**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**

**KHOA CÔNG NGHỆ THÔNG TIN**

**BÀI TẬP LỚN**

**MÔN: AN TOÀN VÀ BẢO MẬT THÔNG TIN**

**Đề tài 3:**

**Ứng dụng của RSA trong chữ ký số và**

**Demo sản phẩm minh họa**

|  |  |
| --- | --- |
| **Giảng viên hướng dẫn** | **: TS.Lê Thị Anh** |
| **Lớp** | **: 20231IT6001001** |
| **Nhóm** | **: 12** |
| **Thành viên nhóm:** | **: Phạm Thị Thùy Trang – 2021604802**  **: Hà Thị An – 2021602015**  **: Nghiêm Hồng Nhung – 2021606477**  **: Trịnh Hương Lan – 2021601499**  **: Nguyễn Như Quỳnh – 2021607666**  **: Vũ Mỹ Duyên - 2021603620** |

**Hà Nội - 2023**

# Lời Cảm ơn

Để có được một bài báo cáo bổ ích, hiệu quả, hoàn chỉnh và đạt kết quả tốt nhất trước hết nhóm em xin gửi tới toàn thể các thầy cô khoa Công nghệ thông tin lời chúc sức khỏe, lời chào chân trọng và lời cảm ơn sâu sắc nhất. Với sự quan tâm, dạy dỗ chỉ bảo tận tình chu đáo của cô Lê Thị Anh, sự giúp đỡ nhiệt tình của các bạn, đến nay nhóm em đã có thể hoàn thành bài báo cáo, đề tài**: Ứng dụng của RSA trong chữ ký số. Demo sản phẩm minh họa**

Nhóm 12 xin gửi lời cảm ơn chân thành nhất tới cô Lê Thị Anh - Giảng viên môn “An toàn và bảo mật thông tin” đã quan tâm, giúp đỡ, vạch kế hoạch hướng dẫn Nhóm 12 hoàn thành một cách tốt nhất bài báo cáo trong thời gian qua. Hơn thế nữa, chúng em đã học được thêm nhiều kiến thức mới cũng như phát triển thêm một số kỹ năng mềm như: Kỹ năng làm việc nhóm, kỹ năng quản lý thời gian,… Cảm ơn cô đã tận tình chỉ bảo, hướng dẫn nhóm trong quá trình học tập và thực hiện đề tài.

Với điều kiện thời gian có hạn cũng như kinh nghiệm còn hạn chế nên bài báo cáo sẽ không tránh khỏi những thiếu sót. Nhóm 12 rất mong nhận được sự chỉ bảo, đóng góp ý kiến của cô để nhóm em có điều kiện bổ sung, nâng cao kiến thức của mình, phục vụ tốt hơn công tác thực tế sau này.

Chúng em xin trân thành cảm ơn!

# Bảng phân công công việc

|  |  |  |
| --- | --- | --- |
| STT | Họ và tên | Tên công việc |
| 1 | Phạm Thị Thùy Trang | * Lý do chọn đề tài. * Chữ ký điện tử. * Kết quả thực hiện. |
| 2 | Hà Thị An | * Đối tượng và phạm vi nghiên cứu. * Giới thiệu về ứng dụng của RSA trong chữ ký số điện tử. * Kiến thức lĩnh hội và bài học kinh nghiệm. |
| 3 | Nghiêm Hồng Nhung | * Phương pháp mã hóa đối xứng. * Tổng quan an toàn và bảo mật thông tin. * Phân tích thiết kế. |
| 4 | Trịnh Hương Lan | * Chữ ký số RSA. * Kiến thức lĩnh hội và bài học kinh nghiệm. * Tổng hợp nội dung và viết báo cáo. |
| 5 | Nguyễn Như Quỳnh | * Thiết kế Powerpoint. * Bố cục đề tài. |
| 6 | Vũ Mỹ Duyên | * Hàm băm . * Phân tích thiết kế. |

# Mục lục

[Lời Cảm ơn 2](#_Toc154258343)

[Mục lục 4](#_Toc154258344)

[Danh mục hình ảnh 5](#_Toc154258345)

[Lời mở đầu 6](#_Toc154258346)

[CHƯƠNG 1: Tổng quan 10](#_Toc154258347)

[1.1 Giới thiệu về ứng dụng của RSA trong chữ ký số điện tử 10](#_Toc154258348)

[1.2 Chữ kí số 11](#_Toc154258349)

[1.2.1. Khái niệm 11](#_Toc154258350)

[1.2.2. Ưu, nhược điểm 11](#_Toc154258351)

[1.2.3. Nguyên lý hoạt động 13](#_Toc154258352)

[1.3 Phương pháp mã hóa bất đối xứng 15](#_Toc154258353)

[1.3.1. Khái niệm 15](#_Toc154258354)

[1.3.2. Ưu, nhược điểm 16](#_Toc154258355)

[1.3.3. Ứng dụng của phương pháp mã hóa bất đối xứng của RSA trong chữ ký số điện tử. 17](#_Toc154258356)

[1.4 Chữ ký số RSA 17](#_Toc154258357)

[1.4.1. Khái niệm 17](#_Toc154258358)

[1.4.2. Cấu tạo 17](#_Toc154258359)

[1.4.3. Nội dung thuật toán 18](#_Toc154258360)

[1.4.4. Thám mã hệ mã RSA 19](#_Toc154258361)

[1.5 Hàm băm MD5 19](#_Toc154258362)

[1.5.1. Khái niệm 19](#_Toc154258363)

[1.5.2. Một số hàm băm phổ biến 20](#_Toc154258364)

[1.5.3. Ưu, nhược điểm 22](#_Toc154258365)

[CHƯƠNG 2: Phân tích thiết kế 23](#_Toc154258366)

[2.1 Phân tích “Ứng dụng Chữ ký số điện tử RSA” 23](#_Toc154258367)

[2.2 Phân tích yêu cầu 24](#_Toc154258368)

[2.3 Phân tích chức năng 26](#_Toc154258369)

[CHƯƠNG 3: Kết quả thực hiện 29](#_Toc154258370)

[3.1 Giao diện chương trình 29](#_Toc154258371)

[3.2 Giới thiệu công cụ triển khai 29](#_Toc154258372)

[3.3 Hướng dẫn cài đặt và chạy chương trình 30](#_Toc154258373)

[3.3.1. Cài đặt thư viện 30](#_Toc154258374)

[3.3.2. Demo chương trình 31](#_Toc154258375)

[CHƯƠNG 4: Kiến thức lĩnh hội và bài học kinh nghiệm 40](#_Toc154258376)

[4.1 Kiến thức lĩnh hội 40](#_Toc154258377)

[4.2 Bài học kinh nghiệm 40](#_Toc154258378)

[4.3 Hướng phát triển 41](#_Toc154258379)

[Tài liệu tham khảo 43](#_Toc154258380)

# Danh mục hình ảnh

[Hình ảnh 1: Quá trình tạo chữ ký 14](file:///C:\Users\SonTrinh\Documents\Báo%20cáo%20ATBMTT.docx#_Toc154258873)

[Hình ảnh 2: Quá trình kiểm tra chữ ký 15](file:///C:\Users\SonTrinh\Documents\Báo%20cáo%20ATBMTT.docx#_Toc154258874)

[Hình ảnh 3 Sơ đồ biểu hiện RSA mã hóa thuật toán. 18](#_Toc154258875)

[Hình ảnh 4: Hàm băm 20](#_Toc154258876)

[Hình ảnh 5: Giải thuật MD5 21](#_Toc154258877)

[Hình ảnh 6: Sơ đồ hệ thống chữ ký số RSA 24](#_Toc154258878)

[Hình ảnh 7: Chức năng tạo chữ ký số và thẩm định chữ ký số 27](file:///C:\Users\SonTrinh\Documents\Báo%20cáo%20ATBMTT.docx#_Toc154258879)

[Hình ảnh 8: Giao diện ban đầu của chương trình 29](file:///C:\Users\SonTrinh\Documents\Báo%20cáo%20ATBMTT.docx#_Toc154258880)

[Hình ảnh 9: Cài đặt thư viện PyQt6 30](file:///C:\Users\SonTrinh\Documents\Báo%20cáo%20ATBMTT.docx#_Toc154258881)

[Hình ảnh 10: Cài đặt thư viện docx 31](file:///C:\Users\SonTrinh\Documents\Báo%20cáo%20ATBMTT.docx#_Toc154258882)

[Hình ảnh 11: Tạo khóa tự động 31](file:///C:\Users\SonTrinh\Documents\Báo%20cáo%20ATBMTT.docx#_Toc154258883)

[Hình ảnh 12: Xác nhận tạo khóa công khai 32](file:///C:\Users\SonTrinh\Documents\Báo%20cáo%20ATBMTT.docx#_Toc154258884)

[Hình ảnh 13: Mã hóa chữ ký 33](file:///C:\Users\SonTrinh\Documents\Báo%20cáo%20ATBMTT.docx#_Toc154258885)

[Hình ảnh 14: Nhận khóa công khai 34](file:///C:\Users\SonTrinh\Documents\Báo%20cáo%20ATBMTT.docx#_Toc154258886)

[Hình ảnh 15: Lưu văn bản mã hóa thành file 35](file:///C:\Users\SonTrinh\Documents\Báo%20cáo%20ATBMTT.docx#_Toc154258887)

[Hình ảnh 16: Giao diện để lưu file 35](#_Toc154258888)

[Hình ảnh 17: Chuyển tiếp văn bản mã hóa 36](file:///C:\Users\SonTrinh\Documents\Báo%20cáo%20ATBMTT.docx#_Toc154258889)

[Hình ảnh 18: Mở văn bản đã được mã hóa 37](file:///C:\Users\SonTrinh\Documents\Báo%20cáo%20ATBMTT.docx#_Toc154258890)

[Hình ảnh 19: Kiểm tra tính đúng sai của mã hóa chữ ký 38](file:///C:\Users\SonTrinh\Documents\Báo%20cáo%20ATBMTT.docx#_Toc154258891)

# Lời mở đầu

1. **Lý do chọn đề tài**

Bảo mật thông tin luôn là vấn đề quan trong hàng đầu trong các lĩnh vực tình báo, quân sự, ngoại giao và đây cũng là một vấn đề đã được nghiên cứu hàng nghìn năm nay. Bảo mật thông tin là duy trì tính bảo mật, tính toàn vẹn và tính sẵn sàng của thông tin. Bảo mật nghĩa là đảm bảo thông tin chỉ được tiếp cận bởi những người được cấp quyền tương ứng. Tính toàn vẹn là bảo vệ sự chính xác, hoàn chỉnh của thông tin và thông tin chỉ được thay đổi bởi những người được cấp quyền. Tính sẵn sàng của thông tin là những người được quyền sử dụng có thể truy xuất thông tin khi họ cần. Vấn đề bảo mật đang được nhiều người tập trung nghiên cứu và tìm mọi phương pháp để đảm bảo an toàn, an ninh cho hệ thống phần mềm, đặc biệt là các hệ thống thông tin trên mạng. Việc chọn đề tài nghiên cứu về “Ứng dụng của RSA trong chữ ký số. Demo sản phẩm minh họa” là một quyết định có tính chiến lược và mang lại nhiều lợi ích đối với cả cộng đồng doanh nghiệp và người sử dụng.

