BỘ GIÁO DỤC VÀ ĐÀO TẠO 

**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP. HCM**

**ĐỒ ÁN CUỐI KỲ**

**S/MIME EMAIL SECURITY ( OUTLOOK 2016 )**

Khoa: **CÔNG NGHỆ THÔNG TIN**

Môn học: **BẢO MẬT THÔNG TIN**

Giảng viên hướng dẫn: **Th.S Tống Thanh Văn**

Sinh viên thực hiện: **Võ Xuân Tuấn 1711061777**

TP. Hồ Chí Minh, 2020

**MỤC LỤC**

MỤC LỤC......................................................................................................................2 CHƯƠNG 1: TỔNG QUAN VỀ S/MIME EMAIL SECURITY..................................3 1.1 Giới thiệu tổng quan ................................................................................................3 1.2 Khuôn dạng của S/MIME ........................................................................................5 1.3 Ứng dụng của S/MIME............................................................................................6 1.3.1. Sign-On một lần...................................................................................................6 1.3.2.

Ký mẫu đơn..........................................................................................................8

CHƯƠNG 2: NGUYÊN LÝ HOẠT ĐỘNG VÀ THUẬT TOÁN SỬ DỤNG.............9 2.1 Nguyên lý hoạt động................................................................................................9 2.2 Thuật toán sử dụng.................................................................................................13 2.2.1. Thuật toán mã hóa chuẩn Triple DES( 3DES ) .................................................13 2.2.2. Thuật toán chìa khóa công khai - RSA..............................................................14 2.2.3. Thuật toán hỗn độn một chỉều ( hashing ) – SHA1 hoặc MD5 .........................15

CHƯƠNG 3: MÔ HÌNH THỰC NGHIỆM.................................................................17 3.1 Thiết lập S/MIME trên Oulook 2016.....................................................................17

2

**CHƯƠNG 1: TỔNG QUAN VỀ S/MIME EMAIL SECURITY 1.1Giới thiệu tổng quan**

Thư điện tử từ khi phát triển đã cho phép mọi người có thể trao đổi thông tin với nhau dưới dạng các thông điệp có định dạng text. Đến đầu những năm 1990, sự phát triển của MIME (Multipurpose Internet Mail Extentions), một giao thức hiện vẫn được sử dụng phổ biến trên thế giới, đã cho phép mọi người có thế gửi cho nhau hình ảnh, âm thanh, chương trình và các dạng file đính kèm khác.

MIME không có các các tính năng bảo mật, do đó khi lưu thông trên mạng nó có thể bị đọc trộm một cách dễ dàng. S/MIME (Secure/Multipurpose Internet Mail Extentions) là phiên bản bảo mật của MIME, nó có một số đặc trung sau:

• Tính bảo mật: Chỉ người nhận mới có thể đọc được thông điệp.

• Tính xác thực: Người nhận biết được thông điệp được đi đến từ ai và người gửi không thể chối cãi được.

• Tính toàn vẹn: Thông điệp không bị thay đổi trên đường đi.

Do đó chúng ta có thể định nghĩa S/MIME như sau:

S/MIME là một giao thức cho phép ký sổ và mã hóa nội dung thư điện tử. S/MIME làm cho việc gửi nhận mail giữa mọi người trờ nên an toàn, tránh được việc xem trộm nội dung, thay đồi thông tin và đám bảo rằng thư điện tử này thực sự đã được gửi từ người có tên trên đó. Hầu hết các ứng dụng thư điện tử ngày nay đều hỗ trợ giao thức S/MIME.

S/MIME cung cấp một sổ khả năng sau:

• Cho phép ký chìa khoá công cộng (Public Key Signatures).

• Mã hoá nội dung dữ liệu của thông điệp e-mail.

Để có thể sử dụng được S/MIME chúng ta cần có:

• Một cặp chìa khóa mật mã để mã hóa.

• Một chứng chỉ dùng để ký số thông điệp.

3

MIME là một chuẩn cho phép mã hoá tài liệu đính kèm thư điện tử (gồm những dữ liệu không phải văn bản). S/MIME là một chuẩn làm tăng thêm tính bảo mật của thông điệp điện tử.

Cặp chìa khóa và chứng chỉ (gọi là chứng chì chìa khoả công cộng - Public Key Certificate) là những thông tin thuộc về cá nhân thuê bao, được phân phối rộng rãi, cho phép mọi người muốn trao đối thông điệp thư điện tử theo giao thức S/MIME với thuê bao đều có thế truy nhập đến.

Chìa khoá mật mã là hết sửc quan trọng vì nó được sử dụng để mã hoá và giải mã thông tin. Hầu hết các cách thức bảo mật ngày nay đều sử dụng Mật mã Chìa khoá Công cộng (Public Key Encryption) để mã hoá thông tin. Điểm khác biệt chính của phương pháp này là chỉ người có chìa khoá mật mã riêng (Private Encryption Key) mới có khá năng giải mã thông điệp đã mã hoá. Nếu X muốn giữ bí mật thông điệp gửi cho Y, X mã hoá nó bằng chìa khoá công cộng của Y, khi đó không ai ngoài Ycó thể xem được nội dung thông điệp. Chỉ có duy nhất Y mới có khả năng giải mã thông điệp bằng cách sử dụng chìa khoá riêng của Y. Đây được gọi là phương pháp bảo mật dựa trên mã hoá chìa khoá công cộng.

