc các điều khoản chủ yếu nói trên.

- Hiển thị điều khoản ở cuối trang web:

Theo cách hiển thị này, thay vì đường dẫn tới một trang web khác thì người bán trực tuyến để toàn bộ điều khoản ở cuối trang. Khách hàng muốn xem hết trang web thì buộc phải thực hiện thao tác cuộn trang và buộc phải đi qua các điều khoản. Tất nhiên, việc đọc hay không tuỳ thuộc vào chính bản thân khách hàng nhưng nó cũng thể hiện rõ thiện chí của người bán trong việc muốn cung cấp, chuyển tải nội dung hợp đồng đến tay khách hàng.

- Hiển thị điều khoản ở dạng hộp thoại (Dialogue Box):

Khách hàng muốn tham gia giao kết hợp đồng phải kéo chuột qua tất cả các điều khoản ở cuối trang rồi mới tới được hộp thoại "tôi đồng ý" hoặc "tôi đã xem các điều khoản hợp đồng". Khi click chuột vào hộp thoại này thì coi như hợp đồng đã được giao kết. Phương pháp này khắc phục những nhược điểm của hai phương pháp trên ở chỗ: khi khách hàng click chuột vào hộp thoại có nội dung như trên, họ sẽ tự có nhu cầu và phải đọc những điều khoản mà họ đồng ý ràng buộc bản thân. Tuy nhiên, cách thể hiện nội dung này không phải là không có nhược điểm. Nhược điểm đó là người truy cập sẽ cảm thấy nản khi phải đọc những điều khoản dài ở cuối trang. Họ có thể bỏ cuộc giữa chừng, đặc biệt là khi mua bán những mặt hàng hoặc dịch vụ có giá trị thấp.

1.6.5.2. Những điều khoản liên quan đến các điều kiện mà hai bên đã đưa vào hợp đồng điện tử

Bên cạnh những nội dung được diễn đạt rõ ràng trên web, các bên giao kết hợp đồng điện tử còn bị ràng buộc bởi những điều khoản ngầm định tức là những điều khoản không có trong hợp đồng điện tử nhưng mặc nhiên được pháp luật và thực tiễn thừa nhận. Ví dụ như hàng hoá phải thuộc quyền sở hữu hợp pháp của người bán; hàng hoá phải là là hàng hoá không trong tình trạng bị tranh chấp; hoặc hàng hoá phải có chất lượng phù hợp với mục đích sử dụng v.v…Tuỳ theo từng loại hợp đồng điện tử là loại hợp đồng có tính dân sự hay tính thương mại mà những điều khoản này có thể được ngầm định trong hợp đồng. Đối với hợp đồng điện tử, các điều khoản liên quan đến hàng hoá, dịch vụ có thể sẽ được giao kết theo những điều khoản riêng. Ví dụ, đối với sản phẩm hay dịch vụ số hoá, người mua thông thường phải trả tiền xong rồi mới được tải sản phẩm. Trong trường hợp này, mặc nhiên ngầm hiểu rằng chương trình tải về phải phù hợp với mục đích sử dụng của nó và phải hoạt động được. Ngoài ra, chương trình còn phải được tải về trong một thời gian hợp lý, nếu không, người bán sẽ hoàn trả lại tiền cho người mua.

1.6.5.3. Một số điều khoản đặc biệt cần lưu ý khi giao kết hợp đồng điện tử

Trong hợp đồng điện tử, có một số điều khoản được coi là các điều khoản đặc biệt quan trọng liên quan tới tính hiệu lực của hợp đồng điện tử. Đó là:

- Điều khoản hình thành hợp đồng (Contract Formation Terms – còn gọi là điều kiện để hợp đồng điện tử có hiệu lực). Trong hợp đồng truyền thống, vấn đề khi nào hợp đồng có hiệu lực đã được quy định bởi rất nhiều quy tắc và thực tiễn thương mại, qua lịch sử phát triển của thương mại. Tuy nhiên, đối với lĩnh vực giao kết trực tuyến, vấn đề này trở nên phức tạp hơn. Thuyết tống phát hay thuyết tiếp thu có còn ý nghĩa nữa không? Chấp nhận chào hàng như thế nào sẽ có hiệu lực và hợp đồng hình thành? Đối với hợp đồng điện tử, một điều dễ nhận thấy là người soạn sẵn hợp đồng luôn muốn dành cho mình nhiều lợi thế.

Do đó, họ luôn quy định sẵn thời điểm phát sinh hiệu lực của hợp đồng bằng cách sử dụng điều khoản hình thành hợp đồng . Điều khoản hình thành hợp đồng thường được quy định như sau:

Hình thành hợp đồng

Các giao dịch của công ty hiện chỉ là các chào hàng tự do. Giá cả và hàng hoá có thể thay đổi. Các Quý khách hàng đồng ý không thay đổi những điều khoản và những điều kiện đã được công ty quy định ở mẫu này. Thoả thuận này chỉ là lời chào hàng từ phía Quý khách hàng mà không ràng buộc cho công ty cho đến khi công ty gửi thư điện tử chấp nhận và quý khách hàng đã nhận được thư điện tử đó. Công ty bảo lưu quyền từ chối lời chào hàng của Quý khách hàng vì bất kỳ lý do gì.

Một điều khoản được soạn sẵn như vậy rõ ràng nhằm bảo vệ quyền lợi của người bán trực tuyến. Vì người mua, khi giao kết hợp đồng điện tử kiểu như thế này sẽ phải đọc kỹ để hiểu rằng nếu mình click vào hộp thoại thì người mua đã tự ràng buộc mình với những điều kiện mà người bán đưa ra và sẽ khó thay đổi theo ý mình. Trong trường hợp này, rõ ràng thuyết tống phát hay tiếp thu sẽ không còn có ý nghĩa nữa.

