Nhom11 Bao Cao BTL Atbmtt 20221 IT6001001

Cơ bản công nghệ thông tin (Trường Đại học Công nghiệp Hà Nội)

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 VIẾT ỨNG DỤNG MINH HỌA

CBHD: ThS. Trần Phương Nhung

Lớp: 20221IT6001001

Nhóm 11

Thành viên nhóm:

1. Bùi Quốc Triệu – 2021600097
2. Phạm Bảo Trung – 2019601001
3. Đàm Văn Tú – 2019604399
4. Hoàng Thanh Tú – 2019600644

Hà Nội – Năm 2023

MỤC LỤC

LỜI NÓI ĐẦU

Bài tập lớn của chúng em có thể được thực hiện một cách suôn sẻ, thành công, không thể không kể đến công lao to lớn trong việc dạy dỗ, truyền đạt kiến thức của giảng viên hướng dẫn ThS. Trần Phương Nhung, Khoa Công nghệ thông tin, trường Đại học Công nghiệp Hà Nội. Những chia sẻ, hướng dẫn của cô thực sự là vốn quý, là nguyên liệu giúp chúng em hoàn thành bài tập lớn một cách tốt nhất!

Đề tài của chúng em được triển khai và gói gọn trong 3 chương, cụ thể như sau:

- Chương 1: Tổng quan: Mô tả tổng quát đề tài nghiên cứu
- Chương 2: Kết quả nghiên cứu: Trình bày những nhiệm vụ, công việc chính khi thực hiện đề tài của Đồ án và kết quả đạt được
- Chương 3: Kiến thức lĩnh hội và bài học kinh nghiệm

CHƯƠNG 1: TỔNG QUAN

1.1. Lý do chọn đề tài

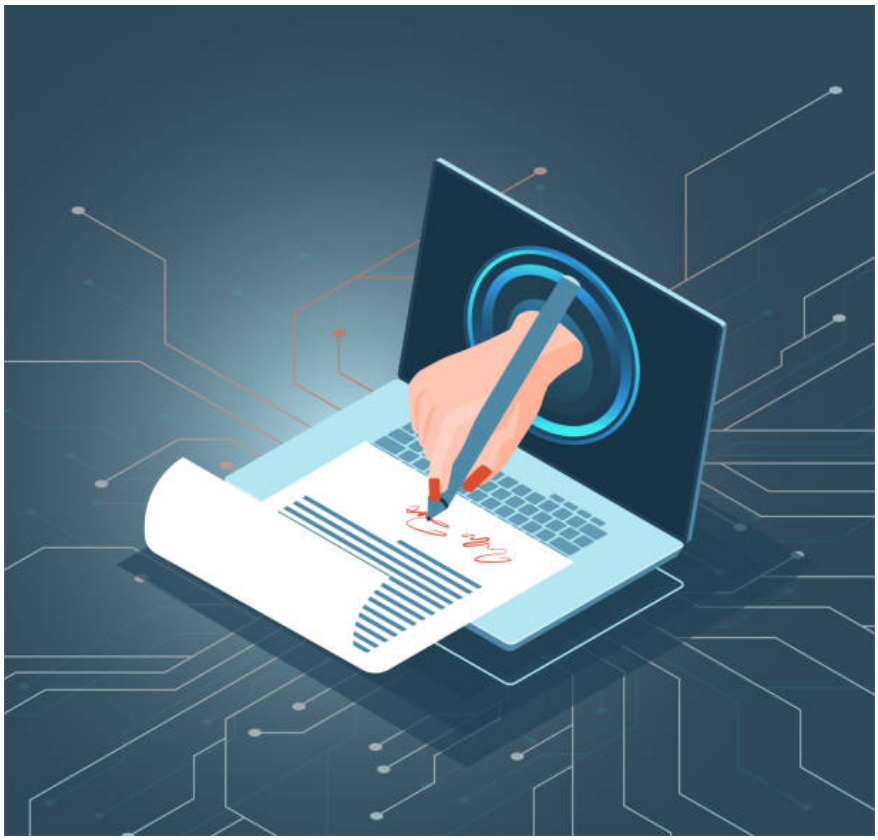
Trong kỷ nguyên công nghệ, kỷ nguyên của tri thức với sự phát triển như vũ bão của công nghệ thông tin thì những ứng dụng của Tin học đã len lỏi vào mọi ngóc ngách. Sự xuất hiện của chữ ký số và chức năng tiền định của nó, đặc biệt là vai trò của nó như là một công cụ trong việc xác định tính nguyên 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.

Vai trò của chữ ký điện tử rất 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 1. Minh họa chữ ký số

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.

1.2. 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.

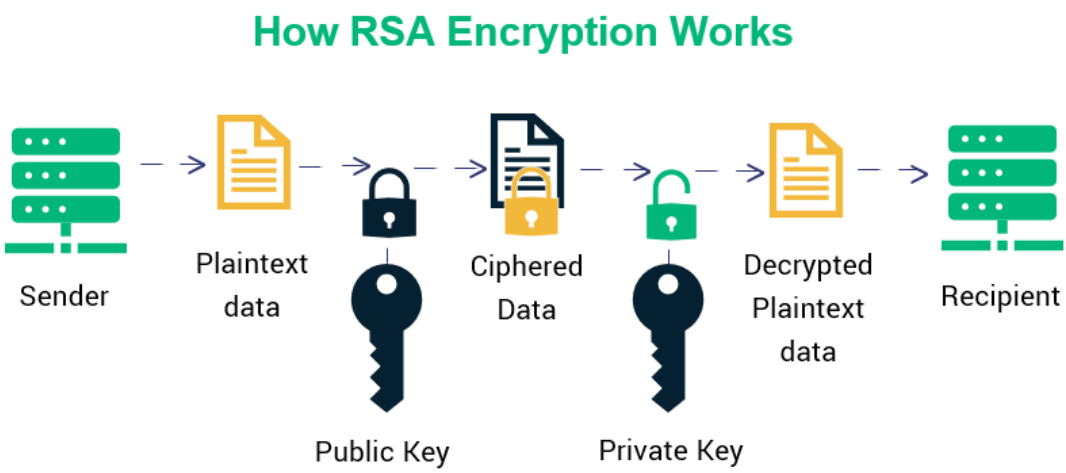
+ Phân loại được các thuật toán được sử dụng để tạo chữ ký điện tử cho dữ liệu:
  - Thuật toán RSA: giải thuật đơn giản, tạo khóa nhanh, độ bảo mật cao.
  - Thuật toán ElGamal: giải thuật có độ phức tạp cao, có khả năng bảo mật mạnh mẽ.
  - Thuật toán DSA: giải thuật đơn giản, tạo chữ ký nhanh, kích 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 2. Mô tả 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
+ 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.

1.3. 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#, Java, Php, Python…)
- Thiết kế giao diện của từng ngôn ngữ

1.4. Lĩnh vực ứng dụng

1.4.1. Ứng dụng trong bảo mật dữ liệu

RSA ra đời với mục đích bảo vệ dữ liệu, do vậy chúng được ứng dụng rất nhiều trong hoạt động hiện đại. Những ứng dụng của RSA trong bảo mật dữ liệu như:

- Chứng thực dữ liệu: chắc hẳn các bạn đã từng gặp tình trạng yêu cầu xác minh bằng cách đưa ra các con số gửi về email hay số điện thoại trước khi đăng nhập. Đây chính là phương pháp bảo mật thông tin, dữ liệu ứng dụng thuật toán RSA để tránh những tình trạng mạo danh, hack tài khoản gây ảnh hưởng cho người dùng và xã hội. Việc chứng thực giúp bảo vệ được tài khoản của bản thân người sử dụng giúp an tâm hơn khi sử dụng các dịch vụ trực tuyến.
- Truyền tải dữ liệu an toàn: hiện nay tình trạng nghe lén, theo dõi hoạt động cũng như lấy cắp dữ liệu cá nhân trên mạng xã hội bị lên án và chỉ trích rất nhiều, bao gồm cả ông lớn Facebook. Không chỉ những trang mạng xã hội, các trang web cũng không tránh khỏi việc lưu lại các hoạt động, hành vi truy cập để phục vụ các mục đích Marketing. Do đó với thuật toán RSA giúp dữ liệu khỏi các cuộc tấn công của kẻ xấu.
- Chữ ký số/ chữ ký điện tử: trên các thẻ ATM luôn có phần chữ ký điện tử đã được mã hóa từ chữ ký của khách hàng khi đăng ký tài khoản tại ngân hàng. Có thể nói, trong lĩnh vực ngân hàng, vấn đề bảo mật thông tin của khách hàng cần được đặt lên hàng đầu, chúng quyết định chất lượng của dịch vụ. RSA được ứng dụng để bảo mật dữ liệu khi người dùng thực hiện những giao dịch ngân hàng, đem lại trải nghiệm tốt và giúp khách hàng an tâm hơn

Hình 3. RSA có nhiều ứng dụng trong bảo mật dữ liệu

1.4.2. Ứng dụng trong công nghệ thông tin

Trong ngôn ngữ lập trình Java, các nhà lập trình viên thường sử dụng những đoạn code chứa RSA để tăng tính bảo mật cho trang web và ứng dụng cũng như đảm bảo an toàn cho người sử dụng.Các đoạn code RSA này có thể hoạt động dưới bất kỳ sự thay đổi nào của môi trường. Ngoài ra, các lập trình viên cũng sử dụng các ngôn ngữ lập trình khác bên cạnh Java có thể tìm hiểu và ứng dụng những tính năng của RSA trong hoạt động làm việc và bảo mật thông tin.Ngày nay việc sử dụng các ứng dụng, trang web trên internet ngày càng gia tăng khiến cho vấn đề bảo mật dữ liệu càng được chú trọng. Những dữ liệu này có thể là những thông tin bí mật cá nhân, thông tin về tài chính,... gây không ít nguy hại cho người sử dụng. Cũng chính vì lý do này mà thuật toán RSA được biết đến và sử dụng nhiều hơn trong tất cả các lĩnh vực đặc biệt là trong ngành ngân hàng.