Mã hoá chìa khoá công cộng rất có hiệu quá bởi vì chìa khoá công cộng có thể được phân phối rộng rãi qua Internet và thông qua các dịch vụ thư mục. Để có thể triển khai và quản lý các cặp chìa khoá công cộng và chìa khọá riêng, phải xây dựng một cơ cấu tổ chức cho việc quản lý an toàn thông tin, cơ cấu tổ chức đó gọi là cơ cở hạ tầng chìa khoá công cộng (Public Key Infrastructure - PKI).

S/MIME cung cấp mã hoá chìa khoá công cộng từ điếm tới điểm cho thông điệp thư điện tử. Một thông điệp được mã hoá bởi người gửi chỉ có thể được giải mã bởi người nhận. Trong suốt thời gian trên đường truyền, nội dung thông điệp không bị giải mã, truy nhập bởi bất kỳ ai. Thông qua chữ ký số (Digital Signature), S/MIME cung cấp xác nhận người gửi và phát hiện sự xâm phạm.

Chứng chỉ S/MIME có thể được sử dụng theo một số cách thức khác nhau như chứng chỉ mật mã chỉa khoá công cộng (PKE) dùng để mã hoá thông tin, chứng chỉ số (CA) để thẩm định tính khởi điểm của thông tin, thiết lập sự tin cậy giữa các ứng dụng và các tổ

4

chức dựa trên cơ sở phát hành chứng chỉ (CA). CA đảm bảo tính tin cậy, trách nhiệm của mình trong các trao đổi dựa vào chứng chỉ số mà nó phát hành.

**1.2Khuôn dạng của S/MIME**

Trước khi đi vào trình bày về khuôn dạng của giao thức S/MIME, chúng ta sẽ cùng tham khảo lại một số kiến thức về giao thức MIME:

Giao thức thư điện tử được xây dựng dựa trên chuẩn RFC 822, theo chuẩn này thì một thông điệp thư điện tử sẽ bao gồm hai phần:

• Phần đầu thông điệp (Message headers).

• Phần thân thông điệp (Message body).

Thông thường, ranh giới để phân tách giữa phần đầu và phần thân của thông điệp thường là một dòng trắng. Nội dung của phần đầu sẽ được viết liền nhau, gồm rất nhiều trường. Mồi trường bao giờ cũng gồm tên trường và giá trị mà nó chứa. Trong phần đầu thông điệp sẽ có một số trường đòi hỏi bắt buộc khi tạo thông điệp thư điện tư như: Data:, From:, To:.. Ngoài ra còn một số trường lựa chọn khác như: Bcc:, Cc:, Message-Id:. Received:, Reply-To:, ReturnPath:, Sender:, Subject:..., mỗi thông điệp trong quá trình phân phát sẽ ghi lại dấu tích các nơi mà nó đã đi qua thông qua trường Received.

Dạng dữ liệu mà thông điệp thư điện tử trao đổi không chỉ có dạng văn bản mà còn có các dạng khác nữa như: âm thanh, hình ảnh, ... do đó đòi hỏi phải có một giao thức mới để biểu diễn các thông tin này. Và MIME là giao thức được xây dựng để làm việc đó. nó được đặc tả trong RFCs 2045 tới 2049. Đặc tả MIME được các ứng dụng mạng sử dụng và triển khai. MIME cho phép mô tả chỉ tiết hơn về kiểu dữ liệu vận chuyển trên mạng gắn trong thông điệp thư điện tử. Thông tin trong phần đầu của thông điệp MIME gồm các thông tin sau: Mime-Version:, Content-Type:, Content-Transfer-Encoding:, Content-ID:, Content-Description:. Content-Disposition:.. Ví dụ trường MIME ContentType sẽ nhận các giá trị sau: text/plain, text/html, muỉtipart/mixed, multipart/alternative, multipart/parallel, message/rfc822, image/gif, video/mpeg, application/postscript, application/octet-stream, ...

5

Như đã đề cập ở trên. S/MIME được xây dựng dựa trên cơ sơe MIME và cung cấp thêm tính năng đảm bảo an khi truyền trên mạng. Do đó, cấu trúc của S/MIME cũng gồm 2 phần chính: phần đầu và phần thân, nhưng trong phần thân của S/MIME, ngoài những thông tin mà MIME có, còn chỉ ra thêm các thông tin mô tả về thuật toán mã hóa (PKCS #1), thông tin mã hoá (PKCS #7), và thông tin về chứng chỉ (PKCS #10). Trong đó: • PKCS #1: Phương pháp mã hoá RAS.

• PKCS #7: Cú pháp mật mã thông điệp.

• PKCS #10: Cú pháp yêu cầu chứng chỉ.

• Agent gửi sử dụng content type = “data” khi thông điệp sử dụng dịch vụ bảo mật trên đó.

• Agent gửi sử dụng content type = “signedData” khi thông điệp gửi đi có chữ ký số.

• Agent giri sir dung content type = “envelopedData” khi áp dụng bảo vệ cá nhân cho thông điệp.

**1.3Ứng dụng của S/MIME**

Một trong những ứng dụng của S/MIME, được mô tả sau đây, sẽ làm giảm rất nhiều thao tác trong quá trình sử dụng, làm tăng hiệu suất làm việc và đảm bảo tính an toàn cao. ứng dụng của S/MIME gồm: Sign-On một lần và ký mẫu đơn sẽ được mô tả chỉ tiết sau đây.

