ĐẠI HỌC DÂN LẬP HẢI PHÒNG
KHOA CÔNG NGHỆ THÔNG TIN

NGUYỄN DANH TUẤN

VẤN ĐỀ QUẢN LÝ KHÓA MẬT MÃ VÀ ỨNG DỤNG TRONG THỎA THUẬN, KÝ KẾT HỢP ĐỒNG

ĐỒ ÁN TỐT NGHIỆP HỆ ĐẠI HỌC CHÍNH QUY
Ngành : Công nghệ thông tin

Hải Phòng, tháng 07 năm 2014

ĐẠI HỌC DÂN LẬP HẢI PHÒNG
KHOA CÔNG NGHỆ THÔNG TIN

VẤN ĐỀ QUẢN LÝ KHÓA MẬT MÃ VÀ ỨNG DỤNG TRONG THỎA THUẬN, KÝ KẾT HỢP ĐỒNG

ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC HỆ CHÍNH QUY
Ngành: Công nghệ thông tin

Sinh viên : Nguyễn Danh Tuấn
Mã số : 110964

Giáo viên hướng dẫn: PGS.TS.Trịnh Nhật Tiến

Hải Phòng, tháng 07 năm 2014

LỜI CẢM ƠN

Lời đầu tiên, em xin được gửi lời cảm ơn chân thành và sâu sắc nhất tới PGS.TS Trịnh Nhật Tiến – người Thầy luôn chỉ bảo, hướng dẫn hết sức nhiệt tình, giúp đỡ em trong suốt quá trình học tập và xây dựng khóa luận.

Em xin chân thành cảm ơn các Thầy, Cô giáo đã dạy dỗ em trong suốt quá trình học tập tại trường Đại học Dân Lập Hải Phòng. Những kiến thức các thầy cô truyền đạt sẽ mãi là hành trang để em vững bước trong tương lai.

Cuối cùng, con xin được gửi lời biết ơn sâu sắc nhất tới Bố mẹ và những người thân trong gia đình, những người luôn dành cho con tình yêu, niềm tin và động viên con trong suốt quá trình học tập.

Hải Phòng, tháng 7 năm 2014

Sinh viên

Nguyễn Danh Tuấn

BẢNG CÁC CHỮ VIẾT TẮT

Từ viết tắt	Ý nghĩa
CSDL	Cơ sở dữ liệu
DSA	Thuật toán ký số
DSS	Digital Signature Standard (Chuẩn chữ ký số)
RSA	Rivest, Shamir, & Adleman (Một công nghệ mã hóa khóa công khai)
SET	Secure Electronic Transaction
S-HTTP	Secure Hypertext Transfer Protocol
SHA	Secure Hash Algorithm (giải thuật băm an toàn)
SSL	Sercure Socket Layer
UNCITRAL	The United Nations Commission on International Trade Law (Ủy ban về luật thương mại của Liên Hợp Quốc)
TMĐT	Thương mại điện tử

BẢNG CÁC KÝ HIỆU TOÁN HỌC

Ký hiệu	Ý nghĩa
||	Nối chuỗi bit
N	Tập các số tự nhiên
$E_K(x)$	Phép mã hoá thông điệp x với khoá K
$D_K(x)$	Phép giải mã thông điệp x với khoá K
Sig(x)	Chữ ký trên thông điệp x
Ver(x, y)	Kiểm tra chữ ký y trên thông điệp x

THUẬT NGỮ VIẾT TẮT

Ký hiệu	Thuật ngữ	Giải thích
PKI	Public Key Infrastructure	Cơ sở hạ tầng khóa công khai
CA	Certificate Authority	Cơ quan chứng thực
RA	Registration Authority	Cơ quan đăng ký cấp chứng chỉ
RSA		Hệ mã hóa RSA
Elgamal		Hệ mã hóa Elgamal
ECC	Elliptic Curve Cryptography	Mã hóa đường cong Elliptic
DES	Data Encryption Standard	Chuẩn mã hóa dữ liệu
DSS	Digital Signature Standard	Chuẩn chữ ký điện tử
DSA	Digital Signature Algorithm	Thuật toán ký số
SHA	Security Hash Algorithm	Hàm băm
FIPS	Federal Information Processing Standards	Chuẩn xử lý thông tin Mỹ
X.509		Định dạng chứng chỉ số
SSL	Secure Socket Layer	Tầng socket an toàn
LDAP	Lightweight Directory Access Protocol	Giao thức truy cập thư mục
OCSP		
CRL	Certificate Revocation List	Danh sách thu hồi chứng chỉ
CDP	CRL Distributed Point	
DHCP	Dynamic Host Configuration Protocol	Giao thức cấp phát địa chỉ động
HTTP	HyperText Transfer Protocol	Giao thức truyền siêu văn bản
HTTPS	Secure HTTP	Giao thức HTTP có hỗ trợ SSL
ARP	Address Resolution Protocol	Giao thức phân giải địa chỉ
AARP	Authentication ARP	Giao thức ARP có xác thực
S-ARP	Secure ARP	Giao thức ARP an toàn
S/MIME	Secure Multipurpose Internet Mail Extensions	Giao thức truyền E-mail
IMAP	Internet Messaging Access Protocol	Giao thức truy cập thông điệp
POP	Post Office Protocol	Giao thức Mail
SMTP	Simple Mail Transfer Protocol	Giao thức truyền Mail
TLS	Transport Layer Security	
RFC	Request For Coments	
PID	Personal ID	
MAC	Machine Access Code	Địa chỉ MAC
AKD	Authoritive Key Distributor	Nhà phân phối khóa

MỤC LỤC

Chương 1. CÁC KHÁI NIỆM CƠ BẢN VỀ AN TOÀN THÔNG TIN

1. TỔNG QUAN VỀ BẢO VỆ THÔNG TIN

1.1. Vai trò của bảo vệ thông tin

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

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

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

+ Bảo vệ an toàn thông tin bằng các biện pháp thuật toán (phầm mềm)

Ba nhóm trên có thể được ứng dụng riêng rẽ hoặc phối kết hợp. Môi trường khó bảo vệ an toàn thông tin nhất và cũng là môi trường đối phương dễ xâm nhập nhất đó là môi trường mạng và quá trình truyền tin.

An toàn thông tin bao gồm các nội dung sau:

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

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

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

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

Để đảm bảo an toàn thông tin dữ liệu trên đường truyền tin và trên mạng máy tính có hiệu quả, thì điều trước tiên là phải lường trước hoặc dự đoán trước các khả năng không an toàn , khả năng xâm phạm, các sự cố rủi ro có thể xảy ra đối với thông tin dữ liệu được lưu trữ và trao đổi trên đường truyền tin và cũng như trên mạng.

Có hai loại hành xi xâm phạm thông tin dữ liệu đó là : vi phạm chủ động và vi phạm thụ động. Vi phạm thụ động chỉ nhằm mục đích cuối cùng là nắm bắt được thông tin (đánh cắp thông tin). Việc làm đó có khi không biết được nội dung cụ thể nhưng có thể dò ra được người gửi, người nhận nhờ thông tin điều khiển giao thức chứa trong phần đầu các gói tin. Kẻ xâm nhập có thể kiểm tra được sô lượng, độ dài và tần số trao đổi. Vì vậy vi phạm thụ động không làm sai lệch hoặc hủy hoại nội dung thông tin dữ liệu được trao đổi. Vi phạm thụ động thường khó phát hiện nhưng có thể có những biện pháp ngăn chặn hiệu quả. Vi phạm chủ động là dạng vi phạm có thể làm thay đổi nội dung, xóa bỏ, làm trễ, xắp xếp lại thứ tự hoặc làm lặp lại gói tin tại thời điểm đó hoặc sau đó một thời gian. Vi phạm chủ động có thể them vào một số thông tin ngoại lai để làm sai lệch nội dung thông tin trao đổi. Vi phạm chủ động dễ phát hiện nhưng để ngăn chặn hiệu quả thì khó khăn hơn nhiều.

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

1.1.2. Các Phương pháp bảo vệ thông tin

1.1.2.1. *Các chiến lược chính*

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

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

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

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

***Nút thắt (Choke Point)**

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

***Điểm nối yếu nhất (Weakest Link)**

Chiến lược này dựa trên nguyên tắc: " Một dây xích chỉ chắc tại mắt duy nhất, một bức tường chỉ cứng tại điểm yếu nhất" Kẻ phá hoại thường tìm những chỗ yếu nhất của hệ thống để tấn công, do dó ta cần phải gia cố các điểm yếu của hệ thống. Thông thường chúng ta chỉ quan tâm đến kẻ tấn công trên mạng hơn là kẻ tiếp cận hệ thống , do đó an toàn vật lý được coi là yếu điểm nhất trong hệ thống của chúng ta.

***Tính toàn cục**

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

***Tính đa dạng bảo vệ**

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

1.1.2.2. *Các mức bảo vệ trên mạng*

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

***Quyền truy nhập**

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

***Đăng ký tên/mật khẩu**

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

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

***Mã hóa dữ liệu**

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

***Bảo vệ vật lý**

Ngăn cản các truy nhập vật lý vào hệ thống. Thường dùng các biện pháp truyền thống như ngăn cấm tuyệt đối người không phận sự vào phòng đặt máy mạng, dùng ổ khóa trên máy tính hoặc các trạm không có ổ lưu trữ ngoài như CD-ROM, USB disk…

***Tường lửa**

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

***Quản trị mạng**

Trong thời đại phát triển của công nghệ thông tin, mạng máy tính quyết định toàn bộ hoạt động của một cơ quan, hay một công ty xí nghiệp. Vì vậy việc bảo đảm cho hệ thống mạng máy tính hoạt động một cách an toàn, không xảy ra các sự cố là một công việc cấp thiết hàng đầu.

Mức độ bảo vệ

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

1.1.2.3 *An toàn thông tin bằng mật mã*

Mật mã là một ngành khoa học chuyên nghiên cứu các phương pháp truyền tin bí mật. Mật mã bao gồm: lập mã và phá mã. Lập mã bao gồm hai quá trình: mã hóa và giải mã.

Để bảo vệ thông tin trên đường truyền người ta thường biến đổi nó từ dạng nhận thức được sang dạng không nhận thức được trước khi truyền đi trên mạng, quá trình này được gọi là mã hóa thông tin (encryption), ở trạm nhận phải thực hiện quá trình ngược lại, tưc là biến đổi thông tin từ dạng không nhận thức được (dữ liệu đã được mã hóa) về dạng nhận thức được (dạng gốc), quá trình này được gọi là giải mã. Đây là một lớp bảo vệ thông tin rất quan trọng và được sử dụng rộng rãi trong môi trường mạng

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

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

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

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

1.2. MỘT SỐ KHÁI NIỆM CƠ BẢN TRONG TOÁN HỌC

1.2.1. Khái niệm trong số học

Số nguyên tố và nguyên tố cùng nhau.

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

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

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

Ký hiệu : gcd(m,n)=1.

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

Đồng dư thức.

Định nghĩa

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

Kí hiệu

$a \equiv b \pmod{n}$

Ví dụ:

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

Tính chất của đồng dư

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

$a \equiv b \bmod n$ khi và chỉ khi a và b có cùng số dư khi chia cho n.

Tính phản xạ: $a \equiv a \bmod n$.

Tính đối xứng : Nếu $a \equiv b \bmod n$ thì $b \equiv a \bmod n$.

Tính giao hoán: Nếu $a \equiv b \bmod n$ và $b \equiv c \bmod n$ thì $a \equiv c \bmod n$.

$a \equiv a1 \bmod n$, $b \equiv b1 \bmod n$ thì $a + b = a1 + b1 \bmod n$ và $ab = a1b1 \bmod n$.

Lớp tương đương đồng dư

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

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

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

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

Phần tử nghịch đảo

Định nghĩa

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

Tính chất

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

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

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

Ví dụ:

4^{-1} = 7 (mod 9) vì 4.7 ≡ 1 (mod 9)

1.2.2. khái niệm trong đại số

**** Khái niệm nhóm***

Khái niệm

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

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

Tính chất tồn tại phần tử trung gian:

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

Tính chất tồn tại phần tử nghịch đảo:

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

Cấp của nhóm

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

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

Cấp của phần tử

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

****Khái niệm nhóm con***

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

$S \in G$, Phần tử trung gian $e \in S$

$x, y \in S \Rightarrow x * y \in S$

****Khái niệm nhóm Cyclic***

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

Với $\forall x \in G: \exists n \in N$ mà $g^n = x$.

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

1.3. VẤN ĐỀ MÃ HÓA

1.3.1. Giới thiệu về mật mã

Mật mã được sử dụng để bảo vệ tính bí mật của thông tin khi thông tin được truyền trên các kênh thông tin công cộng như các kênh bưu chính điện thoại, mạng internet v.v… Giả sử một người gửi A muốn gửi đến người nhận B một văn bản (chẳng hạn một bức thư) p, để bảo mật A lập cho p một bản mật mã c, và thay cho việc gửi p, A gửi cho B bản mật mã c, B nhận được c và "giải mã" c để lại được văn bản p như A định gửi. Để A biến p thành c và B biến ngược lại c thành p, A và B phải thỏa thuận trước với nhau các thuật toán lập mã và giải mã, và đặc biệt một khóa mật mã chung K để thực hiện các thuật toán đó.

Người ngoài, không biết các thông tin đó (đặc biệt không biết khóa K), cho dù có lấy trộm được c trên cũng khó tìm được văn bản p mà hai người A và B muốn gửi cho nhau.

1.3.1.1. *Khái niệm mật mã*

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

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

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

Theo nghĩa hẹp, "mật mã" chủ yếu dùng để bảo mật dữ liệu, quan niệm: Mật mã học là khoa học nghiên cứu mật mã(Tạo mã và phân tích mã)

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

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

1.3.1.2.*Các bước mã hóa*

1/. Mã hóa: là quá trình chuyển thông tin có thể đọc được (gọi là bản rõ) thành thông tin "khó" thể đọc được theo cách thông thường (gọi là bản mã).
Đó là một trong những kỹ thuật để bảo mật thông tin.
2/. Giải mã: là quá trình chuyển thông tin ngược lại từ bản mã thành bản rõ.
3/. Thuật toán mã hóa hay giải mã là thủ tục để thực hiện mã hóa hay giải mã.
4/. Khóa mã hóa là một giá trị làm cho thuật toán mã hóa thực hiện theo cách riêng biệt và sinh ra bản rõ riêng. Thông thường khóa càng lớn thì bản mã càng an toàn. Phạm vi các giá trị có thể có của khóa được gọi là Không gian khóa.
5/. Hệ mã hóa là tập các thuật toán, các khóa nhằm che giấu thông tin, cũng như làm rõ nó.

1.3.1.3. *Sơ đồ mã hóa*

Một sơ đồ hệ thống mật mã là bộ năm
S = (P, C, K, E, D) thỏa mãn các điều kiện:
P: là một tập hữu hạn các ký tự bản rõ.
C: là một tập hữu hạn các ký tự bản mã.
K: là một tập hữu hạn các khóa.
E: là một ánh xạ từ KxP vào C, được gọi là phép lập mật mã.
D: là một ánh xạ từ KxC vào P, được gọi là phép giải mã.
Với $\mathbf{k} \in \mathbf{K}$ ta định nghĩa $\mathbf{e_k} \in \mathbf{E}$, $\mathbf{e_k}$: $\mathbf{P} \rightarrow \mathbf{C}$, $\mathbf{d_k} \in \mathbf{D}$, $\mathbf{d_k}$: $\mathbf{C} \rightarrow \mathbf{P}$; $\mathbf{e_k}$, $\mathbf{d_k}$ được gọi là hàm lập mãvà hàm giải mã tương ứng với khóa mật mã k. Các hàm đó phải thỏa mãn hệ thức: $\mathbf{d_k}(\mathbf{e_k}(\mathbf{x})) = \mathbf{x}$, $\forall\ \mathbf{x} \in \mathbf{P}$.

1.3.1.4. *Những tính năng của hệ mã hóa*

Cung cấp một mức cao về tính bảo mật, toàn vẹn, chống chối bỏ và xác thực.
+ Tính bảo mật: Bảo đảm bí mật cho các thông báo và dữ liệu bằng việc che giấu thông tin nhờ các kỹ thuật mã hóa.
+ Tính toàn vẹn: Bảo đảm với các bên rằng bản tin không bị thay đổi trên đường truyền tin.
+ Chống chối bỏ: Có thể xác nhận rằng tài liệu đã đến từ ai đó, ngay cả khi họ cố gắng từ chối nó.
+ Tính xác thực: Cung cấp hai dịch vụ:

Nhận dạng nguồn gốc của một thông báo, đảm bảo rằng nó là đúng sự thực.

Kiểm tra định danh của người đang đăng nhập hệ thống, tiếp tục kiểm tra đặc điểm của họ trong trường hợp ai đó cố gắng kết nối và giả danh là người sử dụng hợp pháp.

1.3.2. Các phương pháp mã hóa

Hiện nay có 2 loại mã hóa chính: mã hóa khóa đối xứng và mã hóa khóa công khai. Hệ mã hóa khóa đối xứng có khóa lập mã và khóa giải mã "giống nhau", theo nghĩa biết được khóa này thì "dễ" tính được khóa kia. Vì vậy phải giữ bí mật cả 2 khóa. Hệ mã hóa khóa công khai thì có khóa lập mã khác khóa giải mã (ke kd), biết được khóa nay cũng "khó" tính được khóa kia. Vì vậy chỉ cần bí mật khóa giải mã, còn công khai khóa lập mã.

1.3.2.1. *Hệ mã hóa khóa đối xứng*

1/. Khái niệm

Hệ mã hóa khóa đối xứng là hệ mã hóa mà biết được khóa lập mã thì có thể "dễ" tính được khóa giải mã và ngược lại. Đặc biệt một số hệ mã hóa có khóa lập mã và khóa giải mã trùng nhau ($\mathbf{k_e} = \mathbf{k_d}$), như hệ mã hóa "dịch chuyển" hay DES. Hệ mã hóa khóa đối xứng còn gọi là Hệ mã hóa khóa bí mật, hay khóa riêng, vì phải giữ bí mật cả 2 khóa. Trước khi dùng hệ mã hóa khóa đối xứng, người gửi và người nhận phải thỏa thuận thuật toán mã hóa và khóa chung (lập mã hay giải mã), khóa phải được bí mật.

Độ an toàn của Hệ mã hóa loại này phụ thuộc vào khóa, nếu để lộ ra khóa này nghĩa là bất kỳ người nào cũng có thể mã hóa và giải mã thông báo trong hệ thống mã hóa.

