

**ĐẠI HỌC THÁI NGUYÊN**  
**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN & TRUYỀN THÔNG**

**NGÔ THỊ THANH HẢI**

**NGHIÊN CỨU GIẢI PHÁP BẢO MẬT VÀ XÁC THỰC  
CHO CÁC GIAO DỊCH HÀNH CHÍNH CÔNG ĐIỆN TỬ  
– SỞ THÔNG TIN VÀ TRUYỀN THÔNG BẮC NINH**

**LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH**

Thái Nguyên - 2017

**ĐẠI HỌC THÁI NGUYÊN**  
**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN & TRUYỀN THÔNG**

**NGÔ THỊ THANH HẢI**

**NGHIÊN CỨU GIẢI PHÁP BẢO MẬT VÀ XÁC THỰC  
CHO CÁC GIAO DỊCH HÀNH CHÍNH CÔNG ĐIỆN TỬ  
– SỞ THÔNG TIN VÀ TRUYỀN THÔNG BẮC NINH**

**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 CẢM ƠN

Lời đầu tiên, tôi xin cảm ơn TS. Phạm Thế Quế, Giảng viên Học viện công nghệ bưu chính viễn thông đã định hướng đề tài và tận tình hướng dẫn, chỉ bảo tôi trong suốt quá trình thực hiện luận văn.

Tôi xin chân thành cảm ơn các thầy, cô trong Trường Đại học Công nghệ thông tin và truyền thông Thái Nguyên đã truyền đạt kiến thức và tạo điều kiện trong thời gian học tập.

Cuối cùng, tôi xin được gửi lời cảm ơn tới gia đình và bạn bè, những người đã luôn bên cạnh, giúp đỡ và động viên tôi trong quá trình học tập cũng như trong suốt quá trình thực hiện luận văn.

Mặc dù đã rất nỗ lực, cố gắng nhưng chắc chắn luận văn của tôi vẫn còn nhiều thiếu sót. Tôi rất mong nhận được những ý kiến đóng góp, chia sẻ của quý thầy cô, anh chị và các bạn.

Tôi xin chân thành cảm ơn!

*Thái Nguyên, ngày tháng 6 năm 2017*

**Người thực hiện**

**Ngô Thị Thanh Hải**

## LỜI CAM ĐOAN

Tôi xin cam đoan luận văn cao học “*Nghiên cứu giải pháp bảo mật và xác thực cho các giao dịch hành chính công điện tử – Sở Thông tin và Truyền thông Bắc Ninh*” của tôi được thực hiện dưới sự hướng dẫn của giáo viên hướng dẫn là TS. Phạm Thế Quế. Các nội dung trong luận văn đều được ghi rõ nguồn gốc ở phía cuối luận văn.

Nếu có phát hiện nào về sự gian lận trong sao chép tài liệu, công trình nghiên cứu của tác giả khác mà không được ghi rõ trong phần tài liệu tham khảo, tôi sẽ chịu hoàn toàn trách nhiệm về kết quả luận văn của mình.

*Thái Nguyên, ngày tháng 6 năm 2017*

**Người thực hiện**

**Ngô Thị Thanh Hải**

# MỤC LỤC

Trang

<b>DANH MỤC CÁC KÝ HIỆU, CÁC CHỮ VIẾT TẮT</b> .....	i
<b>DANH MỤC BẢNG BIỂU</b> .....	iii
<b>DANH MỤC CÁC HÌNH</b> .....	iv
<b>MỞ ĐẦU</b> .....	1
<b>CHƯƠNG I: TỔNG QUAN AN TOÀN BẢO MẬT HỆ THỐNG THÔNG TIN</b> ..	3
1.1 Khái niệm chung về an toàn thông tin [1].....	3
1.1.1 Giới thiệu .....	3
1.1.2 Các mục tiêu an toàn thông tin [2] .....	4
1.1.3 Các tiêu chí đánh giá một hệ thống thông tin an toàn, bảo mật	5
1.1.4 Các hành vi vi phạm an toàn và bảo mật thông tin .....	7
1.1.5 Một số hình thức tấn công hệ thống thông tin [2].....	8
1.2 Kỹ thuật phát hiện và ngăn chặn xâm nhập [3] .....	11
1.2.1 Tường lửa (Firewall) .....	11
1.2.2 Hệ thống phát hiện xâm nhập.....	14
1.3 Bảo vệ thông tin bằng kỹ thuật mật mã [1].....	15
1.3.1 Hệ mật mã .....	15
1.3.2 Bảo vệ thông tin bằng kỹ thuật mật mã khoá đối xứng .....	17
1.3.3 Thuật toán trao đổi khoá Diffie-Hellman.....	19
1.4 Bảo vệ thông tin bằng mật mã khoá bất đối xứng [1] .....	21
1.4.1 Khái niệm .....	21
1.4.2 Thuật toán mật mã RSA .....	23
1.4.3 Chuyển đổi văn bản rõ .....	25
1.4.4 Đánh giá kỹ thuật mật mã bất đối xứng .....	26
1.4.5 Một số hệ mật mã khoá công khai khác.....	27
<b>CHƯƠNG II: XÁC THỰC DÙNG CHỮ KÝ ĐIỆN TỬ VÀ CHỨNG THỰC SỐ</b> .....	28
2.1 Cơ chế xác thực nguồn gốc thông tin [8].....	28