**1.3.1 Sign-On một lần**

Những người thường xuyên sử dụng mạng thường phải nhớ vô số mật khẩu cho vô số dịch vụ mà họ sử dụng. Ví dụ như người sử dụng phải vào những mật khẩu khác nhau khi log vào mạng, khi lấy thư điện tử. Khi sử dụng dịch vụ thư mục, khi dùng chương trình lịch tổng hợp và khi truy cập các máy chủ khác. Quá nhiều mật khẩu đang làm đau đầu cả người sử dụng và các nhà quản trị hệ thống. Người sử dụng gặp phải khó khăn khi nhớ các mật khẩu, do đó có xu hướng đặt các mật khẩu dễ đoán và viết chúng ớ những chỗ nhiều người nhìn thấy. Các nhà

6

quản trị giữ mỗi cơ sở dữ liệu mật khẩu khác nhau trên một máy chú khác nhau và do đó phải đương đầu với vấn đề bảo mật do các mật khẩu được gửi qua mạng quá thường xuyên và liên tục.

Để giải quyết vấn đề này, phải tìm ra một cách nào đó để người sử dụng chỉ phải login một lần, dùng một mật khẩu và được xác nhận để có thể truy cập đến tất cả các tài nguyên được phép truy cập trên mạng - mà không cần phải gửi một mật khẩu nào qua mạng. Khả năng này được gọi là Sign-On một lần.

Cả chứng chỉ SSL và chứng chỉ S/MIME đều có thể giữ một vai trò quan trọng trong giải pháp Sign-On một lần tổng thể. Ví dụ, một dạng Sign-on một lần do các sản phẩm Netscape hỗ trợ dựa trên xác nhận khách hàng SSL, người sử dụng có thể login một lần dùng một mật khẩu đến cơ sở dữ liệu chìa khoá riêng của khách hàng địa phương, được xác nhận có quyền truy nhập đến tất cả các máy chủ hỗ trợ SSL mà người sử dụng được phép sử dụng - không cần gửi bất cứ mật khẩu nào qua mạng. Việc này làm việc truy cập của người sử dụng trở lên đơn giản hơn, các nhà quản trị có thể kiểm soát việc truy cập bằng cách quản lý danh sách các CA chứ không phải một danh sách dài những người sử dụng và mật khẩu của họ.

Ngoài việc dùng chứng chỉ, một giải pháp Sign-On một lần hoàn chỉnh còn phải thỏa mãn nhu cầu phối hợp với hệ thống của doanh nghiệp hoạt động dựa trên mật khẩu hay những hình thức xác nhận khác, ví dụ như hệ thống hệ điều hành nền.

7

**1.3.2 Ký mẫu đơn**

Rất nhiều hình thức thương mại điện tử yêu cầu phải cung cấp bằng chứng là người sử dụng đã xác nhận một giao dịch. Mặc dù SSL cung cấp các xác nhận khách hàng trong suốt quá trình kết nối SSL, nó không cung cấp xác nhận liên tục cho những giao dịch có thế xảy ra trong quá trình kết nối đó. S/MIME cung cấp xác nhận liên tục cho thư điện tử, nhưng thương mại điện tử thường đòi hỏi phải điền vào một mẫu đơn trên trang web hơn là gửi thư điện tử.

Công nghệ ký mẫu đơn thoả mãn nhu cầu cung cấp xác nhận liên tục cho những giao dịch tài chính. Ký mẫu đơn cho phép người sử dụng kết hợp chữ ký số của mình với những dữ liệu của trang web do giao dịch tạo ra. ví dụ như một lệnh mua hàng hay những chứng từ tài chính khác. Chìa khoá riêng đi cùng với chứng chỉ SSL khách hàng hoặc chứng chỉ S/MIME đều có thể dùng cho mục đích này.

Khi người sử dụng bấm vào nút chấp nhận (submit) trên mẫu đơn của trang web hỗ trợ ký mẫu đơn. một hộp hội thoại sẽ hiện ra cho thấy văn bàn chính xác sẽ được ký. Người tạo mẫu đơn có thể chỉ định loại chứng chỉ được phép dùng hoặc cho phép người sử dụng chọn một trong các chứng chỉ SSL khách hàng và chứng chỉ S/MIME. Khi người sử dụng bấm vào OK, văn bản được ký, và cả văn bản và chữ ký số được gửi đến máy chủ. Khi đó máy chủ có thể sử dụng một tiện ích gọi là công cụ kiếm tra chữ ký (Signature Verification Tool) để xác định hiệu lực của chữ ký số.

8

**CHƯƠNG 2: NGUYÊN LÝ HOẠT ĐỘNG VÀ THUẬT TOÁN SỬ DỤNG**

**2.1 Nguyên lý hoạt động**

Giao thức S/MIME sử dụng các thuật toán và phương pháp mã hoá sau: • Thuật toán mã hoá chuẩn - RC2 hoặc TripleDES (symmetric cipher - thuật toán đối xứng).

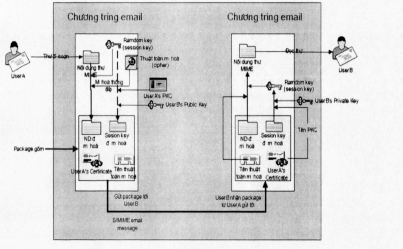
• Thuật toán mã hoá chìa khoá công khai - RSA (asymmetric cipher - thuật toán không đôi xứng).

• Thuật toán hỗn độn một chỉều (hashing) - SHA1 hoặc MD5.

*Cơ chế làm việc của SMIME có thể biểu diễn thành 3 phần như sau:* • S/MIME - đảm bảo tính báo mật.

• S/MIME - đảm bảo tính xác thực.

• S/MIME - đảm bảo tính bảo mật và tính xác thực.