Sự mã hóa và giải mã của hệ thống mã hóa khóa đối xứng biểu thị bởi:

$\mathbf{E_k}$: $\mathbf{P \rightarrow C}$, $\mathbf{D_k}$: $\mathbf{C \rightarrow P}$

2/. Ví dụ:

+ Hệ mã hóa cổ điển là Mã hóa khóa đối xứng: dễ hiểu, dễ thực thi, nhưng có độ an toàn không cao. Vì giới hạn tính toán chỉ trông phạm vi bảng chữ cái, sử dụng trong bản tin cần mã, ví dụ $\mathbf{Z}_{26}$ nếu dùng các chữ cái tiếng anh. Với hệ mã hóa cổ điển, nếu biết khóa lập mã hay thuật toán lập mã, có thể "dễ" xác định được bản rõ, vì "dễ" tìm được khóa giải mã.

+ Hệ mã hóa DES (1973) là Mã hóa khóa đối xứng hiện đại, có độ an toàn cao.

3/. Đặc điểm.

Ưu điểm:

Hệ mã hóa khóa đối xứng mã hóa và giải mã nhanh hơn Hệ mã hóa khóa công khai.

Hạn chế:

(i). Mã hóa khóa đối xứng chưa thật an toàn với lý do sau:

Người mã hóa và người giải mã có "chung" một khóa. Khóa phải được giữ bí mật tuyệt đối, vì biết khóa này "dễ" xác định được khóa kia và ngược lại.

(ii). Vấn đề thỏa thuận khóa và quản lý khóa chung là khó khăn và phức tạp. Người gủi và người nhận phải luôn thống nhất với nhau về khóa. Việc thay đổi khóa là rất khó và dễ bị lộ. Khóa chung phải được gửi cho nhau trên kênh an toàn.

Mặt khác khi hai người (lập mã, giải mã) cùng biết "chung" một bí mật, thì càng khó giữ được bí mật!

4/. Nơi sử dụng hệ mã hóa khóa đối xứng.

Hệ mã hóa khóa đối xứng thường được sử dụng trong môi trường mà khóa chung có thể dễ dàng trao chuyển bí mật, chẳng hạn trong cùng một mạng nội bộ. Hệ mã hóa khóa đối xứng thường dùng để mã hóa những bản tin lớn, vì tốc độ mã hóa và giải mã nhanh hơn hệ mã hóa công khai.

1.3.2.2. *Hệ mã hóa khóa phi đối xứng (hệ mã hóa khóa công khai)*

1/. Khái niệm

Hệ mã hóa khóa phi đối xứng là Hệ mã hóa có khóa lập mã và khóa giải mã khác nhau ($\mathbf{k_e} \neq \mathbf{k_d}$), biết được khóa này cũng "khó" tính được khóa kia.

Hệ mã hóa này còn được gọi là Hệ mã hóa khóa công khai vì:

+ Khóa lập mã cho công khai, gọi là khóa công khai (Public key).

+ Khóa giải mã giữ bí mật, còn gọi là khóa riêng (Private key) hay khóa bí mật.

Một người bất kỳ có thể dùng khóa công khai để mã hóa bản tin, nhưng chỉ người nào có đúng khóa giải mã thì mới có khả năng đọc được bản rõ.

Hệ mã hóa khóa công khai hay Hệ mã hóa phi đối xứng do Diffie và Hellman phát minh vào những năm 1970.

2/. Ví dụ

Hệ mã hóa RSA, hệ mã hóa ELGAMAL,….

3/. Đặc điểm.

Ưu điểm:

(i). Thuật toán được viết một lần, công khai cho nhiều lần dùng, cho nhiều người dùng, họ chỉ cần giữ bí mật cho khóa riêng của mình.

(ii). Khi biết các tham số ban đầu của hệ mã hóa, việc tính ra cặp khóa công khai và bí mật phải là "dễ" , tức là trong thời gian đa thức.

Người gửi có bản rõ P và khóa công khai, thì "dễ" tạo ra bản mã C.

Người nhận có bản mã C và khóa bí mật, thì "dễ" giải được thành bản rõ P.

(iii). Người mã hóa dùng khóa công khai, người giải mã giữ khóa bí mật. Khả năng lộ khóa bí mật khó hơn vì chỉ có một người giữ gìn.

Nếu thám mã biết khóa công khai, cố gắng tìm khóa bí mật, thì chúng phải đương đầu với bài toán "khó".

(iv). Nếu thám mã biết khóa công khai và bản mã C, thì việc tìm ra bản rõ P cũng là bài toán "khó", số phép thử là vô cùng lớn, không khả thi.

Nhược điểm:

Hệ mã hóa khóa công khai: mã hóa và giải mã chậm hơn hệ mã hóa khóa đối xứng.

4/. Nơi sử dụng hệ mã hóa khóa công khai.

Hệ mã hóa khóa công khai thường được sử dụng chủ yếu trên các mạng công khai như Internet, khi mà việc trao đổi chuyển khóa bí mật tương đối khó khăn.

Đặc trưng nổi bật của hệ mã hóa công khai là khóa công khai (public key) và bản mã (ciphertext) đều có thể gửi đi trên một kênh truyền tin không an toàn.

Có biết cả khóa công khai và bản mã, thám mã cũng không dễ khám phá được bản rõ.

Nhưng vì có tốc độ mã hóa và giải mã chậm, nên hệ mã hóa khóa công khai chỉ dùng để mã hóa những bản tin ngắn, ví dụ như mã hóa khóa bí mật gửi đi.

Hệ mã hóa khóa công khai thường được sử dụng cho cặp người dùng thỏa thuận khóa bí mật của hệ mã hóa khóa riêng.

1.4. VẤN ĐỀ CHỮ KÝ SỐ

1.4.1. Khái niệm "chữ ký số"

1.4.1.1. *Giới thiệu "chữ ký số"*

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

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

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

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

"Chữ ký số" không được sử dụng nhằm bảo mật thông tin mà nhằm bảo vệ thông tin không bị người khác cố tình thay đổi để tạo ra thông tin sai lệch. Nói cách khác, "chữ ký số" giúp xác định được người đã tạo ra hay chịu trách nhiệm đối với một thông điệp.

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

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

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

1.4.1.2. *Sơ đồ chữ ký số*

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 $Sig_k \in S$, $Sig_k : P \rightarrow A$,

Thuật toán kiểm tra chữ ký $Ver_k \in V$, $Ver_k : P \times A \rightarrow$ {đúng, sai}, thoả mãn điều kiện sau với mọi $x \in P$, $y \in A$

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

Chú ý

Thường dùng hệ mã hóa khóa công khai để lập "Sơ đồ chữ ký số". Ở đây, khóa bí mật a dùng làm khóa "ký", khóa công khai b dùng làm khóa kiểm tra "chữ ký". (Ngược lại với mã hóa, dùng khóa công khai b lập mã, khóa bí mật a giải mã.)

Điều này là hoàn toàn tự nhiên, "ký" cần giữ bí mật nên phải dùng khóa bí mật a để "ký". Còn "chữ ký" là công khai cho mọi người biết, nên họ dùng khóa công khai b để kiểm tra.

1.4.1.3. ***Phân loại "Chữ ký số"***

1.4.1.3.1. *Phân loại chữ ký theo đặc trưng kiểm tra chữ ký*

1). Chữ ký khôi phục thông điệp:

Là loại chữ ký, trong đó người gửi chỉ cần gửi "chữ ký" , người nhận có thể khôi

phục lại được thông điệp, đã được "ký" bởi "chữ ký" này.

2). Chữ ký đi kèm thông điệp:

Là loại chữ ký, trong đó người gửi chỉ cần gửi "chữ ký", phải gửi kèm cả thông điệp đã được "ký" bởi "chữ ký" này. Ngược lại, sẽ không có được thông điệp gốc.

Ví dụ:Chữ ký Elgamal là chữ ký đi kèm thông điệp, sẽ trình bày trong mục sau.

1.4.1.3.2. *Phân loại chữ ký theo mức an toàn*

1). Chữ ký "không thể phủ nhận":

Nhằm tránh việc nhân bản chữ ký để sử dụng nhiều lần, tốt nhất là người gửi tham gia trực tiếp vào việc kiểm thử chữ ký. Điều đó được thực hiện bằng một giao thức

kiểm thử, dưới dạng một giao thức mời hỏi và trả lời.

Ví dụ: Chữ ký không phủ định (Chaum- van Antverpen), trình bày trong mục sau.

2). Chữ ký "một lần":

Để bảo đảm an toàn, "Khóa ký" chỉ dùng 1 lần (one - time) trên 1 tài liệu.

Ví dụ: Chữ ký một lần Lamport. Chữ ký Fail - Stop (Van Heyst & Pedersen).

1.4.1.3.3. *Phân loại chữ ký theo ứng dụng đặc trưng*

Chữ ký "mù" (Blind Signature).

Chữ ký "nhóm" (Group Signature).

Chữ ký "bội" (Multy Signature).

Chữ ký "mù nhóm" (Blind Group Signature).

Chữ ký "mù bội" (Blind Multy Signature).

Chương 2. CÁC KHÁI NIỆM CƠ BẢN VỀ THƯƠNG MẠI ĐIỆN TỬ

2.1. TỔNG QUAN VỀ CÁC HOẠT ĐỘNG THƯƠNG MẠI ĐIỆN TỬ

2.1.1 Khái niệm thương mại điện tử.

Theo Ủy ban Châu Âu: *Thương mại điện tử được hiểu là việc thực hiện hoạt động kinh doanh qua các phương tiện điện tử. Nó dựa trên việc xử lý và truyền dữ liệu điện tử dưới dạng text, âm thanh và hình ảnh.*

Theo Tổ chức Thương mại Thế giới: *Thương mại điện tử bao gồm việc sản xuất, quảng cáo, bán hàng và phân phối sản phẩm được mua bán và thanh toán trên mạng Internet, nhưng được giao nhận một cách hữu hình cả các sản phẩm được giao nhận cũng như những thông tin số hóa thông qua mạng Internet.*

Vai trò tác động

Cùng với sự phát triển của Internet và world wide web, TMĐT ra đời và ngày càng phát triển, ngày càng khẳng định vị thế của nó trong đời sống xã hội. Và nó ngày càng có những tác động to lớn trong đời sống của con người. Trong hoạt động thương mại, TMĐT góp những vai trò đáng kể:

***Với doanh nghiệp*:**

TMĐT xuất hiện và phát triển, giúp cho các doanh nghiệp có thể tương tác với nhau hay tìm kiếm khách hàng nhanh hơn, tiện lợi hơn với một chi phí thấp hơn nhiều so với thương mại truyền thống. TMĐT làm cho việc cạnh tranh toàn cầu phát triển, và sự tiện lợi trong việc so sánh giá cả khiến cho những người bán lẻ hưởng chênh lệch giá ít hơn. Từ khi TMĐT ra đời, nó tạo điều kiện cho các doanh nghiệp vừa và nhỏ và các doanh nghiệp ở các nước mới phát triển có thể cạnh tranh với cách doanh nghiệp lớn. Nó giúp cách doanh nghiệp có thể giới thiệu hàng hóa đến khách hàng một cách tự động, nhanh chóng nhất, nó giúp giảm chi phí liên lạc, giao dịch, chi phí marketing.

Với người tiêu dùng:

TMĐT giúp người mua có thể tìm hiểu, nghiên cứu các thông số hàng hóa và các dịch vụ kèm theo sản phẩm một cách tiện lợi nhất, nhanh nhất. Họ có thể so sánh hàng hóa cũng như giá cả của hàng hóa để đưa ra quyết định lựa chọn hợp lý nhất, ở đó, họ có thể mùa hàng hóa với giá cả thấp nhất hợp lý nhất có thể.

TMĐT giúp người tiêu dùng có thể dễ dàng đưa ra những yêu cầu đặc biệt của mình cho các nhà doanh nghiệp đáp ứng, họ có thể giảm gia đầu giá trực tuyến trên toàn cầu hay cũng có thể liên lạc với những người tiêu dùng khác có cùng nhu cầu với mình để mua hàng theo lô với giá rẻ hơn. Internet cách mạng hoá marketing bán lẻ và marketing trực tiếp. Người tiêu dùng có thể mua sắm bất cứ sản phẩm nào của nhà sản xuất và những nhà bán lẻ trên khắp thế giới…. Tất cả đều được thực hiện ngay tại nhà.

***Với ngành ngân hàng và các ngành dịch vụ khác*:**

Khi TMĐT phát triển, ngành ngân hàng, ngành giáo dục, tư vấn, thiết kế, marketting và rất nhiều những dịch vụ tương ứng đã và đang thay đổi rất nhiều về cách thức, chất lượng dịch vụ. Ngành ngân hàng từ giữ tiền truyền thống, đã chuyển sang lưu trữ, giao dịch và quản lý đồng tiền số dựa vào internet và TMĐT …

Ngày càng nhiều doanh nghiệp và người tiêu dùng từ nhiều quốc gia khác nhau tham gia vào TMĐT, Doanh thu từ TMĐT ngày càng chiếm tỷ trọng lớn trong doanh thu thương mại.... Ngành quảng cáo trực tuyến mang lại những lợi nhuận khổng lồ cho doanh nghiệp cũng như cho chính phủ. TMĐT ngày càng có những tác động to lớn.

Thứ nhất, nó phá vỡ giới hạn không gian và thời gian kinh doanh.

Thứ hai, TMĐT tạo mối quan hệ trực tiếp giữa nhà cung cấp với người tiêu dùng.

Thứ ba, TMĐT làm giảm đáng kể sự phỏng đoán: Thương mại trong xã hội công nghiệp truyền thống thường được xây dựng trên một thế giới – sự phỏng đoán. Nói một cách khác đại lý và người bán lẻ đều tham gia vào việc phỏng đoán: khách hàng muốn cái gì?

Thứ tư, tạo lên một sự lựa chọn phong phú, và các yêu cầu phong phú đa dạng hơn: Khách hàng có thể đưa ra yêu cầu những cái mà họ muốn có, và những yêu cầu đó có thể được đáp ứng.

Thứ năm, tác động của bất động sản đối với kinh doanh giảm đáng kể: Với TMĐT, chúng ta đã chuyển vào xã hội mạng, Các giao dịch sẽ dựa vào hệ thống giao nhận trực tiếp và số lượng những người trung gian sẽ giảm đi rất nhiều.

Thứ sáu, thương mại quốc tế giữa các cá nhân ngày càng phát triển hơn.

Thứ bảy, Cuộc cách mạng tiếp thị của các sản phẩm và dịch vụ số hóa ngày càng phát triển mạnh.

Thứ tám, TMĐT tạo sức mạnh cải tổ gây ra biến đối của ngân hàng truyền thống.

Thứ chín, Cước viễn thông sẽ là khoản thu lớn nhất của chính phủ.

Thứ mười, TMĐT phát triển, các luật mới cũng cần được phát triển và ban hành.

2.1.2 Các đặc trưng của Thương mại điện tử.

1) Các bên tiến hành giao dịch không tiếp xúc trực tiếp với nhau và không đòi hỏi phải biết nhau từ trước.

2) Được thực hiện trên thị trường không có biên giới (thị trường thống nhất toàn cầu) và trực tiếp tác động tới môi trường cạnh tranh toàn cầu.

3) Trong hoạt động giao dịch có sự tham gia của ít nhất ba chủ thể, một bên không thể thiếu được là người cung cấp dịch vụ mạng, và các cơ quan chứng thực.

4) Đối với thương mại điện tử, thì mạng lưới thông tin chính là thị trường.

2.1.3 Các mô hình thương mại điện tử.

Mô hình B2C (Business–To–Customer: Nhà cung cấp tới khách hàng):
B2C là hình thức giao dịch giữa một doanh nghiệp và người tiêu dùng tại các cửa hàng trên Internet thường là các Website Internet, bao gồm việc hỗ trợ khách hàng trực tuyến và bán lẻ hàng hóa trực tuyến. Thường không đòi hỏi hóa đơn chứng từ. Mô hình này còn gọi là mô hình luôn bán điện tử (E – Business).

Mô hình B2B (Business to Business: Nhà cung cấp tới nhà cung cấp):
B2B là loại hình cho phép thực hiện giao dịch giữa các doanh nghiệp với nhau hay giữa các chi nhánh với tổng công ty. Các hoạt động có thể gồm đàm phán ký kết hợp đồng, đặt hàng qua hệ thống catalog trực tuyến, quản lý điều phối hàng hóa giữa các chi nhánh, tìm kiếm đối tác, đấu giá gọi thầu và bao gồm cả việc bán lẻ hàng hóa trực tuyến. Giao dịch B2B phải có hóa đơn chứng từ điện tử đầy đủ giá trị pháp lý. Mô hình này còn gọi là mô hình TMĐT (E – Commerce).

Mô hình P2P (Peer to Peer: cá nhân tới cá nhân):
P2P là việc kinh doanh TMĐT giữa người tiêu dùng và người tiêu dùng (hai nhóm đối tượng trong đó người bán và người mua đều là cá nhân.

Mô hình B2G (Business To Government–doanh nghiệp với Chính phủ):
B2G gồm mọi giao dịch giữa các doanh nghiệp với cơ quan chính quyền. Bên cạnh việc mua bán hàng hoá, chính phủ có thể cung cấp các dịch vụ của mình cho doanh nghiệp qua mạng như thu thuế, trả tiền, đăng ký kinh doanh.

2.2. MỘT SỐ BÀI TOÁN VỀ AN TOÀN THÔNG TIN TRONG GIAI ĐOẠN THỎA THUẬN KÝ KẾT HỢP ĐỒNG ĐIỆN TỬ

2.2.1. GIỚI THIỆU

Quy trình TMĐT không khác nhiều so với thương mại truyền thống. Đó là một quá trình mua bán hàng hóa, hay quy trình của một thương vụ thương mại thông qua các phương tiện điện tử. Quy trình thương mại nói chung và TMĐT nói riêng đều có các giai đoạn sau:

1/.Quảng bá, giới thiệu sản phẩm (Marketing).

2/.Thỏa thuận và Ký kết hợp đồng.

3/.Thanh toán và chuyển giao sản phẩm.

Một trang TMĐT an toàn, trước hết nó phải đảm bảo những yêu cầu an toàn thông tin như đã trình bày trong chương I. Ngoài những yêu cầu an toàn thông tin và phương pháp giải quyết chung trong giao dịch điện tử, trong TMĐT có những yêu cầu an toàn thông tin riêng đặc trưng và những phương pháp giải quyết riêng.

Trong mỗi quá trình thương vụ TMĐT đều có những vấn đề thách thức, những bài toán đặt ra trong an toàn thông tin, an toàn TMĐT: như bản quyền, bảo mật thông tin, toàn vẹn thông tin, chống từ chối dịch vụ, tránh gian lận trong giao dịch, trong thanh toán… Ở mỗi quá trình thương vụ TMĐT đều có những bài toán riêng của nó, trong chương này ta sẽ nghiên cứu các bài toán an toàn thông tin đặc trưng đặt ra trong mỗi quy trình thương vụ TMĐT.

