

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

MAI THỊ HOA HUỆ

**NGHIÊN CỨU XÂY DỰNG BẢO MẬT VÀ XÁC THỰC
TÀI LIỆU ĐIỆN TỬ DỰA TRÊN PKI VÀ ỨNG DỤNG
VÀO TRƯỜNG ĐẠI HỌC HẠ LONG**

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

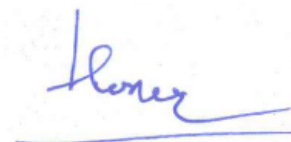
MAI THỊ HOA HUỆ

NGHIÊN CỨU XÂY DỰNG BẢO MẬT VÀ XÁC THỰC
TÀI LIỆU ĐIỆN TỬ DỰA TRÊN PKI VÀ ỨNG DỤNG
VÀO TRƯỜNG ĐẠI HỌC HẠ LONG

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. Hồ Văn Hương



THÁI NGUYÊN - 2017

LỜI CAM ĐOAN

Tác giả xin cam đoan rằng số liệu và kết quả nghiên cứu trong luận văn là hoàn toàn trung thực chưa hề được sử dụng và công bố trong bất kỳ một công trình khoa học nào. Các thông tin, tài liệu trình bày trong luận văn đã được ghi rõ nguồn gốc.

Tác giả luận văn

Mai Thị Hoa Huệ

LỜI CẢM ƠN

Trong quá trình học tập, nghiên cứu viết luận văn, được sự giúp đỡ của Trường Đại học Công nghệ Thông tin và Truyền thông, các thầy giáo, cô giáo, các tổ chức, đồng nghiệp trong và ngoài tỉnh đã tạo điều kiện về vật chất, thời gian và cung cấp tài liệu giúp đỡ tôi hoàn thành luận văn.

Tôi xin chân thành cảm ơn sự giúp đỡ quý báu của các thầy, cô giáo, các tổ chức, đồng nghiệp và người hướng dẫn khoa học **TS. Hồ Văn Hương** đã hết lòng hướng dẫn và giúp đỡ tôi rất nhiều trong nghiên cứu khoa học và thực hiện hoàn thành luận văn này.

Tác giả xin trân trọng cảm ơn!

Tác giả luận văn

Mai Thị Hoa Huệ

MỤC LỤC

LỜI CAM ĐOAN	i
LỜI CẢM ƠN	ii
MỤC LỤC	iii
DANH MỤC CÁC TỪ VIẾT TẮT	vi
DANH MỤC CÁC BẢNG.....	vii
DANH MỤC CÁC HÌNH.....	viii
MỞ ĐẦU	1
1. Nhu cầu bảo mật và xác thực văn bản điện tử	1
2. Lý do chọn đề tài.....	1
3. Mục đích nghiên cứu.....	1
4. Phương pháp nghiên cứu.....	2
5. Bố cục của luận văn	2
CHƯƠNG 1: GIỚI THIỆU CHUNG VỀ MẬT MÃ	3
1.1. Mật mã khóa đối xứng	3
1.1.1. Khái niệm.....	3
1.1.2. Bảo vệ tính bí mật của thông tin với mật mã khóa đối xứng	3
1.2 . Mật mã khóa công khai.....	4
1.2.1. Khái niệm.....	4
1.2.2 . Bảo vệ thông tin với mật mã khóa công khai.....	4
1.2.3. Thuật toán RSA	6
1.2.4. Hệ mật ElGamal trên đường cong elliptic	7
1.2.5. Sơ đồ trao đổi khóa Elliptic	9
1.2.6. Thuật toán chữ ký số Elliptic (ECDSA)	10
1.2.7. So sánh giữa Elliptic và RSA	11
1.3. Kết hợp mật mã đối xứng và mật mã khóa công khai	13
1.4. Kết luận chương 1	14

