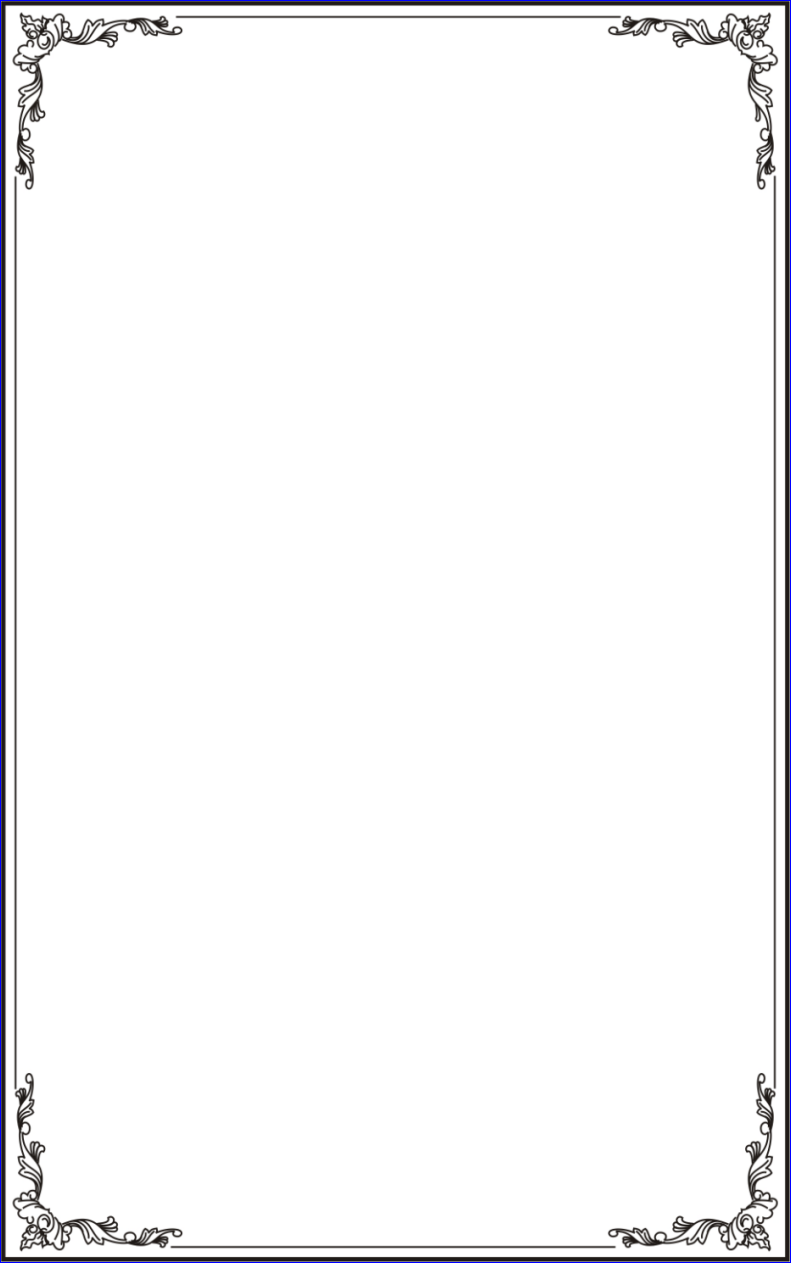
**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**

**KHOA CÔNG NGHỆ THÔNG TIN**

**----------------------------**

BÁO CÁO BÀI TẬP LỚN THUỘC HỌC PHẦN:

AN TOÀN VÀ BẢO MẬT THÔNG TIN

**Đề tài:** **Ứng dụng của RSA trong chữ ký số điện tử và Demo sản phẩm minh họa.**

Giảng viên hướng dẫn: TS. Lê Thị Anh

Lớp: 20231IT6001001Nhóm: 15

Sinh viên thực hiện:Phạm Thị Liễu – 2021608600

Nguyễn Công Mạnh – 2021606960

Ngô Văn Minh – 2020600435

Đỗ Thị Thanh Thảo – 2021606971

Chu Quốc Vương - 2021606512

***Hà nội, năm 2023***

LỜI MỞ ĐẦU

Để hoàn thành học phần An toàn và bảo mật thông tin, chúng em đã nhận được rất nhiều sự giúp đỡ và hướng dẫn tận tình của cô Lê Thị Anh. Các thành viên trong nhóm đã nỗ lực hết sức để hoàn thành bài tập lớn một cách tốt nhất, tuy nhiên vì kiến thức và kinh nghiệm còn hạn chế nên khó tránh khỏi những thiếu sót. Chúng em rất mong nhận được những lời đóng góp, nhận xét từ cô để có thể rút ra được bài học, giúp bài tập lớn được hoàn thiện hơn nữa.

Chúng em xin chân thành cảm ơn!

1. Lý do chọn đề tài

Mật mã học là một trong những vấn đề quan trọng trong lĩnh vực bảo mật và an toàn thông tin. Đặc biệt trong hệ thống mã hóa khóa công khai thì việc xác thực thông tin là vô cùng quan trọng, để giải quyết điều đó, người ta đã đưa ra một cách giải quyết hiệu quả là chữ ký số điện tử.

Trong thời đại mạng lưới thông tin phát triển với tốc độ nhanh chóng và mạnh mẽ hiện nay, nhu cầu bảo mật thông tin trở thành một ưu tiên hàng đầu. Chữ ký số điện tử không chỉ đảm bảo tính toàn vẹn của thông tin mà còn thể hiện tính xác thực của người gửi. Điều này thúc đẩy chúng ta cần tìm hiểu sâu hơn về cách mà thuật toán RSA hoạt động và tại sao nó trở thành một trong những phương pháp phổ biến nhất cho việc tạo chữ ký số.

Hệ mã hóa RSA - hệ mã hóa điển hình của mật mã công khai cùng với hàm băm mật mã học một chiều chính là những công cụ chính trong việc tạo ra chữ ký số điện tử. Việc áp dụng kiến thức về RSA vào việc tạo và xác minh chữ ký số có ứng dụng rất rõ ràng trong thực tế, từ việc xác minh giao dịch tài chính đến việc bảo vệ thông tin cá nhân.

Nắm vững về RSA không chỉ là vấn đề lý thuyết mà còn liên quan đến phát triển kỹ năng nghiên cứu và phân tích, giúp chúng ta hiểu rõ hơn về cơ chế hoạt động của hệ thống bảo mật trong thế giới kỹ thuật số ngày nay. Đây là cơ hội để rèn luyện khả năng tư duy phản biện và áp dụng kiến thức vào các vấn đề thực tế, đặc biệt trong lĩnh vực an ninh thông tin ngày càng phức tạp. Vì vậy, xuất phát từ nhu cầu thực tiễn, chúng em chọn đề tài báo cáo môn An toàn và bảo mật thông tin: **“*Ứng dụng của RSA trong chữ ký số điện tử*”.**

1. Mục đích

Tập trung tìm hiểu về Ứng dụng của RSA trong chữ ký số điện tử, từ thuật toán đến việc áp dụng thực tiễn trong việc bảo vệ tính toàn vẹn và xác thực thông tin trong môi trường kỹ thuật số.

