

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

ĐỖ VĂN CẢNH

**NGHIÊN CỨU HỆ THỐNG CHỨNG THỰC SỐ
VÀ TRIỂN KHAI ỨNG DỤNG**

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Thái Nguyên - 2014

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

ĐỖ VĂN CẢNH

**NGHIÊN CỨU HỆ THỐNG CHỨNG THỰC SỐ
VÀ TRIỂN KHAI ỨNG DỤNG**

Chuyên ngành: Khoa học máy tính

Mã số: 60 48 01

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Người hướng dẫn khoa học: TS.Hồ Văn Hương

Thái Nguyên- 2014

LỜI CAM ĐOAN

Tôi xin cam đoan rằng, đây là công trình nghiên cứu của tôi trong đó có sự giúp đỡ tận tình của thầy hướng dẫn Tiến Sĩ Hồ Văn Hương, và sự hỗ trợ của các đồng nghiệp và một số bạn của tôi. Các nội dung nghiên cứu và kết quả trong đề tài này là hoàn toàn trung thực.

Trong luận văn, tôi có tham khảo đến một số tài liệu của một số tác giả và một số website đã được liệt kê tại phần Tài liệu tham khảo ở cuối luận văn.

Thái Nguyên, ngày tháng năm 2014

Tác giả

Đỗ Văn Cảnh

LỜI CẢM ƠN

Để hoàn thành chương trình cao học và viết luận văn này, chúng tôi đã nhận được sự hướng dẫn, giúp đỡ và góp ý nhiệt tình của quý thầy cô trường Đại học Công nghệ thông tin và truyền thông Thái Nguyên.

Trước hết, chúng tôi xin chân thành cảm ơn đến quý thầy cô giáo trường Đại học Công nghệ thông tin và truyền thông Thái Nguyên, đặc biệt là những thầy cô đã tận tình dạy bảo cho chúng tôi trong suốt thời gian học tập tại trường.

Tôi xin gửi lời biết ơn sâu sắc đến Tiến sĩ Hồ Văn Hương đã dành rất nhiều thời gian và tâm huyết hướng dẫn nghiên cứu và giúp tôi hoàn thành luận văn tốt nghiệp.

Nhân đây, tôi xin chân thành cảm ơn Ban Giám hiệu trường Đại học công nghệ thông tin và truyền thông Thái Nguyên đã tạo rất nhiều điều kiện để chúng tôi học tập và hoàn thành tốt khóa học.

Mặc dù tôi đã có nhiều cố gắng hoàn thiện luận văn bằng tất cả sự nhiệt tình và năng lực của mình, tuy nhiên không thể tránh khỏi những thiếu sót, tôi rất mong nhận được những đóng góp quý báu của quý thầy cô và các bạn.

Lời cảm ơn sau cùng chúng tôi xin dành cho gia đình, đồng nghiệp và những người bạn đã hết lòng quan tâm và tạo điều kiện tốt nhất để tôi hoàn thành luận văn tốt nghiệp này!

Tôi xin chân thành cảm ơn!

Thái Nguyên, ngày tháng 1 năm 2014

Người thực hiện

Đỗ Văn Cảnh

MỤC LỤC

MỤC LỤC	i
DANH MỤC HÌNH VẼ	iii
DANH MỤC CÁC CHỮ VIẾT TẮT	iv
LỜI NÓI ĐẦU	1
Chương 1:TÌM HIỂU VỀ LÝ THUYẾT MẬT MÃ	3
1.1. Mật mã khoá đối xứng.....	4
1.1.1. Khái niệm.....	4
1.1.2. Bảo vệ tính bí mật của thông tin với mật mã khoá đối xứng	4
1.1.3. Ưu nhược điểm của mật mã khoá đối xứng	4
1.2. Mật mã khoá công khai	5
1.2.1. Khái niệm.....	5
1.2.2. Bảo vệ thông tin với mật mã khoá công khai	5
1.2.3. Ưu nhược điểm của mật mã khoá công khai	7
1.2.4. Thuật toán RSA	8
1.3. Sử dụng kết hợp mật mã khoá đối xứng và khoá công khai	9
1.4. Chữ ký số.....	10
1.5. Hàm băm.....	12
Chương 2:HẠ TẦNG KHÓA CÔNG KHAI	14
2.1. Các khái niệm cơ bản	14
2.1.1. Khái niệm PKI	14
2.1.2. Các khái niệm liên quan	15
2.2. Các thành phần của PKI	20
2.2.1. Tổ chức chứng thực	20
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. Cách thức hoạt động và chức năng của PKI.....	22
2.3.1. Quá trình khởi tạo cặp khoá – Key Pair Generation.....	24
2.3.2. Quá trình tạo chữ ký số - Digital Signature Generation	25
2.3.3. Quá trình mã hoá thông điệp và gắn chữ ký số - Message Encrytion and Digital Signature Application	25

