

ĐẠI HỌC THÁI NGUYÊN
KHOA CÔNG NGHỆ THÔNG TIN



Nguyễn Thị Hồng Minh

CHỮ KÝ SỐ VÀ CÁC VẤN ĐỀ BẢO MẬT THÔNG TIN

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Thái Nguyên - 2010

ĐẠI HỌC THÁI NGUYÊN
KHOA CÔNG NGHỆ THÔNG TIN



Nguyễn Thị Hồng Minh

CHỮ KÝ SỐ VÀ CÁC VẤN ĐỀ BẢO MẬT THÔNG TIN

Chuyên ngành: Khoa học máy tính

Mã số: 604801

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

NGƯỜI HƯỚNG DẪN KHOA HỌC: PGS.TS. Đoàn Văn Ban

Thái Nguyên - 2010

LỜI CAM ĐOAN

Tôi xin cam đoan bản luận văn “Chữ ký số và các vấn đề bảo mật thông tin” là công trình nghiên cứu của tôi, dưới sự hướng dẫn khoa học của PGS.TS Đoàn Văn Ban, tham khảo các nguồn tài liệu đã được chỉ rõ trong trích dẫn và danh mục tài liệu tham khảo. Các nội dung công bố và kết quả trình bày trong luận văn này là trung thực và chưa được ai công bố trong bất kỳ công trình nào.

Thái nguyên, ngày 10 tháng 10 năm 2010

Nguyễn Thị Hồng Minh

LỜI CẢM ƠN

Trước tiên tôi xin gửi lời cảm ơn chân thành nhất đến thầy PGS. TS Đoàn Văn Ban đã định hướng và nhiệt tình hướng dẫn, giúp đỡ tôi rất nhiều về mặt chuyên môn trong quá trình làm luận văn.

Tôi xin gửi lời biết ơn sâu sắc đến các thầy, các cô đã dạy dỗ và truyền đạt những kinh nghiệm quý báu cho chúng tôi trong suốt hai năm học cao học tại khoa Công nghệ thông tin - Đại học Thái Nguyên.

Tôi xin cảm ơn bạn bè, đồng nghiệp và gia đình, những người luôn gần gũi động viên, chia sẻ cùng tôi trong suốt thời gian làm luận văn tốt nghiệp.

Thái Nguyên, tháng 11 năm 2010

MỤC LỤC

LỜI CAM ĐOAN	
LỜI CẢM ƠN.....	
MỤC LỤC	
DANH MỤC CÁC TỪ VIẾT TẮT	5
DANH MỤC CÁC HÌNH.....	6
CÁC KÍ HIỆU DÙNG TRONG LUẬN VĂN.....	7
Mở đầu	8
1. Lý do chọn đề tài.....	8
2. Mục tiêu nghiên cứu.....	9
3. Phương pháp nghiên cứu.....	10
4. Tổng quan luận văn.....	10
Chương 1: Một số hệ mật mã khoá thông dụng.....	12
1.1 Giới thiệu.....	12
1.2 Hệ mã khoá bí mật	13
Hệ mã DES/ AES	13
1.3 Hệ mã hoá công khai.....	17
1.3.1 Các khái niệm cơ bản.....	17
1.3.2 Một số khái niệm toán học cơ sở	18
1.3.3 Các nguyên lý của hệ mật mã công khai.....	23
1.3.4 Hệ mã logarithm rời rạc	26
1.3.5 Hệ ElGamal.....	28
1.3.6 Hệ RSA	29
1.4 Độ an toàn của RSA.....	34
1.4.1 Tạo vỏ bọc an toàn cho văn bản.....	35
1.4.2 Xác thực chủ thể.....	36
1.5 Quản lý khoá	36
1.5.1 Phân phối khoá cho giải thuật mật mã đối xứng.....	37
1.5.2 Phân phối khoá cho giải thuật mật mã không đối xứng.....	39
1.5.3 Phát sinh và lưu giữ khoá bí mật.....	42

1.6 Kết luận chương.....	
Chương 2: Chữ ký số.....	
2.1 Giới thiệu	
2.2 Xác thực thông báo và các hàm xác thực	
2.2.1 Xác thực thông báo	
2.2.2 Các hàm xác thực	50
2.3 Chữ ký số	57
2.3.1 Chữ ký số dùng mật mã khoá công khai	57
2.3.2 Lược đồ chữ ký số.....	61
2.4 Các kiểu tấn công vào lược đồ chữ ký.....	70
2.5 Kết luận chương	70
2.5.1 Tính pháp lý và ứng dụng chữ ký số trong và ngoài nước.....	71
Chương 3: Cài đặt demo chương trình	76
3.1 Lĩnh vực ứng dụng của chương trình.....	76
3.2 Chức năng của chương trình	76
3.2.1 Phần bảo mật thông tin.....	76
3.2.2 Phần chữ ký số	77
3.3 Một số màn hình giao diện của chương trình.....	77
3.4 Kết luận chương	81

