**BỘ CÔNG THƯƠNG**

**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**

**======\*\*\*======**

****

BÀI TẬP LỚN

Môn: An toàn và bảo mật thông tin

**ĐỀ TÀI: TÌM HIỂU VỀ CHỮ KÝ ĐIỆN TỬ RSA VÀ ỨNG DỤNG MINH HỌA**

|  |  |
| --- | --- |
| GVHD: | Ths Trần Phương Nhung |
| Lớp: | 20214IT6001001 |
| Nhóm: | 12 |
| Thành viên: | Cao Văn Sơn – 2020600313 |
|  | Bùi Mạnh Thắng – 2019601338 |
|  | Nguyễn Đức Thắng – 2019603964 |
|  |  |
|  |  |

Hà Nội, Năm 2022

LỜI CẢM ƠN

Để bài tập lớn kết thúc môn học được thực hiện thành công, em xin cảm ơn giảng viên hướng dẫn THS. Trần Phương Nhung, Khoa Công nghệ thông tin, Trường đại học Công nghiệp Hà Nội đã chia sẻ những kiến thức quý báu, hướng dẫn tận tình và có những góp ý trong suốt quá trình thực hiện đề tài để chúng em có thể hoàn thành tiểu luận một cách tốt nhất.

Sau khi nghiên cứu đề tài và kết thúc khóa học, chúng em đã học hỏi và tích lũy được kiến thức và kinh nghiệm từ thầy đi trước để hoàn thiện và phát triển bản thân. Bên cạnh đó, đây cũng là cơ hội giúp chúng em nhận ra mình cần hoàn thiện thêm những gì để chuẩn bị cho một hành trình dài phía trước.

Do kiến thức của bản thân còn hạn chế và thiếu kinh nghiệm thực tiễn nên nội dung bài nghiên cứu khó tránh những thiếu sót. Chúng em rất mong nhận được ý kiến đóng góp của thầy, cô giáo và những người quan tâm đến đề tài này để đề tài này của chúng em được hoàn thiện hơn nữa.

*Chúng em xin chân thành cảm ơn!*

# LỜI MỞ ĐẦU

Ngày nay trong mọi hoạt động của con người thông tin đóng một vai trò quan trọng không thể thiếu. Xã hội càng phát triển nhu cầu trao đổi thông tin giữa các thành phần trong xã hội ngày càng lớn. Mạng máy tính ra đời đã mang lại cho con người rất nhiều lợi ích trong việc trao đổi và xử lý thông tin một cách nhanh chóng và chính xác. Chính từ những thuận lợi này đã đặt ra cho chúng ta một câu hỏi, liệu thông tin đi từ nơi gửi đến nơi nhận có đảm bảo tuyệt đối an toàn, ai có thể đảm bảo thông tin của ta không bị truy cập bất hợp pháp. Thông tin được lưu giữ, truyền dẫn, cùng sử dụng trên mạng lưới thông tin công cộng có thể bị nghe trộm, chiếm đoạt, xuyên tạc hoặc phá huỷ dẫn đến sự tổn thất không thể lường được. Đặc biệt là đối với những số liệu của hệ thống ngân hàng, hệ thống thương mại, cơ quan quản lý của chính phủ hoặc thuộc lĩnh vực quân sự được lưu giữ và truyền dẫn trên mạng. Nếu như vì nhân tố an toàn mà thông tin không dám đưa lên mạng thì hiệu suất làm việc cũng như hiệu suất lợi dụng nguồn dữ liệu đều sẽ bị ảnh hưởng. Trước các yêu cầu cần thiết đó, việc mã hoá thông tin sẽ đảm bảo an toàn cho thông tin tại nơi lưu trữ cũng như khi thông tin được truyền trên mạng.

Các phương thức tấn công thông qua mạng ngày càng tinh vi, phức tạp có thể dẫn đến mất mát thông tin, thậm chí có thể làm sụp đổ hoàn toàn hệ thống thông tin của tổ chức. Vì vậy an toàn thông tin là nhiệm vụ quan trọng, nặng nề và khó đoán trước đối với các hệ thống thông tin.

Một trong những ứng dụng của an toàn thông tin là chữ ký số. Với đặc điểm là đơn giản cho người sử dụng mà vẫn đảm bảo được tính bảo mật, kỹ thuật sử dụng chữ ký số là một trong những kỹ thuật được sử dụng phổ biến, đa dạng trong hầu hết các lĩnh vực, nhất là Tài chính, Ngân hàng, Kế toán…Vì lý do đó, chúng em quyết định nghiên cứu về “Giải thuật tạo chữ ký điện tử sử dụng thuật toán RSA và viết ứng dụng minh họa”.

MỤC LỤC

[LỜI MỞ ĐẦU 3](#_Toc113546487)

[DANH MỤC HÌNH ẢNH 6](#_Toc113546488)

[Chương 1. TỔNG QUAN 7](#_Toc113546489)

[1.1 Lý do chọn đề tài 7](#_Toc113546490)

[1.2 Nội dung nghiên cứu 9](#_Toc113546491)

[1.3 Các kiến thức cần nắm vững 12](#_Toc113546492)

[1.4 Lĩnh vực hoạt động của đề tài 12](#_Toc113546493)

[1.4.1 Ứng dụng trong bảo mật dữ liệu 12](#_Toc113546494)

[1.4.2 Ứng dụng trong công nghệ thông tin 13](#_Toc113546495)

[1.4.3 Ứng dụng trong Chính phủ điện tử 14](#_Toc113546496)

[1.4.4 Ứng dụng trong Thương mại điện tử 14](#_Toc113546497)

[Chương 2. KẾT QUẢ NGHIÊN CỨU 15](#_Toc113546498)

[2.1 Một số khái niệm 15](#_Toc113546499)

[2.2 Cấu tạo thuật toán RSA 17](#_Toc113546500)

[2.3 Ưu điểm và nhược điểm của chữ ký điện tử 18](#_Toc113546501)

[2.3.1 Ưu điểm chữ ký điện tử 18](#_Toc113546502)

[2.3.2 Nhược điểm chữ ký điện tử 20](#_Toc113546503)

[2.4 Quá trình hoạt động của chữ ký điện tử 20](#_Toc113546504)

[2.4.1 Quá trình ký 21](#_Toc113546505)

[2.4.2 Quá trình kiểm tra chữ ký 22](#_Toc113546506)

[2.5 Quá trình thực hiện của chữ ký điện tử 23](#_Toc113546507)

[2.5.1 Quá trình ký bên gửi 23](#_Toc113546508)

[2.5.2 Quá trình kiểm tra chữ ký bên nhận 24](#_Toc113546509)

[2.6 Chi phí và tốc độ thực hiện thuật toán RSA 24](#_Toc113546510)

[2.6.1 Chi phí 24](#_Toc113546511)

[2.6.2 Tốc độ của hệ RSA 25](#_Toc113546512)

[2.6.3 Hiệu xuất thực hiện 25](#_Toc113546513)

[2.7 Nội dung thuật toán 25](#_Toc113546514)

[2.7.1 Quá trình tạo khóa 25](#_Toc113546515)

[2.7.2 Quá trình giải mã 26](#_Toc113546516)

[2.7.3 Ví dụ minh họa giải thuật RSA 26](#_Toc113546517)

[2.7.4 Một số lưu ý về giải thuật RSA 28](#_Toc113546518)

[2.8 Cài đặt và triển khai trên ngôn ngữ C# 28](#_Toc113546519)

[2.8.1 Cài đặt chương trình 28](#_Toc113546520)

[2.8.2 Hướng dẫn chạy chương trình 31](#_Toc113546521)

[2.9 Phân công công việc 35](#_Toc113546522)

[Chương 3. KIẾN THỨC LĨNH HỘI VÀ BÀI HỌC KINH NGHIỆM 36](#_Toc113546523)

[3.1 Nội dung đã thực hiện 36](#_Toc113546524)

[3.2 Hướng phát triển 37](#_Toc113546525)

[3.3 Những kết quả đạt được 40](#_Toc113546526)

[Kết luận 41](#_Toc113546527)

[Tài liệu tham khảo 42](#_Toc113546528)

# DANH MỤC HÌNH ẢNH

[Hình 1.1 Minh họa chữ ký điện tử 8](#_Toc113546529)

[Hình 1.2 Minh họa giải thuật RSA 11](#_Toc113546530)

[Hình 1.3 Ứng dụng chữ ký điện tử trong chính phủ điện tử 14](#_Toc113546531)

[Hình 1.4 Chữ ký số trong thương mại điện tử 14](#_Toc113546532)

[Hình 2.1 Quá trình tạo chữ ký 22](#_Toc113546533)

[Hình 2.2 Quá trình kiểm tra chữ ký 23](#_Toc113546534)

[Hình 2.3 Thiết kế giao diện chương trình 29](#_Toc113546535)

[Hình 2.4 Hàm tạo khóa 29](#_Toc113546536)

[Hình 2.5 Hàm băm dữ liệu và ký 30](#_Toc113546537)

[Hình 2.6 Hàm kiểm tra chữ ký 31](#_Toc113546538)

[Hình 2.7 Giao diện chương trình demo 32](#_Toc113546539)

[Hình 2.8 Thao tác của người gửi 32](#_Toc113546540)

[Hình 2.9 Thao tác của người nhận 33](#_Toc113546541)

[Hình 2.10 Kết quả kiểm tra chữ ký đúng 33](#_Toc113546542)

[Hình 2.11 Kết quả kiểm tra chữ ký sai 34](#_Toc113546543)

[Hình 3.1 Minh họa RSA 37](#_Toc113546544)

[Hình 3.2 Minh họa mật mã công khai 38](#_Toc113546545)

[Hình 3.3 Minh họa thuật toán bảo mật 39](#_Toc113546546)

# TỔNG QUAN

## Lý do chọn đề tài

Chúng ta đang sống trong kỷ nguyên công nghệ, kỷ nguyên của tri thức với sự phát triển như vũ bão của công nghệ thông tin thì những ứng dụng của Tin học đã len lỏi vào mọi ngóc ngách. Sự xuất hiện của chữ ký số và chức năng tiền định của nó, đặc biệt là vai trò của nó như là một công cụ trong việc xác định tính nguyên gốc, xác định tác giả, bảo đảm tính toàn vẹn của tài liệu số, đã đóng một vai trò vô cùng quan trọng trong việc xác định địa vị pháp lý của tài liệu số trong giao dịch số. Việc sử dụng chữ ký số trong phần lớn trường hợp là cơ sở khẳng định giá trị pháp lý của những văn bản điện tử tương đương với tài liệu giấy. Hiện nay, chữ ký số là phương tiện duy nhất để xác nhận giá trị pháp lý của tài liệu điện tử.

