TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI

KHOA CÔNG NGHỆ THÔNG TIN

BÁO CÁO THỰC NGHIỆM

Học phần: An toàn và bảo mật thông tin

ĐỀ TÀI: CHỮ KÝ SỐ VÀ ỨNG DỤNG TRONG THƯƠNG MẠI ĐIỆN TỬ.

GVHD: **Lê Thị Anh**

Sinh viên: Tống Khánh Linh – 2021601786

Nguyễn Hồng Ánh – 2021607039

Lê Thị Ngọc Mai – 2021606921

Phan Thị Sao Mai – 2021607248

Quách Thị Hồng Minh – 2021605370

Nhóm: 7

Lớp: 20231IT6001001**. Khóa:** 16

Hà Nội – Năm 2023

MỤC LỤC

LỜI NÓI ĐẦU

Ngày nay, sự bùng nổ của thương mại điện tử đã đem lại nhiều tiện ích và thuận lợi không ngờ cho cả người tiêu dùng và doanh nghiệp. Tuy nhiên, cùng với sự phát triển này là sự gia tăng về quy mô và độ phức tạp của các mối đe dọa an ninh mạng, đặt ra những thách thức không nhỏ đối với tính bảo mật và tính toàn vẹn của thông tin trong các giao dịch trực tuyến.

Trong bối cảnh đó, chữ ký số nổi lên như một công cụ không thể thiếu, giúp xây dựng một hệ thống an ninh mạng vững chắc, đồng thời tạo ra sự tin cậy và khả năng xác thực cho các giao dịch trực tuyến. Đề tài này sẽ tập trung nghiên cứu sâu rộng về chữ ký số và ứng dụng của nó trong thương mại điện tử.

Chữ ký số giúp xác minh nguồn gốc và tính toàn vẹn của tài liệu, đảm bảo rằng nó không bị thay đổi và được tạo ra bởi người ký cụ thể. Nó không chỉ bảo vệ thông tin cá nhân mà còn giúp đảm bảo tính xác thực và nguyên tắc trong quá trình giao dịch. Đồng thời, việc sử dụng chữ ký số cũng mở ra nhiều cơ hội mới, từ việc tăng cường bảo mật thông tin đến việc thúc đẩy sự tin tưởng từ phía khách hàng.

Để tìm hiểu sâu hơn về chữ ký số và ứng dụng của nó, chúng em đã cùng nhau xây dựng và hoàn thành báo cáo thực nghiệm với nội dung đề tài "Chữ ký số và ứng dụng trong thương mại điện tử". Đề tài này sẽ đi sâu vào cách chữ ký số hoạt động, cũng như cách nó được tích hợp và ứng dụng trong môi trường thương mại điện tử. Khám phá những lợi ích mà chữ ký số mang lại và đồng thời xem xét những thách thức và cơ hội khi triển khai chúng trong thực tế.

Các vấn đề cụ thể sẽ được trình bày trong báo cáo thực nghiệm với nội dung gồm 3 chương:

Chương 1: Tổng quan về an toàn bảo mật thông tin và chữ ký số trong thương mại điện tử

Chương 2: Kỹ thuật sử dụng

Chương 3: Mô phỏng và đánh giá

CHƯƠNG 1. TỔNG QUAN VỀ AN TOÀN BẢO MẬT THÔNG TIN VÀ CHỮ KÝ SỐ TRONG THƯƠNG MẠI ĐIỆN TỬ

1.1. An toàn và bảo mật thông tin

1.1.1. Tìm hiểu chung về an toàn và bảo mật thông tin

An toàn bảo mật thông tin (bảo mật thông tin) là quá trình và tập hợp các biện pháp được triển khai để bảo vệ thông tin khỏi các mối đe dọa của kẻ tấn công và bảo đảm tính bảo mật, toàn hiện, sẵn sàng và tư nhân của Information. Nó liên quan đến việc bảo vệ thông tin khỏi các hành vi trái phép như truy cập trái phép, sửa đổi, tiết lộ, hủy hoại hoặc mất mát thông tin.

An toàn bảo mật thông tin đóng vai trò quan trọng trong các tổ chức, doanh nghiệp, cơ quan phủ chính và cá nhân, giả định rằng thông tin quan trọng và nhạy cảm được bảo vệ và chỉ có những người có quyền truy cập mới có thể truy cập và sử dụng.

Để đảm bảo an toàn bảo mật thông tin, các biện pháp bao gồm việc sử dụng mã hóa, quản lý quyền truy cập, xác thực người dùng, giám sát hệ thống, sao lưu dữ liệu, đào tạo nhân viên về an ninh thông tin tin và tuân thủ các quy tắc và quy định liên quan đến bảo mật.

Các phương pháp bảo vệ an toàn thông tin dữ liệu có thể được quy tụ vào ba nhóm sau:

- Bảo vệ an toàn thông tin bằng các biện pháp hành chính.

- Bảo vệ an toàn thông tin bằng các biện pháp kỹ thuật (phần cứng).

- Bảo vệ an toàn thông tin bằng các biện pháp thuật toán (phần mềm).

Ba nhóm trên có thể được ứng dụng riêng rẽ hoặc phối kết hợp. Môi trường khó bảo vệ an toàn thông tin nhất và cũng là môi trường đối phương dễ xân nhập nhất đó là môi trường mạng và truyền tin. Biện pháp hiệu quả nhất và kinh tếnhất hiện nay trên mạng truyền tin và mạng máy tính là biện pháp thuật toán. An toàn thông tin bao gồm các nội dung sau:

- Tính bí mật: tính kín đáo riêng tư của thông tin

- Tính xác thực của thông tin, bao gồm xác thực đối tác (bài toán nhận danh), xác thực thông tin trao đổi.

- Tính trách nhiệm: đảm bảo người gửi thông tin không thể thoái thác trách nhiệm về thông tin mà mình đã gửi.

1.1.2. Tầm quan trọng của bảo mật thông tin

An toàn bảo mật thông tin là một yếu tố cực kỳ quan trọng trong thế giới kỹ thuật số ngày nay. Đây là những lý do quan trọng vì sao an toàn bảo mật thông tin được coi là tầm quan trọng:

• **Bảo vệ thông tin cá nhân**: Với sự phát triển của Internet và công nghệ thông tin, thông tin cá nhân của chúng ta trở nên dễ dàng tiếp cận hơn bao 7 giờ hết. An toàn bảo mật thông tin giúp đảm bảo rằng thông tin cá nhân như tên, địa chỉ, số điện thoại, thông tin tài chính và y tế không bị lộ ra ngoài và không bị lạm dụng.

• **Bảo vệ quyền riêng tư**: An toàn bảo mật thông tin đóng vai trò quan trọng trong bảo vệ quyền riêng tư của cá nhân và tổ chức. Nếu thông tin riêng tư của người dùng bị xâm phạm, điều này có thể gây ra những hậu quả nghiêm trọng như vi phạm quyền riêng tư, mất danh dự và thậm chí bị kích động xâm hại tâm lý.

• **Đảm bảo an ninh quốc gia**: An toàn bảo mật thông tin cũng là một yếu tố quan trọng để đảm bảo an ninh quốc gia. Thông tin quan trọng về chính trị, quân sự, kinh tế và công nghệ được coi là tài sản quốc gia và cần được bảo vệ chặt chẽ để ngăn chặn các cuộc tấn công, gián điệp và lừa đảo từ các thế lực thù địch.

• **Đảm bảo hoạt động ổn định của tổ chức và hệ thống**: An toàn bảo mật thông tin là yếu tố không thể thiếu để đảm bảo hoạt động ổn định của các tổ chức và hệ thống. Một cuộc tấn công mạng có thể gây ra sự gián đoạn, mất mát dữ liệu, hoặc ngừng hoạt động của các hệ thống quan trọng như ngân hàng, viễn thông, điện lực và hệ thống giao thông.

• **Đảm bảo uy tín và niềm tin**: An toàn bảo mật thông tin đóng vai trò quan trọng trong việc xây dựng uy tín và niềm tin từ phía khách hàng, đối tác và công chúng. Khi mọi thông tin được bảo vệ an toàn, người dùng và các bên liên quan sẽ có niềm tin vào tổ chức và dịch vụ của nó, từ đó tạo nên một môi trường kinh doanh và giao dịch tin cậy.

Vì những lý do trên, an toàn bảo mật thông tin không chỉ là một yếu tố quan trọng mà còn là một trách nhiệm đối với cá nhân, tổ chức và xã hội. Việc đảm bảo an toàn bảo mật thông tin đòi hỏi sự nhận thức, chuẩn bị và triển khai các biện pháp bảo mật phù hợp để bảo vệ thông tin và đối phó với các mối đe dọa mạng ngày càng tinh vi và phức tạp.

1.2. Chữ ký số.

Chữ ký số là một kỹ thuật toán học được sử dụng để xác thực tính xác thực và tính toàn vẹn của tin nhắn, phần mềm hoặc tài liệu kỹ thuật số.