- Điều khoản miễn, giảm trách nhiệm (Linitation and Exclusion of Liability): Người bán trực tuyến luôn sử dụng loại điều khoản này để chối bỏ hoặc cố ý giảm thiểu trách nhiệm của mình càng nhiều càng tốt.

- Điều khoản thanh toán và giao hàng (Payment and Delivery terms): Trong các hợp đồng điện tử, điều khoản này được quy định rất chi tiết. Phương thức thanh toán chủ yếu là phương thức điện tử, theo đó người mua cung cấp số thẻ tín dụng cho người bán. Phần lớn rủi ro thuộc về người mua. Việc thanh toán chỉ coi như hoàn tất khi người bán nhận được tiền chứ không phải vào thời điểm người mua nhập số thẻ tín dụng. Ngoại trừ những công ty làm ăn chân chính, các công ty "ma" thường xuyên phủ nhận việc tiền đã đến tay họ.

Tuy nhiên, trong thực tiễn giải quyết tranh chấp phát sinh từ giao kết và thực hiện hợp đồng điện tử, để bảo vệ người mua trực tuyến, một số ít toà án cho rằng, nếu người bán mô tả quy trình thanh toán và người mua đã thực hiện đúng chỉ dẫn đó thì coi như người mua đã hoàn thành nghĩa vụ thanh toán của mình.

1.6.5.4. Vấn đề về lỗi kỹ thuật trong nội dung hợp đồng điện tử

Khi giao kết hợp đồng điện tử qua trang web, người mua dường như phải tự mình làm mọi việc, tự chọn hàng, số lượng, phương thức thanh toán đến việc giao hàng v.v.v nên dễ phạm phải các lỗi về thao tác kỹ thuật. Những lỗi này mang tính khách quan, thể hiện sự không thống nhất giữa thao tác bên ngoài với ý chí bên trong của người mua, do bị ảnh hưởng bởi yếu tố kỹ thuật của công nghệ tin học. Trong trường hợp này, không thể ràng buộc người mua vì các lỗi kỹ thuật đó. Trong thực tiễn, một số nước cho phép người mua không bị ràng buộc bởi hiệu lực của hợp đồng bằng cách thông báo ngay cho người bán về lỗi kỹ thuật này. Tuy nhiên, trường hợp này hiếm khi được toà án chấp nhận vì theo quan điểm của toà án, người bán được coi là phải có sự thuần phục, nhuần nhuyễn trong kỹ thuật mua bán trực tuyến.

Chương 2. MỘT SỐ TÌNH HUỐNG TRONG THỎA THUẬN HỢP ĐỒNG ĐIỆN TỬ

2.1. MỘT SỐ RỦI RO TRONG THỎA THUẬN HỢP ĐỒNG ĐIỆN TỬ

Khi áp dụng một phương thức hiện đại như các phương tiện điện tử trong giao kết hợp đồng thì các bên cạnh các tiện ích mà giao kết hợp đồng điện tử mang lại, các bên phải đối mặt với một số rủi ro nhất định, cả về mặt kỹ thuật, về mặt thương mại cũng như về mặt pháp lý.

Khái niệm rủi ro trong giao kết hợp đồng điện tử

Rủi ro trong giao kết hợp đồng điện tử là những tổn thất, mất mát xảy ra trong quá trình thực hiện các giao dịch điện tử của những người sử dụng, nó có tác động xấu đến sự tồn tại và phát triển của doanh nghiệp, cũng như lợi ích của người sử dụng.

2.1.1. Rủi ro từ vấn đề pháp lý

Rủi ro liên quan đến vấn đề pháp lý thường đưa đến tranh chấp kiện tụng kéo dài có thể ảnh hưởng đến hoạt động kinh doanh của doanh nghiệp. Rủi ro pháp lý có nguồn gốc từ:

- Hệ thống pháp luật về hợp đồng điện tử chưa đầy đủ. Các quy định hướng dẫn giao kết hợp đồng điện tử chưa rõ ràng.

- Sự thiếu kiến thức về pháp lý của các chủ thể tham gia giao kết hợp đồng điện tử

- Sự thiếu chặt chẽ trong những hợp đồng được ký kết theo phương thức TMĐT

- Có sự vi phạm luật quốc gia như luật chống độc quyền, chống phân biệt chủng tộc

- Để phòng tránh được những rủi ro liên quan đến vấn đề pháp lý doanh nghiệp cần chủ động có cố vấn về luật pháp có đủ năng lực để đảm bảo các hoạt động của doanh nghiệp là hợp pháp cũng như có thể giải quyết các vấn đề pháp lý khi xảy ra.

2.1.2. Rủi ro về thiếu thông tin

Sự bùng nổ thông tin hiện nay với sự hỗ trợ của mạng Internet đã góp phần không nhỏ vào sự thành công của các doanh nghiệp ứng dụng TMĐT nhưng cũng là sự mở đầu cho những thất bại của những doanh nghiệp chậm đổi mới và thiếu thông tin trong kinh doanh. Rủi ro về thông tin thể hiện như sau:

- Thiếu thông tin về phía đối tác dẫn đến bị phía đối tác lừa không thanh toán hoặc không thực hiện hợp đồng.

- Thiếu thông tin về sự thay đổi giá cả của sản phẩm trên thị trường

- Thiếu thông tin hoặc thông tin bất đối xứng về những thay đổi công nghệ sản xuất sản phẩm trên thị trường.