1.4.3. 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.

1.4.4. Ứng dụng trong Thương mại điện tử

Ngày nay, cùng với sự phát triển nhanh chóng của khoa học công nghệ, các hoạt động thương mại điện tử (TMĐT) được đẩy mạnh và nhanh chóng được ứng dụng rộng rãi trong mọi ngành nghề và tất nhiên, đi kèm theo đó luôn là các vấn đề an toàn bảo mật thông tin được đặt ra.

Một trong giải pháp bảo mật thông tin ứng dụng trong TMĐT là sử dụng kỹ thuật mã hóa RSA.

Chữ ký số được dùng để:

- Chứng thực danh tính người tham gia giao dịch, xác thực tính an toàn của giao dịch điện tử qua mạng Internet.
- Chứng thực tính nguyên vẹn của hợp đồng, tài liệu,...
- Ứng dụng xác thực trong Internet banking
- Ứng dụng xác thực trong giao dịch chứng khoán
- Ứng dụng xác thực trong mua bán, đấu thầu qua mạng

CHƯƠNG 2: KẾT QUẢ NGHIÊN CỨU

2.1. Giới thiệu

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 $k<2^{64}$ 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

2.2. Chữ ký điện tử

2.2.1. Ưu, nhược điểm

2.2.1.1. Ưu điểm

- **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.

2.2.1.2. Nhược điểm

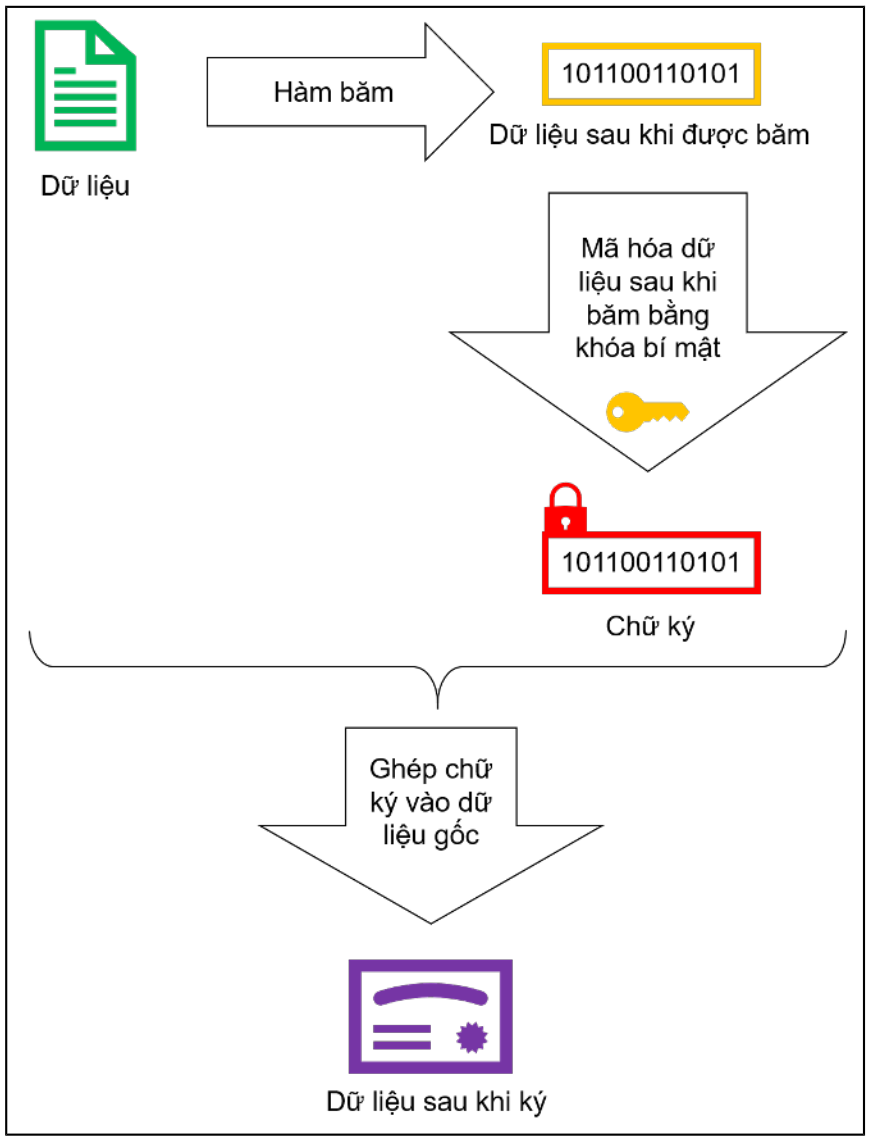
- **Sự an toàn và tính bảo mật cử chữ ký điện tử phụ thuộc vào thuật toán được sử dụng:** Chữ ký điện tử được tạo ra bởi việc sử dụng các hàm băm và các hệ thống mã hóa. Bởi vậy mức độ an toàn và tính bảo mật của chữ ký điện tử sẽ phụ thuộc vào việc lựa chọn các hàm băm đàng tin cậy và các hệ thống mã 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, …

2.2.2. Nguyên lý hoạt động

2.2.2.1. 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.

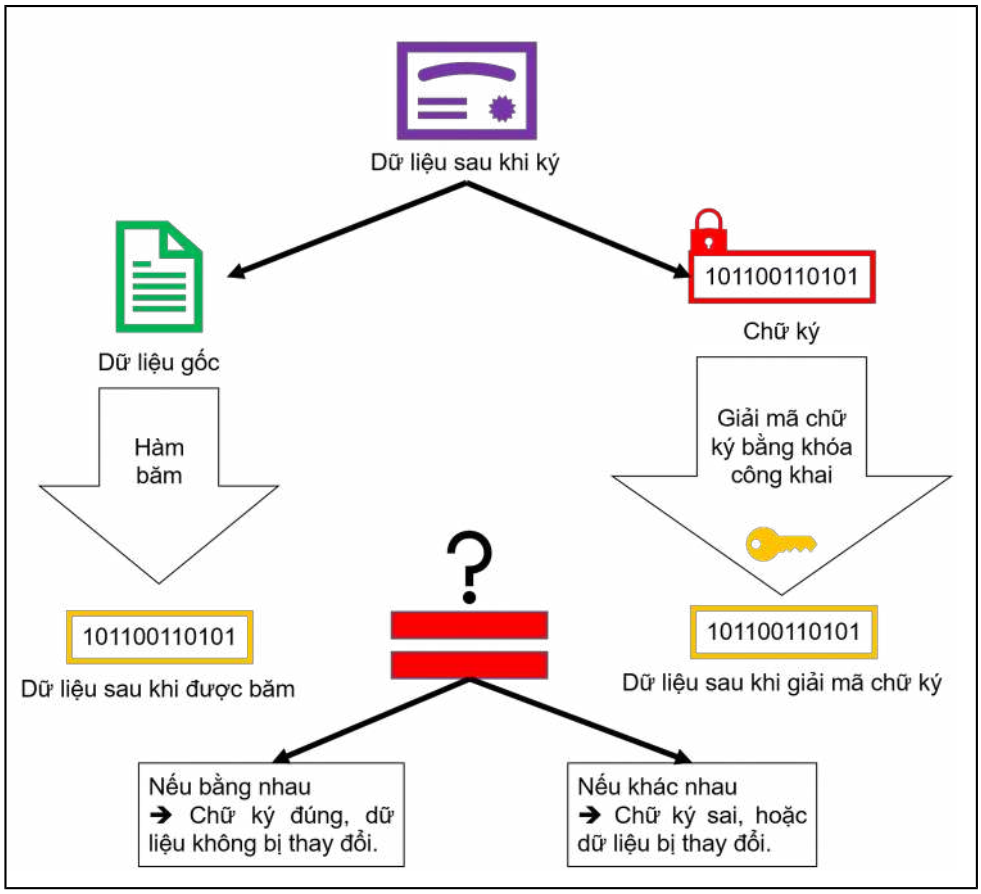


Hình 4. Quá trình tạo chữ ký

2.2.2.2. 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 5. Quá trình kiểm tra chữ ký

2.3. Chữ ký điện tử RSA

2.3.1. 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.

Bảng 1. Cấu tạo thuật toán RSA

2.3.2. Nội dung thuật toán RSA

2.3.1.1. 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:
  - $0 < b < \Phi(n)$
  - GCD (b, Φ(n)) = 1
- Bước 4: Giải phương trình $a=b^{-1} \bmod \Phi(n)$ để tìm khóa giải mã a (sử dụng thuật toán euclide mở rộng)
- Bước 5: Ta sẽ có:
  - Khóa công khai: K_{pub}= {b, n}.

+ Khóa bí mật: K_{pr}= {a, p, q}.

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

2.3.1.2. Quá trình mã hóa và giải mã

- **Quá trình mã hóa** ta sẽ sử dụng public key (Khóa công khai) K_{pub}= {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) K_{pr}= {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.

2.3.1.3. Quá trình ký và xác thực chữ ký

Việc ký tên và xác thực chữ ký số sử dụng hệ mã hóa RSA tương tự như quá trình mã hóa mà giải mã ở trên. Tuy nhiên vai trò của public key và private thì có thay đổi đôi chút.

Để tạo chữ ký, người gửi sẽ dùng private key và người nhận sẽ dùng public key để xác thực chữ ký đó.

Tuy nhiên, vì bản tin rất dài nên việc mã hóa toàn bộ bản tin sẽ rất mất thời gian. Vì vậy, trong thực hành, chữ ký số thường sử dụng phương pháp mã hóa giá trị hash của bản tin. Việc này mang lại rất nhiều lợi ích như:

- Các hàm hash là hàm 1 chiều, vì vậy dù có được hash cũng không thể biết được bản tin gốc như thế nào.
- Độ dài hash là cố định và thường rất nhỏ, vì vậy chữ số sẽ không chiếm quá nhiều dung lượng.
- Giá trị hash còn có thể dùng để kiểm tra lại bản tin nhận được có nguyên vẹn hay không?