9

Hình trên là sơ đồ làm việc của quá trình tạo một thông điệp theo giao thức bảo mật thư điện tử-S/MIME nhằm đảm bảo tính bảo mật của thông điệp. Để minh hoạ chúng ta cùng tìm hiểu một ví dụ sau: Trong ví dụ này A thực hiện gửi cho B một thông điệp được xây dựng dựa trên giao thức S/MIME:

1. Đầu tiên chương trình thư điện tử của A tạo ra một khoá ngẫu nhiên (session key), khoá này sẽ được sử dụng trong thuật toán mã hoá đối xứng 2. Tiếp theo chương trình thư điện tử của A thực hiện mã hoá thông điệp dùng thuật toán mã hoá đối xứng với chỉa khoá là khoá ngẫu nhiên được tạo ờ trên

3. Chương trình thư điện tử của A thực hiện mã hoá chìa khoá trên bằng thuật toán có trong PKC với chìa khoá là khoá công cộng của B.

4. Chương trình thư điện tử của A sẽ thực hiện đóng gói thông tin theo đúng giao thức S/MIME. Khi đó gói sẽ gồm: thông điệp đã được mã hoá, khoá ngẫu nhiên đã được mã hoá, chứng chỉ sổ theo chuẩn X.509 của A, và tên của thuật toán mã hoá dữ liệu.

5. Sau khi đã tạo được gói tin, chương trình thư điện tử của A sẽ thực hiện gửi thông điệp tới B theo giao thức gửi nhận mail thông thường.

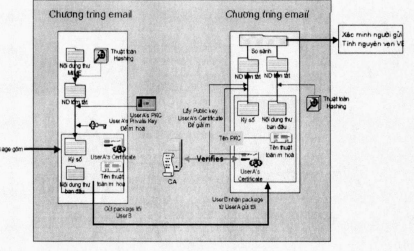
6. Chương trình thư điện tử của B sẽ nhận gói tin.

7. Chương trình thư điện tử của B sẽ sử dụng khoá riêng (bí mật) của B và thuật toán trong PKC để giải mã chìa khoá ngẫu nhiên.

8. Cuối cùng chương trình thư điện tử của B sử dụng thuật toán mã hoá dữ liệu với chìa khoá là khoá ngẫu nhiên thu được sau khi giải mã ở bước trên.

Cơ chế này nhằm đảm bảo tính xác thực thông qua việc xác minh người gửi và tính nguyên vẹn của văn bản ban đầu.

10



Hình trên là sơ đồ của quá trình tạo một thông điệp theo giao thức bảo mật S/MIME nhằm đảm bảo tính xác thực của thông điệp. Để minh hoạ chúng ta tìm hiểu thông qua một

ví dụ mô tả quá trình gửi/nhận theo giao thức S/MIME – đảm báo tính xác thực của thông điệp:

1. Chương trình thư điện tử của A sử dụng hàm hỗn độn (hashfunction) để tạo ra một thông điệp hỗn độn dựa trên thông điệp gốc ban đầu.

2. Chương trình thư điện tử của A thực hiện mã hoá thông điệp hỗn độn vừa nhận được dựa vào thuật toán trong PKC với khoá là chìa khoá riêng của A

3. Cuối cùng chương trình thư điện tử của A sẽ tạo một package gồm: thông điệp gốc ban đầu, thông điệp hỗn độn đã được mã hoá, chứng chỉ số của A và tên thuật toán mã hoá

4. Chương trình thư điện tử của A sau đó thực hiện gửi package tới B thông qua giao thức SMTP

5. Chương trình thư điện tử của B nhận gói tin do A gửi tới

6. Chương trình thư điện tử của B thực hiện xác minh chứng chỉ của A (đính kèm trong gói tin mà B nhận được) bằng cách xác minh chừ ký của CA đã cấp chứng chỉ cho A

11

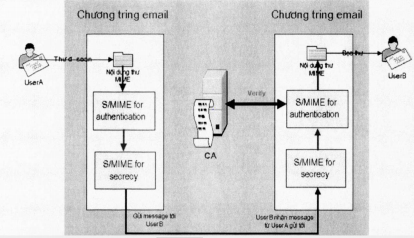
7. Chương trình thư điện tử của B thực hiện lẩy khoá công cộng của A từ chứng chỉ cá nhân của A

8. Chương trình thư điện từ của B sẽ sử dụng khoá công cộng của A để tiến hành giải mã nội dung thông điệp hỗn độn

9. Chương trình thư điện tử của B sẽ tạo ra một bản thông điệp hỗn độn mới bằng cách sử dụng hàm hỗn độn đối với thông điệp gốc ban đầu

10.Chương trình thư điện tử của B sẽ thực hiện so sánh hai thông điệp hỗn độn đó với nhau để xác minh địa chỉ người gừi và tính nguyên vẹn của thông điệp ban đầu.

Bên trên tôi đã trình bày hai cơ chế của S/MIME - đám bảo tính bảo mật và đảm báo tính xác thực. Nhưng để ứng dụng giao thức S/MIME vào thực tế, chúng ta phảii áp dụng kết hợp cả hai cơ chế trên. Dưới đây là sơ đồ mô tả cơ chế hoạt động của giao thức S/MIME:



Để minh hoạ cơ chế làm việc của giao thức S/MIME chúng ta cùng tìm hiểu ví dụ sau:

1. Đầu tiên thông điệp được làm cho có giá trị, tức là chúng ta thực hiện ký nội dung thông điệp bằng CA, áp dụng chỉều đi của quá trình S/MIME-đảm bảo tính xác thực để ký

2. Sau đó, gói tin ký bởi CA được mã hoá, áp dụng chỉều đi của quá trình đám bảo tính bảo mật

12

3. Gói tin bảo mật được gửi tới cho người nhận

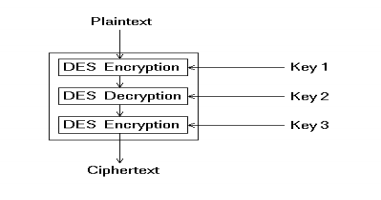
4. Người nhận sẽ sử dụng khoá riêng của họ để thực hiện giải mã khoá ngẫu nhiên (session key)

5. Người nhận sẽ sử dụng khoá ngẫu nhiên để giải mã gói tin báo mật 6. Cuối cùng người nhận thực hiện xác minh tính xác thực của gói tin. Áp dụng chỉều đến của quá trình đám bảo tính xác thực của gói tin để xác minh địa chỉ người gửi và tính nguyên vẹn của thông tin ban đầu.