Chữ ký điện tử có vai trò quan trọng đối với nhiều cá nhân, doanh nghiệp trong thời ký phát triển bùng nổ của công nghệ thông tin. Chữ ký số dùng cho các văn bản số, cho biết toàn bộ văn bản đã được ký bởi người ký. Và người khác có thể xác minh điều này. Chữ ký số tương tự như chữ ký thông thường, đảm bảo nội dung tài liệu là đáng tin cậy, chính xác, không hề thay đổi trên đường truyền và cho biết người tạo ra tài liệu là ai. Tuy nhiên, chữ ký số khác chữ ký thường, vì nó tùy thuộc vào văn bản. Chữ ký số sẽ thay đổi theo văn bản còn chữ ký thường thì không hề thay đổi.

Chữ ký số được sử dụng để cung cấp chứng thực chủ sở hữu, tính toàn vẹn dữ liệu và chống chối bỏ nguồn gốc trong rất nhiều các lĩnh vực.

Giải pháp dùng chữ ký số là tối ưu vì nó có hiệu lực pháp luật, do đó không cần in ấn tài liệu mà vẫn có thể xác nhận được tài liệu, đảm bảo tính toàn vẹn và không chối bỏ. Chữ ký số được phát hành bởi bên thứ ba là cơ quan chứng thực có thẩm quyền cấp phát, thu hồi, quản lý chứng chỉ số cho các thực thể thực hiện các giao dịch an toàn ( Certificate Authority hoặc CA) nên đảm bảo tính khách quan. Như vậy, quá trình tạo chữ ký số, xác nhận các yêu cầu pháp lý, bao gồm xác thực người ký, xác thực tin nhắn, là thành công và hiệu quả.

Chính vì những ưu điểm của chữ ký số, nó được dùng trong nhiều ứng dụng: Đảm bảo an ninh truyền thông, ngân hàng trực tuyến, thương mại điện tử, đảm bảo an ninh cho thư điện tử, …



Hình . Minh họa chữ ký điện tử

Hiện nay, có nhiều thuật toán được sử dụng để tạo chữ ký số như RSA, ElGamal, … Các thuật toán này cung cấp nhiều lựa chọn để tạo chữ ký số cho dữ liệu giúp xác thực danh tính, đảm bảo tính toàn vẹn của dữ liệu. Trong đó, thuật toán RSA là thuật toán được sử dụng phổ biến nhất để tạo chữ ký số. Bởi các ưu điểm của nó so với các thuật toán khác như: tốc độ tạo khóa, tạo chữ ký nhanh; tốc độ thẩm định dữ liệu nhanh; không yêu cầu hệ thống phần cứng mạnh; khả năng bảo mật cao phụ thuộc vào kích thước khóa tạo ra; được hỗ trợ phát triển với nhiều thư viện được cung cấp sẵn trên nhiều ngôn ngữ, nền tảng khác nhau như: C++, C#, Java, Php, JavaScript, …

Vì vậy chúng em đã quyết định chọn đề tài tìm hiểu về chữ ký điện tử RSA và viết ứng dụng minh họa. Để có thể ứng dụng được các ưu điểm của thuật toán RSA trong việc mã hóa dữ liệu, tạo ra chữ ký điện tử với độ an toàn, bảo mật cao giúp ích cho các hoạt động trong đời sống của các cá nhân, doanh nghiệp. Từ đó góp phần phát triển nền kinh tế, nâng cao đời số của người dân.

## Nội dung nghiên cứu

* Nắm vững các khái niệm quan trọng về an toàn bảo mật thông tin, về mã hóa.
* Khái niệm, vai trò của chữ ký điện tử:
  + Nắm được khái niệm của chữ ký điện tử:
    - Khóa bí mật: khóa dùng để tạo chữ ký số
    - Khóa công khai: khóa dùng để kiểm tra chữ ký số, nó được tạo bởi khóa bí mật tương ứng trong cặp khóa
    - Ký số: Khi đưa khóa bí mật vào chương trình phần mềm để tự động tạo và gắn chữ ký số vào thông điệp dữ liệu
    - Người ký: Thuê bao dùng đúng khóa bí mật của mình để ký số vào một thông điệp dữ liệu dưới tên của mình.
    - Người nhận: các tổ chức, cá nhân nhận được thông điệp dữ liệu ký bởi người ký, sử dụng chứng thư số của người ký đó để kiểm tra chữ ký số trong thông điệp dữ liệu nhận được và tiến hành các hoạt động, giao dịch có liên quan.
  + Phân loại được các thuật toán được sử dụng để tạo chữ ký điện tử cho dữ liệu:
    - Thuật toán RSA: giải thuật đơn giản, tạo khóa nhanh, độ bảo mật cao.
    - Thuật toán ElGamal: giải thuật có độ phức tạp cao, có khả năng bảo mật mạnh mẽ.
    - Thuật toán DSA: giải thuật đơn giản, tạo chữ ký nhanh, kích thước chữ ký nhỏ, dễ dàng ứng dụng trong các lĩnh vực không yêu cầu cao về tính bảo mật.
  + Tìm hiểu vai trò của chữ ký điện tử trong đời sống xã hội
* Nguyên lý hoạt động của chữ ký điện tử:
  + Các bước xây dựng một hệ thống chữ ký điện tử:
    - Tạo chữ ký (ở bên gửi)
    - Kiểm tra, xác thực chữ ký (ở bên nhận)
  + Các bước tạo chữ ký điện tử
    - Sinh khóa
    - Băm dữ liệu
    - Tạo chữ ký bằng cách mã hóa dữ liệu sau khi băm
    - Ghép chữ ký với dữ liệu gốc
  + Các bước kiểm tra, xác thực chữ ký điện tử
    - Tách chữ ký với dữ liệu gốc
    - Băm dữ liệu gốc
    - Giải mã chữ ký
    - So sánh dữ liệu sau khi băm và chữ ký sau khi được giải mã
    - Thông báo kết quả kiểm tra
* Ưu điểm và nhược điểm của chữ ký điện tử
  + Ưu điểm:
    - Tính toàn vẹn dữ liệu
    - Xác thực người ký
    - Chống thoái thác
    - Tiết kiệm thời gian
    - Chính xác và bảo mật
    - Có thể dùng mọi lúc mọi nơi
    - Tăng cường bảo mật cho phần mềm, web, …
    - Có thể tích hợp chung với các hệ thống
  + Nhược điểm:
    - Sự an toàn phụ thuộc vào thuật toán sử dụng
    - Khó chứng minh khi có sai sót
    - Khó khăn trong xử lý các thủ tục
* Giải thuật RSA:



Hình . Minh họa giải thuật RSA

* + Các bước tạo khóa
    - B1: Chọn p, q là 2 số nguyên tố
    - B2: Tính n và
    - B3: Chọn b với và ước chung lớn nhất của b với là 1
    - B4: Tính
    - B5: Xác định khóa: khóa công khai {b, n}; khóa bí mật {a, p, q}
  + Quá trình mã hóa và giải mã
  + VD minh họa giải thuật RSA
  + Lưu ý về giải thuật RSA
* Triển khai bài toán:
  + Lựa chọn các ngôn ngữ để xây dựng ứng dụng demo về chữ ký điện tử
  + Sử dụng ngôn ngữ C# với thư viện hỗ trợ xây dựng hệ thống tạo và kiểm tra chữ ký điện tử RSA được cung cấp từ Microsoft với tốc độ và tính bảo mật cao.
  + Sử dụng ngôn ngữ Python với cộng đồng hỗ trợ lớn, nhiều thư viện đa dạng cung cấp nhiều sự lựa chọn với nhiều chức năng phù hợp với các mục đích sử dụng của chữ ký số RSA.
  + Sử dụng ngôn ngữ JavaScript với khả năng linh hoạt trong xây dựng giao diện web và số lượng thư viện RSA lớn giúp việc xây dựng ứng dụng demo nhanh chóng và dễ dàng.

## Các kiến thức cần nắm vững

* Khái niệm an toàn và bảo mật thông tin
* Chữ ký điện tử
* Nguyên lý hoạt động của chữ ký điện tử
* Giải thuật RSA, tạo khóa, mã hóa, giải mã
* Ngôn ngữ lập trình (C++, C#, Java, Php, …)
* Thiết kế giao diện ví dụ

## Lĩnh vực hoạt động của đề tài

### Ứng dụng trong bảo mật dữ liệu

Với mục đích ra đời là thuật toán mã hóa tư vấn công cuộc bảo vệ dữ liệu RSA đã và đang đóng vai trò rất cần thiết và được ứng dụng trong nhiều hoạt động tiên tiến.

* Chứng thực khi truy cập:
  + Người trải nghiệm đọc hẳn từng gặp trường hợp truy cập vào tài khoản cá nhân và được hệ thống yêu cầu đưa ra con số đã gửi về địa chỉ email, số điện thoại để xác thực đăng nhập. Đây là một trong những phương pháp bảo mật dữ liệu ứng dụng thuật toán RSA.
  + Với tình trạng mạo danh, hack tài khoản gây ra nhiều hậu quả cho không chỉ nhiều cá nhân mà còn toàn xã hội, việc chứng thực khi đăng nhập thật sự vô cùng cần thiết, giúp người dùng bảo vệ được tài khoản của bản thân và yên tâm khi sử dụng các dịch vụ trực tuyến.
* Truyền tải dữ liệu an toàn
  + Rất nhiều mạng xã hội đã bị chỉ trích, bao gồm cả ông lớn Facebook khi liên tục có những động thái nghe lén, theo dõi hoạt động và dữ liệu của người dùng. Không chỉ những mạng xã hội, các trang web bạn đọc truy cập cũng sẽ không tránh khỏi việc lưu lại những hoạt động, hành vi truy cập của bạn từ đấy đưa ra những kết luận phục vụ công cuộc chạy quảng cáo trên những công cụ mạng như Youtube, Facebook, Instagram, …
* Chữ ký số / chữ ký điện tử
  + Trên những chiếc thẻ ATM luôn có phần chữ ký điện tử được mã hóa từ chữ ký của khách hàng giao dịch khi đăng ký tạo tài khoản ngân hàng. Có thể nói, với ngành tài chính – ngân hàng việc đảm bảo an toàn bảo mật cho khách hàng được xem như yếu tố lần đầu, tiên quyết quyết định chất lượng dịch vụ. RSA đã được ứng dụng để những giao dịch ngân hàng có tính bảo mật tuyệt đối cũng như đem lại trải nghiệm an tâm cho người dùng.

### Ứng dụng trong công nghệ thông tin

Các đoạn code RSA hoạt động bất kể sự thay đổi của môi trường. Các lập trình viên sử dụng các tiếng nói của một dân tộc lập trình khác kế bên Java cũng có thể tìm hiểu và ứng dụng RSA trong hoạt động làm việc.