Chữ ký số đem lại nhiều giá trị hơn chữ ký tay rất nhiều. Có lẽ cũng vì vậy, việc xử lý chữ ký số phức tạp hơn hẳn chữ ký tay truyền thống.

- Quá trình ký ta sẽ sử dụng private key (Khóa bí mật) K_{pr}= {a, p, q}:

1. Với thông điệp x = M (M: message), ta sử dụng hàm băm để băm tin nhắn, ta được thông điệp sau khi băm là: h = hash(x).

2. Hàm ký : y

- **Quá trình xác thực chữ ký** ta sẽ sử dụng public key (Khóa công khai) K_{pub}= {b, n}:

1. Thực hiện băm tin nhắn: h = hash(x)

2. Giải mã chữ ký: h’ =

3. So sánh h với h’: Nếu h = h’ thì chữ ký hợp lệ, ngược lại chữ ký không hợp lệ

2.3.3. Đánh giá

2.3.2.1. 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.

2.3.2.2. 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.

2.3.2.3. Hiệu suất

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).

2.4. Hàm băm MD5

2.4.1. Giới thiệu

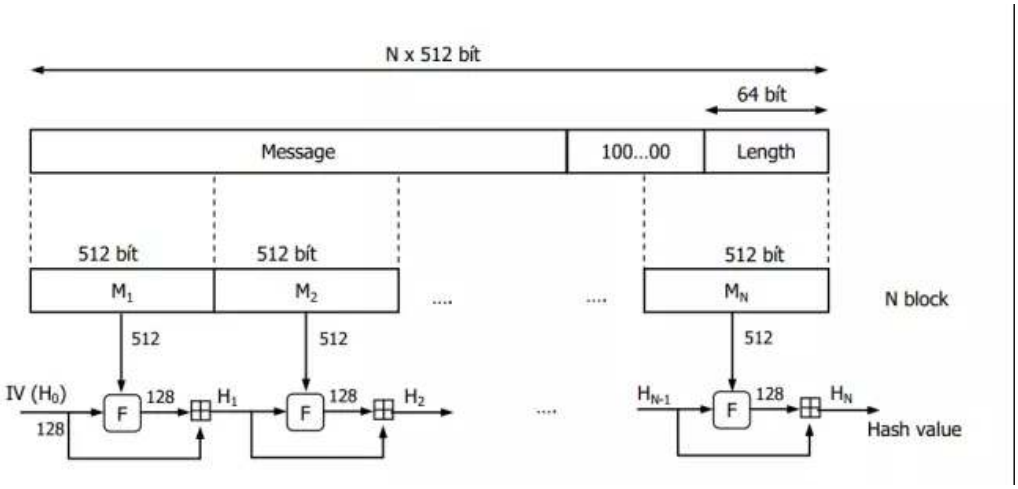
MD5 được phát minh bởi Ron Rivest ,người đã tham gia xây dựng RSA.MD5 viết tắt của chữ Message Digest,được phát triển lên từ MD4 và trước đó là MD2,do MD2 và MD4 không còn an toàn. Kích thước của MD5 là 128 bit.

2.4.2. Thuật toán MD5

- Input: xâu đầu vào x

- Output: chuỗi băm 128 bit

- Sơ đồ thuật toán:



Hình 6. Sơ đồ thuật toán MD5

Trước tiên thông điệp được đệm vào dãy padding 100...00. Chiều dài của dãy padding được chọn sao cho thông điệp cuối cùng đi kèm với dãy 64 bít biểu thị độ dài thông điệp có thể chia làm N block 512 bit M1,M2,...,MN.Quá trình tính giá trị băm của thông điệp là quá trình lũy tiến. Trước tiên block M1 kết hợp với giá trị khởi tạo H0 thông qua hàm F để tính giá trị hash H1. Sau đó block M2 đượckết hợp với H1 để cho ra giá trị hash là H2. Block M3 kết hợp với H2 cho ra giá trị H3. Cứ như vậy cho đến block MN thì có giá trị băm của toàn bộ thông điệp là HN.

- H0 là một dãy 128 bit được chia thành 4 từ 32 bit, ký hiệu 4 từ 32 bit trên là abcd. Với a, b, c, d là các hằng số như sau (viết dưới dạng thập lục phân):

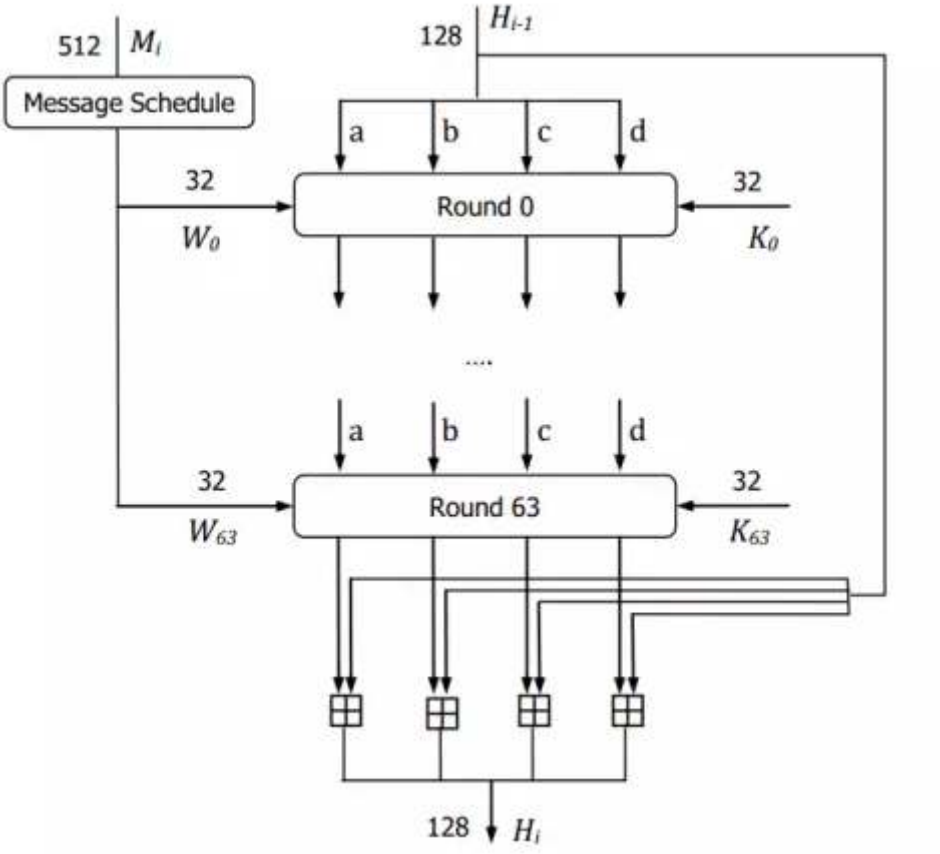
a = 01234567

b = 89abcdef

c = fedbca98

d = 76543210

- Cấu trúc của hàm F như sau:



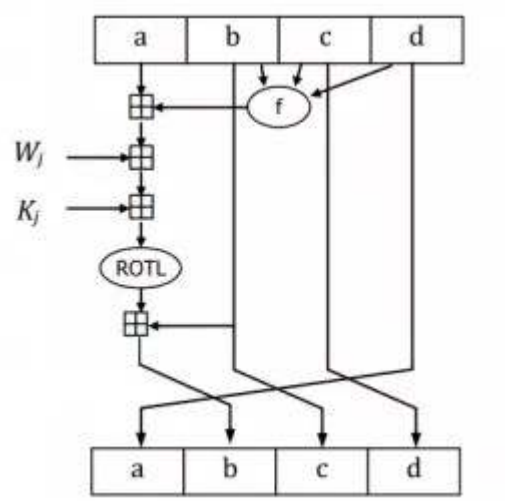
Hình 7. Cấu trúc hàm F của MD5

Tại mỗi bước lũy tiến, các giá trị abcd của giá trị hash Hi-1 được biến đổi qua 64 vòng từ 0 đến 63. Tại vòng thứ j sẽ có 2 tham số là Kj và Wj đều có kích thước 32 bit. Các tham số Kj được tính từ công thức: Kj là phần nguyên của số 2^32 abs(sin(i)) với i biểu diễn theo rad.

Giá trị block Mi 512 bit được biến đổi qua một hàm message schedule cho ra 64 giá trị W0, W1,..., W63 mỗi giá trị 32 bit. Block Mi 512 bit được chia thành 16 block 32 bit ứng với các giá trị W0, W1, ..., W15 (16×32=512). Tiếp theo, 16 giá trị này được lặp lại 3 lần tạo thành dãy 64 giá trị.

Sau vòng cuối cùng, các giá trị abcde được cộng với các giá trị abcd của Hi-1 để cho ra các giá trị abcd của Hi. Phép cộng ở đây là phép cộng modulo 232.

Tiếp theo tìm hiểu cấu trúc của một vòng. Việc biến đổi các giá trị abcd trong vòng thứ i được thể hiện trong hình bên dưới.