Chữ ký điện tử đóng vai trò quan trọng trong việc bảo vệ thông tin. Trong môi trường số hóa ngày nay, thông tin di động và truyền tải nhanh chóng, và đôi khi nó có thể bị đe dọa bởi các mối quan ngại về bảo mật. Chữ ký điện tử không chỉ đảm bảo tính toàn vẹn của dữ liệu mà còn xác định nguồn gốc của nó, từ đó tạo nên một lớp an ninh bổ sung. Mặt pháp lý cũng là một yếu tố quan trọng khi chọn đề tài này. Việc nghiên cứu về chữ ký điện tử giúp hiểu rõ hơn về những quy định và chuẩn mực pháp luật liên quan. Sự chấp nhận pháp lý của chữ ký điện tử tăng cường khả năng sử dụng chúng trong các giao dịch pháp lý và kinh doanh quốc tế, mở ra cơ hội mới cho sự phát triển của các doanh nghiệp và tổ chức.

Ngoài ra, chữ ký điện tử mang lại hiệu suất và tính tiện ích cao. Việc ký kết và xác nhận các tài liệu có thể diễn ra một cách nhanh chóng và thuận tiện, giúp tối ưu hóa quy trình làm việc và tiết kiệm thời gian cho cả cá nhân và tổ chức. Chữ ký điện tử còn liên quan đến sự phát triển của công nghệ blockchain. Kết hợp chữ ký điện tử với blockchain mang lại lợi ích về minh bạch và đáng tin cậy, giúp tăng cường sự tin tưởng trong các quá trình giao dịch và lưu trữ dữ liệu.

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. RSA được sử dụng để tạo ra cặp khóa (khóa riêng tư và khóa công khai) để thực hiện quá trình ký và xác nhận chữ ký số điện tử. Khóa riêng tư được giữ bí mật và chỉ được sử dụng để ký, trong khi khóa công khai được chia sẻ và dùng để xác nhận chữ ký. Các ưu điểm của RSA 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: Python, C++, C#, Java, Php, JavaScript, …

Vì thế, nhóm chúng e chọn đề tài nghiên cứu “Ứng dụng của RSA trong chữ ký số điện tử”. 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. Đề tài này chúng ta cần nắm vững được cách mã hóa thông tin bằng hệ mã hóa RSA và cách áp dụng chữ ký điện tử trong an toàn và bảo mật thông tin.

1. **Tổng quan**

An toàn và bảo mật thông tin là một lĩnh vực liên quan đến việc bảo vệ thông tin khỏi những truy cập, sử dụng, tiết lộ, thay đổi hoặc phá hủy trái phép. Thông tin có thể là dữ liệu cá nhân, thông tin kinh doanh, thông tin bí mật nhà nước, hoặc bất kỳ loại thông tin nào khác có giá trị đối với cá nhân, tổ chức hoặc quốc gia.

Ba nguyên tắc cơ bản của an toàn và bảo mật thông tin là: Tính bảo mật, tính toàn vẹn và tính sẵn sàng. Các mối đe dọa an toàn và bảo mật thông tin bao gồm: Truy cập trái phép (Đây là mối đe dọa phổ biến nhất đối với an toàn và bảo mật thông tin), sử dụng trái phép, tiết lộ thông tin, thay đổi thông tin, phá hủy thông tin. Có nhiều biện pháp khác nhau có thể được thực hiện để bảo vệ an toàn và bảo mật thông tin như: quản lý truy cập, mật mã hóa, sao lưu, giáo dục người dùng.

An toàn và bảo mật thông tin là một lĩnh vực quan trọng đối với tất cả cá nhân và tổ chức. Bằng cách thực hiện các biện pháp bảo vệ thích hợp, chúng ta có thể giúp bảo vệ thông tin của mình khỏi những truy cập, sử dụng, tiết lộ, thay đổi hoặc phá hủy trái phép.

1. **Mục đích nghiên cứu**

Đề tài nghiên cứu các kỹ thuật bảo mật thông tin phục vụ cho việc phân tích thiết kế và xây dựng ứng dụng chữ ký số điện tử RSA.

1. **Đối tượng và phạm vi nghiên cứu**

* Đối tượng nghiên cứu:

RSA có thể được sử dụng để tạo và xác thực chữ ký số điện tử cho người dùng, các tổ chức và doanh nghiệp. Chữ ký số điện tử RSA đảm bảo tính toàn vẹn và xác thực của thông tin kỹ thuật số.

Ngoài ra, RSA còn có thể được áp dụng trong việc tạo và xác thực chữ ký số điện tử cho các cơ quan chính phủ, đảm bảo tính bảo mật và xác thực của thông tin quan trọng

* Phạm vi nghiên cứu: Nghiên cứu ứng dụng của RSA trong chữ ký số điện tử.

1. **Bố cục đề tài**

Đề tài của chúng em được triển khai và gói gọn trong 4 chương, cụ thể như sau:

Chương 1: Tổng quan.

Chương 2: Phân tích thiết kế.

Chương 3: Kết quả thực hiện.

Chương 4: Kiến thức lĩnh hội và bài học kinh nghiệm.

# Tổng quan

## Giới thiệu về ứng dụng của RSA trong chữ ký số điện tử

RSA (Rivest-Shamir-Adleman) là một thuật toán mã hóa công khai được sử dụng rộng rãi trong lĩnh vực bảo mật thông tin. Nó cũng được áp dụng trong chữ ký số điện tử để đảm bảo tính toàn vẹn và xác thực của thông tin điện tử. Dưới đây là một số ứng dụng của RSA trong chữ ký số điện tử:

* Tạo chữ ký số điện tử: RSA cho phép người dùng tạo ra cặp khóa bao gồm khóa công khai và khóa bí mật. Người dùng sử dụng khóa bí mật để tạo chữ ký số điện tử cho một tài liệu hoặc thông điệp. Quá trình tạo chữ ký RSA bao gồm việc áp dụng hàm băm (Hash function) cho tài liệu và sau đó ký số hóa kết quả băm bằng khóa bí mật.
* Xác thực chữ ký số điện tử: Đối tượng nhận thông điệp có thể sử dụng khóa công khai tương ứng để xác thực chữ ký số điện tử. Quá trình xác thực chữ ký RSA bao gồm giải mã chữ ký số điện tử bằng khóa công khai để thu được giá trị băm. Sau đó, người nhận so sánh giá trị băm thu được với giá trị băm của tài liệu ban đầu. Nếu hai giá trị băm khớp nhau, điều đó chứng tỏ chữ ký số điện tử là hợp lệ và tài liệu không bị thay đổi trong quá trình truyền tải.
* Tính bảo mật và toàn vẹn: RSA cung cấp tính bảo mật cao vì quá trình tạo chữ ký số điện tử dựa trên khóa bí mật không thể suy luận được từ khóa công khai. Nếu khóa bí mật được bảo mật tốt, không có ai khác ngoài người tạo chữ ký có thể tạo chữ ký hợp lệ cho thông điệp. Nếu thông điệp bị thay đổi sau khi được ký, giá trị băm sẽ khác nhau và chữ ký sẽ không được xác thực.

Ứng dụng của RSA trong chữ ký số điện tử đảm bảo tính toàn vẹn, xác thực và không thể chối bỏ của thông tin điện tử. Nó được sử dụng rộng rãi trong giao dịch điện tử, chứng thực người dùng, xác nhận tài liệu quan trọng và nhiều ứng dụng khác liên quan đến bảo mật thông tin.

## Chữ kí số

### Khái niệm

Chữ ký số là mô hình sử dụng các kỹ thuật mật mã để gắn với mỗi người sử dụng một cặp khóa công khai – bí mật và qua đó có thể ký các văn bản điện tử cũng như trao đổi các thông tin mật.

### Ưu, nhược điểm

1. Ưu điểm

* Tính xác thực:

Mỗi chữ ký số được xây dựng bằng các hệ thống mã hoá bất đối xứng và hàm băm. Hệ mã hoá bất đối xứng tạo ra 2 khoá riêng biệt: 1 khoá công khai (public key) được share cho tất cả mọi người biết, có công dụng dùng để xác minh văn bản và chữ ký đi kèm là của đúng người chủ sở hữu gửi; 1 khoá bí mật (private key) được giữ kín bí mật chỉ có người gửi biết. Quy trình xác thực chữ ký số sẽ phân tích và so sánh 2 chuỗi mã hoá của 2 chữ ký (được tạo ra bằng hàm băm) để xác thực chủ sở hữu của văn bản đã được ký đó là người gửi chứ không phải ai khác. Cũng khó có thể tránh khỏi việc chữ ký bị giả mạo, thế nhưng nếu chúng ta quản lý tốt chữ ký số thì tỉ lệ giả mạo sẽ rất thấp.