RSA là thuật toán được ứng dụng toàn cầu, đặc trưng trong lĩnh vực ngân hàng và bảo mật dữ liệu nói chung. Với những chia sẻ trong bài viết trên.

### Ứng dụng trong Chính phủ điện tử

* Ứng dụng trong các hoạt động của Bộ Tài chính nhằm xác thực chữ ký cho các văn bản pháp lý.
* Ứng dụng trong các hoạt động của Bộ Công thương nhằm xác thực chữ ký cho các văn bản pháp lý.



Hình . Ứng dụng chữ ký điện tử trong chính phủ điện tử

### Ứng dụng trong Thương mại điện tử

* Xác thực việc mua bán, đặt hàng trực tuyến.
* Thanh toán trực tuyến.
* Xác thực trong các giao dịch tiền ảo.



Hình . Chữ ký số trong thương mại điện tử

# KẾT QUẢ NGHIÊN CỨU

## 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 (Digital 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):
  + Giải thuật kiểm tra chữ ký số.
  + Phương pháp khôi phục dữ liệu từ thông điệp.

*Hàm băm (Hash Function)* 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 digest) 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.
* Hàm băm SHA-2 thực chất bao gồm hai thuật toán băm: SHA-256 và SHA-512. SHA-224 là một biến thể của SHA-256 với các giá trị khởi tạo và đầu ra bị cắt bỏ khác nhau. SHA-384 và SHA-512/224 và SHA-512/256 ít được biết đến là tất cả các biến thể của SHA-512. SHA-512 an toàn hơn SHA-256 và thường nhanh hơn SHA-256 trên các máy 64 bit như AMD64. Do có nhiều phiên bản thuật toán khác nhau do đó kích thước đầu ra của họ SHA-2 cũng khác nhau tùy theo thuật toán. Phần mở rộng của tên phía sau tiền tố “SHA” chính là độ dài của thông điệp băm đầu ra. Ví dụ với SHA-224 thì kích thước đầu ra là 224 bit (28 byte), SHA-256 tạo ra 32 byte, SHA-384 tạo ra 48 byte và cuối cùng là SHA- 512 tạo ra 64 byte. Và chúng ta có thể đã biết rằng Bitcoin sử dụng hàm băm SHA-256 là một phiên bản trong họ SHA-2 này.
* SHA-3 được NIST phát hành vào ngày 5 tháng 8 năm 2015. Đây có lẽ là tiêu chuẩn hàm băm mới nhất cho đến hiện nay. SHA-3 là một tập con của họ nguyên thủy mật mã rộng hơn là Keccak. Thuật toán Keccak được đưa ra bởi Guido Bertoni, Joan Daemen, Michael Peeters và Gilles Van Assche. Keccak dựa trên cấu trúc bọt biển (sponge). Cấu trúc này cũng có thể được sử dụng để xây dựng các nguyên thủy mã hóa khác như các hệ mật mã dòng. SHA-3 cũng có các kích cỡ đầu ra tương tự như SHA-2 bao gồm: 224, 256, 384 và 512 bit.
* MD5: Trong mật mã học, MD5 (viết tắt của tiếng Anh Message-Digest algorithm 5, Thuật toán Tiêu hóa-tin nhắn 5) là một hàm băm mật mã học được sử dụng phổ biến với giá trị băm (hash) dài 128-bit. Là một chuẩn Internet (RFC 1321), MD5 đã được dùng trong nhiều ứng dụng bảo mật, và cũng được dùng phổ biến để kiểm tra tính toàn vẹn của tập tin. Một bảng băm MD5 thường được diễn tả bằng một số hệ thập lục phân 32 ký tự.

Ví dụ: Ta có thể mô phỏng trực quan một hệ mật mã khóa công khai như sau: Bob muốn gửi cho Alice một thông tin mật mà Bob muốn duy nhất Alice có thể đọc được. Để làm được điều này, Alice gửi cho Bob một chiếc hộp có khóa đã mở sẵn (Khóa công khai) và giữ lại chìa khóa. Bob nhận chiếc hộp, cho vào đó một tờ giấy viết thư bình thường và khóa lại (như loại khóa thông thường chỉ cần sập chốt lại, sau khi sập chốt khóa ngay cả Bob cũng không thể mở lại được-không đọc lại hay sửa thông tin trong thư được nữa). Sau đó Bob gửi chiếc hộp lại cho Alice. Alice 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.

*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 cả chữ ký số kèm theo bản rõ và tự khôi phục thông điệp từ chữ ký số.

* Thuật toán sinh khóa cho lược đồ chữ ký RSA
* Thuật toán sinh chữ ký RSA
* Thuật toán chứng thực chữ ký RSA

## Cấu tạo thuật toán RSA

|  |  |
| --- | --- |
| Khóa bí mật | Dùng để tạo ra chữ ký số RSA |
| Khóa công khai | Tác dụng trong việc thẩm định, kiểm tra chữ ký số và xác thực về người dùng. Nó được tạo bởi khóa bí mật tương ứng trong mỗi cặp khóa. |
| Người ký | Đối tượng dùng khóa bí mật của mình để ký số vào một dữ liệu nào đó thể hiện tên mình. |
| Người nhận | Đối tượng nhận được thông điệp dữ liệu được ký số, bằng việc sử dụng các chứng thư số để kiểm tra chữ ký số cho dữ liệu nhận được. Ngoài ra còn tiến hành các hoạt động, giao dịch điện tử. |
| Ký số | Đưa khóa bí mật RSA vào phần mềm tự động tạo và gắn chữ ký số cho thông điệp dữ liệu nào đó. |

## Ưu điểm và nhược điểm của chữ ký điện tử

### Ưu điểm chữ ký điện tử

* **Đảm bảo tính toàn vẹn dữ liệu:** Việc sử dụng chữ ký điện tử giúp xác minh dữ liệu có bị thay đổi hay không.
* **Giúp xác thực người ký dễ dàng:** Có thể xác minh thông tin của người ký dữ liệu điện tử một các dễ dàng thông qua khóa công khai của hệ mã.
* **Chống thoái thác:** Khi chữ ký điện tử được tạo ra, người ký sẽ không thể phủ nhận việc đã ký chữ ký đó.
* **Tiết kiệm thời gian:** Sử dụng chữ ký điện tử giúp cho việc thực hiện ký kết các giao dịch, hợp đồng, phát hành hóa đơn, báo cáo, … một cách nhanh chóng thay vì phải chuyển văn bản giấy và ký tay. Việc dùng chữ ký điện tử trong trường hợp này sẽ tiết kiệm được tối đa thời gian ký. Bên cạnh đó có thể tiết kiệm được thời gian đi lại, gặp gỡ đối tác để ký tay; không phải mất thời gian in giấy tờ.
* **Tiết kiệm chi phí:** Các tổ chức không cần sử dụng đến giấy tở cho các văn bản. Họ sẽ tiết kiệm được chi phí cho các nguồn lực vật chất, thời gian, nhân sự và không gian văn phòng. Tác động tích cực đến môi trường. Giảm thiểu sử dụng giấy cũng cắt giảm chất thải vật lý do giấy tạo ra.
* **Giúp truy xuất nguồn gốc dễ dàng:** Chữ ký điện tử tạo ra một dấu vết kiểm tra giúp lưu trữ hồ sơ nội bộ dễ dàng hơn cho doanh nghiệp. Với việc tất cả mọi thông tin được ghi lại và lưu trữ bằng kỹ thuật số, thì cơ hội mắc lỗi trong hồ sở hoặc làm thất lạc dữ liệu sẽ giảm đáng kể.
* **Chính xác và bảo mật thông tin:** Việc sử dụng chữ ký số sẽ đảm bảo việc không tẩy xóa, thay đổi các thông tin như thực hiện ký giấy, đảm bảo tính toàn vẹn của dữ liệu, là bằng chứng cho các giao dịch điện tử, nội dùng điện tử được ký kết. Chữ ký số được tạo ra bởi những thông tin dữ liệu phức tạp thông qua mã hóa và khó bị giả mạo nên sẽ giúp bảo mật thông tin một cách an toàn.
* **Có thể sử dụng chữ ký điện tử mọi lúc, mọi nơi:** Chữ ký điện tử có thể được sử dụng mọi lúc và mọi nơi không phải phụ thuộc vào giờ làm việc hành chính, thời tiết hay địa lý. Việc ký kết các hợp đồng, văn bản điện tử trở nên dễ dàng và nhanh chóng.
* **Giúp hạn chế tối đa việc làm giả chữ ký, gian lận thủ tục:** Để sử dụng chữ ký điện tử để ký văn bản điện tử, cần phải có khóa bí mật của hệ mã hóa sử dụng cho việc ký. Vì vậy, khi sử dụng chữ ký điện tử sẽ hạn chế việc làm giả chữ ký; đem lại sự minh bạch trong việc xác nhận quyền và nghĩa vụ của các bên trong nội dung văn bản ký.
* **Tăng cường bảo mật cho các hệ thống truyền thông Internet:** Ứng dụng chữ ký số vào việc ký kết các văn bản, hợp đồng, truyền dữ liệu trực tuyến trở lên an toàn hơn, người dùng có thể xác minh tính toàn vẹn của dữ liệu cũng như xác thực danh tính người thực hiện ký dữ liệu.
* **Hỗ trợ bảo mật các hệ thống BlockChain:** Chữ ký số đảm bảo rằng chỉ những chủ sở hữu hợp pháp của tiền điện tử mới có thể ký một giao dịch để chuyển tiền.

