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

DANH MỤC NHỮNG TỪ 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 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

DANH MỤC HÌNH