Hình 8. Biến đổi các giá trị abcd trong vòng thứ i của MD5

Note: Phép + trong sơ đồ trên là phép cộng modul 2^32 Ở đây c lấy giá trị của b, d lấy giá trị của c, a lấy giá trị của d. Giá trị b được tính qua hàm:

t = a + f(b,c,d) + Wi + Ki

b = b + ROTL(t,s)

Trong đó : Hàm f(x,y,z):

f (x,y,z) = (x ^ y) v (_x ^ z) nếu vòng từ 0 đến 15

f (x,y,z) = (z ^ x) v (_z ^ y) nếu vòng từ 16 đến 32

f (x,y,z) = x xor y xor z nếu vòng từ 32 đến 48

f (x,y,z) = y xor (x v _z) nếu vòng từ 49 đến 63

Hàm ROTL(t, s): t được dịch vòng trái s bit, với s là các hằng số cho vòng thứ i như sau:

i	*s*	*i*	*s*
0, 4, 8, 12	7	32, 36, 40, 44	4
1, 5, 9, 13	12	33, 37, 41, 45	11
2, 6,10, 14	17	34, 38, 42, 46	16
3, 7, 11, 15	22	35, 39, 43, 47	23
16, 20, 24, 28	5	48, 52, 56, 60	6
17, 21, 25, 29	9	49, 53, 57, 61	10
18, 22, 26, 30	14	50, 54, 58, 62	15
19, 23, 27, 31	20	51, 55, 59, 63	21

Bảng 2. Hằng số s tương ứng với vòng thứ i của MD5

2.5. Thiết kế, cài đặt chương trình demo thuật toán trong Java

2.5.1. Giao diện chương trình demo

Hình 9. Giao diện chương trình demo

2.5.2. Cài đặt và triển khai

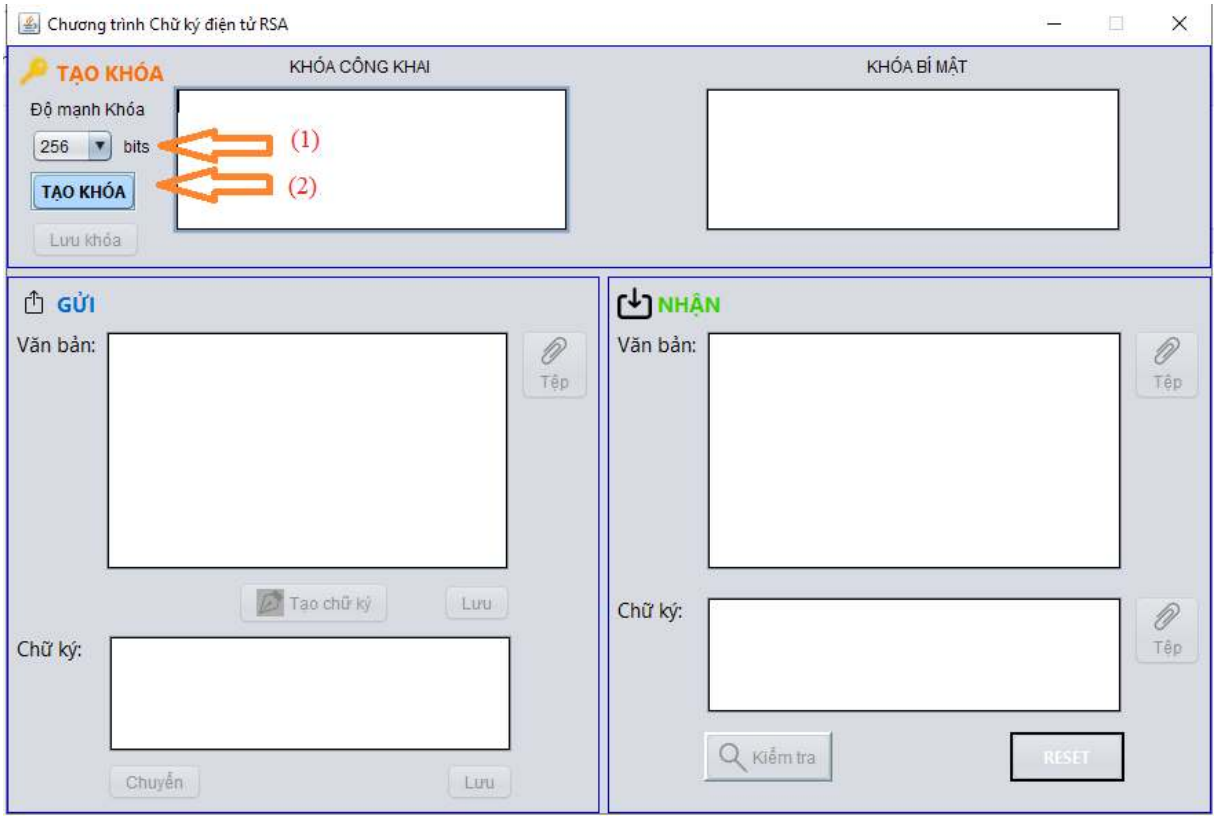
2.5.2.1. Giới thiệu công cụ triển khai

- IDE: Sử dụng NetBeans

NetBeans là một môi trường phát triển tích hợp (IDE) cho Java. NetBeans cho phép các ứng dụng được phát triển từ một tập hợp các thành phần phần mềm được gọi là *modules*. NetBeans chạy trên Windows, macOS, Linux và Solaris. Ngoài việc phát triển Java, nó còn có các phần mở rộng cho các ngôn ngữ khác như PHP, C, C++, HTML5, và JavaScript. Các ứng dụng dựa trên NetBeans, bao gồm NetBeans IDE, có thể được mở rộng bởi các nhà phát triển bên thứ ba.

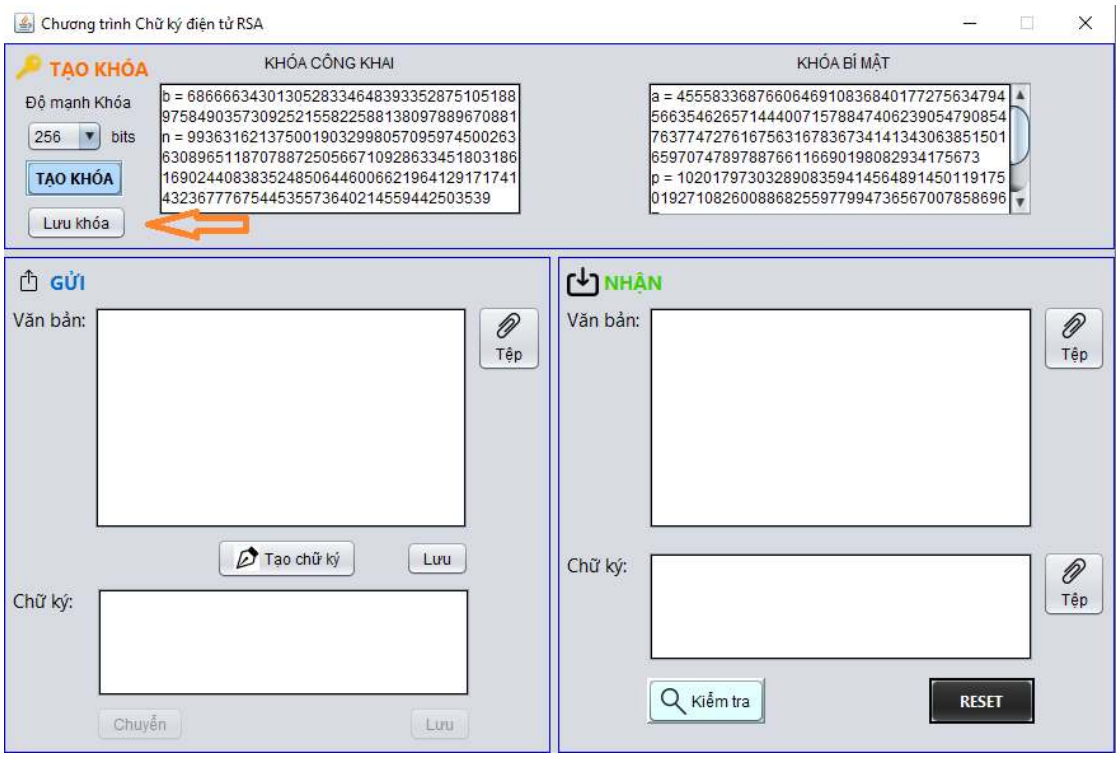
2.5.2.2. Hướng dẫn cài đặt và chạy chương trình

Tạo khóa: Chạy file .jar của chương trình (trên máy phải cài đặt sẵn JVM), ta được phần mềm như dưới đây. Chọn (1) để tùy chọn độ mạnh của chữ ký (theo bit). Chọn Tạo khóa để tạo khóa

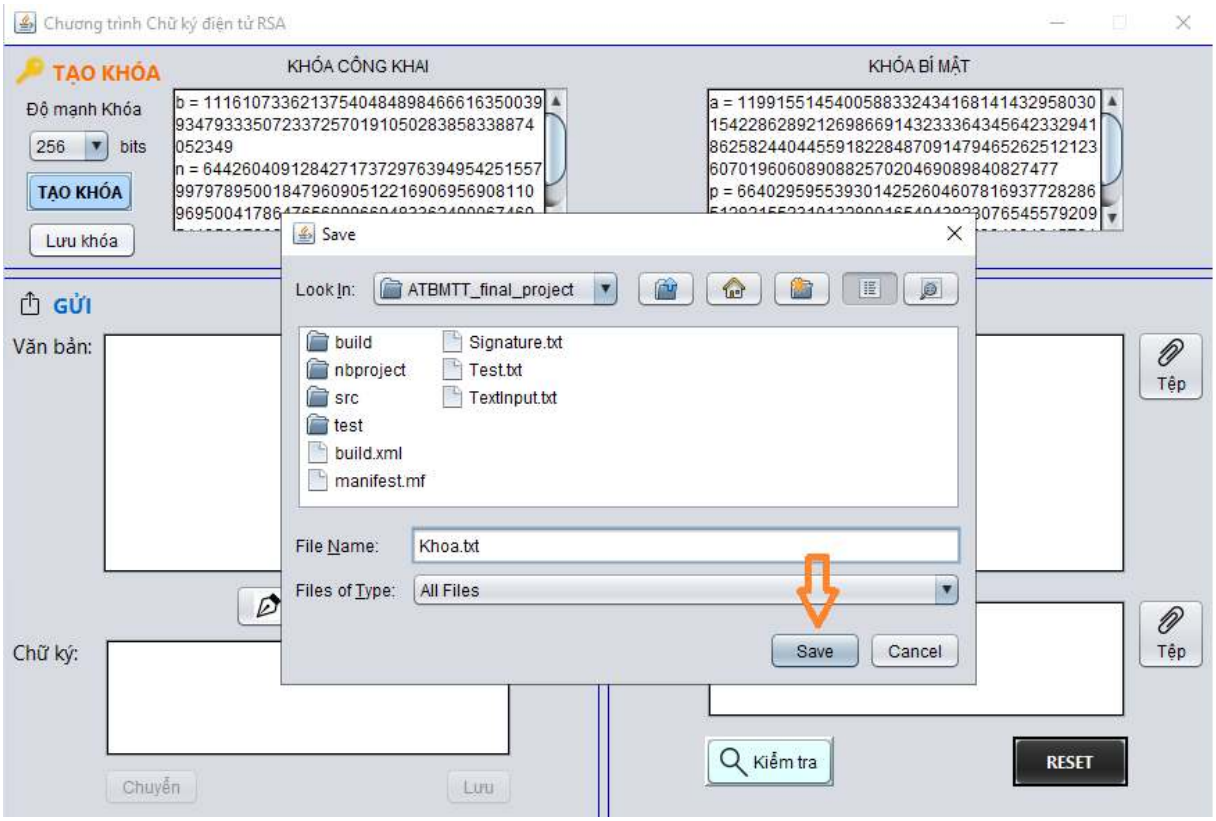


Hình 10. Tạo khóa trong chương trình demo

Sau khi tạo khóa, có thể chọn Lưu khóa để lưu khóa đã tạo ra 1 file trong đường dẫn bất kỳ, chọn tên file rồi bấm Save

