

**BỘ CÔNG THƯƠNG**

**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**

**BÁO CÁO ĐỀ ÁN MÔN HỌC**  

ĐỀ TÀI NGHIÊN CỨU:

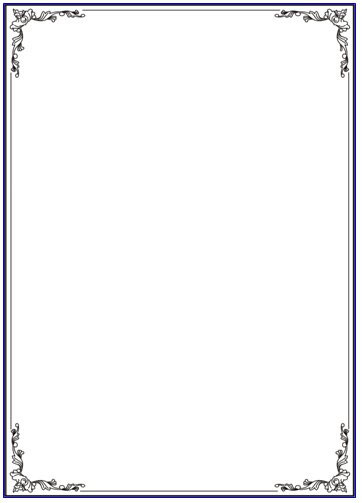
**CHỮ KÝ SỐ VÀ ỨNG DỤNG**

**TRONG**

**THƯƠNG MẠI ĐIỆN TỬ**

Giảng viên hướng dẫn: TS. Lê Thị Anh

Hà Nội, 12/2023



**BỘ CÔNG THƯƠNG**

**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**

**BÁO CÁO ĐỀ ÁN MÔN HỌC**  

An toàn bảo mật thông tin

ĐỀ TÀI NGHIÊN CỨU:

**“CHỮ KÝ SỐ VÀ ỨNG DỤNG TRONG THƯƠNG MẠI ĐIỆN TỬ ”**

Giảng viên hướng dẫn: TS. Lê Thị Anh

Sinh viên thực hiện:

Phùng Thị Lan Anh 2021DHDLKD01 - K16 - Khoa KTKT

Hồ Thủy Linh 2021DHDLKD01 - K16 - Khoa KTKT

Nguyễn Phương Linh 2021DHDLKD01 - K16 - Khoa KTKT

Trần Thị Thanh Thảo 2021DHDLKD01 - K16 - Khoa KTKT

Hoảng Văn Trúc 2021DHDLKD01 - K16 - Khoa KTKT

Hà Nội, 12/2023

**MỤC LỤC**

[**DANH MỤC TỪ VIẾT TẮT 3**](#_13410evcy404)

[**DANH MỤC BẢNG BIỂU 4**](#_nsxd0fbl50z8)

[**LỜI CẢM ƠN 5**](#_qn8pakjakboy)

[**LỜI MỞ ĐẦU 6**](#_lmtxpg910ums)

[**CHƯƠNG 1: TỔNG QUAN CHUNG 7**](#_eop9ygdrp5ea)

[1.1 Giới thiệu 7](#_o12wre7ho8kg)

[1.1.1 Lý do nghiên cứu 7](#_trfta7ujfwyo)

[1.1.2 Mục tiêu nghiên cứu 8](#_rdwvhcd8ipqi)

[1.1.3 Ý nghĩa và sự cần thiết của chữ ký số trong thương mại điện tử 8](#_txv2uljhcwt9)

[1.2 Cơ sở lý thuyết 9](#_gbfvn2hq46uh)

[1.2.1 Về thương mại điện tử 9](#_j7mtld3wls5)

[1.2.2 Về chữ ký số 10](#_how7sdsfr967)

[1.2.3 Tầm quan trọng của chữ ký số trong bảo mật thông tin 13](#_kq9g6iyrlw24)

[**CHƯƠNG 2: KỸ THUẬT SỬ DỤNG 14**](#_rcjt8wwf0ah5)

[2.1 Mã hóa thông tin và mật mã khóa công khai 14](#_nsjgw6k13lcc)

[2.1.1 Mã hóa thông tin 14](#_lsr148fzmfgc)

[2.1.2 Mật mã khóa công khai 15](#_9s5h78c157vo)

[2.2 Hàm băm 15](#_5ydq573wqlo4)

[2.2.1 Sơ lược về hàm băm 15](#_48tj13lr4uvj)

[2.2.2 Sử dụng hàm băm trong chữ ký số 16](#_nnoi52b92s21)

[2.2.3 Hàm băm SHA-256 17](#_gnuxjaynrukz)

[2.3 Sơ đồ chữ ký số RSA 18](#_gjz7idtkeoic)

[2.3.1 Thuật toán sinh khóa và sinh chữ ký số 18](#_vngwhn43asl2)

[2.3.2 Thuật toán xác nhận chữ ký 19](#_gjqtunbmcyu4)

[2.3.3 Độ an toàn của sơ đồ chữ ký số RSA 20](#_vjer4ljamyqi)

[2.4 Cơ sở hạ tầng khóa công khai (PKI) 21](#_1i9djznzvttw)

[2.4.1 Khái niệm 21](#_hy4kj2z4euk7)

[2.4.2 Nguyên tắc hoạt động của cơ sở hạ tầng khóa công khai 22](#_c7rfci56svgv)

[2.4.3 Cấu trúc phân tầng của hệ thống PKI 24](#_yxo05ftupj7l)

[2.5 Cấp phát và xác thực chữ ký số 25](#_f591axjecidu)

[2.5.1 Chứng thực số 25](#_i9f0p4e1zmjd)

[2.5.2 Cấp phát chữ ký số 26](#_x8mzq7ux0ltf)

[2.5.3 Xác thực chữ ký số 27](#_xps07auiwcj1)

[**CHƯƠNG 3: ỨNG DỤNG VÀ DEMO 28**](#_kw59pq6xdjpk)

[3.1 Ứng dụng của chữ ký số trong thương mại điện tử 28](#_vb0lvlmyfr30)

[3.1.1 Mã hóa và bảo mật 28](#_62ivwn5q3tiz)

[3.1.2 Chứng thực người dùng 28](#_gmmkl19m055p)

[3.1.3 Bảo Mật Giao Dịch Trực Tuyến 28](#_f7knflfl8yqq)

[3.1.4 Đăng Nhập An Toàn và Quản Lý Người Dùng 29](#_uyrs6himjeim)

[3.1.5 Bảo Mật Dữ Liệu và Lưu Trữ 30](#_k026lek51da)

[3.2 Demo “Tạo và xác thực chữ ký số” bằng Python 30](#_im2bj46ct39g)

[3.3 Thảo luận kết quả 34](#_k839gwt5gepn)

[3.3.1 So sánh và đánh giá phương pháp thuật toán chữ ký số trong thương mại điện tử 34](#_o06pow63rsr7)

[3.3.2 Đề xuất cải tiến và hướng phát triển trong tương lai 36](#_moevdh81eiz9)

[3.3.3 Một số giải pháp cụ thể có thể được áp dụng 36](#_d1kd1s11vj8n)

[**KẾT LUẬN 37**](#_s87we2cvitsh)

[**TÀI LIỆU THAM KHẢO 38**](#_e3i13gjoa3ev)

# 

# **DANH MỤC TỪ VIẾT TẮT, TIẾNG ANH**

|  |  |  |
| --- | --- | --- |
| STT | TỪ VIẾT TẮT | ĐỊNH NGHĨA |
| 1 | TMĐT | Thương mại điện tử |
| 2 | RSA | Hệ mật mã khóa công khai |
| 3 | PKI | Public Key Infrastructure: Hệ thống khóa công khai |
| 4 | CA | Certificate Authority: Nhà cung cấp chứng thực số |
| 5 | public key | Khóa công khai |
| 6 | private key | Khóa bí mật |
| 7 | server | Máy chủ |
| 8 | client | Khách hàng |
| 9 | hash function | Hàm băm |
| 10 | Credit-Card | Thẻ ngân hàng |
| 11 | SHA-256 | Secure Hash Algorithm 256 Bit: thuật toán băm 256 bit |
| 12 | ID | Identification - nhận dạng |
| 13 | PEM | Privacy Enhanced Mail: Thư nâng cao quyền riêng tư |
| 14 | PSS | Probabilistic Signature Scheme: Sơ đồ chữ ký |
| 15 | UTF-8 | 8-bit Unicode Transformation Format: Định dạng chuyển đổi Unicode 8-bit |

# 

# **DANH MỤC HÌNH ẢNH**

|  |  |  |
| --- | --- | --- |
| HÌNH | TÊN HÌNH | TRANG |
| Hình 1: | Sơ đồ thể hiện quá trình tạo chữ ký số | 13 |
| Hình 2: | Ví dụ về hàm băm | 17 |
| Hình 3: | Thuật toán hàm băm SHA-256 | 19 |
| Hình 4: | Quá trình sinh chữ ký số | 20 |
| Hình 5: | Quá trình xác thực chữ ký số | 21 |
| Hình 6: | Quá trình xây dựng một hệ thống PKI | 23 |
| Hình 7: | Mô tả quá trình tạo và kiểm tra chữ ký số | 25 |
| Hình 8: | Cấu trúc của một hệ thống PKI | 25 |
| Hình 9: | Hàm generate\_key\_pair() | 32 |
| Hình 10: | Hàm sign\_message() | 33 |
| Hình 11: | Hàm verify\_signature() | 34 |
| Hình 12: | Quy trình thực hiện | 35 |

# **LỜI CẢM ƠN**

Lời đầu tiên, nhóm tác giả xin trân trọng cảm ơn tới sự giúp đỡ tới các tập thể, các cá nhân trong và ngoài nhà trường đã tạo điều kiện cho nhóm trong quá trình học tập và thực hiện đề tài.

Trước hết, nhóm tác giả xin được bày tỏ lòng biết ơn sâu sắc tới TS. Lê Thị Anh đã tận tình chỉ bảo và hướng dẫn nhóm trong suốt khoảng thời gian thực hiện đề tài. Không có sự nhiệt huyết và những lời góp ý hữu ích của Cô, nhóm tác giả sẽ không thể hoàn thành đề tài trong thời gian có hạn. Nhóm tác giả mong rằng sẽ có thêm cơ hội được làm việc với Cô trong thời gian tới.

Bên cạnh đó, nhóm tác giả xin gửi lời cảm ơn đến người thân, bạn bè và Quý thầy cô, Giảng viên Trường Đại học Công nghiệp Hà Nội đã luôn ủng hộ, giúp đỡ và tạo điều kiện tốt nhất để nhóm tác giả có điều kiện tham gia nghiên cứu và hoàn thiện đề tài.

Nhóm tác giả xin trận trọng cảm ơn!

# **LỜI MỞ ĐẦU**

Hiện nay, ở tất cả các nước phát triển cũng như đang phát triển, mạng máy tính đang ngày càng đóng vai trò thiết yếu trong mọi lĩnh vực hoạt động của toàn xã hội, và một khi nó trở thành phương tiện điều hành các hệ thống thì nhu cầu bảo mật thông tin được đặt lên hàng đầu. Nhu cầu này không chỉ có ở các bộ máy an ninh, quốc phòng, quản lý nhà nước,…mà đã trở thành bức thiết trong nhiều hoạt động kinh tế xã hội: tài chính, ngân hàng, thương mại điện tử,…và thậm chí trong cả một số hoạt động thường ngày của người dân (thư điện tử, thanh toán, tín dụng,…).

Vấn đề bảo mật đang được nhiều người tập trung nghiên cứu và tìm mọi giải pháp để đảm bảo an toàn, an ninh cho hệ thống phần mềm, đặc biệt là các hệ thống thông tin trên mạng.