1. Bố cục chính

Ngoài phần mở đầu và kết luận, báo cáo được chia thành 3 chương:

* Chương 1: Tổng quan về chữ ký số điện tử
* Chương 2: Hệ mật mã hóa công khai RSA
* Chương 3: Phân tích và thiết kế chương trình
* Chương 4: Thực nghiệm và đánh giá

1. Phương pháp

* Tìm kiếm thông tin, thu thập tài liệu từ các nguồn uy tín như sách về mật mã học hay bài báo khoa học từ các hội thảo về an ninh mạng.
* Tìm hiểu, vận dụng và kế thừa một số các hàm mật mã đã có trên Internet hoặc tài liệu liên quan.
* Áp dụng các kiến thức đã được học từ học phần An toàn và bảo mật thông tin.

MỤC LỤC

[LỜI MỞ ĐẦU 1](#_Toc154322027)

[1. Lý do chọn đề tài 1](#_Toc154322028)

[2. Mục đích 2](#_Toc154322029)

[3. Bố cục chính 2](#_Toc154322030)

[4. Phương pháp 2](#_Toc154322031)

[MỤC LỤC 3](#_Toc154322032)

[Danh mục hình ảnh 4](#_Toc154322033)

[CHƯƠNG 1: TỔNG QUAN VỀ CHỮ KÝ SỐ ĐIỆN TỬ 5](#_Toc154322034)

[1.1. Giới thiệu chung 5](#_Toc154322035)

[1.2. Một số khái niệm 5](#_Toc154322036)

[1.3. Đặc điểm và vai trò của chữ ký số điện tử 6](#_Toc154322037)

[1.4. Kiến trúc chữ ký số tổng quát 7](#_Toc154322038)

[1.5. Một số điểm hạn chế 8](#_Toc154322039)

[CHƯƠNG 2: HỆ MẬT MÃ HÓA CÔNG KHAI RSA 10](#_Toc154322040)

[2.1 Giới thiệu 10](#_Toc154322041)

[2.2 Nguyên lý hoạt động cơ bản 11](#_Toc154322042)

[2.3 Giải thuật RSA 11](#_Toc154322043)

[2.4 Ứng dụng RSA trong chữ ký số điện tử 12](#_Toc154322044)

[CHƯƠNG 3: PHÂN TÍCH VÀ THIẾT KỂ CHƯƠNG TRÌNH 14](#_Toc154322045)

[3.1 Lược đồ chữ ký số RSA 14](#_Toc154322046)

[3.2 Thiết kế chương trình ứng dụng 17](#_Toc154322047)

[3.3 Nhược điểm của chữ ký số sử dụng RSA 19](#_Toc154322048)

[CHƯƠNG 4: THỰC NGHIỆM VÀ ĐÁNH GIÁ 21](#_Toc154322049)

[4.1 Thực nghiệm chương trình 21](#_Toc154322050)

[4.2 Đánh giá 23](#_Toc154322051)

[KẾT LUẬN 24](#_Toc154322052)

[TÀI LIỆU THAM KHẢO 25](#_Toc154322053)

Danh mục hình ảnh

Hình 1. Kiến trúc chữ ký số tổng quát 7

Hình 2. Ví dụ minh họa 10

Hình 3. Sơ đồ giải thuật RSA 11

Hình 4. Lược đồ chữ ký số RSA 14

Hình 5. Sơ đồ thuật toán tạo chữ ký 14

Hình 6. Sơ đồ thuật toán chứng thực chữ ký 15

Hình 7. Thuật toán SHA-1 16

Hình 8. Hàm tạo khóa 18

Hình 9. Mã hóa 18

Hình 10. Giải mã 18

Hình 11. SHA-1 19

Hình 12. Giao diện chương trình ứng dụng 21

Hình 13. Nhấn chọn tạo khóa 22

Hình 14. Nhấn chọn tạo chữ ký 22

Hình 15. Trường hợp chữ ký toàn vẹn 23

Hình 16. Trường hợp chữ ký bị thay đổi 23

CHƯƠNG 1: TỔNG QUAN VỀ CHỮ KÝ SỐ ĐIỆN TỬ

* 1. Giới thiệu chung

Chữ ký số điện tử là một phần quan trọng trong việc đảm bảo tính toàn vẹn, xác thực và bảo mật thông tin trong môi trường kỹ thuật số ngày nay. Nó thường được sử dụng để chứng minh nguồn gốc và sự xác thực của thông tin điện tử, tương tự như việc chữ ký trên giấy tờ vật lý.

Về cơ bản, chữ ký số điện tử là một tập hợp các dữ liệu mã hóa được tạo ra bằng các phương pháp mã hóa đối xứng hoặc không đối xứng, kèm theo thông tin cụ thể về người tạo chữ ký và dữ liệu đã được ký. Chữ ký số điện tử có hai mục tiêu chính:

**Tính Xác Thực:** Nó giúp xác định rõ người tạo ra thông tin, đảm bảo tính xác thực và không bị sửa đổi của dữ liệu.

**Tính Toàn Vẹn:** Chữ ký số cũng bảo vệ tính toàn vẹn của dữ liệu, cho phép nhận biết bất kỳ sự thay đổi nào trong thông tin đã ký.

Kỹ thuật của chữ ký số điện tử thường dựa trên việc sử dụng các phép toán số học phức tạp và các thuật toán mã hóa như RSA, DSA, hoặc ECDSA để tạo ra và xác minh chữ ký.

* 1. Một số khái niệm

**Chữ ký số (Digital Signature)**: là một chuỗi dữ liệu liên kết với một thông điệp (message) và thực thể tạo ra thông điệp.

**Giải thuật tạo ra chữ ký số (Digital Signature generation algorithm)** là một phương pháp sinh chữ ký số.

**Giải thuật kiểm tra chữ ký số (Digital Signature verification algorithm )** là một phương pháp xác minh tính xác thực của chữ ký số, có nghĩa là nó thực sự được tạo ra bởi 1 bên chỉ định.