1.2.1. Ưu điểm của chữ ký số.

Văn bản pháp luật và hợp đồng: Chữ ký số có tính ràng buộc về mặt pháp lý. Điều này khiến chúng trở nên lý tưởng cho bất kỳ tài liệu pháp lý nào yêu cầu chữ ký được xác thực bởi một hoặc nhiều bên và đảm bảo rằng hồ sơ không bị thay đổi.

Hợp đồng mua bán: Ký kết kỹ thuật số hợp đồng và hợp đồng mua bán xác thực danh tính của người bán và người mua, đồng thời cả hai bên có thể chắc chắn rằng chữ ký có tính ràng buộc về mặt pháp lý và các điều khoản của thỏa thuận không bị thay đổi.

Chứng từ tài chính: Bộ phận tài chính ký điện tử hóa đơn để khách hàng có thể tin tưởng rằng yêu cầu thanh toán là từ người bán phù hợp chứ không phải từ kẻ xấu đang cố lừa người mua gửi thanh toán đến tài khoản lừa đảo.

Dữ liệu sức khỏe: Trong ngành chăm sóc sức khỏe, quyền riêng tư là điều tối quan trọng đối với cả hồ sơ bệnh nhân và dữ liệu nghiên cứu. Chữ ký số đảm bảo rằng thông tin bí mật này không bị sửa đổi khi nó được truyền giữa các bên đồng ý. Các cơ quan chính quyền liên bang, tiểu bang và địa phương có chính sách và quy định chặt chẽ hơn nhiều công ty thuộc khu vực tư nhân. Từ việc phê duyệt giấy phép đến đóng dấu chúng vào bảng chấm công, chữ ký điện tử có thể tối ưu hóa năng suất bằng cách đảm bảo đúng người tham gia phê duyệt phù hợp.

Chứng từ vận chuyển: Giúp nhà sản xuất tránh các lỗi vận chuyển tốn kém bằng cách đảm bảo bản kê khai hàng hóa hoặc vận đơn luôn chính xác. Tuy nhiên, giấy tờ vật lý rất cồng kềnh, không phải lúc nào cũng dễ dàng lấy được trong quá trình vận chuyển và có thể bị thất lạc. Bằng cách ký điện tử các chứng từ vận chuyển, người gửi và người nhận có thể nhanh chóng truy cập vào tệp, kiểm tra xem chữ ký có được cập nhật hay không và đảm bảo rằng không có sự giả mạo nào xảy ra.

1.2.2. Hạn chế của chữ ký số

Sự phụ thuộc vào quản lý khóa: Chữ ký số dựa vào việc quản lý an toàn các khóa mật mã. Điều này có nghĩa là người gửi phải giữ khóa riêng của họ an toàn và bảo mật khỏi bị truy cập trái phép, trong khi người nhận phải xác minh khóa

chung của người gửi để đảm bảo tính xác thực của nó. Bất kỳ sai sót nào trong việc quản lý khóa đều có thể ảnh hưởng đến tính bảo mật của chữ ký số.

Độ phức tạp: Chữ ký số yêu cầu một quy trình phức tạp về tạo khóa, ký và xác minh. Điều này có thể gây khó khăn cho việc triển khai và sử dụng chúng đối với những người dùng không rành về kỹ thuật.

Khả năng tương thích: Các thuật toán và định dạng chữ ký số khác nhau có thể không tương thích với nhau, gây khó khăn cho việc trao đổi các tin nhắn đã ký giữa các hệ thống và ứng dụng khác nhau.

Công nhận pháp lý: Mặc dù chữ ký số được công nhận hợp pháp ở nhiều quốc gia nhưng tình trạng pháp lý của chúng có thể không rõ ràng ở tất cả các khu vực pháp lý. Điều này có thể hạn chế tính hữu dụng của chúng trong bối cảnh pháp lý hoặc quy định.

Thu hồi: Trong trường hợp có sự xâm phạm chính hoặc các vấn đề bảo mật khác, chữ ký số phải được thu hồi để ngăn chặn việc sử dụng sai mục đích. Tuy nhiên, quá trình thu hồi có thể phức tạp và có thể không hiệu quả trong mọi trường hợp.

Chi phí: Chữ ký số có thể kéo theo chi phí bổ sung cho việc quản lý khóa, cấp chứng chỉ và các dịch vụ liên quan khác, điều này có thể khiến chúng trở nên đắt đỏ đối với một số người dùng hoặc tổ chức.

Phạm vi giới hạn: Chữ ký số cung cấp khả năng xác thực và bảo vệ tính toàn vẹn cho tin nhắn nhưng chúng không cung cấp tính bảo mật hoặc bảo vệ chống lại các loại tấn công khác, chẳng hạn như tấn công từ chối dịch vụ hoặc phần mềm độc hại.

1.3. Ứng dụng của chữ ký số.

Sử dụng chữ ký số để kê khai thuế, khai báo hải quan: Nhằm tiết kiệm thời gian xếp hàng chờ đợi của doanh nghiệp, cũng như phần nào giảm tải cho bộ phận tiếp nhận hồ sơ giấy của cơ quan Thuế/ Hải quan, việc sử dụng chữ ký số để thực hiện thủ tục trực tuyến trên cổng dịch vụ công là giải pháp tối ưu để đảm bảo sự nhanh gọn, thuận tiện cho cả hai bên. Theo đó, doanh nghiệp không cần in tờ khai mẫu, đóng dấu mộc đỏ và tới nộp trực tiếp tại cơ quan nhà nước. Người đại diện

kê khai chỉ cần truy cập và đăng ký tài khoản trên hệ thống cổng dịch vụ điện tử của Thuế/Hải quan, sử dụng chữ ký số để thực hiện các thủ tục hành chính cần thiết mọi lúc mọi nơi như: Kê khai thuế; Nộp hồ sơ khai thuế; Nộp thuế điện tử; Yêu cầu hoàn thuế, được giải quyết hoàn thuế nhanh chóng; Nhận thông báo thực hiện nghĩa vụ về thuế của cơ quan Thuế…; Thực hiện mọi thủ tục hải quan cho hàng hóa nhập khẩu/xuất khẩu (mở tờ khai hải quan, nộp hồ sơ chứng từ, nộp thuế điện tử VAT/ thuế xuất nhập khẩu/ thuế tiêu thụ đặc biệt,…).; Chữ ký số đã góp phần tạo sự thông thoáng và tăng cường hiệu quả cho các thủ tục hành chính về Thuế/Hải quan. Điều này đã được chứng minh qua các con số VNPT tổng hợp như sau: Giảm được 92% các lỗi đến từ việc xác thực công cụ khác; giảm 86% cho chi phí in ấn, xử lý tài liệu; tiết kiệm hơn 22.000h lao động mỗi năm hay giảm 66% việc thất lạc tài liệu. Đồng thời việc ứng dụng chữ ký số còn giúp tăng 85% hiệu suất làm việc của người lao động.

Dùng chữ ký số phát hành hóa đơn điện tử: Nhắc tới ứng dụng chữ ký số trong doanh nghiệp thì không thể thiếu hóa đơn điện tử – một loại chứng từ chứng minh giao dịch mua bán hàng hóa thường ngày. Theo quy định pháp luật, hóa đơn điện tử của doanh nghiệp muốn đảm bảo tính hợp lệ và hợp pháp thì bắt buộc phải có chữ ký số (ngoại trừ những loại hóa đơn đặc biệt như điện, nước, viễn thông, hóa đơn điện tử khởi tạo từ máy tính tiền…). Loại chữ ký này là yếu tố để kiểm tra, đánh giá và phát hiện tình trạng gian lận, giả mạo hóa đơn. Ngoài ra, doanh nghiệp có thể linh động lựa chọn ký số từng hóa đơn, hoặc ký tốc độ cao cho nhiều hóa đơn cùng lúc để phát hành theo lô lớn… giúp rút ngắn quy trình phát hành và xử lý, thuận tiện đối chiếu dữ liệu, đồng thời tiết kiệm các chi phí vận hành liên quan, tăng khả năng tiếp cận với khách hàng tiềm năng.