Ứng dụng mã hóa và bảo mật thông tin trong các hệ thống thương mại điện tử, giao dịch chứng khoán,… đã trở nên phổ biến trên thế giới và sẽ ngày càng trở nên quen thuộc với người Việt Nam. Tháng 7/2000, thị trường chứng khoán lần đầu tiên được hình thành tại Việt Nam; các thẻ tín dụng bắt đầu được sử dụng, các ứng dụng hệ thống thương mại điện tử đang ở bước đầu được quan tâm và xây dựng. Do đó, nhu cầu về các ứng dụng mã hóa và bảo mật thông tin trở nên rất cần thiết.

Chính vì những vấn đề thực tiễn trên, bài viết với đề tài: “Ứng dụng Chữ ký số trong thương mại điện tử” sẽ tập trung nghiên cứu một trong những phương pháp bảo vệ an toàn dữ liệu có tính an toàn cao nhất hiện nay là hệ mật mã có khóa công khai RSA, chữ ký số, chứng thực chữ ký số, công nghệ bảo mật sử dụng cho thương mại điện tử,…

# **CHƯƠNG 1: TỔNG QUAN CHUNG**

## 1.1 Giới thiệu

### 1.1.1 Lý do nghiên cứu

Thương mại điện tử (TMĐT) đang phát triển mạnh mẽ trên thế giới và Việt Nam. Theo thống kê của Hiệp hội Thương mại điện tử Việt Nam (VECOM), năm 2022, tổng mức bán lẻ qua TMĐT đạt 150,000 tỷ đồng, tăng 25,6% so với năm 2021. Trong đó, doanh số bán lẻ qua sàn thương mại điện tử đạt 112,000 tỷ đồng, tăng 29,6% so với năm 2021.

Sự phát triển của TMĐT kéo theo nhu cầu sử dụng chữ ký số ngày càng tăng. Chữ ký số là một dạng chữ ký điện tử được tạo ra bằng các kỹ thuật mật mã học, có giá trị pháp lý tương đương với chữ ký tay. Chữ ký số được sử dụng để xác thực danh tính của người ký, đảm bảo tính toàn vẹn và không thể chối bỏ của dữ liệu được ký.

Việc ứng dụng chữ ký số trong TMĐT mang lại nhiều lợi ích cho các bên tham gia giao dịch, bao gồm:

* Tiết kiệm chi phí, thời gian và công sức: Chữ ký số giúp các bên tham gia giao dịch không cần phải in ấn, ký tay và gửi các văn bản giấy qua đường bưu điện. Điều này giúp tiết kiệm chi phí in ấn, vận chuyển, lưu trữ và bảo quản hồ sơ.
* Nâng cao hiệu quả và tính chuyên nghiệp: Chữ ký số giúp các giao dịch điện tử diễn ra nhanh chóng, thuận tiện và an toàn hơn. Điều này góp phần nâng cao hiệu quả và tính chuyên nghiệp trong hoạt động TMĐT.
* Giảm thiểu rủi ro gian lận: Chữ ký số giúp đảm bảo tính toàn vẹn và không thể chối bỏ của dữ liệu được ký. Điều này giúp giảm thiểu rủi ro gian lận trong các giao dịch điện tử.

Ta có thể thấy việc nghiên cứu "Chữ ký số và ứng dụng của chữ ký số trong thương mại điện tử" là cần thiết và có ý nghĩa thực tiễn. Nghiên cứu về chữ ký số và ứng dụng của chúng trong thương mại điện tử trở thành một hành trình quan trọng để khám phá và áp dụng kiến thức để giải quyết các thách thức bảo mật và xác thực trong môi trường trực tuyến ngày nay.

### 1.1.2 Mục tiêu nghiên cứu

Đề tài tập trung tìm hiểu cơ sở toán học của lý thuyết mật mã, thuật toán và độ phức tạp của hệ mật mã có khoá công khai RSA, hàm băm mật mã, các vấn đề về chứng thực thông qua sơ đồ chữ ký RSA. Ngoài ra, đề tài trình bày và xây dựng kỹ thuật ứng dụng trong việc chứng thực chữ ký số, và ứng dụng chữ ký số trong thương mại điện tử .

### 1.1.3 Ý nghĩa và sự cần thiết của chữ ký số trong thương mại điện tử

Nhằm giải quyết vấn đề bảo mật an toàn cho các giao dịch thanh toán điện tử, đã có rất nhiều các giải pháp được đưa ra và đều xoay quanh việc mã hóa văn bản và chữ ký số là một trong số những giải pháp đó. Chữ ký số là công nghệ xác thực, đảm bảo an ninh, an toàn cho các giao dịch trong môi trường Internet, giúp chúng ta giải quyết vấn đề về toàn vẹn dữ liệu, là bằng chứng để ngăn chặn việc chối bỏ trách nhiệm trên nội dung đã ký, giúp các doanh nghiệp, tổ chức, cá nhân có thể yên tâm với các giao dịch thanh toán của mình trong môi trường Internet.

Chữ ký số RSA là một thuật toán mã hóa bất đối xứng được sử dụng rộng rãi trong thương mại điện tử để đảm bảo tính xác thực, toàn vẹn và không chối bỏ của các giao dịch điện tử. Chữ ký số RSA là một công nghệ quan trọng giúp đảm bảo an toàn cho các giao dịch thương mại điện tử. Việc ứng dụng chữ ký số RSA trong thương mại điện tử đang ngày càng trở nên phổ biến và cần thiết.

Chữ ký số RSA hỗ trợ xác thực danh tính người tham gia giao dịch, đảm bảo giao dịch được thực hiện bởi chính người đó, người ký không thể chối bỏ việc ký tài liệu. Bên cạnh đó, chữ ký số còn chứng thực tính nguyên vẹn của tài liệu, đảm bảo tài liệu không thay đổi sau khi thực hiện. Cụ thể, chữ ký số RSA được ứng dụng trong các giao dịch thương mại điện tử sau:

* Giao dịch mua sắm trực tuyến: Chữ ký số RSA được sử dụng để xác thực danh tính của người mua và đảm bảo tính nguyên vẹn của đơn hàng.
* Thanh toán điện tử: Chữ ký số RSA được sử dụng để xác thực danh tính của người mua và đảm bảo tính an toàn của giao dịch thanh toán.
* Hợp đồng điện tử: Chữ ký số RSA được sử dụng để chứng thực tính nguyên vẹn của hợp đồng và đảm bảo tính ràng buộc của hợp đồng.
* Cấp chứng chỉ điện tử: Chữ ký số RSA được sử dụng để xác thực danh tính của người được cấp chứng chỉ điện tử.

Việc ứng dụng chữ ký số RSA trong thương mại điện tử mang lại nhiều lợi ích cho cả người mua, người bán và các cơ quan quản lý, bao gồm:

* Tăng cường bảo mật: giúp bảo vệ thông tin cá nhân, thông tin tài chính và các thông tin nhạy cảm khác của người mua, người bán và các cơ quan quản lý.
* Tăng cường tính minh bạch: giúp tăng cường tính minh bạch của các giao dịch thương mại điện tử, giúp người mua và người bán dễ dàng kiểm tra tính xác thực và tính toàn vẹn của các giao dịch.
* Tăng cường hiệu quả: giúp đơn giản hóa các thủ tục giao dịch thương mại điện tử, giúp các giao dịch được thực hiện nhanh chóng và dễ dàng hơn.

## 1.2 Cơ sở lý thuyết

### 1.2.1 Về thương mại điện tử

*Khái niệm thương mại điện tử*

Thương mại điện tử được biết đến với nhiều tên gọi khác nhau như "thương mại điện tử" (Electronic commerce), "thương mại trực tuyến" (Online trade), "thương mại không giấy tờ" (Paperless commerce) hoặc "kinh doanh điện tử" (E-business). Tuy nhiên, "thương mại điện tử" vẫn là tên gọi phổ biến nhất và được dùng thống nhất trong các văn bản hay công trình nghiên cứu của các tổ chức hay các nhà nghiên cứu. Thương mại điện tử bắt đầu bằng việc mua bán hàng hóa và dịch vụ thông qua các phương tiện điện tử và mạng viễn thông, các doanh nghiệp tiến tới ứng dụng công nghệ thông tin vào mọi hoạt động của mình, từ bán hàng, marketing, thanh toán đến mua sắm, đào tạo, phối hợp hoạt động với nhà cung cấp, đối tác, khách hàng,...

*Giao dịch trong thương mại điện tử và những nguy cơ mất an toàn thông tin*

Giữa giao dịch thương mại truyền thống và giao dịch TMĐT có nhiều điểm khác biệt cơ bản trong việc nhận và chuyển tải thông tin giữa các bên tham gia giao dịch. Về mặt công nghệ, giao dịch trên cơ sở truyền thống và giao dịch số hóa khác nhau về nguyên tắc, thao tác thực hiện và những quy định về luật pháp. Từ đó nảy sinh các vấn đề mới trong giao dịch TMĐT. Nếu việc tạo ra, gửi và nhận một tài liệu trên giấy phức tạp, mất nhiều thời gian và chi phí thì việc tạo, gửi và nhận các tài liệu trên các phương tiện điện tử rất thuận tiện, nhanh chóng và ít tốn kém. Tuy vậy, một tài liệu trên giấy khi được ký (bản gốc) mang tính duy nhất và không thể sao chép. Ngược lại một tài liệu điện tử không có tính chất này, nó dễ dàng tạo ra các bản sao giống hệt và không thể phân biệt các bản sao này với các bản gốc. Bản chất của TMĐT là hình thức kinh doanh qua mạng Internet. Internet ngoài việc đem lại nhiều lợi ích còn là môi trường phát triển TMĐT, thì nó cũng là môi trường rất thuận lợi cho kẻ phá hoại thực hiện các ý đồ xấu của mình như xem trộm thông điệp trên đường truyền, tấn công phá hoại nội dung thông tin, giả mạo thông điệp hay giả mạo người dùng,…Ngoài ra, khi giao dịch thương mại điện tử thì các tài liệu giữa các bên gửi cho nhau dễ dàng bị kẻ xấu (hacker) đánh cắp, thay thế sửa sai hoặc cố tính phá hỏng thông tin hay nguy cơ mạo danh chối cãi nguồn gốc,... những điều này có thể làm mất đi cơ hội kinh doanh hoặc làm suy giảm nghiêm trọng uy tín của doanh nghiệp. Vì vậy, trong giao dịch thương mại nói chung và giao dịch thương mại điện tử nói riêng, việc đảm bảo an toàn thông tin trong giao dịch và rất quan trọng và cần thiết. Một trong những biện pháp bảo đảm an toàn thông tin trong giao dịch thương mại điện tử đó là sử dụng chữ ký số. Sử dụng chữ ký số nhằm đảm bảo tính toàn vẹn, duy nhất và không bị sửa đổi bởi người khác của dữ liệu trong giao dịch. Chữ ký số là một công cụ bảo mật an toàn nhất hiện nay. Nó là bằng chứng xác thực người gửi chính là tác giả của thông điệp mà không phải là một ai khác. Không những thế, khi chữ ký số được gắn với một thông điệp điện tử thì đảm bảo rằng thông tin trên đường chuyển đi sẽ không bị thay đổi bởi bất kỳ một người nào ngoài người ký ban đầu. Mọi sự thay đổi dù nhỏ nhất sẽ đều bị phát hiện một cách dễ dàng.