**Một hệ chữ ký số (Figital Signature Scheme)** bao gồm giải thuật tạo chữ số và giải thuật kiểm tra chữ kỹ số.

**Quá trình tạo chữ ký số (Digital Signature signing process)** bao gồm:

* Giải thuật tạo chữ ký số.
* Phương pháp chuyển dữ liệu thông điệp thành dạng có thể ký được

**Quá trình kiểm tra chữ ký số (Digital signature verification process)** gồm:

* Giải thuật kiểm tra chữ ký số, và
* Phương pháp khôi phục dữ liệu từ thông điệp

**Hàm băm (Hash Funtion)** là hàm toán học chuyển đổi thông điệp (message) có độ dài bất kỳ (hữu hạn) thành một dãy bít có độ dài cố định (tùy thuộc vào thuật toán băm). Dãy bít này được gọi là thông điệp rút gọn.(message disgest) hay giá trị băm (hash value), đại diện cho thông điệp ban đầu.

Hàm băm SHA-1: Thuật toán SHA-1 nhận thông điệp ở đầu vào có chiều dài k<264 bit, thực hiện xử lý và đưa ra thông điệp thu gọn (message digest) có chiều dài cố định 160 bits. Quá trình tính toán cũng thực hiện theo từng khối 512bits, nhưng bộ đệm xử lý dùng 5 thanh ghi 32-bits. Thuật toán này chạy tốt với các bộ vi xử lý có cấu trúc 32 bits.

* 1. Đặc điểm và vai trò của chữ ký số điện tử

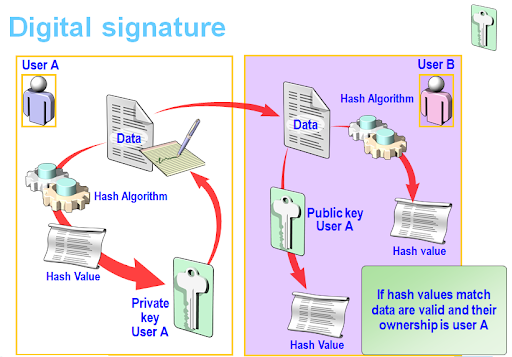
**Đặc điểm:**

* Khóa bí mật: Chỉ có người chủ mới biết
* Khóa công khai: Có thể truy cập thông qua phương tiện thông dụng vào bất cứ thời điểm nào. Chứa trong một thư mục công cộng, đảm bảo tính chính xác và không giả mạo.
* Chứng thư số: Công bố khóa công khai, được cấp phát bởi tổ chức có thẩm quyền
* Độ dài khóa: Tương ứng tính an toàn của kháo, có độ dài (thông dụng là 512, 1024, 2048, 4096, khóa càng dài mã càng chậm)
* Tính pháp lý: Được cấp phát theo quy trình an toàn với các thông số kỹ thuật đảm bảo được lưu trữ an toàn
* Tính khả dụng: Được lưu trong các thiết bị cá nhân như USB-token, smart card, ngày càng dễ sử dụng

**Vai Trò:**

* Tính xác thực: Chữ ký số điện tử là dấu hiệu cho sự xác thực của thông tin. Nó cho phép người nhận xác nhận rằng thông tin chưa bị sửa đổi và đến từ nguồn đã được xác thực.
* Tính toàn vẹn: Chữ ký số cũng bảo vệ tính toàn vẹn của dữ liệu. Bất kỳ sự thay đổi nào trong dữ liệu đã ký sẽ làm thay đổi chữ ký số, cung cấp cảnh báo về sự thay đổi này.
* Đảm bảo an toàn giao dịch: Trong các giao dịch trực tuyến, chữ ký số điện tử chính là cơ chế quan trọng giúp đảm bảo tính xác thực và bảo mật của giao dịch giữa các bên.
* Phòng ngừa xâm nhập: Nó giúp ngăn chặn các loại tấn công như tin tặc hoặc sửa đổi dữ liệu trong quá trình truyền tải.

Chữ ký số điện tử không chỉ là một phương tiện bảo mật thông tin mà còn là yếu tố quyết định trong việc xác định tính tin cậy và an toàn của dữ liệu trong môi trường kỹ thuật số ngày nay.

* 1. Kiến trúc chữ ký số tổng quát

Hình 1. Kiến trúc chữ ký số tổng quát

***Quá trình ký (bên gửi)***

* Tính toán chuỗi đại diện (message digest/ hash value) của thông điệp sử dụng một giải thuật băm (Hashing algorithm)
* Chuỗi đại diện được ký sử dụng khóa riêng (Private key) của người gửi và 1 giải thuật tạo chữ ký (Signature/ Encryption algorithm). Kết quả chữ ký số (Digital signature) của thông điệp hay còn gọi là chuỗi đại diện được mã hóa (Encryted message digest)
* Thông điệp ban đầu (message) được ghép với chữ ký số( Digital signature) tạo thành thông điệp đã được ký (Signed message)
* Thông điệp đã được ký (Signed message) được gửi cho người nhận

***Quá trình kiểm tra chữ ký (bên nhận)***

* Tách chữ ký số và thông điệp gốc khỏi thông điệp đã ký để xử lý riêng;
* Tính toán chuỗi đại diện MD1 (message digest) của thông điệp gốc sử dụng giải thuật băm (là giải thuật sử dụng trong quá trình ký)
* Sử dụng khóa công khai (Public key) của người gửi để giải mã chữ ký số -> chuỗi đại diện thông điệp MD2
* So sánh MD1 và MD2:
* Nếu MD1 =MD2 -> chữ ký kiểm tra thành công. Thông điệp đảm bảo tính toàn vẹn và thực sự xuất phát từ người gửi (do khóa công khai được chứng thực).
* Nếu MD1 <>MD2 -> chữ ký không hợp lệ. Thông điệp có thể đã bị sửa đổi hoặc không thực sự xuất phát từ người gửi.
  1. Một số điểm hạn chế

Chữ ký số đóng vai trò quan trọng trong việc xác định địa vị pháp lý của tài liệu số, giúp xác định tính nguyên gốc, tác giả và bảo đảm tính toàn vẹn của tài liệu. Nó giúp khẳng định giá trị pháp lý của văn bản điện tử, tương đương với tài liệu giấy. Tuy nhiên, chữ ký số cũng có những hạn chế:

