

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

**TRẦN THU HIỀN DỊU**

**NGHIÊN CỨU GIẢI PHÁP BẢO MẬT  
THƯ ĐIỆN TỬ TRÊN HỆ MÃ NGUỒN MỞ**

**LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH**

**THÁI NGUYÊN - NĂM 2014**

## **LỜI CAM ĐOAN**

Tôi cam đoan luận văn này là do bản thân nghiên cứu và thực hiện theo sự hướng dẫn khoa học của thầy giáo **TS. Hồ Văn Hương**.

Tôi hoàn toàn chịu trách nhiệm về tính pháp lý quá trình nghiên cứu khoa học của luận văn này.

*Thái Nguyên, ngày 29 tháng 09 năm 2014*

**Người cam đoan**

**Trần Thu Hiền Dịu**

## LỜI CẢM ƠN

Trước tiên em xin chân thành cảm ơn thầy giáo **TS.Hồ Văn Hương** công tác tại **Ban Cơ yếu Chính phủ** đã tận tình hướng dẫn, giúp đỡ, chỉ bảo và luôn tạo điều kiện cho em hoàn thành luận văn này.

Em xin chân thành cảm ơn các thầy, các cô trong trường **Đại Học Công Nghệ Thông Tin và Truyền Thông Thái Nguyên và Viện Công Nghệ Thông Tin** đã giảng dạy, giúp đỡ và tạo điều kiện thuận lợi cho em trong suốt thời gian học tập tại trường.

Em xin gửi lời cảm ơn tới các bác, các chú và các anh chị công tác tại **Công Ty ECOIT** đã cho em một môi trường rất tốt để em được thực tập, học hỏi trong suốt quá trình thực tập và nghiên cứu luận văn tốt nghiệp.

Em đã cố gắng để hoàn thành luận văn trong phạm vi và khả năng cho phép nhưng chắc chắn sẽ không tránh khỏi những khiếm khuyết. Em rất mong nhận được sự cảm thông và tận tình chỉ bảo, nhận xét đóng góp ý kiến quý báu của quý thầy cô.

*Thái Nguyên, ngày 29 tháng 09 năm 2014*

**Tác giả luận văn**

**Trần Thu Hiền Dịu**

## MỤC LỤC

Danh mục các từ viết tắt.....	iii
Danh mục các hình vẽ.....	iv
MỞ ĐẦU.....	1
Chương 1. TỔNG QUAN VỀ AN TOÀN THƯ TÍN ĐIỆN TỬ.....	4
1.1. Thư điện tử.....	4
1.1.1. Giới thiệu thư điện tử [11].....	4
1.1.2. Tổng quan về thư điện tử.....	4
1.1.3. Cấu trúc thư điện tử.....	7
1.1.4. Các giao thức trong thư điện tử.....	8
1.2. Các hình thức đe dọa tính an toàn của thông tin khi sử dụng Email.....	10
1.2.1. Sự thiếu bảo mật trong hệ thống Email.....	10
1.2.2. Các nguy cơ trong quá trình gửi Email [9].....	11
1.3. Hệ điều hành mã nguồn mở [3].....	14
1.3.1. Giới thiệu chung về Linux.....	14
1.3.2. Các thành phần của Linux.....	15
1.3.3. Một số đặc điểm của hệ điều hành Linux.....	16
Chương 2. BẢO MẬT THƯ ĐIỆN TỬ DỰA TRÊN MÃ HÓA.....	19
2.1. Cơ sở lý thuyết mật mã [1], [2], [4].....	19
2.1.1. Giới thiệu chung về mật mã.....	19
2.1.2. Hệ mật mã khóa công khai RSA.....	22
2.1.3. Thuật toán băm.....	23
2.1.4. Chữ ký số.....	24
2.1.5. Chứng thư số.....	28
2.2. Bảo mật email với SSL và TLS [11].....	33
2.3. Bảo mật email với mã hóa khóa bất đối xứng (PGP và S/MIME) [11].....	35
2.3.1. Giới thiệu về PGP và S/MIME.....	35