2.2.2. MỘT SỐ BÀI TOÁN TRONG THỎA THUẬN VÀ KÝ KẾT HỢP ĐỒNG

Việc thỏa thuận hợp đồng thương mại gồm hai giai đoạn là 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 2 bên hoặc nhiều bên có ý muốn quan hệ đối tác với nhau, nhằm tiến đến một thoả 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 ký 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 đề nảy 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. Ngoài ra trong thỏa thuận hợp đồng còn có một số bài toán đặc trưng riêng, trong phần này sẽ đề cập đến.

2.2.2.1. *Bảo đảm tính toàn vẹn 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 một 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 được 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 bản hợp đồng và B ký chấp nhận hợp đồng, hay nếu B không đồng ý với tất cả các điều khoản, B bổ xung một số điều khoản để thỏa thuận lại và gửi lại cho A. Trong quá trình bản hợp đồng đã được 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 thông tin của bản hợp đồng này.

Giải pháp:

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 số và chứng chỉ điện tử.

Khi nội dung của bản hợp đồng bị 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 là 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 chuyển đi sẽ không bị thay đổi. Mọi sự thay đổi dù nhỏ nhất sẽ đều bị phát hiện dễ dàng.

2.2.2.2. *Bảo đảm tính xác thực*

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 bên 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 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, hay các địa chỉ ảo, 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, John gửi một thông báo đã xác thực cho Mary. Có thể xảy ra tranh chấp giữa hai thành viên như sau:

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

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

Giải pháp:

Các tranh chấp xảy ra giữa người gửi và người nhận không có sự tin cậy tuyệt đối. Có nhiều giải pháp cho vấn đề xác thực như hàm băm, chứng chỉ điện tử, chữ ký số. 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 ta để giải quyết tranh chấp.

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

- Chữ ký số phải là một mẫu bít 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 lưu giữ bản sao của chữ ký số.

2.2.2.3. *Chống chối bỏ hợp đồng giao dịch*

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 minh bạch. Giao kết hợp đồng TMĐT được thực hiện trong môi trường Internet …, các bên tham gia ký kết hợp đồng xa nhau về 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 X ở nước ngoài. Sau khi thỏa thuận ký kết hợp đồng, Công ty X chuyển hàng đến ông A (kèm theo đó là chi phí vận chuyển, thuế hải quan), khi sản phẩm đến, ông A thay đổi ý kiến, không muốn mua sản phẩm này nữa, và ông A đã chối bỏ những gì mình đã thỏa thuận (không có bên thứ 3 thực nào xác nhận cuộc thỏa thuận hợp đồng mua hàng giữa ông A và công ty X) … Việc này gây thiệt hại cho công ty X.

Trường hợp công ty X mang hàng đến cho ông A, nhưng mặt hàng không đúng như trong thỏa thuận, mà công ty X 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 các đối tượng tham gia TMĐT. Chống chối bỏ giao dịch là bài toán quan trọng trong quá trình thỏa thuận hợp đồng trong TMĐT.

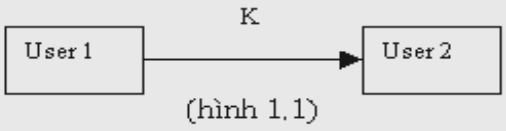
Giải pháp:

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 chống 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 chứng minh xác thực rằng anh A có tham gia vào một giao dịch điện tử nào hay không, chữ ký trên văn bản giao dịch có đúng đích thực của anh A hay không, nếu đó là chữ ký của A mà A chối bỏ, sẽ có giao thức chứng minh, buộc A không được chối bỏ giao dịch hợp đồng đã thỏa thuận. Chương trình thử nghiệm sẽ mô phỏng ứng dụng của chữ ký không thể phủ nhận trong quy trình đặt đơn hàng trực tuyến.

Chương 3. MỘT SỐ PHƯƠNG PHÁP QUẢN LÝ KHÓA MẬT MÃ DÙNG TRONG THỎA THUẬN KÝ KẾT HỢP ĐỒNG

3.1. GIỚI THIỆU KHÓA VÀ MỘT SỐ KHÁI NIỆM LIÊN QUAN

Trong một mạng liên lạc dữ liệu, giả sử rằng một user ở một terminal đang liên lạc với một chương trình ứng dụng hay một user ở một terminal khác ở trong cùng một vùng hay ở một vùng khác, các user này dùng chung một khoá (khoá chính K). Khoá K này có thể là một khoá bí mật được cung cấp và được chấp nhận trước bởi các user hoặc một khoá được cấp phát động bởi hệ thống và gán cho các user này, được gọi là



(hình 1.1)

khoá mã hoá dữ liệu hoặc khoá giải mã dữ liệu.

Một khoá chính được dùng để bảo mật liên lạc được gọi là khoá giao tiếp chính (primary communication key - KC). Khoá mã hoá dữ liệu chỉcó tác dụng trong khoảng thời gian của một phiên liên lạc và được gọi là khoá phiên (session key - KS).

Đối với bảo mật file, khoá mã hoá dữ liệu dùng để bảo vệ file gọi là khoá file (file key - KF). Khoá file được tạp bởi người dùng cuối hoặc bởi hệ thống. File đã mã hoá có thể được giải mã ở một terminal hoặc một host bất kỳ nào có chứa sẵn khoá KF này.

Khoá phụ (secondary key - KN) trong đó N biểu diễn nút, là một loại khoá mã hoá khoá được dùng đẻ bảo vệ các khoá chính. Khi một khoá phụ được dùng để bảo vệ khoá trong môi trường giao tiếp thì được gọi là khoá giao tiếp phụ (secondary communication key - KNC), còn khi áp dụng trong môi trường cơ sở dữ liệu thì được gọi là khoá tập tin phụ (secondary file key - KNF).

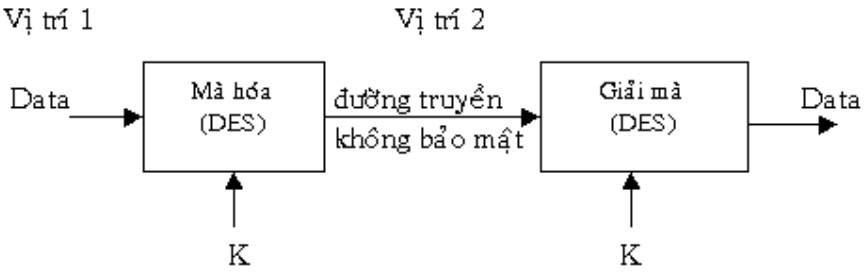
Trong một môi trường giao tiếp, một khoá chính chỉ tồn tại trong khoảng thời gian hai người dùng cuối trao đổi dữ liệu với nhau. Thông thường khoá sẽ chỉ tồn tại trong khoảng vài phút hoặc vài giờ, ít khi tồn tại hơn một ngày. Ngược lại khoá chính được dùng để bảo vệ dữ liệu lưu trữ có thể tồn tại trong khoảng vài năm hoặc trong suốt thời gian mà tập tin được lưu trữ. Còn khoá phụ thông thường được dưa vào hệ thống lúc có yêu cầu cài đặt thông qua bộ tạo khoá, các khoá phụ được lưu trữ lâu dài (vài tháng hoặc vài năm) và không được thay đổi.

Đối với bảo mật liên lạc, các khoá phiên liên lạc được tạo ra ở host và sau đó được truyền đến một nút nhận (terminal hoặc host) thông qua một mạng liên lạc(giả sử là không an toàn). Khoá phiên liên lạc được bảo mật bằng cách mã hoá nó bởi một khoá khác (khoá mã hoá khoá) mà được cài sẵn ở nút nhận. Mỗi nút nhận có một khoá mã hoá khoá duy nhất. Do đó nếu khoá này bị hỏng thì chỉ ảnh hưởng đến tính an toàn ở tại terminal này mà không làm ảnh hưởng đến tính an toàn ảu toàn bộ mạng.

Trong một số hệ thống riêng biệt, một tập các khoá mã hoá khoá được dùng để mã hoá các khoá phiên liên lạc được truyền từ host này đến host khác và một tập các khoá mã hoá khoá khác được dùng để mã hoá các khoá phiên liên lạc được truyền từ host đến terminal. Vì vậy mỗi hos phải chứa khoá mã hoá đến host và terminal mà nó liên lạc đến (được gọi là khoá chủ của host – KM – key master), trong khi mỗi terminal chỉ cần chứa một khoá mã hoá đến host mà nó liên lạc (được gọi là khoá chủ của terminal – KTM – key terminal master).

Hệ mật mã chứa thuật toán mã hoá (như là DES) và một bộ nhớ cố định để chứa các khoá chủ (như là KM, KTM ở host hoặc KTM ở terminal). Nó chỉ có thể được truy xuất thông qua các giao tiế hợp pháp. Vì một số lượng lớn các khoá mã hoá được dùng ở bộ xử lý của host nên cần phải có các thủ tục tự động tạo ra và quản lý các khoá này. Bộ tạo khoá sẽ tạo ra các khoá mã hoá khoá mà chúng được yêu cầu bởi host hoặc có thể được chỉ định bởi các user. Nó có đặc quyền thêm vào, thay đổi và huỷ bỏ các khoá. Bộ quản lý khoá có nhiệm vụ mã hoá lại một khoá từ việc mã hoá bởi một khoá khác.

Các nút mà ở đó đòi hỏi mã hoá dữ liệu thì phải chứa các thuật toán mã hoá giống nhau và mỗi nút phải có một bản sao của cùng một khoá mã hoá K. Hai nút phải luôn luôn sử dụng một khoá mã hoá dữ liệu chung để cho phép liên lạc an toàn với nhau. Nhờ vậy sẽ giảm thiểu hư hỏng nếu một khoá bị phá hỏng.



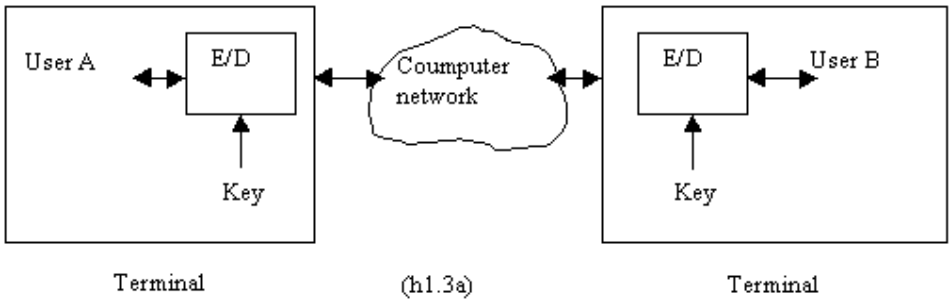
(hình 1.2)

- Các mức bảo mật:

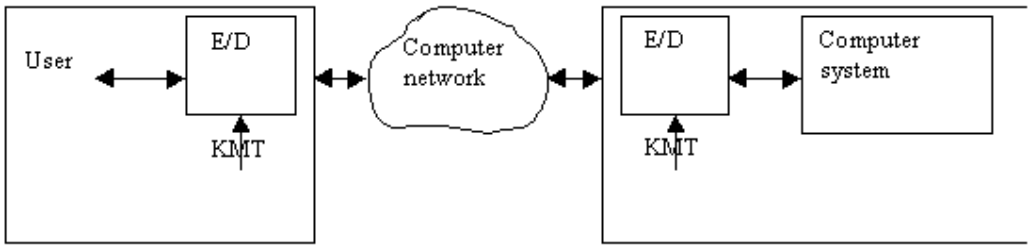
. Giữa terminal với terminal (mã hóa cuối-cuối): (h1.3a)

. Giữa terminal với host: (h1.3b)

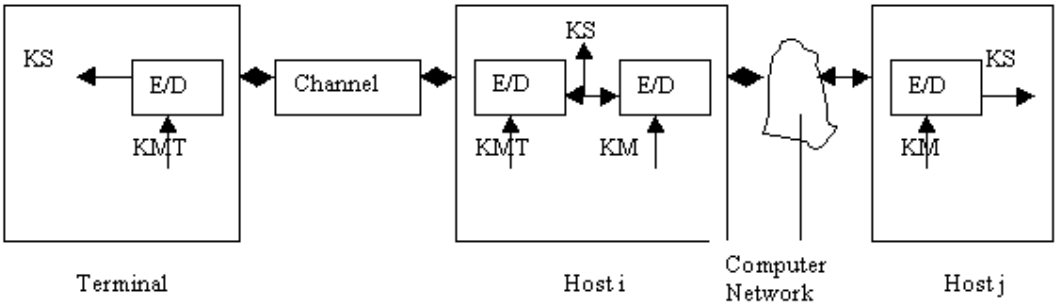
. Giữa host với host: (h1.3c)



Terminal (h1.3a) Terminal



Terminal (h1.3b) Host



(h1.3c)

Để bảo mật khi truyền thông, người ta sử dụng các giải thuạt mã hoá đối xứng (hệ thống khoá bí mật) và mã hoá không đối xứng (hệ thông khoá công khai). Hệ thống khoá công khai có ưu điểm hơn hệ thống khoá bí mật ở chỗ không cần có kênh an toàn để troa đổi khoá mật. Tuy nhiên, đáng tiéc là hầu hết các hệ thống mã hoá khoá công khai đều chậm hơn nhiều so với các hệ thống khoá bí mật như DES. Vì vậy trong thực tế hệ thống khoá bí mật thường được dùng để mã hoá các bức điện dài. Nhưng khi đó chúng ta phải giải quyết bài toán trao đổi khoá mật

3.2. VẤN ĐỀ QUẢN LÝ KHÓA CÔNG KHAI

3.2.1.Giới thiệu về PKI

1). Cơ sở hạ tầng về Mật mã khoá công khai (Public Key Infrastructure – PKI).

PKI có thể hiểu là*: Tập hợp các công cụ, phương tiện* cùng *các giao thức* bảo đảm an toàn truyền tin cho các giao dịch trên mạng máy tính công khai. Đó là *nền móng* mà trên đó các ứng dụng, các hệ thống an toàn bảo mật thông tin được thiết lập.

Theo nghĩa đầy đủ, PKI gồm 3 phần chính:

Phần 1: Tập hợp các công cụ, phương tiện, giao thức bảo đảm an toàn thông tin.

Phần 2: Hành lang pháp lý: Luật giao dịch điện tử, các Qui định dưới luật.

Phần 3: Các tổ chức điều hành giao dịch điện tử (CA, RA, LRA,…).

Ba thành phần trên thiết lập một *Hệ thống tin cậy* trên mạng máy tính công khai.

2).*Hệ thống có các khả năng sau*:

- Bảo đảm *bí mật* các thông tin truyền trên mạng: thực thể không được cấp quyền không thể xem trộm bản tin.
- Bảo đảm *toàn vẹn* các thông tin truyền trên mạng: thực thể không được cấp quyền không có thể sửa đổi bản tin.
- Bảo đảm *xác thực* các thông tin truyền trên mạng: thực thể nhận bản tin có thể định danh được thực thể gửi bản tin và ngược lại.
- Bảo đảm hỗ trợ các yêu cầu *chống chối cãi*.

Nhờ những khả năng đó, trên hệ thống này, các thực thể không biết mặt nhau, *từ xa có thể tiến hành các giao dịch trong niềm tin cậy lẫn nhau.*

3).*Xây dựng PKI* là công việc của mỗi nước, không ai thay thế ta được. Nếu dùng hệ thống sẵn có của nước ngoài thì không lấy gì làm bảo đảm an toàn, bí mật của riêng ta. Mặt khác khi có sự cố an toàn truyền thông chúng ta không có cơ cở khoa học để xử lý, không phải mỗi lần gặp sự cố lại phải mời nước ngoài.

* Khác với các phần mềm thông thường, đây là phần mềm bảo mật, chúng ta phải tự làm hệ thống bảo mật cho riêng mình. Điều đó tin cậy hơn. Mặt khác khi nắm vững cơ chế bảo mật của mình, chúng ta sẽ khắc phục được hậu quả khi xảy ra các sự cố truyền thông.

* Mỗi ngành nghề, mỗi lĩnh vực có yếu cầu "an toàn và bảo mật" riêng, vì vậy hiện nay người ta thường xây dựng PKI cho riêng mình.

* Cũng có ý kiến cho rằng nên dùng PKI chung cho mọi ngành nghề, mọi lĩnh vực. Quan điểm này cũng giống như dùng phần mềm quản lý chung cho mọi ngành nghề, mọi lĩnh vực! Thực tế đã không xảy ra như vậy.

* Ở nước ta một số cơ sở có nghiên cứu vấn đề trên nhưng mới ở mức sử dụng công nghệ của nước ngoài. Họ chưa đủ lực lượng để lý giải một cách khoa học các giải pháp, công nghệ này.

* Một số cơ sở khác chỉ nghiên cứu lý thuyết, chưa nghiên cứu giải pháp, công nghệ.

4). Nước ta đã có nhu cầu xây dựng Cơ sở hạ tầng về Mật mã khoá công khai (PKI):

- 2002, chúng ta đã chuyển các đề thi vào đại học qua mạng máy tính tới một số địa điểm thi một cách an toàn. Tuy vậy chưa có hệ thống thực hiện thường xuyên.
- Ngày 2-5-2002, đã có Quyết định số 44/2002/QĐ-TTg của Thủ tướng Chính phủ: "Về việc sử dụng chứng từ điện tử làm chứng từ kế toán".
- Ngày 29/11/ 2005, Quốc hội đã thông qua "Luật giao dịch điện tử".
  Ngày 1/3/2006, "Luật giao dịch điện tử" tại Việt nam đã có hiệu lực

3.2.2. Nội dung PKI

3.2.2.1. *Các thành phần kỹ thuật cơ bản của PKI*

Nội dung nghiên cứu (Mã hóa, Ký số, Chứng chỉ số)

Mã hóa.

Mã hóa là công cụ cơ bản của việc đảm bảo an toàn dữ liệu. Ở thời kỳ sơ khai, con người đã sử dụng nhiều phương pháp để bảo vệ các thông tin bí mật, nhưng tất cả các phương pháp đó chỉ mang tính nghệ thuật hơn là khoa học. Ban đầu, mật mã học được sử dụng phổ biến cho quân đội, qua nhiều cuộc chiến tranh, vai trò của mật mã ngày càng quan trọng và mang lại nhiều thành quả không nhỏ như các hệ mã cổ điển Caeser, Playfair,…Chúng đã là nền tảng cho mật mã học này nay.