Ký kết hợp đồng điện tử với đối tác: Với chữ ký số, doanh nghiệp có thể thực hiện các giao dịch thương mại hoàn toàn trực tuyến. Thay vì hai bên phải di chuyển và trực tiếp gặp mặt tại trụ sở/ chi nhánh công ty, thì các tài liệu như thư ngỏ hợp tác, hợp đồng, thỏa thuận sẽ được gửi đi bằng email đến phía đối tác và được ký kết nhanh chóng bằng thiết bị máy tính hoặc điện thoại thông minh… Quy trình này làm giảm các đầu việc thủ công khác như đóng gói thư từ,

dán tem, chờ đợi nhân viên bưu điện… đặc biệt tiết kiệm thời gian và tiền bạc trong trường hợp hai bên doanh nghiệp có khoảng cách xa về mặt địa lý như doanh nghiệp ở ngoại tỉnh hoặc công ty nước ngoài, cắt giảm được các khoản tiền xăng xe, ăn uống, chi phí vé máy bay, khách sạn… Chưa kể, trong trường hợp có sai sót, cần chỉnh sửa hợp đồng thì khoản phí trên có thể càng dôi lên gấp bội. Theo thống kê chi phí dựa trên các dịch vụ hợp đồng điện tử tích hợp chữ ký số hiện có trên thị trường, với 1 lần ký kết hợp đồng, doanh nghiệp chỉ cần chi từ khoảng 5.000 – 20.000 VND. Đặc biệt, một số nhà cung cấp như VNPT có mức giá cực kỳ cạnh tranh, chỉ từ 5.000 VND/ 1 lần ký. Có thể nói đây là khoản phí tối thiểu giúp doanh nghiệp tối ưu được lợi nhuận ở mức cao nhất. Bên cạnh đó, chữ ký số không chỉ rút ngắn thời gian và khoảng cách giao dịch, mà còn gián tiếp mang lại trải nghiệm hài lòng và tăng khả năng giữ chân khách hàng cho doanh nghiệp.

Ngoài ra còn một số ứng dụng khác trong thương mại điện tử như:

Chứng thực danh tính người tham gia giao dịch: Chữ ký số giúp xác thực danh tính của các bên tham gia giao dịch, từ đó tạo ra một môi trường giao dịch an toàn và có thể tin cậy. Bằng việc mã hóa thông tin, chữ ký số đảm bảo rằng chỉ những người được ủy quyền mới có thể truy cập thông tin giao dịch.

Chứng thực tính nguyên vẹn của văn bản, tài liệu: Khi một tài liệu được ký bằng chữ ký số, bất kỳ sự thay đổi nào đối với nội dung tài liệu sau đó sẽ làm hỏng chữ ký. Điều này giúp người nhận biết được nếu tài liệu đã bị can thiệp hoặc chỉnh sửa sau khi đã được ký.

Xác thực trong Internet banking: Ngân hàng trực tuyến sử dụng chữ ký số để xác thực danh tính của khách hàng và xác nhận giao dịch, từ đó giảm thiểu rủi ro gian lận và tăng cường bảo mật cho các giao dịch trực tuyến.

Thanh toán điện tử: Trong việc thanh toán điện tử, chữ ký số giúp đảm bảo rằng thông tin về giao dịch được giữ an toàn và chỉ những người có quyền truy cập mới có thể xem hoặc thay đổi nó.

Xác thực trong giao dịch chứng khoán: Trên thị trường chứng khoán, chữ ký số giúp đảm bảo rằng chỉ những người được ủy quyền mới có thể thực hiện các giao dịch, từ đó giảm thiểu rủi ro gian lận và tăng cường tính minh bạch.

Xác thực trong mua bán, đấu thầu qua mạng: Trong các giao dịch mua bán và đấu thầu trực tuyến, chữ ký số được sử dụng để xác thực danh tính của các bên tham gia, đảm bảo rằng chỉ những người có quyền mới có thể thực hiện các giao dịch. Điều này tạo nên một môi trường giao dịch công bằng và minh bạch.

Ứng dụng trong Giao dịch bất động sản trực tuyến: Trong các giao dịch bất động sản trực tuyến, chữ ký số có thể giúp xác nhận danh tính của các bên và đảm bảo rằng các chi tiết về giao dịch được ghi lại chính xác và không bị thay đổi sau khi đã được thỏa thuận.

Xác thực trạng thái phần mềm: Các nhà sản xuất, cung cấp phần mềm có thể sử dụng chữ ký số để chứng minh rằng một phiên bản cụ thể của một ứng dụng là chính thức và chưa bị chỉnh sửa kể từ khi nó được phát hành.

Ứng dụng trong giao dịch B2B: Bởi thương mại điện tử giữa các doanh nghiệp (B2B) vốn cần nhiều giấy tờ, thủ tục xác minh nên chữ ký số đặc biệt phù hợp với các doanh nghiệp có đối tượng khách hàng, đối tác,… là các doanh nghiệp khác.

Ứng dụng trong Chính phủ điện tử (e-Government): Chữ ký số cũng có thể sử dụng rộng rãi trong các dịch vụ chính phủ điện tử, giúp đảm bảo rằng thông tin cá nhân của người dân được bảo vệ và rằng chỉ những người có quyền mới có thể truy cập vào các dịch vụ cung cấp.

Các phần mềm chữ ký số ở Việt Nam hiện nay như: 1Office – CA, chữ ký số Misa chữ ký số FPT-CA, chữ ký số Viettel-CA, chữ ký số BKAV-CA, chữ ký số VNPT-CA, chữ ký số Vina-CA, phần mềm chữ ký số New-CA,…

1.4. Tầm quan trọng của chữ ký số trong thương mại điện tử

Trong bối cảnh môi trường thương mại điện tử ngày nay, sự bảo mật thông tin trở thành một ưu tiên hàng đầu do sự tăng cường quy mô và phức tạp của các giao dịch trực tuyến. Trước những mối đe dọa ngày càng tiên tiến, việc đảm bảo

tính toàn vẹn và xác thực của thông tin giao dịch không chỉ là một yếu tố quan trọng mà còn là yếu tố quyết định sự thành công của các doanh nghiệp thương mại điện tử.

Trong thương mại điện tử ngày nay, an toàn và bảo mật thông tin đóng vai trò quan trọng để đảm bảo sự tin tưởng của người tiêu dùng và doanh nghiệp. Tuy nhiên, tình hình hiện tại đối mặt với một số thách thức:

Tăng Cường Các Hệ Thống Phòng Thủ:

- Do sự phát triển của công nghệ, cần phải liên tục nâng cao và tăng cường các hệ thống bảo mật để ngăn chặn các mối đe dọa ngày càng tinh vi.

Quản Lý Dữ Liệu Người Dùng:

- Dữ liệu cá nhân của người dùng ngày càng trở thành mục tiêu cho các cuộc tấn công. Quản lý và bảo vệ dữ liệu này là một thách thức lớn.

Tăng Cường Năng Lực Phòng Chống Tấn Công:

- Cần đào tạo nhân sự và triển khai công nghệ để phòng ngừa và phản ứng nhanh chóng trước các hình thức tấn công mới và tiên tiến. Đảm bảo bảo mật an toàn trong các giao dịch hoặc thanh toán.

Tầm quan trọng của chữ ký số trong thương mại điện tử:

- Xác thực đồng thời và tính xác thực cao: chữ ký số không chỉ đảm bảo tính xác thực của các đối tác thương mại mà còn cung cấp một cơ chế xác thực đồng thời, giảm thiểu rủi ro gian lận và mạo danh trong quá trình giao dịch.
- Bảo vệ tính toàn vẹn của thông tin: Chữ ký số đóng vai trò quan trọng trong việc bảo vệ tính toàn vẹn của dữ liệu giao dịch. Nó giúp ngăn chặn bất kỳ sửa đổi nào không hợp lý và đảm bảo rằng thông tin không bị thay đổi trái ý muốn.
- Tạo sự tin tưởng từ phía khách hàng: việc tích hợp chữ ký số tạo ra sự tin tưởng mạnh mẽ từ phía khách hàng. Khả năng đảm bảo an toàn và bảo mật của thông tin cá nhân và tài khoản tài chính là yếu tố quyết định sự lựa chọn của khách hàng.

Mục tiêu:

- Nghiên cứu cơ bản về cách chữ ký số hoạt động và tại sao nó là một công cụ quan trọng trong bảo mật thông tin.
- Mô phỏng chữ ký số

Ý nghĩa:

- Hiểu rõ hơn về cách chữ ký số giúp củng cố tính bảo mật của thông tin giao dịch.
- Nắm vững cơ sở lý thuyết và áp dụng chữ ký số để tối ưu hóa bảo mật trong môi trường thương mại điện tử.

1.5. Công cụ sử dụng.

Ngôn ngữ lập trình Pyhton: Python là một ngôn ngữ lập trình bậc cao, nổi bật với cú pháp ngắn gọn và dễ đọc, giúp người lập trình giảm độ phức tạp của mã nguồn và tăng cường sự hiệu quả trong quá trình phát triển. Sự ngắn gọn này không chỉ giúp giảm thời gian viết mã mà còn tạo điều kiện thuận lợi cho việc bảo trì và mở rộng mã nguồn trong tương lai.

Một trong những đặc điểm quan trọng của Python là hỗ trợ lập trình hướng đối tượng (OOP). Điều này cho phép người lập trình tổ chức mã nguồn một cách cấu trúc và tái sử dụng mã nguồn dễ dàng hơn thông qua việc sử dụng các khái niệm như lớp và đối tượng.

