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

PHAN THỊ KIM QUẾ

PHÁT TRIỂN MỘT HẠ TẦNG KHÓA CÔNG KHAI CƠ BẢN DỰA TRÊN BỘ CÔNG CỤ CRYPTOSYS

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Thái Nguyên - 2015

Số hóa bởi Trung tâm Học liệu – ĐHTN http://www.lrc.tnu.edu.vn

LỜI CAM ĐOAN

Em xin cam đoan, toàn bộ nội dung liên quan tới đề tài được trình bày trong luận văn là bản thân em tự tìm hiểu và tìm tòi dưới sự hướng dẫn khoa học của thầy T.S Lương Thế Dũng.

Các tài liệu, số liệu tham khảo được trích dẫn đầy đủ nguồn gốc. Em xin chịu trách nhiệm trước pháp luật lời cam đoan của mình.

Học viên thực hiện

Phan Thị Kim Quế

MỤC LỤC

DANH MỤC CÁC TỪ VIẾT TẮT

CA	Certificate Authority
CRLs	Certificate Revocation Lists
DES	Data Encryption Standard
DNS	Domain Name System
DSA	Directory System Agent
DSS	Directory Service Server
IEEE	Institute of Electrical & Electronic Engineers
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
MD5	Message Digest 5 Hash Algorithm
OCSP	Online Certificate Status Protocol
PGP	Pretty Good Privacy
PKC	Public Key Certificate
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
RA	Registration Authorities
RAO	Registration Authorities Operator
RFC	Request For Comments
RSA	Rivest Shamir Adleman
S/MIME	Secure Multipurpose Internet Mail Extensión
SHA-1	Secure Hash Standard
SSL	Secure Socket Layer
TTP	Trusted Third Party
TLS	Transport Layer Security

DANH MỤC HÌNH VẼ

MỞ ĐẦU

1. Lý do chọn đề tài

Trong kỷ nguyên của công nghệ thông tin, tính phổ biến rộng rãi của Internet một mặt đem lại nhiều ứng dụng tiện lợi, thú vị và dần thay thế các hoạt động truyền thống trong thế giới thực, mặt khác nó đặt ra các vấn đề về sự an toàn, tính tin cậy của những giao dịch trên Internet. Cơ sở hạ tầng khóa công khai (PKI) có thể đáp ứng, giải quyết những vấn đề cơ bản nhất cho những yêu cầu trên. Dựa trên các dịch vụ cơ bản về chứng thực số và chữ ký số, một PKI chính là bộ khung của các chính sách, dịch vụ và phần mềm mã hóa, đáp ứng nhu cầu bảo mật của người sử dụng.

Không chỉ nằm trong lĩnh vực thương mại điện tử, chứng thực số hiện còn được sử dụng như một dạng chứng minh thư cá nhân. Tại các nước công nghệ phát triển, chứng thực số CA được tích hợp vào các chip nhớ nằm trong thẻ căn cước, thẻ tín dụng để tăng cường khả năng bảo mật, chống giả mạo, cho phép chủ thẻ xác thực danh tính của mình trên nhiều hệ thống khác nhau, chẳng hạn như xe Bus, thẻ rút tiền ATM, kiểm soát hải quan v.v..

Từ tính cấp thiết của các vấn đề trong thực tế, em xin mạnh dạn trình bày tổng quát về cơ sở hạ tầng khóa công khai. Đề tài đi vào hướng " ***Phát triển một hạ tầng khóa công khai cơ bản dựa trên bộ công cụ Cryptosys"***.

2. Mục đích và nhiệm vụ

* Mục đích

Đề tài này tập trung vào hướng phát triển một hạ tầng khóa công khai cơ bản dựa trên bộ công cụ *Cryptosys PKI (PKI- Public Key Infrastructure).*

Các kết quả của đề tài sẽ được ứng dụng trong xây dựng thử nghiệm mô hình triển khai hạ tầng mật mã khóa công khai PKI.