Ngày nay, khi toán học được áp dụng cho mật mã học thì lịch sử của mật mã học đã sang trang mới. Việc ra đời các hệ mã hóa đối xứng không làm mất đi vai trò của các hệ mật mã cổ điển mà còn bổ sung cho ngành mật mã nhiều phương pháp mã hóa mới. Từ năm 1976, khi hệ mật mã phi đối xứng (mật mã khóa công khai) ra đời, nhiều khái niệm mới gắn với mật mã học đã xuất hiện: chữ ký số, hàm băm, mã đại diện, chứng chỉ số. Mật mã học không chỉ áp dụng cho quân sự mà còn cho các lĩnh vực kinh tế xã hội khác (giao dịch hành chính, thương mại điện tử).

Hiện nay có nhiều phương pháp mã hóa khác nhau, mỗi phương pháp có ưu, nhược điểm riêng. Tùy theo yêu cầu của môi trường ứng dụng nào, người ta có thể dùng phương pháp này hay phương pháp kia. Có những môi trường cần phải an toàn tuyệt đối bất kể thời gian và chi phí. Có những môi trường lại cần giải pháp dung hòa giữa bảo mật và chi phí.

Các thông điệp cần chuyển đi và cần được bảo vệ an toàn gọi là bản rõ (plaintext), và được ký hiệu là P. Nó có thể là một dòng các bít, các file, âm thanh số hoá,... Bản rõ được dùng để lưu trữ hoặc để truyền đạt thông tin. Trong mọi trường hợp bản rõ là thông điệp cần mã hoá. Quá trình xử lý một thông điệp trước khi gửi được gọi là quá trình mã hoá (encryption). Một thông điệp đã được mã hoá được gọi là bản mã (ciphertext), và được ký hiệu là C. Quá trình xử lý ngược lại từ bản mã thành bản rõ được gọi là quá trình giải mã (decryption).

Hệ mật mã là tập hợp các thuật toán, các khóa nhằm che dấu thông tin tin cũng như làm rõ nó.

Hệ mật mã được định nghĩa là bộ năm (P,C,K,E,D), trong đó:

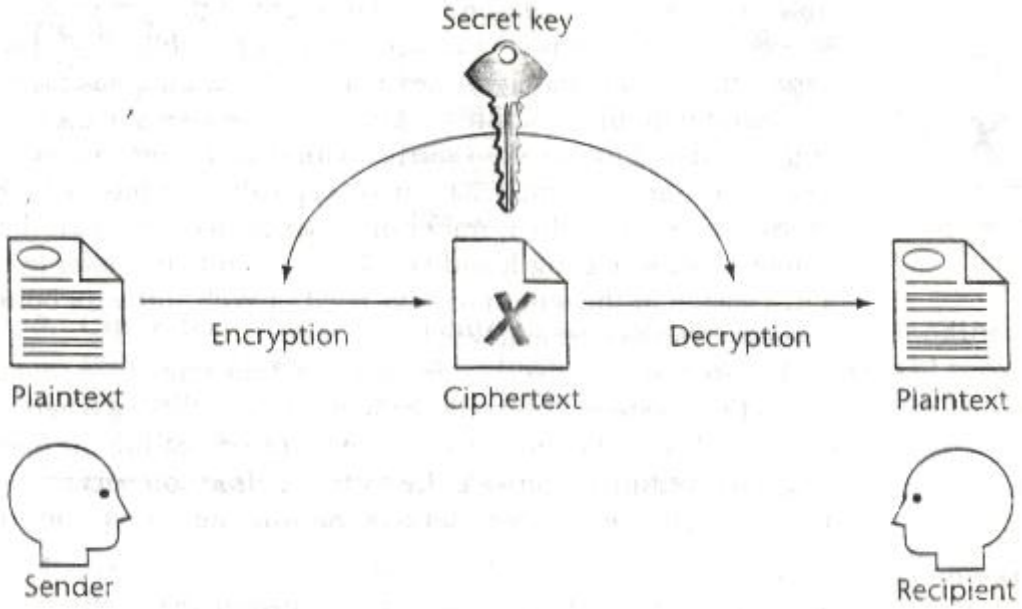
- P là tập hữu hạn các bản rõ có thể
- C là tập hữu hạn các bản mã có thể
- K là tập hữu hạn khóa có thể
- E là tập các hàm lập mã
- D là tập các hàm giải mã. Với mỗi $k \in K$ có một hàm lập mã $E_k \in E$ ($E_k: P \rightarrow C$) và một hàm giải mã $D_k \in D$ ($D_k : C \rightarrow P$) sao cho $D_k(E_k(x)) = x$, $\forall\ x \in P$.

Hiện nay các hệ mật mã được phân làm hai loại chính là: Hệ mật mã đối xứng và hệ mật mã phi đối xứng (hay còn gọi là hệ mật mã khóa công khai).

Một số hệ mật mã đối xứng là: Caesar, IDEA, DES, Triple DES.

Một số hệ mật mã công khai là: RSA, Elgamal, ECC.

** Hệ Mã hóa khóa đối xứng*



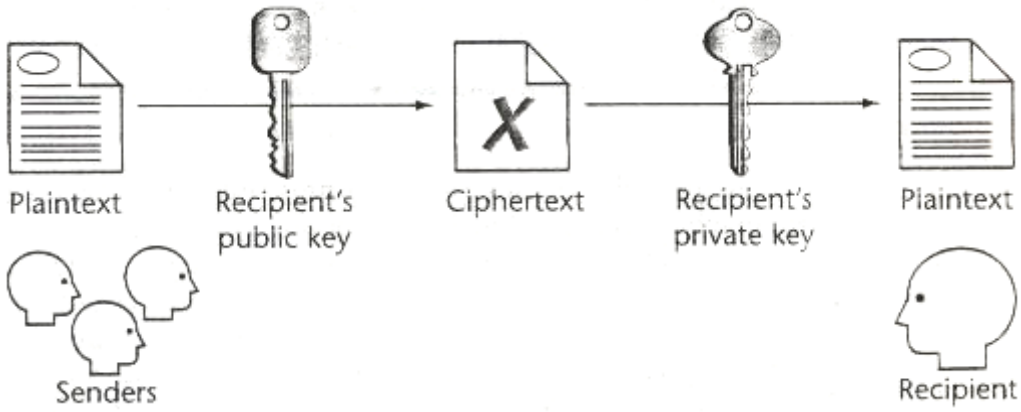
** Ưu điểm:*

- Tốc độ mã hóa nhanh.
- Sử dụng đơn giản: chỉ cần dùng một khoá cho cả 2 bước mã và giải mã.

** Nhược điểm:*

- Các phương mã hoá cổ điển đòi hỏi người mã hoá và người giải mã phải cùng chung một khoá. (Chính xác là biết khóa này "dễ dàng" xác định khoá kia). Khi đó khoá phải được giữ bí mật tuyệt đối. Mặt khác 2 người cùng giữ chung một bí mật thì "khó" "bí mật".
- Vấn đề quản lý và phân phối khoá là khó khăn và phức tạp khi sử dụng hệ mã hoá cổ điển. Người gửi và người nhận phải luôn luôn thông nhất với nhau về vấn đề khoá. Việc thay đổi khoá là rất "khó" và dễ bị lộ.
- Khuynh hướng cung cấp khoá dài, lại phải được thay đổi thường xuyên cho mọi người, trong khi vẫn duy trì cả tính an toàn và chi phí, sẽ cản trở rất nhiều tới việc phát triển hệ mật mã cổ điển.

** Hệ Mã hóa khóa công khai*



** Ưu điểm:*

- Dùng cặp khóa để mã hóa nên không cần bảo mật khóa mã hóa, chỉ cần bảo mật khóa giải mã.
- Có thể dùng mã hóa khóa công khai để tạo chữ ký điện tử, chứng chỉ số.

** Nhược điểm:*

- Tốc độ mã hóa / giải mã chậm, "khó" thực hiện việc mã hóa các bản tin dài.

Ký số.

Với thỏa thuận thông thường trên giấy, hai đối tác xác nhận sự đồng ý bằng cách kí tay vào cuối các hợp đồng. Bằng cách nào đó người ta phải thể hiện đó là chữ kí của riêng họ và kẻ khác không thể giả mạo. Mọi cách sao chép chữ kí trên giấy thường dễ bị phát hiện, vì bản sao có thể phân biệt được với bản gốc.

Các giao dịch hợp tác trên mạng cũng được thực hiện theo cách tương tự, nghĩa là hai đối tác trên hai nút mạng cũng phải kí vào Bản thỏa thuận. Chỉ khác là văn bản truyền trên mạng được biểu diễn dưới dạng "số" (chỉ dùng chữ số 0 và 1), ta gọi nó này là "văn bản số" (điện tử). Do đó chữ kí trên "văn bản số" khác với chữ kí trên văn bản giấy thông thường.

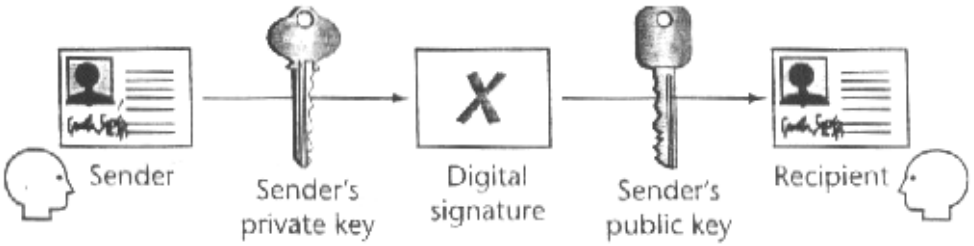
Việc giả mạo và sao chép lại đối với "văn bản số" là việc hoàn toàn dễ dàng, không thể phân biệt được bản gốc với bản sao. Như vậy "chữ kí" ở cuối "văn bản số" không thể chịu trách nhiệm đối với toàn bộ nội dung văn bản loại này. Do đó Chữ kí thể hiện trách nhiệm đối với toàn bộ "văn bản số" phải là "*chữ kí*" được kí trên từng bit của văn bản loại này. Bản sao của "chữ kí số" có tư cách pháp lí.

Chữ kí thông thường được kiểm tra bằng cách so sánh nó với chữ kí gốc. Ví dụ, ai đó kí một tấm séc để mua hàng, người bán phải so sánh chữ kí trên mảnh giấy với chữ kí gốc nằm ở mặt sau của thẻ tín dụng để kiểm tra. Dĩ nhiên, đây không phải là phương pháp an toàn vì nó dễ dàng bị giả mạo.

"Chữ kí số" có thể được kiểm tra chính xác nhờ dùng một thuật toán kiểm tra công khai. Như vậy, bất kỳ ai cũng có thể kiểm tra được chữ kí số. Việc dùng một sơ đồ chữ kí an toàn có thể sẽ ngăn chặn được khả năng giả mạo.

** Đại diện thông điệp*

Vì "*Chữ kí số* " được kí trên từng bit của "văn bản số", nên độ dài của nó ít nhất cũng bằng văn bản cần kí. Như vậy sẽ tốn kém chỗ nhớ cũng như thời gian "kí" và



thời gian truyền "Chữ kí số ". Trên thực tế thay vì kí trên "văn bản số", người ta kí trên "*Đại diện*" (*Digest*) của nó.

Để ký trên "văn bản số" dài, đầu tiên phải tạo "đại diện" của văn bản nhờ "*Hàm băm* ". Một thông điệp được đưa qua hàm băm sẽ tạo ra xâu bit với độ dài cố định và ngắn hơn được gọi là "*Đại diện*" (*Digest*). Mỗi thông điệp đi qua 1 hàm băm chỉ cho duy nhất 1 "*Đại diện*". Ngược lại, "khó" tìm được 2 thông điệp khác nhau mà có cùng một "*Đại diện*" (ứng với cùng 1 hàm băm).

Hàm băm kết hợp với "chữ ký số" ở trên sẽ tạo ra một loại "*chữ ký điện tử* " vừa an toàn (không thể cắt / dán), vừa có thể dùng để *kiểm tra tính toàn vẹn* của thông điệp.

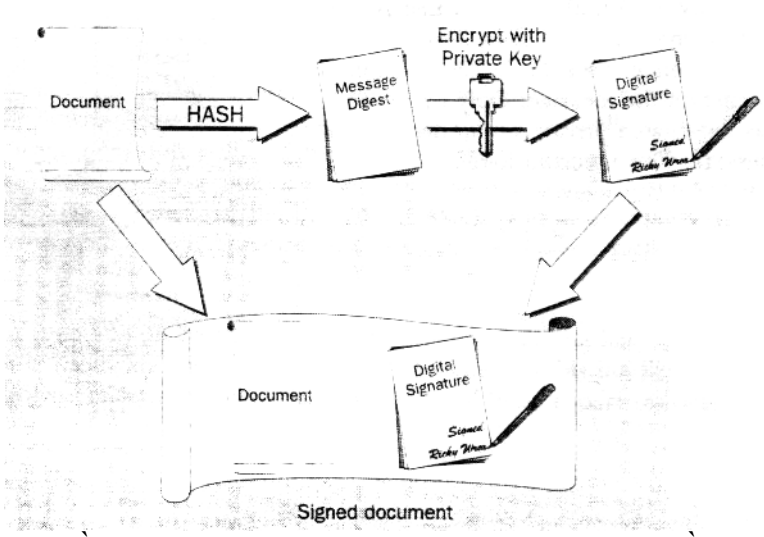
1). Người gửi: *Tạo ra* "chữ ký số".

* Đưa thông điệp cần gửi qua hàm băm tạo ra "*Đại diện*".

* Mã hoá "*Đại diện*" bằng khoá riêng (private) của người gửi để tạo ra "chữ ký số".

* Mã hoá thông điệp và chữ ký bằng khoá công khai (public) của người nhận, gửi đi.

2). Người nhận: *Định danh người ký, kiểm tra tính toàn vẹn* của thông điệp.



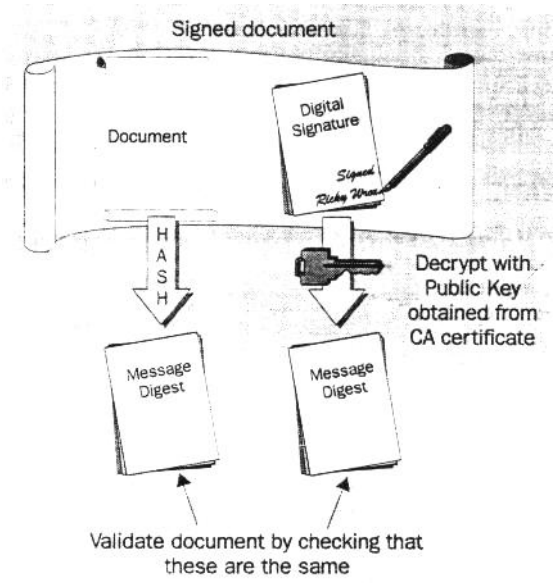
* Giải mã thông điệp bằng khoá riêng của mình, giải mã chữ ký bằng khoá công khai của người gửi để lấy "*Đại diện*" ra.

* Cho thông điệp qua hàm băm để tạo ra "*Đại diện*" mới.

* So sánh "*Đại diện*" mới với "*Đại diện*" nhận được.

Nếu chúng giống nhau thì người nhận có thể vừa *định danh* được người gửi, vừa *kiểm tra tính toàn vẹn* của thông điệp.

Chứng chỉ số.



Việc sử dụng mã hóa hay ký số chỉ giải quyết được vấn đề bảo mật và xác thực thông điệp. Tuy nhiên "khó" thể đảm bảo rằng người ký là đối tác thật. Trong nhiều trường hợp cần thiết phải "*chứng minh*" bằng phương tiện điện tử *danh tính* của ai đó. Ví dụ phải "*chứng minh*" rằng người người ký là "*chủ đích thực*" *hiện thời* của chìa khóa ký.

Một cách giải quyết là dùng "*Chứng chỉ số*" để xác nhận "*chủ đích thực*" *hiện thời* của khóa công khai.

Chứng chỉ số là một tệp tin điện tử dùng để *nhận diện* một cá nhân, một máy dịch vụ, một thực thể nào đó. Nó gắn định danh của đối tượng đó với một khóa công khai, giống như bằng lái xe, hộ chiếu, chứng minh thư.

Chứng chỉ số là kết quả của dự án phát triển chuẩn thư mục X.500 của ITU-T phát triển vào cuối những năm thập niên 90. Chứng chỉ số được ITU-T đặc tả trong tài liệu X.509 và dần được thay đổi qua các phiên bản cho phù hợp với thực tế. Hiện nay Chứng chỉ X.509 phiên bản 3 được sử dụng trong các hệ thống xác thực.

Một nơi có thể chứng nhận các thông tin của một thực thể là đúng, nó được gọi là cơ quan *xác thực chứng chỉ* (Certificate Authority - CA). Đó là một đơn vị có thẩm quyền xác nhận định danh và cấp các chứng chỉ số. CA có thể là một đối tác thứ ba độc lập hoặc tổ chức tự vận hành một hệ thống tự cấp các chứng chỉ cho nội bộ.

Các phương pháp để xác định định danh phụ thuộc vào các chính sách mà CA đặt ra. Chính sách lập ra phải đảm bảo việc cấp chứng chỉ số phải đúng đắn, ai được cấp và mục đích dùng vào việc gì. Thông thường, trước khi cấp một chứng chỉ số, CA sẽ công bố các thủ tục cần thiết phải thực hiện cho các loại chứng chỉ số.

Chứng chỉ số chứa khóa công khai, được gắn với một tên duy nhất của một đối tượng (như tên của một cá nhân hay máy dịch vụ). Chứng chỉ số giúp ngăn chặn việc sử dụng khóa công khai cho việc giả mạo. Chỉ có khóa công khai được chứng thực bởi chứng chỉ số sẽ làm việc với khóa bí mật tương ứng. Nó được sở hữu bởi đối tượng với định danh đã được ghi trong chứng chỉ số.

Ngoài khóa công khai, chứng chỉ số còn chứa thông tin về đối tượng như tên mà nó nhận diện, hạn dùng, tên của CA cấp chứng chỉ số, mã số … *Quan trọng nhất* là chứng chỉ số phải có "*chữ ký số*" của CA đã cấp chứng chỉ đó. Giống như chứng chỉ đã được "*đóng dấu*", để cho người dùng khóa công khai có thể kiểm tra.

Một người muốn sử dụng Hệ mã hóa khóa công khai để mã hóa thông báo và gửi cho người nhận, người gửi phải có bản sao khóa công khai của người nhận.

Một người muốn kiểm tra chữ ký số của người khác, họ phải có bản sao khóa công khai của người ký.

Chúng ta gọi cả hai thành viên (mã hóa thông báo và kiểm tra chữ ký số) là những người sử dụng khóa công khai.