- Thiếu hiểu biết về thị trường mục tiêu mà doanh nghiệp thâm nhập.

Để khắc phục được rủi ro về mặt thông tin điều quan trọng là doanh nghiệp, người sử dụng phải điều tra các khách hàng tiềm năng, thẩm định năng lực tài chính của các đối tác để đảm bảo họ có đủ khả năng thanh toán và thực hiện đơn hàng cũng như không có yếu tố lừa đảo.

Ngoài ra, TMĐT và các giao dịch điện tử qua mạng đang ngày càng trở thành nhu cầu cấp thiết. Các thông tin được truyền đi trong TMĐT và các giao dịch đều là những thông tin rất quan trọng như đơn đặt hàng, số tài khoản, thông tin về sản phẩm, khuyến mại, giảm giá, hợp đồng và các điều khoản giao dịch…Tuy nhiên, với các thủ đoạn tinh vi, nguy cơ bị ăn cắp thông tin qua mạng ngày càng gia tăng. Hiện nay, giao dịch qua Internet chủ yếu sử dụng phương thức TCP/IP. Đây là giao thức cho phép các thông tin được gửi từ máy tính này tới máy tính khác qua một loạt các máy trung gian hoặc mạng riêng biệt. Chính điều này đã tạo cơ hội cho những kẻ trộm công nghệ cao và các hacker có thể thực hiện các hoạt động phi pháp. Các thông tin được truyền trên mạng đều có thể gặp một số rủi ro sau:

- Bị nghe trộm, xem trộm: thông tin vẫn không bị thay đổi nhưng tính bí mật của nó không còn.

- Bị giả mạo (Tampering): Các thông tin trong khi truyền đi bị thay đổi hoặc thay thế khi đến tay người nhận.

- Bị mạo danh: (Impersonation): Thông tin được gửi tới cá nhân mạo nhận là người nhận hợp pháp theo 2 hình thức. Hình thức thứ nhất là bắt chước, tức là một cá nhân có thể giả vờ như người khác bằng cách sử dụng địa chỉ email của một người khác hoặc giả mạo một tên miền của một trang web. Hình thức thứ 2 là xuyên tạc, tức là một cá nhân hay một tổ chức có thể đưa những thông tin không đúng sự thật về họ như một trang web mạo nhận ăn cắp tín dụng và không bao giờ gửi hàng cho khách hàng

2.1.3. Rủi ro từ khía cạnh kỹ thuật và an ninh mạng

Trong lĩnh vực này, có 3 bộ phận rất dễ bị tấn công và tổn thương khi thực hiện các giao dịch TMĐT đó là: Hệ thống khách hàng, máy chủ của doanh nghiệp và đường dẫn thông tin. Có bẩy dạng rủi ro nguy hiểm nhất đối với an ninh của các website và các giao dịch giao kết hợp đồng điện tử.

- Các đoạn mã nguy hiểm: Bao gồm nhiều mối đe dọa mang tính rủi ro khác nhau như virus, worm. Đây là các chương trình máy tính có khả năng nhân bản hoặc tự tạo các bản sao của chính mình và lây lan ra các chương trình, các tệp dữ liệu khác trên máy tính.

- Tin tặc và các chương trình phá hoại: Tin tặc là thuật ngữ chỉ những người truy cập trái phép vào một website hay một hệ thống máy tính. Lợi dụng các điểm yếu (hay còn gọi là các lỗ hổng) trong hệ thống bảo vệ của website và lợi dụng ưu điểm của internet là một hệ thống mở để tấn công nhằm phá hỏng những hệ thống bảo vệ của website hay hệ thống máy tính của một tổ chức.

- Gian lận thẻ tín dụng: trong thương mại truyền thống, gian lận thẻ tín dụng có thể xảy ra trong trường hợp thẻ tín dụng bị mất, bị đánh cắp, các thông tin về số thẻ, mã PIN, các thông tin về khách hàng bị tiết lộ và sử dụng bất hợp pháp, hoặc trong trường hợp xảy ra các rủi ro khác. Trong TMĐT, các hành vi gian lận xảy ra đa dạng và phức tạp hơn. Nếu như trong thương mại truyền thống, việc mất thẻ hoặc bị đánh cắp thẻ là mối đe dọa lớn nhất đối với khách hàng, thì trong TMĐT mối đe dọa lớn nhất là việc mất các thông tin liên quan đến thẻ hoặc các thông tin liên quan đến giao dịch sử dụng thẻ trong quá trình diễn ra giao dịch. Các tệp dữ liệu thẻ tín dụng của khách hàng thường là những mục tiêu hấp dẫn đối với các tin tặc khi tấn công các website TMĐT để lấy cắp các thông tin cá nhân của khách hàng như tên, địa chỉ, số điện thoại…để mạo danh khách hàng lập các khoản tín dụng mới nhằm phục vụ những mục tiêu khác.

Một sự lo ngại khác của người bán là sự phủ định đối với các đơn hàng quốc tế. Trong trường hợp một khách hàng quốc tế đặt hàng và sau đó từ chối hành động này, người bán trực tuyến thường không xác định rằng thực chất hàng hóa đã được giao đến tay khách hàng hay chưa và chủ thẻ tín dụng có thực sự là người đã thực hiện đơn đặt hàng hay không?

- Sự lừa đảo: lừa đảo trong TMĐT là việc tin tặc sử dụng các địa chỉ thư điện tử giả hoặc mạo danh một người nào đó thực hiện những hành động phi pháp. Sự lừa đảo cũng có thể liên quan đến sự thay đổi hoặc làm chệch hướng các liên kết web đến một địa chỉ khác với các địa chỉ thực hoặc tới một website giả mạo website thực cần liên kết.

