

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



PHAN TRỌNG QUÂN

**NGHIÊN CỨU ỨNG DỤNG CƠ SỞ HẠ TẦNG KHÓA CÔNG
KHAI CHO AN TOÀN VÀ BẢO MẬT THƯ ĐIỆN TỬ**

CHUYÊN NGÀNH : HỆ THỐNG THÔNG TIN

MÃ SỐ: 60.48.01.04

LUẬN VĂN THẠC SĨ KỸ THUẬT

(Theo định hướng ứng dụng)

NGƯỜI HƯỚNG DẪN KHOA HỌC: GS.TS NGUYỄN BÌNH

HÀ NỘI - 2016

Luận văn được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học: GS.TS Nguyễn Bình

Phản biện 1: TS. Nguyễn Khắc Lịch

Phản biện 2: PGS.TS. Hà Quốc Trung

Luận văn sẽ được bảo vệ trước Hội đồng chấm luận văn thạc sĩ tại
Học viện Công nghệ Bưu chính Viễn thông
Vào lúc: 9 giờ 35 ngày 20 tháng 8 năm 2016

Có thể tìm hiểu luận văn tại:

- Thư viện của Học viện Công nghệ Bưu chính Viễn thông

MỞ ĐẦU

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. Như chúng ta có thể thấy thư điện tử đang ngày càng được sử dụng rộng rãi trong các lĩnh vực của đời sống xã hội. Hệ thống thư điện tử cho phép thực hiện các giao dịch một cách nhanh chóng hiệu quả. Tuy nhiên, trong môi trường internet thiếu an toàn, thư điện tử dễ dàng bị đọc trộm, thay đổi nội dung, mạo danh trước khi đến người nhận. Trong môi trường truyền thống chúng ta bảo vệ nội dung thư bằng phong bì và chữ ký. Còn trong môi trường truyền thông điện tử trực tuyến, thư điện tử được bảo vệ bằng việc sử dụng chứng thư số, chữ ký số.

Quá trình ký vào thư điện tử và các tệp đính kèm nhằm đảm bảo tính xác thực và chống chối bỏ trong các giao dịch trực tuyến. Điều đó giúp người nhận kiểm tra tính toàn vẹn của thư điện tử. Mã hóa nội dung thư và các tệp đính kèm để đảm bảo chỉ người nhận hợp lệ mới xem được nội dung thư. 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.

Các công ty và doanh nghiệp lớn đã nhận ra cần phải bảo mật cho thư điện tử. Đứng trước nhu cầu thực tế đó, rất nhiều công ty bảo mật đã phát triển các giải pháp, sản phẩm để bảo vệ thông tin liên quan đến trao đổi email trên môi trường internet. Hiện nay có rất nhiều sản phẩm bảo mật thư điện tử đã được triển khai, chẳng hạn như Ca-microsoft, Safe-mail, Hushmail.com, CipherMail gateway, ...

Giải pháp CipherMail email encryption gateway sẽ là một máy chủ email MTA dùng để mã hóa và giải mã thư điện tử vào/ra. CipherMail gateway có ưu

điểm hoàn toàn tương thích với bất kỳ cơ sở hạ tầng thư điện tử hiện có.

Để có thể hiểu biết sâu hơn về mã hóa và giải mã thư điện tử, học viên đã chọn đề tài **“Nghiên cứu ứng dụng cơ sở hạ tầng khóa công khai cho an toàn và bảo mật thư điện tử”** làm đề tài luận văn tốt nghiệp của mình.

Mục đích, đối tượng, phạm vi và phương pháp nghiên cứu

Luận văn tiến hành nghiên cứu, tìm hiểu các vấn đề cơ bản về quá trình ứng dụng hạ tầng khóa công khai vào ký thư điện tử và các tệp đính kèm nhằm đảm bảo tính xác thực và chống chối bỏ trong quá trình gửi/nhận email. Từ đó ứng dụng vào việc xây dựng mô hình giải pháp CipherMail email encryption gateway, một máy chủ Mail Transfer Agent (MTA) dùng để mã hóa và giải mã thư điện tử gửi/nhận.

Thông qua phương pháp nghiên cứu lý thuyết và phương pháp nghiên cứu thực nghiệm, tác giả đã tiếp cận nghiên cứu các vấn đề mã hóa và giải mã email. Từ đó phân tích được các yêu cầu của công việc, vận dụng các kết quả lý thuyết để ứng dụng hệ thống cụ thể tại Viện nghiên cứu và phát triển Viettel để đánh giá và phân tích kết quả.

Cấu trúc luận văn

Nội dung của luận văn được trình bày trong ba phần chính như sau:

1. Phần mở đầu

2. Phần nội dung: bao gồm ba chương

Chương 1: Tổng quan về an toàn và bảo mật thư điện tử.

Chương 2: xây dựng hạ tầng khóa công khai PKI và ứng dụng PKI trong an toàn bảo mật thư điện tử.

Chương 3: Ứng dụng mã hóa, chữ ký số cho thư điện tử.

3. Phần kết luận

CHƯƠNG 1: TỔNG QUAN VỀ AN TOÀN VÀ BẢO MẬT THƯ ĐIỆN TỬ

1.1 Lý thuyết chung về thư điện tử

Hệ thống thư điện tử cho phép người dùng trao đổi thư điện tử với nhau. Hệ thống này bao gồm một hoặc nhiều máy chủ thư tín (mail server), trên đó có cài đặt một phần mềm mail server để quản lý tài khoản của người dùng, thực hiện việc trao đổi thư giữa những người dùng và trao đổi thư với các máy chủ thư tín khác. [2]

1.1.1 Các thành phần cơ bản của hệ thống thư điện tử

Hệ thống này bao gồm bốn phần tử chính: MUA (Mail User Agent), MTA (Mail Transfer Agent), MDA (Mail Delivery Agent), MRA (Mail Retrieval Agent).

1.1.1.1 Mail User Agent (MUA)

1.1.1.2 Mail Transfer Agent (MTA)

Khi các thư được gửi đến từ MUA, MTA có nhiệm vụ nhận diện người gửi và người nhận từ thông tin đóng gói trong phần header và điền các thông tin cần thiết vào header. Sau đó MTA sẽ chuyển thư cho MDA để chuyển đến hộp thư ngay tại MTA, hoặc chuyển cho Remote MTA [2].

1.1.1.3 Mail Delivery Agent (MDA)

1.1.1.4 Mail Retrieval Agent (MRA)

1.1.2 Cấu trúc một thư điện tử

1.2 Một số giao thức hoạt động trong hệ thống thư điện tử

Hệ thống mail [3] được xây dựng dựa trên một số giao thức: SMTP, POP, S/MIME và IMAP.

1.2.1 Giao thức sử dụng để gửi thư điện tử

Giao thức SMTP

SMTP [2] là giao thức tin cậy, chịu trách nhiệm phân phát thư điện tử. Nó chuyển thư từ hệ thống mạng này sang hệ thống mạng khác, chuyển thư trong hệ thống mạng nội bộ.

1.2.2 Một số giao thức sử dụng để nhận thư điện tử

Có hai giao thức chính thường được dùng bởi các ứng dụng máy thư khách để truy cập thư tín từ các máy chủ : POP và IMAP.