### Nhược điểm chữ ký điện tử

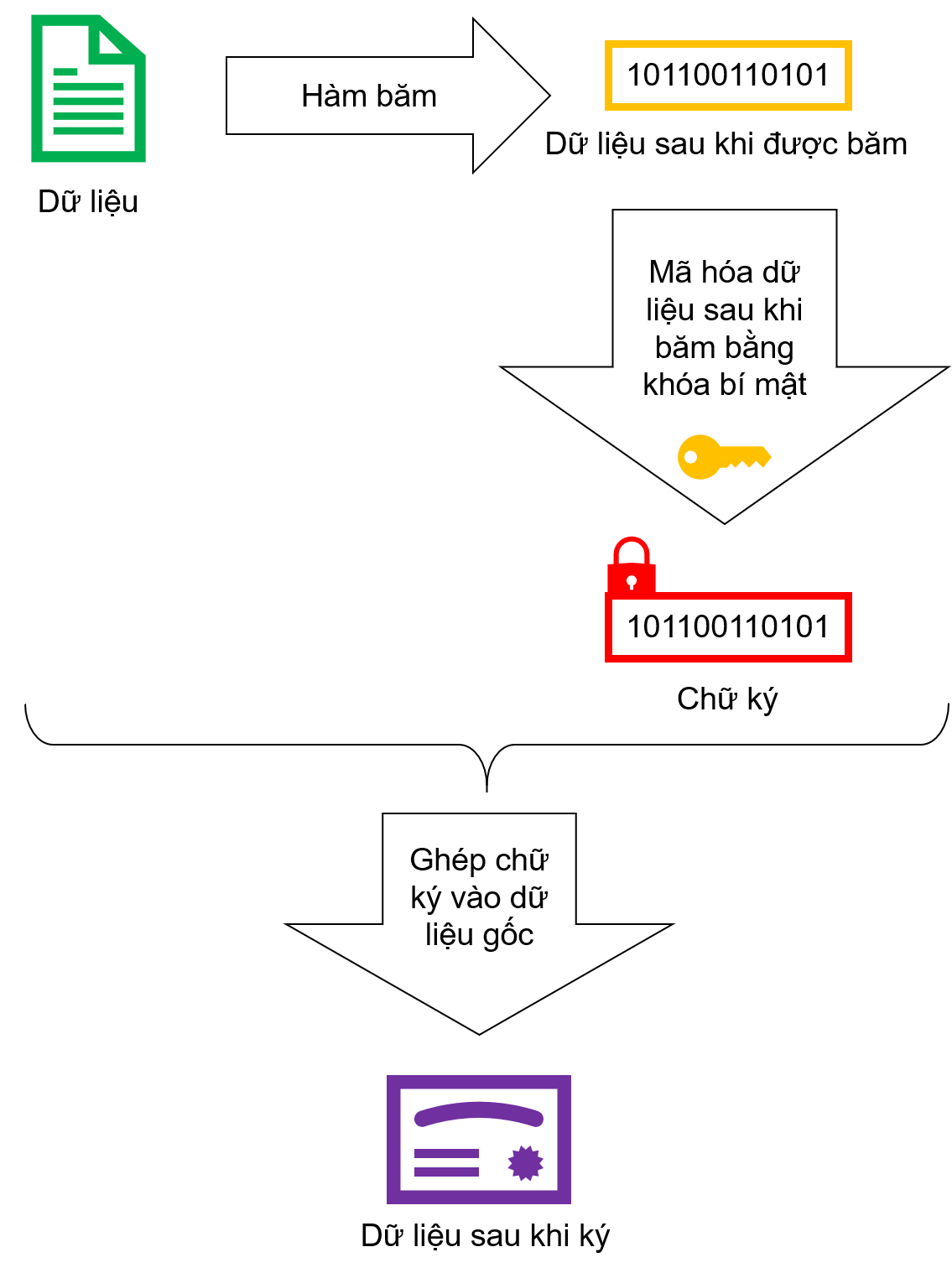
* **Sự an toàn và tính bảo mật cử chữ ký điện tử phụ thuộc vào thuật toán được sử dụng:** Chữ ký điện tử được tạo ra bởi việc sử dụng các hàm băm và các hệ thống mã hóa. Bởi vậy mức độ an toàn và tính bảo mật của chữ ký điện tử sẽ phụ thuộc vào việc lựa chọn các hàm băm đàng tin cậy và các hệ thống mã hóa có tính bảo mật cao.
* **Có thể bị giả mạo chữ ký nếu xảy ra sai sót:** Nếu các khóa bí mật của hệ mã hóa bị rò rỉ hoặc bằng cách nào đó bị xâm phạm, các thuộc tính xác thực và chống thoái thác sẽ bị vô hiệu; từ đó dẫn đến khả năng giả mạo chữ ký, giả mạo danh tính để thực hiện các hoạt động phi pháp.
* **Khó chứng minh, xác thực chữ ký nếu để xảy ra sai sót:** Chữ ký điện tử được tạo nên bởi những thông tin, dữ liệu phức tạp nên trường hợp chứng minh, kiểm chứng lại chữ ký sẽ gây ra khó khăn cho người sử dụng. Người sử dụng cần cải thiện tối đa tính bảo mật của chữ ký điện tử để tránh trường hợp sai sót không mong muốn xảy ra.
* **Khó khăn khi thực hiện các thủ tục:** Khi tiến hành ký, xác thực chữ ký điện tử có thể gặp các lỗi như: hệ thống máy tính chưa tương thích, khả năng truy cập mạng, …

## Quá trình hoạt động của chữ ký điện tử

Hoạt động tạo ra chữ ký điện tử yêu cầu phải có 1 cặp khóa là khóa bí mật (private key) và khóa công khai (public key). Khóa này được tạo ra bởi một hệ mã hóa đảm bảo các tiêu chí an toàn về bảo mật. Người ký sẽ giữ khóa bí mật và dùng để mã hoá thông tin tạo ra chữ ký số, người nhận phải có khóa công khai của người ký tương ứng cặp với khóa bí mật để giải mã chữ ký số nhằm đối chiếu thông tin.

### Quá trình ký

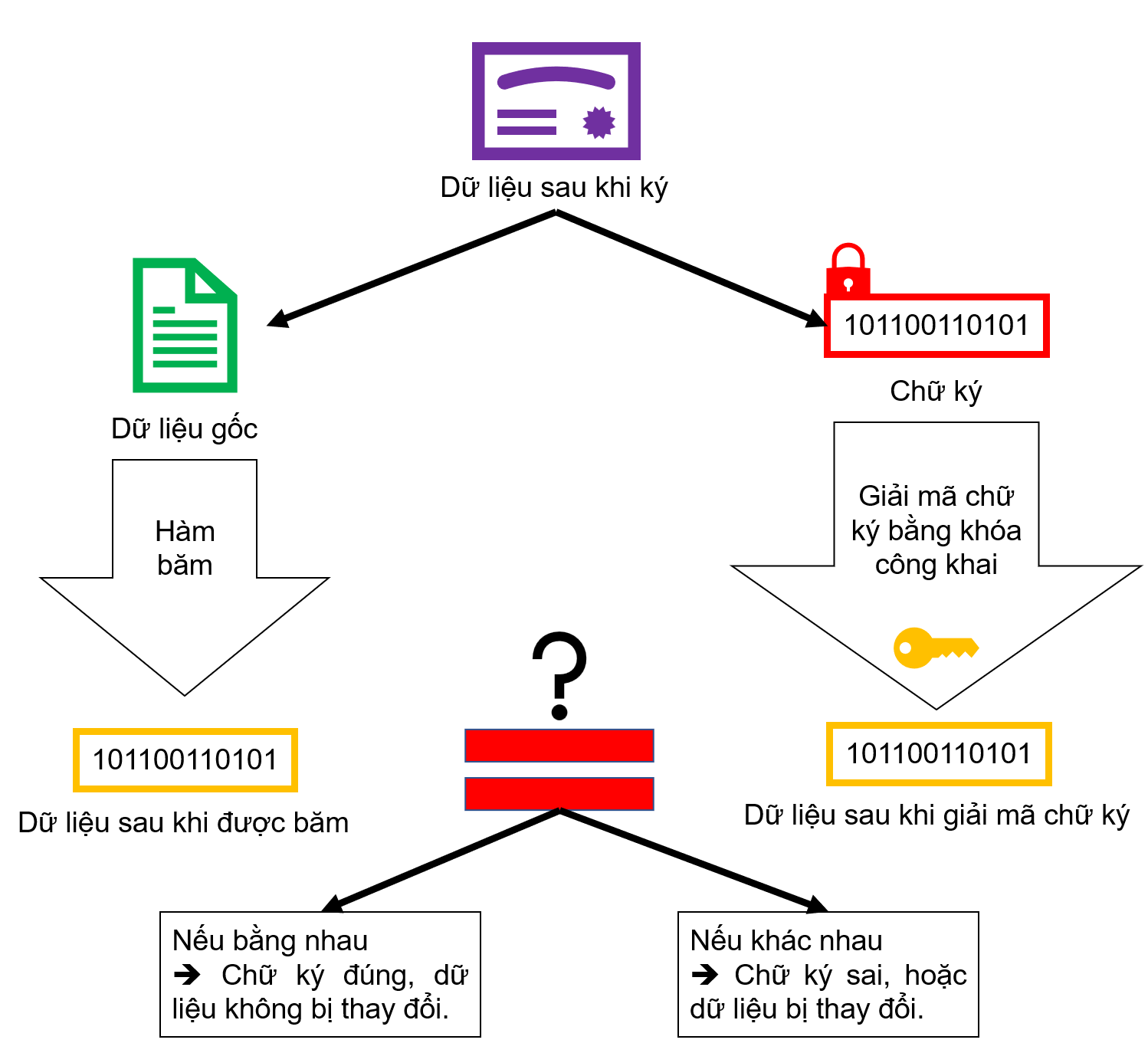
* **B1:** Tạo khóa bằng hệ mã hóa gồm khóa bí mật và khóa công khai. Sử dụng khóa bí mật để tạo chữ ký.
* **B2:** Sử dụng thuật toán băm (MD5 hoặc SHA), để băng dữ liệu cần ký thành một chuỗi ký tự duy nhất với độ dài cố định. Có thể gọi là chuỗi H1.
  + Lưu ý thuật toán băm dữ liệu phải được thống nhất giữa người ký và người xác nhận để có được kết quả chính xác giống nhau khi kiểm tra chữ ký.
  + Lý do mã hóa dữ liệu sau khi được băm thay vì toàn bộ dữ liệu là vì dữ liệu sau khi được băm sẽ trở thành một chuỗi có độ dài cố định. Điều này giúp tiết kiệm thời gian và giảm kích thước lưu trữ của chữ ký.
  + Giá trị sau khi băm là duy nhất. Bất kỳ thay đổi nào trong dữ liệu ngày cả thay đổi một ký tự cũng sẽ dẫn đến giá trị khác. Thuộc tính này cho phép người sử dụng có thể xác định được tính toàn vẹn của dữ liệu.
* **B3:** Sử dụng khóa bí mật để mã hóa chuỗi được băm từ dữ liệu ban đầu theo hệ mã hóa được chọn. Bản mã của quá trình mã hóa chính là chữ ký số được tạo ra.
* **B4:** Gửi dữ liệu cần xác thực và chữ ký cho người nhận. Có thể thực hiện theo 2 cách:
  + Gửi riêng chữ ký và dữ liệu gốc cho người nhận.
* Ghép chữ ký vào nội dung của dữ liệu cần ký và gửi dữ liệu sau khi ghép cho người nhận. Người nhận sau khi nhận được sẽ cần tách chữ ký ra khỏi dữ liệu gốc để có thể xác thực chữ ký.