Khi khóa công khai được gửi đến người sử dụng khóa công khai, thì không cần thiết phải giữ bí mật khóa công khai này. Tuy nhiên, người sử dụng khóa công khai phải đảm bảo rằng khóa công khai được sử dụng đúng là của đối tác. Nếu kẻ phá hoại dùng khóa công khai khác thay thế cho khóa công khai hợp lệ, thì nội dung thông báo đã mã hóa có thể bị lộ, chữ ký số có thể bị làm giả.

Rõ ràng khóa công khai *cần phải được xác thực trước khi dùng*.

Đối với nhóm thành viên nhỏ, yêu cầu trên có thể được thỏa mãn dễ dàng. Ví dụ trường hợp hai người quen biết nhau, khi người này muốn truyền thông an toàn với người kia, họ có thể có được bản sao khóa công khai của nhau bằng cách trao đổi các đĩa nhớ có ghi các khóa công khai của từng người. Như vậy đảm bảo rằng các khóa công khai được lưu giữ an toàn trên mỗi hệ thống cục bộ của từng người. Đây chính là hình thức *phân phối khóa công khai thủ công*.

Phân phối khóa công khai thủ công như trên là không thực tế hoặc không thỏa đáng khi số lượng người dùng là quá lớn và nơi làm việc phân tán. Hệ thống cấp chứng chỉ khóa công khai giúp cho việc phân phối khóa công khai có hệ thống và chuẩn mực.

** Hệ thống cấp chứng chỉ khóa công khai*

CA phát hành các chứng chỉ cho những người nắm giữ cặp khóa công khai và khóa riêng. Chứng chỉ gồm có khóa công khai và thông tin dùng để nhận dạng duy nhất chủ thể (subject) của chứng chỉ. Chủ thể của chứng chỉ có thể là một người, thiết bị, hoặc một thực thể có nắm giữ khóa riêng tương ứng. Khi chủ thể của chứng chỉ là một người hoặc một thực thể nào đó, chủ thể thường được nhắc đến như là một thực thể (subscriber) của CA. Các chứng chỉ được CA ký, bằng khóa riêng của CA.

Một khi các chứng chỉ số được thiết lập, công việc của người sử dụng khóa công khai rất đơn giản. Giả thiết rằng, họ đã có khóa công khai của CA một cách bí mật (ví dụ: thông qua phân phối khóa công khai thủ công) và tin cậy CA phát hành các chứng chỉ hợp lệ. Nếu người dùng cần khóa công khai của một thuê bao nào đó của CA, anh ta có thể thu được khóa công khai của thuê bao bằng cách tìm trong bản sao chứng chỉ của họ, lấy ra khóa công khai. Tất nhiên trước đó anh ta phải kiểm tra chữ ký trên chứng chỉ có đúng là của CA không.

Hệ thống cấp chứng chỉ như trên là đơn giản và kinh tế khi được thiết lập trên diện rộng và tự động, bởi vì một trong các đặc tính quan trọng của chứng chỉ là: "Các chứng chỉ có thể được phát hành mà không cần phải bảo vệ thông qua các dịch vụ an toàn truyền thông để đảm bảo xác thực và toàn vẹn".

Chúng ta không cần giữ bí mật khóa công khai, như vậy chứng chỉ không phải là bí mật. Hơn nữa, ở đây không đòi hỏi các yêu cầu về tính xác thực và toàn vẹn do *các chứng chỉ tự bảo vệ*. Chữ ký của CA trong chứng chỉ đã cung cấp tính xác thực và toàn vẹn. Người dùng khóa công khai trong các chứng chỉ như trên được gọi là thành viên tin cậy.

Kẻ truy nhập trái phép định làm giả chứng chỉ khi chứng chỉ này đang lưu hành cho những người sử dụng khóa công khai, họ sẽ phát hiện ra việc làm giả, bởi vì chữ ký của CA có thể được kiểm tra chính xác. Chính vì thế các chứng chỉ khóa công khai được phát hành theo cách không an toàn, ví dụ như thông qua các máy chủ, các hệ thống thư mục, các giao thức truyền thông không an toàn.

Lợi ích cơ bản của hệ thống cấp chứng chỉ là: người sử dụng khóa công khai có được số lượng lớn các khóa công khai của nhiều người dùng một cách tin cậy, nhờ khóa công khai của CA. Lưu ý rằng chứng chỉ số chỉ có nghĩa khi CA phát hành các chứng chỉ hợp lệ.

3.2.2.2. *Công nghệ và giao thức thử nghiệm phần kỹ thuật của PKI*

Nội dung nghiên cứu

+ Công nghệ OpenCA.
+ Công nghệ SSL.
+ Giao thức truyền tin an toàn tầng liên kết dữ liệu.
+ Giao thức truyền tin an toàn tầng ứng dụng.

Công nghệ OpenCA.

OpenCA là dự án đồ sộ, có mục đích xây dựng PKI hoàn chỉnh, chuyên nghiệp, OpenCA được phát triển liên tục từ năm 1999. Từ năm 2001, OpenCA đã bắt đầu được sử dụng cho các đơn vị cỡ vừa và lớn.

OpenCA sử dụng giao diện web, hỗ trợ hầu hết các web Browser chính, hỗ trợ sản phẩm mã nguồn mở.

* Các Module chương trình trong OpenCA.

- *Giao tiếp công cộng*: Giao diện web để người sử dụng có thể truy cập qua Internet. Người dùng có thể *đăng kí xin cấp chứng chỉ* trực tiếp qua Module này.
- *Giao tiếp LDAP*: *Danh bạ các khoá công khai*, người dùng lấy khoá công khai từ Module này để mã hoá tài liệu, trước khi gửi đến đơn vị dùng openCA.
- *Giao tiếp RA*: Đơn vị điều hành RA sử dụng Module này để cập nhật các thông tin cá nhân của *người xin cấp chứng chỉ*.
- *Giao tiếp OCSP*: Module hỗ trợ *kiểm tra chứng chỉ* còn hiệu lực hay không. OCSP có tác dụng như việc công bố CRL, nhưng tính năng ưu việt hơn CRL.
- *Giao tiếp CA*: *Module kí số* riêng rẽ, cho phép CA làm theo nguyên tắc an ninh - tách biệt khỏi mạng công cộng, để bảo vệ tối đa khoá bí mật. Điều này khiến cho openCA trở nên an toàn hơn các phần mềm CA khác có trên thị trường hiện nay.

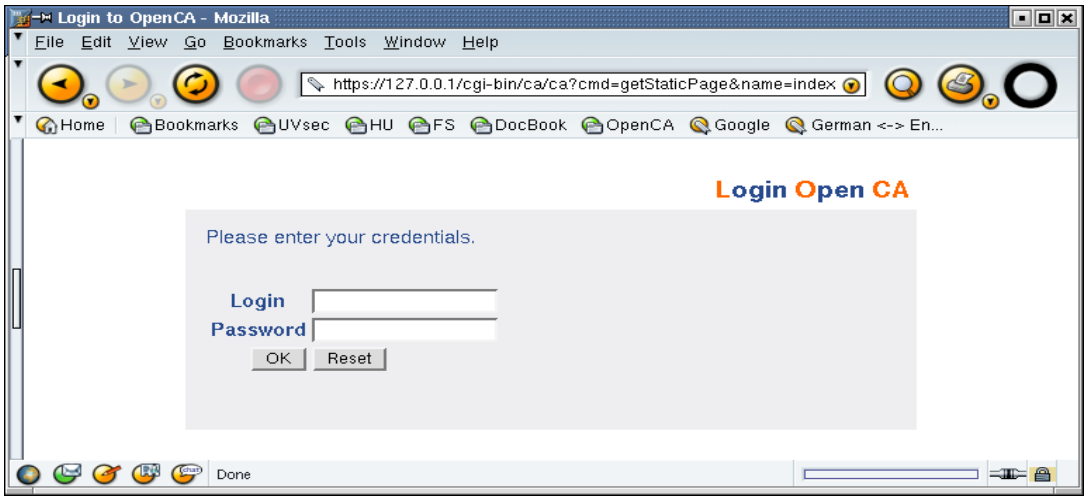
** Các tính năng ưu việt khác của OpenCA, ngoài tính năng thiết yếu của PKI.*

- Đăng nhập bằng chứng chỉ.
- Hệ thống quản lý mềm dẻo.
- Sử dụng được các tính năng của X.509 mở rộng.
- OpenCA là phần mềm mã nguồn mở miễn phí, có tài liệu chi tiết đầy đủ.

OpenCA được thiết kế cho một hạ tầng phân tán. Nó có thể không chỉ điều khiển một CA offline và một RA online, mà còn giúp ta xây dựng một cấu trúc thứ bậc với nhiều mức khác nhau. OpenCA không phải là một giải pháp nhỏ cho các nghiên cứu vừa và nhỏ. Nó hỗ trợ tối đa cho các tổ chức lớn như các trường đại học, các công ty lớn.

** Các vấn đề chính trong công nghệ OpenCA.*

- Thiết kế, cài đặt một hạ tầng.
- Các hoạt động được thực hiện một cách offline bởi người quản trị.
- Các thao tác phía người dùng.
- Các mô tả kỹ thuật của OpenCA.



Đăng nhập OpenCA

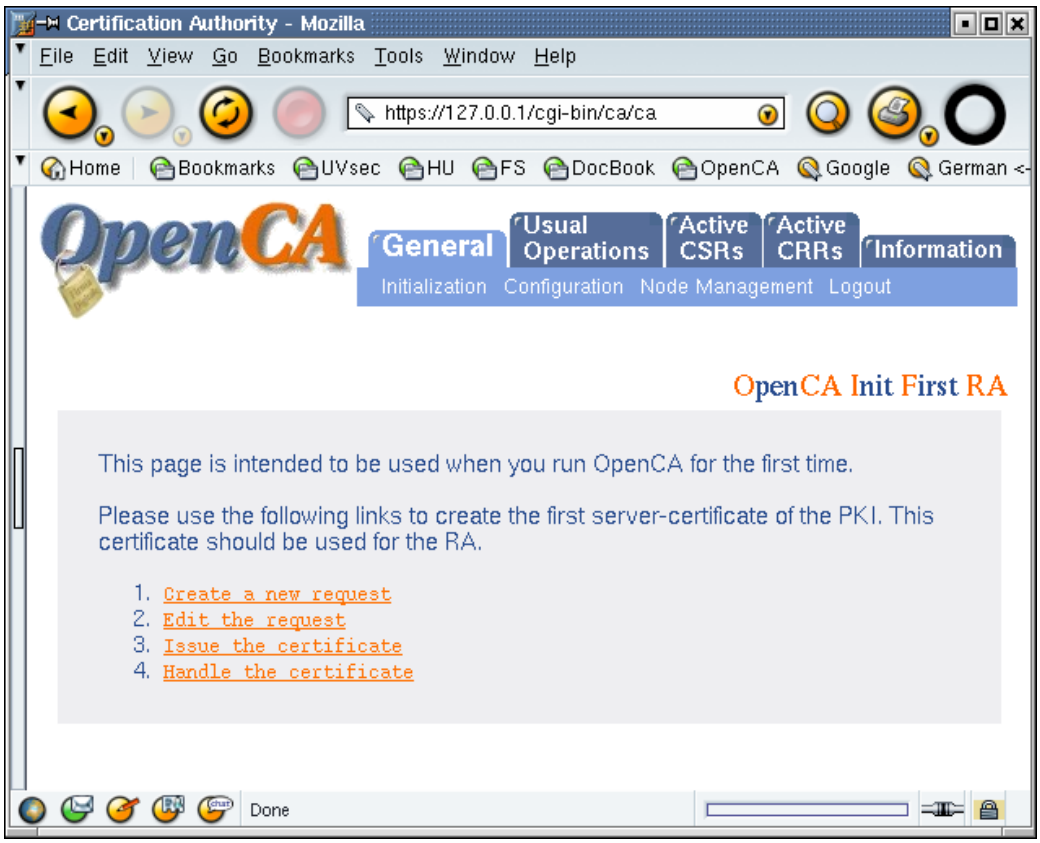
Sử dụng OpenCA


Certification Authority - Mozilla
File Edit View Go Bookmarks Tools Window Help
https://127.0.0.1/cgi-bin/ca/ca
Home Bookmarks UVsec HU FS DocBook OpenCA Google German <-> En...
OpenCA
General
Usual Operations
Active CSRs
Active CRRs
Information
Initialization Configuration Node Management Logout
Please use one of the following links. WATCH OUT, you can delete the CA secret key that will be impossible to recover, so be careful and know what you are going to do.
Please note that the dB initialization is required only once just after CA installation.
DB Setup
Initialize Database
Key pair Setup
Generate new CA secret key
Request Setup
Generate new CA Certificate Request (use generated secret key)
Certificate Setup
Selfsigned CA-Certificate
Generate Self Signed CA Certificate (from altready generated request)
Signed by another CA
Export CA Certificate Request
Import CA certificate (approved by Root CA)
Final Setup
Rebuild CA Chain
Export Configuration
Done

Bước 1


Certification Authority - Mozilla
File Edit View Go Bookmarks Tools Window Help
https://127.0.0.1/cgi-bin/ca/ca
Home Bookmarks UVsec HU FS DocBook OpenCA Google German <-
OpenCA
General
Usual Operations
Active CSRs
Active CRRs
Information
Initialization Configuration Node Management Logout
OpenCA Init First User
This page is intended to be used when you run OpenCA for the first time.
Please use the following links to create the first user of the PKI. This user should be an administrator.
1. Create a new request
2. Edit the request
3. Issue the certificate
4. Handle the certificate
Done

Bước 2


Certification Authority - Mozilla
File Edit View Go Bookmarks Tools Window Help
https://127.0.0.1/cgi-bin/ca/ca
Home Bookmarks UVsec HU FS DocBook OpenCA Google German
OpenCA
General
Usual Operations
Active CSRs
Active CRRs
Information
Initialization Configuration Node Management Logout
OpenCA Init First RA
This page is intended to be used when you run OpenCA for the first time.
Please use the following links to create the first server-certificate of the PKI. This certificate should be used for the RA.
1. Create a new request
2. Edit the request
3. Issue the certificate
4. Handle the certificate
Done

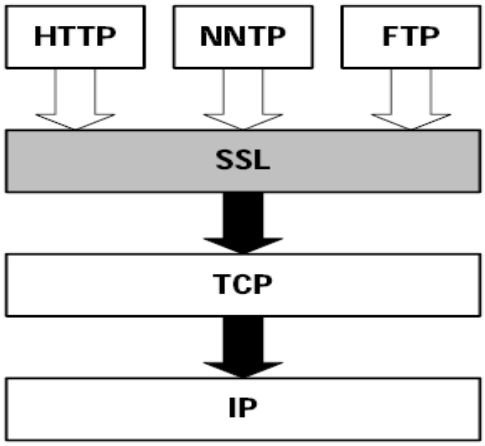
Bước 3

Công nghệ SSL.

SSL là *giao thức đa mục đích*, được thiết kế để tạo ra các giao tiếp giữa hai chương trình ứng dụng trên một cổng định trước (Socket 443), nhằm mã hoá toàn bộ thông tin gửi / nhận. Giao thức SSL được hình thành và phát triển đầu tiên năm 1994 bởi nhóm nghiên cứu Netscape, dẫn dắt bởi Elgamal và nay đã trở thành chuẩn bảo mật cài đặt trên Internet.

SSL được thiết kế độc lập với tầng ứng dụng, để đảm bảo tính bí mật, an toàn và chống giả mạo luồng thông tin qua Internet giữa hai ứng dụng bất kỳ, thí dụ giữa Webserver và các trình duyệt (Browsers), do đó được sử dụng rộng rãi trong nhiều ứng dụng khác nhau trên môi trường Internet.

Toàn bộ cơ chế và hệ thống thuật toán mã hoá trong SSL được phổ biến công khai, trừ khoá phiên (Session key) được sinh ra tại thời điểm trao đổi giữa hai ứng dụng là ngẫu nhiên và bí mật đối với người quan sát trên mạng máy tính. Ngoài ra, giao thức SSL còn đòi hỏi người dùng phải được chứng thực bởi đối tượng thứ ba (CA) thông qua chứng chỉ số (Digital Certificate) dựa trên mật mã công khai (ví dụ RSA).



Vị trí SSL trong mô hình OSI

SSL được thiết kế như là một giao thức riêng cho vấn đề bảo mật, có thể hỗ trợ cho nhiều ứng dụng. Giao thức SSL hoạt động bên trên TCP / IP và bên dưới các ứng dụng tầng cao hơn như là HTTP (HyperText Transfer Protocol), LDAP (Lightweight Directory Access Protocol) hoặc IMAP (Internet Messaging Access Protocol). Hiện nay SSL được sử dụng chủ yếu cho các giao dịch trên Web.

SSL cho phép một Server (có hỗ trợ SSL) tự xác thực với một Client (cũng hỗ trợ SSL), ngược lại cho phép Client tự xác thực với Server. SSL cho phép cả hai máy thiết lập một kết nối được mã hoá.

* Chứng thực SSL Server: cho phép Client xác thực được Server muốn kết nối. Trình duyệt sử dụng kỹ thuật mã hóa công khai để chắc chắn rằng chứng chỉ và public ID của Server là có giá trị, được cấp phát bởi một CA (trong danh sách các CA tin cậy của Client).

* Chứng thực SSL Client: cho phép Server xác thực được Client muốn kết nối. Server cũng sử dụng kỹ thuật mã hoá khoá công khai để kiểm tra chứng chỉ của Client và public ID là đúng, được cấp phát bởi một CA.

* Mã hoá kết nối: tất cả các thông tin trao đổi giữa Client và Server được mã hoá trên đường truyền, nhằm nâng cao khả năng bảo mật. Điều này rất quan trọng đối với cả hai bên, khi có các giao dịch mang tính riêng tư. Ngoài ra, tất cả các dữ liệu được gửi đi trên một kết nối SSL đã được mã hoá, còn được bảo vệ nhờ cơ chế tự động phát hiện các xáo trộn, thay đổi trong dữ liệu.

** Hai tầng trong Giao thức SSL.*

Record Protocol là tầng thấp nhất của SSL Nó được dùng để *đóng gói* một số giao thức ở mức cao hơn. Một trong những giao thức được đóng gói là SSL

Handshake Protocol là giao thức cho phép Server và Client *xác thực* lẫn nhau. Chúng thoả thuận thuật toán mã hoá và các khoá mật mã trước khi thực hiện gửi hoặc nhận dữ liệu.