1.2.2.1 Giao thức POP

1.2.2.1.1 Khái niệm

1.2.2.2 Giao thức IMAP

1.2.3 *Giao thức S/MIME*

Giao thức MIME [9] quy định cách thức định dạng nội dung các thông điệp email (email message) giữa các thẻ thông email. Định dạng MIME rất phức tạp, cho phép đưa bất kỳ dạng file hoặc tài liệu vào một thông điệp email như text, âm thanh, hình ảnh hoặc các định dạng dữ liệu.

1.2.3.1 Các chức năng S/MIME

- Mã hóa thư:
 - + Tạo khóa ngẫu nhiên tương ứng với thuật toán mã hóa đối xứng được chọn.
 - + Mã hóa bằng khóa công khai của người nhận.
 - + Mã hóa nội dung thư với khóa ngẫu nhiên vừa tạo.
- Xác thực thư, có chuyển mã:
 - + Chọn một hàm băm tương ứng với khả năng của người nhận.
 - + Áp dụng hàm băm lên nội dung thư.
 - + Mã hóa hàm băm bằng khóa riêng của người gửi.

1.2.3.3 Quá trình chứng thư S/MIME:

S/MIME sử dụng chứng thư X.509 [9] phiên bản 3. Mỗi client có một danh sách các chứng thư cho CA tin cậy và có các chứng thư và cặp khóa công khai/ khóa riêng của mình. Chứng thư cần được ký bởi các CA tin cậy.

1.3 Các yếu tố mất an toàn thông tin thư điện tử

1.3.1 *Hiểm họa đọc lén thư điện tử*

1.3.2 *Mạo danh*

1.3.2.1 *Mạo danh địa chỉ IP [3]*

1.3.2.2 *Mạo danh thư điện tử*

1.4 Giải pháp công nghệ bảo vệ thư điện tử an toàn

1.4.1 Giải pháp công nghệ Safe-mail

1.4.2 Giải pháp công nghệ Hushmail

1.4.3 Giải pháp công nghệ CipherMail email encryption gateway

CipherMail gateway [9] là giải pháp mã nguồn mở. CipherMail là một máy chủ email MTA để mã hóa thư điện tử vào/ra tại gateway.

CipherMail với các tính năng sau:

- Hỗ trợ chuẩn mã hóa S/MIME (mã hóa và ký số qua CipherMail gateway).
- Hỗ trợ chuẩn mã hóa PDF.
- Hỗ trợ tính năng DLP

1.4.4 Lựa chọn công nghệ bảo vệ thư điện tử an toàn.

Với phần giới thiệu các công nghệ bảo vệ thư an toàn ở trên. Học viên lựa chọn giải pháp công nghệ CipherMail gateway để bảo vệ an toàn cho thư điện tử. Vì giải pháp này hoàn toàn là miễn phí, dễ dàng triển khai và áp dụng ngay vào hạ tầng hiện có của hệ thống thư điện tử. Ngoài ra Hệ thống CipherMail gateway sử dụng giao thức S/MIME dùng để mã hóa và ký số cho thư điện tử.

1.5 Lựa chọn công nghệ triển khai thư điện tử an toàn

Giới thiệu các công nghệ thư điện tử

1.5.1 Exchange server

Exchange server [12] là phần mềm do Microsoft phát triển chuyên phục vụ các giải pháp email và trao đổi thông tin trong doanh nghiệp. Phiên bản hiện tại Exchange server là bản Exchange Server 2016.

Phiên bản này giúp đơn giản hóa công việc quản lý, bảo vệ thông tin liên lạc và đặc biệt là đáp ứng nhu cầu của doanh nghiệp trong việc đồng bộ hóa các thiết bị di động.

1.5.2 Lotus Domino

Hệ thống mail Lotus Domino của IBM hỗ trợ các giao thức gửi nhận mail như là SMTP, POP3, IMAP và MIME.

Kết luận chương 1: Chương này nói về cấu trúc của một thư điện tử, một hệ thống thư tín điện tử, các giao thức được sử dụng cho thư điện tử và các giao thức bảo mật cho thư điện tử. Đồng thời chương này cũng giới thiệu các giải pháp công nghệ bảo vệ an toàn thư điện tử, từ đó học viên lựa chọn giải pháp mã nguồn mở CipherMail email encryption gateway để bảo vệ hệ thống thư điện tử được an toàn. Ngoài ra, học viên lựa chọn giải pháp Exchange Server cho hệ thống mail server sẽ được thiết kế theo mô hình ở chương 3 của luận văn này.

CHƯƠNG 2: XÂY DỰNG HẠ TẦNG KHÓA CÔNG KHAI PKI VÀ ỨNG DỤNG PKI TRONG AN TOÀN BẢO MẬT THƯ ĐIỆN TỬ

2.1 Đặt vấn đề

Việc xác thực và kiểm tra tính toàn vẹn dữ liệu trong quá trình trao đổi thư điện tử là một trong các biện pháp đảm bảo an toàn thông tin và vấn đề này là thực sự cần thiết và cấp bách để bảo vệ an toàn cho thư điện tử. Học viên nghiên cứu lý thuyết mã hóa, chữ ký số trên nền cơ sở hạ tầng khóa công khai để đảm bảo an toàn và bảo mật thư điện tử.

Hạ tầng khóa công khai là một bộ khung cơ bản để xây dựng mô hình an ninh, bảo mật trong thương mại điện tử. Phương pháp mã hóa này cho phép mã hóa từng bức thư điện tử và trên môi trường internet thư điện tử không thể bị đọc lén bởi bất kỳ ai ngoài những người thực sự được nhận thư. Chữ ký số cho thư điện tử nhằm chứng minh nguồn gốc và tính xác thực của một thông báo thư điện tử. Người sử dụng, ngoài hình thức bảo mật thông thường như mật khẩu, cũng phải dùng một chứng thực số cá nhân để khẳng định danh tính của mình, xác nhận các hoạt động giao dịch của mình với dịch vụ ngân hàng, thương mại điện tử, giao dịch chứng khoán... Chứng thực số sẽ giúp nhà quản lý đảm bảo rằng khách hàng không thể chối cãi các giao dịch của mình, khi họ đã dùng chứng thực số. Từ đó đặt ra các vấn đề quản lý (cấp phát, xác thực) thu hồi và cấp phát lại chứng thực số.

2.2 Cơ sở hạ tầng khóa công khai

Cơ sở hạ tầng bảo mật khóa công khai PKI (Public Key Infrastructure) là một khái niệm mô tả toàn bộ nền tảng cơ sở nhằm cung cấp các dịch vụ quản lý truy cập, tính toàn vẹn, tính xác thực, tính bí mật và tính chống chối bỏ. Nền tảng này bao gồm các hệ thống phần mềm như nhà phát hành chứng chỉ, kho chứa dữ liệu phân cứng sử dụng hỗ trợ trong quá trình trao đổi khóa, các chính sách

Mã hóa và chữ ký số đã trở thành một phần không thể thiếu được đối với thương mại điện tử cũng như các lĩnh vực đòi hỏi an toàn và bảo mật. PKI cung cấp

cơ sở hạ tầng giúp cho việc sử dụng mã hóa và chữ ký số một cách dễ dàng và trong suốt đối với người sử dụng.

