ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐH CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

NGUYỄN VĂN THỰC

CHỮ KÝ SỐ VÀ ỨNG DỤNG

LUẬN VĂN THẠC SỸ KHOA HỌC MÁY TÍNH

Chuyên ngành : Khoa học máy tính
Mã số : 60 48 01

Thái Nguyên, năm 2011

LỜI CẢM ƠN

Tôi xin chân thành cảm ơn **PGS.TS. Đặng Văn Đức** đã trực tiếp hướng dẫn, tạo mọi điều kiện thuận lợi cho tôi trong suốt quá trình nghiên cứu và thực hiện báo cáo luận văn. Thầy đã định hướng nghiên cứu, giúp tôi hoàn thành tốt luận văn này.

Trong quá trình học tập và thực hiện luận văn tốt nghiệp tại Trường Đại học Công nghệ Thông tin và Truyền thông - Đại học Thái Nguyên, tôi xin chân thành cảm ơn các thầy cô trong đào tạo sau Đại học, các thầy cô đã trực tiếp giảng dạy, giúp đỡ tôi hoàn thành tốt chương trình học tập và luận văn tốt nghiệp.

Tôi xin cảm ơn toàn thể các anh chị học viên lớp Cao học Khoa học máy tính, cùng gia đình, bạn bè đã động viên giúp đỡ tôi trong quá trình học tập cũng như nghiên cứu đề tài Luận văn này.

Học viên

Nguyễn Văn Thực

MỤC LỤC

DANH MỤC CÁC KÝ HIỆU VÀ CHỮ VIẾT TẮT

STT	TÊN VIẾT TẮT	Ý NGHĨA
1	RSA	Hệ mật mã khóa công khai
2	DES	Hệ mật mã khóa đối xứng
3	PKI	Public key infrastructure - Hạ tầng khóa công khai
4	VRS	Hệ thống báo cáo điều hành VRS (VNPT Reports System)
5	AIS	Hệ thống thông tin điều hành AIS (Administrative Information System)
6	CA	Bộ cấp chứng thực số (Certificate Authorities)
7	IIS	Internet Information Services
8	DNS	Domain Name System
9	WAN	Wide Area Networks
10	LAN	Local Area Network
11	MMC	Microsoft Management Console
12	CRL	Certificate Revocation List
13	LDAP	Giao thức truy nhập nhanh dịch vụ thư mục (Lightweight Directory Access Protocol)
14	RA	Thành phần cấp quyền đăng nhập (Registration Authorities)
15	TSA	Thành phần gán nhãn thời gian (Timestamp Authorities)
16	OCSP	Online Certificate Status Protocol

DANH MỤC CÁC HÌNH VẼ ĐỒ THỊ

MỞ ĐẦU

Trong sự phát triển không ngừng của ngành Công nghệ thông tin kéo theo là rất nhiều ứng dụng vào đời sống của con người, tạo cho chúng ta sự thoái mái trong việc giao tiếp, trao đổi thông tin, tất cả các sự việc đều được cập nhật một cách nhanh chóng trên các phương tiện truyền thông. Mọi thông tin của cá nhân, tập thể, doanh nghiệp, hay thâm chí của các Bộ, Ban ngành các cấp đều có thể được đưa lên mạng Internet. Làm thế nào để có thể khẳng định những thông tin đó là của ai? để giải quyết vấn đề này không nên sử dụng con dấu hay chữ ký thông thường mà sử dụng chữ ký số là một giải pháp tốt nhất.

Mặt khác sự bùng nổ phương thức truyền thông tin thông qua Internet và các phương tiện truyền thông khác đã đưa chúng ta đến việc cần phải đối mặt với việc bảo mật những thông tin cá nhân, thông tin riêng tư, các thông tin cá nhân riêng tư có thể bị thay đổi khi đưa lên Internet, để đảm bảo sự không thể chối cãi khi ai đó đưa thông tin cá nhân của người khác lên mạng Internet cần phải chứng thực rằng mình đã đưa ra thông tin đó, để khi cần thì các cơ quan pháp luật có thể sử dụng khi có sự kiện tụng, hay tranh chấp.

Trong sự phát triển không ngừng của ngành Công nghệ thông tin kéo theo là rất nhiều ứng dụng vào đời sống của con người, tạo cho chúng ta sự thoái mái trong việc giao tiếp, trao đổi thông tin, tất cả các sự việc đều được cập nhật một cách nhanh chóng trên các phương tiện truyền thông. Mọi thông tin của cá nhân, tập thể, doanh nghiệp, hay thâm chí của các Bộ, Ban ngành các cấp đều có thể được đưa lên mạng Internet. Làm thế nào để có thể khẳng định những thông tin đó là của ai? để giải quyết vấn đề này không nên sử dụng con dấu hay chữ ký thông thường mà sử dụng chữ ký số là một giải pháp tốt nhất.