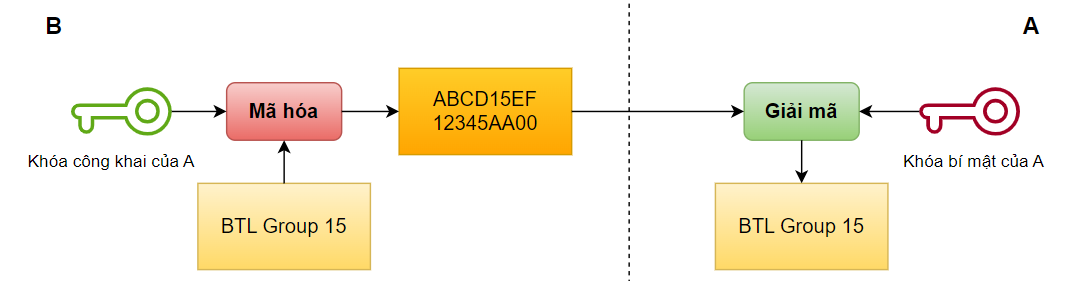
* Sự lệ thuộc vào máy móc và chương trình phần mềm: chữ ký số là một chương trình phần mềm máy tính. Để kiểm tra tính xác thực của chữ ký cần có hệ thống máy tính và phần mềm tương thích
* Vấn đề bản gốc, bản chính: Với văn bản điện tử đã được ký bằng chữ ký số, người ta có thể copy lại và bản copy từ bản chính (hoặc bản copy từ bản copy) không có gì khác biệt so với bản chính duy nhất được ký. Đây là thách thức đối với công tác văn bản và cả nền hành chính. Khái niệm bản gốc, bản chính trong văn bản hành chính sẽ phải xem xét lại đối với văn bản điện tử.
* Sự có thời hạn của chữ ký điện tử: Chữ ký điện tử là chương trình phần mềm được cấp có thời hạn cho người sử dụng. Về lý thuyết, văn bản sẽ có hiệu lực pháp lý khi được ký trong thời hạn sử dụng của chữ ký. Tuy nhiên, thực tế hiệu lực pháp lý của văn bản hoàn toàn có thể bị nghi ngờ khi chữ ký số hết thời hạn sử dụng.
* Tính bảo mật không tuyệt đối: chữ ký số là một bộ mật mã được cấp cho người sử dụng, đây là phần mềm máy tính không phụ thuộc vào vật mang tin nên không có khả năng tách biệt khỏi chủ nhân của chữ ký. Có thể tồn tại một số nhóm đối tượng có thể có được mật mã như: bộ phận cung cấp phần mềm, bộ phận cài đặt phần mềm, những người có thể sử dụng máy tính có cài đặt phần mềm, mật mã có thể bị đánh cắp hoặc được chuyển giao.

CHƯƠNG 2: HỆ MẬT MÃ HÓA CÔNG KHAI RSA

* 1. Giới thiệu

RSA là một **thuật toán mã hóa bất đối xứng** được sử dụng rộng rãi để bảo mật dữ liệu, đặc biệt là dữ liệu truyền qua Internet. Được phát triển bởi Ron Rivest, Adi Shamir và Leonard Adleman vào năm 1997, RSA sử dụng hai khóa khác nhau: khóa công khai (được chia sẻ rộng rãi) và khóa riêng tư (được giữ bí mật). Cả hai khóa này đều có thể được sử dụng để mã hóa tin nhắn.

RSA hoạt động như một cơ chế đóng/mở cửa, sử dụng khóa công khai và khóa riêng tư để mã hóa và giải mã tin nhắn. Điều này đã khiến RSA trở thành thuật toán bất đối xứng phổ biến nhất, với các ưu điểm về bảo mật, toàn vẹn và xác thực. RSA được sử dụng trong nhiều giao thức như SSH, OpenPGP, S/MIME, SSL/TLS và cũng được sử dụng trong các trình duyệt và phần mềm. Xác minh chữ ký RSA là một trong những hoạt động thường xuyên nhất trong các hệ thống kết nối Internet.

**Ví dụ mô phỏng trực quan một hệ mật mã khoá công khai**: B muốn gửi cho A một thông tin mật mà B muốn duy nhất A có thể đọc được. Để làm được điều này, A gửi cho B một chiếc hộp có khóa đã mở sẵn (Khóa công khai) và giữ lại chìa khóa. B nhận chiếc hộp, cho vào đó một tờ giấy viết thư bình thường và khóa lại (như loại khoá thông thường chỉ cần sập chốt lại, sau khi sập chốt khóa ngay cả B cũng không thể mở lại được- không đọc lại hay sửa thông tin trong thư được nữa). Sau đó B gửi chiếc hộp lại cho A. A mở hộp với chìa khóa của mình và đọc thông tin trong thư. Trong ví dụ này, chiếc hộp với khóa mở đóng vai trò khóa công khai, chiếc chìa khóa chính là khóa bí mật.

Hình 2. Ví dụ minh họa

* 1. Nguyên lý hoạt động cơ bản

Trong mật mã RSA, việc tạo public key và private key là phần quan trọng và phức tạp nhất. Đầu tiên, hai số nguyên tố lớn **p** và **q** được tạo ra ngẫu nhiên bằng thuật toán Rabin-Miller. Sau đó, module **n = p\*q** được tính toán và giá trị của **n** sẽ được dùng cho cả public key và private key.

Tiếp theo, cần tính giá trị hàm số Euler **φ(n) = (p - 1)\*(q - 1)**. Chọn một số tự nhiên e sao cho **(e, φ(n)) = 1**, tức là **e** và **φ(n**) là hai số nguyên tố cùng nhau.

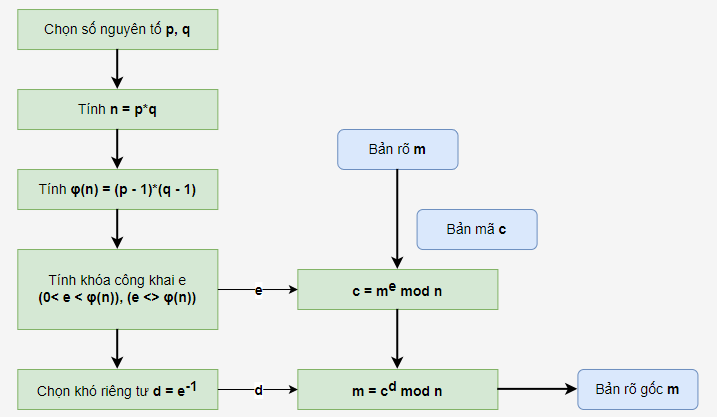
Public key bao gồm module **n** và số mũ công khai **e**. Người ta thường chọn **e** nhỏ để giải mã nhanh, thông thường **e = 65537**.

Private key gồm mô đun **n** và số mũ riêng **d**, được tính toán bằng thuật toán Euclide mở rộng để tìm phép nhân nghịch đảo đối với tâm của **n**, sao cho **(d\*e) mod φ(n) = 1**.

CT mã hóa một thông điệp **m** thành một thông điệp mã hóa **c= me mod n**.

CT giải mã thông điệp mã hóa **c** trở lại thông điệp gốc **m = cd mod n**.