2.2.1 Mật mã khóa công khai

Mật mã học khóa công khai (Bất đối xứng) :

- Mật mã học khóa công khai là một chuyên ngành của mật mã học cho phép người sử dụng trao đổi các thông tin mật mà không cần phải trao đổi các khóa chung bí mật trước đó. Điều này được thực hiện bằng cách sử dụng một cặp khóa có quan hệ toán học với nhau là khóa công khai và khóa cá nhân (hay khóa bí mật).
- Trong mật mã học khóa công khai, khóa cá nhân phải được giữ bí mật trong khi khóa công khai được phổ biến công khai. Trong 2 khóa, một dùng để mã hóa và khóa còn lại dùng để giải mã. Điều quan trọng đối với hệ thống là không thể tìm ra khóa bí mật nếu chỉ biết khóa công khai.

2.2.2 Ứng dụng mật mã khóa công khai

Đây là phương pháp sử dụng hai mã khóa một mã khóa sử dụng trong quá trình mã hóa và một mã khóa sử dụng trong quá trình giải mã. Hai khóa này có quan hệ với nhau về mặt thuật toán sao cho dữ liệu được mã hóa bằng khóa này sẽ được giải mã bằng khóa kia. Nếu bạn muốn gửi đi một email đã được mã hóa, thứ đầu tiên mà cần phải có đó là public key của họ. Nếu người nhận muốn biết ai đã gửi email cho họ, họ cũng cần phải có public key của người gửi để xác nhận danh tính người gửi.

2.2.3 Khái niệm hạ tầng khóa công khai (PKI)

Khái niệm hạ tầng khóa công khai (PKI) thường được dùng chỉ toàn bộ hệ thống bao gồm cả nhà cung cấp chứng thực số (CA) cùng cơ chế liên quan đồng thời với toàn bộ việc sử dụng các thuật toán mã hóa công khai trong việc trao đổi thông tin. PKI cho phép các giao dịch điện tử được diễn ra đảm bảo tính bí mật, toàn vẹn và xác thực lẫn nhau mà không cần trao đổi các thông tin bảo mật từ trước. Mục tiêu chính của PKI là cung cấp khóa công khai và xác định mối liên hệ giữa khóa và định dạng người dùng.

2.2.4 Thành phần cơ bản của một PKI

Máy trạm PKI (PKI client) [1] : Là thiết bị cuối trong một hệ thống PKI.

Nhà cung cấp chứng thực số (CA): là một tổ chức chuyên cung cấp và xác thực các chứng thư số. Một chứng thư số có 3 thành phần chính:

- Thông tin về đối tượng được cấp gồm: tên, địa chỉ, điện thoại, email...
- Khóa công khai (Public key) của đối tượng được cấp: là một giá trị được nhà cung cấp chứng thực đưa ra như một khóa mã hóa, kết hợp cùng với một khóa cá nhân được tạo ra từ khóa công khai để tạo thành cặp mã hóa bất đối xứng.
- Chữ ký số của CA cấp chứng thực: Đây chính là sự xác nhận của CA, bảo đảm tính chính xác và hợp lệ của chứng thư. Muốn kiểm tra một chứng thư số, trước tiên phải kiểm tra chữ ký số CA có hợp lệ hay không.

2.2.5 Các dịch vụ PKI

2.2.5.1 Dịch vụ cốt lõi của PKI

PKI [5], [6] được kết hợp từ 3 dịch vụ cơ bản sau:

Xác thực (Authentication): Đảm bảo cho một người dùng rằng một thực thể nào đó đúng là đối tượng mà họ cần khẳng định.

Tính toàn vẹn (Integrity): Đảm bảo dữ liệu không bị thay đổi, nếu có thay đổi thì bị phát hiện. Để đảm bảo tính toàn vẹn, một hệ thống phải có khả năng phát hiện những thay đổi dữ liệu trái phép. Mục đích là giúp cho người nhận dữ liệu xác minh được rằng dữ liệu không bị thay đổi.

Bảo mật (Confidentiality): Đảm bảo tính bí mật của dữ liệu, không ai có thể đọc được nội dung của dữ liệu ngoại trừ những người dùng định trước và các dữ liệu nhạy cảm đều cần được bảo mật.

2.2.5.2 Các dịch vụ PKI hỗ trợ

2.3 Tổng quan chữ ký số và chứng thực số

2.3.1 Hàm băm mật mã học

2.3.1.1 Hàm băm

Hàm băm (tiếng Anh: hash function) là hàm sinh ra các giá trị băm tương ứng với mỗi khối dữ liệu (có thể là một chuỗi ký tự, một đoạn tin nhắn...). Để đảm bảo tính toàn vẹn của dữ liệu (không bị thay đổi so với dữ liệu ban đầu), người ta

đưa ra các phương thức mã hóa một chiều sử dụng các thuật toán băm. Hàm băm thường được dùng trong bảng băm nhằm giảm chi phí tính toán khi tìm một khối dữ liệu trong một tập hợp (nhờ việc so sánh các giá trị băm nhanh hơn việc so sánh những khối dữ liệu có kích thước lớn).

2.3.1.2 Đảm bảo tính toàn vẹn dữ liệu

- Hàm băm mật mã học có tính chất là hàm 1 chiều. Từ khối dữ liệu hay giá trị băm đầu vào chỉ có thể đưa ra 1 giá trị băm duy nhất. Như chúng ta đã biết đối với tính chất của hàm 1 chiều. Một người nào đó dù bắt được giá trị băm họ cũng không thể suy ngược lại giá trị, đoạn tin nhắn băm khởi điểm.

2.3.2 Chữ ký số

2.3.2.1 Chữ ký số

Chữ ký số (Digital Signature) chỉ là tập con của chữ ký điện tử. Chữ ký số là chữ ký điện tử dựa trên kỹ thuật mã hóa với khóa công khai, trong đó, mỗi người có một cặp khóa (một khóa bí mật và một khóa công khai). Khóa bí mật không bao giờ được công bố, trong khi đó, khóa công khai được tự do sử dụng. Để trao đổi thông điệp bí mật, người gửi sử dụng khóa công khai của người nhận để mã hóa thông điệp gửi, sau đó, người nhận sẽ sử dụng khóa bí mật tương ứng của mình để giải mã thông điệp.

Chữ ký điện tử là thông tin được mã hoá bằng khoá riêng của người gửi, được gửi kèm theo văn bản nhằm đảm bảo cho người nhận định danh, xác thực đúng nguồn gốc và tính toàn vẹn của tài liệu nhận được. Chữ ký điện tử thể hiện văn bản gửi đi là đã được ký bởi chính người sở hữu một khoá riêng tương ứng với một chứng chỉ điện tử nào đó.

Chữ ký số hình thành dựa trên nền tảng hạ tầng khóa công khai PKI kỹ thuật này bao gồm một cặp khóa: khóa bí mật và khóa công khai. Trong đó, khóa bí mật được người sử dụng để ký (hay mã hóa) một dữ liệu điện tử, còn khóa công khai được người nhận sử dụng để mở dữ liệu điện tử đó (giải mã) và xác thực danh tính người gửi.