### 1.2.2 Về chữ ký số

*Khái niệm Chữ ký số*

Theo Điều 1, Khoản 4, Nghị định số 26/2007/NĐ-CP, chữ ký số là một dạng chữ ký điện tử (hay còn gọi là sơ đồ chữ ký số) được tạo ra bằng sự biến đổi một thông điệp dữ liệu, sử dụng hệ thống mật mã không đối xứng; được sử dụng để xác thực danh tính, bảo vệ tính toàn vẹn và bảo mật của các giao dịch điện tử. Chữ ký số tương đương với chữ ký viết tay hoặc con dấu được đóng dấu, nhưng cung cấp tính bảo mật cao hơn nhiều. Mỗi người dùng chữ ký số phải có một cặp khóa gồm khóa công khai (public key) và khóa bí mật (private key). Khóa bí mật dùng để tạo chữ ký số. Khóa công khai dùng để thẩm định chữ ký số.

*Khả năng của chữ ký số*

Chữ ký số có thể đảm bảo tính toàn vẹn của tài liệu từ đầu đến cuối và cũng có thể cung cấp thông tin xác thực về người khởi tạo tài liệu. Chữ ký số giúp thiết lập các đảm bảo sau:

* Tính xác thực (Authenticity): Chữ ký số giúp đảm bảo rằng người ký chính là người mà họ tuyên bố.
* Tính toàn vẹn (Integrity): Chữ ký số giúp đảm bảo rằng nội dung không bị thay đổi hoặc giả mạo kể từ khi được ký số.
* Chống thoái thác (Non-repudiation): Chữ ký số giúp chứng minh nguồn gốc của nội dung được ký cho tất cả các bên, chống giả mạo, mạo danh hoặc từ chối với bất kỳ nội dung đã ký. Chữ ký số có thể được sử dụng như một bằng chứng pháp lý trong trường hợp tranh chấp, vì nó chứng minh rõ người ký không thể từ chối việc ký tài liệu.
* Tính bảo mật cao: chữ ký số có 2 lớp mã khóa, đảm bảo tính bảo mật và không bị đánh cắp thông tin bởi hacker.

*Cấu tạo chữ ký số*

Chữ ký số hiện nay chủ yếu được mã hóa bằng hệ mã hóa công khai dựa trên thuật toán gốc RSA, bao gồm các thành phần chính như sau:

* Khóa bí mật (private key): một bộ phận không thể thiếu trong cặp khóa khi tạo chữ ký số.
* Khóa công khai (public key): loại khóa không thể thiếu trong cặp khóa khi kiểm tra chữ ký số. Khóa công khai được tạo bởi khóa bí mật tương ứng trong cặp khóa.
* Người ký: chủ thể sẽ dùng khóa bí mật đã được cung cấp để thực hiện ký vào một thông điệp dữ liệu dưới tên mình
* Người nhận: là tổ chức hoặc cá nhân nhận thông điệp dữ liệu được ký số bởi người ký, bằng việc sử dụng các chứng thư số của người ký để kiểm tra chữ ký số ở thông điệp dữ liệu nhận được và sau đó tiến hành các hoạt động, giao dịch liên quan.
* Ký số: là việc đưa khóa bí mật vào một phần mềm để tự động tạo và gắn chữ ký số vào thông điệp dữ liệu nào đó.

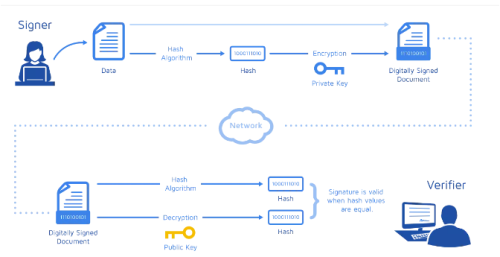
*Tiến trình tạo chữ ký số*

Chữ ký số được tạo ra theo 4 bước sau:

Bước 1: Từ văn bản cần ký, người ký sử dụng một phần mềm ký (thường sử dụng phần mềm chạy thuật toán RSA hoặc SHA2) để tính toán tạo ra giá trị hash (giá trị hash là 1 dãy những ký tự 0/1 và là duy nhất, bất kỳ thay đổi nào trong dữ liệu ngay cả thay đổi một ký tự cũng sẽ dẫn đến giá trị hash khác). Sau đó, mã hóa giá trị hash này bằng khóa riêng của người ký (private key). Khóa này tạo thành chữ ký số. Nhiều chữ ký và định dạng chữ ký có thể được đính kèm vào một văn bản/tin nhắn, mỗi chữ ký tham chiếu đến các phần khác nhau

Bước 2: Người gửi truyền chữ ký số kèm với với giá trị hash

Bước 3: Người nhận giải mã chữ ký số bằng khóa công khai (public key) của người gửi để tạo lại giá trị hash.

Bước 4: Người nhận xác minh giá trị hash tìm được ở bước 3 với giá trị hash tạo ra ở bước 1 xem hai giá trị này có giống nhau không. Nếu hàm hash được giải mã (ở bước 3) khớp với hàm hash được tính toán (ở bước 1) thì chứng tỏ dữ liệu không thay đổi kể từ lần được ký. Nếu hai hàm hash không khớp, dữ liệu đã bị giả mạo và bị xâm phạm. Hoặc chữ ký được tạo bằng private key không tương ứng với public key do người ký cung cấp.

(*Hình 1: Sơ đồ thể hiện quá trình tạo chữ ký số*)

### 1.2.3 Tầm quan trọng của chữ ký số trong bảo mật thông tin

Chữ ký số là một công nghệ an toàn thông tin quan trọng, đóng vai trò quan trọng trong việc xác thực danh tính, bảo vệ tính toàn vẹn và bảo mật của các giao dịch điện tử. Trong môi trường số, các giao dịch điện tử ngày càng trở nên phổ biến, tuy nhiên cũng tiềm ẩn nhiều rủi ro về an toàn thông tin, như: Rủi ro giả mạo danh tính; Rủi ro thay đổi dữ liệu; Rủi ro chối bỏ giao dịch. Chữ ký số giúp giải quyết những rủi ro này bằng cách cung cấp các tính năng: Xác thực danh tính; Bảo vệ tính toàn vẹn dữ liệu; Chống chối bỏ giao dịch. Chữ ký số có thể được ứng dụng trong nhiều lĩnh vực khác nhau để bảo vệ thông tin, bao gồm: Thương mại điện tử, tài chính ngân hàng, giáo dục, y tế,..

Chính vì vậy, chữ ký số có tầm quan trọng đặc biệt trong bảo mật thông tin, đặc biệt là trong các giao dịch điện tử. Chữ ký số giúp đảm bảo tính an toàn, bảo mật và hợp pháp của các giao dịch điện tử, góp phần thúc đẩy phát triển thương mại điện tử và các hoạt động kinh tế, xã hội khác trong môi trường số.

Với những ưu điểm vượt trội, chữ ký số ngày càng được ứng dụng rộng rãi trong nhiều lĩnh vực khác nhau, góp phần bảo vệ thông tin và thúc đẩy phát triển kinh tế, xã hội. Chữ ký số không chỉ là một công cụ bảo mật thông tin mạnh mẽ mà còn có tầm quan trọng lớn trong việc đảm bảo tính toàn vẹn, xác thực và an toàn của thông tin trong môi trường số hóa ngày nay.

# 

# **CHƯƠNG 2: KỸ THUẬT SỬ DỤNG**

## 2.1 Mã hóa thông tin và mật mã khóa công khai

### 2.1.1 Mã hóa thông tin

Có rất nhiều thông tin mà chúng ta không muốn người khác biết khi gửi đi như: thông tin về Credit-Card, thông tin về kinh doanh của công ty, thông tin về tài khoản cá nhân, thông tin về cá nhân như số chứng minh thư, số thẻ...

Các thông tin bí mật được cung cấp cho các máy tính quan mạng Internet bằng nhiều phương thức khác nhau ví dụ: Một cách bảo mật đơn giản nhưng minh bạch nhất là lưu các thông tin bí mật trên các bộ nhớ có thể xóa được (Removable Storage) như đĩa mềm. Tuy nhiên dạng bảo mật phổ biến nhất vẫn là dựa vào quá trình mã hoá dữ liệu (Encryption).

Các hệ thống mã hoá trong máy tính phổ biến nhất thuộc một trong hai loại sau:

* Mã hoá với khoá đối xứng (Symmetric-key Encryption) : Trong phương pháp mã hoá với khoá đối xứng, mỗi máy tính có một khoá bí mật (dạng mã) dùng để mã hoá các gói thông tin trước khi chúng được gửi qua mạng tới các máy tính khác. Phương pháp mã hoá với khoá đối xứng đòi hỏi người sử dụng phải xác định được những máy tính nào đang liên lạc trao đổi thông tin với nhau để cài đặt khóa này trên mỗi máy.
* Mã hoá với khoá công khai (Public-key Encryption): Phương pháp mã hoá này khác biệt với mã hoá với khóa đối xứng ở chỗ mỗi máy tính sẽ sở hữu một cặp khóa, bao gồm khóa công khai và khóa bí mật. Khóa công khai dùng để mã hoá dữ liệu, trong khi khóa bí mật sẽ được giữ kín và chỉ sử dụng để giải mã. Khi một máy tính muốn gửi thông tin mật đến máy tính khác, nó sẽ sử dụng khóa công khai của máy đích để mã hoá dữ liệu. Điều này đồng nghĩa với việc bất kỳ ai cũng có thể sử dụng khóa công khai để mã hoá, nhưng chỉ máy tính đích mới có khả năng giải mã với khóa bí mật của mình. Phương pháp này không đòi hỏi việc trao đổi khóa trước giống như mã hóa với khóa đối xứng, giảm bớt công đoạn xác định khóa giữa các máy tính.

### 2.1.2 Mật mã khóa công khai

Năm 1976, Whitfield Diffie và Martin Hellman đã đề xuất khái niệm mật mã hóa khóa bất đối xứng, và đưa ra phương pháp trao đổi khóa công khai. Trước khi khái niệm mật mã học bất đối xứng ra đời, để đảm bảo tính bí mật khi trao đổi thông tin, các thuật toán mã hóa thông tin được xây dựng trên mật mã học đối xứng. Trong loại mật mã này, giữa các bên trao đổi thông tin cần phải cần gặp gỡ hoặc trao đổi qua một kênh bảo mật một khóa bí mật. Điều này đã hạn chế ứng dụng của mật mã học vào việc đảm bảo tính riêng tư, bí mật trong cuộc sống, và sự thật thì cho tới những năm đó, mật mã học chủ yếu chỉ được ứng dụng trong lĩnh vực quân sự, an ninh quốc phòng.

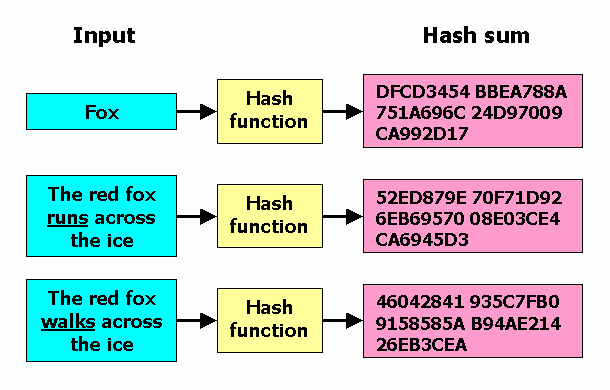
Mật mã hóa khóa công khai (bất đối xứng) cho phép người sử dụng trao đổi các thông tin mật mà không cần phải trao đổi các khóa chung bí mật trước đó. Điều này được thực hiện bằng cách sử dụng một cặp khóa có quan hệ toán học với nhau là khóa công khai và khóa cá nhân (hay khóa bí mật). Trong mật mã hóa 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.