**2.2 Thuật toán sử dụng**

2.2.1 Thuật toán mã hóa chuẩn TripleDES( 3DES )

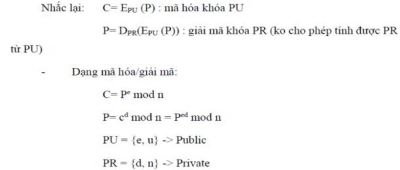
Thuật toán DES (Data Encryption Standard) được chính phủ Mỹ tạo ra năm 1977 (NIST và NSA) dựa trên các công việc mà IBM làm. DES thuộc loại mã khối 64 bits với khoá dài 64 bits. Thuật toán DES đầu tiên đã được nghiên cứu trong thời gian dài.Thuật toán 3DES cải thiện độ mạnh của thuật toán DES bằng việc sử dụng một quá trình mã hóa và giải mã sử dụng 3 khóa. Các chuyên gia xác định rằng 3DES rất an toàn. Nhược điểm của nó là chậm hơn một cách đáng kể so với các thuật toán khác. Bản thân DES đã chậm do dùng các phép hoán vị bit. Lý do duy nhất để dùng 3DES là nó đó được nghiên cứu rất kỹ lưỡng.



13

2.2.2 Thuật toán mã hóa chìa khóa công khai – RSA

Thuật toán RSA được phát minh năm 1978. Thuật toán RSA có hai khóa: khóa công khai (hay khóa công cộng) và khóa bí mật (hay khóa cá nhân). Mỗi khóa là những số cố định sử dụng trong quá trình mã hóa và giải mã. Khóa công khai được công bố rộng rãi cho mọi người và được dùng để mã hóa. Những thông tin được mã hóa bằng khóa công khai chỉ có thể được giải mã bằng khóa bí mật tương ứng. Nói cách khác, mọi người đều có thể mã hóa nhưng chỉ có người biết khóa cá nhân (bí mật) mới có thể giải mã được. Thuật toán sử dụng chế độ mã hóa khối P, C là một số nguyên ∈ (0, n)

• Người gửi và người nhận biết giá trị của n và e, nhưng chỉ người nhận biết giá trị của d.

• Mục đích: tìm các giá trị e, d, n (chọn) để tính P và C

• Nhận xét:

Có thể tìm giá trị của e, d, n sao cho Ped = P mod n với P < n

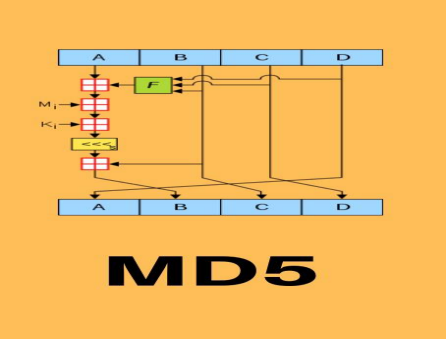
Không thể xác định d nếu biết e và n.

14

2.2.3 Thuật toán hỗn độn một chỉều ( hashing ) – SHA1 hoặc MD5

|  |  |  |
| --- | --- | --- |
|  | MD5 | SHA-1 |
| Bảo Mật | Bảo mật thấp hơn SHA | Bảo mật cao hơn MD5 |
| Kích thước giá trị băm | 128 bit | 160 bit |
| Tốc độ | Nhanh hơn, chỉ 64 lặp lai | Chậm hơn MD5 , 80 lần lặp lại |

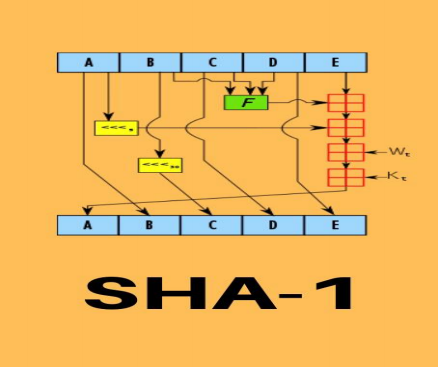
• MD5 : là 1 thuật toán có đầu vào là một thông điệp có độ dài tuỳ ý và có đầu ra là 1 chuỗi có độ dài cố định 128bit. Thuật toán được thiết kế để chạy trên các máy tính 32 bit.



15

• SHA-1: vì MD5 không còn được xem là an toàn, nên người ta đã xây dựng thuật toán băm khác. Một trong những thuật toán đó là SHA-1 mà đã được chính phủ Mỹ chọn làm chuẩn quốc gia. SHA-1 có kích thước giá trị băm là 160 bit.