2.3.2.2 Tạo và kiểm tra chữ ký số

Chữ ký số giúp xác định được người tạo ra hay chịu trách nhiệm đối với một thông điệp được ký. Một phương pháp chữ ký số phải bao gồm ít nhất 3 thuật toán chính, đó là thuật toán dùng để tạo khóa, thuật toán dùng để tạo ra chữ ký số và thuật toán tương ứng để xác nhận chữ ký số.

Tạo chữ ký số:

- Sử dụng giải thuật băm (hash) một chiều để thay đổi thông điệp cần truyền đi. Kết quả thu được một message digest gọi là bản phân tích văn bản hay tóm tắt thông điệp.

- Tiếp tục sử dụng giải thuật SHA (Secure Hash Algorithm) nên thu được message digest có độ dài 160 bits.

- Sử dụng khóa bí mật của người gửi để mã hóa bản phân tích văn bản thu được ở các bước trước. Trong bước này, thông thường, người ta sử dụng giải thuật RSA. Kết quả thu được trong bước này là chữ ký điện tử của thông điệp ban đầu.

- Gộp chữ ký điện tử vào thông điệp ban đầu. Công việc này gọi là ký nhận thông điệp.

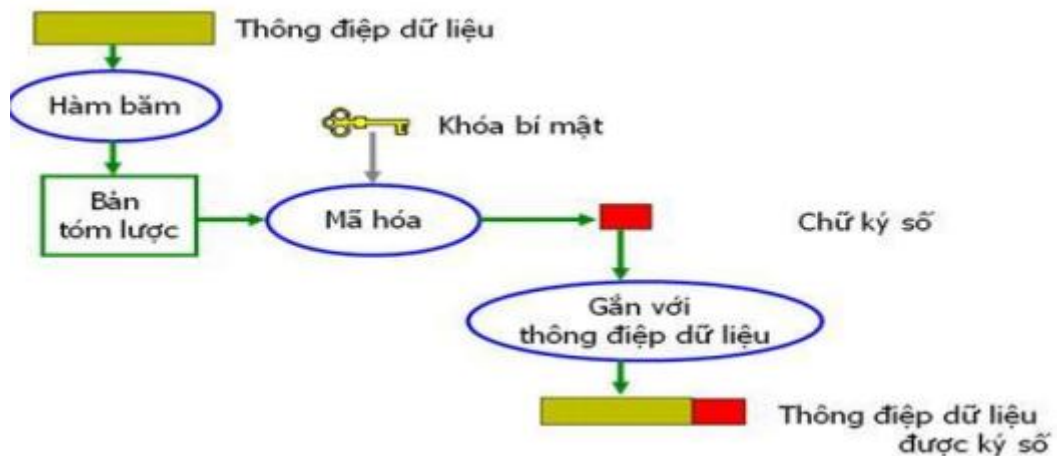
- Sau khi đã ký nhận thông điệp, mọi sự thay đổi trên thông điệp sẽ bị phát hiện trong giai đoạn kiểm tra. Ngoài ra, việc ký nhận này đảm bảo người nhận tin tưởng vào thông điệp này xuất phát từ người gửi chứ không phải ai khác.

Kiểm tra lại thông điệp:

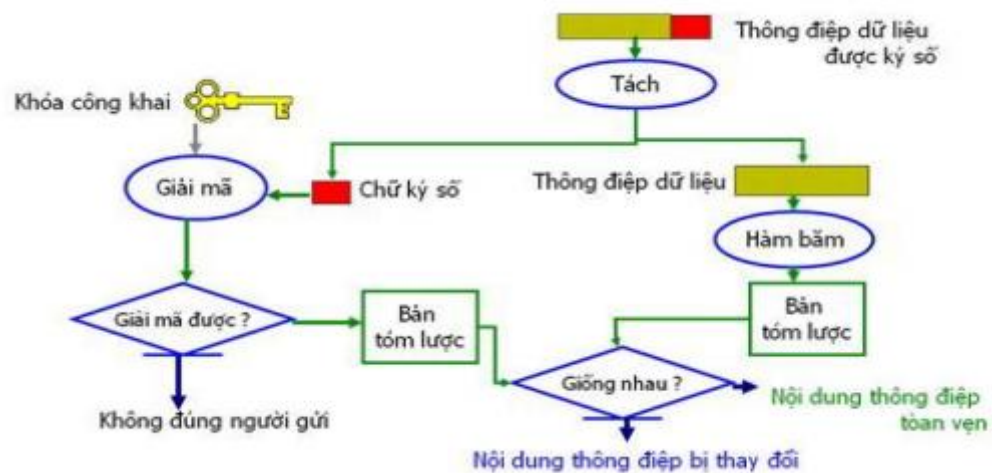
- + Người nhận sử dụng khóa công khai của người gửi để giải mã chữ ký điện tử đính kèm trong thông điệp.

- + Sử dụng giải thuật SHA để băm thông điệp đính kèm.

- + So sánh kết quả thu được ở hai bước trên. Nếu trùng nhau thì ta kết luận thông điệp này không bị thay đổi trong quá trình gửi, người gửi là chính xác và ngược lại.



Hình 2.5: Lược đồ tạo chữ ký số



Hình 2.6: Lược đồ kiểm tra chữ ký số

Bản chất của thuật toán tạo chữ ký số là đảm bảo nếu chỉ biết thông điệp thì rất khó (hầu như không thể) tạo ra chữ ký số của người gửi nếu không biết khóa bí mật của người gửi. Nên nếu phép so sánh cho kết quả đúng thì có thể xác nhận người gửi là chính xác.

2.3.2.3 Ứng dụng của chứng thư số

Mã hóa thông tin: Mã hóa thông tin với khóa công khai đảm bảo chỉ có người chủ của khóa công khai đó mới đọc được. Dù thông tin có bị đánh cắp trên đường truyền thì tính bí mật của thông tin vẫn được đảm bảo.

Toàn vẹn thông tin: Chữ ký số có thể cho bạn biết thông tin có bị thay đổi trên đường truyền hay không. Nhưng nó không bảo vệ thông tin không bị sửa đổi.

Xác thực: Người gửi có thể biết chắc rằng thông tin đã gửi đến đúng người hay chưa

nhờ vào việc xác thực khóa công khai của người nhận. Người nhận cũng có thể biết người gửi có phải là đối tác thực sự hay không nhờ vào chữ ký số.

Chống chối cãi nguồn gốc: Khi sử dụng chứng thư số, người gửi phải chịu trách nhiệm hoàn toàn về những thông tin có chứng thư số đi kèm. Chứng thư số có thể xem như bằng chứng để khẳng định tác giả của gói tin khi anh ta cố tình chối cãi, phủ nhận dữ liệu không phải do mình gửi đi.