Quan hệ giữa khóa công khai và khóa bí mật có tính chất một chiều, có nghĩa là từ việc sở hữu khóa bí mật ta dễ dàng tìm ra được khóa công khai, tuy nhiên cho dù biết được khóa công khai thì việc tìm ra khóa bí mật ra rất khó (khó theo nghĩa khối lượng và thời gian tính toán được yêu cầu là rất lớn, lên tới hàng trăm năm). Cơ sở toán học của tính chất một chiều này là nhờ vào các hàm toán học một chiều (one-way function). Một ví dụ về hàm dạng này là bài toán phân tích thừa số nguyên tố: giả sử ta có một vài số nguyên tố lớn, từ các số này ta tìm tích của chúng thì đơn giản; ngược lại từ tích số, việc phân tích ra các thừa số nguyên tố này là khó. Nếu các số này là lớn, cỡ 1024 hoặc 2024 bít thì việc phân tích thừa số nguyên tố này có thể đòi hỏi máy tính năng lực lớn nhất bây giờ chạy mất vài chục năm. Thời gian này là quá lớn đối với nhu cầu cần giữ bí mật của một khóa bí mật trong vài năm.

## 2.2 Hàm băm

### 2.2.1 Sơ lược về 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...). Giá trị băm đóng vai trò gần như một khóa để phân biệt các khối dữ liệu, tuy nhiên, người ta chấp nhận hiện tượng trùng khóa hay còn gọi là đụng độ và cố gắng cải thiện giải thuật để giảm thiểu sự đụng độ đó. 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).

Hàm băm là các thuật toán không sử dụng khóa để mã hóa, nó có nhiệm vụ băm thông điệp được đưa vào theo một thuật toán h một chiều nào đó, rồi đưa ra một văn bản băm gọi là văn bản đại diện có kích thước cố định. Do đó người nhận không biết được nội dung hay độ dài ban đầu của thông điệp đã được băm bằng hàm băm. Giá trị ban đầu của hàm băm là duy nhất và không thể suy ngược lại được nội dung thông điệp từ giá trị băm này

*Hình 2: Ví dụ về hàm băm*

Một hàm băm được xem là bảo mật và an toàn phải đảm bảo các tính chất sau:

* Có thể áp dụng với thông báo đầu vào có độ dài bất kỳ.
* Tạo ra giá trị băm y = h(x) có độ dài cố định, h(x) dễ dàng tính được với bất kỳ x nào
* Tính một chiều: Với mọi đầu ra y cho trước không thể tìm được x' sao cho h(x') bằng giá trị y cho trước.

### 2.2.2 Sử dụng hàm băm trong chữ ký số

Các sơ đồ ký số thường chỉ được sử dụng để ký các bức thông điệp có kích thước nhỏ và sau khi ký, bản ký số có kích thước lớn hơn bản thông điệp gốc (gấp đôi). Trên thực tế, ta cần phải ký các văn bản có kích thước lớn lên đến hàng MB, sau đó ta phải gửi kèm cả chữ ký số lẫn đoạn thông điệp gốc để xác nhận, điều này làm cho dung lượng thông tin truyền qua mạng trở nên rất lớn. Một cách để giải quyết vấn đề trên là băm thông điệp thành nhiều đoạn, sau đó ký lên các đoạn đó độc lập nhau. Nhưng sử dụng biện pháp này lại gặp phải một số vấn đề khác của chữ ký số đó là:

* Không giải quyết được vấn đề kích thước truyền lớn
* Các chữ ký "an toàn" thì tốc độ chậm vì chúng dùng nhiều phép tính số học
* Sau khi ký, nội dung của thông điệp có thể bị xáo trộn các đoạn với nhau, hoặc một số đoạn có thể bị mất mát, không đảm bảo tính toàn vẹn của thông điệp.

Chính vì vậy, giải pháp cho vấn đề vướng mắc trên là dùng hàm băm để trợ giúp cho việc ký số với những tính chất sau:

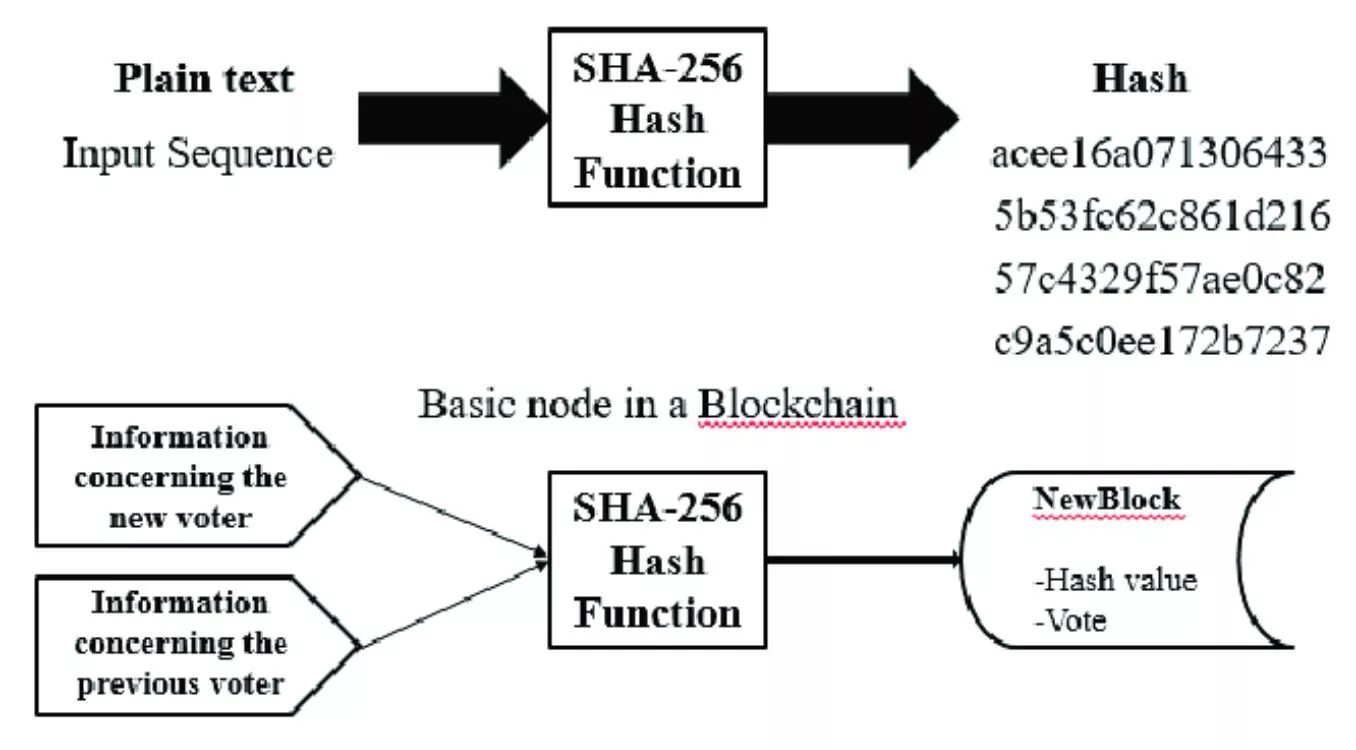
* Hàm băm tạo ra một đoạn chuỗi băm có độ dài duy nhất, giúp giảm kích thước cần tính toán giảm cả thời gian thực hiện và dung lượng truyền.
* Tăng tính bảo mật cho chương trình, mỗi đoạn văn bản chỉ có thể tạo ra một chuỗi băm duy nhất không trùng lặp.
* Tránh sự trùng lặp thông điệp khi ký trên các đoạn văn bản khác nhau.

### 2.2.3 Hàm băm SHA-256

SHA-256 (thuộc họ hàm băm SHA-2) là hàm băm mật mã lấy đầu vào và tạo ra giá trị băm 256 bit - 32 byte) được thiết kế bởi NSA (Cơ quan An ninh Quốc gia) và được NIST (Viện Tiêu chuẩn và Công nghệ Quốc gia) tiêu chuẩn hóa thành một trong những tiêu chuẩn xử lý thông tin liên bang (FIPS 180-4) vào năm 2001.

SHA-256 là viết tắt của Secure Hash Algorithm 256 Bit và được sử dụng để bảo mật bằng mật mã. Thuật toán băm mật mã tạo ra các hàm băm không thể đảo ngược và duy nhất. Số lượng hàm băm có thể có càng lớn, thì xác suất để hai giá trị sẽ tạo ra cùng một giá trị băm càng nhỏ. SHA-256 được cho là được sử dụng rộng rãi nhất do sự cân bằng tuyệt vời giữa tính dễ thực hiện, tốc độ tính toán và bảo mật mật mã. Thuật toán này rất an toàn và được nhiều nơi trên thế giới sử dụng nó để lưu trữ mật khẩu, kiểm tra các tài liệu kỹ thuật số, thuật toán này được áp dụng không chỉ cho tập tài liệu hoặc văn bản, mà nó còn được áp dụng cho bất kỳ tài liệu kỹ thuật số nào: đoạn video, văn bản, âm thanh, tệp lệnh vào trong thuật toán, nó sẽ trả về một giá trị đặc biệt và duy nhất cho từng đối tượng dữ liệu.

Thuật toán cho SHA-256:

*Hình 3: Thuật toán hàm băm SHA-256*

Trong thuật toán SHA, giá trị băm ban đầu là cố định và thông tin được sử dụng để thay đổi giá trị này là dữ liệu đầu vào. Đối với SHA-256, dữ liệu đầu vào được chia thành 64 byte một lần. Dữ liệu này được đặt tên là “khối tin nhắn”. Nếu lượng dữ liệu đầu vào vượt quá 64 byte, nhiều khối thông báo sẽ được hình thành.

Sau đó, giá trị băm ban đầu được thay đổi bằng cách sử dụng khối thông báo đầu tiên để tính giá trị băm mới. Ngoài ra, nó cũng được thay đổi trong khối thông báo tiếp theo để có được giá trị băm mới và lặp lại quá trình này cho đến hết. Kết quả cuối cùng là giá trị băm được tính trên khối tin nhắn cuối cùng.

## 2.3 Sơ đồ chữ ký số RSA

Đặc điểm của sơ đồ chữ ký này là mức độ tính toán phụ thuộc hoàn toàn vào độ lớn của giải thuật giải quyết các bài toán nhân số nguyên – bài toán lũy thừa. Sơ đồ chữ ký bao gồm cả hai loại kèm thông điệp và khôi phục thông điệp. Sơ đồ chữ ký RSA được phát minh bởi 3 nhà nghiên cứu Rivest, Shamir và Adleman, đây là sơ đồ có ứng dụng thực tế rộng rãi nhất dựa trên công nghệ sử dụng khoá chung. Các phương pháp tấn công RSA đầu tiên (multicative property) và các vấn đề khác liên quan tới chữ ký RSA, do Davia, Jonge và Chaum đưa ra.