Cộng đồng Python rộng lớn và tích cực, cung cấp nhiều thư viện và framework mạnh mẽ, giúp giảm bớt gánh nặng phát triển và tăng tốc quá trình xây dựng ứng dụng. Sự đa dạng của các thư viện này hỗ trợ nhiều lĩnh vực, từ phân tích dữ liệu, trí tuệ nhân tạo, đến phát triển web.

Python cũng thể hiện tính chất đa nền tảng, có thể chạy trên nhiều hệ điều hành khác nhau, từ Windows đến Linux và macOS, tạo ra sự linh hoạt trong triển khai ứng dụng. Những đặc tính này khiến Python trở thành một công cụ lập trình mạnh mẽ, phù hợp cho cả những dự án phức tạp và nhu cầu ứng dụng đa dạng.

CHƯƠNG 2. KỸ THUẬT SỬ DỤNG

2.1. Cơ sở lý thuyết.

2.1.1. Các khái niệm cơ bản.

Public-Key Algorithms (thuật toán khóa công khai còn được gọi là mã hóa bất đối xứng - asymmetric algorithms): khóa để mã hóa khác với khóa giải mã. Thêm nữa khóa giải mã không thể được tìm ra từ khóa mã hóa. Khóa mã hóa (public key) và khóa giải mã (private key).

DSA (Digital Signature Algorithms – được sử dụng như một phần tiêu chuẩn chữ ký số) là một thuật toán khóa công khai khác. Nó không thể được sử dụng để mã hóa mà chỉ dùng cho chữ ký số.

Hàm một chiều: khái niệm hàm một chiều là trọng tâm của mật mã khóa công khai. Hàm một chiều không phải là giao thức.Hàm một chiều tương đối dễ tính toán nhưng khó đảo ngược hơn đáng kể. Nghĩa là cho x dễ tính f(x) nhưng với f(x) thì khó tính x. Trong ngữ cảnh này, "khó" được định nghĩa như sau: sẽ mất hàng triệu năm để tính x từ f(x), ngay cả khi tất cả máy tính trên thế giới đều được giao giải quyết vấn đề đó. Đập vỡ một cái đĩa là một ví dụ điển hình về hàm một chiều. Thật dễ dàng để đập vỡ một cái đĩa thành hàng nghìn mảnh nhỏ. Tuy nhiên, không dễ để xếp tất cả những mảnh nhỏ đó lại với nhau vào một chiếc đĩa.

Hàm băm một chiều (One-way hash functions): hàm băm một chiều có nhiều tên: hàm nén, hàm rút gọn, tóm tắt tin nhắn, dấu vân tay, tổng kiểm tra mật mã, kiểm tra tính toàn vẹn của tin nhắn (MIC - message integrity check) và mã phát hiện thao tác (MDC - manipulation detection code). Hàm băm một chiều là một khối xây dựng khác cho nhiều giao thức.

Hàm băm đã được sử dụng trong khoa học máy tính từ lâu. Hàm băm là một hàm, toán học hay nói cách khác, lấy chuỗi đầu vào có độ dài thay đổi (được gọi là tiền ảnh pre-image) và chuyển đổi nó thành chuỗi đầu ra có độ dài cố định (thường nhỏ hơn) (được gọi là giá trị băm – hash value). Hàm băm đơn giản sẽ là hàm lấy ảnh trước và trả về một byte bao gồm XOR của tất cả các byte đầu vào.

Hàm băm một chiều là hàm băm hoạt động theo một hướng: Dễ dàng tính toán một hàm băm giá trị từ ảnh trước, nhưng thật khó để tạo ra ảnh trước băm thành một giá trị cụ thể. Hàm băm được đề cập trước đây không phải là một chiều: cho trước một giá trị byte cụ thể, việc tạo ra một chuỗi byte có XOR là giá trị đó là chuyện đơn giản. Hàm băm một chiều tốt cũng không bị xung đột: Thật khó để tạo ra hai ảnh trước có cùng giá trị băm. Hàm băm là công khai.

Chữ ký viết tay từ lâu đã được sử dụng làm bằng chứng về quyền tác giả hoặc ít nhất là sự đồng ý với nội dung của tài liệu. Điều gì khiến chữ ký lại có sức thuyết phục đến vậy?

- Chữ ký là xác thực. Chữ ký thuyết phục người nhận tài liệu rằng người ký đã cố tình ký vào tài liệu.
- Chữ ký không thể giả mạo. Chữ ký là bằng chứng cho thấy người ký chứ không phải ai khác đã cố tình ký vào tài liệu.
- Chữ ký không thể sử dụng lại được. Chữ ký là một phần của tài liệu; một người vô đạo đức không thể chuyển chữ ký sang một tài liệu khác.
- Văn bản đã ký không thể thay đổi được. Sau khi tài liệu được ký, nó không thể được thay đổi.
- Chữ ký không thể bị bác bỏ. Chữ ký và tài liệu là những thứ vật chất. Người ký tên sau đó không thể khẳng định rằng mình đã không ký nó.

2.1.2. Ký tài liệu bằng mật mã khóa công khai (Signing Documents with Public-Key Cryptography)

Giao thức cơ bản của chữ ký số:

- Alice mã hóa tài liệu bằng khóa riêng của mình, từ đó ký vào tài liệu.
- Alice gửi tài liệu đã ký cho Bob.
- Bob giải mã tài liệu bằng khóa chung của Alice, từ đó xác minh chữ ký.

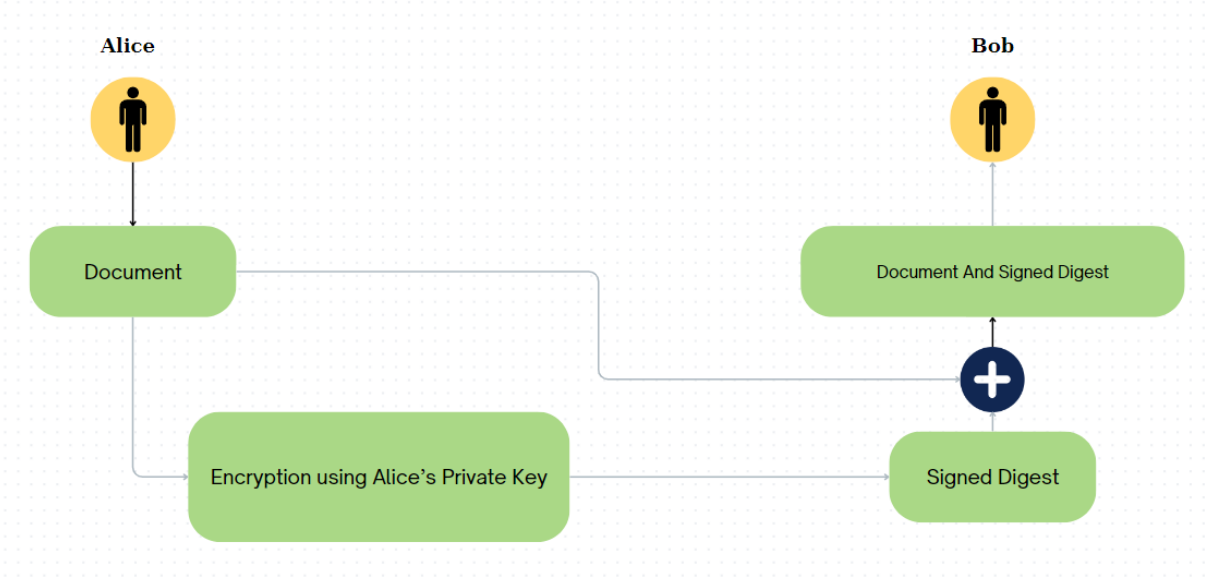

Image 1. Ký tài liệu bằng mật mã khóa công khai

Giao thức này cũng đáp ứng các đặc điểm:

1. Chữ ký là xác thực; Khi Bob xác minh tin nhắn bằng khóa chung của Alice, anh ấy biết rằng cô ấy đã ký nó.
2. Chữ ký không thể giả mạo; chỉ có Alice biết khóa riêng của cô ấy.
3. Chữ ký không được sử dụng lại; chữ ký là một chức năng của tài liệu và không thể chuyển sang bất kỳ tài liệu nào khác.
4. Văn bản đã ký không được sửa đổi; nếu có bất kỳ thay đổi nào đối với tài liệu, chữ ký sẽ không thể được xác minh bằng khóa chung của Alice nữa.
5. Chữ ký không thể bị bác bỏ. Bob không cần sự giúp đỡ của Alice để xác minh chữ ký của cô ấy.