* Tính toàn vẹn và bảo mật

Giả sử A cần gửi cho B một thông điệp mật kèm chữ ký điện tử, A sẽ sử dụng khoá công khai của B để mã hoá thông điệp rồi dùng khoá cá nhân của mình để mã hoá chữ ký, sau đó gửi cả thông điệp lẫn chữ ký cho B. B sẽ dùng khoá công khai của A để giải mã chữ ký, rồi dùng khoá cá nhân của mình để giải mã thông điệp của A. Văn bản được bảo vệ và xác thực qua nhiều lớp, đảm bảo và xác nhận nội dung của văn bản được ký không bị sửa đổi, đem lại sự tin tưởng cho các bên tham gia giao dịch.Việc tạo chữ ký và kiểm chứng chữ ký thường được thực hiện nhờ hàm băm nên các mã hash tạo ra không trùng nhau và chỉ được sử dụng duy nhất trong 1 giao dịch, ngăn việc sử dụng lại chữ ký số nhằm mục đích khác.

* Tính trách nhiệm và duy nhất

Vì chỉ có người gửi mới có khoá bí mật để tạo chữ ký số, giảm thiểu việc một bên giao dịch trốn tránh và từ chối văn bản đã gửi là của mình, chữ ký số bảo vệ quyền lợi của bên hợp tác còn lại và cũng có thể được dùng làm chứng cứ để bên thứ ba giải quyết.

* Tiết kiệm thời gian, công sức

Thay thế cho việc vận chuyển văn bản, thực hiện ký tay theo cách thủ công, chữ ký số giúp giảm thiểu thời gian, chi phí hành chính và phương tiện để các bên giao dịch có thể ký số một cách nhanh chóng, chính xác và an toàn, mọi lúc mọi nơi, không cần chuẩn bị hồ sơ bản cứng lẫn sắp xếp nhân sự để thực hiện ký kết

* Tính linh động

Dựa theo nhu cầu sử dụng và phù hợp với mọi đối tượng sử dụng từ văn phòng đến cá nhân, từ công nhân đến doanh nhân, chữ ký số chia thành hai dạng:

+ Sử dụng USB Token chứa chữ ký số: Loại chữ ký số thông dụng nhất dành cho các công ty văn phòng sử dụng với lưu lượng vừa phải, gồm một chiếc USB token có chứa các thông tin của khách hàng, lưu giữ khóa bí mật và chứng thư số của thuê

+ Chữ ký số không cần sử dụng USB token: Thường gọi là chữ ký số online, sử dụng công nghệ đám mây (cloud - based) giúp việc ký văn bản trở nên đơn giản, tiết kiệm chi phí và có thể thực hiện mọi lúc mọi nơi

1. 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, …

### Nguyên lý hoạt động

1. Quá trình ký

* Bước 1: Tạo khóa bằng hệ mã hóa gồm khóa bí mật và khóa công khai. Sử dụng khóa bí mật để tạo chữ ký.
* Bước 2: 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.
* Bước 3: 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.
* Bước 4: 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.

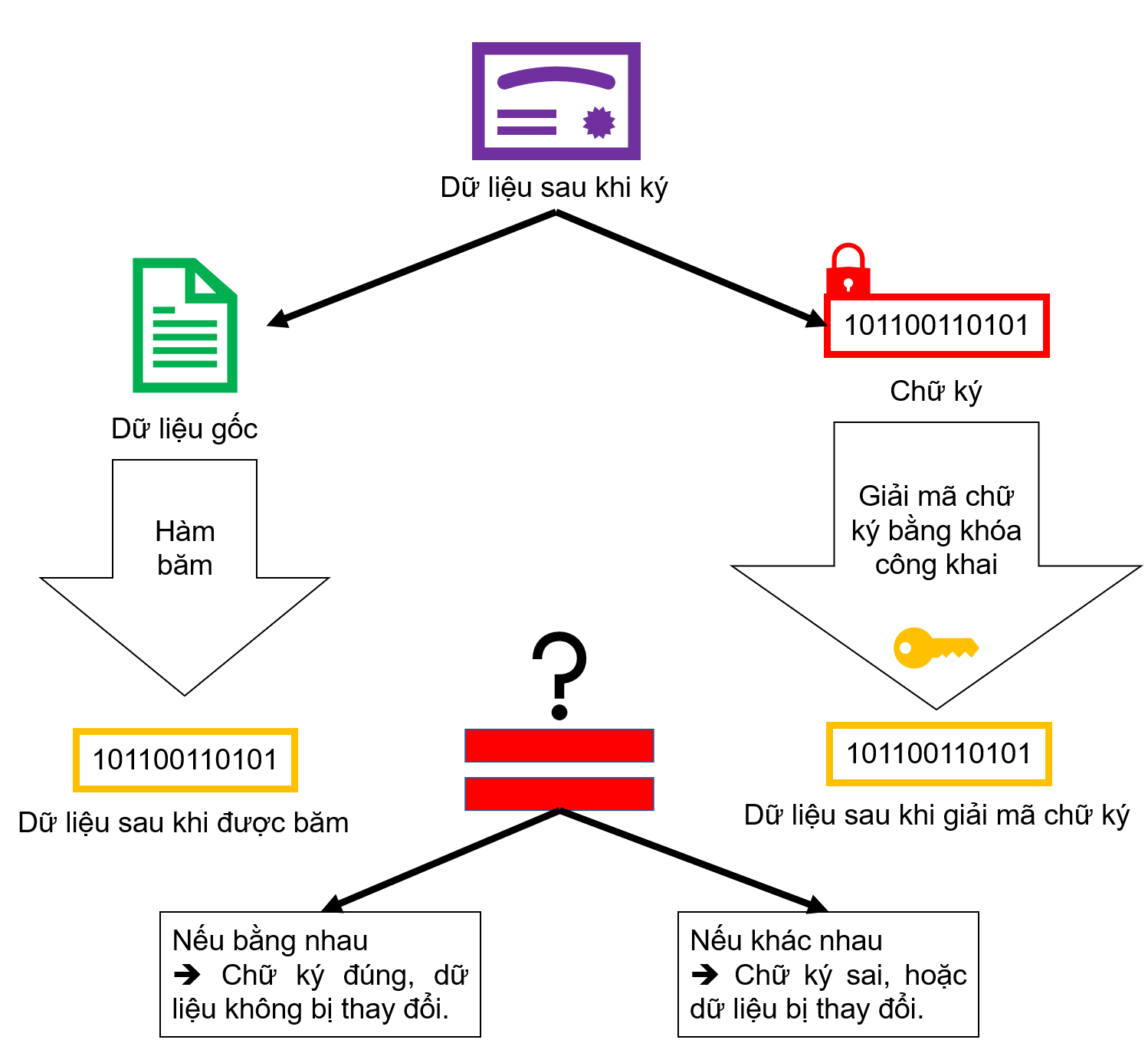
Graphical user interface, application, Teams

Description automatically generated

Hình ảnh 1: Quá trình tạo chữ ký

1. Quá trình kiểm tra chữ ký

* Bước 1: 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.
* Bước 2: 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.
* Bước 3: 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.
* Bước 4: 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 ảnh 2: Quá trình kiểm tra chữ ký

## Phương pháp mã hóa bất đối xứng

### Khái niệm

Phương pháp mã hóa bất đối xứng của RSA trong chữ ký số điện tử hoạt động dựa trên hai khóa: khóa bí mật (private key) và khóa công khai (public key). Khóa bí mật được giữ bí mật bởi người ký, còn khóa công khai được chia sẻ với người nhận.

Để tạo chữ ký số điện tử, người ký sử dụng khóa bí mật để mã hóa một hàm băm của thông tin được ký. Hàm băm là một hàm toán học được sử dụng để biến đổi thông tin thành một chuỗi ký tự có độ dài cố định.

Hàm băm của thông tin được ký được gọi là bản mã băm. Bản mã băm có thể được giải mã bằng khóa công khai, nhưng chỉ có người ký mới có khóa bí mật để mã hóa bản mã băm.

Để xác minh chữ ký số điện tử, người nhận sử dụng khóa công khai để giải mã bản mã băm. Nếu bản mã băm có thể được giải mã thành hàm băm của thông tin được ký, thì chữ ký là hợp lệ.

Mã hóa bất đối xứng thường bao gồm ba thành phần chính:

* *Tạo khóa* : Trong bước này, bên nhận sẽ tạo ra một cặp khóa (public key và private key). Bên nhận sẽ giữ lại private key và truyền cho bên gửi public key. Vì public key này là công khai nên có thể truyền tự do mà không cần bảo mật.
* *Mã hóa* : Ở bước này, bên gửi trước khi gửi dữ liệu sẽ mã hóa dữ liệu bằng thuật toán mã hóa bất đối xứng với key là public key từ bên nhận.
* *Giải mã* : Ở bước này, bên nhận sẽ giải mã dữ liệu nhận được bằng thuật toán được sử dụng ở bên gửi, với key giải mã là private key.

### Ưu, nhược điểm

* Ưu điểm
* Tính xác thực: Chữ ký số điện tử RSA đảm bảo rằng người ký chính là người mà họ tuyên bố.
* Tính toàn vẹn: Chữ ký số điện tử RSA đảm bảo rằng thông tin được ký không bị thay đổi kể từ khi được ký.
* Khả năng mở rộng: Chữ ký số điện tử RSA có thể được sử dụng để ký bất kỳ loại thông tin nào, bao gồm văn bản, tài liệu, hình ảnh, video,...
* Nhược điểm:
* Chi phí: Chữ ký số điện tử RSA yêu cầu sử dụng khóa bí mật và khóa công khai, điều này có thể gây ra chi phí cho người ký.
* Khả năng bảo mật: Khóa bí mật phải được bảo mật cẩn thận, nếu khóa bí mật bị lộ, thì chữ ký số điện tử có thể bị giả mạo.