2.3.3 Cấp phát và xác thực chứng thư số

2.3.3.1 Cấp phát chứng thư số

2.3.4 Thẩm quyền chứng thư

Trong PKI [5] có một số người có thẩm quyền, những người này được tin cậy bởi tất cả người dùng khác. Họ có nhiệm vụ chính là gắn một cặp khóa công khai với một định danh đã cho và chứng nhận việc gắn kết này bằng cách ký số một cấu trúc dữ liệu có chứa biểu diễn của định danh (gọi là chứng thư); thành phần này được gọi là những Certification Authority - CA.

2.3.5 Tính cấp thiết

2.4 Ứng dụng PKI cho an toàn và bảo mật thư điện tử

2.4.1 Cơ sở hạ tầng khóa công khai cho hệ thống thư điện tử

PKI [5] cung cấp một cặp khóa, trong đó có một chìa là khóa công khai (Public key) để có thể sử dụng dịch vụ, chìa khóa còn lại là chìa khóa bí mật (Private key) mà người sử dụng phải giữ bí mật. Hai chìa khóa này có liên quan mật thiết đến nhau, sao cho một thông điệp được mã hóa bởi một chìa khóa mật mã công khai thì chỉ giải mã được bởi một chìa khóa bí mật tương ứng.

2.4.1.1 Mã hóa

2.4.1.2 Chống giả mạo

2.4.1.3 Xác thực

2.4.1.4 Chống chối bỏ nguồn gốc

2.4.1.5 Chữ ký điện tử

2.4.2 Chữ ký số dùng cho thư điện tử

2.4.2.1 Quá trình mã hóa thư điện tử

Giả sử A muốn gửi một thông điệp điện tử bí mật cho B và giả sử A đã có khóa công khai của B (có thể do B trao đổi trực tiếp cho A hay thông qua chứng nhận khóa công khai của B).

- + Giai đoạn 1: Mã hóa thông điệp bằng một phương pháp mã hóa đối xứng an toàn, Máy tính của A sẽ phát sinh ngẫu nhiên khóa bí mật K được sử dụng để mã hóa toàn bộ thông điệp cần gửi đến cho B bằng phương pháp mã hóa đối xứng an toàn được chọn.

- + Giai đoạn 2: Mã hóa khóa bí mật K bằng một phương pháp mã hóa bất đối xứng sử dụng khóa công khai của B.

Nội dung thông điệp sau khi mã hóa ở giai đoạn 1 cùng với khóa bí mật K được mã hóa ở giai đoạn 2 sẽ được gửi cho B dưới dạng một bức thư điện tử.

2.4.2.2 Quá trình giải mã thư điện tử

- + Giai đoạn 1: Giải mã khóa bí mật K [3, tr.270,271] : B sử dụng khóa riêng của mình để giải mã khóa bí mật K bằng phương pháp mã hóa bất đối xứng mà A đã dùng để mã hóa khóa K.

- + Giai đoạn 2: Giải mã thông điệp của A: B sử dụng khóa bí mật K để giải mã toàn bộ thông điệp của A bằng phương pháp mã hóa đối xứng mà A đã dùng.

2.4.2.3 Nhận xét - Đánh giá

Sử dụng kỹ thuật trên đây [3, tr.271], người gửi thư có thể yên tâm rằng bức thư của mình chỉ có thể được giải mã bởi người nhận hợp lệ, bởi vì chỉ có người này mới có được mã khóa riêng để giải mã được khóa bí mật K và từ đó giải mã được nội dung của thông điệp.

Kết luận chương 2:

Chương 2 đã trình bày những khái niệm cơ bản, các phương pháp, công nghệ và kỹ thuật sử dụng mã hóa khóa công khai để cung cấp một cơ sở hạ tầng bảo mật. Ứng dụng cơ sở hạ tầng khóa công khai cho phép một tổ chức tận dụng tốc độ của mạng internet trong khi vẫn bảo vệ các thông tin thư điện tử quan trọng khỏi việc nghe trộm, giả mạo, và truy cập trái phép.

CHƯƠNG 3: ỨNG DỤNG MÃ HÓA, CHỮ KÝ SỐ CHO THƯ ĐIỆN TỬ

3.1 Đặt vấn đề

3.2 Giới thiệu chung về hệ thống CipherMail Email Encryption Gateway

3.2.1 Giới thiệu về CipherMail

Giải pháp CipherMail [9] là máy chủ MTA để mã hóa và giải mã email vào ra. Do CipherMail như máy chủ SMTP chung, nó tương thích với bất kỳ cơ sở hạ tầng thư điện tử hiện có và có thể được đặt trước hoặc sau các máy chủ email đã được triển khai. CipherMail thường được cài đặt như là một máy chủ “lưu trữ và chuyển tiếp”. Do đó thư chỉ được lưu trữ tạm thời trên CipherMail đến khi nó được chuyển đến đích.

CipherMail hiện hỗ trợ hai chuẩn mã hóa S/MIME và mã hóa PDF. S/MIME cung cấp các dịch vụ xác thực, toàn vẹn và chống chối bỏ (sử dụng chứng chỉ X.509[8]) và bảo vệ chống đánh chặn tin nhắn S/MIME sử dụng PKI để mã hóa và ký.

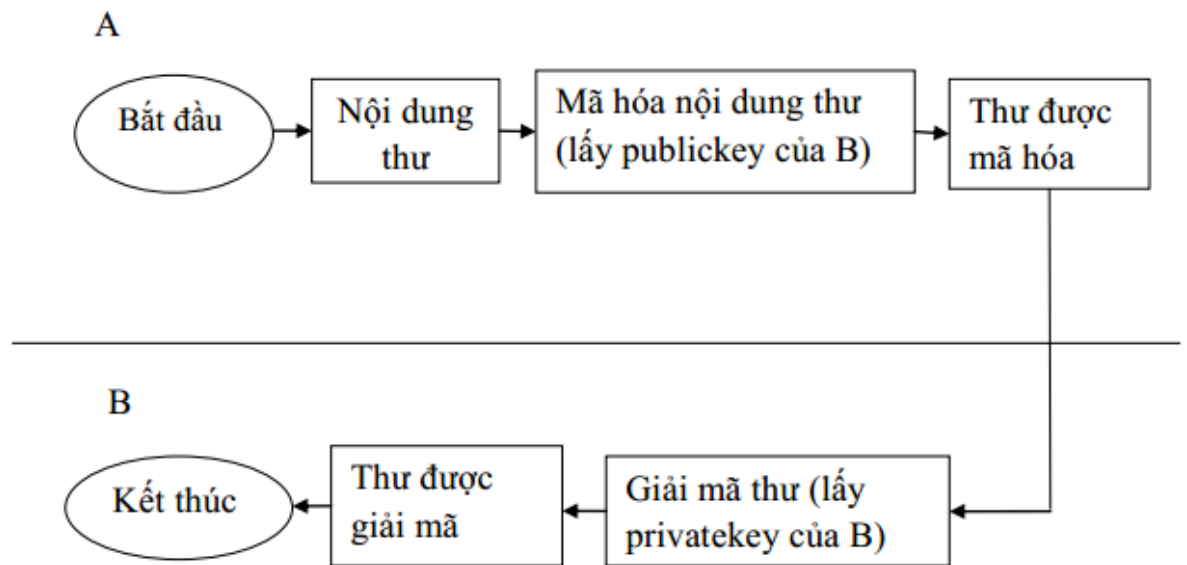
3.2.2 Các đặc điểm và chức năng

3.2.2.1 Đặc điểm

3.2.2.2 Chức năng

3.2.3 Lưu đồ hoạt động hệ thống CipherMail Gateway

Mã hóa thư và giải mã thư:



Hình 3.6: Sơ đồ mã hóa và giải mã thư

A muốn gửi cho B một bức thư mã hóa, A tiến hành soạn thảo nội dung bức thư và lấy public key của B để mã hóa nội dung của bức thư, sau đó A gửi bức thư đã được mã hóa tới B.