* 1. Giải thuật RSA

Sơ đồ giải thuật RSA được dùng trong việc tạo khóa, mã hóa và giải mã:

Hình 3. Sơ đồ giải thuật RSA

* Tạo khóa

|  |  |
| --- | --- |
| **Lý thuyết** | **Ví dụ** |
| Bước 1: tạo 2 số nguyên tố lớn ngẫu nhiên p và q | Chọn 2 số nguyên tố là 23 và 41 |
| Bước 2: tính n = p\*q  và φ(n) = (p-1)(q-1) | n = 23\*41 = 943  φ(n) =22\*40 = 880 |
| Bước 3: chọn một số ngẫu nhiên e  (0< e< φ(n)) sao cho UCLN(e, φ(n)) = 1 | Chọn e = 7 vì UCLN(7, 880) = 1 |
| Bước 4: tính d = e-1 bằng cách dùng thuật toán Euclide: tìm số tự nhiên x sao cho d = (x\* φ(n)+1)/e | D = (x\* φ(n)+1)/e  => 7d = 1 + 880x  => d = 503 và x = 4 |
| Bước 5: Khóa công khai là n và e  Khóa bí mật là d | Có n = 943 và e = 7  d = 503 |

* Mã hóa và giải mã

|  |  |
| --- | --- |
| **Lý thuyết** | **Ví dụ** |
| Bước 1: B nhận khóa công khai của A | B nhận khóa công khai n = 943 và e = 7 |
| Bước 2: B biểu diễn thông tin cần gửi thành số m (0 <= m <= n-1) | Thông tin cần gửi m = 35 |
| Bước 3: tính c = me mod n | c = 357 mod 943 |
| Bước 4: gửi c cho A | c = 545 |
| Bước 5: giải mã, tính m = cd mod n  => m là thông tin A nhận được | m = 545503 mod 943  => m = 35 |

* 1. Ứng dụng RSA trong chữ ký số điện tử

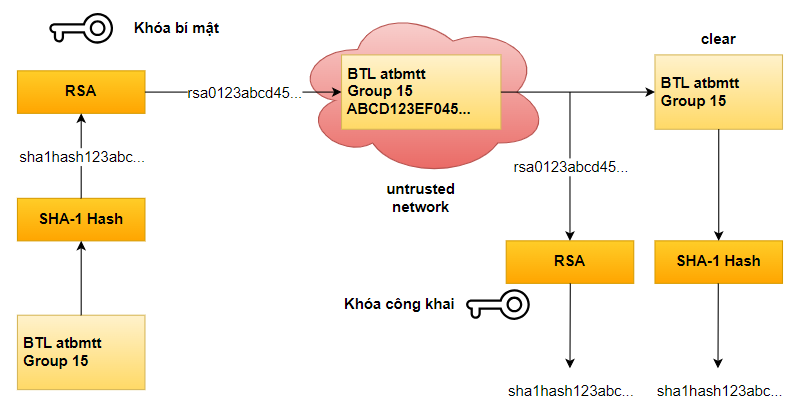
RSA đóng vai trò quan trọng trong việc tạo ra chữ ký số điện tử, giúp tăng cường bảo mật và đảm bảo tính toàn vẹn của dữ liệu:

* Xác định nguồn gốc: RSA cho phép tạo chữ ký với khóa bí mật mà chỉ người chủ mới biết. Điều này giúp xác định nguồn gốc của thông điệp, đảm bảo rằng nó đến từ người gửi chính xác.
* Bảo đảm tính toàn vẹn của dữ liệu: Tin nhắn được ký bằng khóa bí mật rất khó có thể bị giả mạo. Điều này giúp bảo đảm tính toàn vẹn của dữ liệu, đảm bảo rằng nó không bị thay đổi trong quá trình truyền.
* Không thể phủ nhận: Người gửi không thể phủ nhận việc đã gửi thông điệp sau khi đã ký nó bằng khóa bí mật của mình.
* Ứng dụng trong thực tế: RSA được sử dụng rộng rãi trong các hoạt động thương mại điện tử. Nó cũng được sử dụng để bảo mật dữ liệu khi người dùng thực hiện các giao dịch ngân hàng, tăng cường độ bảo mật của hệ thống thông tin truyền thông, an ninh mạng và trong các hoạt động pháp lý, tài liệu chính phủ, hợp đồng kinh doanh,...

CHƯƠNG 3: PHÂN TÍCH VÀ THIẾT KỂ CHƯƠNG TRÌNH

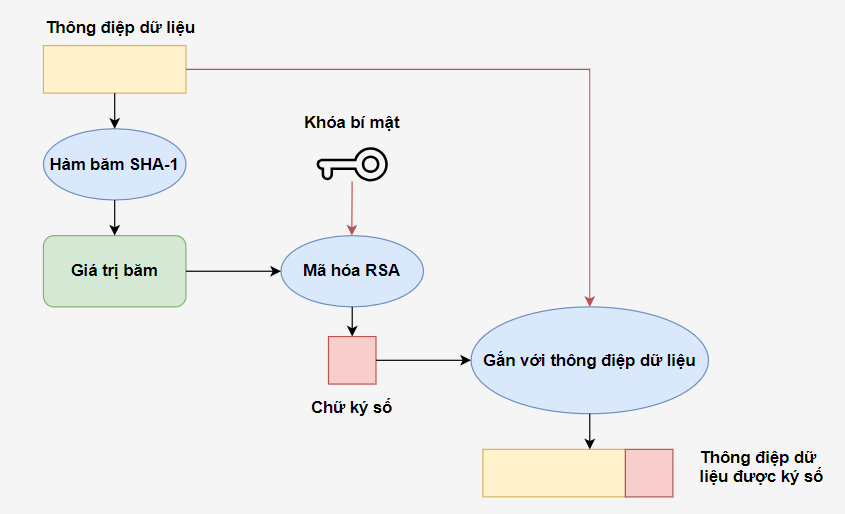
1. Lược đồ chữ ký số RSA

Độ an toàn của lược đồ chữ ký RSA dựa vào độ an toàn của hệ mã RSA. Lược đồ bao gồm chữ ký số kèm theo bản rõ và khôi phục thông điệp từ chữ ký số.