* Nhiệm vụ

Nghiên cứu các quá trình thực hiện mã hóa và giải mã công khai

Tìm hiểu các thuật toán

Thực hiện đưa ra các giải pháp

Ứng dụng trong hệ mã cụ thể PKI

So sánh với kết quả thực thi của hệ mã khi chưa áp dụng

3. Phương pháp nghiên cứu

Nghiên cứu dựa trên việc tìm hiểu các giải thuật xử lý dựa trên bộ công cụ Cryptosys PKI.

Thu thập các tài liệu đã xuất bản, các bài báo trên các tạp trí khoa học và các tài liệu trên mạng Internet có liên quan đến vấn đề đang nghiên cứu.

Tìm hiểu, vận dụng và kế thừa các thuật toán và qui trình mã đã công bố kết quả.

4. Đối tượng và phạm vi nghiên cứu

- **Đối tượng nghiên cứu**

Đi vào nghiên cứu kỹ thuật, công nghệ, triển khai hạ tầng mật mã khóa công khai (PKI- Public Key Infrastructure) áp dụng an toàn một số giao dịch qua cổng thông tin điện tử, từ đó phân tích và nêu ra các giải pháp phù hợp. Từ các kết quả thu được, đề tài đưa ra cách xây dựng thử nghiệm mô hình triển khai hạ tầng mật mã khóa công khai PKI.

- **Phạm vi nghiên cứu**

Đề tài thực hiện triển khai hạ tầng mật mã khóa công khai (PKI- Public Key Infrastructure) áp dụng an toàn một số giao dịch qua cổng thông tin điện tử.

Đề tài giới hạn trong phạm vi nghiên cứu để đưa ra giải pháp, việc triển khai ứng dụng thực tiễn cần có thêm các điều kiện về thời gian và quy mô.

5. Ý nghĩa khoa học của đề tài

Nghiên cứu tổng hợp cơ sở lý thuyết, phương pháp luận, các công cụ cho việc phát triển hệ thống cơ sở hạ tầng khóa công khai phục vụ cho việc cấp phát chứng chỉ số. Góp phần giải quyết bài toán xác thực các thực thể tham gia vào trao đổi thông tin liên lạc qua cổng giao dịch điện tử.

Các phương pháp mật mã gồm: Phương pháp mã hoá khóa bí mật và phương pháp mã hóa khóa công khai. Phương pháp mã hóa khóa công khai thì tập trung vào

mã khóa công khai (PKI) cơ bản dựa trên nền bộ thư viện Cryptosys PKI. Với Phương pháp mã bí mật chỉ trình bày sơ bộ mang tính so sánh.

6. Bố cục của luận văn

Luận văn được trình bày trong chương, có phần mở đầu, phần kết luận, phần tài liệu tham khảo. Các nội dung cơ bản của luận văn được trình bày theo cấu trúc như sau:

Mở đầu

1. Lý do chọn đề tài
2. Mục đích và nhiệm vụ
3. Phương pháp nghiên cứu
4. Đối tượng và phạm vi nghiên cứu
5. Ý nghĩa khoa học của đề tài.

Chương 1: Tổng quan về PKI

Chương 2: Kiến trúc và các thuật toán trong Cryptosys PKI

Chương 3: Xây dựng chương trình thử nghiệm

Kết luận

Đánh giá và nêu ưu nhược điểm của đề tài. Trình bày các kết quả thu được sau khi thực hiện đề tài.

Hướng phát triển tiếp theo của đề tài.

6. Đóng góp của luận văn

Luận văn hệ thống các cơ sở lý thuyết cơ bản về hệ mật mã khóa công khai. Xây dựng chương trình thử nghiệm mô hình PKI cơ bản dựa trên nền bộ công cụ lập trình Cryptosys PKI (PKI- Public Key Infrastructure).

Mô hình này hoàn toàn có thể phát triển tạo ra cơ sở hạ tầng khóa công khai đáp ứng trong thực tế.

Giúp người sử dụng hiểu rõ hơn về khả năng ứng dụng mật mã trong các bài toán bảo mật thông tin.

Ngoài ra giúp người sử dụng hiểu rõ hơn hệ thống PKI, từ đó có thể vận hành tốt các hệ thống PKI trong thực tế.