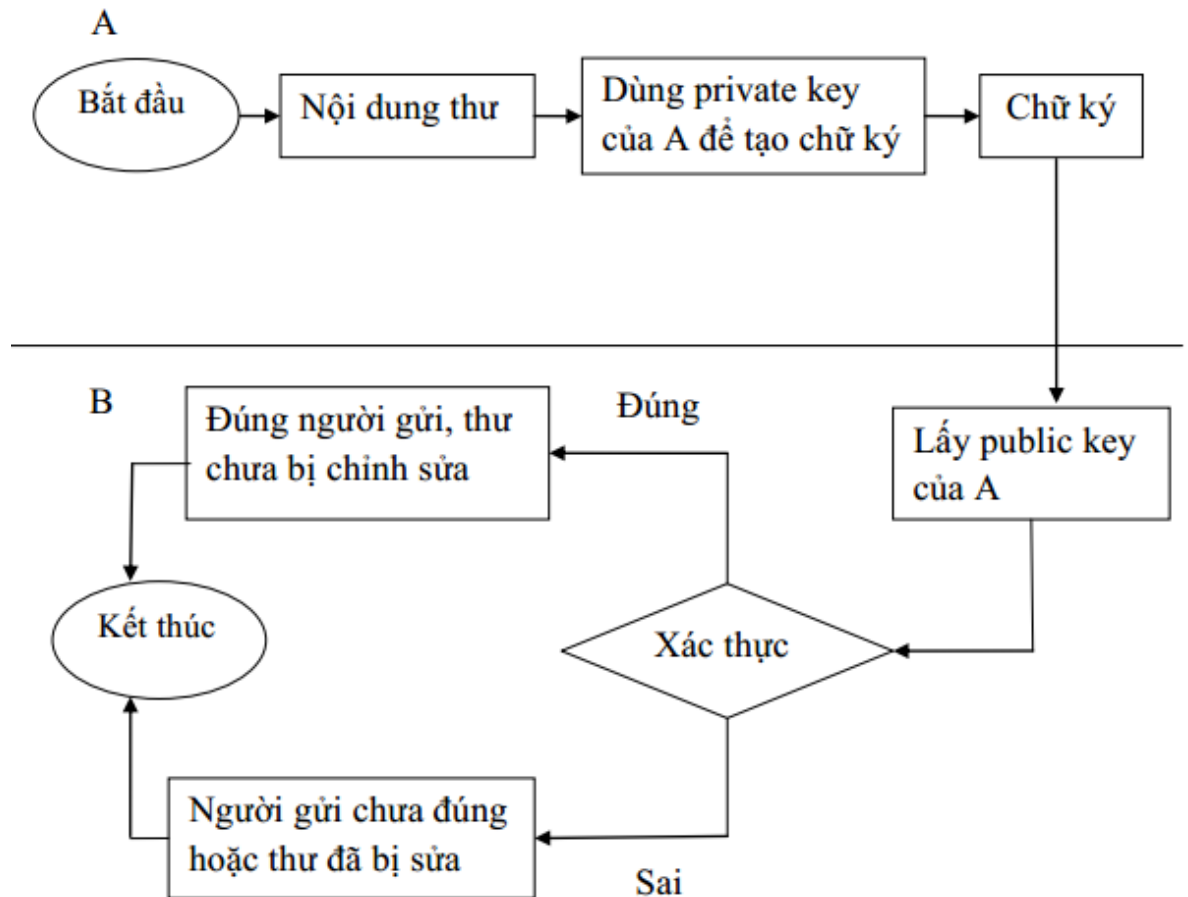
B nhận được bức thư mã hóa từ A gửi tới, để đọc được nội dung bức thư, B tiến hành giải mã bức thư bằng cách lấy private key của mình để giải mã và đọc được nội dung thư do A gửi tới.

Sơ đồ gửi thư kèm chữ ký và xác thực

Trong ký số sử dụng phương pháp tách chữ ký và dữ liệu ký. Do vậy, dữ liệu cần ký không được ghép vào khuôn dạng chữ ký đầu ra, dữ liệu cần ký được băm thông qua một hàm băm, dữ liệu băm được ký bởi khóa bí mật của người ký. ID của chứng thư số người ký cũng được ghép với chữ ký đầu ra. Để thuận tiện cho xác thực dữ liệu, chứng thư số của người ký cũng được ghép với chữ ký đầu ra. Khuôn dạng chữ ký đầu ra gồm các thông tin chính sau: Tên hàm băm sử dụng, chữ ký số, chứng thư số của người ký, ID người ký.

Xác thực được thực hiện theo quy trình ngược lại với ký số. Người nhận xác thực chữ ký sẽ thực hiện các bước: Tách thuật toán hàm băm đã sử dụng, sử dụng thuật toán băm giống như người ký để băm dữ liệu rõ được một bản tóm lược mới. Tách chữ ký số, chứng thư số người ký. Lấy khóa công khai từ chứng thư số người ký và giải mã chữ ký để thu được bản tóm lược gốc của dữ liệu ký. Sau đó so sánh

tóm lược mới và tóm lược gốc nếu 2 bản tóm lược giống nhau, chữ ký được xác thực. Ngược lại, chữ ký sẽ không được xác thực.



Hình 3.7: Sơ đồ gửi thư kèm chữ ký và xác thực

A muốn gửi cho B một bức thư có kèm chữ ký, A băm nội dung thư của mình và dùng private key của mình mã hóa kết quả băm để sinh khóa. Thư gửi đi bao gồm nội dung thư và phần chữ ký.

B xác thực xem người gửi thư đó có phải là A hay không và nội dung có bị chỉnh sửa hay không. B băm nội dung thư và giải mã chữ ký bằng public key của A trên Key Store, nếu kết quả giải mã chữ ký và kết quả băm là trùng nhau thì xác thực chính xác A là người gửi, nếu không trùng nhau thì A không là chủ nhân của bức thư đó hoặc nội dung thư đã bị chỉnh sửa.

