

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

NGÔ THU PHƯƠNG

**NGHIÊN CỨU CƠ SỞ HẠ TẦNG
KHÓA CÔNG KHAI PKI ỨNG DỤNG CHỨNG THỰC
CHO CÁC GIAO DỊCH HÀNH CHÍNH CÔNG ĐIỆN TỬ**

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

THÁI NGUYÊN - 2017

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

NGÔ THU PHƯƠNG

NGHIÊN CỨU CƠ SỞ HẠ TẦNG
KHÓA CÔNG KHAI PKI ỨNG DỤNG CHỨNG THỰC
CHO CÁC GIAO DỊCH HÀNH CHÍNH CÔNG ĐIỆN TỬ

Chuyên ngành: Khoa học máy tính

Mã số: 60.48.01.01

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Người hướng dẫn khoa học: TS. Phạm Thế Quế

THÁI NGUYÊN - 2017

LỜI CAM ĐOAN

Tôi cam đoan đây là công trình nghiên cứu của riêng tôi, dưới sự chỉ dẫn của TS. Phạm Thế Quế. Các số liệu, kết quả nêu trong luận văn là trung thực, luận văn này cho đến nay chưa được bảo vệ tại bất kỳ hội đồng nào và chưa hề được công bố trên bất kỳ phương tiện nào khác.

Thái nguyên, ngày tháng năm 2017

Tác giả luận văn

Ngô Thu Phương

LỜI CẢM ƠN

Em xin chân thành cảm ơn thầy giáo TS. Phạm Thế Quế đã tận tình hướng dẫn và tạo mọi điều kiện cho em hoàn thành luận văn.

Em xin chân thành cảm ơn các thầy cô giáo, các cán bộ nhân viên phòng đào tạo, ban lãnh đạo Trường Đại học Công nghệ thông tin và Truyền thông đã giúp đỡ tạo điều kiện cho em hoàn thành luận văn này.

Cuối cùng, em xin chân thành cảm ơn sự quan tâm giúp đỡ của gia đình, cơ quan, bạn bè và tập thể lớp Cao học K14B đã cổ vũ động viên em hoàn thành luận văn của mình.

Tuy đã cố gắng nhưng do thời gian và trình độ có hạn nên chắc chắn luận văn này còn nhiều thiếu sót và hạn chế nhất định. Kính mong nhận được sự góp ý của thầy cô và các bạn.

Thái nguyên, ngày tháng năm 2017

Học viên

Ngô Thu Phương

MỤC LỤC

LỜI CAM ĐOAN	i
LỜI CẢM ƠN	ii
MỤC LỤC	iii
DANH MỤC NHỮNG TỪ VIẾT TẮT	vi
DANH MỤC BẢNG	vii
DANH MỤC HÌNH	viii
MỞ ĐẦU	1
1. Lý do chọn đề tài	1
2. Ý nghĩa khoa học của đề tài	2
3. Đối tượng và phạm vi nghiên cứu	2
4. Những nội dung nghiên cứu chính	2
CHƯƠNG 1 CƠ SỞ HẠ TẦNG KHÓA CÔNG KHAI	3
1.1 Hệ mật mã khóa bất đối xứng [2]	3
1.1.1 Khái niệm	3
1.1.2 Thuật toán mật mã RSA	5
1.1.3 Chuyển đổi văn bản rõ	7
1.1.4 Đánh giá kỹ thuật mật mã bất đối xứng.....	8
1.1.5 Một số kỹ thuật phá mã RSA.....	9
1.1.6 Một số hệ mật mã khóa công khai khác	9
1.2 Hàm băm bảo mật	9
1.2.1 Giới thiệu.....	9
1.2.2 Các tính chất của hàm băm bảo mật	10
1.2.3 Ứng dụng hàm băm bảo mật	11
1.2.4 Hàm băm bảo mật SHA	12
1.2.5 Hàm băm MD5.....	13
1.3 Chữ ký số [2].....	14