### Ứng dụng của phương pháp mã hóa bất đối xứng của RSA trong chữ ký số điện tử.

* Thương mại điện tử: Chữ ký số điện tử RSA được sử dụng để ký các hợp đồng, hóa đơn,... trong thương mại điện tử.
* Chính phủ: Chữ ký số điện tử RSA được sử dụng để ký các văn bản, tài liệu chính phủ.
* Y tế: Chữ ký số điện tử RSA được sử dụng để ký các hồ sơ y tế.
* Tài chính: Chữ ký số điện tử RSA được sử dụng để ký các giao dịch tài chính.

## Chữ ký số RSA

### Khái niệm

RSA được hiểu là một thuật toán mật mã hóa khóa công khai. Đây cũng là thuật toán đầu tiên phù hợp cho việc tạo ra chữ ký điện tử và mã hóa chúng. Nó là sự tiến bộ vượt bậc nằm trong lĩnh vực mật mã học và áp dụng thành công vào việc sử dụng khóa công cộng.

Chữ ký số RSA rất phổ biến trong thương mại điện tử, giao dịch trực tuyến vì nó đảm bảo an toàn khi điều kiện độ dài khóa đủ lớn.

RSA được Ron Rivest, Adi Shamir và Len Adleman giới thiệu năm 1977 tại Học viện Công nghệ Massachusetts (MIT).

RSA dựa trên tính khó của bài toán phân tích các số lớn ra thừa số nguyên tố.

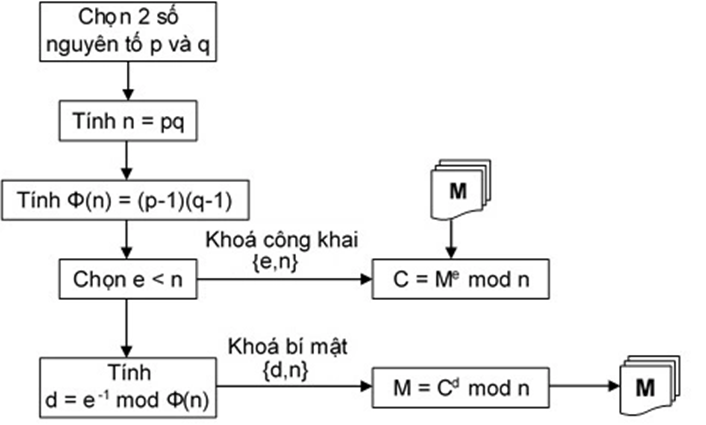
Biết một số nguyên tố nhân chúng với nhau để thu được một hợp số là dễ còn biết hợp số, phân tích nó ra thừa số nguyên tố là khó.

### Cấu tạo

Chữ ký số RSA gồm một cặp khóa được mã hóa không đối xứng như một khóa công khai (Public Key) và khóa bí mật (Private Key). Cụ thể như sau:

* Khóa bí mật: Dùng để tạo ra chữ ký số RSA
* Khóa công khai: được công bố rộng rãi cho mọi người và được dùng 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.

### Nội dung thuật toán



Hình ảnh 3 Sơ đồ biểu hiện RSA mã hóa thuật toán.

1. Sinh khóa cho hệ mã RSA

* Bước 1: Sinh 2 số nguyên tố lớn p và q, với p # q, q > 120 chữ số.
* Lựa chọn ngẫu nhiên và độc lập.
* Bước 2: Tính n = p\*q và Φ(n) = ( p – 1)( q – 1) ( Hàm phi Euler)
* Bước 3: Chọn 1 số ngẫu nhiên e, 1 < e < Φ(n) sao cho và là số nguyên tố cùng nhau với Φ(n)

gcd( e,Φ(n)) = 1

* Bước 4: Sử dụng thuật toán Euclide mở rộng để tính số d, 1 < d < Φ(n) sao cho

d = e-1 mod Φ(n)

* Bước 5: Khóa công khai là (e, n), khóa bí mật là (d, p,q).

Giá trị thường dùng nhất là e = 65537.

1. Mã hóa và giải mã cho hệ mã RSA

Với Public key (e, n) và Private key (d, p, q) ⇒ mã hóa phía người gửi và giải mã phía người nhận.

* Thực hiện mã hóa RSA:
* Thông điệp ban đầu: m (0 < m < n)
* Sử dụng khóa công khai (e, n) để tính thông điệp mã hóa c:

c = me mod n

* Sau đó c sẽ được chuyển đến người nhận.
* Thực hiện giải mã RSA:
* Người nhận bằng Private key (d, p, q) để tính lại thông điệp gốc đã mã hóa c:
* c được giải mã để lấy được m theo công thức :

m = cd mod n

Đây chính là cách đảo ngược padding để lấy m và có lại dữ liệu mã hóa.

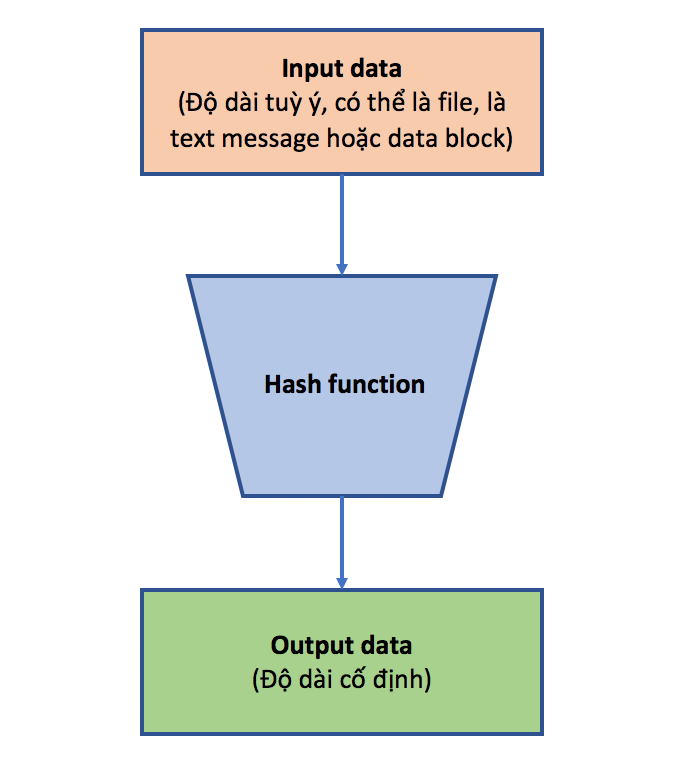
### Thám mã hệ mã RSA

* Để giải mã được mã hóa RSA phải tìm được khóa bí mật d.
* Tức là phần tử nghịch đảo của e modulo Φ(n).
* Để làm được điều trên trước hết phải tìm Φ(n).
* Việc tìm giá trị Φ(n) không dê hơn so với việc phân tích n vì khi biết Φ(n) và n ta có thể phân tích đươc n = p\*q
* Hệ mật RSA được gọi là an toàn nếu chọn số nguyên tố p, q đủ lớn để việc phân tích thành phần khóa công khai n thành tích 2 thừa số nguyên tố là khó để thực hiện trong thời gian thực.

## Hàm băm MD5

### Khái niệm

Hash function hay còn gọi là “hàm băm” là hàm nhận một input đầu vào, từ input đó tạo ra một giá trị output (hay còn gọi là “hash value” – “giá trị băm”) tương ứng. Giá trị đầu vào có thể có độ dài tuỳ ý nhưng giá trị băm thì luôn có độ dài cố định. Hash function là hàm mã hoá một chiều.



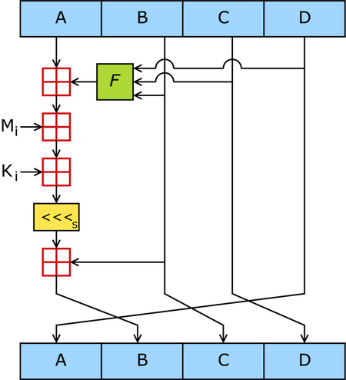
Hình ảnh 4: Hàm băm

Một hàm băm tốt cần đáp ứng các tính chất sau:

* Tính đồng nhất: Với một đầu vào cố định, hàm băm sẽ luôn trả về cùng một bản tóm tắt.
* Tính bất biến: Với một đầu vào khác nhau, hàm băm sẽ trả về các bản tóm tắt khác nhau.
* Tính phân tán: Một thay đổi nhỏ trong đầu vào sẽ dẫn đến một thay đổi lớn trong bản tóm tắt.
* Kích thước cố định: Bản tóm tắt của hàm băm có độ dài cố định.

### Một số hàm băm phổ biến

* Secure Hash Function (SHA): Họ SHA bao gồm 4 thuật toán hash khác nhau là SHA-0, SHA-1, SHA-2, and SHA-3.
* SHA-0: Hash function 160-bit, được công bố bởi NIST (National Institute of Standards and Technology) vào năm 1993. Do có một vài nhược điểm nên nó không được dùng phổ biến
* SHA-1: Hash function 160-bit, ra đời năm 1995, khắc phục một số nhược điểm của SHA-0. SHA-1 được sử dụng để xây dựng giao thức SSL (Secure Socket Layer). Vào năm 2005, một phương pháp đã được tìm thấy để phát hiện ra các va chạm của SHA-1 trong khoảng thời gian khả thi khiến khả năng sử dụng lâu dài của SHA-1 bị nghi ngờ.
* SHA-2: Công bố lần đầu năm 2001, bao gồm một số biến thể là SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 và SHA-512/256. Cho đến nay thì chưa thấy có báo cáo nào về phương pháp tạo ra đụng độ trong SHA-2. Mặc dù SHA-2 là họ hash function mạnh nhưng thiết kế của nó vẫn dựa trên SHA-1 nên NIST vẫn muốn có thiết kế của hash function mới cạnh tranh với SHA-2
* SHA-3: Năm 2012, NIST chọn thuật toán Keccak là để xây dựng SHA-3. Thuật toán Keccak có performance (hiệu năng) và khả năng chống “đụng độ” rất tốt.
* MD5 (MD là viết tắt của Message Digest) Là hash function 128-bit (dùng 128 bit để lưu giá trị băm), giá trị băm được biểu diễn bằng chuỗi 32 ký tự mã 16 (32 hexadecimal characters). MD5 được sử dụng rộng rãi để kiểm tra tính toán vẹn khi truyền file.



