ĐẠI HỌC THÁI NGUYÊN
TR□ỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

HỒ THỊ LÂM BÌNH

TÌM HIỂU NGUYÊN NHÂN GÂY TỔN THẤT DỮ LIỆU VÀ PHƯƠNG PHÁP BẢO VỆ THÔNG TIN TRONG CHUYỂN GIAO HỒ SƠ Y TẾ ĐIỆN TỬ

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

THÁI NGUYÊN - NĂM 2014

LỜI CAM ĐOAN

Những kết quả nghiên cứu được trình bày trong luận văn là hoàn toàn trung thực, không vi phạm bất cứ điều gì trong luật sở hữu trí tuệ và pháp luật Việt Nam. Nếu sai, tôi hoàn toàn chịu trách nhiệm trước pháp luật.

TÁC GIẢ LUẬN VĂN

Hồ Thị Lâm Bình

LỜI CẢM ƠN

Đầu tiên, tôi xin gửi lời cảm ơn chân thành và sâu sắc nhất tới PGS.TS. Trịnh Nhật Tiến đã định hướng và nhiệt tình hướng dẫn giúp đỡ tôi rất nhiều về mặt chuyên môn, để tôi hoàn thành luận văn này.

Tôi xin gửi lời biết ơn đến các thầy, các cô đã giảng dạy và truyền đạt những kinh nghiệm quý báu cho chúng tôi trong suốt hai năm học cao học tại trường Đại học CNTT&TT - Đại học Thái Nguyên.

Tôi xin cảm ơn gia đình và các bạn học viên lớp CK11G - trường Đại học CNTT&TT - Đại học Thái Nguyên những người đã luôn bên cạnh động viên, chia sẻ và khích lệ tôi trong suốt thời gian học tập và làm luận văn tốt nghiệp.

Thái Nguyên, tháng 09 năm 2014

HỒ THỊ LÂM BÌNH

MỤC LỤC

DANH MỤC CÁC KÝ HIỆU, CÁC CHỮ VIẾT TẮT

ATTT		An toàn thông tin
BHYT		Bảo hiểm y tế
BMTT		Bảo mật thông tin
CA	Certificate Authority	Chứng thực chữ ký số
EMR	(Electronic Medical Record)	Hồ sơ y tế điện tử
DNS	Domain Name System	Hệ thống tên miền
DES	Data Encryption Standard	Mã hóa dữ liệu (Mã hóa khóa bí mật)
DSS	(Digital Signature Standard)	Chuẩn chữ ký số
MD	Message Digest	Mã hóa dữ liệu hoặc (tóm tắt thông điệp), hàm băm
PKI	Public Key Infrastructure	Mã khóa công khai trên mạng riêng ảo
Public key		Khoá công khai
Private key		Khoá bí mật
RSA	Rivest Shamir Adleman	Mã hóa dữ liệu (Mã hóa khóa công khai)
SHA	Secure Hash Algorithm	Thuật giải băm an toàn
SSL	Secure Socket Layer	Giao thức bảo mật
XML	Extensible Markup Language	Ngôn ngữ đánh dấu mở rộng
YTĐT		Y tế điện tử

DANH MỤC CÁC BẢNG

DANH MỤC CÁC HÌNH VẼ

MỞ ĐẦU

1. Lý do chọn đề tài

Nguy cơ mất an toàn thông tin do nhiều nguyên nhân, đối tượng tấn công đa dạng… Thiệt hại từ những vụ tấn công mạng là rất lớn, đặc biệt là những thông tin thuộc lĩnh vực kinh tế, an ninh, y tế… Do đó, việc xây dựng hàng rào kỹ thuật để ngăn chặn những truy cập trái phép trở thành nhu cầu cấp bách trong các hoạt động truyền thông. Vì vậy các thông tin truyền đi phải đảm bảo tính chính xác, không bị sửa đổi và rất nhiều trường hợp cần được đảm bảo tính bảo mật thông tin và cần được xác thực đúng người gửi, người nhận. Xuất phát từ thực tế, nhiều biện pháp về an toàn thông tin ra đời.

Luận văn "*Tìm hiểu nguyên nhân gây tổn thất dữ liệu và phương pháp bảo vệ thông tin trong chuyển giao hồ sơ y tế điện tử*" được nghiên cứu và thực hiện trên các vấn đề cuộc sống đòi hỏi việc trao đổi thông tin hàng ngày giữa các tổ chức và cá nhân mà yêu cầu là an toàn và bảo mật thông tin được đề ra, kèm theo là demo thử nghiệm ứng dụng chữ ký số RSA.

2. Đối tượng và phạm vi nghiên cứu

Đối tượng nghiên cứu

Nghiên cứu các giải pháp mã hóa để bảo mật thông tin, những phương pháp, kỹ thuật tạo các chữ ký số trên tài liệu, văn bản điện tử để xác thực nguồn gốc tài liệu hay văn bản người gửi.

Các hệ mật mã khóa công khai (trong đó hệ mã RSA được sử dụng là đối tượng nghiên cứu chính của đề tài) nhằm phát hiện các phép xử lý toán học cần tối ưu, ngoài ra từ hệ mã đưa ra phương pháp mã hóa tệp văn bản để bảo vệ thông tin. Từ kết quả thu được bước đầu đề tài đưa ra một cách xây dựng thử nghiệm vào chữ ký số áp dụng được các kết quả tối ưu.

Luận văn sẽ tập trung nghiên cứu và làm rõ hơn về ý tưởng, cơ sở toán học, thuật toán và độ phức tạp của mã hóa nói chung và của hệ mã hóa công khai nói riêng.