1.3.1 Khái niệm chữ ký số	14
1.3.2 Quy trình tạo và kiểm tra chữ ký số	15
1.3.3 Những vấn đề còn tồn tại của chữ ký số	18
1.4 Cơ sở hạ tầng khóa công khai PKI [3]	19
1.4.1 Khái niệm	19
1.4.2 Chức năng chủ yếu của PKI	21
1.4.3 Các thành phần PKI	22
1.4.4 Các thủ tục trong PKI	23
1.4.5 Khái niệm chứng thực số	24
1.5 Một số thuật toán quản lý khóa [2]	25
1.5.1 Thuật toán trao đổi khoá Diffie-Hellman	25
1.5.2 Đánh giá độ an toàn thuật toán trao đổi khoá Diffie-Hellman	26
1.5.3 Quản lý khoá công khai trong mật mã bất đối xứng	27
1.5.4 Sử dụng mật mã bất đối xứng để trao đổi khoá bí mật	29
Kết luận chương	31
CHƯƠNG 2 KỸ THUẬT XÁC THỰC THÔNG TIN TRONG GIAO DỊCH ĐIỆN TỬ	32
2.1 Giới thiệu chung xác thực thông tin	32
2.2 Các kỹ thuật xác thực thông tin [2]	33
2.2.1 Sử dụng các thuật toán mật mã khóa đối xứng	34
2.2.2 Sử dụng các thuật toán mật mã khóa bất đối xứng	35
2.2.3 Sử dụng mã xác thực MAC	36
2.2.4 Sử dụng các hàm băm bảo mật	37
2.2.5 Xác thực thông tin dùng chữ ký điện tử	38
2.2.6 Xác thực thông tin dùng chữ ký điện tử và chứng thực điện tử	40
2.3 Các giao thức xác thực	42
2.3.1 Mật khẩu	42
2.3.2 Các giao thức xác thực trong mô hình điểm - điểm	43
2.3.3 Xác thực trong các hệ thống phân tán	44

2.3.4 Giao thức xác thực Kerberos 4.....	48
2.3.5 Giao thức xác thực Kerberos 5.....	52
Kết luận chương.....	55
CHƯƠNG 3 GIẢI PHÁP XÁC THỰC CHO CÁC GIAO DỊCH HÀNH CHÍNH CÔNG ĐIỆN TỬ	56
3.1 Dịch vụ hành chính công.....	56
3.1.1 Khái niệm.....	57
3.1.2 Các đặc trưng cơ bản của dịch vụ hành chính công.....	57
3.2 Mô hình xác thực người dùng hành chính công.....	58
3.2.1 Các thành phần hệ thống xác thực	58
3.2.2 Hệ thống ký hiệu	59
.....	60
3.2.3 Hoạt động hệ thống xác thực thông tin ... Error! Bookmark not defined.	
3.3 Các quy trình xác thực hệ thống thông tin hành chính công	60
3.3.1 Quy trình cấp và quản lý chứng thực khóa	60
3.3.2 Quy trình xác thực thông tin	63
3.3.3 Một số nhận xét.....	64
3.4 Cài đặt thử nghiệm	65
3.5 Đánh giá kết quả thử nghiệm..... Error! Bookmark not defined.	
KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN	68
TÀI LIỆU THAM KHẢO	70