• Đầu vào của thuật toán là một thông điệp có chỉều dài bất kì nhỏ hơn 264 bit, SHA 1 cho ra kết quả là một thông điệp rút gọn có độ dài 160 bit



16

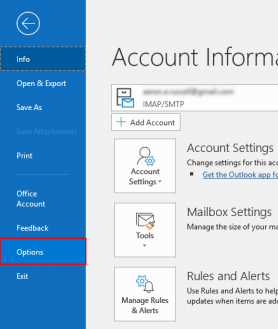
**CHƯƠNG 3: MÔ HÌNH THỰC NGHIỆM**

**3.1 Thiết lập S/MIME trên Outlook 2016**

**Bước 1:** Tải xuống tệp PKCS#12 cùng với chứng chỉ của bạn từ nhà cung cấp chứng chỉ bằng cách nhấp vào liên kết bên trong email khi mua hàng và làm theo hướng dẫn trên màn hình trong trình duyệt của bạn. Bạn sẽ được nhắc nhở tạo mật khẩu khi tải xuống (Lưu ý: giữ mật khẩu này an toàn để cần dùng sau này). Lưu tệp thật kỹ đảm bảo không bị mất nó, nếu mất sẽ không đọc được tin nhắn mã hóa bằng khóa công khai của mình.

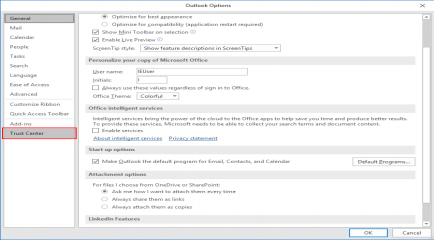
Lưu ý: Khi tải xuống tệp bạn sẽ phải chọn thuật toán mã hóa RSA and ECDSA, bạn hãy chọn RSA.

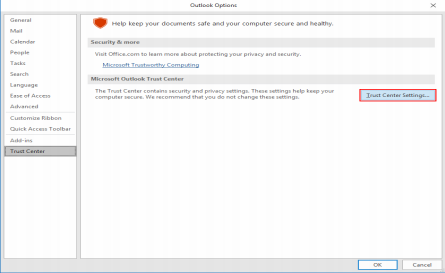
**Bước 2:** Mở Outlook, click **File** và sau đó click **Options**.



17

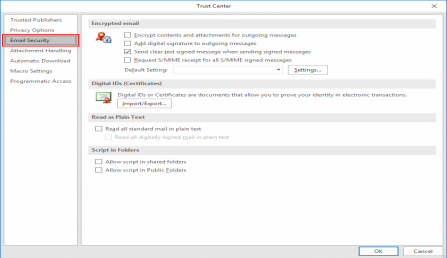
**Bước 3:** Click chọn **Trust Center**.

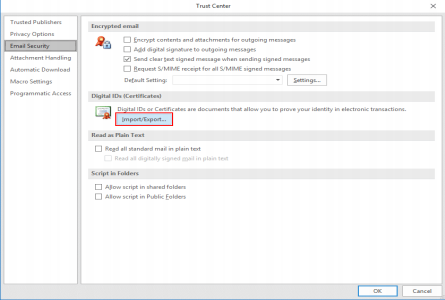
**Bước 4:** Mở **Trust Center Settings**.



18

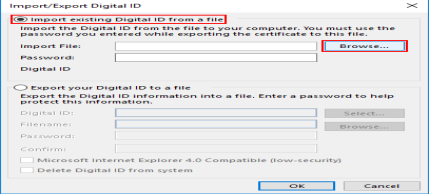
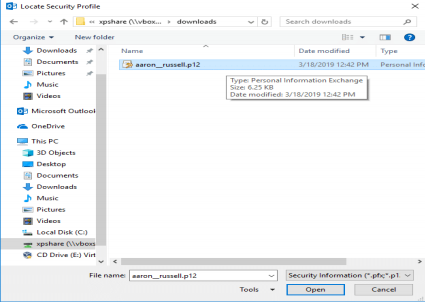
**Bước 5:** Chọn **Email Security**.

**Bước 6:** Click **Import/Export**.

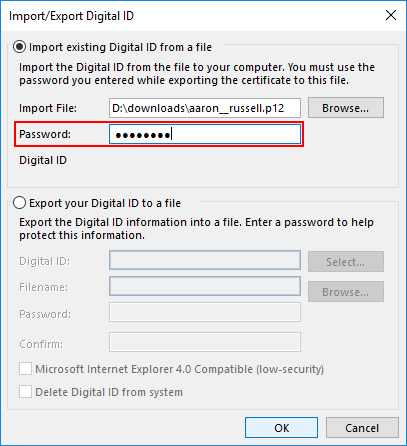


19

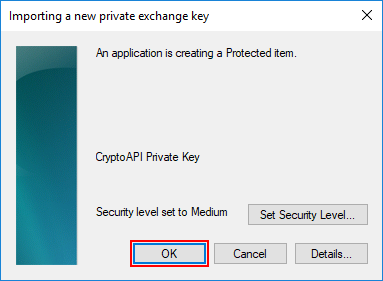
**ước 7:** Chọn file.

Tích chọn **Import existing Digital ID from a file** sau đó click **Browse… Bước 8:** Chọn tệp **PKCS#12** vừa được tải về. Tệp có đuôi **.p12**.