2.3.4. Quá trình nhận thông điệp và gửi sự kiểm chứng xác nhận	26
2.3.5. Quá trình giải mã thông điệp	26
2.3.6. Quá trình kiểm tra nội dung thông điệp.....	26
2.4. Các dịch vụ của PKI	26
2.4.1. Các dịch vụ cốt lõi của PKI	26
2.4.2. Các dịch vụ PKI hỗ trợ	30
2.5. Các mô hình kiến trúc của PKI.....	33
2.5.1. Mô hình kiến trúc đơn.....	33
2.5.2. Mô hình danh sách tin cậy	34
2.5.3. Mô hình phân cấp	35
2.5.4. Mô hình mạng lưới	37
2.5.5. Kiến trúc CA bắc cầu _ Bridge CA Architecture	40
2.6. Ứng dụng của PKI trong ký số và bảo mật dữ liệu	41
2.6.1. Mã hóa	41
2.6.2. Chống giả mạo	41
2.6.3. Xác thực	41
2.6.4. Chống chối bỏ nguồn gốc	42
2.6.5. Chữ ký số	42
2.6.6. Bảo mật website.....	42
2.6.7. Code Signing	42
2.6.8. Chứng thực số.....	43
2.7. Thực trạng PKI ở Việt Nam	44
2.7.1. Các văn bản của Đảng và Nhà nước quy định về chứng thực chữ ký số	44
2.7.2. Một số nhà cung cấp dịch vụ chứng thực chữ ký số công cộng đầu tiên tại Việt Nam.....	45
Chương 3: ỨNG DỤNG MÔ HÌNH PKI TRONG HỆ THỐNG MAIL AN TOÀN ...	47
VÀ WEB AN TOÀN.....	47
3.1. Ứng dụng mô hình PKI trong hệ thống mail an toàn.	47
3.1.1. Xây dựng mô hình và mô tả hoạt động của mô hình:.....	47
3.1.2. Hướng dẫn thực hiện	48
3.2. Ứng dụng mô hình PKI trong hệ thống Web an toàn.....	65
3.2.1. Xây dựng mô hình và mô tả hoạt động :	65

3.2.2. Hướng dẫn thực hiện:	65
TÀI LIỆU THAM KHẢO	74

DANH MỤC HÌNH VẼ

Hình 1.1. Mã hóa khóa bí mật	4
Hình 1.2. Mã hóa khóa công khai.....	6
Hình 1.3. Xác thực thông tin	6
Hình 1.4. Ký và mã hoá với khóa công khai	7
Hình 1.5. Kết hợp mật mã khóa đối xứng và công khai - Quá trình mã hoá	9
Hình 1.6. Kết hợp mật mã khóa đối xứng và công khai - Quá trình giải mã	10
Hình 1.7. Quy trình tạo chữ ký số và xác minh chữ ký số	12
Hình 2.1. Chứng thư số	15
Hình 2.2. Các thành phần PKI.....	20
Hình 2.3. Mô hình hoạt động của PKI.....	23
Hình 2.4. Mô hình khoá công khai dùng đảm bảo tính bí mật	24
Hình 2.5. Mô hình dùng khoá công khai để xác thực	25
Hình 2.6. Mô hình khoá công khai bí mật và xác thực	26
Hình 2.7. Xác thực từ xa sử dụng cặp ID/Mật khẩu.....	28
Hình 2.8. Xác thực từ xa dựa trên khoá công khai.....	29
Hình 2.9. Mô hình kiến trúc CA đơn.....	33
Hình 2.10. Mô hình kiến trúc danh sách tin cậy CA	34
Hình 2.11. Mô hình kiến trúc CA phân cấp	35
Hình 2.12. Mô hình kiến trúc CA lưới	37
Hình 2.13. Mô hình kiến trúc cầu CA	40
Hình 3.1. Mô hình PKI trong hệ thống mail an toàn.....	47
Hình 3.2. Request chứng thư	48
Hình 3.4. Mô hình PKI trong hệ thống web an toàn	65
Hình 3.5. Request chứng thư trong web.....	65