Mặt khác sự bùng nổ phương thức truyền thông tin thông qua Internet và các phương tiện truyền thông khác đã đưa chúng ta đến việc cần phải đối mặt với việc bảo mật những thông tin cá nhân, thông tin riêng tư, các thông tin cá nhân riêng tư có thể bị thay đổi khi đưa lên Internet, để đảm bảo sự không thể chối cãi khi ai đó đưa thông tin cá nhân của người khác lên mạng Internet, trao đổi thông tin giữa các cơ quan, trong một cơ quan cần phải chứng thực rằng mình đã đưa ra thông tin đó, để khi cần thì các cơ quan pháp luật có thể sử dụng khi có sự kiện tụng, hay tranh chấp.

Cấu trúc của luận văn bao gồm 3 chương với những nội dung cụ thể như sau:

Chương 1: Tổng quan về mật mã và ứng dụng chữ ký số

Chương 2: Chứng chỉ số và hệ thống chứng thực số

Chương 3: Cài đặt hệ thống chứng chỉ số thử nghiệm

CHƯƠNG 1:
TỔNG QUAN VỀ MẬT MÃ VÀ ỨNG DỤNG CHỮ KÝ SỐ

1.1. Giới thiệu:

Mật mã đã được con người sử dụng từ lâu đời. Các hình thức mật mã sơ khai đã được tìm thấy từ khoảng bốn nghìn năm trước trong nền văn minh Ai Cập cổ đại. Trải qua hàng nghìn năm lịch sử, mật mã đã được sử dụng rộng rãi ở khắp nơi trên thế giới từ Đông sang Tây để giữ bí mật cho việc giao lưu thông tin trong nhiều lĩnh vực hoạt động giữa con người và các quốc gia, đặc biệt trong các lĩnh vực quân sự , chính trị, ngoại giao.

Mật mã trước hết là một loại hoạt động thực tiễn, chức năng chính của nó là để giữ bí mật thông tin. Ví dụ muốn gửi một văn bản từ một người gửi A đến một người nhận B, A phải tạo cho văn bản đó một bản mã mật tương ứng và thay vì gửi văn bản rõ thì A chỉ gửi cho B bản mã mật, B nhận được bản mã mật và khôi phục lại văn bản mã mật mình nhận được thành văn bản rõ để hiểu được thông tin mà A muốn gửi cho mình.

Do văn bản gửi đi thường được chuyển qua các con đường công khai nên người khác có thể "lấy trộm" được, nhưng vì đó là bản mật mã nên không đọc hiểu được nội dung thông tin; Còn A có thể tạo ra bản mã mật và B có thể giải bản mã mật thành bản rõ để hiểu được là do hai người đã có một thoả thuận về một chìa khóa chung, chỉ với khóa chung này thì A mới tạo được bản mã mật từ bản rõ và B mới khôi phục được bản rõ từ bản mã mật. Khóa chung đó được gọi là khóa mật mã. Để thực hiện được một phép mật mã, ta còn cần có một thuật toán biến bản rõ cùng với khóa mật

mã thành bản mã mật và một thuật toán ngược lại biến bản mật cùng với khóa mật mã thành bản rõ. Các thuật toán đó được gọi tương ứng là thuật toán lập mã và thuật toán giải mã. Các thuật toán này thường không nhất thiết phải giữ bí mật, mà cái luôn cần được giữ bí mật là khóa mật mã.

Trong thực tiễn, có những hoạt động ngược lại với hoạt động bảo mật là khám phá bí mật từ các bản mã "lấy trộm" được, hoạt động này thường được gọi là mã thám hay phá khóa. [3]

1.2. Khái niệm hệ mật mã

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

1 . P là tập hữu hạn các các bản rõ có thể

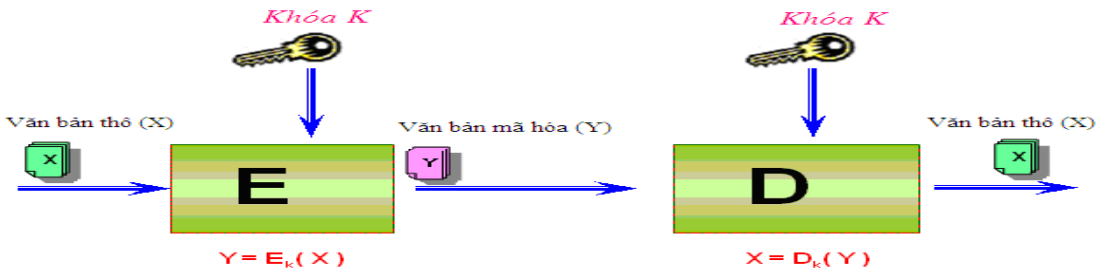
2 . C tập hữu hạn các bản mã có thể

3 . K là tập hữu hạn các khóa có thể

4 . E là tập các hàm lập mã

5 . 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 $d_k (e_k(x)) = x$, $x \in P$

Quá trình mã hóa và giải mã



Hình 2.1 : Quá trình mã hóa và giải mã

1.3. Hệ mật mã đối xứng

1.3.1. Khái niệm

Trong các hệ mã đối xứng chỉ có một khóa được chia sẻ giữa các bên tham gia liên lạc, trao đổi thông tin.