2.1.1	Giới thiệu chung.....	28
2.1.2	Kỹ thuật xác thực thông tin.....	28
2.2	Hàm băm bảo mật.....	32
2.2.1	Hàm băm bảo mật là gì.....	32
2.2.2	Ứng dụng hàm băm bảo mật.....	33
2.2.3	Hàm băm bảo mật SHA.....	34
2.2.4	Hàm băm MD5.....	35
2.3	Chữ ký số [8].....	36
2.3.1	Khái niệm.....	36
2.3.2	Phân loại chữ ký số.....	38
2.3.3	Các phương pháp thực hiện chữ ký số.....	38
2.3.4	Chuẩn chữ ký DSS.....	40
2.3.5	Thuật toán tạo chữ ký DSA.....	42
2.3.6	Những vấn đề còn tồn tại của chữ ký số.....	43
2.4	Cơ sở hạ tầng khóa công khai PKI [9].....	44
2.4.1	Khái niệm.....	44
2.4.2	Chức năng chủ yếu của PKI.....	47
2.4.3	Các thành phần PKI.....	48
2.4.4	Các thủ tục trong PKI.....	50
2.4.5	Ưu nhược điểm của việc ứng dụng hệ thống PKI.....	50
2.5	Chứng thực số trong môi trường hạ tầng khóa công khai PKI [9].....	51
2.5.1	Khái niệm.....	51
2.5.2	Xác thực thông tin dùng chữ ký điện tử và chứng thực điện tử..	53
<b>CHƯƠNG III: CÀI ĐẶT VÀ THỬ NGHIỆM BÀI TOÁN XÁC THỰC CHO</b>		
<b>CÁC GIAO DỊCH HÀNH CHÍNH CÔNG ĐIỆN TỬ</b> .....		56
3.1	Mô hình giao dịch Chính phủ - Công dân (G to C).....	56
3.1.1	Khái niệm.....	56
3.1.2	Hệ thống giao dịch hành chính công điện tử.....	56
3.1.3	Mô hình xác thực hệ thống thông tin liên thông.....	57
3.1.4	Các mức độ dịch vụ hành chính công.....	58
3.1.5	Thủ tục sử dụng các dịch vụ hành chính công một cửa.....	58

3.2	Nhu cầu triển khai chữ ký điện tử cho các giao dịch hành chính công tại Sở Thông tin và Truyền thông.....	59
3.2.1	Hiện trạng dịch vụ công.....	59
3.2.2	Các điểm yếu về bảo mật trong giao dịch hành chính công .....	60
3.3.3	Ứng dụng PKI và các yêu cầu của Sở TT&TT .....	60
3.3	Một số đề xuất về tổ chức cung cấp quản lý chứng chỉ số .....	61
3.3.1	Đề xuất mô hình CA .....	61
3.3.2	Kiến trúc các thành phần thiết bị .....	61
3.3.3	Tính năng sản phẩm đề xuất .....	61
3.4	Giải pháp triển khai.....	60
3.4.1	Xây dựng một hệ thống CA riêng tại Sở TT&TT.....	63
3.4.2	Đăng ký sử dụng với một tổ chức cung cấp dịch vụ chứng thực số	63
3.4.3	Lưu trữ và bảo vệ khóa bí mật sử dụng cho chữ ký số .....	63
3.5	Triển khai thử nghiệm.....	64
3.5.1	Ứng dụng java mô phỏng quá trình ký và xác thực chữ ký .....	64
3.5.2	Kết quả thử nghiệm.....	65
	<b>KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN</b> .....	67
	<b>TÀI LIỆU THAM KHẢO</b> .....	69

## DANH MỤC CÁC KÝ HIỆU, CÁC CHỮ 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	Thuật toán mã hóa
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	Bảo mật rất mạnh
PKI	Public Key Infrastructure	Cơ sở hạ tầng khoá công khai

RA	Registration Authority	Nhà quản lý đăng ký
RSA	Rivest-Shamir-Aldeman	Thuật toán mật mã hóa khóa công khai
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
URL	Uniform Resource Locator	Bộ định vị tài nguyên
AES	Advanced Encryption Standard	Chuẩn mã hoá tiên tiến
ANSI	American National Standards Institute	Viện tiêu chuẩn quốc gia Mỹ
CA	Certification Authority CRL	Nhà cung cấp chứng thực
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
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

**DANH MỤC BẢNG BIỂU**

Bảng 2.1. Các phiên bản SHA.....	35
Bảng 2.2. So sánh các thông số giữa SHA-1 và MD5.....	36
Bảng 3.1. Kết quả thử nghiệm.....	66