- Sự khước từ dịch vụ: Đây là hậu quả của việc các hacker sử dụng những biện pháp khác nhau để làm tràn ngập hoặc dẫn tới tắc nghẽn mạng truyền thông hoặc sử dụng số lượng lớn máy tính tấn công vào một mạng (dưới dạng các yêu cầu phân bố dịch vụ) từ nhiều điểm khác nhau gây nên sự quá tải về khả năng cung cấp dịch vụ, mạng máy tính ngừng hoạt động và người sử dụng không thể truy cập được vào website đó. Qua đó làm giảm doanh số hoạt động của các website, giảm uy tín và tiếng tăm của doanh nghiệp.

- Kẻ trộm trên mạng: Đây là một dạng của chương trình nghe trộm, giám sát sự di chuyển của thông tin trên mạng. Khi sử dụng các mục đích hợp pháp, nó có thể giúp phát hiện các lỗ hổng trên mạng. Ngược lại, nếu sử dụng vào các mục đích phạm tội, nó sẽ trở thành những mối nguy hiểm rất lớn và khó có thể phát hiện.

- Xem lén thư điện tử: bằng cách sử dụng các đoạn mã ẩn bí mật gắn vào một thông điệp thư điện tử, cho phép người xem lén có thể giám sát toàn bộ các thông điệp chuyển tiếp được gửi cùng với thông điệp ban đầu.

Những rủi ro trên làm ảnh hưởng đến tính bảo mật thông tin của các bên giao kết hợp đồng, nó nảy sinh rủi ro như việc đánh cắp thông tin cá nhân, giả mạo là người mua hàng gây tổn thất cho người bán, hay lừa đảo lấy thông tin thẻ tín dụng…Tất cả những biểu hiện của rủi ro này gây tổn thất xấu đến hoạt động giao kết và thực hiện hợp đồng điện tử.

2.1.4. Rủi ro từ phía sử dụng người dùng

2.1.4.1. Rủi ro từ phía người mua do các yếu tố khách quan của môi trường thương mại điện tử mang lại

- Người mua không thể chắc chắn được rằng website do một công ty hợp pháp quản lý và sở hữu.

- Người mua không thể chắc chắn được rằng trang web không chứa đựng các đoạn mã nguy hiểm hoặc các nội dung không lành mạnh.

- Người mua không thể chắc chắn được rằng web server sẽ không cung cấp các thông tin của người sử dụng cho một người khác, cho một tổ chức khác. Điều này tương đương với thông tin của người sử dụng có thể bị đánh cắp, đây cũng là mối đe dọa rất lớn đối với khách hàng.

2.1.4.2. Rủi ro từ phía doanh nghiệp do các yếu tố khách quan của môi trường thương mại điện tử mang lại.

- Doanh nghiệp sẽ không thể chắc chắn được rằng người sử dụng không xâm nhập vào trang web để thay đổi các trang và nội dung trên các trang của website.

- Doanh nghiệp sẽ không thể chắc chắn được rằng người sử dụng sẽ không phá hoại website để những người khác không thể sử dụng được.

2.1.4.3. Rủi ro từ cả phía doanh nghiệp và người sử dụng

Rủi ro khách quan từ môi trường thương mại điện tử:

- Doanh nghiệp và người tiêu dùng không thể biết chắc được rằng đường truyền sẽ không bị một bên thứ ba theo dõi.

- Doanh nghiệp và người tiêu dùng sẽ không thể biết chắc được rằng thông tin được truyền giữa hai bên sẽ không bị thay đổi.

Rủi ro chủ quan từ phía người bán/người mua cố tình vi phạm

- Khách hàng thanh toán nhưng người bán không giao hàng.

- Khách hàng thanh toán nhưng người bán giao hàng lỗi hoặc kém phẩm chất hoặc hàng bị đổ vỡ hỏng hóc.

- Khách hàng thanh toán nhưng tiền không đến được tay người bán hàng.

- Người bán chuyển hàng nhưng người kinh doanh từ chối nhận hàng.

- Người bán giao hàng nhưng người mua không thanh toán…

2.2. MỘT SỐ BÀI TOÁN TRONG THỎA THUẬN HỢP ĐỒNG ĐIỆN TỬ VÀ CÁCH GIẢI QUYẾT

2.2.1. Khái niệm:

Thỏa thuận hợp đồng thương mại điện tử gồm hai bước: Đàm phán hợp đồng và ký kết hợp đồng. Đàm phán hợp đồng là thực hiện một hoặc nhiều cuộc đối thoại, thương lượng giữa hai bên hoặc nhiều bên có ý muốn quan hệ đối tác với nhau, nhằm tiến đến một thỏa thuận chung, đáp ứng yêu cầu cá nhân hoặc yêu cầu hợp tác kinh doanh của các bên tham gia đàm phán.

Ký kết hợp đồng là xác nhận các nội dung đã đàm phán thỏa thuận ở trên, từ đó bản hợp đồng có hiệu lực.

Với internet việc thỏa thuận hợp đồng giảm được nhiều thời gian trao đổi giữa doanh nghiệp với doanh nghiệp đối tác cũng như các khách hàng của họ. Cũng giống như thỏa thuận hợp đồng thương mại truyền thống các vấn đề đàm phán, thỏa thuận, ký kết đều phải tuân theo luật thương mại.