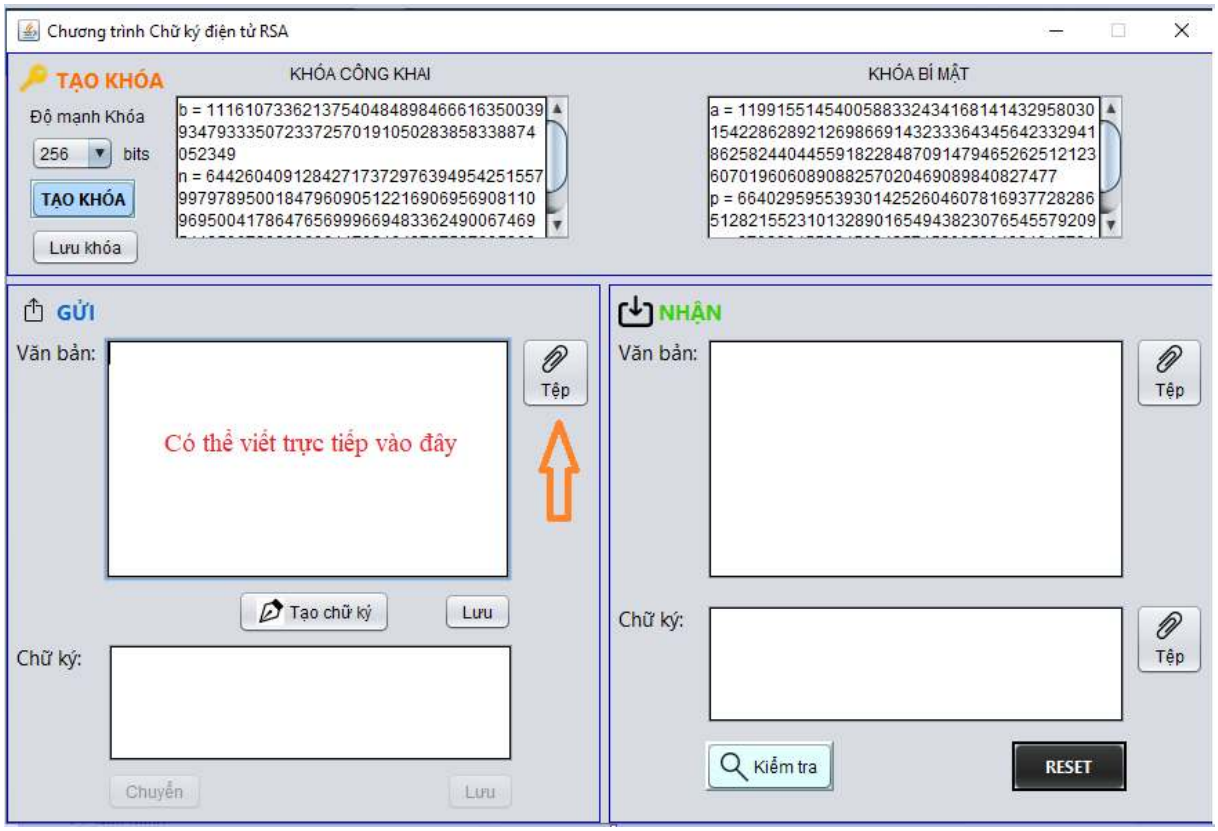


Hình 11. Lưu khóa trong chương trình demo

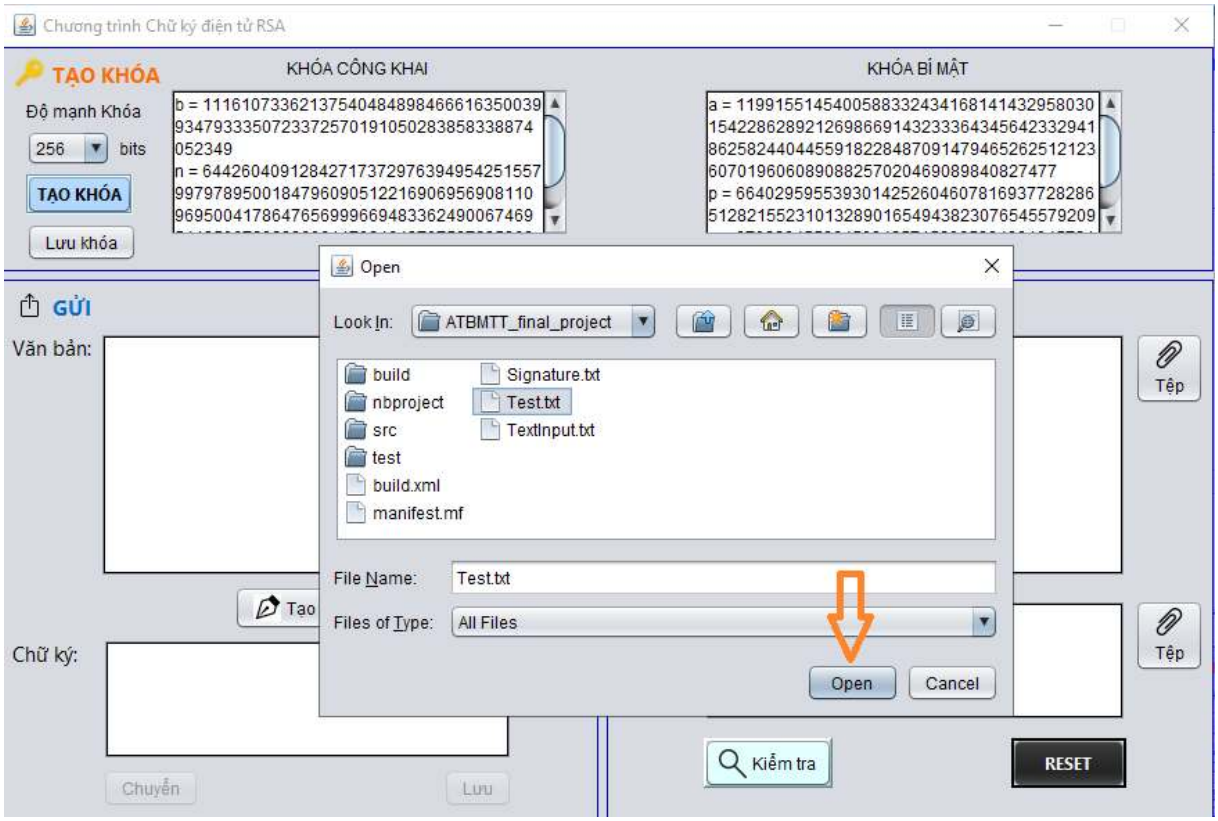


Hình 12. Cửa sổ lưu khóa trong chương trình demo

Gửi: Chọn tệp văn bản bạn muốn gửi bằng cách bấm vào nút Tệp (Hoặc bạn có thể ghi trực tiếp văn bản bạn muốn gửi vào ô trống của phần Văn bản). Khi đã chọn được Tệp, bấm Open.