Hình . Quá trình tạo chữ ký

### Quá trình kiểm tra chữ ký

* **B1:** Nhận dữ liệu gốc và chữ ký của người ký. Nếu chữ ký được ghép vào dữ liệu gốc thì cần tách riêng nội dung và chữ ký để có thể xử lý độc lập.
* **B2:** Ở phần nội dung gốc, người nhận làm công việc giống như người ký đó là sử dụng chương trình thuật toán băm (MD5 hoặc SHA) đã được thống nhất với người ký để băm dữ liệu gốc. Có thể gọi là chuối H2.
* **B3:** Người nhận sử dụng khóa công khai do người ký cung cấp để giải mã chữ ký, từ đó thu được chỗi H1 là một chuỗi có độ dài cố định được sinh ra sau khi người ký băm dữ liệu gốc.
* **B4:** Đối chiếu thông tin trùng khớp giữa chuỗi H1 và chuỗi H2. Nếu khớp nhau tức nội dung của dữ liệu chính xác không bị thay đổi, xác định được người tạo chính là người ký và hoàn tất quá trình kiểm tra chữ ký. Nếu thông tin chuỗi H1 và H2 không trùng khớp, tức là nội dung bị thay đổi hoặc chữ ký không chính xác.
* **Lưu ý:** Bất kỳ thay đổi dù là nhỏ nhất vào nội dung thông điệp (dữ liệu) sau khi đã khởi tạo chữ ký điện tử cũng sẽ tạo ra kết quả hoàn toàn khác ở phía người nhận khi họ băm dữ liệu và thực hiện đối chiếu với chữ ký đã được mã hóa.



Hình . Quá trình kiểm tra chữ ký

## Quá trình thực hiện của chữ ký điện tử

### 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 (Encrypted 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.

## Chi phí và tốc độ thực hiện thuật toán RSA

### Chi phí

Để thực hiện thuật toán RSA phần lớn tốn chi phí thực hiện các phép tính cơ bản như : Tạo khóa, mã hóa, giải mã. Quá trình mã hóa, giải mã tương được với chi phí thực hiện các phép tính lũy thừa modulo 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 của hệ RSA

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.

### Hiệu xuất 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).

## Nội dung thuật toán

### Quá trình tạo khóa

Có 5 bước chính để tạo khóa trong thuật toán RSA.

* Bước 1: Tạo hai số nguyên tố lớn ngẫu nhiên p và q.
* Bước 2: Tính n=q\*p và Φ(n)= (p-1) \* (q-1).
* Bước 3: Chọn b ngẫu nhiên sao cho:
  + 0 < b < Φ(n)
  + GCD (b, Φ(n)) = 1
* Bước 4: Giải phương trình a=b-1modΦ(n) để tìm khóa giải mã a (sử dụng thuật toán euclide mở rộng)
* Bước 5: Ta sẽ có:
  + Khóa công khai: Kpub= {b, n}.
  + Khóa bí mật: Kpr= {a, p, q}.

Mấu chốt của quá trình tạo khóa trong RSA là tìm được bộ 3 số tự nhiên b, a và n.

### Quá trình giải mã

Quá trình mã hóa ta sẽ sử dụng public key (Khóa công khai) Kpub= {b, n} để mã hóa một thông điệp x bất kỳ. Ta có công thức mã hóa như sau:

Trong đó x ∈ Zn = {0, 1, …, n-1}

Quá trình giải mã ta sẽ sử dụng private key (Khóa bí mật) Kpr= {a, p, q} để giải mã một thông điệp y bất kỳ. Ta có công thức giải mã như sau:

Đối với hai công thức trên ta có thể sử dụng thuật toán bình phương và nhân để lấy được giá trị cần tìm.

### Ví dụ minh họa giải thuật RSA

Ta có ví dụ ngắn như sau:

Cho p=5, q=7 là hai số nguyên tố. Hãy mã hóa thông điệp x=32 và giải mã thông điệp vừa được mã hóa.

n = q\*p = 5\*7=35, Φ(n) = (p-1) \* (q-1) = 4 \*6 =24

Chọn b = 5 vì b>0, b<24 và GCD (b, Φ(n)) = GCD (5, 24) =1

a = b-1modΦ(n) = 5-1mod24.

Áp dụng thuật toán euclide mở rộng ta có

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Bước | ri | qi+1 | ri+1 | ri+2 | Si | Ti |
| 0 | 24 | 4 | 5 | 4 | 1 | 0 |
| 1 | 5 | 1 | 4 | 1 | 0 | 1 |
| 2 | 4 | 4 | 1 | 0 | 1 | -4 |
| 3 |  |  |  |  | -1 | 5 |

Với i=0, r0=24, r1=5, q1=4, r2 =4, S0=1, T0=0

Với i=1, r1=5, r2=4, q2=1, r3 =1, S1=0, T1=1

Với i=2, r2=4, r3=1, q3=4, r4 =0, S2=1, T2=-4

Với i=3, r3=4, r4=0, S3=-1, T3=5

Vậy ta có a = b-1modΦ(n) = 5-1mod24 = 5

* Mã hóa:

y = xbmod n = 325mod 35

Chuyển b=5 sang hệ nhị phân ta được b= 101(2).

Khởi tạo p =1.

Áp dụng thuật toán bình phương và nhân ta có bảng sau:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| i | b(i) | p=p\*p | p=p\*mod (35) | p\*x | p=p\*mod (35) |
| 2 | 1 | 1 | 1 | 32 | 32 |
| 1 | 0 | 1024 | 9 |  | 9 |
| 0 | 1 | 81 | 11 | 352 | 2 |

Với i=2, b(i) = 1, p = p\*p = 1, p=p\* mod35 =1, p= p\*x=32, p=p\* mod35 = 32

Với i=1, b(i) = 0, p = p\*p = 1024, p=p\* mod35 = 9

Với i=0, b(i)= 1, p=p\*p =81, p=p\*mod35 =11, p= p\*x=352, p=p\* mod35 = 2

Vậy ta có ta mã hóa được y = 2

* Giải mã: x = yamod n = 25mod 35

Chuyển a=5 sang hệ nhị phân ta được a= 101(2).

Khởi tạo p =1.

Áp dụng thuật toán bình phương và nhân ta có bảng sau:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| i | a(i) | p=p\*p | p=p\*mod (35) | p\*x | p=p\*mod (35) |
| 2 | 1 | 1 | 1 | 2 | 2 |
| 1 | 0 | 4 | 4 |  | 4 |
| 0 | 1 | 16 | 16 | 32 | 32 |

Với i=2, a(i) = 1, p = p\*p = 1, p=p\* mod35 =1, p= p\*x=2, p=p\* mod35 = 2

Với i=1, a(i) = 0, p = p\*p = 4, p=p\* mod35 = 4

Với i=0, a(i)= 1, p=p\*p =16, p=p\*mod35 =16, p= p\*x=32, p=p\* mod35 = 32

Vậy ta giải mã được x = 32.

### Một số lưu ý về giải thuật RSA

Mức độ bảo mật của RSA phụ thuộc rất lớn vào khả năng phân tích thừa số nguyên tố của các số lớn. Bởi vì chúng ta cung cấp public một cách rộng rãi, nếu việc phân tích thừa số nguyên tố đơn giản, thì việc bị lộ private là không thể tránh khỏi.

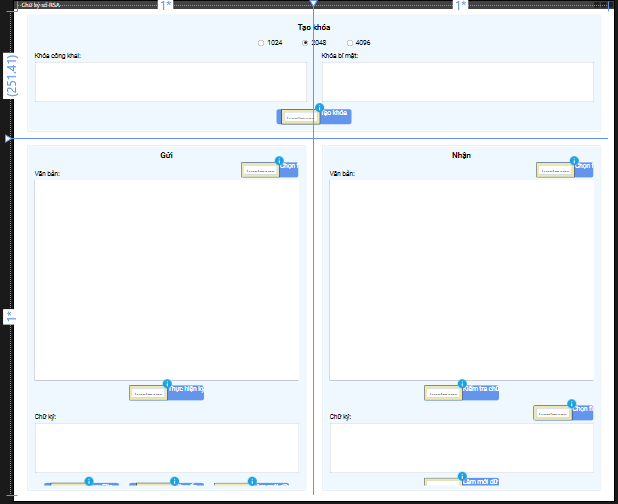
Vì vậy, khi sinh khóa, chúng ta cần chọn các số nguyên tố p và q một cách ngẫu nhiên. Bản thân hai số nguyên tố này cũng rất lớn, và để việc phân tích thừa số nguyên tố khó khăn hơn, hai số nguyên tố này sẽ không có cùng độ dài. Trong tương lai gần, có lẽ vẫn chưa có một phương pháp hiệu quả nào cho phép thực hiện điều này với các máy tính cá nhân.

Ngày từ năm 1993, thuật toán Shor đã được phát triển và chỉ ra rằng máy tính lượng tử có thể giải bài toán phân tích ra thừa số trong thời gian đa thức. Rất may là những điều này mới chỉ là lý thuyết vì đến thời điểm hiện tại và trong vài năm tới, máy tính lượng tử vẫn chưa hoàn thiện.

## Cài đặt và triển khai trên ngôn ngữ C#

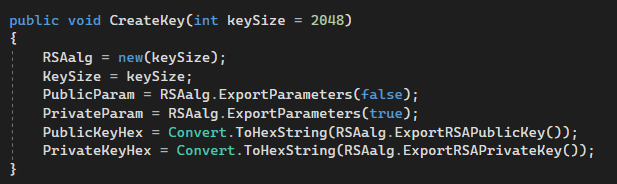
### Cài đặt chương trình

* Ngôn ngữ được sử dụng: C#.
* Giao diện đồ họa: WPF trên nền dotNET 6.0.
* Trình biên tập mã nguồn: Visual Studio 2022.
* Xây dựng giao diện đồ họa:



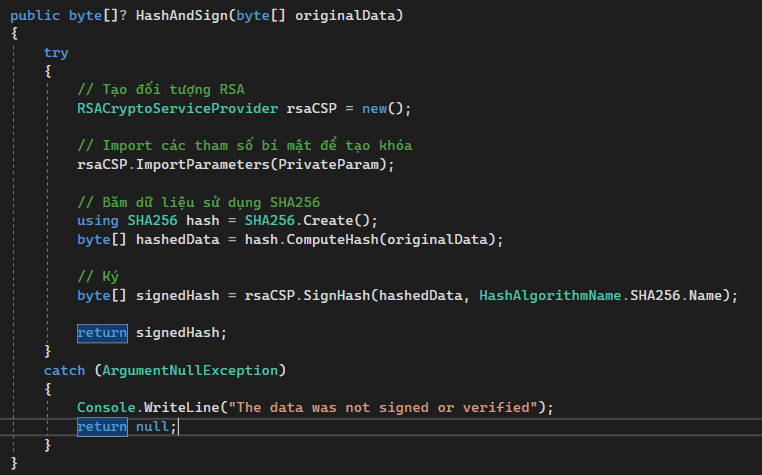
Hình . Thiết kế giao diện chương trình

* Xây dựng các hàm xử lý chính:
  + Hàm tạo khóa: sử dụng thư viện RSACryptoServiceProvider được cung cấp bởi Microsoft. Cho phép tạo khóa nhanh, với kích thước khóa lớn, đảm bảo tính an toàn và bảo mật cao.