Ký tài liệu và dấu thời gian (Signing Documents and Timestamps)

Thực ra, Bob có thể lừa Alice trong một số trường hợp nhất định. Anh ta có thể sử dụng lại tài liệu và chữ ký cùng nhau. Sẽ không có vấn đề gì nếu Alice ký một hợp đồng (bản sao khác của cùng một hợp đồng là gì, ít nhiều?), nhưng sẽ rất thú vị nếu Alice ký vào séc kỹ thuật số.

Giả sử Alice gửi cho Bob một tấm séc kỹ thuật số có chữ ký trị giá 100 đô la. Bob mang séc đến ngân hàng để xác minh chữ ký và chuyển tiền từ tài khoản này sang tài khoản khác. Bob, một nhân vật vô đạo đức, đã lưu một bản sao của séc kỹ thuật số. Tuần sau, anh ta lại mang nó đến ngân hàng (hoặc có thể đến ngân hàng khác).

Ngân hàng xác minh chữ ký và chuyển tiền từ tài khoản này sang tài khoản khác. Nếu Alice không bao giờ cân đối sổ séc của mình thì Bob có thể duy trì việc này trong nhiều năm.

Do đó, chữ ký số thường bao gồm dấu thời gian. Ngày, giờ ký được đính kèm vào tin nhắn và được ký cùng với phần còn lại của tin nhắn. Ngân hàng lưu trữ dấu thời gian này trong cơ sở dữ liệu. Bây giờ, khi Bob cố gắng thanh toán séc của Alice lần thứ hai, ngân hàng sẽ kiểm tra dấu thời gian dựa trên cơ sở dữ liệu của nó. Vì ngân hàng đã thanh toán séc từ Alice bằng séc tương tự dấu thời gian, ngân hàng gọi cảnh sát. Sau đó, Bob dành nhiều năm trong nhà tù để đọc các giao thức mật mã.

2.1.3. Ký tài liệu bằng mật mã khóa công khai và hàm băm một chiều (Signing Documents with Public-Key Cryptography and One-Way Hash Functions)

Trong triển khai thực tế, các thuật toán khóa công khai thường kém hiệu quả để ký các tài liệu dài. Bob không cần sự giúp đỡ của Alice để xác minh chữ ký của cô ấy. Để tiết kiệm thời gian, các giao thức chữ ký số thường được triển khai bằng hàm băm một chiều thay vì ký một tài liệu, Alice ký vào hàm băm của tài liệu. Trong giao thức này, cả hàm băm một chiều và thuật toán chữ ký số đều được thỏa thuận trước.

1. Alice tạo ra hàm băm một chiều của tài liệu.
2. Alice mã hóa hàm băm bằng khóa riêng (private key) của mình, từ đó ký vào tài liệu.
3. Alice gửi tài liệu và hàm băm đã ký cho Bob.
4. Bob tạo ra hàm băm một chiều của tài liệu mà Alice đã gửi. Sau đó, anh ta sử dụng thuật toán chữ ký số để giải mã hàm băm đã ký bằng khóa chung của Alice. Nếu hàm băm đã ký khớp với hàm băm anh ta tạo ra thì chữ ký là hợp lệ.

Tốc độ tăng lên đáng kể và vì khả năng hai tài liệu khác nhau có cùng 160-bit hash chỉ có 1 trong 2^160, bất kỳ ai cũng có thể đánh đồng chữ ký của hàm băm với chữ ký của tài liệu một cách an toàn. Nếu sử dụng hàm băm không một chiều,

sẽ dễ dàng tạo ra nhiều tài liệu được băm thành cùng một giá trị, do đó bất kỳ ai ký một tài liệu cụ thể sẽ bị lừa ký vào vô số tài liệu.

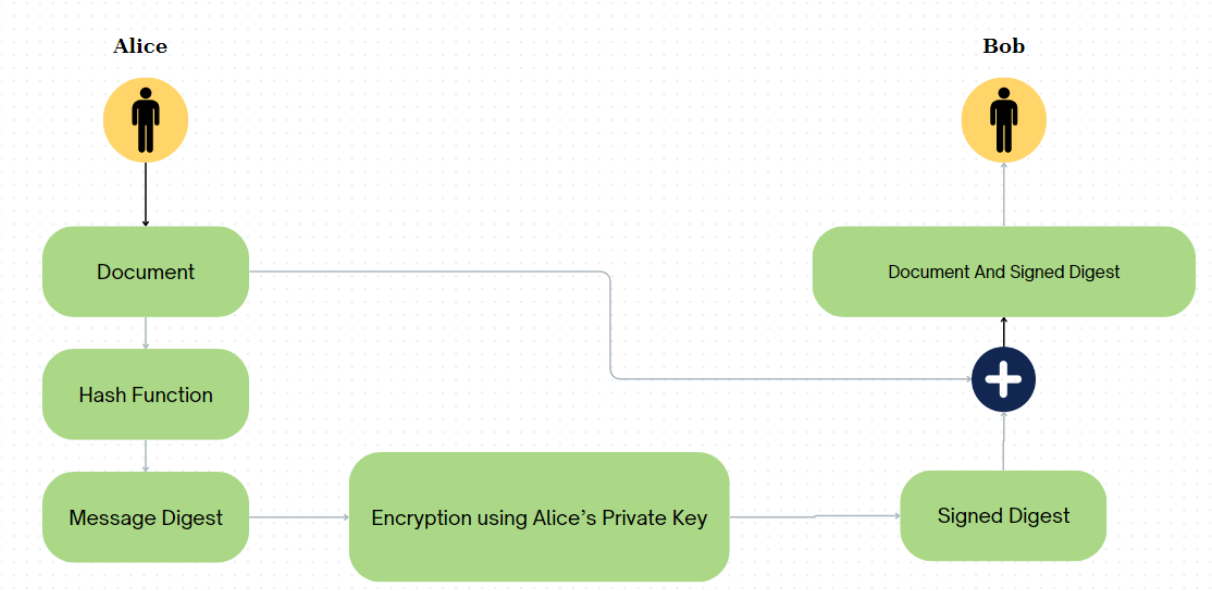

Image 2. Ký tài liệu bằng mật mã khóa công khai và hàm băm một chiều

Giao thức này có những lợi ích khác. Đầu tiên, chữ ký có thể được giữ tách biệt khỏi tài liệu. Thứ hai, yêu cầu lưu trữ tài liệu và chữ ký của người nhận nhỏ hơn nhiều. Hệ thống lưu trữ có thể sử dụng loại giao thức này để xác minh sự tồn tại của tài liệu mà không cần lưu trữ nội dung của chúng. Cơ sở dữ liệu trung tâm chỉ có thể lưu trữ các giá trị băm của tệp. Nó hoàn toàn không cần phải xem các tập tin; người dùng gửi hàm băm của họ đến cơ sở dữ liệu và cơ sở dữ liệu sẽ đánh dấu thời gian gửi và lưu trữ chúng. Nếu có bất kỳ sự bất đồng nào trong tương lai về việc ai đã tạo tài liệu và khi nào thì cơ sở dữ liệu có thể giải quyết vấn đề đó bằng cách tìm hàm băm trong các tệp của nó. Hệ thống này có ý nghĩa rất lớn liên quan đến quyền riêng tư: Alice có thể giữ bản quyền cho một tài liệu nhưng vẫn giữ bí mật tài liệu đó. Chỉ khi cô ấy muốn chứng minh bản quyền của mình thì cô ấy mới phải công khai tài liệu đó.

Nonrepudiation and Digital Signatures (Chống chối bỏ và chữ ký số)

Alice có thể gian lận bằng chữ ký điện tử và không thể làm gì được. Cô ấy có thể ký một tài liệu và sau đó khẳng định rằng cô ấy không làm vậy. Đầu tiên, cô ấy ký vào văn bản một cách bình thường. Sau đó, cô công bố khóa riêng của mình một cách ẩn danh, thuận tiện để mất nó ở nơi công cộng hoặc chỉ giả vờ làm

một trong hai điều đó. Alice sau đó tuyên bố rằng chữ ký của cô ấy đã bị xâm phạm và những người khác đang sử dụng nó, giả vờ là cô ấy. Cô ấy từ chối ký vào tài liệu và bất kỳ tài liệu nào khác mà cô ấy đã ký bằng khóa riêng đó. Điều này được gọi là sự thoái thác.

Dấu thời gian có thể hạn chế tác động của kiểu gian lận này, nhưng Alice luôn có thể khẳng định rằng chìa khóa của cô ấy đã bị xâm phạm trước đó. Nếu Alice tính toán thời gian tốt, cô ấy có thể ký một văn bản và sau đó thành công. khẳng định rằng cô ấy không làm vậy. Đây là lý do tại sao có nhiều thảo luận về khóa riêng được chứa trong các mô-đun chống giả mạo (tamper-resistant modules)—để Alice không thể lấy được khóa riêng của cô ấy và lạm dụng nó.