Hình 4. Lược đồ chữ ký số RSA

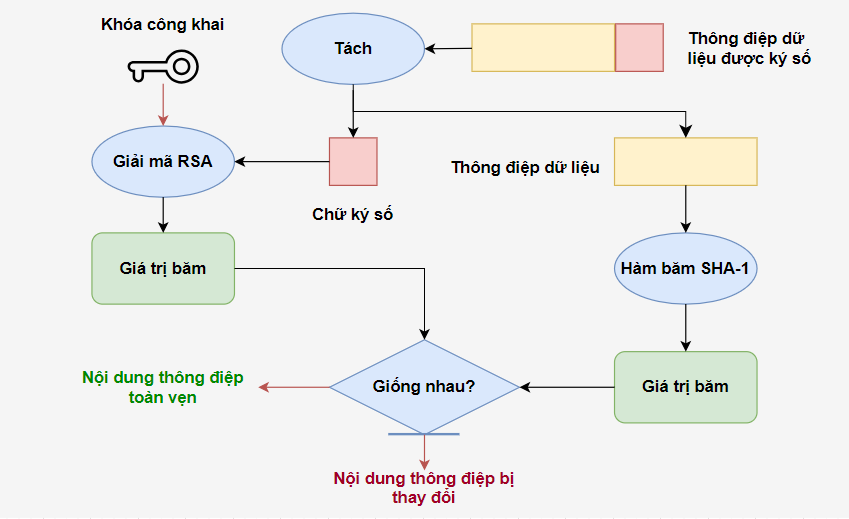
1. ***Thuật toán tạo chữ ký số RSA***



Hình 5. Sơ đồ thuật toán tạo chữ ký

* Tính toán chuỗi đại diện của thông điệp dữ liệu sử dụng hàm băm SHA-1
* Chuỗi đại diện được ký sử dụng khóa riêng (Khóa bí mật) của người gửi và giải thuật tạo chữ ký RSA. Kết quả chữ ký số của thông điệp dữ liệu hay còn gọi là chuỗi đại diện được mã hóa bởi giải thuật RSA
* Thông điệp dữ liệu ban đầu được ghép với chữ ký số tạo thành thông điệp dữ liệu đã được ký và được gửi cho người nhận

1. ***Thuật toán chứng thực chữ ký số RSA***

**

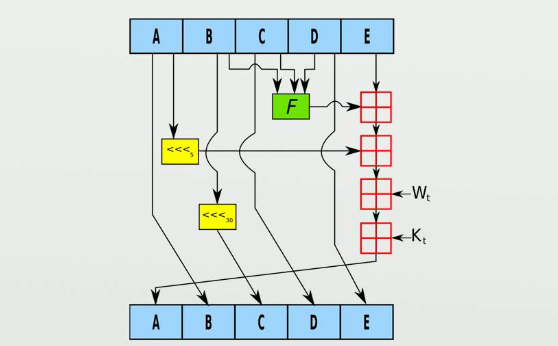
Hình 6. Sơ đồ thuật toán chứng thực chữ ký

* Tách chữ ký số RSA và thông điệp gốc khỏi thông điệp dữ liệu đã được ký để xử lý riêng;
* Tính toán chuỗi đại diện MD1 của thông điệp gốc sử dụng giải thuật băm (là giải thuật sử dụng trong quá trình ký là SHA-1)
* Sử dụng khóa công khai của người gửi để giải mã chữ ký số RSA tạo thành chuỗi đại diện thông điệp MD2
* So sánh MD1 và MD2:
  + Nếu MD1 = MD2 => chữ ký kiểm tra thành công. Thông điệp đảm bảo tính toàn vẹn và thực sự xuất phát từ người gửi (do khóa công khai được chứng thực).
  + Nếu MD1 <> MD2 => chữ ký không hợp lệ. Thông điệp có thể đã bị sửa đổi hoặc không thực sự xuất phát từ người gửi.

1. ***Thuật toán SHA-1***

**Định nghĩa**

SHA-1 viết tắt của Secure Hash Algorithm 1 là một thuật toán sử dụng hàm Cryptographic Hash để thu thập đầu vào và cho ra các giá trị Hash 160 bit (20byte). Trong đó, giá trị Hash này được gọi là Message Digest, nó bao gồm một chuỗi các số thập lục phân dài 40 chữ số.



Hình 7. Thuật toán SHA-1

SHA-1 đã được phát triển bởi Cơ quan An ninh Quốc gia Hoa Kỳ (NSA) và được công bố vào năm 1993. Ban đầu, nó được sử dụng rộng rãi trong các ứng dụng mật mã và bảo mật dữ liệu.

**Nguyên lý hoạt động**

SHA-1 (Secure Hash Algorithm 1) hoạt động bằng cách chuyển đổi một đoạn dữ liệu đầu vào thành một giá trị hash cố định có độ dài 160 bit (20 byte)

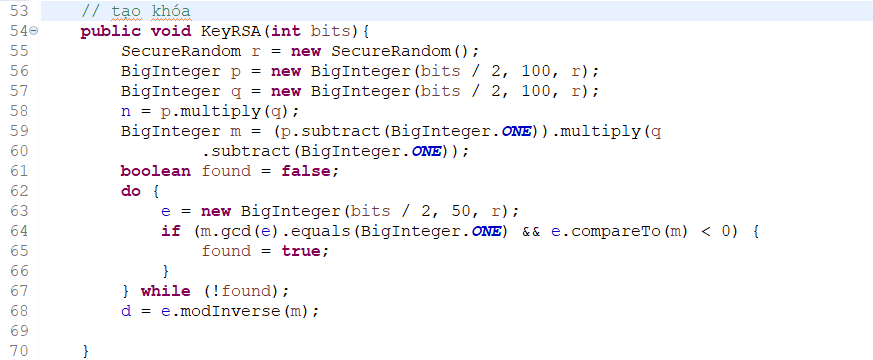
* Chuẩn bị dữ liệu đầu vào: Dữ liệu đầu vào (thường là một chuỗi byte) được chia thành các khối có độ dài cố định (512-bit hay 64-byte).
* Thêm bits padding: Để đảm bảo rằng dữ liệu có thể được chia thành các khối 512-bit, SHA-1 sẽ thêm các bits padding vào dữ liệu.
* Khởi tạo giá trị ban đầu (IV): SHA-1 sử dụng một bộ giá trị ban đầu cố định (Initialization Vector – IV) để bắt đầu quá trình hash.
* Xử lý từng khối dữ liệu: Dữ liệu đầu vào được chia thành các khối 512-bit và sau đó được xử lý một khối sau một khối.
* Xử lý trong các vòng lặp: Mỗi khối dữ liệu được chia thành năm 32-bit words, và trong mỗi vòng lặp của quá trình hash, các words này được sử dụng để tạo ra các giá trị tạm thời.
* Kết hợp các giá trị tạm thời: Cuối cùng, các giá trị tạm thời được kết hợp lại với nhau để tạo ra giá trị hash cuối cùng.
* Kết quả hash: Khi tất cả các khối dữ liệu đã được xử lý, giá trị hash cuối cùng được trả về là kết quả của quá trình SHA-1.

1. Thiết kế chương trình ứng dụng
2. ***Tổng quan***

* Công cụ hỗ trợ: Eclipse
* Ngôn ngữ lập trình: Java
* Thư viện GUI: Java Swing
* Sử dụng BigInteger trong gói java.math.\* cung cấp hầu hết các hàm dựng và các hàm số học cho phép thao tác thuận lợi với số nguyên lớn
* Một số hàm sử dụng:
  + Hàm dựng BigInteger (int bitLength, int certainty, Random rnd): sinh số nguyên tố ngẫu nhiên với số bit cho trước;
  + Hàm BigInteger add(BigInteger val): cộng 2 số nguyên lớn;
  + Hàm BigInteger subtract(BigInteger val): trừ 2 số nguyên lớn;
  + Hàm BigInteger multiply(BigInteger val): nhân 2 số nguyên lớn;
  + Hàm gcd(BigInteger val): Tìm USCLN của 2 số lớn
  + Hàm mod(BigInteger m): Tính modulo (phần dư) của phép chia nguyên;
  + Hàm BigInteger modInverse(BigInteger m): tính modulo nghịch đảo (this-1mod m);
  + Hàm BigInteger modPow(BigInteger exponent, BigInteger m): Tính (thisexponent mod m).

