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

DANH MỤC CÁC KÝ HIỆU, CÁC CHỮ VIẾT TẮT

AES	Advanced Encryption Standard	Chuẩn mã hoá tiên tiến
ANSI	American National Standards Institude	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 Ecryption 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	Thuật toán mã hoá dữ liệu quốc tế
ISO	Algorithm International Organization for Standardization	Tổ chức tiêu chuẩn hoá quốc tế
ISP	Internet Service Provider Internet	Nhà cung cấp dịch vụ
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 Institude	Viện tiêu chuẩn quốc gia Mỹ
CA	Certification Authority CRL	Nhà cung cấp chứng thực
DES	Data Ecryption 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