Ngoài những vấn để này sinh như trong thỏa thuận hợp đồng thông thường, thỏa thuận hợp đồng trực tuyến còn có những vấn đề khác như những vấn đề an toàn thông tin trong giao dịch: xác minh nguồn gốc giao dịch, đảm bảo bí mật, toàn vẹn thông tin thỏa thuận ký kết hợp đồng, chống chối bỏ giao dịch.

2.2.2. Vấn đề bảo toàn thông tin hợp đồng trực tuyến

Bài toán:

Trong thỏa thuận hợp đồng trực tuyến giữa A và B về đặt mua và cung cấp một loại mặt hàng hay dịch vụ nào đó, giả sử A là người soạn hợp đồng và gửi đến B xem xét và thỏa thuận, nếu B đồng ý với các điều khoản của hợp đồng thì B sẽ ký lên hợp đồng đó. Vấn đề đặt ra là liệu có kẻ thứ ba trái phép nào đó đã chặn xem và sửa bản hợp đồng đó, nội dung bản hợp đồng B nhận được có đúng với nội dung mà A đã soạn thảo?

Khi B nhận đươc bản hợp đồng từ A, giả sử trên đường truyền bản hợp đồng không bị sửa đổi, B đồng ý với các điều khoản trong hợp đồng và B chấp nhận hợp đồng, hay nếu B không đồng ý với tất cả các điều khoản, B bổ sung vào một số điều khoản để thỏa thuận lại và gửi lại cho A. Trong qua trình bản hợp đồng mà B ký gửi về A, liệu bản hợp đồng đó có đúng như bản hợp đồng mà B đã gửi hay đã bị sửa đổi - bị xâm phạm tính toàn vẹn trong bản hợp đồng này.

Giải pháp kỹ thuật:

Để đảm bảo tính toàn vẹn của bản hợp đồng trực tuyến trong khi chúng được truyền đi trên mạng trước hết ta cần một kênh truyền an toàn, với các Phương pháp đảm bảo tính toàn vẹn trong giao dịch nói chung, một kỹ thuật đặc trưng quan trọng để đảm bảo tính toàn vẹn hợp đồng giao dịch là dùng chữ ký điện tử và chứng chỉ điện tử.

Khi nội dung của bản hợp đồng thay đổi, thì chữ ký trên bản hợp đồng đó cũng phải thay đổi theo. Chữ ký điện tử nhằm đảm bảo tính toàn vẹn, duy nhất và không bị sửa đổi dữ liệu gốc bởi người khác. Chữ ký là bằng chứng xác thực người gửi chính là tác giả của thông điệp mà không phải của một ai khác. Không những thế, khi chữ ký điện tử được gắn với thông điệp điện tử thì đảm bảo rằng thông tin trên đường chuyền đi sẽ không bị thay đổi. Mọi sự thay đổi dù nhỏ nhất sẽ đều bị phát hiện dễ dàng.

2.2.3. Vấn đề xác thực thông tin hợp đồng trực tuyến

Bài toán:

Xác thực là một thủ tục nhằm kiểm tra các thông báo nhận được, xem chúng có đến từ một nguồn hợp lệ và có bị sửa đổi hay không. Xác thực thông báo cũng có thể kiểm tra tính trình tự và tính đúng lúc. Chữ ký số là một kỹ thuật xác thực. Nó cũng bao gồm nhiều biện pháp để chống lại việc chối bỏ đã gửi hay đã nhận thông báo của hai bên gửi và nhận.

Khi nhận được đơn đặt hàng hay giao dịch nào đó, chủ doanh nghiệp phải biết rõ thông tin đó có phải đã đến từ một nguồn đáng tin cậy hay không? Khách hàng cũng như doanh nghiệp cần phải biết chính xác rằng họ đang giao dịch với ai và đối tác giao dịch của họ có đáng tin cậy không, có an toàn không?

Đôi khi khách hàng, hay các nhà giao dịch không biết được mình đang giao dịch với ai. Rất nhiều công ty ma, các địa chỉ ảo hay các website giả mạo website của doanh nghiệp để lừa gạt khách hàng, gây thiệt hại không nhỏ cho khách hàng giao dịch, hay các doanh nghiệp tham gia TMĐT . . .

Xác thực thông báo sẽ bảo vệ hai thành viên (trao đổi thông báo qua thành viên thứ ba). Tuy nhiên hai thành viên không bảo vệ lẫn nhau. Giả thiết, A đã gửi một xác thực thông báo cho B. Có thể xảy ra tranh chấp giữa hai thành viên như sau:

B có thể làm giả một thông báo khác và tuyên bố rằng thông báo này có nguồn gốc tử A. B có thể tạo một thông báo và gắn mã xác thực bằng khóa chung của họ.

A có thể chối bỏ đã gửi thông báo. Vì B có thể làm giả thông báo và vì vậy không có cách nào có thể chứng minh A đã gửi thông báo.

Giải pháp kỹ thuật:

Các tranh chấp có thể xảy ra giữa người gửi và người nhận không có sự tin tưởng. có nhiều giải pháp cho vấn đề xác thực như hàm băm, chữ ký số, chứng chỉ điện tử . . . Giải pháp thường dùng là chữ ký số. Chữ ký số, tương tự như chữ ký bằng tay, nó phải có một số tính chất sau:

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

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

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

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

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

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

- Tạo ra chữ ký số dễ dàng.

- Dễ nhận ra và dễ kiểm tra chữ ký.