Mặc dù không thể làm gì trước sự lạm dụng có thể xảy ra này, nhưng người ta có thể thực hiện các bước để đảm bảo rằng chữ ký cũ không bị vô hiệu bởi các hành động được thực hiện khi tranh chấp chữ ký mới. (Ví dụ: Alice có thể "làm mất" chìa khóa của mình để không phải trả tiền cho Bob về chiếc xe cũ mà anh ấy đã bán cho cô ấy ngày hôm qua và trong quá trình đó, tài khoản ngân hàng của cô ấy bị vô hiệu hóa.) Giải pháp là người nhận tài liệu đã ký phải đóng dấu thời gian cho tài liệu đó.

2.2. Nền tảng toán học.

2.2.1. Lý thuyết độ phức tạp

Lý thuyết độ phức tạp cung cấp một phương pháp để phân tích độ phức tạp tính toán của các kỹ thuật và thuật toán mật mã khác nhau. So sánh các thuật toán và kỹ thuật mã hóa và xác định tính bảo mật của chúng. Lý thuyết thông tin cho chúng ta biết rằng tất cả các thuật toán mã hóa (ngoại trừ các miếng đệm một lần) đều có thể bị phá vỡ. Lý thuyết phức tạp cho biết liệu chúng có thể bị phá vỡ trước nhiệt độ động của vũ trụ chấm dứt hay không.

Độ phức tạp của thuật toán: Độ phức tạp của thuật toán đư ợc xác định bởi sức mạnh tính toán cần thiết để thực hiện nó. Độ phức tạp tính toán của một thuật toán thư ờng đư ợc đo bằng hai biến: T (đối với độ phức tạp về thời gian) và S (đối với độ phức tạp về không gian hoặc yêu cầu bộ nhớ). Cả T (time) và S (space)

thường được biểu diễn dưới dạng hàm của n, trong đó n là kích thư ớc của đầu vào. (Có các thư ớc đo độ phức tạp khác: số lượng bit ngẫu nhiên, băng thông truyền thông, lượng dữ liệu, v.v.

ví dụ: nếu độ phức tạp về thời gian của một thuật toán nhất định là $4n^2$+ 7n + 12 thì độ phức tạp tính toán là n^2, biểu thị O(n^2).

2.2.2. Lý thuyết số (Number Theory)

Số học module (Modular Arithmetic)

$$(10 + 13) \bmod 12 = 23 \bmod 12 = 11 \bmod 12$$

giải thích: 23 mod 12 bằng 11 tức là 23 chia 12 lấy dư được 11

Hoặc cách biểu diễn khác:

$$23 \equiv 11 \pmod{12}$$

Đối với mọi số nguyên a, phần dư module n của nó là một số nào đó nằm trong khoảng từ 0 đến n – 1. Định nghĩa mod này có thể khác với định nghĩa đư ợc sử dụng trong một số ngôn ngữ lập trình.

Ví dụ: toán tử modulo của PASCAL đôi khi trả về số âm. Nó trả về một số nằm trong khoảng -(n - 1) và n - 1. Trong C, toán tử % trả về phần còn lại từ phép chia của biểu thức đầu tiên cho biểu thức thứ hai; đây có thể là số âm nếu một trong hai toán hạng âm. Đối với tất cả các thuật toán trong cuốn sách này, hãy đảm bảo bạn thêm n vào kết quả của toán tử modulo nếu nó trả về số âm.

Số nguyên tố (Prime Numbers)

Số nguyên tố là số nguyên lớn hơn 1, chỉ có ước là 1 và chính nó: Không có số nào khác chia hết cho số đó. Hai là số nguyên tố. Tương tự là 73, 2521, 2365347734339 và 2^756839 - 1. Có vô số số nguyên tố. Mật mã, đặc biệt là mật mã khóa công khai, thường sử dụng các số nguyên tố lớn (512 bit và thậm chí lớn hơn).

Ước chung lớn nhất (Greatest Common Divisor): Hai số nguyên tố cùng nhau (co-prime) khi chúng không có ước chung nào ngoài 1. Nói cách khác, nếu ước chung lớn nhất của a và n bằng 1. Điều này được viết: gcd(a,n) = 1

Một cách để tính ước số chung lớn nhất của hai số là sử dụng thuật toán Euclid. Euclid đã mô tả thuật toán này trong cuốn sách Elements, đư ợc viết vào khoảng năm 300 trước Công nguyên. Ông không phát minh ra nó. Các nhà sử học tin rằng thuật toán này có thể có tuổi đời hơn 200 năm. Đây là thuật toán không tầm thường lâu đời nhất còn tồn tại cho đến ngày nay và nó vẫn là một thuật toán tốt. Knuth mô tả thuật toán và một số sửa đổi hiện đại.

Nghịch đảo module 1 số **(**Inverses Modulo a Number)**:** Nghịch đảo phép nhân của 4 là 1/4, vì 4*1/4 = 1. Đối với phép toán module nó sẽ phức tạp hơn:
Ví dụ: 4*x 1 ≡ (mod 7)
Phương trình trên tương đương với việc tìm x và k sao cho:
4x = 7k + 1, trong đó x và k đều là số nguyên.
Bài toán tổng quát là tìm x sao cho:
1 = (a*x) mod n
Hay còn được viết là:

$$a^{-1} \equiv x \ (mod\ n)$$

Nói chung, $a^{-1} \equiv x \ (mod\ n)$ có nghiệm duy nhất nếu a và n nguyên tố cùng nhau. Nếu a và n không nguyên tố cùng nhau thì $a^{-1} \equiv x \ (mod\ n)$ không có nghiệm. Nếu n là số nguyên tố thì mọi số từ 1 đến n-1 đều là số nguyên tố cùng nhau với n và có đúng một modulo n nghịch đảo trong phạm vi đó.

Tạo số nguyên tố: Thuật toán khóa công khai cần số nguyên tố. Việc phân tích các số nguyên tố lớn rất khó nhưng tạo ra lại rất đơn giản. Điều đặc biệt ở đây là đi tìm câu trả lời một số n có phải là số nguyên tố hay không? Tìm câu hỏi n có phải là số nguyên tố hay không dễ hơn câu hỏi phân tích các thừa số nguyên tố của n.

2.3. Thuật toán chữ ký số.

Thuật toán chữ ký số (DSA) là biến thể của thuật toán chữ ký Schnorr và ElGamal. Thuật toán sử dụng các tham số sau:
p: tham số là một số nguyên tố dài L bit (L từ 512 bit đến 1024 hoặc có thể đến 2048 bit (theo tiêu chuẩn của NIST), và L là bội số của 64.)

q: là một thừa số nguyên tố 160 bit của p – 1

g: là tham số được tính theo công thức sau:

$$g = h^{(p-1)/q} \bmod p$$

trong đó h là một số bất kỳ nhỏ hơn (p – 1) mà sao cho: $h^{(p-1)/q} \bmod p > 1$

Sau đó private key và public key sẽ được tạo ra như sau:

Private key là x: là một số nguyên nhỏ hơn q

Public key là y được tính theo công thức:

$$y = g^x \bmod p$$

Thuật toán cũng sử dùng hàm băm một chiều H(m).

Đề ký tài liệu m, Alice sẽ làm như sau:

Alice tạo ra một số ngẫu nhiên k nhỏ hơn q.

Alice tạo ra r, s theo công thức:

$$r = (g^k \bmod p) \bmod q$$

$$s = \left(k^{-1}(H(m) + x * r)\right) \bmod q$$

Các tham số r và s là chữ ký của Alice; Alice gửi những thứ này (tài liệu và chữ ký) cho Bob.

Để xác minh chữ ký của Alice, Bob cần tính các tham số w, u_1, u_2, v :

$$w = s^{-1} \bmod q$$

$$u_1 = (H(m) * w) \bmod q$$

$$u_2 = (r * w) \bmod q$$

$$v = ((g^{u_1} * y^{u_2}) \bmod p) \bmod q$$

Nếu v = r thì chữ ký được xác minh.

