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

Thái Nguyên – 2012

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 Yến

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

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.
$\mathscr{C}$	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