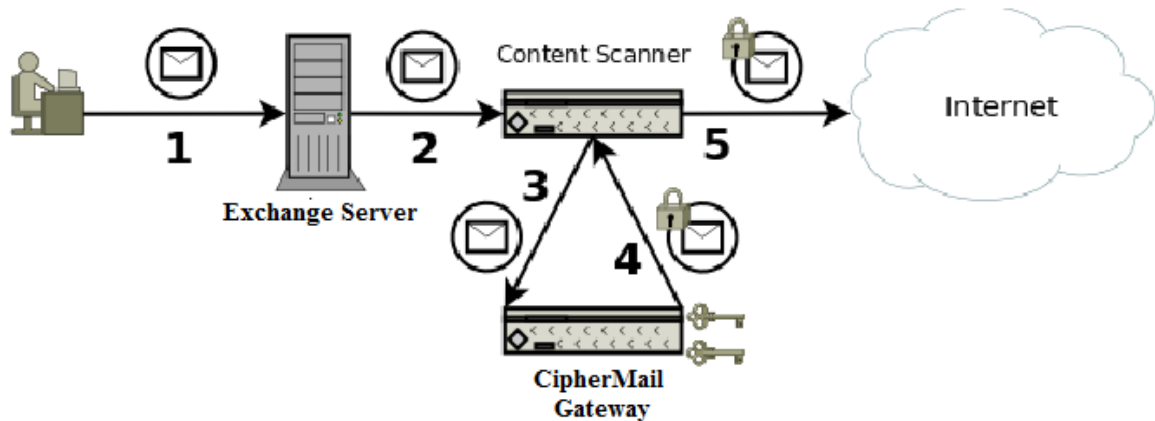
3.3 Một số ưu nhược điểm triển khai CipherMail gateway

3.4 Thiết kế hệ thống thư điện tử an toàn với CipherMail gateway

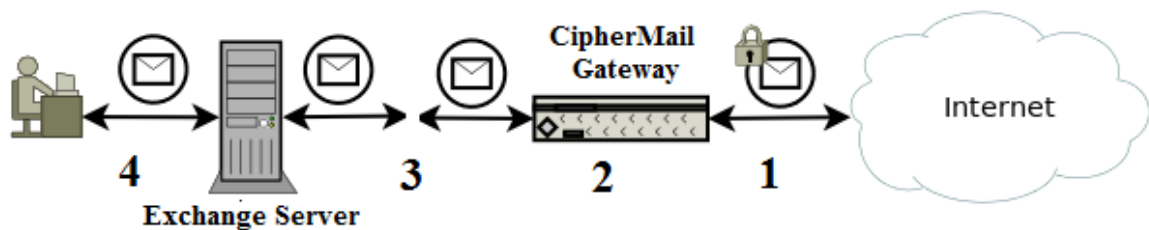
3.4.1 Đặt bài toán

3.4.2 Thiết kế hệ thống thư an toàn với CipherMail

Thiết kế điển hình của mã hóa thư điện tử Gateway có thể nhìn thấy hình sau



Hình 3.8: Hệ thống mã hóa qua CipherMail gateway [9]

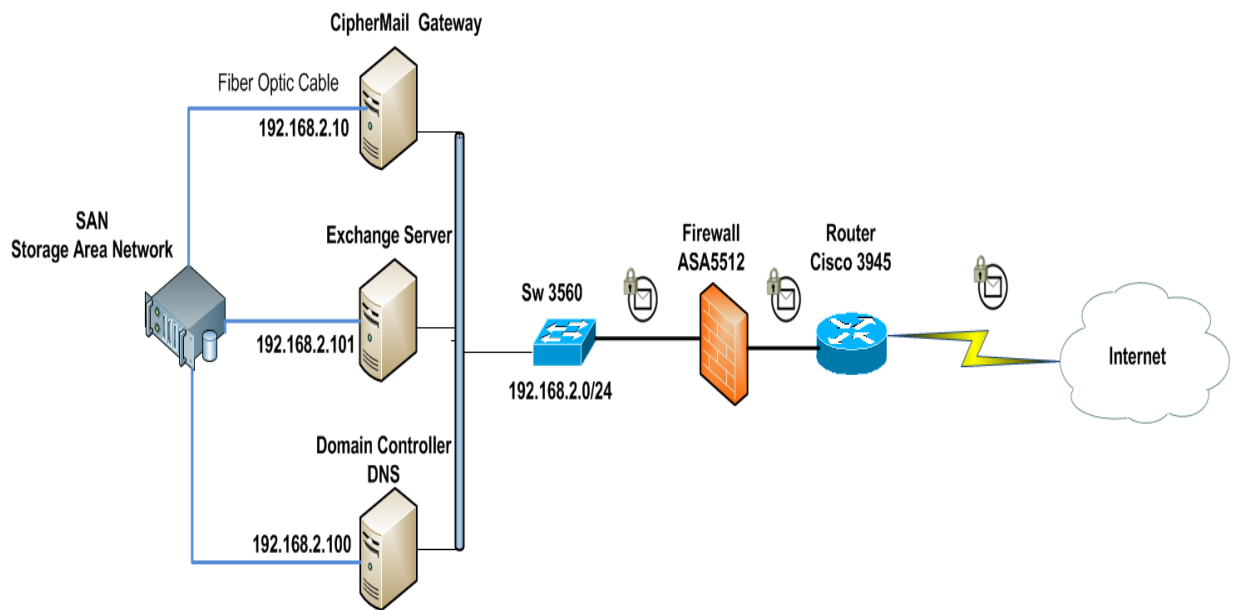


Hình 3.9: Hệ thống giải mã qua CipherMail gateway [9]

Mail gateway: Một mail gateway là một máy kết nối giữa các mạng dùng các giao thức truyền thông khác nhau hoặc kết nối các mạng khác nhau dùng chung giao thức. Ví dụ một mail gateway có thể kết nối mạng TCP/IP với một mạng chạy bộ giao thức SNA (System Network Architecture). Một mail gateway đơn giản nhất dùng để kết nối hai mạng dùng chung giao thức hoặc mailer. Khi đó mail gateway chuyển mail giữa domain nội bộ và các domain bên ngoài.

3.5 Xây dựng hệ thống thử nghiệm

3.5.1 Mô hình triển khai



Hình 3.10: Mô hình triển khai

3.5.2 Cài đặt và cấu hình CipherMail gateway

3.5.2.1 Yêu cầu phần mềm

3.5.2.2. Cài đặt

3.5.2.3 Cấu hình CipherMail gateway mã hóa S/MIME

CipherMail hỗ trợ ký số và mã hóa S/MIME. Cả người gửi và người nhận yêu cầu chứng thư số và khóa riêng. Vì thế CipherMail có thể cài đặt sẵn một server CA để phát hành chứng thư và khóa miễn phí cho người dùng bên trong và bên ngoài.

Người dùng bên ngoài, không phải cài đặt một CipherMail gateway, có thể dùng bất kỳ mail client nào có khả năng để gửi và nhận mail mã hóa khi chứng thư số được cài đặt. Tuy nhiên người dùng bên trong và bên ngoài không yêu cầu sử dụng CA đã được cài đặt sẵn. Nếu người nhận bên ngoài đã có chứng thư số S/MIME thì chứng thư này có thể được sử dụng thay thế.

3.6 Đánh giá hệ thống thử nghiệm

Trường hợp gửi thư không mã hóa :

Hầu như mọi email trên internet đều được truyền qua giao thức SMTP theo dạng MIME chưa có sự đảm bảo an toàn. Hệ thống thư điện tử cho phép thực hiện các giao dịch một cách nhanh chóng hiệu quả. Tuy nhiên, trong môi trường internet thiếu an toàn, thư điện tử dễ dàng bị đọc trộm, thay đổi nội dung, mạo danh trước

khi đến người nhận.