2.4. Xây dựng chương trình mô phỏng thuật toán.

Thủ tục kiểm tra số nguyên tố:

Vào: số nguyên n

Ra: n có phải số nguyên tố ? (True hoặc False)

```
def is_prime(n):
    if n < 2 then return False
```

```
        # tính toán phạm vi lặp để kiểm tra
        scope = int(math.sqrt(n) + 1)
        for i in range(2,scope):
                if n % i == 0 then return False
        <nếu không thì nó là số nguyên tố>
        return True
```

Thủ tục tạo số nguyên tố:

```
def generate_prime(min_value, max_value):
        prime_number = random.randrange(min_value, max_value)
        # trong khi không phải số nguyên tố thì random lại
        while cho đến khi nó là số nguyên tố:
                prime_number = random.randrange(min_value, max_value)
        return prime_number
```

Thủ tục tịm nghịch đảo module (mod inverse)

```
def mod_inverse(a,b):
        # (a * x) % b = 1
        for i in range(1,b):
                if (a * i) % b == 1 then return i
        < không tìm được kết quả>
        return -1
```

Thủ tục hash_message (hast tài liệu)

```
def hash_message(message):
        hash_value = message truyền vào hash function
        return hash_value
```

Thủ tục tìm tham số h:

```
def find_h_parameter(p,q):
        # tham số p, q được sử dụng trong công thức tham số g
        for h in range(1,p-1):
```

```
            if pow(h, (p-1)//q, p) > 1 then return h
        <không tìm được kết quả>
        return -1
```

Thủ tục tạo các tham số p,q,g

```
def generate_parameter():
        q = generate_prime(1000, 5000)
        p = generate_prime(1000, 60000)
        while cho đến khi p – 1 chia hết cho q:
                p = generate_prime(1000, 60000)
        h = find_h_parameter(p, q)
        g = pow(h, (p-1)//q, p)
        return p, q, g
```

Thủ tục tạo cặp Private key và Public key:

```
def generate_key_pair():
        p, q, g = generate_parameter()
        # Private key: x ; Public key: y
        x = random giá trị nhỏ hơn q
        y = g**x mod p
        return 1 bộ tham số chứa x, 1 bộ tham số chứa y
```

Thuật toán ký:

Lưu đồ thuật toán ký tài liệu:

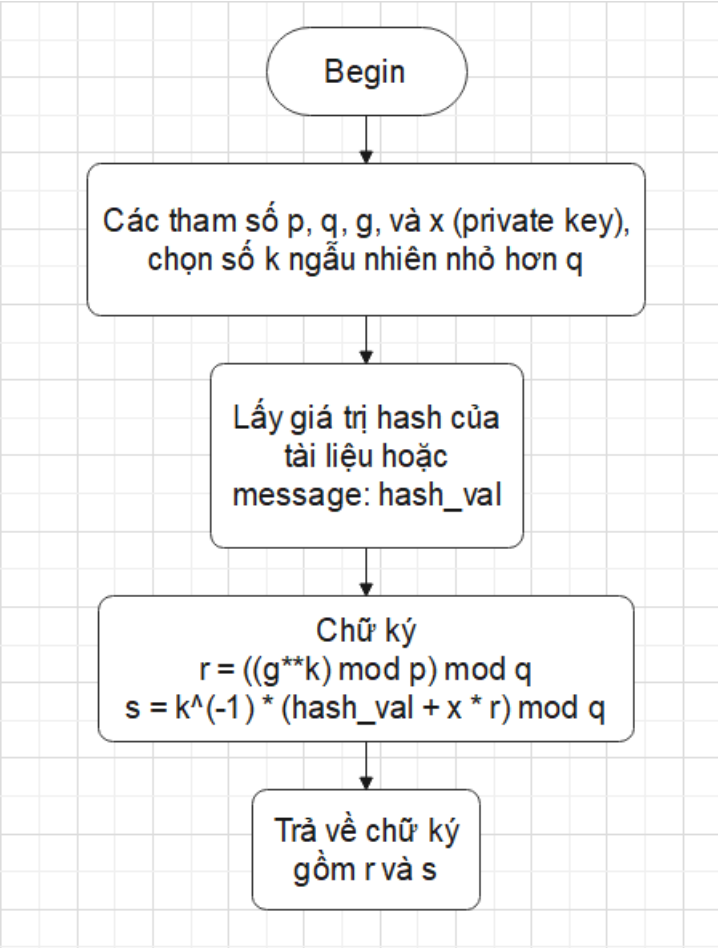

Image 3. Lưu đồ thuật toán quá trình ký tài liệu

Thủ tục ký tài liệu hoặc message:

def signature(message, private_key):

p, q, g, x = giải nén các tham số từ bộ private key trả về

hash_val = hash_message(message)

k = random giá trị số nguyên nhỏ hơn q

ký tài liệu

r = ((pow(g,k) mod p) mod q

s = (mod_inverse(k,q) * (hash_val + x * r) mod q

trả về chữ ký gồm r, s

Thuật toán xác minh chữ ký:

Lưu đồ thuật toán xác minh chữ ký:

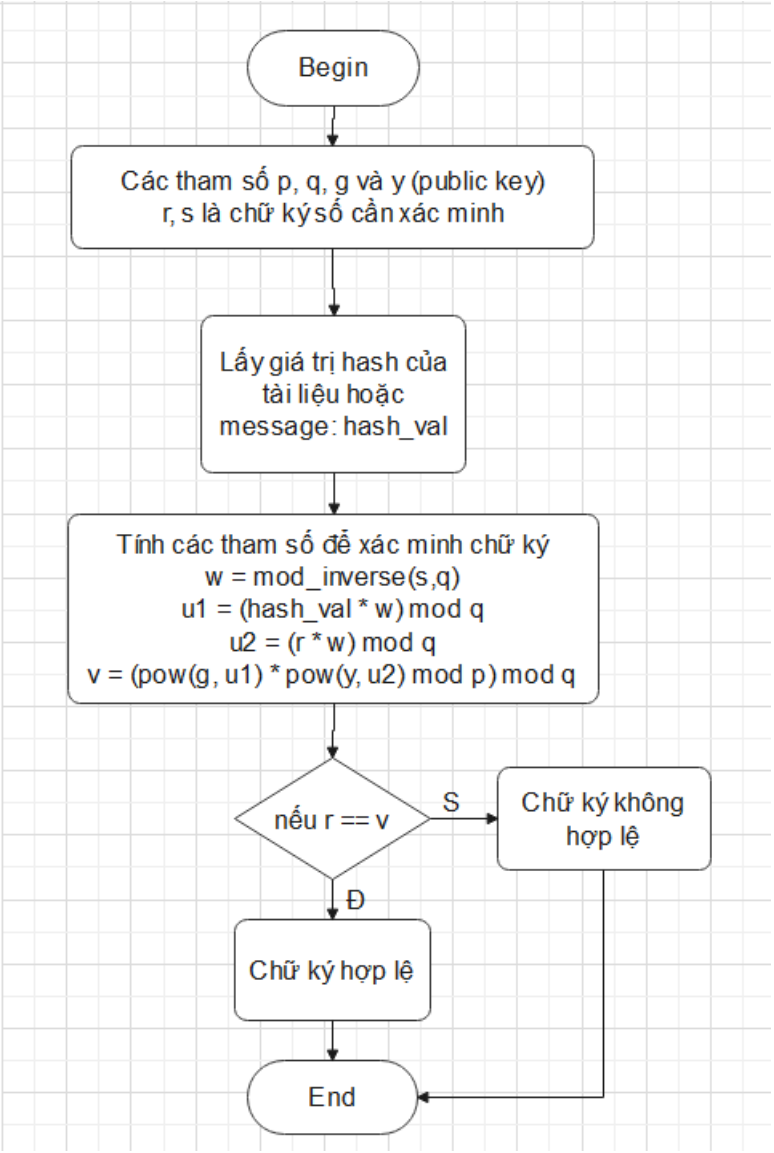

Image 4. Lưu đồ thuật toán xác minh chữ ký

Thủ tục xác minh chữ ký:

```
def vefiry(message, sign, public_key):
        p, q, g, y  = giải nén từ public key
        r, s = giải nén từ chữ ký
        hash_val = hash_message(message)
        w = mod_inverse(s, q)
        u1 =  (hash_val * w) mod q
        u2 = (r * w) mod q
        v = (pow(g,u1) * pow(y, u2) mod p) mod q
        if r == v then return True
        <nếu xác minh chữ ký không thành công> return False
```

CHƯƠNG 3. MÔ PHỎNG VÀ ĐÁNH GIÁ

3.1. Mô phỏng thuật toán.

Ví dụ với các tham số p = 27191, q = 2719, h = 2

g = $h^{(p-1)/q}$ mod p = 4096 mod 45853 = 1024

x chọn ngẫu nhiên nhỏ hơn q: chọn x = 892

y = $g^x \ mod \ p$ = 111

Ví dụ đoạn tài liệu có giá trị hash value là:

5767641308109300314800510755071958354011698523669642386092346649

0497932824681

Chọn k ngẫu nhiên bằng 1742.

Khi đó tính được r = 2054, s = 25

Khi xác minh:

w = 2284, u1 = 1542, u2 = 1061, v = 2054

Chương trình hoạt động đúng. Chương trình mã nguồn python tại file main.py.

3.2. Đánh giá:

3.2.1. Đánh giá độ phức tạp:

Tìm số nguyên tố (generate_prime): Trong hàm này, chúng ta sử dụng thuật toán kiểm tra số nguyên tố và thực hiện việc tạo số nguyên tố trong một khoảng cho trước. Độ phức tạp của việc kiểm tra số nguyên tố thường là O(sqrt(n)), và quá trình tạo số nguyên tố có thể lặp lại nhiều lần. Do đó, độ phức tạp có thể được mô tả là O(k * sqrt(n)), với k là số lần lặp và n là giới hạn trên của số nguyên tố.