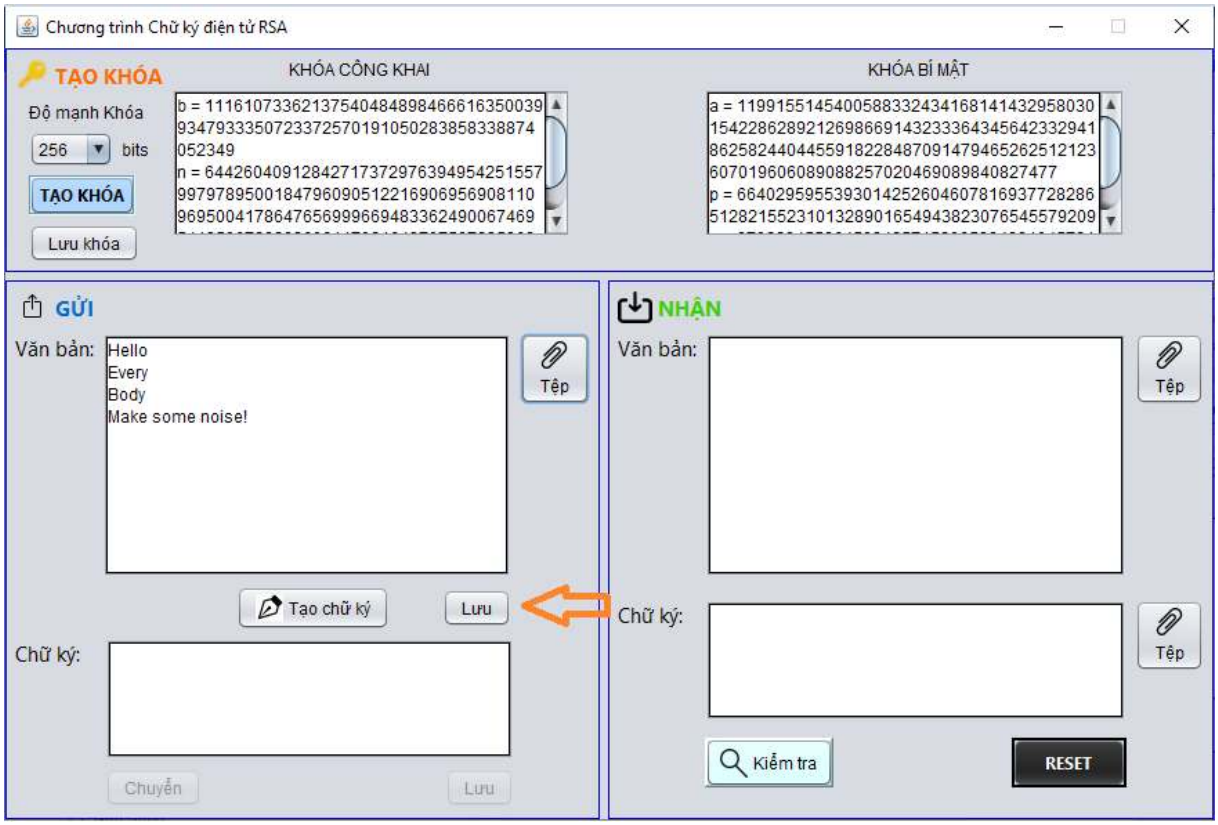


Hình 13. Tạo văn bản để gửi trong chương trình demo

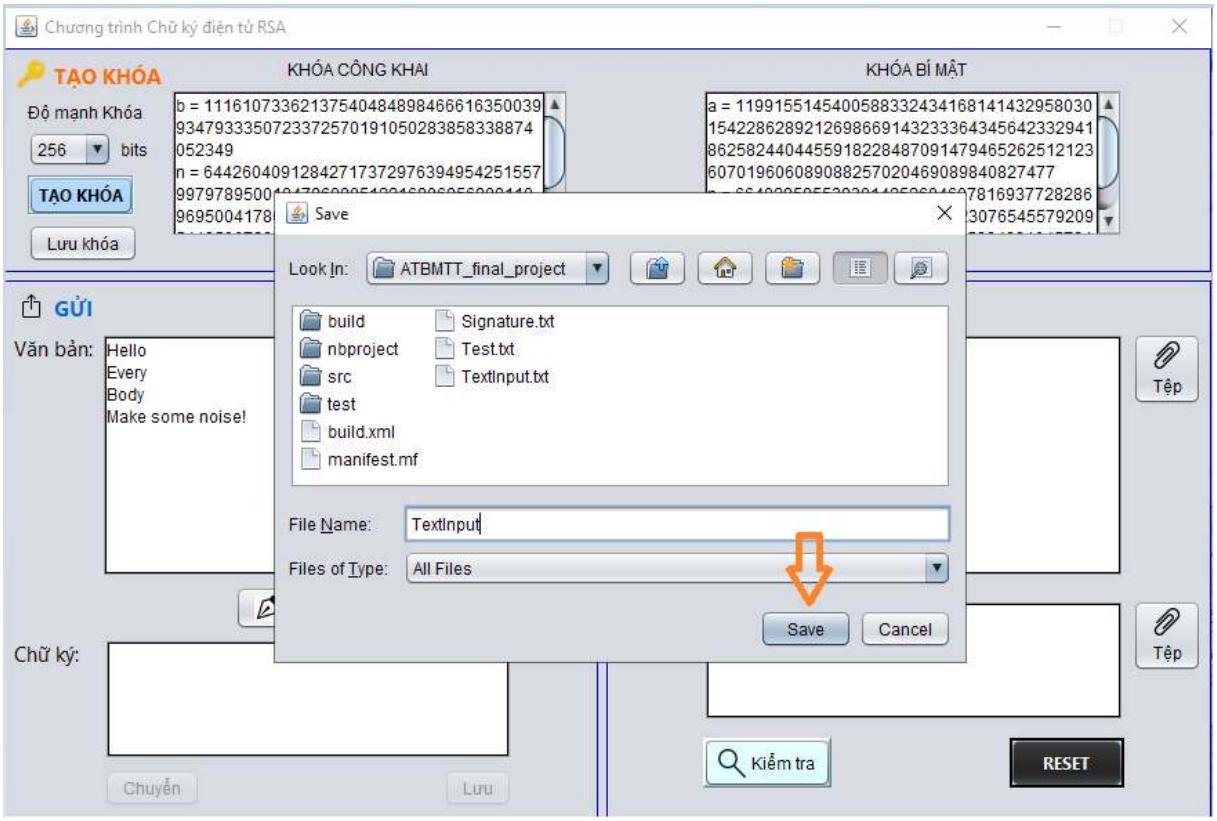


Hình 14. Cửa sổ chọn file văn bản của chương trình demo

Sau khi nhập xong văn bản, nếu bạn nhập thủ công trực tiếp, bạn có thể chọn lưu văn bản bằng cách chọn Lưu, điền tên file và bấm Save.