### 2.3.1 Thuật toán sinh khóa và sinh chữ ký số

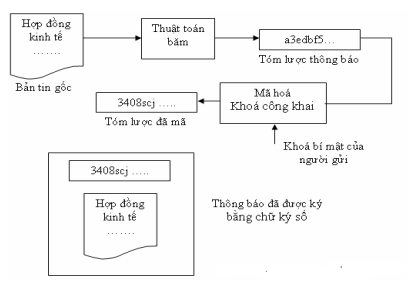
Thực thể A tạo khóa công khai và khóa bí mật RSA tương ứng theo phương thức sau:

* Chọn 2 số nguyên tố lớn ngẫu nhiên p, q. Nhằm có sự an toàn tối đa nên chọn p và q có độ dài bit bằng nhau.
* Tính n = p.q và φ(n) = (p−1).(q−1).
* Chọn ngẫu nhiên một số nguyên e thỏa mãn điều kiện 1< e <φ(n) sao cho gcd(e,φ(n)) = 1 hay e với gcd là ước số chung lớn nhất.
* Sử dụng giải thuật Euclid mở rộng để tính toán số tự nhiên duy nhất d sao cho 1< d < φ(n) và e.d = 1 (mod φ(n)).

Kết quả là ta có được cặp khóa: khóa công khai K’ = (n,e) và khóa bí mật K” = (n,d).

Thực thể A ký trên thông điệp m dựa vào khóa bí mật đã có. Để ký một thông điệp m, người ký thực hiện các bước sau:

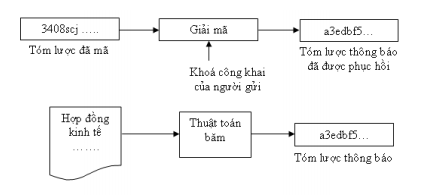
* Dùng hàm băm H để băm thông điệp m: tính m’ = H(m), một số nguyên trong khoảng [0,n-1]
* Tạo chữ ký số sử dụng khóa bí mật (n,d) để tính: y = mod n.

Chữ ký của m là y và được gửi kèm với thông điệp m đến người nhận. 

*Hình 4: Quá trình sinh chữ ký số*

### 2.3.2 Thuật toán xác nhận chữ ký

Thực thể B có thể xác nhận được chữ ký của A bằng khóa công khai và khôi phục lại thông điệp chữ ký. Để xác nhận chữ ký, người nhận thực hiện các bước sau:

* Sử dụng khóa công khai (n,e) của người ký (A) để giải mã chữ ký: m’ = mod n.
* Sử dụng cùng hàm băm H với người ký để băm lấy thông điệp m: m = (m’).
* Chấp nhận chữ ký nếu h′=h. Ngược lại từ chối chữ ký. 

*Hình 5: Quá trình xác thực chữ ký số*

### 2.3.3 Độ an toàn của sơ đồ chữ ký số RSA

Độ an toàn của chữ ký số RSA phụ thuộc vào bài toán tách n thành hai số nguyên tố p và q. Vì nếu biết được p và q thì sẽ biết được bí mật ϕ(n) sau đó dựa vào công thức e.d ≡ 1 (mod ϕ(n)), với e là khóa công khai đã biết thì có thể tính được khóa bí mật d.

Nếu sơ đồ ký số thực hiện đơn giản thì tội phạm dễ dàng lừa. Ví dụ như họ có thể chọn ngẫu nhiên y và tính toán độ lớn: m = (mod n) . Rõ ràng quá trình thẩm tra (m,y) là hoàn toàn đúng. Ngoài ra do tính chất nhân của hàm RSA, tức là nếu có hai bức điện và tương ứng với nó là 2 chữ ký và thì dễ dàng hình thành chữ ký thứ ba với bức điện thứ ba :

Để chống lại sự giả mạo chữ ký theo phương pháp trên thì một phương pháp đơn giản là thêm thông tin phụ vào bức điện M, có nghĩa là m = M||I, ở đây I là dấu hiệu nhận dạng ví dụ như I = ”tên tác giả”.

Ngoài ra kết hợp với việc ký lên giá trị hàm băm hash của bức điện, tức là ký lên giá trị: m = hash(M). Vì những tính chất của hàm băm hash sẽ chống lại khả năng giả mạo trên trừ xác suất rất nhỏ, vì nếu khó có thể tìm được bức điện mà giá trị băm của nó trùng với giá trị hàm băm hash đã cho.

## 2.4 Cơ sở hạ tầng khóa công khai (PKI)

### 2.4.1 Khái niệm

Cơ sở hạ tầng khóa công khai, hay còn được biết đến với tên gọi PKI (Public Key Infrastructure), là nền tảng của mật mã học khóa công khai, một cơ sở hạ tầng an ninh cung cấp khả năng xác thực và bảo mật thông tin trong môi trường truyền thông không an toàn như internet. PKI sử dụng cặp khóa công khai và khóa bí mật để thực hiện các chức năng như xác thực, mã hóa, và ký số. Hệ thống được xây dựng bởi một bên thứ ba được ủy quyền gọi là CA (Certificate Authority), cung cấp các dịch vụ tin cậy liên quan đến việc cấp phát/thu hồi chứng thư số (có thể coi như một chứng minh thư số) cho một người dùng; xác thực một chứng thư số có tương ứng với người dùng hay không , …

Mục đích chính của PKI là cung cấp các cặp khóa và các dịch vụ liên quan sử dụng chúng. Khái niệm hạ tầng khóa công khai thường được dùng để chỉ toàn bộ hệ thống bao gồm nhà cung cấp chứng thực số (CA - Certificate Authority) cùng các cơ chế liên quan đồng thời với toàn bộ việc sử dụng các thuật toán mã hóa công khai trong trao đổi thông tin.

PKI là một tập hợp các thiết bị phần cứng, phần mềm, con người và các thủ tục cần thiết phát hành/thu hồi thẻ, lưu trữ, phân phối, thu hồi các khóa và chứng chỉ số dựa trên mật mã khóa công khai. Các thành phần này kết hợp với nhau để thiết lập một phương thức trao đổi thông tin trong môi trường mạng đảm bảo tính xác thực định danh đối tác ở mức an toàn cao nhất.

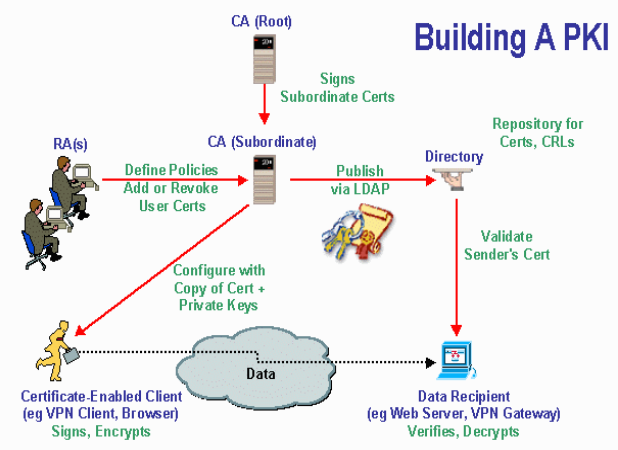
Nhiệm vụ chính của PKI là sử dụng chiến lược mã hóa khóa công cộng (public key encryption) để tạo, quản lý và thu hồi các thẻ chứng thực. Cụ thể:

* Tạo và xác định tính hợp lệ của chữ ký số
* Đáp ứng sự đăng ký thẻ của người sử dụng mới
* Xác thực người sử dụng và phân phối thẻ chứng thực đến họ
* Thu hồi các thẻ chứng thực hết hạn
* Tạo các private key và public key cho các PKI client

Trong kỷ nguyên bùng nổ của công nghệ thông tin, mọi giao dịch từ xa có thể thông qua internet. Tuy nhiên, mặt khác khó mà bảo đảm rằng những giao dịch trên Internet luôn an toàn. Cơ sở hạ tầng khóa công khai (PKI) đã đáp ứng những yêu cầu cấp thiết đó. Dựa trên cách sử dụng của chìa khóa mật mã công cộng và chữ ký điện tử, 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.

### 2.4.2 Nguyên tắc hoạt động của cơ sở hạ tầng khóa công khai

PKI cung cấp một cặp chìa khóa, trong đó có một chìa là chìa khóa công khai (Public key) để có thể sử dụng dịch vụ, chìa 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.

*Hình 6: Quá trình xây dựng một hệ thống PKI*

*Hoạt Động Cơ Bản của Hệ Thống PKI*

* Người ký sử dụng khóa bí mật của mình để tạo ra một hàm băm của thông điệp dữ liệu. Hàm băm là một hàm toán học biến đổi một thông điệp dữ liệu thành một chuỗi ký tự có độ dài cố định.
* Người ký sử dụng khóa công khai của mình để mã hóa hàm băm. Chữ ký số là kết quả của quá trình mã hóa.
* Người nhận sử dụng khóa công khai của người ký để giải mã chữ ký số. Nếu hàm băm được giải mã thành đúng nội dung của thông điệp dữ liệu, thì chữ ký số được xác nhận là hợp lệ.

*Quy Trình Tạo Cặp Khóa Công Khai và Khóa Bí Mật*

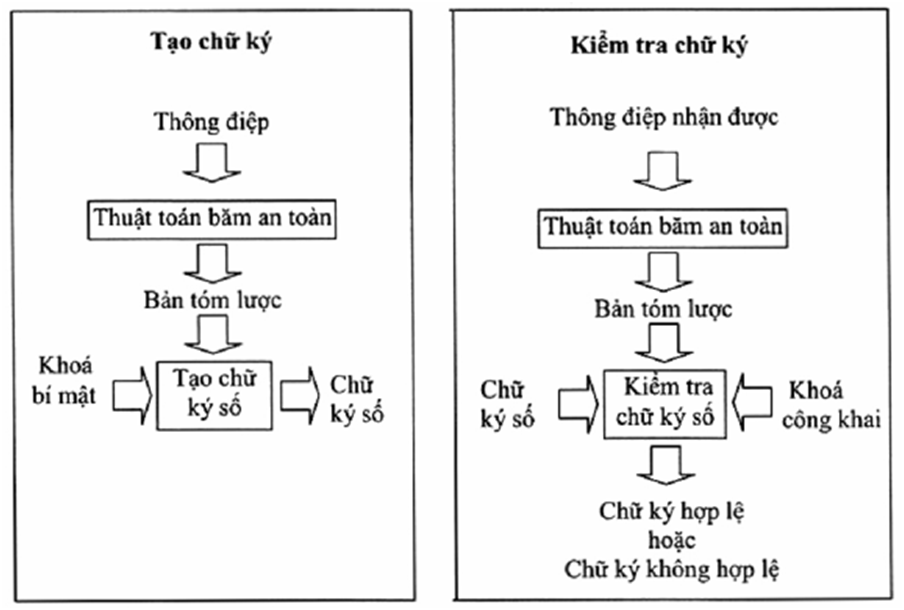
* Tạo Cặp Khóa: Người dùng hoặc tổ chức tạo một cặp khóa mới. Quá trình này tạo ra một khóa công khai và một khóa bí mật được tạo ngẫu nhiên và có quan hệ toán học đặc biệt.
* Lưu Trữ Khóa Bí Mật: Khóa bí mật được lưu trữ một cách an toàn và chỉ có sẵn cho người sở hữu. Điều này có thể được thực hiện thông qua việc sử dụng các phương tiện bảo mật vật lý hoặc mã hóa mạnh mẽ.
* Phân phối Khóa Công Khai: Khóa công khai được phân phối cho những người khác mà người sở hữu muốn giao tiếp với. Khóa công khai có thể được đăng ký và ký tên bởi một tổ chức chứng thực để đảm bảo tính xác thực.