DANH MỤC NHỮNG TỪ VIẾT TẮT

AES	Advanced Encryption Standard	Chuẩn mã hoá tiên tiến
ANSI	American National Standards Institute	Viện tiêu chuẩn quốc gia Mỹ
CA	Certification Authority	Nhà cung cấp chứng thực
CRL	Certificate Revocation List	Danh sách chứng thực thu hồi
DES	Data Encryption Standard	Chuẩn mã dữ liệu
DNS	Domain Name System	Hệ thống tên miền
DSA	Digital Signature Algorithm	Thuật toán chữ ký điện tử
DSS	Digital Signature Standard	Chuẩn chữ ký điện tử
EDI	Electronic Data Interchange	Trao đổi dữ liệu điện tử
FIPS	Federal Information Processing Standard	Chuẩn xử lý thông tin liên bang Mỹ
FTP	File Transfer Protocol	Giao thức truyền file
HTTP	Hyper Text Transport Protocol	Giao thức truyền siêu văn bản
IDEA	International Data Encryption Algorithm	Thuật toán mã hoá dữ liệu quốc tế
ISO	International Organization for Standardization	Tổ chức tiêu chuẩn hoá quốc tế
ISP	Internet Service Provider	Nhà cung cấp dịch vụ Internet
ITU	International Telecommunication Union	Liên minh viễn thông quốc tế
MD5	Message Digest 5	
NIST	National Institute of Standards and Technology	Viện quốc gia về chuẩn và công nghệ
OSI	Open System Interconnection	Kết nối giữa các hệ thống mở
PGP	Pretty Good Private	
PKI	Public Key Infrastructure	Cơ sở hạ tầng khoá công khai
RA	Registration Authority	Nhà quản lý đăng ký
RSA	Rivest-Shamir-Aldeman	
SET	Secure Electronic Transaction	Giao dịch điện tử an toàn
SHA	Secure Hash Algorithm	Thuật toán băm an toàn
TCP/IP	Transmission Control Protocol / Internet protocol	Giao thức điều khiển truyền dẫn/ giao thức Internet
URL	Uniform Resource Locator	Bộ định vị tài nguyên

DANH MỤC BẢNG

Bảng 1.1: Các phiên bản SHA	13
Bảng 1.2: So sánh các thông số giữa SHA-1 và MD5.....	13
Bảng 3.1: Kết quả thử nghiệm	67

DANH MỤC HÌNH

Hình 1.1: Cấu trúc hệ thống mật mã khóa bất đối xứng	5
Hình 1.2: Một ứng dụng điển hình của hàm băm	10
Hình 1.3: Định nghĩa chữ ký số	15
Hình 1.4: Sơ đồ tổng quát tạo chữ ký số	16
Hình 1.5: Sơ đồ tổng quát kiểm tra chữ ký số	17
Hình 1.6: Sơ đồ tổng quát tạo và kiểm tra chữ ký số	17
Hình 1.7: Các thành phần cơ bản của một PKI	23
Hình 1.8: Thuật toán trao đổi khoá Diffie-Hellman	26
Hình 1.9: Dùng mật mã bất đối xứng để trao đổi khoá	29
Hình 2.1: Xác thực thông tin dùng mật mã đối xứng	34
Hình 2.2: Sử dụng khóa bất đối xứng để trao đổi khóa bí mật	35
Hình 2.3: Xác thực thông tin dùng mật mã bất đối xứng	35
Hình 2.4: Xác thực thông tin dùng MAC	36
Hình 2.5: Xác thực thông tin dùng hàm băm	37
Hình 2.6: Xác thực dùng hàm băm và mật mã bất đối xứng	38
Hình 2.7: Xác thực thông tin dùng chữ ký số	39
Hình 2.8: Xác thực thông tin dùng chữ ký số	39
Hình 2.9: Minh họa xác thực sử dụng chứng chỉ số và chữ ký điện tử	40
Hình 2.10: Sơ đồ minh họa quá trình xin cấp chứng chỉ số	41
Hình 2.11: Giao thức xác thực PAP	44
Hình 2.12: Giao thức xác thực CHAP	44
Hình 2.13: Thủ tục xác thực Kerberos 4	49
Hình 2.14: Xác thực giữa hai lãnh địa Kerberos	52
Hình 3.1: Mô hình tổng quát cấp chứng thực khóa	62
Hình 3.2: Quy trình khởi tạo chứng thực khóa cho người sử dụng	63
Hình 3.3: Giao diện chương trình demo chữ ký số... Error! Bookmark not defined.	
Hình 3.4: Giao diện kiểm tra chuỗi toàn vẹn	Error! Bookmark not defined.