2.3.2. Khả năng tương thích với Email Client .....	36
2.3.3. Mã hóa và xác thực bằng PGP .....	37
2.3.4. Mã hóa và xác thực bằng S/MIME .....	39
2.4. Bảo mật email với PEM.....	40
2.5. Giải pháp bảo mật cho thư điện tử [7] .....	41
Chương 3. XÂY DỰNG PHẦN MỀM DEMO BẢO MẬT THƯ TÍN ĐIỆN TỬ .....	45
3.1. Giới thiệu hệ thống Zimbra Mail Server [14] .....	45
3.1.1. Zimbra Collaboration Suite .....	45
3.1.2. Quá trình cài đặt hệ thống Zimbra Mail Server .....	48
3.2. Phân tích thiết kế xây dựng hệ thống bảo mật thư điện tử trên Zimbra Mail Server .....	53
3.3. Hệ thống thư điện tử Zimbra .....	59
3.3.1. Khởi động hệ thống .....	59
3.3.2. Nạp public Key vào tài khoản.....	60
3.3.3. Đăng nhập bằng eToken .....	62
3.3.4. Gửi thư mã hóa và giải mã.....	63
3.3.5. Gửi thư kèm chữ ký và xác thực .....	65
KẾT LUẬN.....	67
TÀI LIỆU THAM KHẢO.....	68

## DANH MỤC CÁC TỪ VIẾT TẮT

CA	Certificate Authority
CRC	Cyclic Redundancy Check
DNS	Domain Name System
HDH	Hệ điều hành
IMAP	Internet Message Access Protocol
MTA	Message Transfer Agent
MD	Message Digest
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
POP	Post Office Protocol
RA	Registration Authority
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SSL	Secure Socket Layer
S/MIME	Secure/Multipurpose Internet Mail Extensions
TLS	Transport Layer Security
ZCS	Zimbra Collaboration Suite

## DANH MỤC CÁC HÌNH VẼ

Hình 2.1. Mô hình hệ mật mã khóa bí mật.....	20
Hình 2.2. Mô hình mã hóa khóa công khai .....	21
Hình 2.3. Lược đồ tạo chữ ký số .....	26
Hình 2.4. Lược đồ kiểm tra chữ ký số .....	26
Hình 2.5. Mã hoá email bằng PGP.....	37
Hình 2.6. Xác thực email bằng PGP .....	38
Hình 2.7. Kết hợp mã hóa và xác thực email bằng PGP.....	38
Hình 2.8. Mô hình Client/Server .....	42
Hình 3.1. Giao diện trang đăng nhập của admin.....	50
Hình 3.2. Giao diện trang của admin .....	51
Hình 3.3. Giao diện trang đăng nhập cho user .....	51
Hình 3.4. Giao diện trang webmail của user .....	52
Hình 3.5. Giao diện soạn thư .....	52
Hình 3.6. Sơ đồ nạp eToken .....	54
Hình 3.7. Sơ đồ đăng nhập bằng eToken .....	55
Hình 3.8. Sơ đồ mã hóa và giải mã thư.....	56
Hình 3.9. Sơ đồ gửi thư kèm chữ ký và xác thực .....	58
Hình 3.10. Đăng nhập vào hệ thống Zimbra bằng cách thông thường.....	60
Hình 3.11. Nạp public key của eToken vào tài khoản .....	60
Hình 3.12. Nhập mã PIN của eToken.....	61
Hình 3.13. Khung thông báo tìm thấy Public key .....	61
Hình 3.14. Hệ thống yêu cầu nhập mã pin của eToken .....	62
Hình 3.15. Đăng nhập thông qua eToken.....	62
Hình 3.16. Trang màn hình hiển thị sau khi đăng nhập .....	63
Hình 3.17. Gửi thư mã hóa .....	63
Hình 3.18. Giải mã thư .....	64
Hình 3.19. Kết quả sau khi giải mã.....	64
Hình 3.20. Gửi thư kèm theo chữ ký .....	65
Hình 3.21. Xác thực người gửi.....	65
Hình 3.22. Kết quả xác thực .....	66