** Thách thức về khóa bảo mật của SSL.*

Trong cộng đồng những người làm bảo mật, một trong các phương pháp để kiểm tra độ an toàn của các thuật toán bảo mật, ngoài cơ sở lý thuyết của thuật toán, là đưa ra các "*thách thức*" (Challenge) với số tiền thưởng tượng trưng, nhằm kiểm tra tính thực tiễn của thuật toán. Sau đây là một số thông tin tham khảo:

* Ngày 14 / 7 / 1995, Hal Finney đặt một thách thức SSL đầu tiên một bản ghi phiên làm việc của trình duyệt Netscape dùng thuật toán RC4-128-EXPORT-20. Ngày 16 / 8 / 1995, David Byers, Eric Young, Adam Back đã phá thách thức này trong vòng 2 giờ, chi phí ước tính 10,000 USD.

* Ngày 19 / 8 / 1995, Hal Finney đặt một thách thức SSL thứ hai cho cộng đồng những người làm mật mã một "*Key Cracking Ring*". Sau đó bị phá trong 32 giờ.

* Ngày 17 / 9 / 1995, Ian Goldberg và David Wagner đã phá được thuật toán sinh số giả ngẫu nhiên (cơ sở cho việc sinh ra số nhận dạng phiên SSL - session ID) của phiên bản Netscape 1.1 trong vòng vài giờ trên một máy trạm. Điều này dẫn đến việc Netscape phải nhanh chóng đưa ra phiên bản để sửa "lỗ hổng" của bảo mật trong trình duyệt của mình. Hiện nay phiên bản mới nhất của Netscape có khả năng bảo mật an toàn cao nhưng chỉ được phép dùng trong phạm vi nước Mỹ.

** Ưu điểm và hạn chế của SSL.*

Ưu điểm:

Tính năng mạnh nhất của SSL / TLS là chúng *xác định được mối quan hệ với các tầng giao thức khác* trong hệ thống kiến trúc mạng OSI. Tại mức cao nhất là phần mềm ứng dụng hoặc các trình duyệt. Chạy phía dưới các ứng dụng này là giao thức tầng ứng dụng, bao gồm Telnet, FTP, HTTP…Bên dưới nữa là giao thức SSL và các thuật toán mã hoá được sử dụng để kết nối. Bên dưới SSL là tầng giao vận. Hầu hết các trường hợp đó là TCP / IP.

Giao thức SSL là duy nhất *không phụ thuộc vào giao thức mạng*. SSL không phụ thuộc vào các tầng giao thức, cho nên SSL trở thành một nền tảng độc lập hay là một thực thể mạng độc lập.

Giao thức SSL *ngăn chặn cách thức tấn công từ điển*. Cách thức này sử dụng từ điển để phá khoá trong hệ mã hoá. SSL khắc phục được điều này bởi cho phép không gian khoá là rất lớn đối với hệ mã hoá được sử dụng. SSL cung cấp hai mức độ tin cậy: 40 bit và 128 bit tuỳ thuộc khả năng của browser. SSL 128 bit và SSL 40 bit: ý nói độ dài của khoá phiên dùng để mã hoá dữ liệu sau khi đã định danh và được thiết lập bằng giải thuật mã hóa khoá công khai (RSA hoặc Diffie-Hellman). Độ dài của khoá phiên càng lớn thì độ bảo mật càng cao. SSL 128 bit có độ tin cậy lớn, theo RSA phải mất hàng tỉ năm mới có thể giải mã được bằng các kỹ thuật hiện nay. Cách thức tấn công từ điển có thể bị ngăn chặn bởi sử dụng phương pháp số nonce (nonce number). Số này được sinh ngẫu nhiên, được Server sử dụng, *nonce number* là một số không thể bị phá khoá.

Giao thức SSL *bảo vệ chính nó* với đối tác thứ 3. Đó là các Client xâm nhập bất hợp pháp dữ liệu trên đường truyền. Client xâm nhập này có thể giả mạo Client hoặc Server, SSL ngăn chặn giả mạo này bằng cách dùng khoá riêng của Server và sử dụng chứng chỉ số. Phương thức "Bắt tay" trong TLS cũng tương tự. Tuy nhiên, TLS tăng cường sự bảo mật bằng cách cho phép truyền phiên bản giao thức, số hiệu phiên làm việc, hệ mã hoá và cách thức nén được sử dụng. TLS bổ xung thêm hai thuật toán "băm" không có trong SSL.

Hạn chế:

Giao thức SSL, giống như bất kỳ công nghệ nào, cũng có những hạn chế. Vì SSL cung cấp các dịch vụ bảo mật, ta cần quan tâm tới các giới hạn của nó.*Giới hạn của SSL* thường nằm trong ba trường hợp sau:

Đầu tiên là do những ràng buộc cơ bản của bản thân giao thức SSL. Đây là hệ quả của việc thiết kế SSL và ứng dụng chịu sự tác động của nó. Thứ hai là giao thức SSL cũng thừa kế một vài điểm yếu từ các công cụ mà nó sử dụng, cụ thể là các thuật toán ký và mã hoá. Nếu các thuật toán này sẵn có điểm yếu, SSL cũng không thể khắc phục chúng. Thứ ba là các môi trường, trong đó SSL được triển khai cũng có những thiếu sót và giới hạn.

Mặc dù trong thiết kế của nó đã xét đến mối quan hệ với rất nhiều ứng dụng khác nhau, SSL rõ ràng được tập trung vào việc bảo mật các giao dịch Web. SSL yêu cầu một giao thức vận chuyển tin cậy như TCP. Đó là yêu cầu hoàn toàn hợp lý trong các giao dịch Web, vì bản thân HTTP cũng yêu cầu TCP. Tuy nhiên, điều này cũng có nghĩa là SSL *không thể thực thi* mà sử dụng một giao thức vận chuyển *không kết nối* như UDP. Vì vậy, giao thức SSL có thể hoạt động hiệu quả với phần lớn các ứng dụng thông thường. Và thực tế là hiện nay SSL đang được sử dụng cho rất nhiều ứng dụng bảo mật, bao gồm truyền file, đọc tin trên mạng, điều khiển truy cập từ xa...

SSL *bị lỗi* khi hỗ trợ dịch vụ bảo mật đặc biệt là "*non-repudiation"* (không thể chối bỏ). Non-repudiation kết hợp chữ ký số tương ứng với dữ liệu, khi được sử dụng một cách hợp lý, nó ngăn ngừa bên tạo và ký dữ liệu từ chối hay phủ nhận điều đó. Giao thức SSL *không cung cấp* các *dịch vụ "non-repudiation*", do đó sẽ không phù hợp với các ứng dụng yêu cầu dịch vụ này.

SSL có *phiên làm việc tồn tại quá lâu* trong quá trình "Bắt tay", khoá phiên được khởi tạo giữa Client và Server sử dụng trong suốt quá trình kết nối. Khi khoá này còn tồn tại, mỗi khi thông điệp được gửi, xuất hiện *lỗ hổng bảo mật* trong kết nối, cho phép kẻ lạ xâm nhập. Giao thức TLS khắc phục được lỗi này bằng cách thay đổi khoá cho mỗi phiên làm việc.

Các giao tiếp thực giữa Client và Server cũng là mục tiêu tấn công bởi chúng lưu trữ các thông điệp giữa hai điểm đầu cuối. Thông điệp trong SSL được mã hoá, tuy nhiên tại mỗi điểm đầu cuối thông điệp được giải mã, SSL *không có cơ chế duy trì sự mã hoá* trong bộ nhớ đệm của hệ thống tương ứng.

Hạn chế khác nữa của SSL là *khả năng sử dụng khóa mã hóa*. Mặc dù một vài Client tại các nước khác có hỗ trợ SSL, nhưng vẫn có hạn chế về ranh giới khi mã hoá. Ranh giới này do chính phủ Mỹ đưa ra, giới hạn số lượng bit được sử dụng trong các hệ mã hoá. SSL có hỗ trợ mã hoá 128 bit trong các phiên giao dịch toàn cầu, nhưng thực tế chỉ được sử dụng hệ mã hoá 40 bit. Các hạn chế này càng cho phép kẻ tấn công có nhiều cơ hội hơn khi tìm cách bẻ khoá hệ thống.

Một vài ý kiến cho rằng hạn chế lớn nhất của SSL không chỉ ở giao thức "Bắt tay" , mà còn tồn tại trong giao thức "Bản ghi" . Trong quá trình "Bắt tay", việc xác thực giữa Client và Server được thực hiện rất nghiêm ngặt do sử dụng chứng chỉ số khoá công khai. Tuy nhiên, trong tầng "Bản ghi", việc *xác thực không được thực hiện* trong giai đoạn kết nối còn lại, do đó kẻ phá hoại có thể mạo danh Client hoặc Server trong quá trình kết nối.

Nhiều ý kiến cho rằng SSL chỉ giới hạn với các ứng dụng thương mại điện tử. Điều này là không đúng. Các tổ chức tài chính có thể sử dụng SSL để truyền số PIN. Các công ty bảo hiểm sử dụng SSL để truyền dữ liệu cho khách hàng.

Giao thức truyền tin an toàn tầng liên kết dữ liệu (DataLink).

Trong mô hình OSI, tầng liên kết dữ liệu là tầng đầu tiên có thể can thiệp vào được bằng phần mềm (thông qua trình điều khiển thiết bị của hệ điều hành). Vì vậy, nó đáng được khảo sát trước tiên - để đảm bảo an toàn thông tin ở mức thấp nhất. Tất nhiên tầng vật lý trong mô hình OSI còn thấp hơn, nhưng nhìn chung nó nằm ngoài phạm trù của mật mã học, vì mật mã học với mục đích đảm bảo an toàn thông tin trong trường hợp thông tin đã bị truy cập trái phép ở mức vật lý.

Trong mạng riêng của một tổ chức, đại đa số kết nối ở tầng liên kết dữ liệu đều dùng chuẩn Ethernet, hoặc tương thích Ethernet, nên chuyên đề này tập trung vào Ethernet như đại diện của tầng liên kết dữ liệu.

** Các nguy cơ đe dọa an toàn truyền tin trên mạng Ethernet.*

- MAC flooding

Mỗi Switch có bộ nhớ để lưu trữ danh sách các địa chỉ MAC tương ứng với mỗi cổng của Switch. Kẻ tấn công có thể tạo ra nhiều địa chỉ MAC giả, vượt quá giới hạn cho phép của Switch, khiến cho nó phải quảng bá (Broadcast) mọi thông tin tới tất cả các cổng thay vì chỉ gửi đến đúng cổng cần gửi. Như vậy kẻ phá hoại có thể nghe trộm toàn bộ thông tin gửi trên mạng Ethernet.

- Port stealing

Kẻ tấn công nhận địa chỉ MAC trùng với địa chỉ của nạn nhân, do đó thông tin có thể không được gửi tới nạn nhân, mà lại gửi cho kẻ tấn công.

- ARP spoofing

Gói tin ARP giả mạo có thể sửa đổi bảng quy đổi giữa địa chỉ tầng mạng và địa chỉ tầng liên kết dữ liệu – sửa đổi hoàn toàn theo ý của kẻ tấn công. Như vậy, thông tin tầng mạng có thể bị trung chuyển cho kẻ tấn công, trước khi tới người nhận, Đó là hình thức tấn công nguy hiểm - MITM.

** Các giải pháp an ninh cho mạng Ethernet.*

- Switch thông minh

Các Switch thông minh có khả năng hiểu các Header của dữ liệu đi qua và có thể điều khiển các hoạt động từ xa. Nếu được chỉnh cấu hình phù hợp, các Switch này có thể ngăn chặn hoàn toàn các cuộc tấn công kiểu MAC flooding và Port stealing. Những cuộc tấn công loại này chỉ có thể ngăn chặn được bằng cách đó. Vì thế, muốn mạng Ethernet được an toàn, sử dụng các Switch thông minh là điều bắt buộc.

- Phần mềm bảo vệ

Các Switch dù cao cấp đến mức nào cũng không đủ để hoàn thiện an ninh cho mạng Ethernet. Nguyên nhân là có các thông tin được giữ riêng ở Client, các Switch không nắm được các thông tin này. Hơn nữa, sau này IPSec được áp dụng rộng rãi thì các thông tin đều được mã hóa trước khi truyền đi và Switch sẽ không có cách nào phân tích được những dữ liệu từ tầng mạng trở lên. Ví dụ như khi bảo vệ ARP tại Switch, thiết bị lọc các gói ARP trái phép cần phải hiểu được sự phân bổ địa chỉ IP động trong giao thức DHCP. Khi giao thức này được mã hóa qua IPSec thì Switch sẽ có được thông tin cần thiết để phân biệt gói ARP trái phép với gói ARP hợp lệ.

Vì vậy, bên cạnh Switch thông minh, triển khai các hệ thống phần mềm bảo vệ trên các máy trạm cũng là điều bắt buộc.

** An ninh cho giao thức ARP.*

Giao thức ARP có thể xem là thành phần cơ bản cấp thấp nhất của mạng Internet. ARP được hoàn thành từ năm 1982 và công bố trong RFC-826. Trong 20 năm qua, ngành công nghệ thông tin đã thay đổi rất nhiều. Các phần mềm "khai thác lỗi" ra đời, khiến các điểm yếu tiềm ẩn trong ARP trở nên cực kì nguy hiểm. Giao thức ARP đã trở thành miếng mồi ngon cho tin tặc khai thác.

Hiện nay chỉ tồn tại duy nhất một giải pháp, đó là các Switch mới của Cisco. Nó được quảng cáo là có thể ngăn chặn được một phần các cuộc tấn công vào ARP, nếu toàn mạng triển khai việc phân phối địa chỉ IP qua DHCP. Tuy nhiên trong các mạng LAN không dùng DHCP thì giải pháp này không thực hiện được. Hơn nữa, giải pháp này không tương thích với IPSec, hạn chế việc xiết chặt hơn nữa an ninh mạng khi cần thiết. Vì vậy, để đảm bảo an ninh Ethernet, ta phải *cải tiến giao thức ARP* chứ không thể tiếp tục chung sống với một giao thức không an toàn.

Trong các phương án cải tiến ARP, có phương án đáng quan tâm, là công trình được tài trợ bởi Bộ Giáo Dục và Nghiên Cứu Italia, mang tên "S-ARP: a Secure Address Resolution Protocol" (http://www.acsac.org/2003/papers/111.pdf). Tuy nhiên giao thức được đề xuất trong sơ đồ này có điểm không hợp lý, dẫn đến hiệu suất tính toán thấp, hơn nữa, lại không được chuẩn hóa vào một hạ tầng mật mã nào, nên ít có khả năng được đưa vào ứng dụng.

Một phương án mới được đề xuất - Committed Address Resolution Protocol (http://selab.edu.ms/). Đây là phương án nâng cấp ARP hiệu quả hiện nay. Hơn nữa, CARP còn sử dụng X.509, phù hợp với PKI mà đề tài lựa chọn. Phương án này không cần người gửi ký vào thông điệp mỗi khi gửi đi, mà người chịu trách nhiệm cho mạng Ethernet sẽ tạo sẵn một văn bản xác thực, cho phép 1 địa chỉ vật lý sử dụng 1 địa chỉ mạng trong thời gian nhất định, tuỳ chọn. Văn bản xác thực này được tái sử dụng suốt trong thời gian đó, giảm nhu cầu tính toán, cho phép một máy có thể trả lời thay các máy khác khi cần thiết, rất hữu dụng cho các thiết bị chưa kịp nâng cấp từ ARP thông thường lên CARP. Điều này khiến cho việc triển khai CARP dễ dàng hơn.

Giao thức truyền tin an toàn tầng ứng dụng (Application).

Tầng ứng dụng là tầng cao nhất theo mô hình OSI, các ứng dụng sử dụng dịch vụ do các tầng dưới cung cấp, vì thế được thừa kế tất cả đặc tính an toàn của các tầng dưới. Nếu kẻ tấn công không thể phá mã được tầng dưới, thì dữ liệu của các tầng trên cũng được đảm bảo.

Vì tính thừa kế, nên hầu hết các ứng dụng chỉ cần sử dụng giao thức TLS bên dưới, là việc truyền tin tầng ứng dụng đã trở nên an toàn:

* Các ứng dụng trao đổi với nhau bằng địa chỉ IP: CARP kết hợp với IPSec đủ để đảm bảo an toàn truyền tin cho ứng dụng.

* Các ứng dụng trao đổi với nhau bằng tên miền: kết hợp CARP và SSL, hoặc kết hợp CARP, IPSec và DNSSEC, đủ đảm bảo an toàn truyền tin cho ứng dụng.

Vì có thể tận dụng các giao thức thấp hơn, nên hầu hết các giao thức truyền tin tầng ứng dụng không áp dụng mật mã vào bảo vệ, mà đơn giản là yêu cầu các giao thức tầng thấp hơn phải sử dụng mật mã.

Cũng có ngoại lệ trong các trường hợp sau, giao thức truyền tin tầng ứng dụng không thừa kế được những đặc tính an toàn của các giao thức tầng thấp hơn:

* Ứng dụng có nhu cầu "Quảng bá" (Broadcast): Ứng dụng cần phải gửi thông điệp quảng bá, vì không mã hoá thông điệp quảng bá nên kẻ tấn công có thể đọc được thông điệp. Khi quảng bá, ứng dụng không biết trước ai có thẩm quyền trả lời thông điệp, nên kẻ tấn công có thể tự nhận là người có thẩm quyền.

Trường hợp này xảy ra ở các giao thức tự động như DHCP, Router Discovery...

* Ứng dụng có nhu cầu "Tiếp sức" (Relay): Thông điệp cần phải trung chuyển qua các trạm trước khi đến đích. Ứng dụng có thể dựa vào các tầng dưới để đảm bảo thông điệp được chuyển an toàn đến trạm trung chuyển, nhưng nếu trạm trung chuyển bị kẻ tấn công kiểm soát, thì thông điệp sẽ bị lộ. Trường hợp này xảy ra ở các giao thức như DHCP, Email...

Bảo vệ DHCP

Hiện nay dự án Ethsec có đề xuất về việc ứng dụng mật mã khoá công khai để bảo vệ DHCP, nhưng chưa được chuẩn hoá nên tạm thời chưa triển khai được

Bảo vệ các giao thức Router Discovery

Hiện nay chưa có biện pháp bảo vệ bằng mật mã khoá công khai, nếu muốn đảm bảo an ninh, người vận hành mạng có thể cấu hình bằng tay các bộ định tuyến thay vì sử dụng các giao thức tự động.

Bảo vệ E-mail

SMTP là giao thức truyền thư điện tử được sử dụng để vận chuyển các Email trên thế giới. SMTP phải dùng các trạm trung chuyển để gửi thư, nên các tầng bảo vệ bên dưới không thể đảm bảo an toàn việc truyền Email.

Thế giới đang sử dụng đồng thời 2 phương thức đảm bảo an toàn cho Email là PGP và S/MIME. PGP không sử dụng X.509 nên ta chỉ quan tâm đến S/MIME.

S/MIME

PKI và S/MIME giúp cho người dùng dễ dàng phát hiện được sự giả mạo thư điện tử. S/MIME có 2 vấn đề tách rời là kí và mã hoá.