Hình ảnh 5: Giải thuật MD5

* Thuật toán MD5 chính hoạt động trên trạng thái 128-bit, được chia thành 4 từ 32-bit, với ký hiệu A, B, C và D. Chúng được khởi tạo với những hằng số cố định. Thuật toán chính sau đó sẽ xử lý các khối tin 512-bit, mỗi khối xác định một trạng thái. Quá trình xử lý khối tin bao gồm bốn giai đoạn giống nhau, gọi là vòng; mỗi vòng gồm có 16 tác vụ giống nhau dựa trên hàm phi tuyến F, cộng mô đun, và dịch trái.
* Hàm băm MD5 thường được ứng dụng trong việc xác thực, kiểm tra tính toàn vẹn hay mã hóa dữ liệu. Tuy nhiên MD5 không được khuyến khích sử dụng cho mục đích này vì nó đã được chứng minh là có thể bị tấn công

### Ưu, nhược điểm

1. Ưu điểm

* Tốc độ và hiệu quả: Hàm MD5 là một hàm băm mật mã học nhanh và hiệu quả. Điều này có nghĩa là nó có thể được sử dụng để tạo ra các bản tóm tắt của dữ liệu lớn mà không cần tốn quá nhiều thời gian hoặc tài nguyên.
* Tính linh hoạt: Hàm MD5 có thể được sử dụng cho nhiều mục đích khác nhau. Nó có thể được sử dụng để xác thực tính toàn vẹn của dữ liệu, kiểm tra tính toàn vẹn của các tập tin hoặc thông điệp, hoặc mã hóa dữ liệu.

1. Nhược điểm

* Tính an toàn: Hàm MD5 đã được chứng minh là có thể bị tấn công bằng kỹ thuật vét cạn. Điều này có nghĩa là, với một lượng sức mạnh tính toán đủ lớn, kẻ tấn công có thể tìm ra các đầu vào khác nhau có cùng bản tóm tắt MD5.

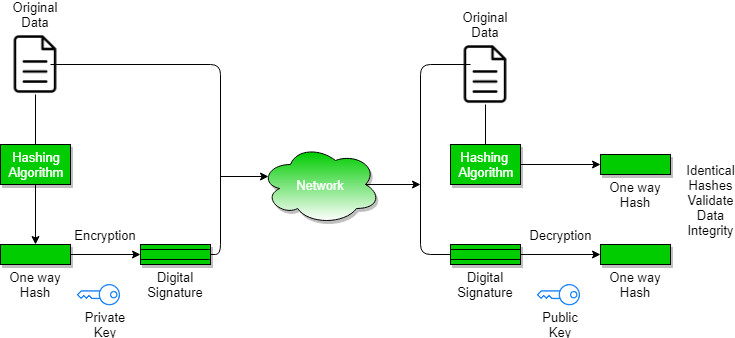
# Phân tích thiết kế

## Phân tích “Ứng dụng Chữ ký số điện tử RSA”

* *Mục đích:* Nhằm phân tích các yêu cầu cơ bản đối với ứng dụng chữ ký số RSA
* *Thực trạng*

Chữ ký số điện tử RSA đang ngày càng được sử dụng phổ biến tại Việt Nam, đặc biệt là trong các lĩnh vực thương mại điện tử, tài chính ngân hàng và hành chính công. Các doanh nghiệp và tổ chức đánh giá cao tính xác thực, bảo mật và tiện lợi của chữ ký số điện tử RSA. Tuy nhiên, chi phí, kiến thức sử dụng và hệ thống kỹ thuật vẫn là những khó khăn cần được giải quyết để thúc đẩy việc ứng dụng chữ ký số điện tử RSA trong tương lai.

Theo kết quả khảo sát, chữ ký số điện tử RSA được ứng dụng trong nhiều lĩnh vực, bao gồm:

* Thương mại điện tử: Chữ ký số RSA được sử dụng để ký kết hợp đồng, tài liệu, chứng từ điện tử, thanh toán điện tử,...
* Chính phủ điện tử: Chữ ký số RSA được sử dụng trong các dịch vụ công trực tuyến, như khai báo thuế, hải quan, kê khai bảo hiểm xã hội,...
* Giáo dục: Chữ ký số RSA được sử dụng để ký kết hợp đồng đào tạo, chứng nhận,...
* Y tế: Chữ ký số RSA được sử dụng để ký kết hồ sơ bệnh án, đơn thuốc,...
* Các lĩnh vực khác: Chữ ký số RSA cũng được ứng dụng trong các lĩnh vực khác như tài chính, ngân hàng, truyền thông,...
  + *Mục tiêu:* Xây dựng ứng dụng chữ ký số RSA bằng ngôn ngữ Python trên môi trường mạng
* *Mô tả hệ thống*

Hình ảnh 6: Sơ đồ hệ thống chữ ký số RSA

* Người tạo chữ ký số sử dụng khóa bí mật để tạo một giá trị băm (hash value) của thông điệp. Giá trị băm là một giá trị duy nhất được tạo ra từ thông điệp. Người tạo chữ ký số sử dụng khóa bí mật để mã hóa giá trị băm. Chữ ký số là giá trị băm đã được mã hóa.
* Người xác minh chữ ký số sử dụng khóa công khai để giải mã giá trị băm. Người xác minh chữ ký số sử dụng một hàm băm để tạo giá trị băm của thông điệp. Người xác minh chữ ký số so sánh giá trị băm của thông điệp với giá trị băm đã giải mã.
* Nếu hai giá trị băm trùng khớp, thì chữ ký số là hợp lệ. Điều này có nghĩa là thông điệp đã được tạo bởi người có khóa bí mật tương ứng với khóa công khai được sử dụng để xác minh chữ ký số.

## Phân tích yêu cầu

* *Ứng dụng Chữ ký số điện tử RSA*
* Là ứng dụng chữ ký số RSA bằng ngôn ngữ Python và hoạt động ổn định
* Cung cấp các chức năng để người gửi và người nhận ký và xác minh chữ ký điện tử
* Phải đáp ứng được các yêu cầu về hiệu năng cao để quá trình thực hiện một cách nhanh chóng, tính dễ sử dụng, tính bảo mật và toàn vẹn thông tin. Ứng dụng chữ ký số RSA cần được thiết kế và triển khai một cách an toàn để đảm bảo tính bảo mật của khóa bí mật và tính toàn vẹn của thông điệp.
* Hiển thị kết quả
* *Người gửi*
* Tạo khóa bí mật và khóa công khai: Người gửi cần tạo một cặp khóa bí mật và khóa công khai để sử dụng cho chữ ký điện tử.
* Ký thông điệp: Người gửi sử dụng khóa bí mật của mình để tạo chữ ký điện tử cho thông điệp.
* Gửi thông điệp và chữ ký điện tử: Người gửi gửi thông điệp và chữ ký điện tử cho người nhận.
* *Người xác minh chữ ký*
* Nhận thông điệp và chữ ký điện tử: Người xác minh chữ ký nhận thông điệp và chữ ký điện tử từ người gửi.
* Xác minh tính xác thực của chữ ký điện tử: Người xác minh chữ ký sử dụng khóa công khai của người gửi để xác minh tính xác thực của chữ ký điện tử.
* Xác minh tính toàn vẹn của thông điệp: Người xác minh chữ ký sử dụng hàm băm để xác minh tính toàn vẹn của thông điệp.
* *Hệ thống ký*
* Tạo và cấp phát khóa: Hệ thống tạo và cấp phát khóa bí mật và khóa công khai cho người dùng.
* Lưu trữ khóa: Hệ thống lưu trữ khóa bí mật và khóa công khai của người dùng một cách an toàn.
* Xác thực người dùng: Hệ thống xác thực người dùng trước khi tạo hoặc xác minh chữ ký điện tử.
* Quản lý chữ ký điện tử: Hệ thống quản lý chữ ký điện tử, chẳng hạn như lưu trữ, tìm kiếm, và xóa chữ ký điện tử.
* Tích hợp với các ứng dụng khác: Hệ thống chữ ký điện tử có thể được tích hợp với các ứng dụng khác, chẳng hạn như phần mềm quản lý tài liệu, hệ thống quản trị nội bộ, v.v.

## Phân tích chức năng

* *Chức năng tạo khóa*

Chức năng tạo khóa trong chữ ký điện tử RSA cho phép người dùng có thể sinh khóa tự động hoặc nhập khóa , là quá trình tạo ra cặp khóa công khai và khóa bí mật. Quá trình này bao gồm các bước sau:

* **Bước 1: Chọn hai số nguyên tố lớn**: Chọn hai số nguyên tố lớn p và q. Các số nguyên tố này là bí mật và không được tiết lộ cho bất kỳ ai.
* **Bước 2: Tính n và φ(n)**: Tính n = p \* q, trong đó n là một số nguyên lớn là thành phần chung của cả khóa công khai và khóa bí mật. Tính số Euler φ(n) = (p - 1) (q - 1), đây là một số nguyên dương tương đối với n.
* **Bước 3: Chọn số e**: Chọn một số e sao cho 1 < e < Φ(e) và e là số nguyên tố cùng nhau với Φ(e). Trong quá trình này, e được chọn là khóa công khai và công khai cho người dùng khác để gửi thông điệp cho bạn.
* **Bước 4: Tính khóa bí mật d**: Tính d sao cho (d \* e) % Φ(n) = 1. Đây là khóa bí mật và chỉ bạn biết.Khóa bí mật dùng để mã hóa thông điệp đã được mã hóa thành hàm băm