## MỞ ĐẦU

### Lý do chọn đề tài

Trong những năm gần đây, Internet phát triển mạnh mẽ và đã trở thành nền tảng chính cho sự trao đổi thông tin trên toàn cầu. Nhờ có Internet mà việc trao đổi thông tin cũng được trở nên tiện lợi và nhanh chóng hơn. Các thông tin nhạy cảm và quan trọng cũng được lưu trữ và trao đổi dưới hình thức điện tử. Chính vì thế nguy cơ lừa đảo, can thiệp, tấn công, phá hoại và ăn cắp thông tin ngày càng trở nên nghiêm trọng và nhu cầu sử dụng mật mã càng cao. Mật mã không chỉ đơn thuần phục vụ cho chính phủ, cho quân đội... mà nó còn được sử dụng cho mọi người để đảm bảo tính riêng tư của mỗi người. Hiện nay, nhu cầu trao đổi thông tin được phát triển rộng khắp, một trong những phương thức phổ biến nhất trên Internet đó là thư điện tử (email), thư điện tử giúp mọi người sử dụng máy tính kết nối Internet có thể trao đổi thông tin với nhau. Do đó, có một số yêu cầu được đặt ra đối với việc trao đổi thông tin trên mạng:

- Bảo mật tuyệt đối thông tin trong giao dịch.
- Đảm bảo tính toàn vẹn của thông tin.
- Chứng thực được tính đúng đắn về pháp lí của thực thể tham gia trao đổi thông tin.

Từ những yêu cầu trên vấn đề đặt ra là cần có phương pháp bảo mật thông tin nhằm cải thiện an toàn trên Internet. Việc tìm ra giải pháp bảo mật dữ liệu, cũng như việc chứng nhận quyền sở hữu của cá nhân là một vấn đề luôn luôn mới. Bảo mật phải được nghiên cứu và cải tiến để theo kịp sự phát triển không ngừng của cuộc sống.

- Làm thế nào để bảo mật dữ liệu?
- Làm sao để tin tức truyền đi không bị mất mát hay bị đánh tráo?



- Làm sao để người nhận biết được thông tin mà họ nhận được có chính xác hay không? đã bị thay đổi gì chưa?

- Làm sao để biết được thông tin này do ai gửi đến? thuộc quyền sở hữu của ai?

Những câu hỏi được đặt ra là một thách thức rất lớn đối với những người nghiên cứu bảo mật. Có rất nhiều cách thức để bảo vệ thông tin trên đường truyền, nhiều giải pháp được đề xuất như: Sử dụng mật khẩu, mã hóa dữ liệu, hay giấu sự tồn tại của dữ liệu... cùng với sự phát triển của các biện pháp bảo mật ngày càng phức tạp, thì các hình thức tấn công ngày càng tinh vi hơn, do đó vấn đề là làm sao đưa ra một giải pháp thích hợp và có hiệu quả theo thời gian và sự phát triển mạnh mẽ của khoa học kỹ thuật.

Với mong muốn nghiên cứu tìm hiểu giải pháp bảo mật cho thư điện tử em đã quyết định lựa chọn đề tài : “*Nghiên cứu giải pháp bảo mật thư điện tử trên hệ mã nguồn mở*”.

### **Đối tượng và phạm vi nghiên cứu**

Đối tượng và phạm vi nghiên cứu của đề tài:

- Tổng quan về thư điện tử
- Tìm hiểu về hệ điều hành mã nguồn mở
- Tìm hiểu về lý thuyết mật mã
- Tìm hiểu các giải pháp bảo mật thư điện tử
- Xây dựng ứng dụng chữ ký số trong bảo mật thư điện tử với hệ

thống thư điện tử Zimbra Mail Server.

### **Hướng nghiên cứu của đề tài.**

Đề tài tập trung tìm hiểu, nghiên cứu về thư điện tử, xây dựng ứng dụng chữ ký số trong bảo mật thư điện tử trên hệ thống Zimbra Mail Server để ký số, mã hóa, giải mã và xác thực mail.

**Những nội dung chính nghiên cứu**

Luận văn gồm 3 chương tập trung nghiên cứu những nội dung chính sau:

Chương 1. Tổng quan về an toàn thư tín điện tử

Chương 2. Bảo mật thư điện tử dựa trên mã hóa

Chương 3. Xây dựng phần mềm demo bảo mật thư tín điện tử

**Ý nghĩa khoa học của đề tài**

Xây dựng và triển khai ứng dụng chữ ký số trong bảo mật thư điện tử tích hợp trên hệ thống thư điện tử Zimbra Mail Server: Cài đặt hệ thống Zimbra Mail Server, tích hợp bảo mật trên hệ thống Zimbra gồm các nhiệm vụ là gửi thư mã hóa, thư kèm chữ ký, giải mã thư mã hóa, và xác thực người gửi.