CHƯƠNG 2: CƠ SỞ HẠ TẦNG KHÓA CÔNG KHAI	15
2.1. Khái niệm về PKI và các khái niệm cơ bản trong PKI	15
2.1.1. Khái niệm PKI	15
2.1.2. Các khái niệm cơ bản trong PKI.....	15
2.2. Các thành phần PKI	20
2.2.1. Tổ chức chứng thực	21
2.2.2. Trung tâm đăng ký	21
2.2.3. Người dùng cuối	22
2.2.4 . Hệ thống lưu trữ	22
2.3. Các dịch vụ PKI	23
2.3.1. Các dịch vụ cốt lõi của PKI	23
2.3.2. Các dịch vụ PKI hỗ trợ	25
2.4. Các mô hình kiến trúc PKI.....	27
2.4.1. Kiến trúc kiểu CA đơn (Single CA)	28
2.4.2. Kiến trúc kiểu CA phân cấp.....	28
2.4.3. Kiến trúc kiểu chứng thực chéo (Cross – certificate)	29
2.4.4. Kiến trúc kiểu Bridge CA	30
2.5. Ứng dụng của PKI trong ký số và bảo mật dữ liệu.....	31
2.5.1. Mã hóa	31
2.5.2. Chống giả mạo	32
2.5.3. Xác thực	32
2.5.4. Chống chối bỏ nguồn gốc	32
2.5.5. Chữ ký điện tử	32
2.5.6. Bảo mật website.....	33
2.5.7. Code Signing.....	33
2.5.8. Chứng thực điện tử	34
2.6. Kết luận chương 2	34

CHƯƠNG 3: XÂY DỰNG ỨNG DỤNG BẢO MẬT VÀ XÁC THỰC

TÀI LIỆU ĐIỆN TỬ	35
3.1. Phân tích	35
3.2. Thiết kế	35
3.3. Các chức năng trong phần mềm	36
3.4. Xây dựng giao diện	37
3.5. Thiết kế lớp	39
3.6. Cài đặt và kiểm thử	41
3.7. Kết luận chương 3	50
KẾT LUẬN	51
TÀI LIỆU THAM KHẢO	53

DANH MỤC CÁC TỪ VIẾT TẮT

CNTT	Công nghệ thông tin
ATTT	An toàn thông tin
CA	Certificate Authority
PKI	Public Key Infastructure
SPKC	Simple Public Key Certificate
AC	Attribute Certificate
ITU	International Telecommunication Union
CRLs	Certificate Revocation Lists
RA	Registration Authorites
DSAs	Directory System Agents
OCSP	Online Certificate Status Protocol
LDAP	Lightweight Directory Access Protocol
DNS	Domain Name System
FTP	File Transfer Protocol
MAC	Message Authentication Code
P2P	Peer to Peer
SSL	Secure Socket Layer

DANH MỤC CÁC BẢNG

Bảng 1.1. So sánh sử dụng RSA và ECC trong quá trình bắt tay của SSL 12

Bảng 1.2. So sánh kích thước khóa RSA và ECC với cùng mức độ an toàn . 12

DANH MỤC CÁC HÌNH

Hình 1.1: Mã hóa khóa bí mật.....	4
Hình 1.2: Mã hóa khóa công khai	5
Hình 1.3: Xác thực thông tin.....	5
Hình 1.4: Ký và mã với khóa công khai	6
Hình 1.5: So sánh mức độ bảo mật giữa ECC với RSA/DSA	12
Hình 1.6: Kết hợp khóa công khai và khóa bí mật	14
Hình 2.1: Chứng thư số.....	15
Hình 2.2: Các thành phần PKI	20
Hình 2.3: Single CA.....	28
Hình 2.4: CA phân cấp.....	29
Hình 2.5: Chứng thực chéo	30
Hình 2.6: Bridge CA	31
Hình 3.1: Giao diện xác thực khóa cá nhân	38
Hình 3.2: Giao diện chính	38
Hình 3.3: Giao diện thông báo	39
Hình 3.4: Lớp Crypto	39
Hình 3.5: Lớp ECDH	40
Hình 3.6: Lớp Data Transfrmer.....	40
Hình 3.7: Lớp ECDSA_Signature.....	41
Hình 3.8: XML Work.....	41
Hình 3.9: Xác thực người dùng.....	42
Hình 3.10: Thông báo file không phải là khóa cá nhân	42
Hình 3.11: Xác thực thất bại	42
Hình 3.12: Xác thực đúng	43
Hình 3.13: Giao diện chính của chương trình.....	43
Hình 3.14: Thông báo cho người dùng kết quả	43
Hình 3.15: file .sign chứa chữ ký.....	44