*Quy Trình Xác Thực và Giao Tiếp*

* Xác Thực: Người gửi sử dụng khóa công khai của người nhận để mã hóa dữ liệu hoặc tạo chữ ký số. Người nhận sau đó sử dụng khóa bí mật của mình để giải mã hoặc xác thực chữ ký.
* Chứng Thực Cặp Khóa: Các cặp khóa có thể được chứng thực bởi một tổ chức chứng thực (CA). CA xác nhận rằng khóa công khai thuộc về người chủ sở hữu nào thông qua việc ký và phát hành chứng chỉ số.
* Phân Phối Chứng Chỉ: Chứng chỉ chứa thông tin về khóa công khai và chủ sở hữu. Chúng có thể được phân phối trên mạng hoặc lưu trữ trong các hệ thống quản lý chứng chỉ.
* Quản Lý Chứng Chỉ Hết Hạn: Chứng chỉ có thời hạn và cần được đổi mới. Quy trình này được thực hiện để đảm bảo tính an toàn và độ tin cậy của hệ thống.

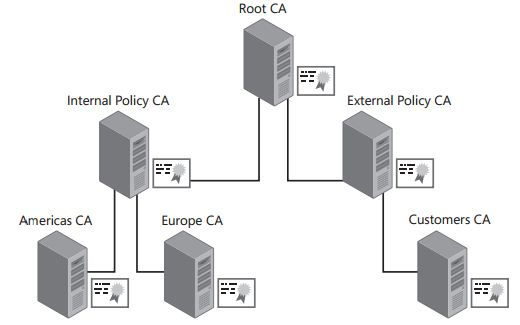
*Chữ Ký Số*

* Tạo Chữ Ký Số: Người gửi sử dụng khóa bí mật của mình để tạo chữ ký số cho dữ liệu. Quy trình này đảm bảo tính xác thực và không thể chối bỏ.
* Xác Thực Chữ Ký: Người nhận sử dụng khóa công khai của người gửi để xác thực chữ ký số. Nếu quá trình này thành công, dữ liệu được coi là an toàn và nguyên vẹn.

*Hình 7: Mô tả quá trình tạo và kiểm tra chữ ký số*

### 2.4.3 Cấu trúc phân tầng của hệ thống PKI

Mô hình này tương ứng với cấu trúc phân cấp với CA gốc và các CA cấp dưới. CA gốc xác nhận các CA cấp dưới, các CA này lại xác nhận các CA cấp thấp hơn. Các CA cấp dưới không cần xác nhận các CA cấp trên.

*Hình 8: Cấu trúc của một hệ thống PKI*

Mô hình phân cấp được minh hoạ như hình ở trên. Trong mô hình này, mỗi thực thể sẽ giữ bản sao khóa công khai của root CA (CA gốc) và kiểm tra đường dẫn của chứng thư bắt đầu từ chữ ký của CA gốc. Đây là mô hình PKI tin cậy sớm nhất và được sử dụng trong PEM.

*Ưu điểm của mô hình:*

* Mô hình này có thể dùng được trực tiếp cho những doanh nghiệp phân cấp và độc lập, cũng như những tổ chức chính phủ và quân đội.
* Cho phép thực thi chính sách và chuẩn thông qua hạ tầng cơ sở.
* Dễ vận hành giữa các tổ chức khác nhau.

*Nhược điểm của mô hình:*

* Có thể không thích hợp đối với môi trường mà mỗi miền khác nhau cần có chính sách và giải pháp PKI khác nhau.
* Các tổ chức có thể không tự nguyện tin vào các tổ chức khác.
* Có thể không thích hợp cho những mối quan hệ ngang hàng giữa chính phủ và doanh nghiệp.
* Những tổ chức thiết lập CA trước có thể không muốn trở thành một phần của mô hình.
* Có thể gây ra sự trội hơn của sản phẩm đối với vấn đề về khả năng tương tác.
* Chỉ có một CA gốc nên có thể gây ra một số vấn đề như thiếu khả năng hoạt động. Thêm vào đó, trong trường hợp khóa cá nhân của CA bị xâm phạm, khóa công khai mới của CA gốc phải được phân phối đến tất cả các người sử dụng cuối trong hệ thống theo một số cơ chế khác nhau.
* Mặc dù có những nhược điểm, song mô hình này vẫn thích hợp với yêu cầu của các tổ chức chính phủ vì cấu trúc phân cấp tự nhiên sẵn có.

## 2.5 Cấp phát và xác thực chữ ký số

### 2.5.1 Chứng thực số

Trong mật mã học, chứng thực khóa công khai (còn gọi là chứng thực số / chứng thực điện tử) là một chứng thực sử dụng chữ ký số để gắn một khóa công khai với một thực thể (cá nhân, máy chủ hoặc công ty...). Một chứng thực khóa công khai tiêu biểu thường bao gồm khóa công khai và các thông tin (tên, địa chỉ...) về thực thể sở hữu khóa đó. Chứng thực điện tử có thể được sử dụng để kiểm tra một khóa công khai nào đó thuộc về ai.

CA phát hành các chứng thực khóa công khai trong đó thể hiện rằng CA đó chứng nhận khóa công khai nằm trong mỗi chứng thực thuộc về cá nhân, tổ chức, máy chủ hay bất kỳ thực thể nào ghi trong cùng chứng thực đó. Nhiệm vụ của CA là kiểm tra tính chính xác của thông tin liên quan tới thực thể được cấp chứng thực. Khi người sử dụng tin tưởng vào một CA và có thể kiểm tra chữ ký số của CA đó thì họ cũng có thể tin tưởng vào khóa công khai và thực thể được ghi trong chứng thực.

### 2.5.2 Cấp phát chữ ký số

Bước 1: Sinh cặp khóa ngẫu nhiên (PKI client)

Tại client hệ thống PKI sẽ cấp phát cặp khóa riêng và khóa công khai và sử dụng thuật toán RSA để sinh cặp khóa ngẫu nhiên. Cặp khóa ngẫu nhiên được sinh ra từ 2 số nguyên tố ngẫu nhiên lập đủ lớn. Cặp khóa ngẫu nhiên ở đây là :

* Khóa công khai: **(n,e)**
* Khóa bí mật: **(n,d)**

Bước 2: Tạo chữ ký số

Sau khi tạo cặp khóa ngẫu nhiên , hệ thống PKI client sẽ tạo ra chữ ký số tương ứng với cặp khóa ngẫu nhiên của từng client và ký theo từng văn bản ngẫu nhiên.

Bước 3: Cấp phát chứng thực số

Sau khi PKI client tạo cặp khóa riêng và khóa công khai đồng thời tạo chữ ký số cho client tương ứng. Thông tin bảo mật sẽ được gửi đến server.

Tại server, server sẽ xác thực những thông tin mà client gửi đến có chính xác và đúng đắn. Nếu thông tin xác thực là đúng đắn (khóa công khai, chữ ký số, giá trị băm của văn bản, tin nhắn) server sẽ cấp phát cho client 1 chứng thực số bao gồm các thông tin sau : tên, tuổi, địa chỉ, các thông tin cá nhân khác, khóa công khai, ngày tạo, ngày hết hạn và ID của chứng thực số. ID của chứng thực số có tính duy nhất với mỗi client.

Bước 4: Thu hồi và cấp phát lại chứng thực số

Một chứng thực số bị thu hồi khi nào :

* Khi mà chứng thực số đã hết hạn sử dụng, chứng thực sẽ bị thu hồi để ra hạn hoặc cấp một chứng thực số mới
* Khi client phát hiện khóa bí mật của người này bị lộ hoặc server phát hiện thấy hàm băm mật mã của mình bị lộ hoặc các thông tin bảo mật khác của 1 client đã bị rò rỉ

Cấp phát lại chứng thực số: Client sẽ gửi yêu cầu đến server yêu cầu và 1 bản thông tin (địa chỉ, khóa công khai,khóa riêng…) của client đăng ký một bản chứng thực số mới.

### 2.5.3 Xác thực chữ ký số

Khi bạn gửi một thông tin kèm chứng chỉ số, người nhận - có thể là đối tác kinh doanh, tổ chức hoặc cơ quan chính quyền - sẽ xác định rõ được danh tính của bạn. Có nghĩa là dù không nhìn thấy bạn, nhưng qua hệ thống chứng chỉ số mà bạn và người nhận cùng sử dụng, người nhận sẽ biết chắc chắn đó là bạn chứ không phải là một người khác. Xác thực là một tính năng rất quan trọng trong việc thực hiện các giao dịch điện tử qua mạng, cũng như các thủ tục hành chính với cơ quan pháp quyền. Các hoạt động này cần phải xác minh rõ người gửi thông tin để sử dụng tư cách pháp nhân. Đây chính là nền tảng của một Chính phủ điện tử, môi trường cho phép công dân có thể giao tiếp, thực hiện các công việc hành chính với cơ quan nhà nước hoàn toàn qua mạng. Có thể nói, chứng chỉ số là một phần không thể thiếu, là phần cốt lõi của Chính phủ điện tử.

Một người thứ 3 bất kỳ (có thể là 1 client khác, khách chưa đăng ký chứng thực số) đều có thể kiểm tra được tính đúng đắn của 1 chứng thực số. Bằng cách PKI client sẽ cung cấp 1 dịch vụ xác thực. Người dùng có thể nhập vào ID của 1 chứng thực số bất kỳ cần kiểm tra và gửi thông tin đó lên server. Nếu chứng thực số tồn tại server sẽ trả lại thông báo cho client vừa kiểm tra.

# 

# **CHƯƠNG 3: ỨNG DỤNG VÀ DEMO**

## 3.1 Ứng dụng của chữ ký số trong thương mại điện tử

### 3.1.1 Mã hóa và bảo mật

Lợi ích đầu tiên của chứng chỉ số là tính bảo mật thông tin. Khi người gửi đã mã hóa thông tin bằng khóa công khai của người nhận, chắc chắn chỉ có người nhận mới giải mã được thông tin để đọc. Trong quá trình truyền thông tin qua Internet, dù có đọc được các gói tin đã mã hóa này, kẻ xấu cũng không thể biết được trong gói tin có thông tin gì. Đây là một tính năng rất quan trọng, giúp người sử dụng hoàn toàn tin cậy về khả năng bảo mật thông tin. Những trao đổi thông tin cần bảo mật cao, chẳng hạn giao dịch liên ngân hàng, ngân hàng điện tử, thanh toán bằng thẻ tín dụng, đều cần phải có chứng chỉ số để đảm bảo an toàn.

### 3.1.2 Chứng thực người dùng

Khi bạn gửi đi một thông tin, có thể là một dữ liệu hoặc một Email, có sử dụng chứng chỉ số, người nhận sẽ kiểm tra được thông tin của bạn có bị thay đổi hay không. Bất kỳ một sự sửa đổi hay thay thế nội dung của thông điệp gốc đều sẽ bị phát hiện. Địa chỉ email, tên domain...đều có thể bị kẻ xấu làm giả để đánh lừa người nhận lây lan virus, ăn cắp thông tin quan trọng. Tuy nhiên, chứng chỉ số thì không thể làm giả, nên việc trao đổi thông tin có kèm chứng chỉ số luôn đảm bảo an toàn.

Khi sử dụng một chứng chỉ số, người nhận - có thể là đối tác kinh doanh, tổ chức hoặc cơ quan chính quyền sẽ xác định rõ được danh tính của bạn. Có nghĩa là dù không nhìn thấy bạn, nhưng qua hệ thống chứng chỉ số mà bạn và người nhận cùng sử dụng, người nhận sẽ biết chắc chắn đó là bạn chứ không phải ai khác. Xác thực là một tính năng rất quan trọng trong việc giao dịch điện tử qua mạng, cũng như các thủ tục hành chính với cơ quan với cơ quan pháp quyền. Các hoạt động này cần phải xác minh rõ người gửi thông tin để sử dụng tư cách pháp nhân. Đây chính là nền tảng của một chính phủ điện tử, môi trường cho phép công dân có thể giao tiếp. Có thể nói, chứng chỉ số là một phần không thể thiếu, là phần cốt lõi của chính phủ điện tử.