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

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

2.2.4. Vấn đề chống chối bỏ hợp đồng trực tuyến

Bài toán:

Với hợp đồng thông thường, đối tác hai bên biết mặt nhau, cùng nhau trực tiếp ký kết hợp đồng với sự chứng kiến của nhiều người với luật giao dịch rõ ràng. Hợp đồng TMĐT được thực hiện trong môi trường internet . . . các bên tham gia ký kết hợp đồng xa nhau về mặt địa lý, thậm chí họ có thể không biết mặt nhau, thì vấn đề chối bỏ hợp đồng có thể xảy ra rất cao, mặt khác luật pháp cho TMĐT chưa đủ, gây ra thiệt hại lớn cho các bên tham gia ký kết hợp đồng.

Ví dụ ông A muốn đặt mua một mặt hàng của công ty B ở nước ngoài. Sau khi thỏa thuận ký kết hợp đồng, ông ty B chuyển hàng đến cho ông A (kèm theo đó là chi phí vận chuyển và thuế hải quan). Khi sản phẩm đến, ông A thay đổi ý kiến, không muốn mua nữa, và ông A đã chối bỏ những gì mình đã thỏa thuận (không có bên thứ ba nào xác nhận thỏa thuận hợp đồng mua hàng giữa ông A và công ty B). Việc này gây thiệt hại cho công ty B.

Trường hợp công ty B mang đến cho ông A, nhưng mặt hàng không đúng như trong thỏa thuận, mà công ty B cứ một mực khẳng định rằng ông A đã đặt mua sản phẩm này. Điều này gây thiệt hại cho ông A.

Như vậy, chối bỏ thỏa thuận hợp đồng gây thiệt hại cho đối tượng tham gia TMĐT. Chống chối bỏ giao dịch là bài toán quan trọng trong quá trình thỏa thuận hợp đồng trong TMĐT.

Giải pháp kỹ thuật:

Để chống chối bỏ hợp đồng giao dịch TMĐT trước hết cần có một hành lang pháp lý cho giao dịch TMĐT. Về mặt kỹ thuật, giải pháp thông dụng để đảm bảo chối bỏ thỏa thuận hợp đồng TMĐT, đó là chữ ký số và chứng thực điện tử. Ví dụ chữ ký không thể phủ nhận được, đó là chữ ký có thể xác minh chứng thực rằng A có tham gia một giao dịch điện tử nào hay không, chữ ký trên văn bản giao dịch có đúng đích thực của A hay không, nếu đó là chữ ký của A mà A chối bỏ, sẽ có giao thức chứng minh, buộc A không thể chối bỏ giao dịch hợp đồng đã thỏa thuận.

Chương 3. TÌM HIỂU CHỮ KÝ KHÔNG THỂ CHỐI BỎ

3.1. GIỚI THIỆU

Chữ ký không thể chối bỏ được công bố bởi Chaum và Van Antverpen vào năm 1989. Nó có một nét riêng mới lạ và thú vị. Quan trọng nhất trong số đó là chữ ký không thể kiểm tra khi không có sự tác động của người ký, A (giả sử A là người ký).

Sự bảo vệ này của A để đề phòng khả năng chữ ký trong tài liệu của mình bị sao chép và phân phối bởi thiết bị điện tử mà không có sự đồng ý của mình.

Ví dụ: A có một phần mềm và chữ ký kèm theo được tạo ra nhờ thuật toán của chữ ký số thông thường. Như vậy, sẽ không tránh khỏi trường hợp phần mềm đó bị sao chép trái phép mà A không biết. Người mua sẽ kiểm tra chữ ký kèm theo nhờ thuật toán kiểm tra công khai Ver và công nhận chữ ký đó là đúng. Vì như chúng ta đã biết bản sao của chữ ký số đồng nhất với bản gốc. Đương nhiên như vậy A sẽ bị mất bản quyền. Để tránh điều bất tiện đó A đã dùng chữ ký không thể chối bỏ. Sự kiểm tra sẽ thành công khi thực hiện giao thức hỏi – đáp.

Lược đồ chữ ký không thể chối bỏ gồm ba phần: thuật toán ký, giao thức kiểm tra, giao thức chối bỏ.

3.2 . SƠ ĐỒ CHỮ KÝ

Một chủ thể A chọn một số nguyên tố dạng Sophie German p = 2q+1, trong đó q cũng là một số nguyên tố, chọn $\alpha \in Z_p^*$ là một phần tử cấp q. Gọi G là nhóm con (theo phép nhân) cấp q sinh ra bởi α của Z_p^*. Sơ đồ chứ ký Chaum – Van Antverpen của A gồm có: P = A = G, cặp khóa K = (K', K'') gồm một khóa bí mật K' = a, và một khóa công khai K'' = (p, α, a, β) trong đó α là một số nguyên dương < p -1 và $\beta = \alpha^a \bmod p$.

Thuật toán ký: A ký trên văn bản $x \in P = Q$ với chữ ký:

$y = Sign_{K'}(x) = x^a \bmod p$.

Giao thức kiểm thử (xác thực)

Định nghĩa: Với văn bản x và chữ ký y người nhận B cùng người ký A thực hiện giao thức kiểm thử sau:

1. B chọn ngẫu nhiên hai số e1, e2 $\in Z_p^*$, tính $c = y^{e1} * \beta^{e2} \bmod p$ và gửi c cho A.
2. A tính $d = c^{a^{-1} \bmod q} \bmod p$ và gửi d cho B.
3. B chấp nhận y là chữ ký của A trên x nếu $d \equiv x^{e1} * \alpha^{e2} \bmod p$.

Ta chứng minh hai định lý sau đây để chứng tỏ tính hợp thức của giao thức kiểm thử và chối bỏ của sơ đồ ký Chaum – Van Antverpren.

