

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

NGUYỄN THỊ YẾN

**ỨNG DỤNG CHỮ KÝ SỐ TRONG BẢO MẬT
THÔNG TIN BƯU ĐIỆN TỈNH THÁI NGUYÊN**

Chuyên ngành: KHOA HỌC MÁY TÍNH

Mã số: 60 48 01

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

HƯỚNG DẪN KHOA HỌC: PGS.TS ĐOÀN VĂN BAN

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 6 năm 2012

Nguyễn Thị Yên

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 Trường Đại học công nghệ thông tin và truyền thông - 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 6 năm 2012

MỤC LỤC

LỜI CAM ĐOAN	1
LỜI CẢM ƠN	2
MỤC LỤC	3
DANH MỤC CÁC KÍ HIỆU VÀ CÁC TỪ VIẾT TẮT	6
DANH MỤC CÁC HÌNH	8
MỞ ĐẦU	10
1. Đặt vấn đề	10
2. Đối tượng và phạm vi nghiên cứu	10
3. Hướng nghiên cứu của đề tài	11
4. Những nội dung nghiên cứu chính	11
5. Tổng quan luận văn	11
CHƯƠNG 1: GIỚI THIỆU VỀ MÃ KHOÁ THÔNG DỤNG	13
1.1. Giới thiệu	13
1.2. Hệ mã khoá bí mật	13
1.3. Hệ mã khoá công khai	19
1.3.1. Các khái niệm cơ bản	19
1.3.2. Một số khái niệm toán học cơ sở	20
1.3.2.1. Modulo số học và các nhóm $Z(p)^*$, $G(p)$	20
1.3.2.2. Quan hệ “đồng dư”	23
1.3.2.3. Số nguyên tố mạnh	25
1.3.2.4. Định lý Fermat nhỏ	26
1.3.2.5. Định lý Lagrange	27
1.3.2.6. Định lý Euler	27
1.3.2.7. Định lý số dư trung hoa	27
1.3.3. Các nguyên lý của hệ mật khoá công khai	28

1.3.4. Một số hệ mã khoá công khai.....	30
1.3.4.1. Hệ mã khoá công khai RABIN.....	30
1.3.4.2. Hệ mã khoá công khai ELGAML	35
1.3.4.3. Hệ mã khoá công khai RSA	37
1.4. Độ an toàn của RSA	41
1.5. Quản lý khoá.....	41
1.5.1. Phân phối khoá cho giải thuật mật mã đối xứng	42
1.5.2. Phân phối khoá cho giải thuật mật mã bất đối xứng	44
1.5.3. Phát sinh và lưu giữ khoá bí mật	47
1.6. Kết luận chương	50
CHƯƠNG 2: CHỮ KÝ SỐ	53
2.1. Giới thiệu	53
2.2. Xác thực thông báo và các hàm xác thực	54
2.2.1. Xác thực thông báo.....	54
2.2.2 Các hàm xác thực.....	55
2.2.2.1. Mã hoá thông báo	55
2.2.2.2. Kỹ thuật xác thực dùng khoá bí mật – MAC.....	56
2.2.2.3. Các hàm băm	58
2.3. Chữ ký số	61
2.3.1. Khái niệm.....	61
2.3.1.1. Khái niệm.....	61
2.3.1.2. Sơ đồ chữ ký số	62
2.3.2. Các ưu điểm của chữ ký số.....	62
2.3.3. Quá trình thực hiện chữ ký số khoá công khai	64
2.3.4. Thuật toán chữ ký RSA	66
2.3.4.1. Sơ đồ.....	66
2.3.4.2. Ví dụ minh hoạ	67

2.3.4.3. Độ an toàn của chữ ký RSA	67
2.3.5. Thuật toán chữ ký DSA/DSS.....	69
2.3.5.1. Sơ đồ	69
2.3.5.2. Ví dụ	70
2.3.5.3. Độ an toàn chữ ký DSA.....	70
2.4. Các kiểu tấn công vào lược đồ chữ ký	77
2.5. Tính pháp lý và ứng dụng chữ ký số trong và ngoài nước.....	72
2.5.1. Trong nước.....	72
2.5.2. Ở một số nước trên thế giới	74
2.5.3. Ứng dụng trong thực tế.....	75
2.6. Kết luận chương.....	76
CHƯƠNG 3: CÀI ĐẶT DEMO CHƯƠNG TRÌNH	77
3.1 Lĩnh vực ứng dụng của chương trình	77
3.2. Chức năng của chương trình.....	78
3.2.1 Phân bảo mật thông tin	78
3.2.1.1 Chức năng mã hóa văn bản.....	78
3.2.1.2 Chức năng giải mã	79
3.2.2 Phân chữ ký số.....	79
3.2.2.1 Thực hiện ký văn bản	79
3.2.2.2 Kiểm tra và xác thực chữ ký.....	80
3.3. Một số màn hình giao diện của chương trình.....	81
3.3.1 Đăng nhập hệ thống.....	81
3.3.2 Một số menu chính	81
3.4. Kết luận chương.....	83
Kết quả và hướng phát triển	84
Kết quả đạt được của luận văn	84
Hướng phát triển	85