20

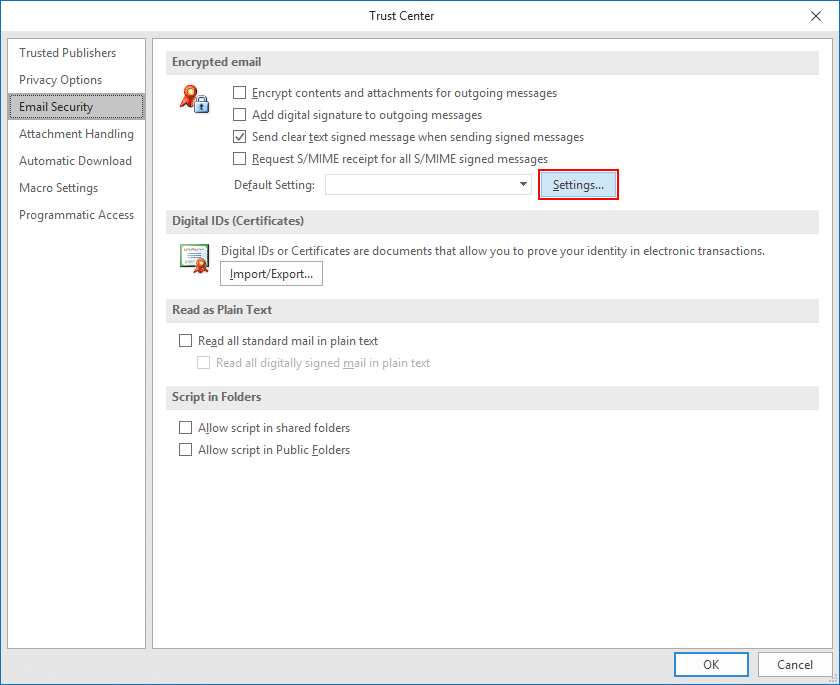
**Bước 9:** Nhập mật khẩu **PKCS#12** sau đó click **OK**. 

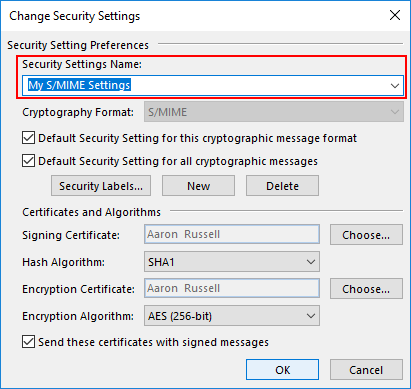
**Bước 10:** Click **OK** khi có của sổ bật lên.



21

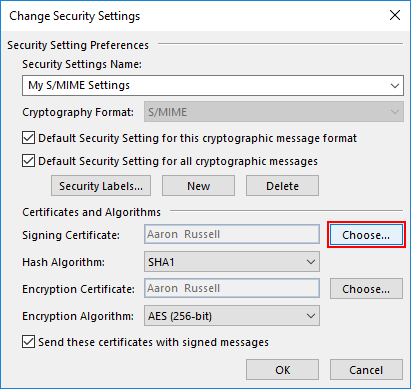
**Bước 11:** Click chọn **Settings**, phía dưới **Encrypted email**.

**Bước 12:** Đặt tên cho cài đặt bảo mật.



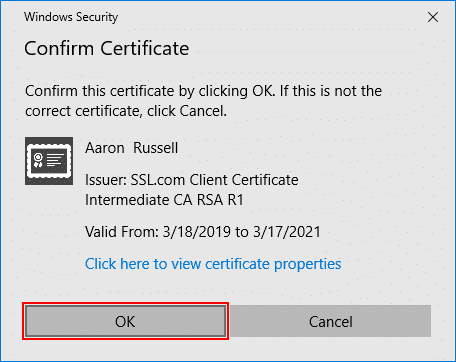
22

**Bước 13:** Chọn **Signing Certificate**.



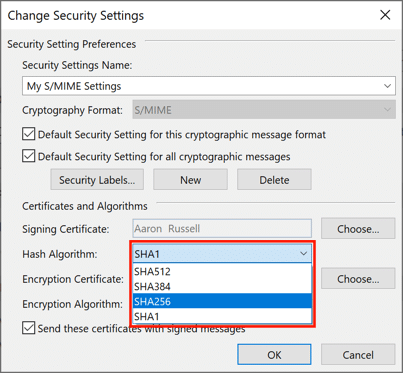
**Bước 14:** Xác nhận hoặc chọn chứng chỉ.

Click **OK** nếu bạn chỉ cài đặt 1 chứng chỉ, nếu cài đặt nhiều chứng chỉ bạn cần chọn chính xác chứng chỉ mình muốn cài đặt.



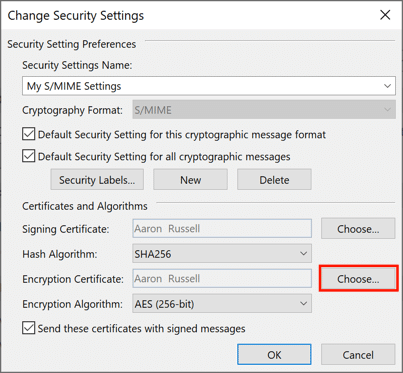
23

**Bước 15:** Click **Choose** và chọn chứng chỉ bạn muốn cài đặt.



**Bước 16:** Click **OK** để đóng cửa sổ **Change Security Settings Bước 17:** Chọn

các thuộc tính bạn mong muốn sau đó click **OK** để đóng cửa sổ.