Định lý: a) Nếu y đúng là chữ ký của A trên x tức là $y = x^a \bmod p$, thì việc B chấp nhận y là chữ ký của A trên x theo giao thức kiểm thử đúng.

b) Nếu $y \neq x^a \bmod p$, tức là y không phải là chữ ký của A trên x, thì việc B theo giao thức kiểm thử, chấp nhận y là chữ ký của A trên x, có thể xảy ra với xác suất 1/q.

Chứng minh: a) Giả sử $y = x^a \bmod p$ khi đó $y^{a-1} = x \bmod p$ (chú ý rằng tất cả các số mũ đều được tính theo mod q). Ta cũng có:

$\beta^{a-1} = \alpha \pmod p$. Do đó, $D = c^{a-1} = y^{e1\ a-1} * \beta^{e2\ a-1} = x^{e1}\ \alpha^{e2} \bmod p$.

Và theo giao thức kiểm thử, B chấp nhận y là chữ ký của A trên x, việc chấp nhận đó là đúng.

b) Bây giờ ta giả sử $y \neq x^a \bmod p$. Trước hết ta chú ý rằng mỗi lời mời hỏi c tương đương với đúng q cặp (e1, e2), vì y và β là các phần tử của nhóm G cấp q. Khi A nhận được câu hỏi c, A không có cách gì để biết B dùng cặp (e1, e2) nào trong q cặp có thể. Ta chứng minh rằng, do $y \neq x^a \bmod p$, nên trong q cặp chỉ có đúng một cặp thỏa mãn đồng dư thức $d = x^{e1}\ \alpha^{e2} \bmod p$.

Thực vậy, ta có thể đặt $c = \alpha^{i,}$ $d = \alpha^j$, $x = \alpha^k$, $y = \alpha^l$, với i, j, k ,l $\in Z_p^*$, vì α là phần tử sinh của G, và hai đồng dư thức $c = y^{e1}\ \beta^{e2} \bmod p$ và $d = x^{e1}\ \alpha^{e2} \bmod p$ tương đương với hai phương trình:

$$i = (le1 + ae2) \pmod q.$$

$$j = (ke1 + e2) \pmod q.$$

Từ giả thiết $y \neq x^a \bmod p \rightarrow l - ak \# 0 \bmod q$, tức là định thức của phương trình trên với ẩn số e1, e2 là $\neq 0 \bmod q$.

Như vậy, mỗi $d \in G$ là câu trả lời đúng (theo giao thức kiểm thử) chỉ có một cặp (e1, e2) trong q cặp có thể. Vì vậy, nếu $y \neq x^a \bmod p$ thì xác suất để B chấp nhận y là chữ ký của A trên x theo giao thức kiểm thử là l/q. Định lý được chứng minh.

Giao thức chối bỏ:

Một vấn đề đặt ra, nếu sự cộng tác của chủ thể ký là cần thiết trong việc kiểm tra chữ ký thì điều gì đã ngăn cản người đó trong việc từ chối chữ ký do người đó tạo ra. Tất nhiên, người đó có thể cho rằng chữ ký đúng đó là giả mạo và từ chối kiểm tra nó hoặc người đó thực hiện một giao thức mà theo đó chữ ký sẽ không được kiểm tra. Vì vậy, một lược đồ chữ ký chống chối bỏ được kết hợp chặt chẽ với một giao thức chối bỏ và nhờ điều đó chủ thể ký có thể chứng minh được chữ ký đó là giả mạo. Nếu người đó từ chối thực hiện một phần trong giao thức chối bỏ, điều đố đồng nghĩa với dấu hiệu chứng minh chữ ký đó là của người đó và người đó đang cố gắng từ chối chữ ký của mình.

Định nghĩa:

1. B chọn ngẫu nhiên hai số $e_1, e_2 \in Z_{P*}$, tính $c = y^{e1} \beta^{e2} \mod p$ và gửi c cho A.
2. A tính $d = c^{a-1} \mod p$ và gửi d cho B.
3. B thử điều kiện $d \neq xe1. A^{e2} \mod p$.
4. B chọn tiếp hai số $f1, f2 \in Z_{P*}$ tính $C = y^{f1}\beta^{f2} \mod p$ và gửi C cho A.
5. A tính $D = C^{a-1} \mod q \mod p$ và gửi D cho B.
6. B thử điều kiện $D \neq x^{f1} \alpha^{f2} \mod p$.
7. B kết luận y là chữ ký giả mạo, nếu $(d \alpha^{-e2})^{f1} = (D \alpha^{-f2})^{e1} \mod p$

Định lý:

a) Nếu $y = x^a \bmod p$ và cả A và B đều tuân thủ giao thức chối bỏ thì

$(d\,\alpha^{-e2})^{f1} = (D\,\alpha^{-f2})^{e1} \bmod p$, tức là giao thức cho kết quả chính thức.

b) Nếu $y \# x^a \bmod p$. A và B đều tuân theo giao thức và có

$$D \neq x^{e1}.\, A^{e2} (\text{mod } p).$$

$$D \neq x^{f1}.\, A^{f2} (\text{mod } p).$$

Khi đó, đồng dư thức $(d\alpha^{-e2})^{f1} = (D\alpha^{-f2})^{e1} \bmod p$ đúng cới xác suất l/q, tức nếu y đúng là chữ ký của A trên x, thì theo giao thức B có thể kết luận rằng nó là giả mạo (một cách sai lầm) với xác suất l/q.