DANH MỤC CÁC KÝ HIỆU VÀ CÁC TỪ VIẾT TẮT

AES	Advance Encryption Standard
ASCII	American Standard Code for Information Interchange
ANSI	American National Standards Institute
DES	Data Encryption Standard
CA	Certificate Authority
FIPS	Federal Information Processing Standard
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
C	Bản mã.
\mathcal{C}	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	Bản rõ
\mathcal{M}	Không gian bản rõ
P	Bản tin rõ.
\mathcal{P}	Hàm số hoá bản rõ. $\mathcal{P} : \mathcal{M} \rightarrow Z_n$
$(n; e)$	Cặp số : n, e là các số nguyên dương.
(e, d)	Ước chung lớn nhất của hai số nguyên dương e và d .

DANH MỤC CÁC HÌNH

	Trang
<i>Hình 1.1 Quá trình thực hiện cơ chế mã hoá.....</i>	14
<i>Hình 1.2 Thuật toán giải mã của hệ DES.....</i>	16
<i>Hình 1.3 Quá trình thực hiện mã hoá khoá công khai.....</i>	19
<i>Hình 1.4 Sơ đồ khối nguyên lý hoạt động của mật mã khoá công khai.....</i>	29
<i>Hình 1.5 Sơ đồ biểu diễn thuật toán mã hóa</i>	37
<i>Hình 1.6 Minh họa quá trình mã hoá khoá công khai.....</i>	39
<i>Hình 1.7 Sơ đồ phân bố khóa của một mạng với một CKD.....</i>	43
<i>Hình 1.8 Sơ đồ phân bố khóa của một network với KD</i>	46
<i>Hình 1.9 Sơ đồ kiểm tra khoá.....</i>	49
<i>Hình 1.10 Sơ đồ bảo vệ khoá</i>	50
<i>Hình 2.1 (a) Lược đồ mã hoá thông báo.....</i>	55
<i>Hình 2.1(b) Mã hoá khoá công khai: xác thực và chữ ký.....</i>	55
<i>Hình 2.1(c) Mã hoá khoá công khai: Bí mật, xác thực và chữ ký</i>	56
<i>Hình 2.2 (a) Xác thực thông báo.....</i>	57
<i>Hình 2.2 (b) Bí mật và xác thực thông báo:Xác thực đối với bản rõ</i>	57
<i>Hình 2.2 (c) Xác thực đối với bản mã.....</i>	57
<i>Hình 2.3 Sơ đồ mô tả quá trình ký và gửi các tệp văn bản.....</i>	64
<i>Hình 2.4 Sơ đồ mô tả quá trình nhận các tệp văn bản</i>	65
<i>Hình 3.1 Chức năng tạo cặp khoá mã hoá</i>	78
<i>Hình 3.2 Nội dung văn bản sau khi mã hoá</i>	78
<i>Hình 3.3 Nội dung văn bản sau khi giải mã</i>	79
<i>Hình 3.4 Chọn tệp văn bản để ký</i>	79
<i>Hình 3.5 Thông báo đã ký văn bản</i>	80
<i>Hình 3.6 Xác lập thông tin người ký.....</i>	80

<i>Hình 3.7 Xác thực chữ ký</i>	<i>81</i>
<i>Hình 3.8 Đăng nhập hệ thống.....</i>	<i>81</i>
<i>Hình 3.9 Menu thao tác với tệp văn bản.....</i>	<i>81</i>
<i>Hình 3.10: Menu chỉnh sửa văn bản.....</i>	<i>82</i>
<i>Hình 3.11: Menu Định dạng văn bản</i>	<i>82</i>
<i>Hình 3.12: Menu Mã hoá và giải mã dữ liệu.....</i>	<i>82</i>