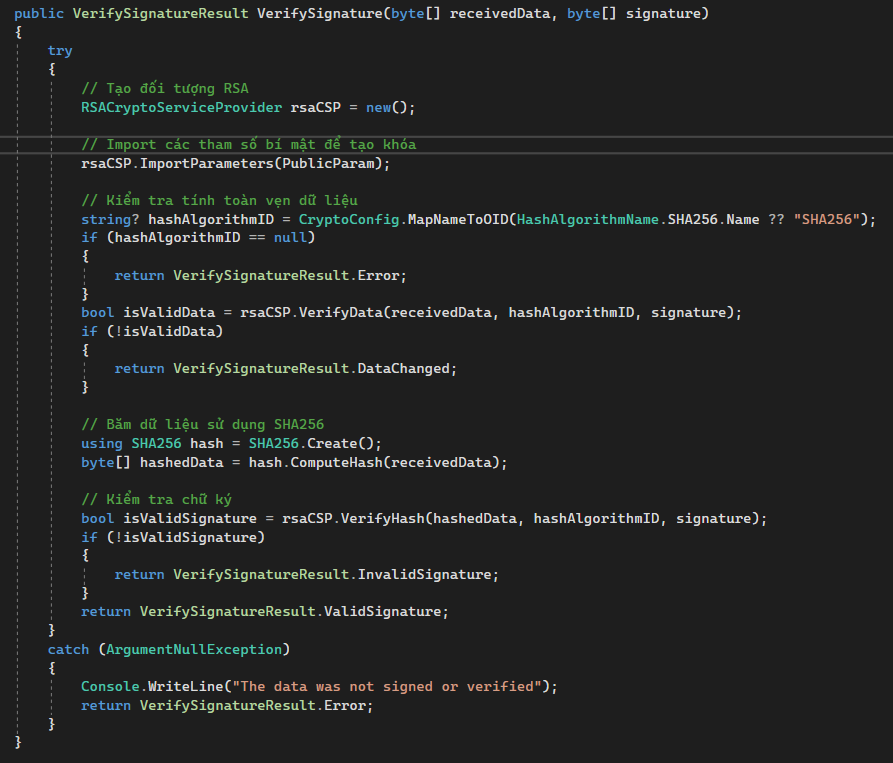
Hình . Hàm tạo khóa

* + Hàm băm dữ liệu và sinh chữ ký: Băm dữ liệu sử dụng thuật toán SHA256. Sau đó mã hóa chuỗi ký tự sau khi băm bằng khóa bí mật được sinh ra từ hàm tạo khóa để tạo ra chữ ký.



Hình . Hàm băm dữ liệu và ký

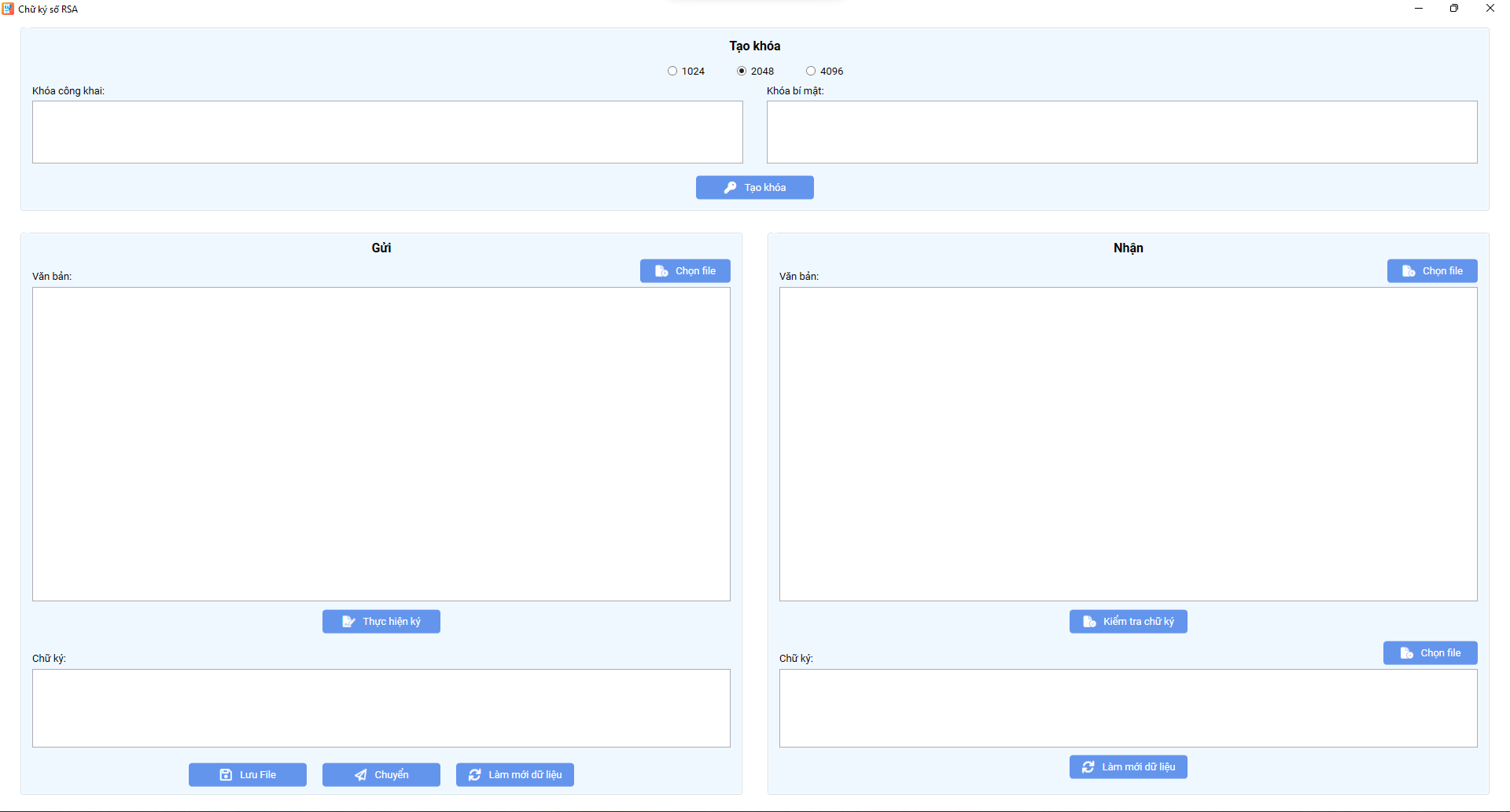
* + Hàm kiểm tra chữ ký: Kiểm tra tính toàn vẹn của dữ liệu và chữ ký bằng cách băm dữ liệu được gửi sử dụng thuật toán SHA256. Sau đó giải mã chữ ký nhận được bằng khóa công khai được tạo ra bời người gửi, để được dữ liệu sau khi băm của bên gửi. So sánh hai dữ liệu sau khi băm của bên gửi và bên nhận để kiểm tra tính toàn vẹn và xác thực được danh tính của người gửi. Nếu hai dữ liệu khác nhau thì dữ liệu đã bị thay đổi hoặc chữ ký của người gửi là không đúng. Ngược lại nếu hai dữ liệu giống nhau, dữ liệu được gửi không bị chỉnh sửa, chữ ký được gửi là chữ ký của người ký.