DANH MỤC CÁC TỪ VIẾT TẮT

AES	Advance Encryption Standard
ASCII	American Standard Code for Information Interchange
ANSI	American National Standards Institute
CA	Certificate Authority
DES	Data Encryption Standard
FIPS	Federal Information Processing Standard 46
IDEA	International Data Encryption Algorithm
IEEE	Institute of Electrical and Electronic Engineers
ITU	International Telecommunication Union
ISO	International Organization for Standardization
MAC	Message Authentication Code
MARS	Multicast Address Resolution Server
MD5	Message Digest 5
NIST	National Institute Of Standards And Technology
OCSP	Online Certificate Status Protocol
PKI	public-key infrastructures
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
TCP/IP	Transfer Control Protocol/Internet Protocol
URL	Uniform Resource Locator

DANH MỤC CÁC HÌNH

Trang	
Hình 1.1	<i>Thuật toán giải mã của hệ DES..... 14</i>
Hình 1.2	<i>Sơ đồ khối nguyên lý hoạt động của mật mã khoá công khai . 25</i>
Hình 1.3	<i>Minh hoạ quá trình mã hoá khoá công khai..... 31</i>
Hình 1.4	<i>Sơ đồ phân bố khóa của một network với một CKD 36</i>
Hình 1.5	<i>Sơ đồ phân bố khóa của một network với KD..... 49</i>
Hình 1.6	<i>Sơ đồ kiểm tra khoá..... 42</i>
Hình 1.7	<i>Sơ đồ bảo vệ khoá..... 43</i>
Hình 2.1 (a)	<i>Lược đồ mã hoá thông báo..... 48</i>
Hình 2.1(b)	<i>Mã hoá khoá công khai: xác thực và chữ ký..... 49</i>
Hình 2.1(c)	<i>Mã hoá khoá công khai: Bí mật, xác thực và chữ ký 49</i>
Hình 2.2 (a)	<i>Xác thực thông báo..... 50</i>
Hình 2.2 (b)	<i>Bí mật và xác thực thông báo:Xác thực đối với bản rõ 50</i>
Hình 2.2 (c)	<i>Xác thực đối với bản mã..... 50</i>
Hình 2.3	<i>Sơ đồ nguyên lý hoạt động của chữ ký số..... 56</i>
Hình 2.4	<i>Sơ đồ tạo và kiểm tra chữ ký số..... 57</i>
Hình 2.5	<i>Sơ đồ quy trình ký..... 60</i>
Hình 2.6	<i>Sơ đồ quy trình xác minh chữ ký 60</i>
Hình 2.7	<i>Tổng quan về chữ ký số với khôi phục thông điệp..... 62</i>
Hình 2.8	<i>Lược đồ tổng quan của chữ ký số với khôi phục thông điệp ... 62</i>
Hình 3.1	<i>Vấn đề chứng thực thông qua trung gian 75</i>

CÁC KÍ HIỆU DÙNG TRONG LUẬN VĂN

- C Bản mã.
- X Không gian các bản mã.
- D, D_k Hàm giải mã, hàm giải mã với khoá k.
- d, d_A Số mũ giải mã, số mũ giải mã của cá thể A.
- E, E_k Hàm mã hoá, hàm mã hoá với khoá k.
- e, e_A Số mũ mã hoá, số mũ mã hoá của cá thể A.
- ID_A Định danh của cá thể A.
- k Khoá mã.
- M Không gian bản rõ
- P Bản tin rõ.
- P Hàm số hoá bản rõ. $P : M \rightarrow Z_n$
- (n; e) Cặp số : n, e là các số nguyên dương.
- (e, d) Ước chung lớn nhất của hai số nguyên dương e và d.

Mở đầu

1. Lý do chọn đề tài

Internet ngày nay đã trở thành mạng truyền dữ liệu được sử dụng phổ biến trên toàn thế giới. Nó được sử dụng để truyền thư điện tử, truy cập các website, kết nối tới các trường học, công sở, giám sát hệ thống từ xa, truyền tệp... Trong tương lai, Internet sẽ trở thành môi trường truyền thông phổ cập cho toàn thế giới.

Rõ ràng tiềm năng của mạng Internet là rất lớn nhưng nó lại bị hạn chế bởi thiết kế mở của mình. Như ta biết giao tiếp qua Internet chủ yếu sử dụng giao thức TCP/IP. Các gói tin truyền từ điểm nguồn tới điểm đích sẽ đi qua rất nhiều máy tính trung gian, vì vậy nó rất dễ bị xâm phạm, can thiệp, theo dõi và giả mạo trên đường truyền và biện pháp bảo mật bằng mật khẩu là không đảm bảo vì có thể bị nghe trộm hoặc bị dò ra nhanh chóng; vì thế đã chuyển sang xu hướng mã hoá.

Nhờ thông tin được người gửi mã hoá trước khi truyền qua mạng Internet nên dù kẻ trộm có “chặn” cũng không thể đọc. Khi tới đích, người nhận sẽ sử dụng một công cụ đặc biệt để giải mã. Phương pháp mã hoá và bảo mật phổ biến nhất đang được thế giới áp dụng là chữ ký số (Digital signature). Với chữ ký số, người sử dụng có thể mã hoá thông tin một cách hiệu quả, chống giả mạo, xác thực danh tính người gửi. Ngoài ra chữ ký số còn là bằng chứng giúp chống chối cãi nguồn gốc, ngăn chặn người gửi chối cãi nguồn gốc tài liệu mình đã gửi.

Đối với các hoạt động trên môi trường mạng ngày càng phát triển như hiện nay, chữ ký số là một hình thức để bảo đảm tính pháp lý của các cam kết. Mặt