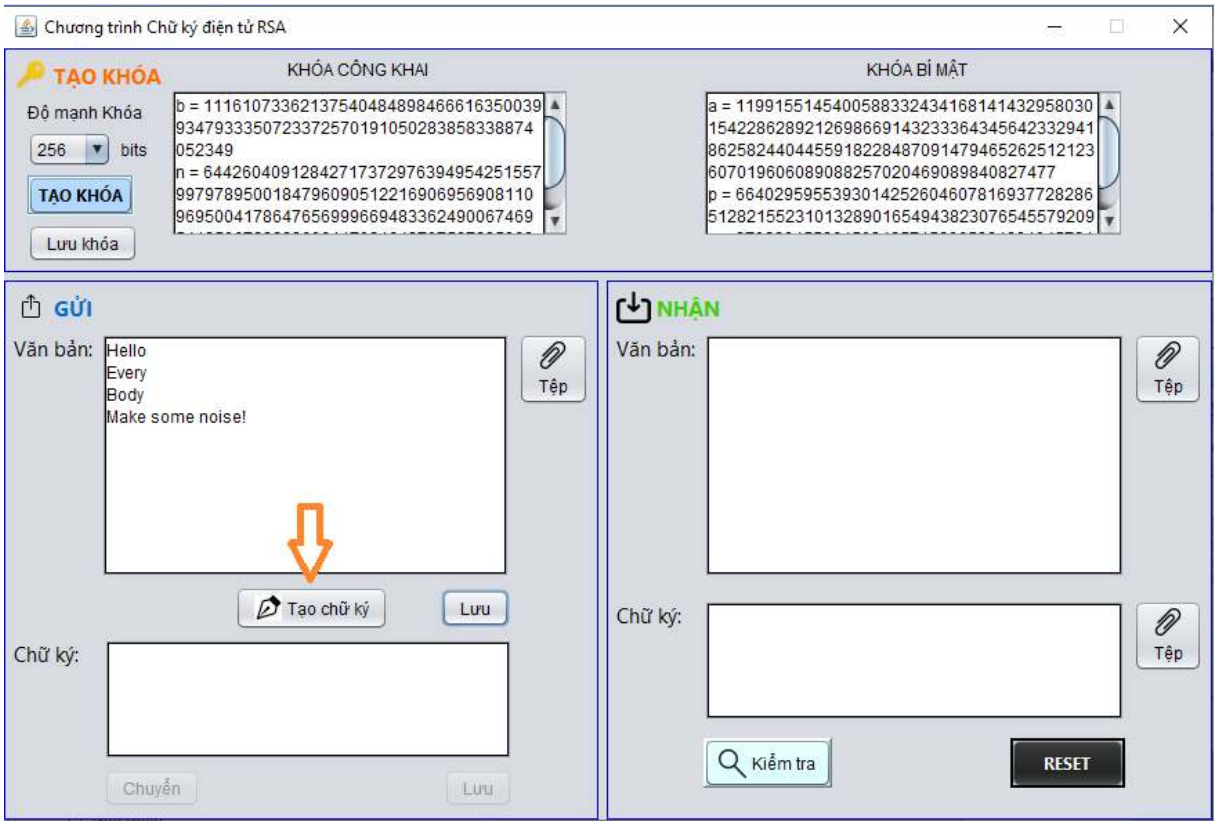


Hình 15. Lưu văn bản để gửi trong chương trình demo



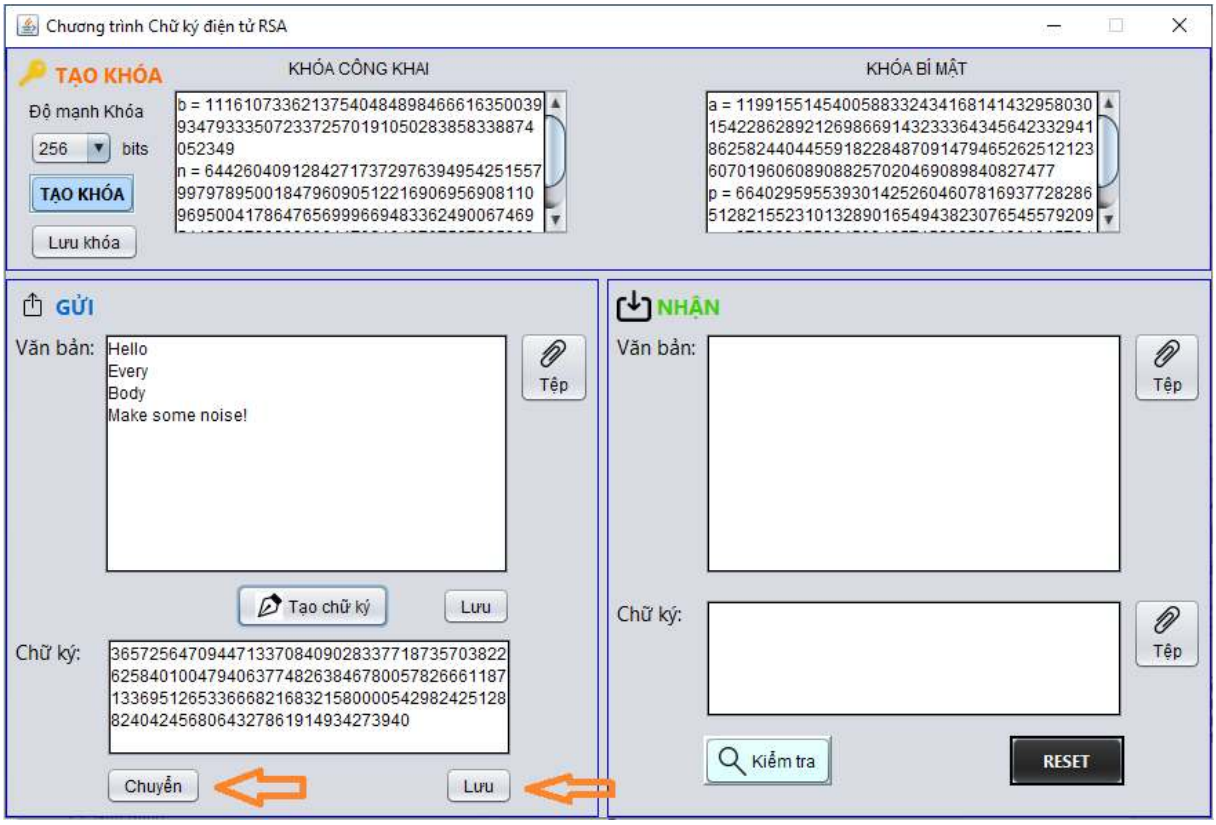
Hình 16. Cửa sổ lưu văn bản trong chương trình demo

Chọn Tạo chữ ký, sau khi tạo chữ ký sẽ hiển thị ở ô bên dưới



Hình 17. Tạo chữ ký trong chương trình demo

Tiếp theo, bạn có thể chọn Chuyển để thông tin về Văn bản và Chữ ký sẽ tự động được chuyển sang phần Nhận. Bạn cũng có thể chọn Lưu để lưu chữ ký tương tự như cách lưu file văn bản.



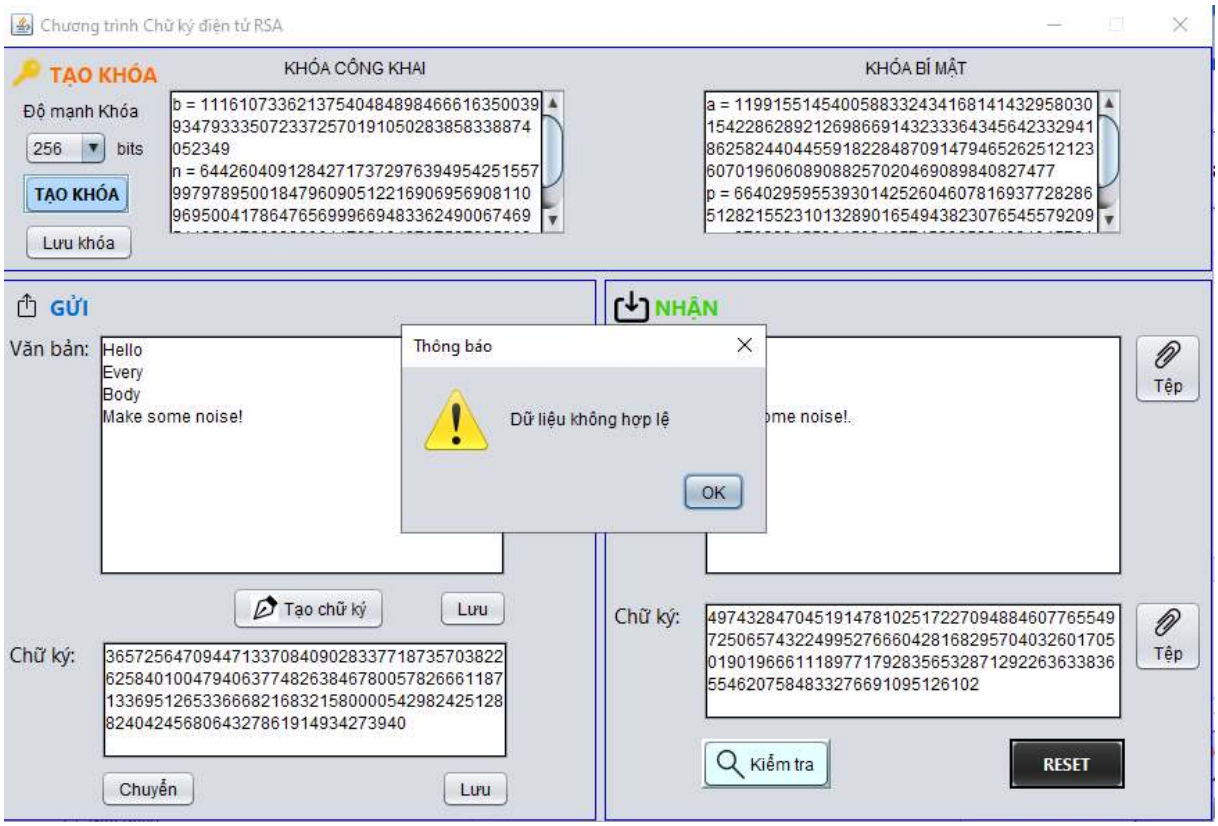
Hình 18. Chuyển hoặc lưu chữ ký trong chương trình demo

Nhận: Bạn có thể nhập thủ công trực tiếp vào ô Văn bản và Chữ ký, hoặc chọn nút Tệp ở bên cạnh 2 ô này để chọn file nhập dữ liệu cho 2 ô trên.

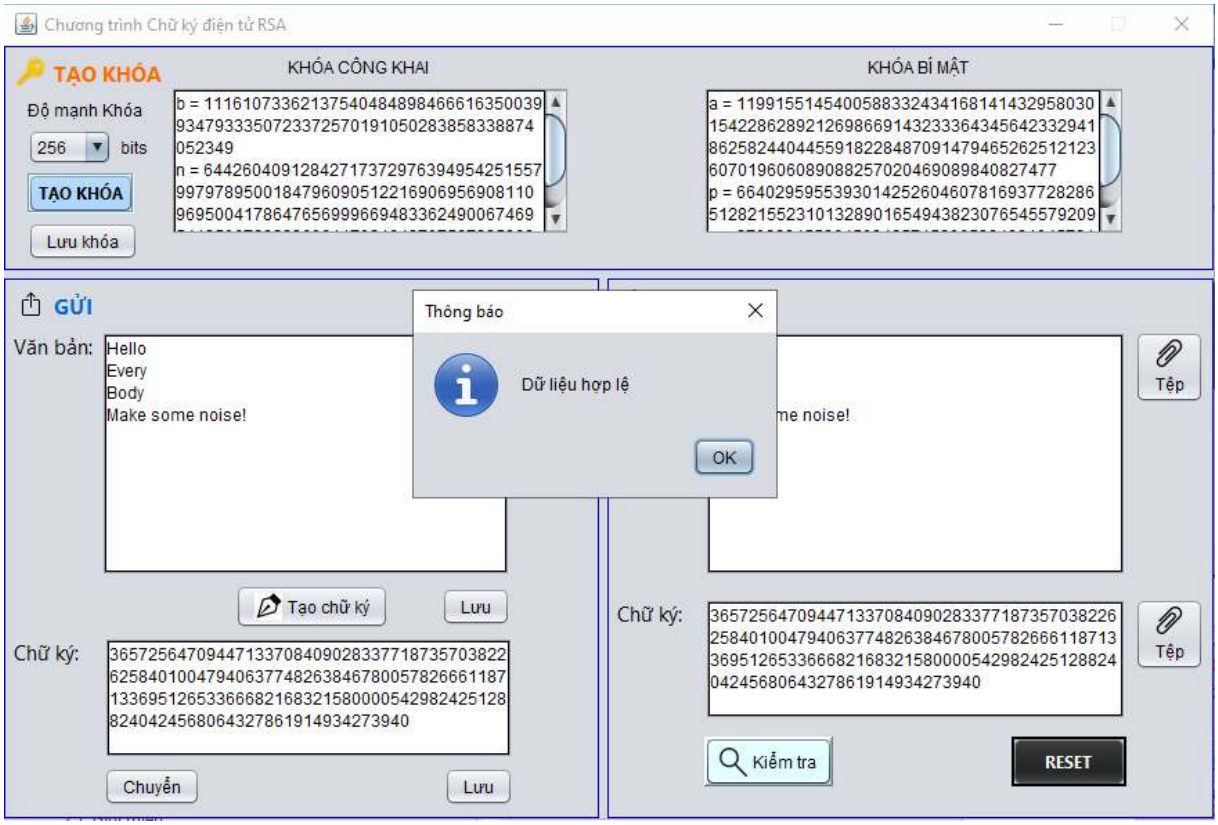
Hình 19. Chọn tệp văn bản và chữ ký trong giao diện Nhận của chương trình demo

Chọn nút Kiểm tra để kiểm tra xem chữ ký có hợp lệ hay không. Chương trình sẽ gửi lại thông báo nếu chữ ký của bạn là hợp lệ (hoặc không hợp lệ)