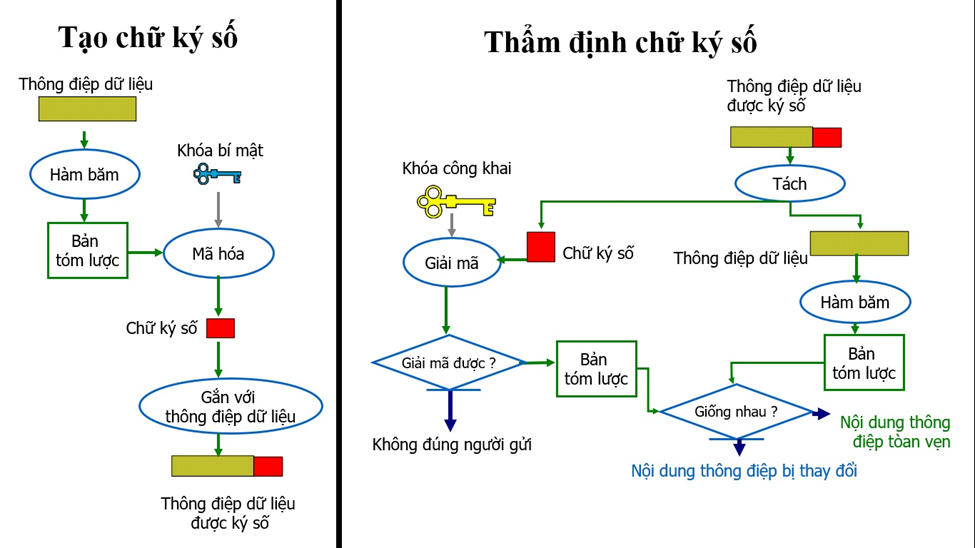
Sau khi hoàn tất quá trình sinh khóa, bạn sẽ có cặp khóa (e, n) là công khai và cặp khóa (d, n) là khóa bí mật. Khóa công khai được chia sẻ với mọi người để mã hóa thông điệp, trong khi khóa bí mật được giữ bí mật để giải mã thông điệp.

* *Chức năng mã hóa chữ ký số*

Chức năng mã hóa trong chữ ký điện tử RSA là quá trình mã hóa thông điệp sử dụng khóa công khai của người nhận. Quá trình này bao gồm các bước sau:

* **Bước 1: Chuẩn bị thông điệp**: Thông điệp cần được mã hóa được chuyển đổi thành một số nguyên m. Quá trình này thường bao gồm việc sử dụng một hàm băm (hash function) để chuyển đổi thông điệp thành một chuỗi số học.
* **Bước 2: Sử dụng khóa công khai**: Sử dụng khóa công khai (e, n) của người nhận, mã hóa thông điệp thành một chữ ký điện tử. Quá trình này được thực hiện bằng cách tính s = me % n, trong đó s là chữ ký điện tử và m là số nguyên tương ứng với thông điệp đã được chuyển đổi.
* **Bước 3: Gửi thông điệp và chữ ký**: Gửi thông điệp ban đầu và chữ ký điện tử (s) cho người nhận.

Quá trình này đảm bảo rằng thông điệp đã được mã hóa chỉ có thể được giải mã bằng cặp khóa bí mật tương ứng và không thể bị thay đổi trong quá trình truyền tải. Người nhận sau đó sẽ sử dụng khóa bí mật của mình để giải mã chữ ký và xác minh tính toàn vẹn của thông điệp đã được nhận.



Hình ảnh 7: Chức năng tạo chữ ký số và thẩm định chữ ký số

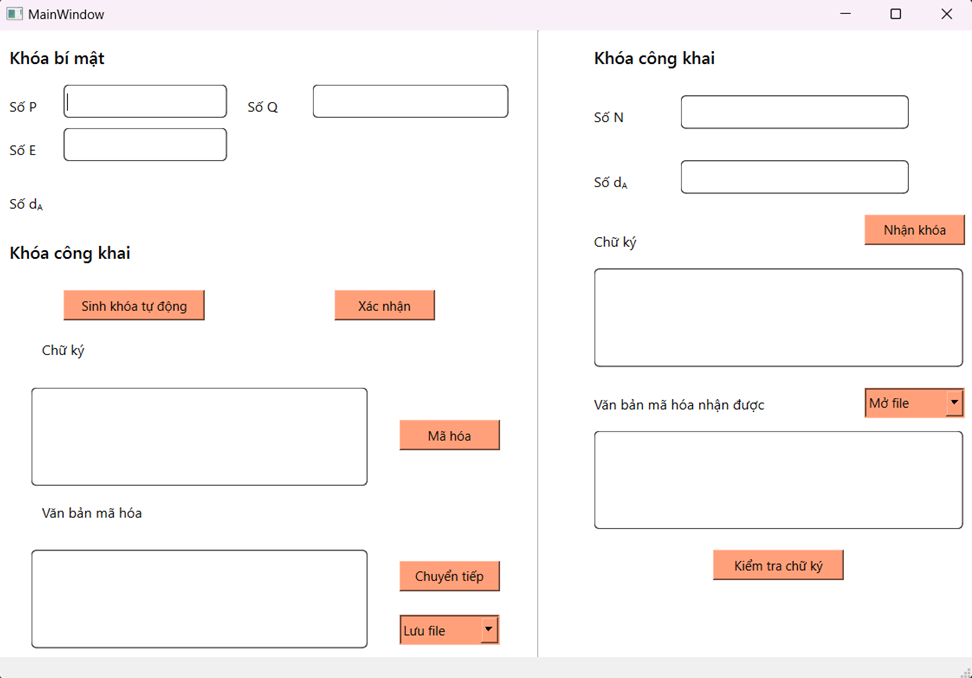
* *Chức năng thẩm định*

Chức năng thẩm định trong chữ ký số điện tử RSA nhằm xác thực tính toàn vẹn của thông điệp và xác thực nguồn gốc của chữ ký số bằng cách giải mã chữ ký số bằng khóa công khai và so sánh giá trị mã băm tính toán được với giá trị mã băm giải mã từ chữ ký số. Bao gồm:

* Nhận đoạn mã hóa: Nhận thông điệp đã được mã hóa từ bên gửi
* Nhận lấy mã công khai: Nhận mã công khải từ bên gửi
* Giải mã: Sử dụng mã công khai và đoạn mã hóa để giải mã: Kết quả là một hàm băm A
* Thẩm định: Người thẩm định nhập đoạn chữ ký để xác minh sau đó mã hóa đoạn chữ ký thành hàm băm B. So sánh hai giá trị hàm băm A và B. Nếu A và B giống nhau (Thông điệp không bị thay đổi). Ngược lại ….

# Kết quả thực hiện

## Giao diện chương trình



Hình ảnh 8: Giao diện ban đầu của chương trình

## Giới thiệu công cụ triển khai

Visual Studio Code (VS Code) là một trình biên soạn mã nguồn mở và miễn phí của Microsoft, được sử dụng phổ biến trong cộng đồng phát triển phần mềm Python và nhiều ngôn ngữ lập trình khác. Dưới đây là một số điểm nổi bật khi sử dụng Visual Studio Code để viết code Python:

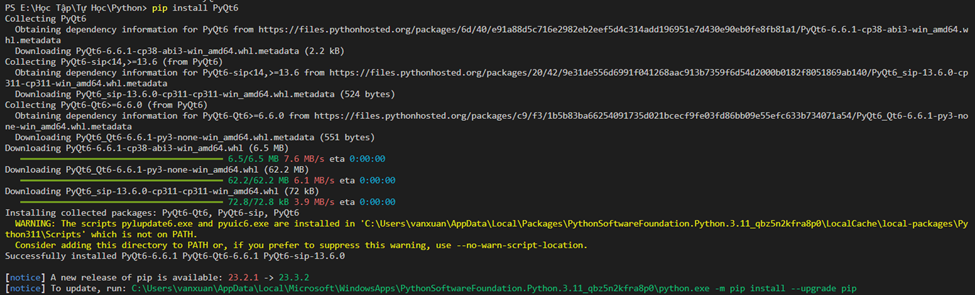
* *Môi trường tích hợp (Integrated Environment*): VS Code cung cấp môi trường tích hợp cho việc viết, gỡ lỗi, và triển khai mã nguồn Python. Chúng ta có thể mở nhiều cửa sổ và thực hiện nhiều nhiệm vụ khác nhau trong cùng một giao diện.
* *Hỗ trợ Python đầy đủ*: VS Code tích hợp với các tính năng hỗ trợ Python mạnh mẽ như IntelliSense (hoàn thành mã), gỡ lỗi tích hợp, kiểm tra lỗi cú pháp, và kiểm tra kiểu.
* *Extensions Python*: Chúng ta có thể mở rộng khả năng của VS Code bằng cách cài đặt các tiện ích mở rộng (extensions) dành cho Python. Các extension như "Python" của Microsoft cung cấp tính năng mở rộng và tương tác với các công cụ và framework Python khác nhau.
* *Gỡ lỗi Tích hợp*: VS Code hỗ trợ gỡ lỗi Python một cách thuận tiện. Chúng ta có thể đặt các điểm dừng, theo dõi giá trị biến, và thậm chí gỡ lỗi ứng dụng chạy từ xa trên môi trường từ xa.
* *Quản lý Phiên bản*: Visual Studio Code tích hợp với hệ thống quản lý phiên bản như Git, giúp chúng ta theo dõi và quản lý sự thay đổi trong mã nguồn.
* *Tích hợp với Jupyter Notebooks*: Nếu chúng ta làm việc với Jupyter Notebooks, VS Code có tích hợp sẵn cho phép bạn mở, tạo, và thực hiện các tác vụ trực tiếp từ giao diện.
* *Hỗ trợ Đa Nền Tảng:* VS Code có sẵn cho Windows, macOS và Linux, giúp đảm bảo tính tương thích trên nhiều hệ điều hành.
* *Chủ Đề và Tùy Chỉnh*: Chúng ta có thể tùy chỉnh giao diện VS Code với nhiều chủ đề và màu sắc, giúp làm việc một cách thoải mái.
* *Dự Án và Tệp Tích hợp:* Quản lý dự án và các tệp tin trực tiếp từ giao diện, giúp chúng ta duyệt qua dự án của mình một cách thuận lợi.