Chứng minh: a) Giả sử $y \neq x^a$ (mod p) và A, B cùng thức hiện giao thức chối bỏ. Do y không là chữ ký của A trền x lên B sữ kiểm thử đúng các bất đồng dư thức trên bước 3 và bước 6 của giao thức. Vì $\beta = \alpha^a \bmod p$, nên ta có:

$$(d\alpha^{-e2})^{f1} = ((y^{e1}\beta^{e2})^{\alpha-1} . \alpha^{-e2})^{f1} (\text{mod } p)$$

$$= y^{\alpha-1\, e1f1}\beta^{e2\, \alpha-1\, f1} . \alpha^{-e2f1} (\text{mod } p) = y^{e1\, \alpha-1f1} (\text{mod } p)$$

Tương tự, ta cũng có: $(D\alpha^{-f2})^{e1} = y^{e1\, \alpha-1f1} (\text{mod } p)$

Như vậy, đồng dư thức ở điểm 7 của giao thức được thử nghiệm đúng và kết luận y là chữ ký giả mạo của A trên x là chính xác, không thể bác bỏ.

b) Bây giờ giả thiết $y = x^a$ (mod p) và A, B cùng thức hiện giao thức chối bỏ. Đặt

$x_0 = d^{l/el}\, \alpha^{=e2/e1} \bmod p$, ta có:

$$x_0^{\,a} = d^{a/e1}\, \alpha^{-ae2/e1} \neq (x^{e1}\, \alpha^{e2})^{a/e1} . \alpha^{-ae2/e1} = x^a \bmod p$$

Theo điểm (b) trong định lý phần giao thức kiểm định, B có thể chấp nhận y là chữ ký của A trên x_0 tức là đồng dư thức:

D = x_0^{f1} .α^{f2} (mod p), với xác suất l/q. Nhưng đồng dư thức đó tương đương với đồng dư thức: (d α^{-e2})^{f1} = (D α^{-f2})^{e1} mod p, tức đồng dư thức này cũng có thể xảy ra với xác suất l/q. Định lý được chứng minh

Trong giao thức này, cặp (e1, e2) được dùng để tạo cặp khóa x_0 với $x_0^a \neq y$ mod p; Còn cặp (f1, f2) được dùng để kiểm thử xem y có là chữ ký của A trên x_0 hay không.

Ví dụ.

Chọn p = 467, q = 233 (p = 2q + 1), α = là phần tử sinh của một nhóm con G cấp 233 của Z^*_{467}. Chọn a = 101, khi đó ta có $\beta = \alpha^a$ mod p = 4^{101} mod 467 = 449.

A có cặp khóa K = (K', K'') với: K' = 101, K'' = (467, 4, 449).

Giả sử A trên văn bản x = 119 với chữ ký: y = 119^{101} mod 467 = 129.

1) B có thể dùng giao thức kiểm thử để biết y có đúng là chữ ký của A trên x hay không như sau: B chọn ngẫu nhiên e1 = 38, e2 = 397 và tính c.

c = 129^{38}. 449^{397} mod 467 = 13.

B gửi c = 13 cho A, A sẻ gửi trả lời lại là d = 9, B thử điều kiện: d = x^{e1}. α^{e2} mod p tức là: 9 = 119^{38}. 4^{397} mod 467

Đồng dư thức đó đúng, B chấp nhận 129 đúng là chữ ký của A trên văn bản 119.

2) Bây giờ ta thử thực hiện giao thức chối bỏ. Giả sử A gửi văn bản x = 286 với chữ ký y = 83. B chọn ngẫu nhiên e1 = 45, e2 = 237, rồi tính c = 129^{45} .449^{237} = 305 và gửi cho A; A trả lời d = 109. B thử điều kiện d $\neq$ x^{e1}. A^{e2} mod p, điều kiện đó được thỏa mãn vì 109 $\neq$ 149 = 286^{45} . 4^{237} mod 467. B lại tiếp tục phần sau của giao thức bằng cách chọn ngẫu nhiên f1 = 125, f2 = 9 và tính c = 129^{125} .449^9 mod 467 = 270, gửi cho A, A trả lời lại D = 68. B thử lại điều kiện D = x^{f1} .α^{f2} mod p, điều kiện này cũng được thỏa mãn vì

68 $\neq$ 25 = 286^{125} .4^9 mod 467.

Bây giờ B thử điều kiện cuối cùng của giao thức bằng cách tính:

$$(d\ \alpha^{-e2})^{f1} = (109.4^{-237})^{125} = 188 \pmod{467}.$$

$$(D\ \alpha^{-f2})^{e1} = (68.\ 4^{-9})^{45} = 188 \pmod{467}.$$

Hai giá trị trên bằng nhau, B có thể kết luận y không phải là chữ ký của A trên x với xác suất sai lầm là 1/233.

Thí dụ này được trình bày với mục đích minh họa, nên chỉ dùng các số nguyên tố p, q bé cho dễ tính. Trong thực tế ứng dụng, để đảm bảo tính an toàn, ta phải dùng số nguyên tố p, q rất lớn. Chẳng hạn, phải là các số có biểu diễn nhị phân cỡ 512 bit, khi đó ta có: $q \geq 2^{510}$ tức là $1/q \leq 2^{-510}$, một xác suất rất bé, có thể bỏ qua. Vì vậy, các yêu cầu đối với giao thức kiểm thử và giao thức chối bỏ như để cập ở trên có thể xem là thỏa mãn.

KẾT LUẬN

Đồ án tốt nghiệp thực hiện được các nội dung sau:

1/. Tìm hiểu về phương pháp bảo vệ thông tin.

2/. Tìm hiểu một số tình huống trong thỏa thuận hợp đồng điện tử và cách giải quyết.

3/. Tìm hiểu về chữ ký không thể chối bỏ.

DANH MỤC TÀI LIỆU THAM KHẢO

Tiếng Việt.

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

Tiếng Anh.

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