DANH MỤC CÁC CHỮ VIẾT TẮT

STT	TÊN VIẾT TẮT	TÊN ĐẦY ĐỦ	DỊCH RA TIẾNG VIỆT
1	CA	Certificate Authority	Thẩm quyền chứng thực
2	CRLs	Certificate Revocation Lists	
3	DES	Data Encryption Standard	Chuẩn mã hóa dữ liệu
4	HTTP	Hypertext Transfer Protocol	Giao thức truyền tải siêu văn bản
5	HTTPS	Secure Hypertext Transfer Protocol	Giao thức truyền tải siêu văn bản an toàn
6	ITU	International Telecommunication Union	Hiệp hội viễn thông quốc tế
7	LDAP	Lightweight Directory Access Protocol	Giao thức truy cập thư mục
8	MAC	Message Authentication Code	Xác thực mã ti nhắn
9	OCSP	Online Certificate Status Protocol	Trạng thái giao thức chứng chỉ trực tuyến
10	PKCS	Public Key Cryptography Standards	Chuẩn mật mã khóa công khai
11	PKI	Public Key Infrastructure	Cơ sở hạ tầng khóa công khai
12	RA	Registration Authority	Thẩm quyền đăng ký
13	RSA	Rivest Shamir Adleman	Thuật toán mã hóa RSA
14	SHA	Secure Hash Algorithm	Thuật toán băm
15	SSL	Secure Socket Layer	Giao thức bảo mật web

LỜI NÓI ĐẦU

Ngày nay, công nghệ thông tin phát triển rất nhanh và được ứng dụng vào hầu hết những lĩnh vực trong cuộc sống. Vai trò của công nghệ thông tin ngày càng được nâng cao, không chỉ dừng lại ở những ứng dụng văn phòng, công nghệ thông tin còn được triển khai ở nhiều lĩnh vực. Bên cạnh những lợi thế trong việc áp dụng công nghệ thông tin, việc sử dụng CNTT còn tiềm ẩn nhiều vấn đề còn tồn tại, trong đó có việc đảm bảo an toàn thông tin ví dụ như bị đánh cắp dữ liệu, được phép đọc các tài liệu mà không đủ thẩm quyền, dữ liệu bị phá hủy ... Do đó, bên cạnh việc triển khai và sử dụng CNTT, chúng ta cũng phải đảm bảo ATTT. Đảm bảo ATTT chính là đảm bảo hệ thống có được ba yếu tố:

- Tính toàn vẹn
- Tính bí mật
- Tính sẵn sàng

Trong lĩnh vực ATTT, sử dụng chứng thư số đã trở thành một trong các phương pháp giúp chúng ta có thể bảo mật thông tin. Với chứng thư số, người sử dụng có thể mã hóa thông tin một cách hiệu quả, chống giả mạo thông tin, xác thực người gửi. Ngoài ra, chứng thư số còn là bằng chứng giúp chống chối cãi nguồn gốc, ngăn chặn người gửi chối cãi nguồn gốc tài liệu mình đã gửi.

PKI là một cơ sở hạ tầng khóa công khai, phục vụ an toàn thông tin. PKI sẽ giúp người dùng xác thực được chủ thể của chứng thư số, cũng như có thể an tâm về tính xác thực của chứng thư số.

Ở Việt Nam hiện nay đã có một số đơn vị cung cấp và triển khai dịch vụ chứng thực số như Ban Cơ yếu Chính phủ, Bộ Thông Tin Truyền Thông, VNPT, Viettel, FPT, BKAV ... Các ứng dụng sử dụng chứng thực số ở Việt Nam chủ yếu là ký, mã hóa dữ liệu, email, web, xác thực quyền truy cập, thanh toán số, ...

Bộ cục đề tài luận văn gồm có 3 phần, với nội dung từng phần cụ thể như sau:

Chương 1: Tìm hiểu về lý thuyết mật mã với các chủ đề chính: mật mã khoá đối xứng, mật mã khoá công khai, hàm băm và chữ ký số làm cơ sở cho việc tìm hiểu hạ tầng khoá công khai PKI.

Chương 2: Hạ tầng khoá công khai đề tài luận văn trình bày về định nghĩa PKI, chức năng chính, các thành phần của PKI, các mô hình kiến trúc, các dịch vụ của PKI và các nhà cung cấp dịch vụ chữ ký số công cộng đầu tiên tại Việt Nam.

Chương 3: Ứng dụng mô hình PKI trong hệ thống mail an toàn, và web an toàn.

Trước khi đi vào trình bày chi tiết nội dung đề tài, em xin gửi lời cảm ơn chân thành tới các thầy cô Trường Đại Học Công Nghệ Thông Tin và Truyền Thông Thái Nguyên. Đặc biệt, em xin gửi lời cảm ơn chân thành tới TS. Hồ Văn Hương, Ban Cơ yếu Chính phủ đã định hướng và giúp đỡ nhiệt tình để em hoàn thành đề tài luận văn này.

Do thời gian hoàn thành đề tài có hạn cũng như khả năng nghiên cứu còn hạn chế cho nên em không tránh khỏi những khiếm khuyết, em rất mong có được những góp ý và giúp đỡ của các thầy cô giáo để em có thể tiếp tục đề tài này ở mức ứng dụng cao hơn trong tương lai.

Em xin chân thành cảm ơn.

Học Viên

Đỗ Văn Cảnh