Người gửi có thể kí thông điệp bằng khoá riêng của họ, mọi người đều có thể biết được bức thư không bị mạo danh bởi một kẻ khác.

Người gửi có thể mã hoá thông điệp bằng khoá công khai của người nhận, do đó chỉ đích thân người nhận mới có thể đọc được thông điệp đó.

Phương pháp thực hiện

- Thu thập và nghiên cứu tài liệu.
- Nghiên cứu giải pháp công nghệ: tìm hiểu các công nghệ để xây dựng hệ thống, kiến trúc bảo mật mạng theo các chuẩn chung trên thế giới, các phần mềm mã nguồn mở sẵn có.
- Thử nghiệm các phần mềm khác nhau để có sự so sánh và đánh giá.
- Xemina trao đổi nhằm đánh giá các công cụ, giúp cho việc lựa chọn giải pháp được chính xác và hợp lý.

Kết quả: 4 báo cáo chuyên đề:

- Công nghệ OpenCA
- Công nghệ SSL
- Giao thức ARP (tầng DataLink)
- Giao thức S/MIME (tầng Application)

3.2.2.3. *Một số giải pháp công nghệ bảo mật và an toàn thông tin trên thế giới*

Để triển khai một Hạ tầng cơ sở về mật mã khóa công khai, trước hết phải có hệ thống cấp chứng chỉ số CA, hiện nay phần mềm CA có nhiều, các nhà cung cấp chứng chỉ số hàng đầu trên thế giới đều có hệ thống CA riêng, sẵn sàng cung cấp cho khách hàng. Nhưng giá thành của những sản phẩm thương mại này rất cao, ví dụ năm 2002, giá chính thức của Verisign, hệ thống cho 250-1000 người dùng có giá 50 000 – 78 000 USD mỗi năm.

Nhược điểm lớn nhất của phần mềm thương mại không phải là giá cả mà là công nghệ, người dùng không thể tự kiểm tra tính an toàn của phần mềm, không thể tự sửa phần mềm hoạt động theo ý mình. Nhược điểm về công nghệ này khiến cho các công ty đa quốc gia hoặc các đơn vị lớn như cấp thành phố trở lên phải tự xây dựng hệ thống CA cho riêng mình.

Nếu dựa trên các công nghệ mở được công nhận rộng rãi, tự xây dựng hệ thống CA là trong tầm tay. Để xây dựng phần mềm CA cho 1000 người dùng, có chất lượng tương đương nước ngoài, phát triển lần đầu ước tính cần 18 - 24 tháng và khoảng 20 000 - 40 000 USD. Giá thành vận hành thấp hơn vì làm chủ được công nghệ, không phải thuê chuyên gia nước ngoài (1 chuyên gia Mỹ có thể thu nhập 100 000 USD/năm). Tuy nhiên tự xây dựng có hai khó khăn chính là thời gian chuẩn bị lâu hơn và phải có một nhóm chuyên gia giỏi trong nước.

Để đánh giá chi tiết, đơn vị có nhu cầu thường thử nghiệm một hệ thống CA đầy đủ để hiểu sâu hơn các nhu cầu của chính đơn vị đó, trước khi lựa chọn giải pháp và công nghệ. Trong trường hợp này, hàng nghìn đơn vị đã lựa chọn Openca - một phần mềm tự do của các nhà khoa học Đức và Ý hợp tác phát triển.

Thời gian gần đây, mỗi tháng có khoảng 9000 lượt download phần mềm Openca. Nhiều đơn vị sau khi thử nghiệm thành công đã chính thức sử dụng Openca cho mục đích lâu dài. Một phần hệ thống PKI của liên minh châu Âu sẽ sử dụng Openca: http://pki.unimo.it/ .

Hoa kỳ cũng xem xét việc sử dụng Openca cho chính phủ điện tử:

http://www.it.vt.edu/organization/isc/irm/projects/PKI_and_Smart_Card_Technologies.html

Trên thế giới hiện nay chưa có nhiều giao thức mật mã được chuẩn hoá sử dụng PKI. Xin liệt kê một số giao thức có thể góp phần hình thành một hạ tầng cơ sở truyền tin an toàn:

- WPA - đã hoàn thiện và được triển khai khá rộng rãi.
- Ethsec - đang phát triển.
- IPSec - gần hoàn thiện, có thể bắt đầu thử nghiệm.
- SSL/TLS - đã được ứng dụng rất rộng rãi.
- S/MIME - đã hoàn thiện và được triển khai rộng rãi.

* WPA: Công nghệ mật mã trên mạng không dây.

Trong tương lai, công nghệ mật mã này sẽ được hỗ trợ bởi tất cả các thiết bị không dây. WPA phụ thuộc vào phần cứng kết nối mạng không dây, nên chỉ khi nào đã lựa chọn phần cứng mới có thể đi sâu nghiên cứu chi tiết.

* Ethsec: Công nghệ mật mã trên mạng Ethernet.

Ethsec là hệ thống mới, đang phát triển, nhưng nó là giải pháp duy nhất ứng dụng mật mã cho việc đảm bảo an toàn truyền tin trên mạng Ethernet. Các hệ thống quan trọng cần phải xem xét nghiêm túc các điểm yếu của mạng Ethernet.

* IPSec:

Công nghệ đảm bảo an toàn truyền tin tầng mạng này là thành phần bắt buộc trong mạng thế hệ tiếp theo - IPv6, và cũng được sử dụng cho IPv4, chủ yếu cho VPN. Tầng mạng là tầng cơ sở trong truyền tin nên thường được kèm sẵn trong các hệ điều hành. Tuy tính năng của IPSec chưa hoàn thiện, nhưng các hệ điều hành chính đều hỗ trợ IPSec, nên ta sẽ không gặp nhiều khó khăn khi triển khai IPSec trên diện rộng.

* SSL/TLS: Giao thức thế hệ mới.

TLS là giao thức thế hệ mới do IETF phát hành, thay thế SSL của Netscape. TLS có nhiều điểm ưu việt hơn hẳn nên tương lai sẽ hoàn toàn thay thế SSL. Hiện tại thư viện OpenSSL hỗ trợ cả SSL cũng như TLS, đây là thư viện tốt nhất hiện nay, đồng thời cũng là phần mềm mã nguồn mở. Việc sử dụng TLS phụ thuộc vào từng ứng dụng nghiệp vụ cụ thể của đơn vị.

* S/MIME: Giao thức thư điện tử.

Giao thức an toàn thư điện tử S/MIME hiện được hỗ trợ bởi tất cả các phần mềm thư điện tử chính. Vì thế sẽ không gặp trở ngại gì khi đưa vào sử dụng. Trong các phần mềm thư điện tử chính, Thunderbird (http://www.mozilla.org/products/thunderbird/) là phần mềm mã nguồn mở miễn phí, có hỗ trợ S/MIME và chạy trên hầu hết các hệ điều hành. Các nghiên cứu sơ bộ đánh giá Thunderbird có đủ tính năng phù hợp cho hệ thống truyền tin an toàn.

3.3.VẤN ĐỀ QUẢN LÝ KHÓA BÍ MẬT

Bởi vì nhiều người đều biết các thuật toán bảo mật, do đó mức độ an toàn của hệ thống mật mã phụ thuộc vào các khoá mã hoá được lưu trữ bí mật như thế nào. Như vậy, mục tiêu của quản lý khoá là bảo đảm các khoá mã hoá không bao giờ ở dạng bản rõ khi chúng ở bên ngoài hệ mật mã, ngoại trừ dưới các điều kiện an toàn trong khi các khoá được khởi tạo lần đầu tiên, hoặc khi được lưu trữ nhàm đảm bảo an toàn khi có hư hỏng.

Trong các hệ mật mã khoá công khai, chỉ cần bảo mật khoá tại nơi đã tạo ra nó. Khi một căp khoá công khai / bí mật bị lộ thì có thể tính toán một cặp khoá khác dễ dàng.

Trong các hệ mật mã khoá bí mật, có nhiều kiểu khoá bí mật khác nhau, song có thể xếp chung vào 2 lớp chính:

+ Các khoá được dùng trức tiếp để mã hoá các bức điện.

+ Các khoá dùng để mã hoá các khoá khác.

3.3.1. Phân phối khoá và thoả thuận khoá

- Sự phân phối khoá (*key distribution*) được định nghĩa là cơ chế một nhóm chọn khoá mật và sau đó truyền nó đến các nhóm khác.
- Thoả thuận khoá (*key agreement*) là giao thức để hai nhóm(hoặc nhiều hơn) liên kết với nhau cùng thiết lập một khoá mật bằng cách liên lạc trên một kênh truyền thông công khai.
- TA (*Trust Authority*) có nhiệm vụ xác minh danh tính của user, chọn và gửi khoá đến user.
- Đối phương bị động (*passive adversary*) nghĩa là hoạt động của anh ta chỉ hạn chế ở mức nghe trộm bức điện truyền trên kênh.
- Đối phương chủ động (*active adversary*) có thể làm nhiều hành vi xấu như:

+ Thay đổi bức điện mà anh ta quan sát khi nó đang được truyền trên mạng.
+ Lưu bức điện cho việc sử dụng lại ở lần sau.
+ Cố gắng giả dạng làm user khác trên mạng.

- Mục tiêu của đối phương chủ động là:

+ Lừa user U và V chấp nhận 1 khoá "không hợp lệ" như là một khoá hợp lệ (khoá không hợp lệ có thể là khoá cũ đã hết hạn sử dụng hoặc khoá do đối phương chọn).
+ Làm cho U và V tin rằng họ có thể trao đổi khoá với người kia khi họ không có khoá.

- Mục tiêucủa phân phối khoá và giao thức thoả thuận khoá là tại thời điểm kết thúc thủ tục, hai nhóm đều co cùng khoá K song không nhóm nào khác biết được(ngoại trừ TA có khả năng). Chắc chắn, việc thiết kế giao thức kiểu này khó khăn hơn nhiều trước đối phương chủ động.
- Sự phân phối khoá trước: với mỗi cặp user {U,V}, TA chọn một khoá ngẫu nhiên $K_{U,V}=K_{V,U}$ và truyền "ngoài dải " đến U,V trên kênh an toàn (nghĩa là việc truyền khoá không xảy ra trên mạng do mạng không an toàn). Biện pháp này gọi là an toàn khôngđiều kiện song nó đòi hỏi một kênh an toàn giữa TA và những người sử dụng trên mạng. Mỗi user phải lưu trữ (n-1) khoá và TA cần truyền n(n-1) khoá. Trong một mạng tương đối nhỏ, điều này trở nên quá tốn kém và như vậy giải pháp hoàn toàn không thực tế.
- Một cách tiếp cận thực tế hơn là TA phân phối khoá trực tiếp. Trong sơ đồ như vậy, TA làm việc như là một server khoá. TA tham gia khoá bí mật K_U với mỗi người dùng U trên mạng. Khi U muốn liên lạc với V, cô ta yêu cầu TA cung cấp cho một khoá phiên liên lạc, TA sẽ toạ ra khoá phiên liên lạc K và gửi nó dưới dạng mã hoá cho U và V để giải mã. Hệ thống mã Kerboros dựa trên biện pháp này.
- Nếu như cảm thấy vấn đề phân phói khoá qua TA không thực tế hoặc không như mong muốn thì biện pháp chung là dùng giao thức thoả thuận khoá. Trong giao thức thoả thuận khoá U và V kết hợp chọn một khoá bằng cách liên lạc với nhau trên kênh công khai. Ý tưởng đáng chú ý này do Martin và Diffie đưa ra độc lập với Merkle. Hai giao thức đáng quan tâm nữa là MTI và Girault.

3.4. MỘT SỐ SƠ ĐỒ THỎA THUẬN KHÓA BÍ MẬT

3.4.1. Sơ đồ thỏa thuận khóa BLOM

- Đối với mạng người user, TA phải tạo và truyền n(n-1) khoá. Nếu n lớn, giải pháp này rất không thực tế vì phải đảm bảo lượng thông tin được truyền một cách an toàn và lượng thông tin mà mỗi user phải lưu trữ một cách bí mật (tên, khoá bí mật của n-1 user khác). Sơ đồ phân phối khoá trước của Blom cho phép giảm lượng thông tin cần để truyền và lưu trữ, trong khi vẫn cho phép mỗi cặp user U và V có thể tính một cách độc lập khoá bí mật $K_{U,V}$.
- Giả sử mạng có n user, khoá được chọn thuộc miền xác định Z_p với phân phối là số nguyên tố (p >= n).
- k là một số nguyên 1<=k<=n-2 biểu thị cho kích thước lớn nhất chống lại sự lien kết của k user mà sơ đồ vẫn còn bảo mật.
- TA sẽ truyền k+1 phần tử của Z_p tới mỗi user qua kênh an toàn (trong sơ đồ phân phối khoá trước cơ bản là n-1). Mỗi cặp user U và V có thể tính khoá $K_{U,V} = K_{U,V}$. Điều kiện an toàn như sau: tập bất kỳ gồm nhiều nhất k user không liên kết từ {U,V} không thể xác định bất kỳ thông tin nào về khoá $K_{U,V}$.
- Xét trường hợp đặc biệt của sơ đồ Blom khi k=1. TA sẽ truyền hai phần tử thuộc Z_p cho mỗi người dùng qua kênh an toàn và bất kỳ người sử dụng riêng W sẽ không thể xác định bất kỳ thông tin nào về $K_{U,V}$ nếu W khác U,V.

Sơ đồ phân phối khoá trước Blom (k=1)

1. Số nguyên tố p được chọn công khai, còn với mỗi người sử dụng U chọn một phần tử $r_U \in Z_p$ là công khai. Các phần tử r_U phải khác biệt nhau.
2. TA chọn 3 phần tử ngẫu nhiên,bí mật a, b, c $\in Z_p$ (không cần khác biệt) và thiết lập đa thức bí mật:
   $f(x,y) = a+ b(x+y)+cxy \pmod p$.
3. Với mỗi user U, TA tính: $g_U(x) = f(x,r_u) \bmod p$ và truyền $g_U(x)$đến người dùng U trên kênh an toàn. Vì $g_U(x)$ là đa thức tuyến tính theo x nên có thể được viết như sau: $g_U(x)= a_U + b_U x \pmod p$
   trong đó : $a_U = a + br_U \bmod p$
   $b_U= b + cr_U \bmod p$
4. Nếu U và V muốn liên lạc với nhau, họ sẽ dùng khoá chung:
   $K_{U,V} = K_{V,U} = f(r_U,r_V) = a + b(r_U + r_V) + cr_Ur_V \pmod p$
   U tính $K_{U,V}$ như sau: $f(r_U,r_V) = g_U(r_V)$
   Còn V tính $K_{V,U}$ như sau: $f(r_U,r_V) = g_V(r_U)$

- Ví dụ:

Giả sử có 3 người sử dụng U, V và W, p = 7, các phần tử công khai là $r_U = 12$, $r_V = 7$, $r_W = 1$.

Giả sử rằng TA chọn a = 8, b = 7, c = 2. Khi đó đa thức f như sau:

$f(x,y) = 8 + 7(x+y) + 2xy$

$g_U(x) = 7 + 14x$

$g_V x) = 6+ 4x$

$g_W(x) = 15+ 9x$

$K_{U,V} = 3$, $K_{U,W} = 4$, $K_{V,W} = 10$

+ U tính $K_{U,V}$ như sau: $K_{U,V} = g_U(r_V) = 7 + 14*7 \bmod 17 = 3$

+ V tính $K_{V,U}$ như sau: $K_{V,U} = g_V(r_U) = 6 + 4*12 \bmod 17 = 3$

- Khi có sự liên kết của hai user {W,X} thì có thể xác định bất kỳ khoá $K_{U,V}$ mà {W,X}khác {U,V}. Bởi vì W và X cùng biết:

$a_W = a + br_W \bmod p$ $\quad b_U = b + cr_U \bmod p$

$a_X = a + br_X \bmod p$ $\quad b_X = b + cr_X \bmod p$

Với 4 phương trình 3 ẩn trên ta có thể dễ dàng tính a, b, c. Một khi biết a, b, c họ có thể thiết lập đa thức f(x,y) và tính khoá $K_{U,V}$ bất kỳ mà họ muốn.

Để tạo sơ đồ vẫn còn an toàn chống lại sự liên minh của k user, TA sẽ sử dụng hàm f(x,y) có dạng:

$$f(x,y) = \sum_{i=0}^{k} \sum_{j=0}^{k} a_{i,j} x^i y^j \bmod p$$

3.4.2 Sơ đồ thỏa thuận khóa DIFFE HELLMAN

Sơ đồ phân phối khoá trước của Diffie – Hellman

1. Số nguyên tố p và phần tử nguyên thuỷ $\alpha \in Z_p^*$ công khai
2. V tính:

   $K_{U,V} = \alpha^{auav} \bmod p = b_U^{av} \bmod p$

   nhờ dùng giái trị b_U công khai nhận từ dấu xác nhận của U và giá trị a_V mật riêng của anh ta.
3. U tính:

   $K_{U,V} = \alpha^{auav} \bmod p = b_V^{au} \bmod p$

   nhờ dùng giá trị b_V công khai nhận từ dấu xác nhận của V và giá trị a_U mật riêng của anh ta.

- Sơ đồ phân phối khoá trước của Diffie – Hellman an toàn về mặt tính toán vì nó liên quan bài toán logarithm rời rạc khó giải.
- Sơ đồ xét trên Z_p với p là số nguyên tố, α là phần tử nguyên thuỷ thuộc Z_p, giá trị của p và α là công khai với mọi người trong mạng, ID(U) là thông tin định danh cho mỗi người sử dụng U trên mạng (ví dụ tên, địa chỉ email, số điện thoại …). Mỗi người sử dụng U có một số mũ mật $a_U (0 \leq a_U \leq p-2)$ (TA không biét giá trị này) và giá trị công khai tương ứng $b_U = \alpha^{au} \bmod p$.
- TA sẽ có một sơ đồ chữ ký với thuật toán xác minh (công khai) ver_{TA} và thuật toán ký mật sig_{TA}
- Mỗi người sử dụng U khi tham gia mạng sẽ có một dấu xác nhận:

  $C(U) = (ID(U), b_U, sig_{TA}(ID(U), b_U))$

Các dấu xác nhận có thể được lưu trữ trong cơ sở dữ liệu công khai hoặc mỗi người dùng tự lưu dấu xác nhận của chính mình. Chữ ký của TA trên dấu xác nhận cho phép bất kỳ ai trên mạng đều có thể xác minh được thông tin trên nó.

U và V rất dễ dàng tính ra khoá chung:

$K_{U,V} = \alpha^{auav} \bmod p$

Ví dụ:

p= 25307, α = 2 là những tham số công khai.