Hình . Hàm kiểm tra chữ ký

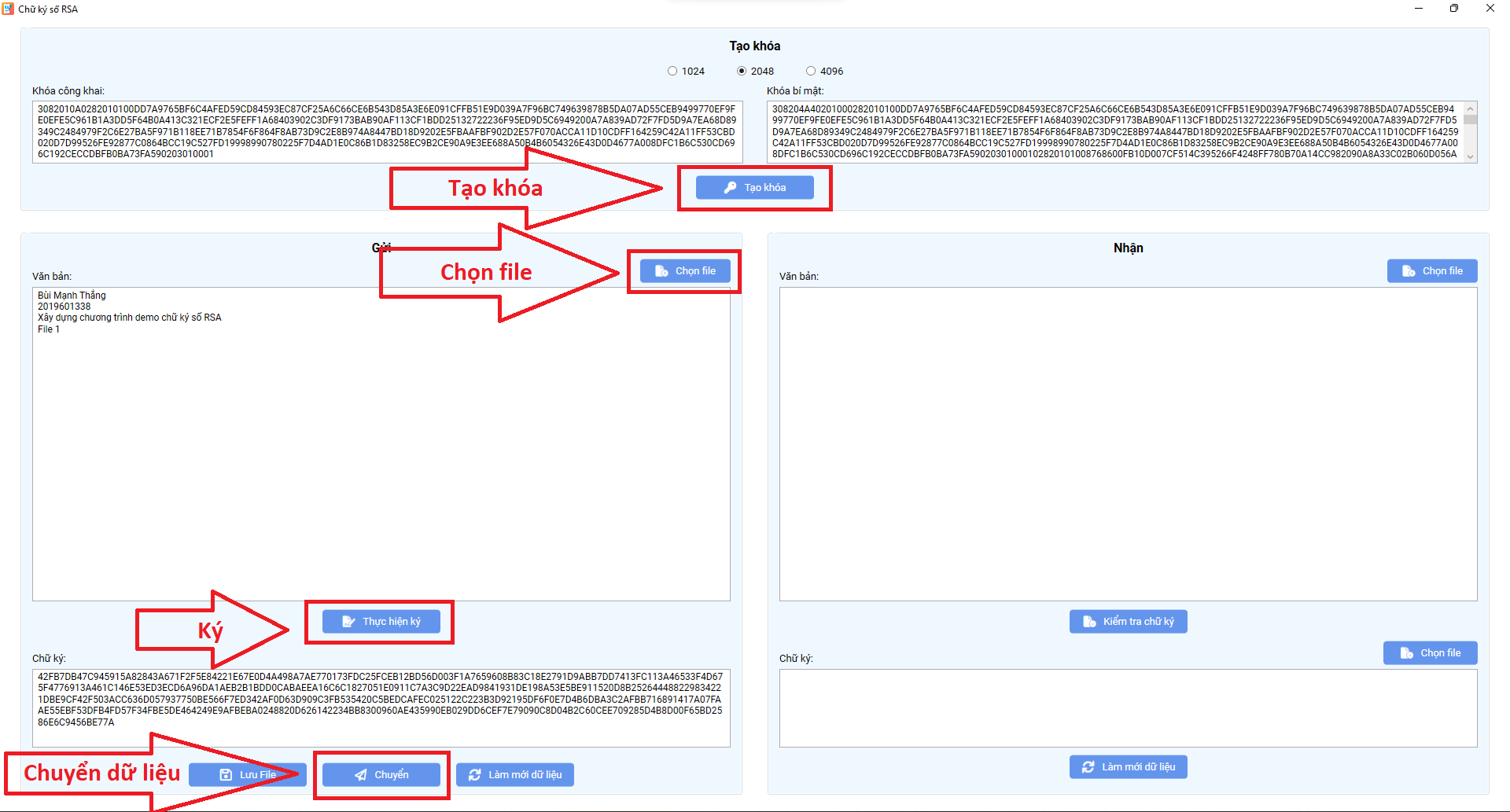
### Hướng dẫn chạy chương trình

* Khởi động chương trình



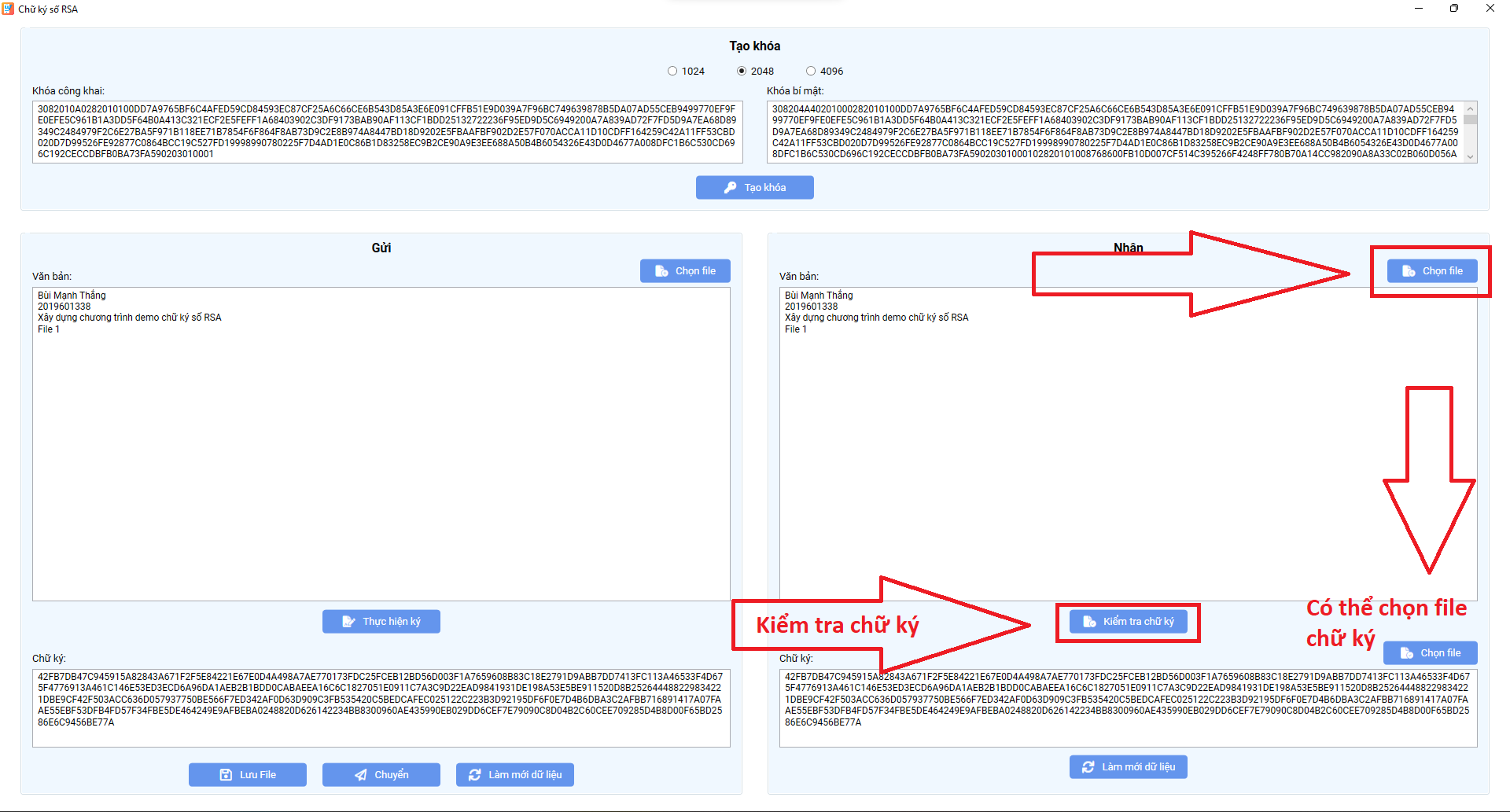
Hình . Giao diện chương trình demo

* Giao diện người gửi:
  + Tạo khóa.
  + Chọn file cần ký.
  + Ký lên file.
  + Chuyển dữ liệu



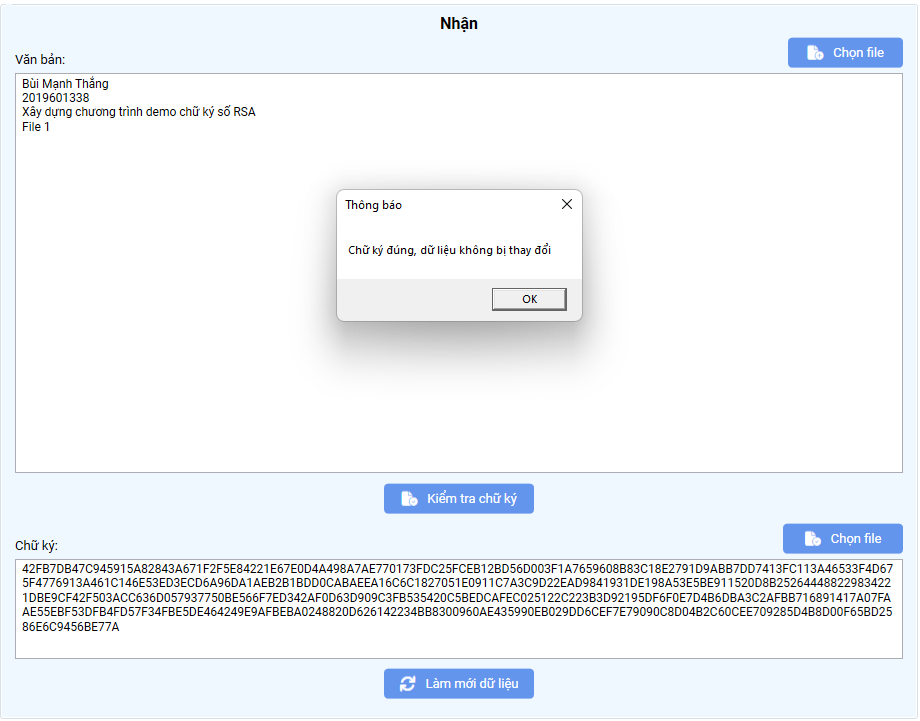
Hình . Thao tác của người gửi

* Giao diện người nhận:
  + Có thể chọn file cần kiểm tra.
  + Có thể chọn file chữ ký.
  + Nhấn kiểm tra chữ ký.



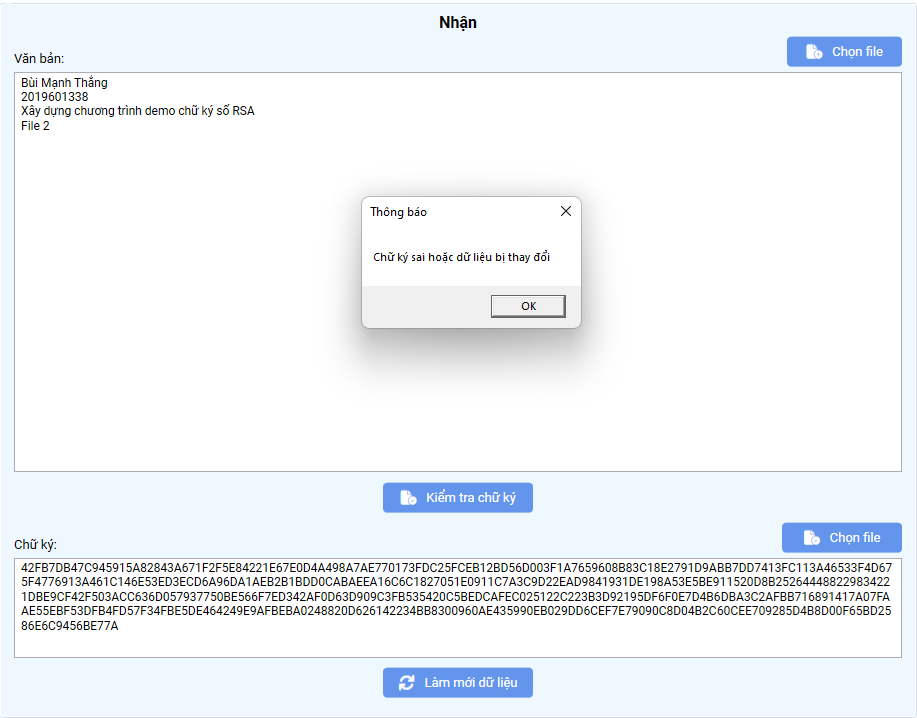
Hình . Thao tác của người nhận

* Thông báo kiểm tra chữ ký thành công



Hình . Kết quả kiểm tra chữ ký đúng

* Thông báo chữ ký sai hoặc dữ liệu bị thay đổi



Hình . Kết quả kiểm tra chữ ký sai

## Phân công công việc

|  |  |
| --- | --- |
| **Tên sinh viên** | **Tên công việc** |
| Cao Văn Sơn | - Trưởng nhóm  - Viết báo cáo, tổng hợp tài liệu  - Viết chương trình demo sử dụng ngôn ngữ javascript để mã hóa, tạo khóa, chữ ký số |
| Nguyễn Đức Thắng | -Viết chương trình demo  - Thu thập tài liệu  - Trình bày nội dung thuật toán, quá trình tạo khóa, giải mã, mã hóa, cho VD minh họa |
| Bùi Mạnh Thắng | - Viết chương trình demo  - Ưu điểm, Nhược điểm của chữ ký điện tử  - Tìm hiểu quá trình thực hiện của RSA  - Giải pháp tối ưu code |