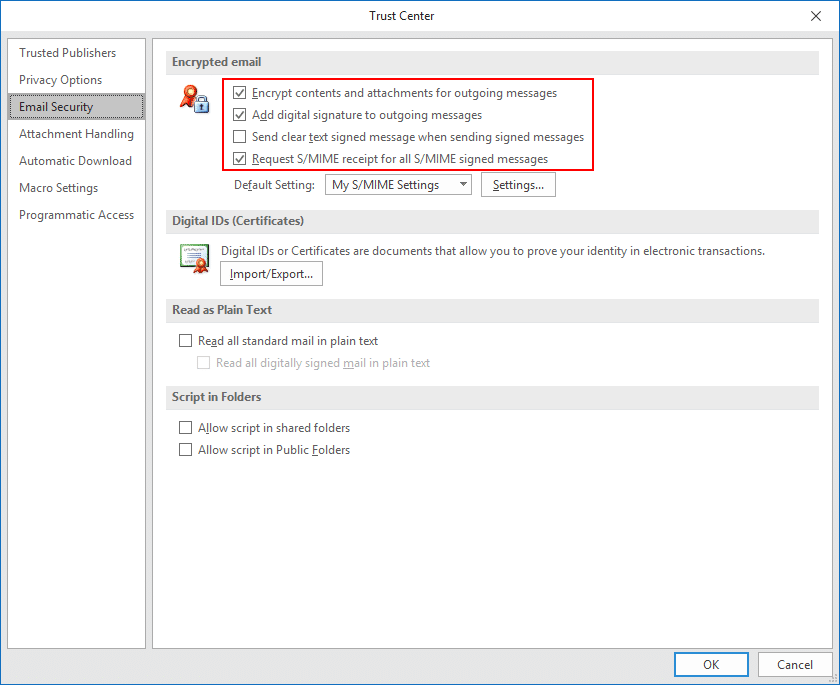


24

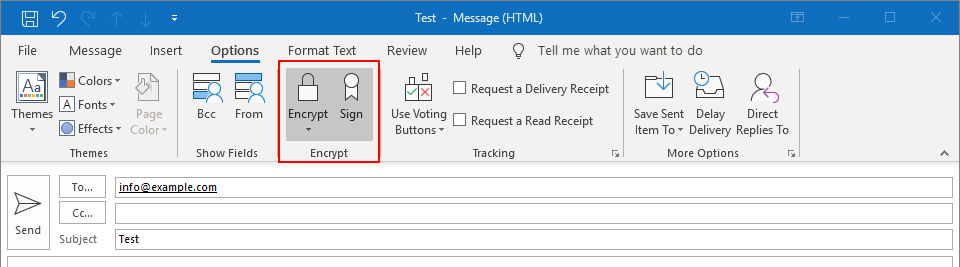
**Bước 17: Đóng cửa sổ.**

Nhấp chuột **OK** để đóng **Thay đổi cài đặt bảo mật** cửa sổ.

**Bước 18:** Chọn tùy chọn chứng chỉ **S/MIME** khi gửi một tin nhắn mới. Bạn có thể chuyển đổi cài đặt mã hóa và chữ kí số dưới phần **Options**.

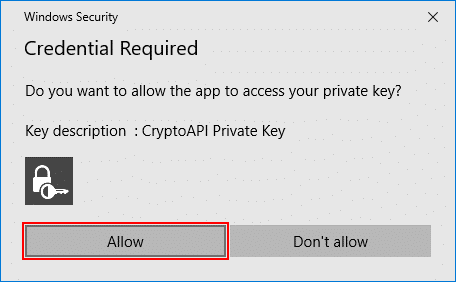


**Bước 19:** Sau khi nhấn gửi, chọn **Allow** khi cửa sổ **Windows Security** bật lên để chấp thuận cho Outlook sử dụng khóa riêng của bạn.

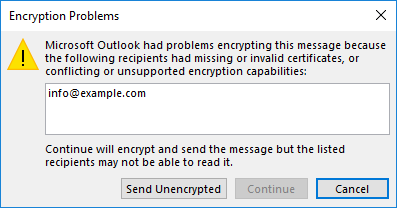


25

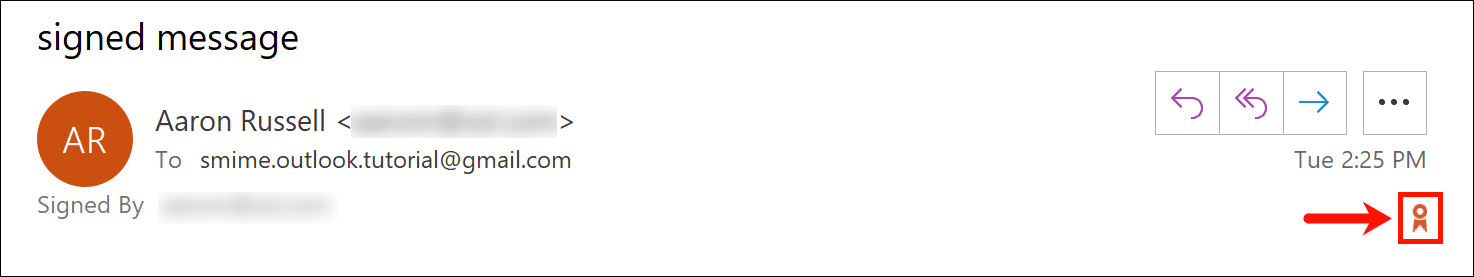
**Bước 20:** Cho phép **Outlook** sử dụng khóa cá nhân của bạn**.**

Sau khi gửi, nhấp vào **Cho phép** trong **Windows Security** hộp thoại xuất hiện, cho phép Outlook sử dụng khóa riêng của bạn.  


**Bước 21: Sự cố tiềm ẩn với mã hóa.**

Lưu ý rằng nếu bạn cố gắng gửi email được mã hóa và không có khóa công khai của người nhận, bạn sẽ nhận được thông báo lỗi cung cấp tùy chọn gửi thư không được mã hóa. Bạn có thể giải quyết vấn đề này đơn giản bằng cách yêu cầu họ gửi cho bạn một email đã ký.

**Bước 22: Xác nhận chữ ký.**

Khi người liên hệ của bạn gửi cho bạn một email đã ký, bạn sẽ thấy một biểu tượng dải băng nhỏ ở góc trên bên phải của thư. Bạn có thể xác nhận thông tin chi tiết của chứng chỉ bằng cách nhấp vào biểu tượng.  


26