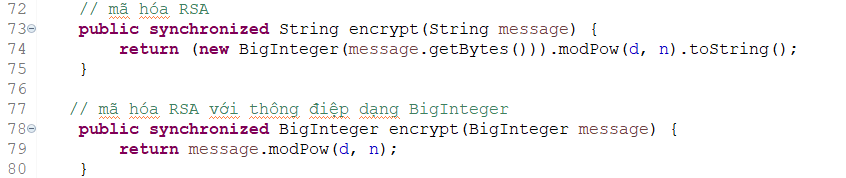
1. ***Chi tiết chương trình***

* Tạo khóa



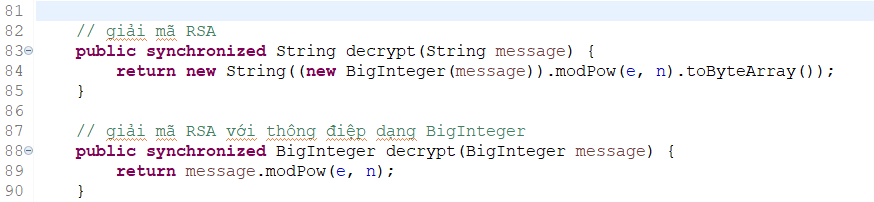
Hình 8. Hàm tạo khóa

* Mã hóa



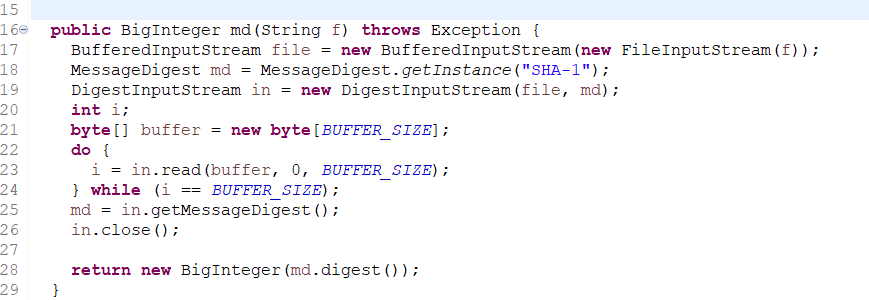
Hình 9. Mã hóa

* Giải mã



Hình 10. Giải mã

* Tính giá trị băm SHA-1 của một tệp dữ liệu



Hình 11. SHA-1

1. Nhược điểm của chữ ký số sử dụng RSA
2. ***Hiệu suất thực hiện***

Tốc độ thực hiện của hệ RSA là một trong những điểm yếu so với các hệ mật mã khóa đối xứng. Theo ước tính, thực hiện mã hóa và giải mã bằng hệ mật mã RSA chậm hơn 100 lần so với hệ mã khóa đối xứng DES (Khi thực hiện bằng phần mềm). Và chậm hơn 1000 lần so với DES (Khi thực hiện bằng phần cứng).

1. ***Chi phí và tốc độ***

* Chi phí: Để thực hiện thuật toán RSA phần lớn tốn chi phí thực hiện các phép tính cơ bản. Quá trình mã hóa, giải mã tương đương với chi phí thực hiện các phép tính lũy thừa module n. Để đảm bảo cho khóa bí mật được an toàn thì thường chọn mũ công khai e nhỏ hơn nhiều so với số mũ bí mật d, do đó chi phí thời gian để thực hiện mã hóa dữ liệu nhỏ hơn nhiều so với thời gian giải mã.
* Tốc độ: Tốc độ của RSA là một trong những điểm yếu của RSA so với các hệ mã đối xứng, so với hệ mã DSA thì RSA chậm hơn từ 100 đến 1000 lần, vì vậy RSA không được dùng để mã hóa khối lượng dữ liệu lớn mà thường dùng để mã hóa dữ liệu nhỏ.

1. ***Các dạng tấn công có thể gặp phải***

* Tấn công lặp: Simons và Norris đã chỉ ra rằng hệ thống RSA có thể bị tấn công khi sử dụng tấn công lặp liên tiếp. Đó là khi kẻ tấn công biết khóa công khai (e, n) và bản mã C thì anh ta có thể tính chuỗi các bản mã sau:

C1 = Ce (mod n) C2 = C1e (mod n) …………………

Ci = Ci-1e (mod n)

Nếu có một phần tử Cj trong chuỗi C1, C2, …, C, … sao cho Cj = C thì khi đó anh ta sẽ tìm được M = Cj-1 bởi vì:

Cj = Cj-1 (mod n)

C = Me (mod n)

* Kiểu tấn công module n dùng chung: Hệ thống RSA có thể bị tấn công khi sử dụng module n dùng chung, nếu một thông điệp M được mã hoá bằng hai khoá công khai e1 và e từ hai thành viên trong hệ thống thì được:

C1 = M e1 (mod n) và C2 = M e2 (mod n)

Sau đó người tấn công dùng thuật toán Euclide mở rộng: e¬1\*a +e2\*b = 1 sao cho gcd(e1, e2 ) = 1 => M được khôi phục lại: M = C1a . C2b mod n.

* Tấn công khi khóa công khai e nhỏ: Hastad đã đưa ra kiểu tấn công khi khoá công khai e nhỏ (e =3) của hệ mã công khai RSA:

Giả sử để gửi thông điệp M đến các người dùng P1, P2 …,Pk với khoá công khai là (ei , ni). A mã hoá M bằng khoá công khai (ei , ni) và gửi các bản mã Ci đến người dùng Pi, biết M < n với i = 1, 2,…, n. Ta có thể nghe trộm kết nối ra ngoài của A và thu thập được k bản mã Ci.

Giả sử các khoá công khai ei = 3 thì có thể khôi phục M nếu k ≥ 3.