Giải pháp nguồn mở CipherMail là một máy chủ email MTA dùng để mã hóa và giải mã thư điện tử vào/ra. Hệ thống triển khai CipherMail mang lại đầy đủ các tính chất cần thiết nhằm thiết lập một môi trường an toàn, tin cậy trong giao tiếp như tính bảo mật, toàn vẹn, tính xác thực và tính chống chối bỏ. Hơn nữa hệ thống có khả năng tích hợp với cơ sở hạ tầng hiện có.

Thay vì phải mua các giải pháp công nghệ để bảo vệ an toàn, bảo mật cho thư điện tử. giải pháp CipherMail gateway sẽ giảm thiểu được chi phí và hệ thống dễ triển khai nên sẽ tiết kiệm được thời gian triển khai.

Hệ thống CipherMail gateway là một server CA để phát hành chứng thư và khóa miễn phí cho người dùng bên trong và bên ngoài. CipherMail hỗ trợ ký số và mã hóa bằng giao thức S/MIME nên các mail client chỉ cần thiết lập chứng thư và khóa riêng một lần..

Hệ thống CipherMail gateway tận dụng được cơ sở hạ tầng hiện có và hệ thống thiết kế, cài đặt trên đã được áp dụng vào môi trường triển khai thực tế cho Viện Nghiên cứu và Phát triển Viettel (Viettel R&D).

Như vậy hệ thống CipherMail gateway giải quyết được bài toán đặt ra đảm bảo an toàn, bảo mật cho thư điện tử khi di chuyển trên môi trường internet. Hệ thống CipherMail gateway đã xây dựng phù hợp với triển khai thực tế và đảm bảo an toàn bảo mật cho thư điện tử.

Tuy nhiên, do thời gian nghiên cứu có hạn, học viên chưa nghiên cứu được hết các chức năng của hệ thống CipherMail gateway. Hệ thống CipherMail gateway dùng chuẩn mã hóa S/MIME vì vậy đòi hỏi các mail client phải hỗ trợ chuẩn mã hóa này và người nhận, gửi gửi phải có chứng thư và khóa riêng. Khi sử dụng hệ thống CipherMail sẽ mất thời gian thiết lập chứng thư, khóa riêng lần đầu tiên cho mail client. Hệ thống CipherMail hỗ trợ tạo chứng thư cho tất cả người dùng nhưng hệ thống được thiết kế ở trên mới chỉ áp dụng cho doanh nghiệp vừa nhỏ.

Kết luận chương 3: Giải pháp CipherMail email encryption gateway là một gói phần mềm mã nguồn mở, triển khai hệ thống mã hóa, ký số hoàn chỉnh, đầy đủ các chức năng. Hệ thống triển khai này mang lại đầy đủ các tính chất cần thiết nhằm thiết lập một môi trường an toàn, tin cậy trong giao tiếp như tính bảo mật, toàn vẹn, tính xác thực và tính chống chối bỏ. Hơn nữa hệ thống có khả năng mở rộng với các hệ thống khác một cách dễ dàng.

KẾT LUẬN

1. Kết quả đạt được

Đề tài “Nghiên cứu ứng dụng cơ sở hạ tầng khóa công khai cho an toàn và bảo mật thư điện tử” là một đề tài khó và rộng. Trong thời gian nghiên cứu, tìm hiểu, xây dựng đề án đã hoàn thành được các nhiệm vụ được đặt ra, cụ thể là:

Về mặt lý thuyết :

- Nghiên cứu tổng quan về an toàn và bảo mật thư điện tử.
- Ứng dụng cơ sở hạ tầng khóa công khai để đảm bảo an toàn và bảo mật cho thư điện tử
- Quan trọng nhất của đề tài đã ứng dụng, triển khai mã hóa, ký số cho thư điện tử bằng cách sử dụng CipherMail gateway. Hệ thống CipherMail gateway sử dụng chuẩn giao thức S/MIME để mã hóa và ký số để bảo mật cho thư điện tử khi di chuyển trên internet.

2. Hạn chế

Sau một thời gian nỗ lực hết mình, về cơ bản luận văn cũng đã nghiên cứu ứng dụng mã hóa và giải mã thư điện tử nhằm đảm bảo an toàn và bảo mật cho các hệ thống cung cấp dịch vụ thư điện tử của doanh nghiệp. Mặc dù đã hết sức cố gắng nhưng trình độ chuyên môn và thời gian thực hiện khóa luận còn hạn hẹp, cũng như mức độ phức tạp của đề tài, học viên chưa nghiên cứu được hết các chức năng của hệ thống CipherMail Gateway. Kính mong Quý Thầy Cô tham khảo đóng góp ý kiến để luận văn được hoàn thiện hơn.

3. Một số hướng nghiên cứu tiếp theo

Sau khi nghiên cứu xong đề tài, học viên xin đưa ra một số hướng nghiên cứu tiếp theo:

- Tích hợp hệ thống CipherMail gateway với các giải pháp clustering thư điện tử, loadblancing cho các máy chủ SMTP, POP3 và các hệ thống lưu trữ dữ liệu lớn.
- Nghiên cứu sâu hơn về các thuật toán mã hóa và giải mã..
- Nghiên cứu ứng dụng chuẩn mã hóa PDF cho thư điện tử.

DANH MỤC TÀI LIỆU THAM KHẢO

Tiếng Việt

- [1] Trần Duy Lai, Lê Mỹ Tú (2006), “*Giáo trình Chứng thực điện tử*”, Học viện Kỹ Thuật Mật Mã, Hà Nội.
- [2] Trần Duy Lai, Hoàng Văn Thúc (2006), “*Giáo trình An toàn thư tín điện tử*”, Học viện mật mã, Thành phố Hà Nội.
- [3] Trần Minh Triết, Dương Anh Đức, “Mã hóa và Ứng dụng”, Khoa công nghệ công thông tin, Trường đại học khoa học tự nhiên, Đại Học Quốc gia thành phố Hồ Chí Minh.

Tiếng Anh

- [4] Carlisle Adams, Steve Lloyd (2002), “Understanding PKI, Standards, and Deployment Consideration”, Addison-Wesley Professional.
- [5] Suranjan Choudhury, Kartik Bhatnagar and Wasim Haque (2001), “PKI Implementation And Design”, M&T Books.
- [6] Andrew Nash, William Duane, Celia Joseph and Derek Brink (2001), “PKI Implementing and Managing E-security”, RSA Press.
- [7] RFC 3161 (2001), "Internet X.509 Public Key Infrastructure Time-Stamp protocol (TSP)".
- [8] ITU-T Recommendation X.509 (2005), "Information technology - Open Systems Interconnection - The Directory: Authentication framework";

Trang web

- [9] <http://www.ciphermail.com>
- [10] <https://www.hushmail.com/>
- [11] <http://www.safe-mail.net>
- [12] <http://technet.microsoft.com>
- [13] <http://www.ietf.org/html.charters/smime-charter.html>
- [14] <https://www.ciphermail.com/documents/ciphermail-SMTP-auth-guide>
- [15] <https://www.clearswift.com/solutions/email-security/secure-email-gateway>