Tìm h (find_h_parameter): Trong hàm này, chúng ta duyệt qua các giá trị của h để tìm giá trị thích hợp. Độ phức tạp của hàm này phụ thuộc vào giá trị của p và q. Trong trường hợp tồi nhất, nó có thể là O(p). Tuy nhiên, nếu p và q có kích thước lớn, độ phức tạp có thể được xấp xỉ là O(1).

Tìm mod inverse (mod_inverse): Trong hàm này, chúng ta sử dụng thuật toán mở rộng Euclid để tìm modular inverse. Độ phức tạp của thuật toán Euclid mở rộng là O(log(min(a, b))), với a và b là hai số đầu vào. Trong trường hợp của bạn, nó sẽ phụ thuộc vào giá trị của s và q.

Tạo khóa và chữ ký (generate_key_pair, signature): Cả hai hàm này đều thực hiện các phép toán số học (lũy thừa, modular inverse, vv.) và có độ phức tạp phụ thuộc vào kích thước của các số nguyên lớn (p, q, g, x, y).

Xác minh (verify): Hàm này thực hiện một số phép toán và có độ phức tạp phụ thuộc vào kích thước của các số nguyên lớn và kích thước của bản tin.

Tổng cộng, độ phức tạp của bài toán sẽ phụ thuộc vào các yếu tố như kích thước của các số nguyên lớn, số lần lặp trong việc tìm số nguyên tố, và độ phức tạp của thuật toán mở rộng Euclid. Độ phức tạp thời gian và không gian của mã này có thể được xấp xỉ là O(k * sqrt(n) + log(min(s, q))) với k là số lần lặp, n là giới hạn trên của số nguyên tố, và s là một số trong các phép toán modular.

3.2.2. Đánh giá bảo mật của thuật toán chữ ký số (DSA):

Bảo mật của DSA: Ở 512 bit, DSA không đủ mạnh để bảo mật lâu dài. DSS không mã hóa bất kỳ dữ liệu nào. Vấn đề thực sự là liệu DSS có dễ bị ai đó giả mạo chữ ký và do đó làm mất uy tín của toàn bộ hệ thống hay không. Khẳng định rõ ràng rằng khả năng bất kỳ ai - giả mạo chữ ký với DSS (tiêu chuẩn chữ ký số - Digital Signature Standard) khi nó được sử dụng và triển khai hợp lý là cực kỳ nhỏ.

Độ An toàn của Số Nguyên Tố p và q:

- p là số nguyên tố: An toàn của DSA dựa chủ yếu vào sự khó khăn của việc phân tích ngược modulo một số nguyên tố lớn p. Việc chọn một số nguyên tố p đủ lớn là quan trọng để ngăn chặn các tấn công brute-force.
- q là một nguyên tố con của (p-1): Việc chọn q đảm bảo rằng số nguyên tố con q là một nhóm nhỏ hơn của độ lớn của p, làm tăng tính an toàn.

Chọn Giá trị g:

- Sự Ngẫu nhiên và An toàn của g: Giá trị g được chọn để đảm bảo rằng nó tạo ra một nhóm có tính ngẫu nhiên và không dễ dàng bị dự đoán. Sự ngẫu nhiên trong giá trị g là quan trọng để ngăn chặn các tấn công phân tích thuật toán.

Độ Ngẫu nhiên của Khóa Riêng (x) và Khóa Công khai (y):

- Khóa Riêng x: Độ ngẫu nhiên của khóa riêng đảm bảo rằng việc dự đoán giá trị của nó là không khả thi. Việc sử dụng một hàm ngẫu nhiên mạnh để tạo khóa riêng là quan trọng.
- Khóa Công khai y: Sự an toàn của khóa công khai phụ thuộc vào tính an toàn của hàm modulo và không thể giải ngược.

Chống tấn công brute-force:

- Sự khó khăn của Tìm Kiếm ngược: Tính an toàn của DSA phụ thuộc vào việc tìm kiếm ngược giá trị của r từ chữ ký và thông điệp đã biết. Nếu việc này trở nên dễ dàng, tính toàn vẹn của hệ thống chữ ký sẽ bị đe dọa.

Kích thước Khóa:

- Độ Dài của Khóa: Kích thước của p và q cũng như độ dài của các khóa riêng và công khai ảnh hưởng đến độ an toàn của DSA. Kích thước khóa lớn hơn sẽ làm cho việc tìm kiếm ngược và các tấn công brute-force trở nên khó khăn hơn.

Sự Hiệu suất:

- Hiệu suất của Thuật toán: Tính hiệu suất của DSA cũng là một yếu tố quan trọng, đặc biệt là đối với các ứng dụng yêu cầu tính toàn vẹn và xác thực cao như trong giao thức mạng.

Tấn công vào k: Mỗi chữ ký yêu cầu một giá trị mới là k và giá trị đó phải được chọn ngẫu nhiên. Nếu Eve khôi phục được k mà Alice dùng để ký một tin nhắn, có lẽ bằng cách khai thác một số thuộc tính của bộ tạo số ngẫu nhiên tạo ra k, cô ấy có thể khôi phục khóa riêng của Alice, x. Nếu Eve nhận được hai tin nhắn được ký bằng cùng một k, ngay cả khi cô ấy không biết đó là gì, cô ấy vẫn có thể khôi phục x. Và với x, Eve có thể tạo ra những chữ ký giả mạo của Alice mà không thể phát hiện được. Trong bất kỳ triển khai DSA nào, một bộ tạo số ngẫu nhiên tốt là điều cần thiết cho tính bảo mật của hệ thống.

3.3. Kết luận

Trong bối cảnh hiện nay, sự phát triển nhanh chóng của thương mại điện tử đã tạo ra môi trường kinh doanh trực tuyến phức tạp và đầy thách thức. Đồng thời,

việc đảm bảo an toàn và bảo mật thông tin trong giao dịch trực tuyến trở thành một yếu tố quyết định đối với sự tin tưởng của người tiêu dùng và doanh nghiệp. Đề tài "Chữ ký số và ứng dụng trong thương mại điện tử" đã tập trung vào việc nghiên cứu và hiểu rõ vai trò của chữ ký số trong việc đảm bảo tính toàn vẹn và xác thực thông tin, đồng thời thấu hiểu về ứng dụng thực tế của nó trong môi trường thương mại điện tử.

Nhóm 7 đã xác định rằng chữ ký số không chỉ đơn giản là một công cụ bảo mật, mà còn đóng vai trò quan trọng trong việc tạo ra một hệ thống thương mại điện tử an toàn và tin cậy. Các lợi ích chủ yếu bao gồm khả năng ngăn chặn các tấn công như thay đổi thông tin giao dịch và xác minh danh tính của các bên tham gia.

Việc thực hiện chữ ký số trong thương mại điện tử đã giúp tăng cường tính an toàn và toàn vẹn của thông tin, đặt nền móng cho một môi trường kinh doanh trực tuyến minh bạch và tin cậy. Nhóm 7 đã nhìn nhận những thách thức cần vượt qua như quản lý khóa và vấn đề liên quan đến quyền riêng tư. Điều này đặt ra yêu cầu cho việc triển khai các biện pháp an ninh hiệu quả và quản lý khóa chặt chẽ.

Trong tương lai, nhận thức về tính quan trọng của chữ ký số và các công nghệ bảo mật liên quan sẽ ngày càng tăng cao. Các doanh nghiệp cần nắm bắt và áp dụng những tiến bộ này để không chỉ đảm bảo sự an toàn cho dữ liệu của họ mà còn tạo ra sự tin tưởng từ phía khách hàng.

Kết luận, đề tài đã làm rõ vai trò to lớn và đặc biệt của chữ ký số trong môi trường thương mại điện tử và đề xuất sự cần thiết của việc đầu tư trong an toàn và bảo mật thông tin để bảo vệ sự tin tưởng và tính minh bạch trong thương mại điện tử hiện đại. Cũng như nhóm đã đạt được các mục tiêu đề ra ban đầu.

TÀI LIỆU THAM KHẢO

[1]. Bruce Schneiner, *Applied Cryptography: Protocols, Algorithms and Source Code in C* , NXB Wiley, 1996

[2]. NIST (2013), Tiêu chuẩn chữ ký số, từ *https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.186-4.pdf*

[3]. Thư viện hashlib python, từ *https://docs.python.org/3.10/library/hashlib.html*

PHỤ LỤC

Hướng dẫn sử dụng chương trình:

Chương trình mô phỏng thuật toán chữ ký số tại file Demo_Nhom7.py:

Để chạy chương trình, di chuyển đến thư mục chứa file Demo_Nhom7.py trên cmd của window bằng lệnh cd, sau đó chạy lệnh py Demo_Nhom7.py.

Có thể thay đổi các cặp private key, public key để kiểm tra chức năng xác minh chữ ký của chương trình.