## Hướng dẫn cài đặt và chạy chương trình

### Cài đặt thư viện

* Thư viện yQt6

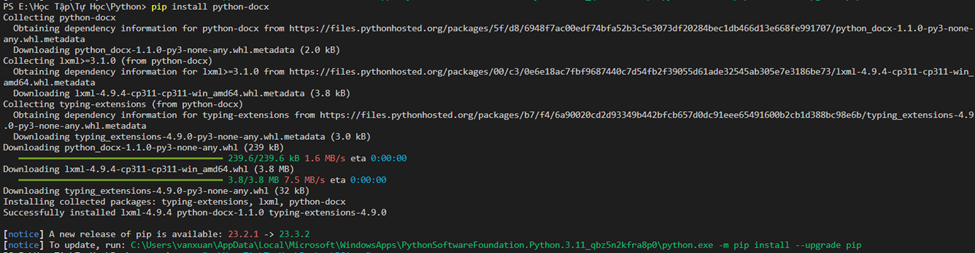
Sử dụng câu lệnh: pip install PyQt6



Hình ảnh 9: Cài đặt thư viện PyQt6

* Thư viện docx

Sử dụng câu lệnh: pip install python-docx.

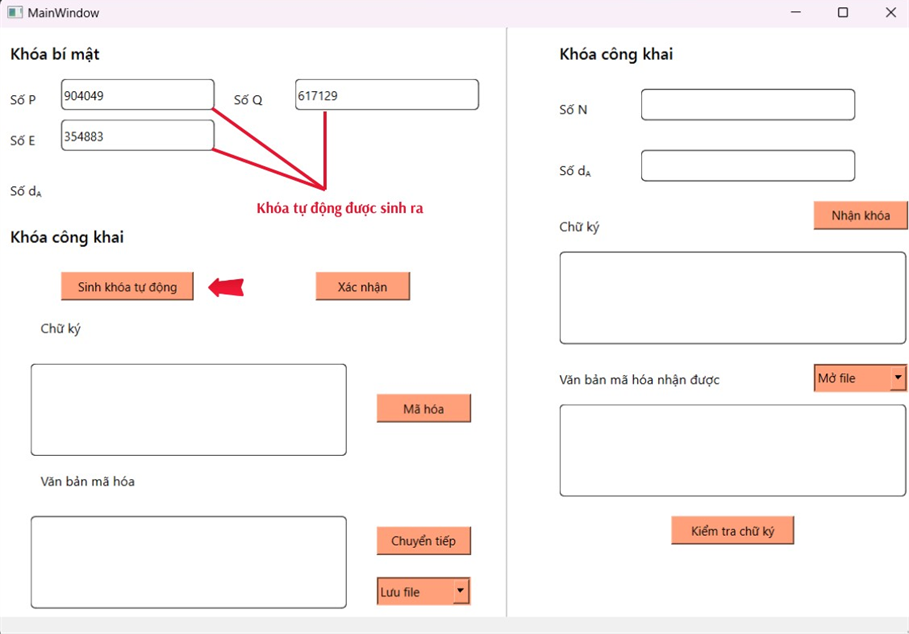


Hình ảnh 10: Cài đặt thư viện docx

### Demo chương trình

* Sinh khóa tự động:

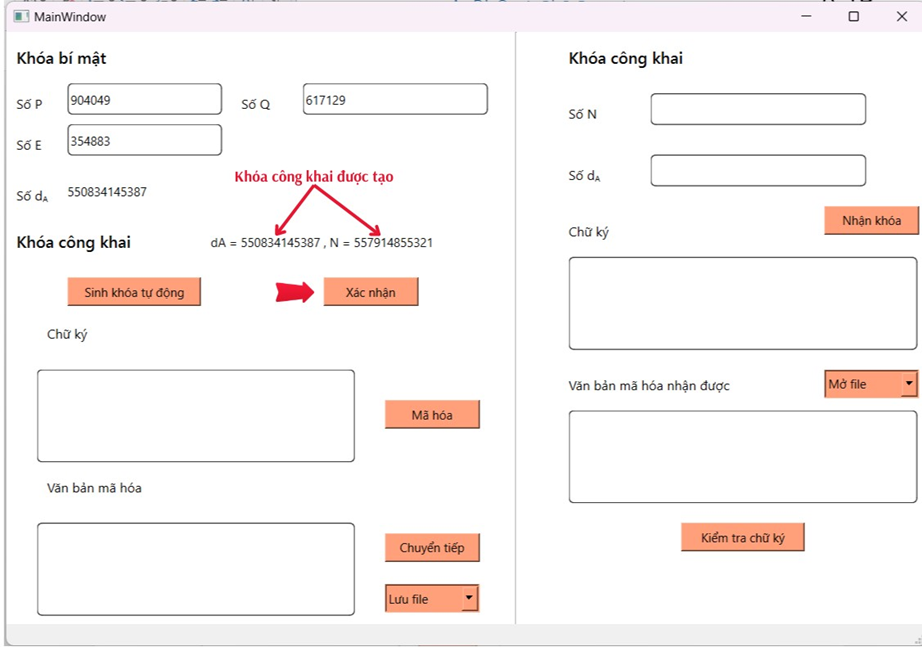
Sau khi chạy file RSA.py trên visual studio code chúng ta được gia diện ban đầu. Sau đó để tạo khóa tự động, chúng ta click vào button sinh khóa tự động để chương trình tạo ra các khóa bí mật (Số P, Số E, Số Q).



Hình ảnh 11: Tạo khóa tự động

* Xác nhận để tạo khóa công khai:

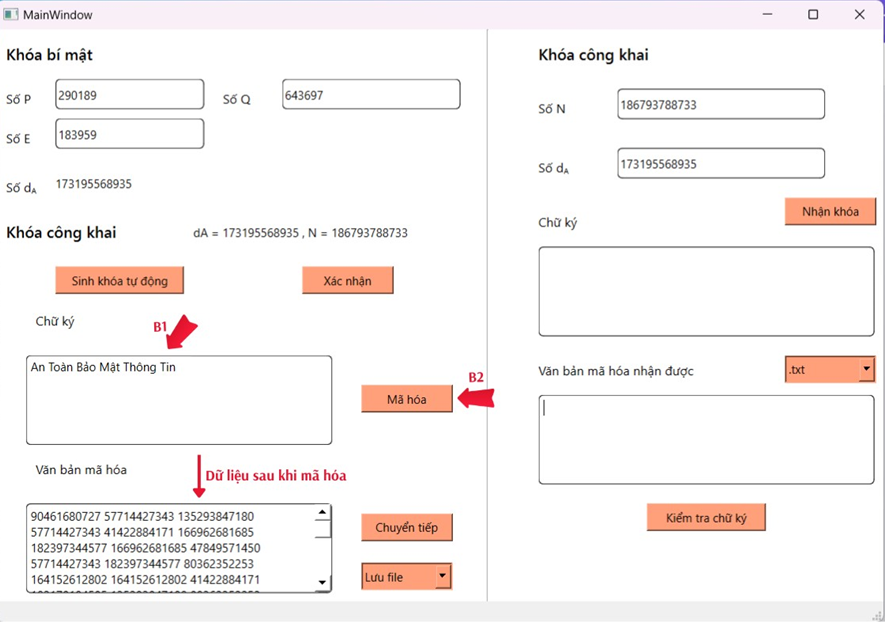
Sau khi đã có khóa bí mật để tạo khóa công khai, chúng ta tiếp tục click vào xác nhận tạo khóa công khai. Khóa công khai sẽ được hiển thị trên dòng khóa công khai(dA, N).



Hình ảnh 12: Xác nhận tạo khóa công khai

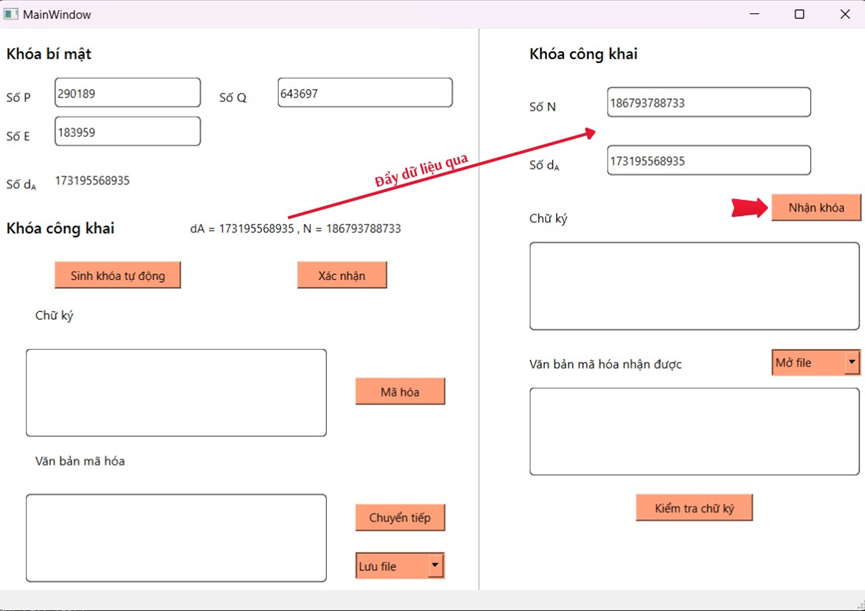
* Nhận khóa công khai:

Khi đã xác nhận đồng ý với khóa công khai như đã in trên màn hình, chúng ta xác nhận nhận khóa đó thì dữ liệu các trường dA và N sẽ tự động chuyển qua cột phía bên phải.