Thực vậy, nếu có được C1, C2, C3 với C1= M3 mod ni; C2= M3 mod n2; C3= M3 mod n3 và gcd(ni, nj) = 1, i ≠ j. Áp dụng định lý số dư Trung Hoa với C1,C2,C3 tìm được: C’ thuộc Zn1n2n3 thỏa C’ = M3 mod n1n2n3

=> M3 là số nguyên. Vậy M= ∛(C^' )

CHƯƠNG 4: THỰC NGHIỆM VÀ ĐÁNH GIÁ

1. Thực nghiệm chương trình

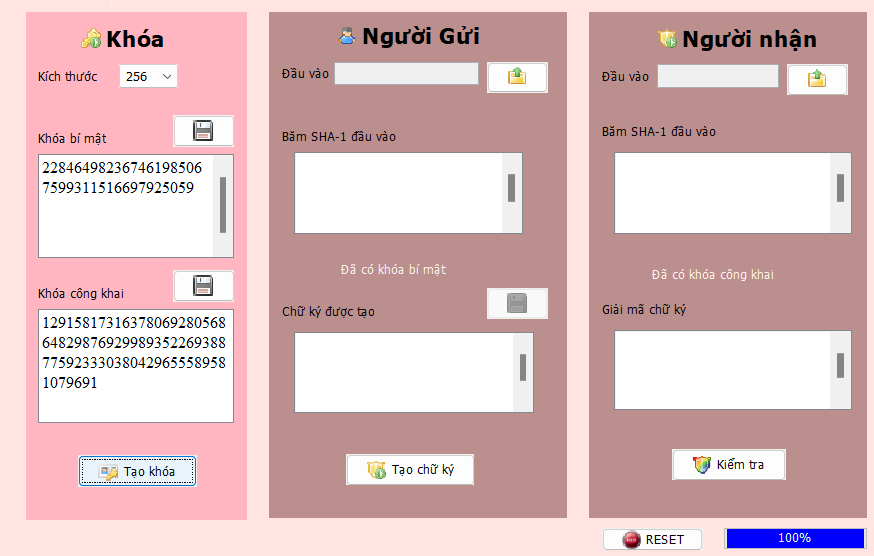
* Giao diện chính



Hình 12. Giao diện chương trình ứng dụng

* Tạo Khóa

Cho phép chọn kích thước khóa nhập khóa hoặc tạo khóa tự động.



Hình 13. Nhấn chọn tạo khóa

* Chọn file và tạo chữ ký số

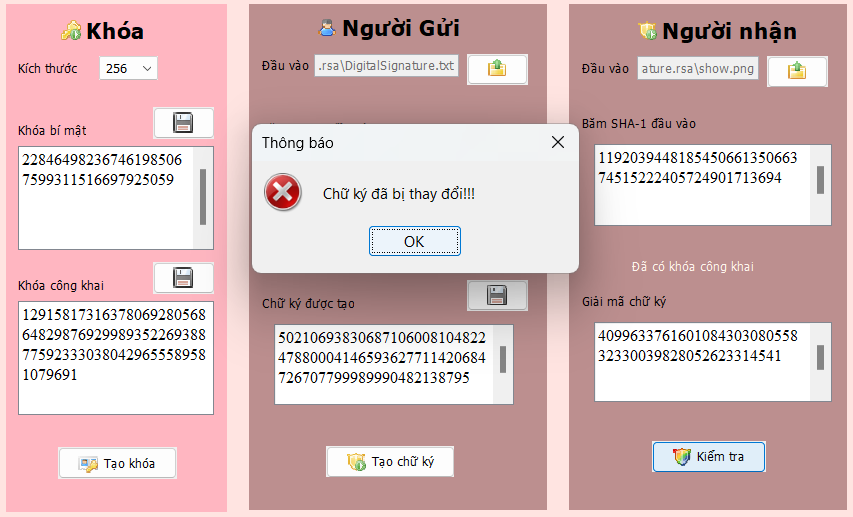


Hình 14. Nhấn chọn tạo chữ ký

* Kiểm tra tính toàn vẹn



Hình 15. Trường hợp chữ ký toàn vẹn



Hình 16. Trường hợp chữ ký bị thay đổi

1. Đánh giá

Chương trình ứng dụng mềm đã được hoàn thiện và có thể chạy bình thường. Các chức năng hoạt động ổn định và đúng với vai trò của nó.

KẾT LUẬN

Sau thời gian tìm hiểu và làm việc nghiêm túc dưới sự hướng dẫn của cô Lê Thị Anh, nhóm 15 chúng em đã hoàn thành cuốn báo cáo bài tập lớn với đề tài: “Ứng dụng RSA vào chữ ký số điện tử và demo sản phẩm minh họa” và đạt được một số kết quả như sau:

1. **Công viện hoàn thành**

* Tìm hiểu và trình bày được nội dung lý thuyết chung về chữ ký số điện tử và hệ mật mã hóa công khai RSA, các khái niệm, đặc điểm, nguyết lý hoạt động, phương pháp mã hóa.
* Tìm hiểu, phân tích và thiết kế chương trình ứng dụng RSA vào chữ ký số điện tử với chức năng bảo mật nội dung cho các tập tin là dữ liệu hoặc các tài liệu, tạo và kiểm tra chữ ký số để xác định tính toàn vẹn và xác thực cho các tập tin đó.

1. **Hạn chế**

* Trong phạm vi thực hiện bài tập lớn thì SHA-1 phù hợp để tìm hiểu giúp hiểu rõ hơn về cách hoạt động của thuật toán băm. Tuy nhiên hiện nay thuật toán SHA-1 không còn được coi là an toàn cho các ứng dụng bảo mật cao như tạo chữ ký số hoặc lưu trữ mật khẩu.
* Chương trình ứng dụng chỉ dừng ở mức cơ bản, một số chức năng khác như hiển thị nguyên lý hoạt động, thông tin tổng quát chưa được hoàn thiện.

1. **Hướng phát triển**

* Tiếp tục học tập và tìm hiểu để có thể nắm được rõ hơn về hoạt động thực tế của chữ ký số điện tử được áp dụng trong các lĩnh vực khác nhau như tài chính, y tế, hoặc an ninh mạng.
* Củng cố kiến thức, rèn luyện, nâng cao kỹ năng mã hóa thông tin đồng thời phân tích và thiết kế chương trình ứng dụng, tích lũy thêm kinh nghiệm cho bản thân.

TÀI LIỆU THAM KHẢO

1. *Giáo trình Nhập môn an toàn thông tin* - *Chương 4: Chữ ký điện tử (Chữ ký số)* – Trần Thị Kim Chi
2. *Luận văn chữ ký số và ứng dụng* – Nguyễn Trọng Hiếu (2011)
3. <https://viblo.asia/p/he-ma-hoa-rsa-va-chu-ky-so-6J3ZgkgMZmB>
4. <https://text.xemtailieu.net/tai-lieu/nghien-cuu-he-mat-ma-rsa-va-ung-dung-trong-chu-ki-dien-tu-1614312.html>
5. <https://viettelnet.vn/chu-ky-so-rsa-la-gi-muc-do-an-toan/>
6. https://devsne.vn/public/post/tim-hieu-ve-chu-ky-so-va-ung-dung-2900