Giả sử U chọn a_U = 3578 và tính:

$b_U = \alpha^{au} \bmod p = 2^{3578} \bmod 25307 = 6113$

sau đó U đặt b_U vào dấu xác nhận của cô ta.

Giả sử V chọn a_V = 19956 và tính:

$b_V = \alpha^{av} \bmod p = 2^{19956} \bmod 25307 = 7984$

sau đó V đặt b_V vào dấu xác nhận của anh ta.

Bây giờ U có thể tính khoá:

$$K_{U,V} = b_V^{au} \bmod p = 7984^{3578} \bmod 25307$$
$$= 3694$$

Còn V cũng có thể tính khoá:

$$K_{U,V} = b_U^{av} \bmod p = 6113^{19956} \bmod 25307$$
$$= 3694$$

Nhờ chữ ký của TA trên dấu xác nhận của người sử dụng nên ngăn cản một cách hiệu quả sự xâm nhập của người sử dụng khác W.

Câu hỏi đặt ra là: liệu W có thể tính $K_{U,V}$ nếu W khác U, V hay không? Hoặc nếu W biết b_U, b_V thì có thể xác định $K_{U,V}$ hay không? Bài toán này được gọi là bài toán Diffie – Hellman.

Bài toán Diffie – Hellman.

Bài toán: I = (p, α, β, γ) trong đó p là số nguyên tố, $\alpha \in Z_p^*$ là phần tử nguyên thuỷ, còn β, $\gamma \in Z_p^*$

Mục tiêu: tính $\beta^{\log} \alpha^{\gamma} \bmod p(= \gamma^{\log} \alpha^{\beta} \bmod p)$

Sơ đồ Diffie – Hellman là an toàn với đối phương bị động nếu và chỉ nếu bài toán Diffie – Hellman là khó giải. Tuy nhiên, giả định cho rằng thuật toán bất kỳ giải được bài toán Diffie – Hellman thì cũng có thể giải được bài toán logarithm vẫn chưa được chứng minh.

Chương 4. THỬ NGHIỆM CHƯƠNG TRÌNH

4.1. BÀI TOÁN LẬP TRÌNH VÀ CHƯƠNG TRÌNH

4.1.1. Mô tả

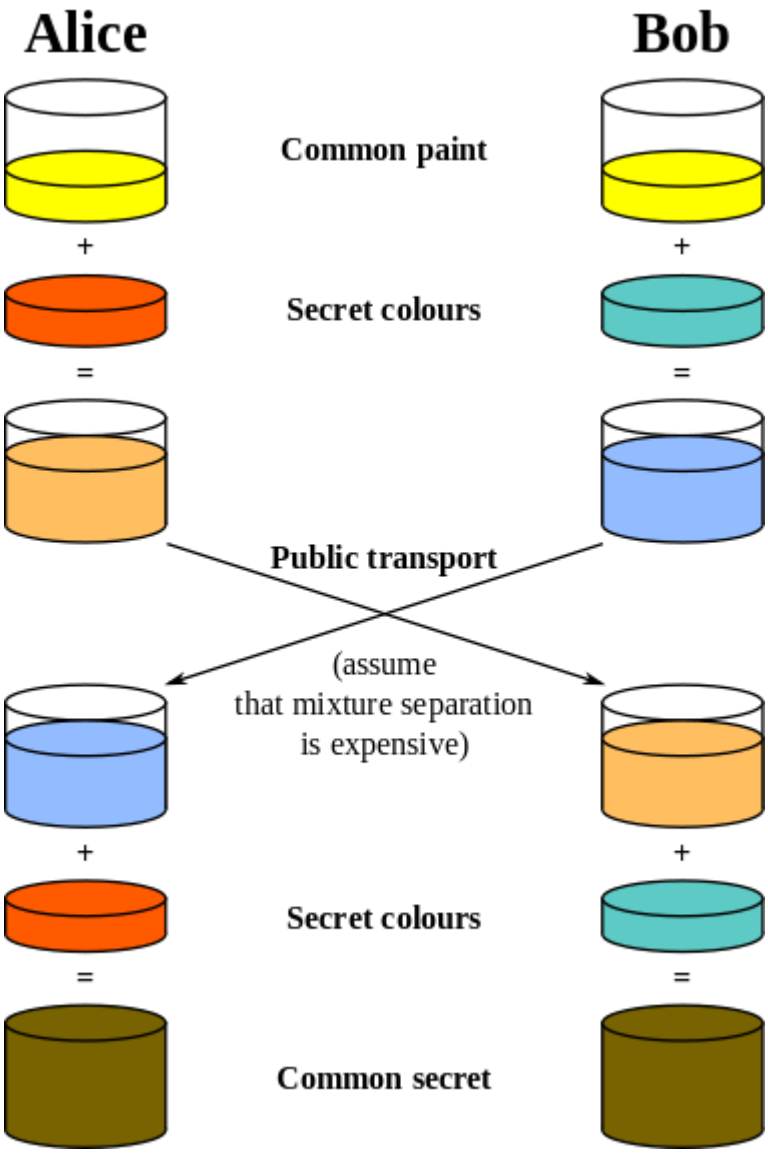
Diffie–Hellman thiết lập bí mật chung để sử dụng cho trao đổi dữ liệu an toàn trên một kênh truyền thông công cộng không an toàn. Sơ đồ sau đây minh họa ý tưởng cơ bản của việc trao đổi khóa thông qua ví dụ về màu sơn.

4.1.2. Ý tưởng cơ bản

Điểm chủ chốt của ý tưởng này là Alice và Bob trao đổi màu sơn bí mật thông qua hỗn hợp sơn.

- Đầu tiên Alice và Bob trộn màu đã biết chung (màu vàng) với màu bí mật riêng của mỗi người.
- Sau đó, mỗi người chuyển hỗn hợp của mình tới người kia thông qua một kênh vận chuyển công cộng.
- Khi nhận được hỗn hợp của người kia, mỗi người sẽ trộn thêm với màu bí mật của riêng mình và nhận được hỗn hợp cuối cùng.

Hỗn hợp sơn cuối cùng là hoàn toàn giống nhau cho cả hai người và chỉ có riêng hai người biết. Mấu chốt ở đây là đối với một người ngoài sẽ rất khó (về mặt tính toán) cho họ để tìm ra được bí mật chung của hai người (nghĩa là hỗn hợp cuối cùng). Alice và Bob sẽ sử dụng bí mật chung này để mã hóa và giải mã dữ liệu truyền trên kênh công cộng. Lưu ý, màu sơn đầu tiên (màu vàng) có thể tùy ý lựa chọn, nhưng được thỏa thuận trước giữa Alice và Bob. Màu sơn này cũng có thể được giả sử là không bí mật đối với người thứ ba mà không làm lộ bí mật chung cuối cùng của Alice và Bob.


Alice
Bob
Common paint
+
+
Secret colours
=
=
Public transport
(assume
that mixture separation
is expensive)
+
+
Secret colours
=
=
Common secret

Giao thức được diễn giải dưới dạng toán học như sau:

Giao thức sử dụng nhóm nhân số nguyên modulo p, trong đó p số nguyên tố, và g là căn nguyên thủy mod p. Trong ví dụ dưới đây, giá trị không bí mật được viết bằng màu xanh, và giá trị bí mật viết bằng màu **đỏ**:

Alice				**Bob**		
Bí mật	Công khai	Tính	Gửi	Tính	Công khai	Bí mật
a	p, g		p,g→			b
a	p, g, A	$g^a \bmod p = A$	A→		p, g	b
a	p, g, A		← B	$g^b \bmod p = B$	p, g, A, B	b
a, **s**	p, g, A, B	$B^a \bmod p = s$		$A^b \bmod p = s$	p, g, A, B	b, **s**

1. Alice và Bob thỏa thuận sử dụng chung một số nguyên tố p=23 và căn nguyên thủy g=5.
2. Alice chọn một số nguyên bí mật ***a***=**6**, và gửi cho Bob giá trị A = g^a mod p
   - A = 5^6 mod 23
   - A = **15,625** mod 23
   - A = 8
3. Bob chọn một số nguyên bí mật ***b***=**15**, và gửi cho Alice giá trị B = g^b mod p
   - B = 5^{15} mod 23
   - B = **30,517,578,125** mod 23
   - B = 19
4. Alice tính **s** = B^a mod p
   - **s** = 19^6 mod 23
   - **s** = **47,045,881** mod 23
   - **s** = **2**
5. Bob tính **s** = A^b mod p
   - **s** = 8^{15} mod 23
   - **s** = **35,184,372,088,832** mod 23
   - **s** = **2**
6. Như vậy Alice và Bob cùng chia sẻ bí mật chung là số **2** vì 6*15 cũng bằng 15*6.

Cả Alice và Bob đều có được giá trị chung cuối cùng vì $(g^a)^b = (g^b)^a \bmod p$. Lưu ý rằng chỉ có a, b và $g^{ab} = g^{ba} \bmod p$ là được giữ bí mật. Tất cả các giá trị khác như p, g, $g^a mod\ p$ và $g^b\ mod\ p$ được truyền công khai. Sau khi Alice và Bob tính được bí mật chung, cả hai có thể sử dụng nó làm khóa mã hóa chung chỉ có hai người biết để gửi dữ liệu trên kênh truyền thông mở.

Trong thực tế để giao thức được an toàn, người ta sử dụng giá trị lớn hơn nhiều cho a, b, và p, vì trong ví dụ trên chỉ có tổng cộng 23 kết quả khác nhau cho n mod 23 (do đó kẻ tấn công chỉ cần thử hết 23 trường hợp là tìm ra khóa bí mật). Nếu số nguyên tố p có ít nhất 300 chữ số, còn a và b có ít nhất 100 chữ số, thì ngay cả những máy tính hiện đại nhất hiện nay cũng không thể tìm được a nếu chỉ biết g, p, $g^b \bmod p$ và $g^a \bmod p$. Bài toán này, gọi là bài toán Lôgarit rời rạc, hiện chưa có cách giải hiệu quả bằng máy tính (vì vậy được sử dụng để tạo khóa công khai).

Lưu ý, g không cần thiết là một căn nguyên thủy có giá trị lớn. Trong thực tế người ta hay sử dụng các giá trị 2, 3 hoặc 5.

4.1.3. Mô tả giao thức

Sau đây là mô tả khái quát của giao thức.

4.1.3.1 Thiết lập khóa

1. Alice và Bob thỏa thuận sử dụng chung một nhóm cyclic hữu hạn G và một phần tử sinh g của G. Phần tử sinh g công khai với tất cả mọi người, kể cả kẻ tấn công. Dưới đây chúng ta giả sử nhóm G là nhóm nhân.
2. Alice chọn một số tự nhiên ngẫu nhiên a và gửi g^a cho Bob.
3. Bob chọn một số tự nhiên ngẫu nhiên b và gửi g^b cho Alice.
4. Alice tính $(g^b)^a$.
5. Bob tính $(g^a)^b$.

Vì giá trị $(g^b)^a$ và $(g^a)^b$ là bằng nhau (do nhóm G có tính kết hợp), cả Alice và Bob đều tính được giá trị g^{ab} và có thể sử dụng nó cho khóa bí mật chung.

4.1.3.2. *Mã hóa*

Thông điệp m trước khi được gửi đi bởi Alice (hoặc Bob) sẽ được mã hóa thành mg^{ab}.

4.1.3.3 *Giải mã*

Để giải mã thông điệp m, gửi dưới dạng mg^{ab}, Bob (hoặc Alice) phải tính được giá trị $(g^{ab})^{-1}$. Giá trị $(g^{ab})^{-1}$ được tính như sau: Vì Bob biết $|G|$, b, và g^a, mặt khác theo định lý Lagrange trong lý thuyết nhóm ta có $x^{|G|} = 1$ với mọi x thuộc G, nên Bob tính được $(g^a)^{|G|-b} = g^{a(|G|-b)} = g^{a|G|-ab} = g^{a|G|}g^{-ab} = (g^{|G|})^a g^{-ab} = 1^a g^{-ab} = g^{-ab} = (g^{ab})^{-1}$.

Việc giải mã bây giờ trở nên dễ dàng: Bob sử dụng $(g^{ab})^{-1}$ đã tính và phục hồi thông điệp nguyên thủy bằng cách tính: $mg^{ab}(g^{ab})^{-1} = m(1) = m$.

4.1.4. Chương trình C đơn giản

```
#include <stdio.h>
#include <math.h>
#include <stdlib.h>
#include <time.h>
#include <conio.h>
 int prime(int num) {
    int i;
    for (i = 2; i*i <= num; ++i)
        if (num % i == 0)
            return 0;
    return 1;
}
 int mod(int base, int expo, int num) {
    int res = 1;
    int i;
    for (i = 1; i <= expo; ++i)
        res = (res * base) % num;
    return res;
}

void main() {
    int p, g, a, b, i, j, r1, r2, k1, k2, k3;
    srand(time(NULL));
    p:
        printf("\nNhap p và g: "); scanf("%d %d", &p, &g);
    if (!prime(p) || !prime(g)) {
        printf("\nCac gia tri nhap khong phai nguyen to... Vui long nhap lai...");
        goto p;
    } else {
        srand(time(NULL));
        a = rand() % 50;
        b = rand() % 50;
        printf("\nSo tao ngau nhien(khoa rieng cua Alice và Bob): %d %d", a, b);
        r1 = mod(g, a, p); // g^a mod p
        r2 = mod(g, b, p); // g^b mod p
        printf("\n Khoa cong khai cua Alice: R1= %d\n Khoa cong khai của Bob: R2 =
%d\n", r1, r2);
        k1 = mod(r2, a, p); // r2^a mod p
        k2 = mod(r1, b, p); // r1^b mod p
        printf("\nKhoa bi mat chung tinh duoc boi Alice: %d", k1);
        printf("\nKhoa bi mat chung tinh duoc boi Bob: %d", k2);
        k3 = mod(g, a * b, p); // g^a*b mod p
        printf("\nKiem tra Khoa bi mat chung: %d", k3); // phai giong k1 và k2
    }
getch(); // Dung man hinh de xem ket qua
}
```

4.1.5. Sơ đồ

Trong giao thức này, hai bên trao đổi khóa là Alice và Bob. Kẻ nghe lén Eve có thể quan sát được thông tin truyền giữa Alice và Bob nhưng không thay đổi nội dung thông tin (tấn công bị động). Sơ đồ sau đây tóm tắt mỗi người biết gì trong mô hình của giao thức.

- Đặt **s** = khóa bí mật được chia sẻ. **s** = **2**
- Đặt g = căn nguyên thủy công khai. g = 5
- Đặt p = số nguyên tố công khai. p = 23
- Đặt **a** = khóa riêng tư của Alice. **a** = **6**
- Đặt A = khóa công khai của Alice. $A = g^a \bmod p = 8$
- Đặt **b** = khóa riêng tư của Bob. **b** = **15**
- Đặt B = khóa công khai của Bob. $B = g^b \bmod p = 19$

Alice		Bob		Eve	
biết	không biết	biết	không biết	biết	không biết
p = 23	**b = ?**	p = 23	**a = ?**	p = 23	**a = ?**
base g = 5		base g = 5		base g = 5	**b = ?**
a = 6		**b = 15**			**s = ?**
$A = 5^{6} \bmod 23 = 8$		$B = 5^{15} \bmod 23 = 19$		$A = 5^{a} \bmod 23 = 8$	
$B = 5^{b} \bmod 23 = 19$		$A = 5^{a} \bmod 23 = 8$		$B = 5^{b} \bmod 23 = 19$	
$s = 19^{6} \bmod 23 = 2$		$s = 8^{15} \bmod 23 = 2$		$s = 19^{a} \bmod 23$	
$s = 8^{b} \bmod 23 = 2$		$s = 19^{a} \bmod 23 = 2$		$s = 8^{b} \bmod 23$	
$s = 19^{6} \bmod 23 = 8^{b} \bmod 23$		$s = 8^{15} \bmod 23 = 19^{a} \bmod 23$		$s = 19^{a} \bmod 23 = 8^{b} \bmod 23$	
s = 2		s = 2			

Lưu ý: Việc Bob giải được khóa riêng tư của Alice, và Alice giải được khóa riêng tư của Alice phải là bài toán khó đối với cả hai. Nếu bài toán tìm khóa riêng tư của Bob không khó đối với Alice (hoặc ngược lại), thì Eve chỉ cần thay thế cặp khóa riêng tư / công khai của mình, gắn khóa công khai của Bob vào khóa riêng tư của mình, tạo ra khóa bí mật chia sẻ giả, và giải ra khóa riêng tư của Bob, sau đó sử dụng nó để tìm ra khóa bí mật chia sẻ giữa Bob và Alice. Eve cũng có thể tìm cách chọn cặp khóa công khai / riêng tư nào đó giúp Eve giải được khóa riêng tư của Bob một cách dễ dàng.

4.2. CẤU HÌNH HỆ THỐNG

Chương trình đã dịch thành file có đuôi **.exe** có thể chạy trên mọi máy có cài hệ điều hành Window.

4.3. HƯỚNG DẪN SỬ DỤNG CHƯƠNG TRÌNH

Chỉ cần nhập 2 số nguyên tố p và g thì chương trình sẽ tự chạy và cho ra kết quả tương ứng .

TÀI LIỆU THAM KHẢO

Tài liệu tiếng việt

[1] PGS.TS Trịnh Nhật Tiến. Một số vấn đề về an toàn thông tin, một số chữ ký dùng trong giao dịch điện tử

[2] PGS.TS Trịnh Nhật Tiến. Giáo trình An toàn dữ liệu

[3] PGS.TS Trịnh Nhật Tiến. Cơ sở hạ tầng mật mã hóa công khai **(**Public Key Infrastructure **–** PKI**)**

Tài liệu tiếng anh

[4] Chaum, David, van Heijst, Eugene and Pfitzmann, Birgit, Cryptographically strong undeniable signatures, unconditionally secure for the signer (extended abstract)

[5] Ecient Convertible Undeniable Signature Schemes - D.Chaum, E. van Heys

Website

[6] **http://en.wikipedia.org**
[7] **http://www.imc.org/rfc3852**

[8] **http://www.imc.org/rfc3370**

[9] **http://www.imc.org/rfc2632**

[10] **http://www.imc.org/rfc2633**

[11] **http://www.imc.org/rfc2631**

[12**]http://www.faqs.org/rfcs/rfc2045.html**
[13**]http://www.imc.org/smime-pgpmime.html**
[14**]http://www.imc.org/terms.html**
[15**]http://laws.justice.gc.ca/en/f-11/59120.html**

[16**]http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paip-pefr1_e.asp**

[17**]http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/CHAP2_6-2_e.asp**

[18**]http://www.openCA.org**