# KIẾN THỨC LĨNH HỘI VÀ BÀI HỌC KINH NGHIỆM

## Nội dung đã thực hiện

* Nắm vững kiến thức về an toàn và bảo mật thông tin.
* Tìm hiểu về thuật toán RSA trong việc tạo khóa, mã hóa, giải mã thông tin.
* Tìm hiểu về khái niệm, lịch sử hình thành, ưu điểm, nhược điểm, vai trò và nguyên lý hoạt động của chữ ký điện tử.
* Tìm hiểu các thức hoạt động của chữ ký điện tử với thuật toán RSA.
* Xây dựng chương trình demo chữ ký điện tử RSA.
* Tăng thêm khả năng làm việc nhóm.
* Có thêm kinh nghiệm về bảo mật thông tin, mã hóa.
* Học được thêm nhiều điều về bản thân mình.
* Thông qua bài tập lớn, nhóm đã biết thêm nhiều kiến thức về các thức hoạt động của chữ ký điện tử. Ứng dụng của chữ ký điện tử và cách chữ ký điện tử được sử dụng trong đời sống, công việc. Hiểu thêm về vai trò và tầm quan trọng của chữ ký điện tử và an toàn bảo mật thông tin trong giai đoạn phát triển mạnh mẽ về công nghệ thông tin.
* Có thêm kiến thức, kỹ năng về các ngôn ngữ lập trình, các giải thuật trong an toàn bảo mật thông tin. Hiểu thêm về cách thức xây dựng một chương trình máy tính, cách thức quản lý mã nguồn, và xây dựng phần mềm hiệu quả.
* Qua quá trình thực hiện bài tập lớn, nhóm cũng đã thu được nhiều kiến thức, kỹ năng trong hoạt động làm việc nhóm, kỹ năng quản lý thời gian, quản lý công việc, cách thức hoạt động của một nhóm bài tập lớn. Bên cạnh đó học tập được các kỹ năng giao tiếp, kỹ năng làm việc của các thành viên trong nhóm.

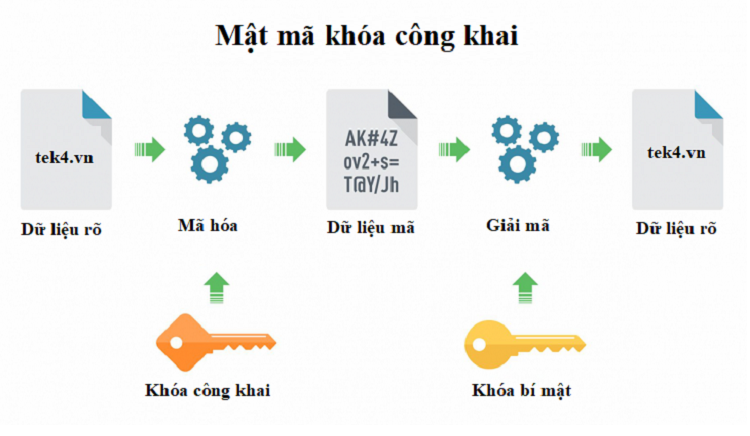
## Hướng phát triển

* Chứng thực khi truy cập
  + Người trải nghiệm đọc hẳn từng gặp trường hợp truy cập vào tài khoản cá nhân và được hệ thống yêu cầu đưa ra con số đã gửi về địa chỉ email, số điện thoại để xác thực đăng nhập. Đây là một trong những phương pháp bảo mật dữ liệu ứng dụng thuật toán RSA.
  + Với tình trạng mạo danh, hack tài khoản gây ra nhiều hậu quả cho không chỉ nhiều cá nhân mà còn toàn xã hội, việc chứng thực khi đăng nhập thật sự vô cùng cần thiết, giúp người dùng bảo vệ được tài khoản của bản thân và yên tâm khi sử dụng các dịch vụ trực tuyến.



Hình . Minh họa RSA

* Truyền tải dữ liệu an toàn
  + Rất nhiều mạng xã hội đã bị chỉ trích, bao gồm cả ông lớn Facebook khi liên tục có những động thái nghe lén, theo dõi hoạt động và dữ liệu của người dùng. Không chỉ những mạng xã hội, các trang web bạn đọc truy cập cũng sẽ không tránh khỏi việc lưu lại những hoạt động, hành vi truy cập của bạn từ đấy đưa ra những kết luận phục vụ công cuộc chạy quảng cáo trên những công cụ mạng như Youtube, Facebook, Instagram, …



Hình . Minh họa mật mã công khai

* Chữ ký số / chữ ký điện tử
  + Trên những chiếc thẻ ATM luôn có phần chữ ký điện tử được mã hóa từ chữ ký của khách hàng giao dịch khi đăng ký tạo tài khoản ngân hàng. Có thể nói, với ngành tài chính – ngân hàng việc đảm bảo an toàn bảo mật cho khách hàng được xem như yếu tố lần đầu, tiên quyết quyết định chất lượng dịch vụ. RSA đã được ứng dụng để những giao dịch ngân hàng có tính bảo mật tuyệt đối cũng như đem lại trải nghiệm an tâm cho người dùng.
  + Các đoạn code RSA hoạt động bất kể sự thay đổi của môi trường. Các lập trình viên sử dụng các tiếng nói của một dân tộc lập trình khác kế bên Java cũng có thể tìm hiểu và ứng dụng RSA trong hoạt động làm việc.
  + RSA là thuật toán được ứng dụng toàn cầu, đặc trưng trong lĩnh vực ngân hàng và bảo mật dữ liệu nói chung. Với những chia sẻ trong bài viết trên.



Hình . Minh họa thuật toán bảo mật

* Giải pháp bảo mật 2 yếu tố

Trên cơ sở mức độ phức tạp của thuật toán phân tích số nguyên thành thừa số, có thể đảm bảo tính an toàn cao của giải pháp bảo mật sử dụng thuật toán RSA. Giải pháp bảo mật sử dụng thuật toán RSA thỏa mãn 5 yêu cầu:

* Độ mật cao (để giải mã được mà không biết khóa thì phải tốn rất, rất nhiều thời gian).
* Thực hiện nhanh (mã hóa và giải mã tốn ít thời gian).
* Có thể dùng chung.
* Chống từ chối (xác định rõ người thực hiện, dùng làm chữ ký điện tử).
* Hiện nay, trên thị trường có nhiều giải pháp bảo mật để tăng cường tính an toàn cho hệ thống công nghệ thông tin đặc biệt cho ngành Tài chính – Ngân hàng. Tuy nhiên, xét về mức độ an toàn dựa trên thuật toán, thì giải pháp sử dụng thuật toán RSA luôn có độ tin cậy cao. Đây là điểm đáng lưu tâm trong bối cảnh nguy cơ rủi ro an ninh an toàn thông tin như hiện nay.

Theo đánh giá của Công ty Forrester Research ([www.forrester.com](http://www.forrester.com/)), một công ty toàn cầu chuyên nghiên cứu thị trường và đánh giá các sản phẩm công nghệ thì giải pháp xác thực hai yếu tố RSA đạt mức an toàn rất cao và đáng tin cậy.

Nhận thức được tầm quan trọng và bảo mật thông tin, Ngân hàng Đầu tư và Phát triển Việt Nam (BIDV) đã nghiên cứu và đầu tư về bảo mật hệ thống công nghệ thông tin, đặc biệt, là giải pháp xác thực hai yếu tố RSA cho hệ thống ngân hàng cốt lõi corebanking và một số giải pháp bảo mật khác cho các ứng dụng phục vụ bảo mật cho các giao dịch của ngân hàng.

## Những kết quả đạt được

* Về công nghệ: Hiểu được cách thức hoạt động RSA.
* Hiểu về quy trình nhiệm vụ của chức năng và biết cách sử dụng hệ mã hóa RSA.
* Về kiến thức đạt được: Biết cách phân tích bài toán và thiết kế giao diện của một hệ thống phần mềm.
* Củng cố lại các kiến thức đã học và biết cách vận dụng.
* Trong quá trình thực hiện đề tài này, chúng em đã cố gắng để tìm hiểu nhưng vì lượng kiến thức còn có hạn nên chúng em chỉ có thể giải quyết được một số chức năng với thời gian nghiên cứu còn hạn chế nên sản phẩm còn chưa được hoàn thiện nên nhóm chúng em rất mong nhận được sự thông cảm của thầy/cô giáo.

# Kết luận

Ngày nay chữ ký điện tử có vai trò rất quan trọng góp phần giúp cho các hoạt động của con người trong nhiều lĩnh vực trở nên an toàn, bảo mật và tiện lợi hơn thay thế cho chữ ký tay. Chữ ký điện tử ngày càng chứng minh được những lợi ích to lớn của nó đối với xã hội. Cùng với sự phát triển của công nghệ thông tin, ngày càng nhiều thuật toán, kỹ thuật nhằm giúp chữ ký điện tử trở nên thông minh và bảo mật hơn, một trong số đó chính là thuật toán RSA. Qua bài tập lớn, nhóm 12 đã nghiên cứu và tìm hiểu được những kiến thức quan trọng của chữ ký điện tở RSA một trong những loại chữ ký điện tử được phát triển và sử dụng phổ biến trong đời sống hiện nay. Thông qua đó thu được nhiều kiến thức và kỹ năng không chỉ về chữ ký điện tử, an toàn bảo mật thông tin mà còn về các kỹ năng làm việc nhóm, kỹ năng xây dựng một chương trình hoàn chỉnh.

Trong quá trình thực hiện bài tập lớn tìm hiểu về chữ ký điện tử RSA và viết ứng dụng minh họa, nhóm 12 đã cố gắng hết sức để tìm hiểu và học hỏi nhưng vì khả năng còn giới hạn không tránh khỏi những sai sót, nên có thể chưa giải quyết được tất cả những vấn đề đặt ra. Chúng em rất mong nhận được sự thông cảm của quý thầy cô và các bạn.

*Chúng em xin chân thành cảm ơn!*

# Tài liệu tham khảo

* An toàn thông tin – TS. Lê Văn Phùng – Nhà xuất bản Thông tin và truyền thông.
* Chữ ký số, chứng chỉ số và cơ sở hạ tầng khóa công khai – Ths. Đỗ Xuân Bình – Nhà xuất bản Bưu điện.
* Giáo trình An Toàn Bảo Mật Hệ Thống Thông Tin – TS Hoàng Xuân Dậu HVCNBCVT. (Chương 4: Các kỹ thuật mã hóa thông tin).
* Lập trình với C# – Phạm Quang Huy – Vũ Trọng Luật – Pham Quang Hiển – Nhà xuất bản Thanh niên.
* Đường vào lập trình Python – Nguyễn Ngọc Giang – Nhà xuất bản Đại học Quốc gia Hà Nội.