### 3.1.3 Bảo Mật Giao Dịch Trực Tuyến

Thanh Toán An Toàn:Chữ ký số đóng vai trò quan trọng trong việc đảm bảo an toàn trong các giao dịch thanh toán trực tuyến. Khi người dùng thực hiện thanh toán, thông tin liên quan đến giao dịch được ký số, giúp xác thực tính toàn vẹn của dữ liệu thanh toán. Điều này đặc biệt quan trọng để ngăn chặn các tình trạng giả mạo giao dịch, làm tăng tính an toàn cho người tiêu dùng trong quá trình mua sắm trực tuyến.

Chứng thực Giao Dịch Tài Chính:Các giao dịch tài chính trực tuyến như chuyển khoản ngân hàng, đầu tư, yêu cầu vay vốn, đều đòi hỏi mức độ bảo mật cao. Chữ ký số giúp xác thực người thực hiện giao dịch và đảm bảo tính toàn vẹn của dữ liệu gửi đi. Việc này ngăn chặn các hành vi giả mạo tài khoản hoặc giao dịch tài chính, giúp bảo vệ tài sản và thông tin cá nhân của người dùng.

Bảo Mật Mua Sắm Trực Tuyến:Trong môi trường mua sắm trực tuyến, chữ ký số đóng vai trò quan trọng trong việc xác nhận tính xác thực của trang web và đảm bảo rằng thông tin cá nhân của người dùng không bị đánh cắp. Điều này làm tăng niềm tin của người tiêu dùng và thúc đẩy sự phát triển của thị trường thương mại điện tử.

### 3.1.4 Đăng Nhập An Toàn và Quản Lý Người Dùng

Tích Hợp Chữ Ký Số vào Quá Trình Đăng Nhập:Chữ ký số có vai trò quan trọng trong việc củng cố tính an toàn và tính xác thực của quá trình đăng nhập. Thông thường, quá trình đăng nhập yêu cầu người dùng nhập một cặp tên người dùng và mật khẩu để xác thực danh tính của họ. Tuy nhiên, việc chỉ sử dụng tên người dùng và mật khẩu có thể tạo ra rủi ro an ninh, đặc biệt nếu thông tin này bị lộ trong các cuộc tấn công mạng.

Tích hợp chữ ký số vào quá trình đăng nhập giúp củng cố an toàn bằng cách sử dụng một phương tiện bổ sung để xác thực người dùng. Khi người dùng nhập thông tin đăng nhập, chữ ký số của họ được sử dụng để tạo ra một mã xác thực, thường là một mã số động hoặc mã QR code. Mã này có thể thay đổi liên tục và chỉ có giá trị trong một khoảng thời gian ngắn, tăng cường tính xác thực và ngăn chặn việc sử dụng thông tin đăng nhập đã bị đánh cắp.

Quản Lý Người Dùng và Phân Quyền: Khi người dùng đăng nhập bằng chữ ký số, hệ thống có thể xác định rõ danh tính của họ và áp dụng các quyền truy cập tương ứng.

Quản lý người dùng thông qua chữ ký số không chỉ giới hạn ở việc kiểm soát quyền truy cập vào các hệ thống quan trọng mà còn đảm bảo tính toàn vẹn của thông tin cá nhân. Hệ thống có thể ghi lại lịch sử hoạt động của người dùng, bao gồm cả các giao dịch và thay đổi dữ liệu, tạo ra một cơ sở dữ liệu kiểm tra và giám sát.

### 3.1.5 Bảo Mật Dữ Liệu và Lưu Trữ

Sử Dụng Chữ Ký Số để Bảo Mật Dữ Liệu: Chữ ký số có thể được tích hợp để bảo mật dữ liệu trong quá trình lưu trữ. Khi dữ liệu được tạo ra hoặc sửa đổi, chữ ký số được tạo để đánh dấu vết và chứng thực tính toàn vẹn của thông tin. Điều này ngăn chặn bất kỳ thay đổi trái phép nào trong dữ liệu và đảm bảo rằng chỉ những người có quyền mới có thể tiếp cận và sửa đổi thông tin.

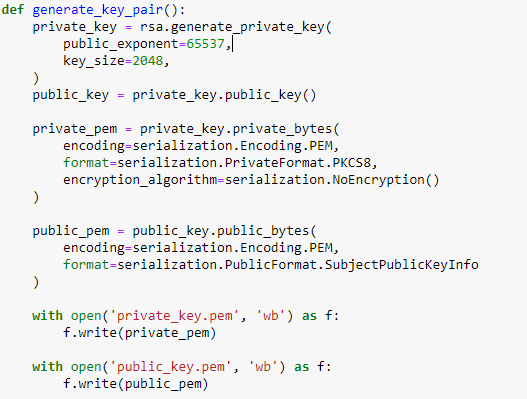
Bảo Mật Cao Đối Với Dữ Liệu Nhạy Cảm: Trong các ứng dụng yêu cầu sự an toàn cao đối với thông tin như dữ liệu cá nhân, y tế, hay tài liệu quan trọng của doanh nghiệp, chữ ký số là một công cụ quan trọng. Dữ liệu có thể được mã hóa và chữ ký số được áp dụng để đảm bảo rằng ngay cả khi dữ liệu bị đánh cắp, kẻ tấn công không thể đọc hoặc sửa đổi nó mà không được phép.

Kiểm Soát Truy Cập và Tổ Chức Dữ Liệu: Chữ ký số cũng hỗ trợ trong việc kiểm soát quyền truy cập và tổ chức dữ liệu. Hệ thống có thể sử dụng chữ ký số để xác định người dùng được ủy quyền và mức độ quyền truy cập của họ vào từng phần dữ liệu. Điều này đảm bảo rằng dữ liệu nhạy cảm chỉ được truy cập bởi những người được ủy quyền và giúp tuân thủ các quy định về bảo mật dữ liệu.

## 3.2 Demo “Tạo và xác thực chữ ký số” bằng Python

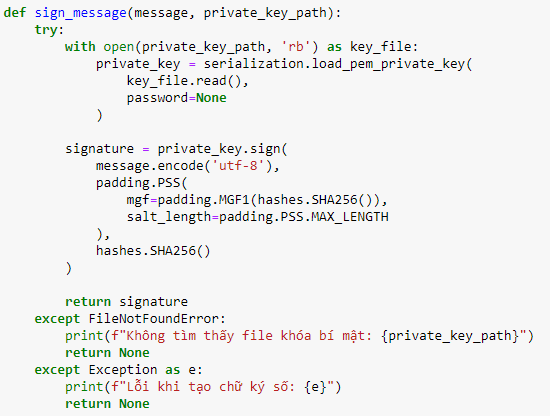
* Ngôn ngữ lập trình được sử dụng là Python
* Thuật toán sử dụng tạo cặp khóa, chữ ký số và xác thực chữ ký số là RSA. Hàm băm mã hóa sử dụng là SHA-256
* Thư viện sử dụng là thư viện “Cryptography”: một thư viện Python chuyên về bảo mật, cung cấp một số các công cụ mã hóa và bảo mật hiện đại như khóa bí mật đối xứng và không đối xứng, hàm hash, và các thuật toán padding.
* Các module chính sử dụng trong thư viện “Cryptography”: “rsa”- cung cấp các công cụ và chức năng để tạo và quản lý các khóa RSA, “serialization”- chứa công cụ để chuyển đổi và lưu khóa., “hashes”- cung cấp các hàm hash và “padding”- cung cấp thuật toán padding sử dụng trong việc tạo và xác minh chữ ký giúp thực hiện các hoạt động bảo mật như tạo và xác minh chữ ký RSA.

Bước 1: Tạo cặp khóa: Tạo hàm generate\_key\_pair() để tạo 2 cặp khóa công khai public\_key và khóa bí mật private\_key

* Để tạo private key, trong hàm generate\_key\_pair() ta sử dụng thư viện “rsa” với các tham số: public\_exponent=65537 - giá trị số mũ công khai phổ biến trong thuật toán RSA; key\_size=2048 - kích thước khóa độ dài 2048 bit, thường được sử dụng cho ứng dụng thường dùng.
* Tiếp theo, ta tạo public key từ private key đã tạo
* Sau đó, ta chuyển private key và public key thành định dạng PEM (Privacy Enhanced Mail) để lưu trữ.
* Private key được lưu vào file "private\_key.pem" và public key được lưu vào file "public\_key.pem" dưới dạng PEM để sử dụng và chia sẻ sau này.

*Hình 9: Hàm generate\_key\_pair()*

Bước 2: Ký Thông Điệp: Tạo hàm sign\_message() tạo chữ ký số cho một thông điệp sử dụng khóa bí mật, với 2 đầu vào “message”- chuỗi tin nhắn cần tạo chữ ký và “private\_key\_path” - đường dẫn đến tệp chứa private key được sử dụng để tạo chữ ký số cho message sử dụng private key được chỉ định.

* Trước hết, hàm mở và đọc tệp private key từ đường dẫn được cung cấp, sau đó sử dụng phương thức serialization.load\_pem\_private\_key() để tải private key từ dữ liệu đã đọc. Quá trình này không yêu cầu mật khẩu nên sử dụng password=None.
* Tiếp theo, tin nhắn được chuyển đổi thành dạng byte mã hóa theo chuẩn UTF-8, sau đó sử dụng private key để ký số cho tin nhắn đã cho với thuật toán ký số PSS và SHA-256 cho việc mã hóa và MGF1 cho việc tạo mã ngẫu nhiên.
* Kết quả chữ ký số được trả về dưới dạng
* Xử lý ngoại lệ: Nếu tệp chứa private key không tồn tại, hàm sẽ in ra thông báo không tìm thấy khóa; Trong trường hợp bất kỳ lỗi nào khác xảy ra trong quá trình tạo chữ ký số, hàm cũng in ra thông báo lỗi tạo chữ ký số 

*Hình 10: Hàm sign\_message()*

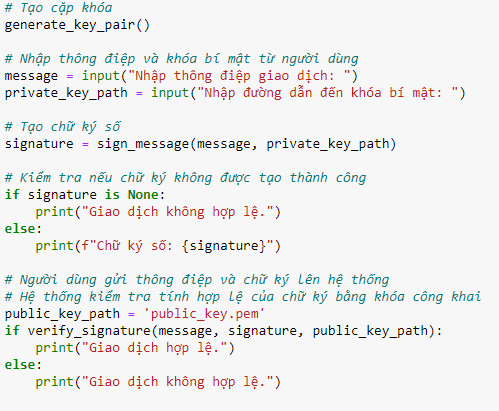
Bước 3: Xác Minh Chữ Ký: Tạo hàm verify\_signature() xác thực chữ ký số cho một thông điệp sử dụng khóa công khai nhận ba đối số là message (thông điệp cần xác thực), signature (chữ ký cần xác thực) và public\_key\_path (đường dẫn đến file chứa khóa công khai).