Hình 20. Kiểm tra dữ liệu trong chương trình demo

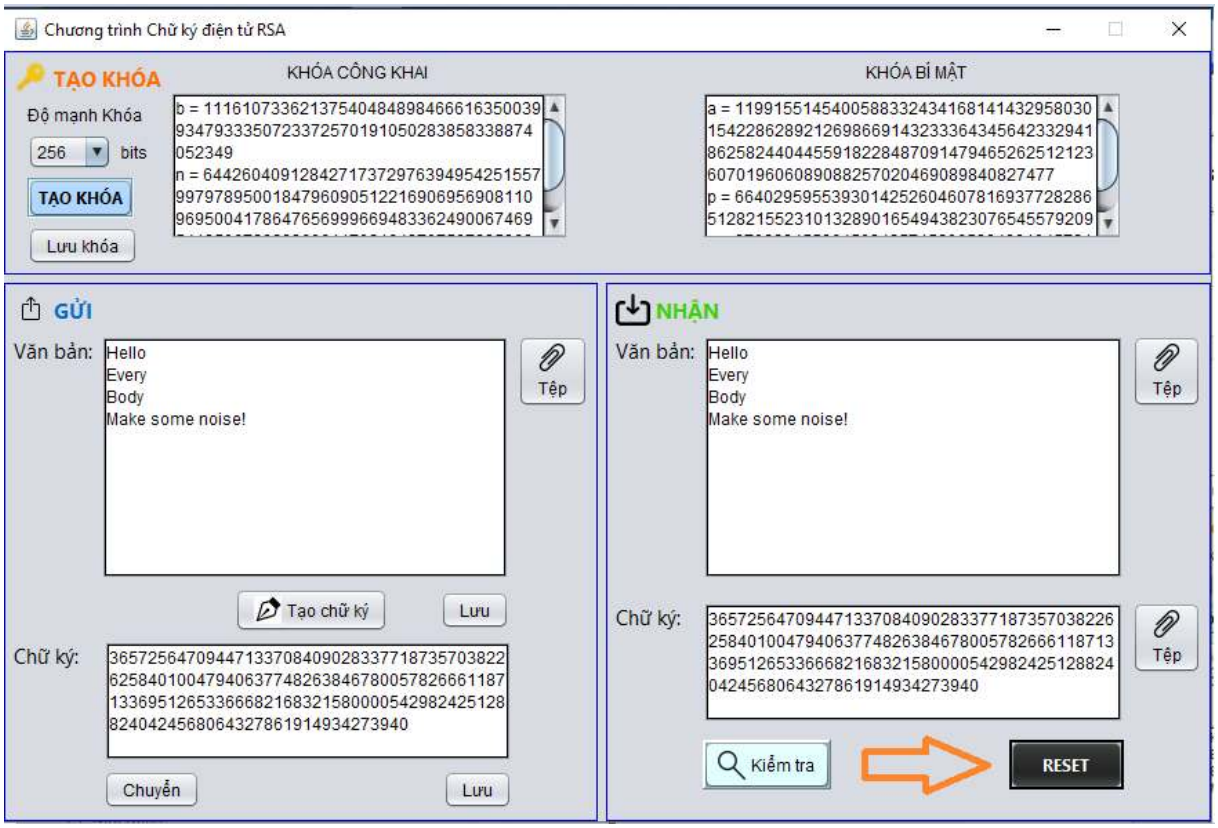


Hình 21. Cửa sổ thông báo dữ liệu không hợp lệ trong chương trình demo



Hình 22. Cửa sổ thông báo dữ liệu hợp lệ trong chương trình demo

Reset: Chọn nút Reset, chương trình quay trở lại trạng thái ban đầu



Hình 23. Reset trong chuwogn trình demo

2.6. Thực hiện bài toán

Phân công công việc của từng thành viên trong nhóm:

Tên sinh viên	Tên công việc
Bùi Quốc Triệu (Nhóm trưởng)	- Làm nội dung chương 3 - Tổng hợp, chỉnh sửa và làm báo cáo - Viết chương trình demo với ngôn ngữ Java
Phạm Bảo Trung (Thư ký)	- Tìm về các khái niệm cơ bản và tìm hiểu về chữ ký điện tử, chữ ký điện tử RSA - Viết chương trình demo với ngôn ngữ C#
Đàm Văn Tú	- Làm nội dung chương 1 - Viết chương trình demo với ngôn ngữ Python
Hoàng Thanh Tú	- Tìm hiểu chữ ký điện tử RSA và Hàm băm MD5 - Viết chương trình demo với ngôn ngữ PHP

Bảng 3. Bảng phân chia nhiệm vụ của các thành viên

CHƯƠNG 3: KIẾN THỨC LĨNH HỘI VÀ BÀI HỌC KINH NGHIỆM

3.1. Nội dung đã thực hiện

- Tìm hiểu và nắm vững được những kiến thức về an toàn và bảo mật thông tin và ứng dụng trong thực tiễn của chúng.

- Tìm hiểu về một số khái niệm cơ bản như:

+ Chữ ký số

+ Chữ ký điện tử RSA

+ Phương pháp mã hóa bất đối xứng ứng dụng trong chữ ký điện tử

+ Hàm băm nói chung và hàm băm MD5 nói riêng

- Tìm hiểu chữ ký điện tử RSA về các nội dung:

+ Các thành phần của chữ ký điện tử RSA

+ Ưu, nhược điểm

+ Nguyên lý hoạt động

+ Quy trình tạo khóa, ký, xác nhận chữ ký RSA

+ Tốc độ, hiệu suất của chữ ký điện tử RSA

+ Ứng dụng của chữ ký điện tử RSA trong thực tế

- Tìm hiểu về hàm băm MD5 về các nội dung:

+ Thuật toán

+ Cấu trúc

+ Ứng dụng

+ Ưu, nhược điểm

- Tìm hiểu về cách hoạt động cũng như lập trình được giao diện của một ngôn ngữ lập trình căn bản (C#, Java, PHP, Python).

- Tìm hiểu về cách triển khai những thuật toán của đề tài được giao vào trong ngôn ngữ lập trình đã chọn

- Tạo ra được ứng dụng với giao diện như yêu cầu và giải quyết được yêu cầu của đề bài

3.2. Kết quả đạt được

- Về kiến thức:

+ Hiểu được về chữ ký điện tử RSA và hàm băm MD5

+ Biết cách phân tích bài toán và giải quyết yêu cầu đặt ra

- Về kĩ năng:

+ Kĩ năng tổ chức, làm việc nhóm

+ Kĩ năng lập trình giao diện và tạo ra một ứng dụng hoàn chỉnh về đề tài được giao

+ Kĩ năng thuyết trình hiệu quả trong công việc

3.3. Hướng phát triển

- Tính khả thi của chủ đề nghiên cứu: Với những kiến thức đã được giảng viên cung cấp sẵn trong quá trình học tập, đồng thời với những kinh nghiệm, kiến thức tổng hợp về các học phần đã được học từ trước, việc thực hiện đề tài là hoàn toàn khả thi. Tuy nhiên, không chỉ bao gồm những kiến thức đã được dạy, sinh viên cũng cần phải tìm tòi, tham khảo các loại tài liệu khác nhau để đưa ra được kết quả cuối cùng một cách hoàn thiện và đạt được các yêu cầu mà bài toán đưa ra.

- Thuận lợi, khó khăn trong quá trình nghiên cứu:

+ Thuận lợi:

- Có được những kiến thức cơ bản thực hiện đề tài được giảng viên cung cấp trước đó.
- Có đủ thời gian nghiên cứu để triển khai đề tài được giao.

+ Khó khăn:

- Cần học thêm nhiều kiến thức bên ngoài để xây dựng được một chương trình với giao diện hoàn chỉnh.
- Giao tiếp, trao đổi giữa các thành viên trong nhóm.

- Hướng phát triển và mở rộng của đề tài:

+ Cá nhân hóa: Kết hợp với lưu trữ dữ liệu bằng hệ quản trị dữ liệu để tang tính bảo mật, thêm chức năng đăng nhập tài khoản để cá nhân hóa cho từng người đồng thời giúp cho phần mềm có thể sử dụng cho nhiều người

Hình 24. Minh họa hướng phát triển Cá nhân hóa

+ Phát triển phần mềm cho nhiều người sử dụng: Không chỉ cho một người sử dụng, phần mềm có thể phát triển thêm để ứng dụng có thể gửi và nhận thông tin từ các tài khoản các khau. Gửi thông tin cho người ta muốn gửi thông qua mã định danh cá nhân tài khoản của người dùng mà ta muốn gửi cung cấp.

Hình 25. Minh họa hướng phát triển Cho nhiều người sử dụng

+ Triển khai đa nền tảng: biến chương trình đã thực hiện xây dựng và chạy được trên đa nền tảng, giúp việc truyền tải thông tin không chỉ trên một loại thiết bị mà có thể thực hiện trên loại thiết bị khác nhau.

Hình 26. Minh họa hướng phát triển Đa nền tảng

+ Xây dựng cổng thông tin trao đổi thông tin giữa các cơ quan, tổ chức với nhau

Hình 27. Minh họa hướng phát triển Cổng thông tin

+ Kết hợp với các phần mềm ứng dụng khác để xác nhận người dùng, tính toàn vẹn của dữ liệu và trách nhiệm của mỗi bên như trong các phần mềm với các hoạt động: mua bán, đặt hàng trực tuyến; thanh toán trực tuyến; giao dịch online; giao dịch ngân hang; giao dịch email; ...

Hình 28. Minh họa hướng phát triển Tích hợp với ứng dụng khác

TÀI LIỆU THAM KHẢO

I. Tài liệu tiếng Việt

1. https://viblo.asia/p/gioi-thieu-ham-bam-md5-LzD5d63wZjY
2. https://vi.wikipedia.org/wiki/MD5
3. https://vi.wikipedia.org/wiki/RSA_(m%C3%A3_h%C3%B3a)
4. https://viblo.asia/p/he-ma-hoa-rsa-va-chu-ky-so-6J3ZgkgMZmB
5. https://viblo.asia/p/tim-hieu-ve-chu-ky-so-va-ung-dung-jvElay0Nlkw

II. Tài liệu tiếng Anh

1. https://en.wikipedia.org/wiki/MD5

PHỤ LỤC

1. Hình minh họa:

2. Bảng biểu