* Ta mở file chứa khóa công khai và sử dụng thư viện serialization để tải khóa công khai trong định dạng PEM từ file.
* Sau đó, chúng ta sử dụng khóa công khai để xác thực chữ ký số cho thông điệp. Chữ ký và thông điệp được mã hóa với định dạng UTF-8 trước khi xác thực. Các tham số khác cũng được xác định trong quá trình xác thực, bao gồm thuật toán PSS và thuật toán hash.
* Nếu quá trình xác thực thành công, hàm sẽ trả về True, ngược lại sẽ bắt các ngoại lệ và in ra thông báo lỗi trên màn hình trước khi trả về False.

*Hình 11: Hàm verify\_signature()*

Bước 4: Thực hiện quy trình

* Bắt đầu bằng việc tạo một cặp khóa với hàm generate\_key\_pair() khi chương trình được khởi động.
* Người dùng được yêu cầu cung cấp thông điệp cần ký và đường dẫn đến khóa bí mật của họ (message và private\_key\_path).
* Sử dụng hàm sign\_message() để tạo chữ ký dựa trên thông điệp và khóa bí mật, thông điệp sẽ được ký bằng khóa bí mật để tạo chữ ký số. Kiểm tra xem chữ ký đã được tạo thành công hay không và in ra thông báo tương ứng.
* Chữ ký và thông điệp sau đó được gửi đến hệ thống hoặc bên thứ ba.
* Hệ thống hoặc bên thứ ba sử dụng hàm verify\_signature() để xác minh tính hợp lệ của chữ ký bằng cách sử dụng khóa công khai. Kết quả của quá trình kiểm tra sẽ được in ra màn hình.

*Hình 12: Quy trình thực hiện*

## 3.3 Thảo luận kết quả

### 3.3.1 So sánh và đánh giá phương pháp thuật toán chữ ký số trong thương mại điện tử

Với sự bùng nổ của các giao dịch trên sàn thương mại điện tử, việc sử dụng chữ ký số trong TMĐT trở nên vô cùng quan trọng, giúp đảm bảo tính bảo mật và xác thực giao dịch trực tuyến. Chữ ký số không chỉ giúp người tiêu dùng tin tưởng hơn khi mua sắm qua mạng mà còn giúp doanh nghiệp chứng minh tính hợp pháp của hợp đồng và giao dịch điện tử. Sử dụng chữ ký số trong TMĐT cần tuân thủ các quy định pháp luật, đảm bảo tính chính xác và hợp pháp, từ đó đảm bảo an toàn cho các bên tham gia giao dịch. Sau đây là 3 phương pháp thuật toán chữ ký số phổ biến trong TMĐT:

*Bảng 1: So sánh và đánh giá phương pháp thuật toán chữ ký số*

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Chữ ký số RSA (RSA Digital Signature)** | **Thuật toán DSA (Digital Signature Algorithm)** | **Thuật toán ECDSA (Elliptic Curve Digital Signature Algorithm)** |
| **Ưu điểm** | **Bảo mật cao**: RSA là một trong những thuật toán chữ ký số an toàn và phổ biến nhất hiện nay.  **Tính linh hoạt**: Có thể dễ dàng tích hợp vào các hệ thống thương mại điện tử khác nhau.  **Tiêu chuẩn hóa**: Được hỗ trợ rộng rãi và được công nhận bởi nhiều tổ chức và tiêu chuẩn. | **Được tiêu chuẩn hóa**: DSA là một thuật toán chữ ký số đã được tiêu chuẩn hóa và được sử dụng trong nhiều ứng dụng khác nhau.  **An toàn**: Khi được sử dụng đúng cách, DSA cung cấp mức độ bảo mật cao.  **Hiệu suất tốt**: khi so với RSA trong quá trình ký số. | **Hiệu suất cao**: So với RSA, ECDSA cung cấp hiệu suất tốt hơn, đặc biệt là trong môi trường có tài nguyên hạn chế.  **Kích thước nhỏ hơn**: Kích thước chữ ký và khóa trong ECDSA thường nhỏ hơn so với RSA, giảm chi phí lưu trữ và truyền thông. |
| **Nhược điểm** | **Tốc độ xử lý**: Một số trường hợp yêu cầu xử lý nhanh có thể gặp khó khăn do tính toán phức tạp của RSA.  **Kích thước chữ ký**: RSA có kích thước chữ ký lớn hơn so với một số thuật toán khác, gây ra chi phí lưu trữ cao hơn. | **Giới hạn về sử dụng:** DSA có một số hạn chế về tính linh hoạt và khả năng sử dụng so với các thuật toán khác như RSA và ECDSA.  **Kích thước cố định:** DSA yêu cầu một kích thước khóa cố định, không linh hoạt như ECDSA. | **Phức tạp hơn trong triển khai:** ECDSA đòi hỏi kiến thức cao hơn trong việc triển khai và quản lý so với RSA.  **Chưa phổ biến rộng rãi:** Mặc dù được công nhận là một thuật toán mạnh mẽ, nhưng ECDSA chưa được sử dụng rộng rãi như RSA trong thực tế. |

Mỗi phương pháp thuật toán chữ ký số đều có những ưu và nhược điểm riêng, tùy thuộc vào yêu cầu cụ thể của hệ thống thương mại điện tử và ngữ cảnh triển khai. Việc lựa chọn phương pháp phù hợp trong thương mại điện tử phụ thuộc vào các yếu tố sau:

* Mức độ an toàn: Với RSA thì độ dài khóa cần phải tăng lên để duy trì cùng mức độ bảo mật, dẫn đến chi phí và tài nguyên tính toán tăng. Với DSA và ECDSA cần lưu ý trong việc tạo và quản lý khóa để tránh các vấn đề an toàn.
* Tính thuận tiện: RSA được phổ biến và được hỗ trợ rộng rãi trong các hệ thống và thư viện mã nguồn mở, việc triển khai và tích hợp cũng đơn giản hơn so với các thuật toán khác. Còn DSA và ECDSA thường được sử dụng trong các chuẩn chữ ký số và các hệ thống có yêu cầu ký số cụ thể.
* Chi phí: RSA cần sử dụng khóa có độ dài lớn để đảm bảo bảo mật, dẫn đến yêu cầu tài nguyên tính toán và lưu trữ cao hơn. DSA và ECDSA yêu cầu tài nguyên tính toán và lưu trữ thấp hơn so với RSA do độ dài khóa ngắn hơn, dẫn đến chi phí giảm.

Tóm lại, việc lựa chọn phương pháp ký điện tử phù hợp trong thương mại điện tử cần được cân nhắc kỹ lưỡng, tùy thuộc vào ngữ cảnh, yêu cầu và các yếu tố như mức độ an toàn cần thiết, yêu cầu về tính thuận tiện và chi phí.

### 3.3.2 Đề xuất cải tiến và hướng phát triển trong tương lai

* Nâng cao độ tin cậy của chữ ký số: Cần có những giải pháp để nâng cao độ tin cậy của chữ ký số, chẳng hạn như sử dụng các thuật toán ký số mạnh hơn và các cơ chế xác thực danh tính đáng tin cậy hơn.
* Đơn giản hóa việc sử dụng chữ ký số: Cần có những giải pháp để đơn giản hóa việc sử dụng chữ ký số, chẳng hạn như tích hợp chữ ký số vào các trình duyệt web và các ứng dụng phổ biến khác.
* Giảm chi phí sử dụng chữ ký số: Cần có những giải pháp để giảm chi phí sử dụng chữ ký số, chẳng hạn như phát triển các mô hình cấp chứng chỉ số miễn phí hoặc giá rẻ.

### 3.3.3 Một số giải pháp cụ thể có thể được áp dụng

* Sử dụng các thuật toán ký số dựa trên mật mã lượng tử: Các thuật toán ký số dựa trên mật mã lượng tử có độ an toàn cao hơn nhiều so với các thuật toán ký số truyền thống.
* Sử dụng mô hình Blockchain (Công nghệ chuỗi khối): Tích hợp chữ ký số với công nghệ blockchain giúp tăng cường tính toàn vẹn và không thay đổi của dữ liệu, cung cấp một phương thức phi tập trung và minh bạch cho quá trình ký số.
* Sử dụng các cơ chế xác thực danh tính dựa trên trí tuệ nhân tạo (AI): Các cơ chế xác thực danh tính dựa trên trí tuệ nhân tạo có thể xác thực danh tính của người dùng một cách đáng tin cậy hơn.
* Tích hợp chữ ký số vào các ứng dụng phổ biến: Các ứng dụng phổ biến như trình duyệt web và các ứng dụng email có thể được tích hợp với chữ ký số để giúp người dùng sử dụng chữ ký số một cách dễ dàng hơn.
* Phát triển các mô hình cấp chứng chỉ số miễn phí hoặc giá rẻ: Các cơ quan cấp chứng chỉ có thể phát triển các mô hình cấp chứng chỉ số miễn phí hoặc giá rẻ để giúp giảm chi phí sử dụng chữ ký số.

Với những giải pháp này, nhóm tác giả tin rằng chữ ký số sẽ trở nên an toàn, tin cậy và dễ sử dụng hơn, góp phần thúc đẩy sự phát triển của thương mại điện tử.

# 

# **KẾT LUẬN**

Chữ ký số hiện nay còn khá mới mẻ đối với phần lớn Doanh Nghiệp Việt Nam, đặc biệt là trong Thương mại điện tử. Chữ ký số đóng vai trò quan trọng, như một công cụ đảm bảo tính bảo mật và xác thực. Bảo đảm tính toàn vẹn của thông tin, tạo nên một môi trường giao dịch an toàn và tin cậy.

Về mặt lý thuyết: Đề tài trình đã bày được ý nghĩa và sự cần thiết của chữ ký số; khái niệm, đặc điểm, vai trò của chữ ký số, thương mại điện tử, đánh giá được tầm quan trọng của chữ ký số trong thương mại điện tử cũng như tính bảo mật thông tin trong giao dịch.

Về kỹ thuật và ứng dụng: Xác định được các thuật toán, các dữ liệu trong thực thi vận hành chữ ký số. Cấu trúc khóa và mô hình lưu hành thông tin dữ liệu. Ứng dụng được nguyên lý và kỹ thuật sử dụng mã khóa công khai, khóa bí mật bằng công cụ lập trình với ngôn ngữ Python. Đánh giá tính an toàn bảo mật qua quá trình thực thi ứng dụng.

Mặc dù đã hết sức cố gắng nhưng trình độ chuyên môn và thời gian thực hiện đề tài còn hạn chế, cũng như mức độ phức tạp của đề tài, nên kết quả đạt được còn gặp phải một số khiếm khuyết.

Hướng phát triển đề tài: Tiếp tục hoàn thiện các chức năng để tăng tính hiệu quả và độ an toàn. Trong tương lai, có thể kết hợp với các công nghệ bảo mật khác để tăng cường hiệu suất và tính linh hoạt của hệ thống.

# 

# **TÀI LIỆU THAM KHẢO**

1. Nguyễn Hoàng Tùng (2009). Ứng dụng chữ ký số trong thương mại điện tử, Khóa luận Khoa Kỹ thuật - Công nghệ - Môi trường, Trường Đại học An Giang.
2. Ths Nguyễn Quang Huy (2022). Ứng dụng chữ ký số trong thương mại điện tử, Tạp chí Công Thương, số 28.
3. Trần Quang Thuận (2010). Nghiên cứu và xây dựng hạ tầng khóa công khai, Khóa luận Trường Đại học Công nghệ, Đại học Quốc gia Hà Nội.
4. Ths Nguyễn Thị Kim Huệ (2015). Chữ ký số trong giao dịch thương mại điện tử, Luận văn Trường Đại học Công nghệ thông tin và Truyền thông, Đại học Thái Nguyên.