Hình ảnh 13: Mã hóa chữ ký

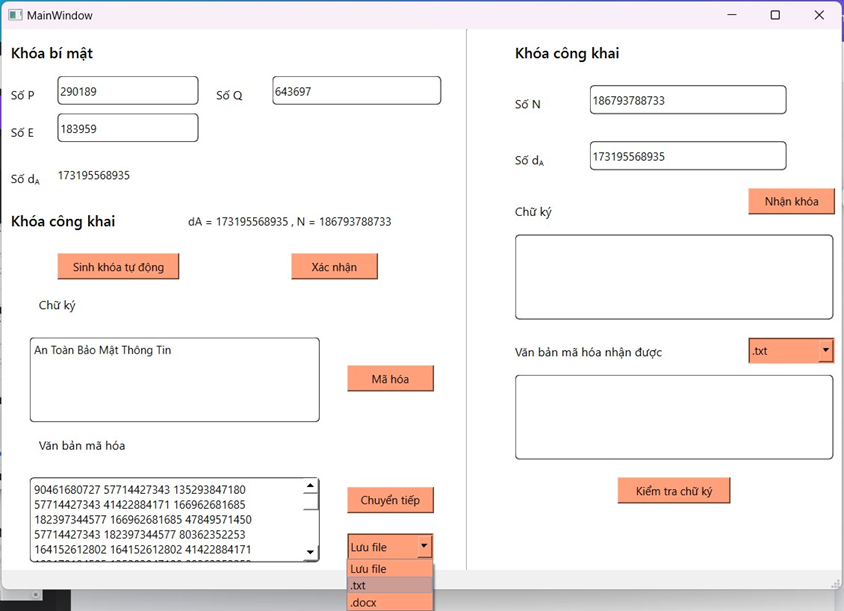
* Mã hóa chữ ký:
* Bước 1: Nhập chữ ký cần mã hóa
* Bước 2: Click vào button mã hóa để mã hóa chữ ký trên và trả dữ liệu sau khi mã hóa về ô lưu văn bản sau khi mã hóa.



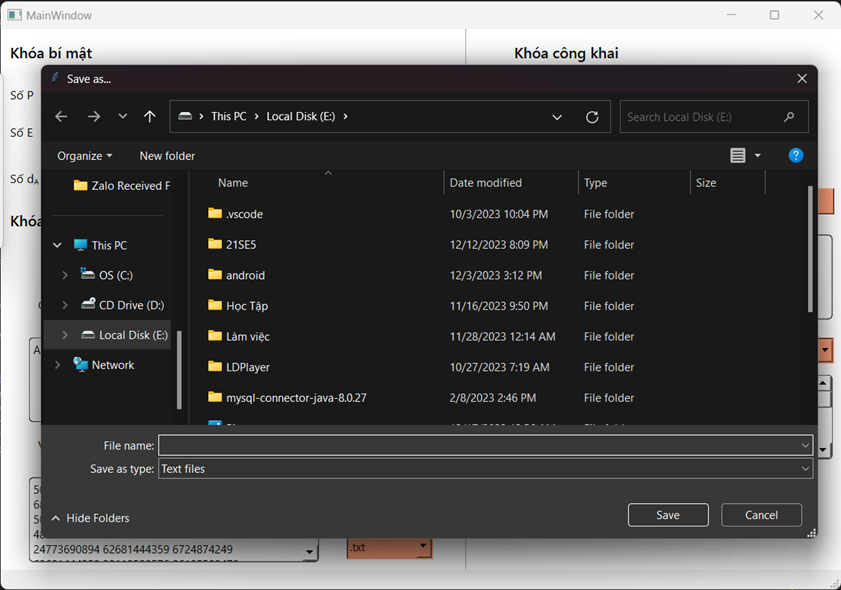
Hình ảnh 14: Nhận khóa công khai

* Lưu văn bản mã hóa:

Ở đây chúng ta có thể lưu văn bản mã hóa dưới 2 dạng file (.txt và .docx). sao khi click vào đuôi file muốn lưu thì chương trình sẽ mở cửa sổ File Explorer để lưu.



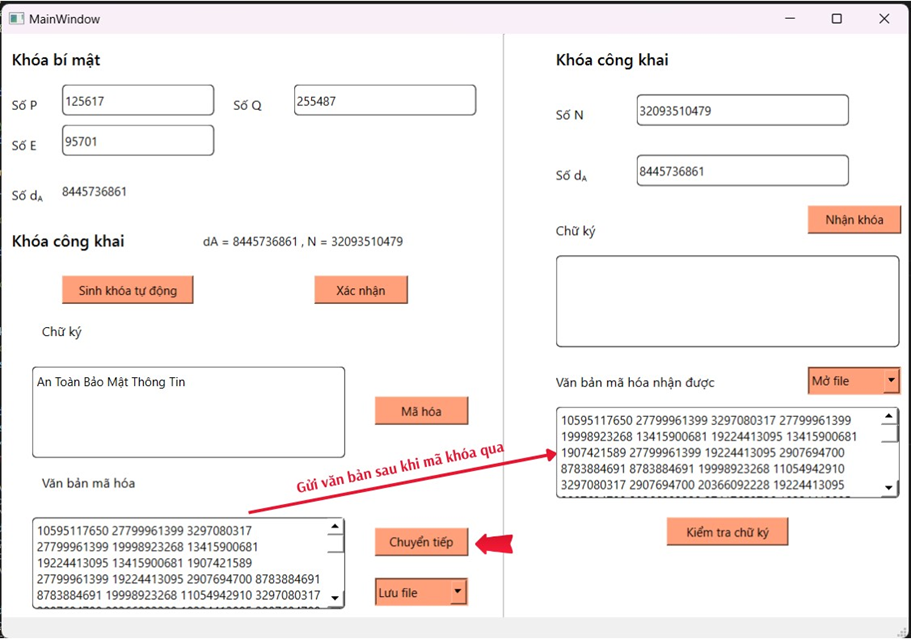
Hình ảnh 15: Lưu văn bản mã hóa thành file



Hình ảnh 16: Giao diện để lưu file

* Chuyển tiếp văn bản mã hóa:

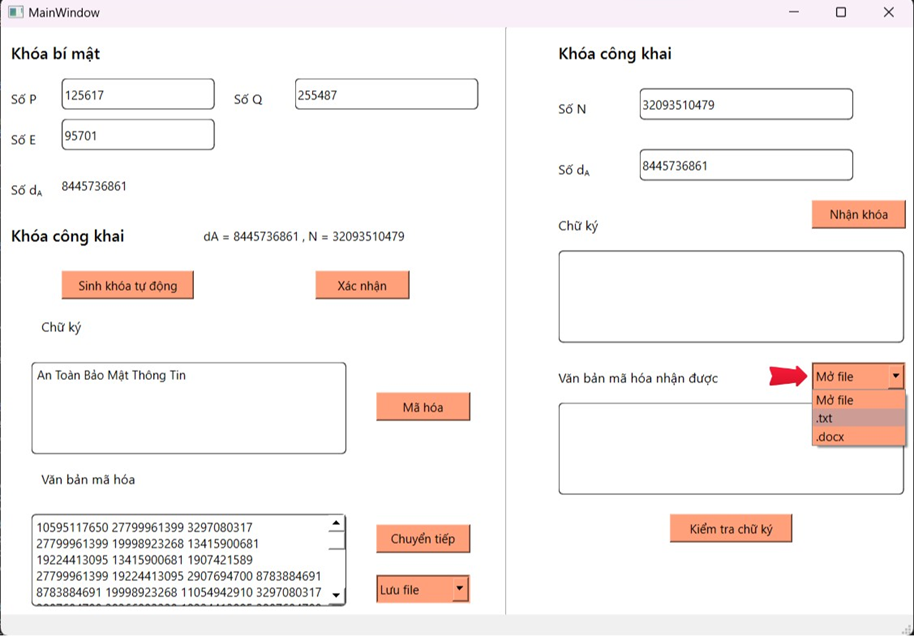
Sau khi đã mã hóa chữ ký chúng ta chuyển tiếp văn bản mã hóa qua ô văn bản mã hóa nhận được phía bên phải.



Hình ảnh 17: Chuyển tiếp văn bản mã hóa

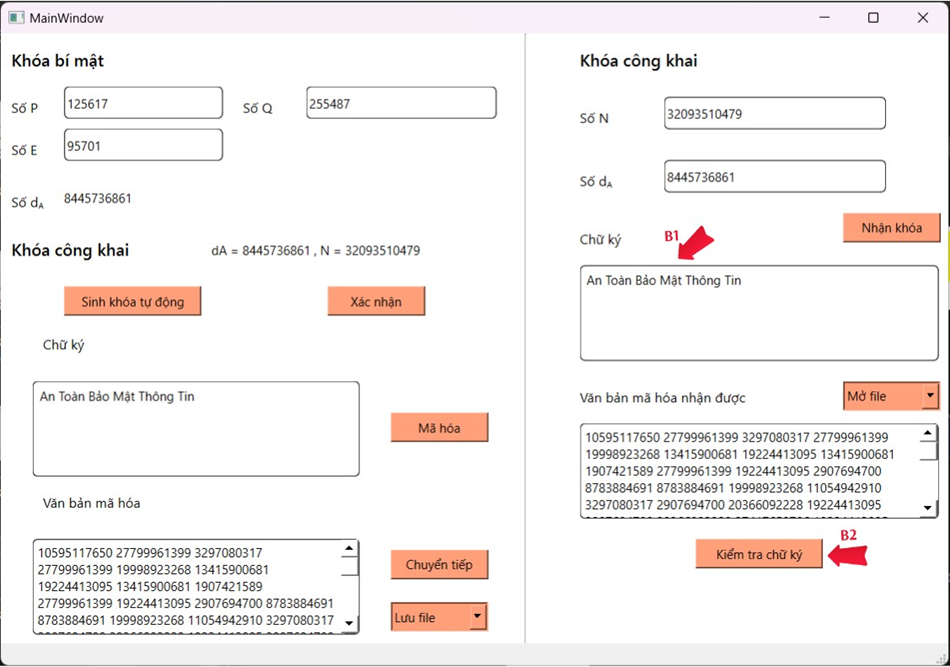
* Mở văn bản mã hóa bằng mở file:

Chúng ta có thể mở file đã lưu trước ở phần lưu file văn bản mã hóa. Kết quả ở ô văn bản mã hóa sẽ được hiển thị ra.



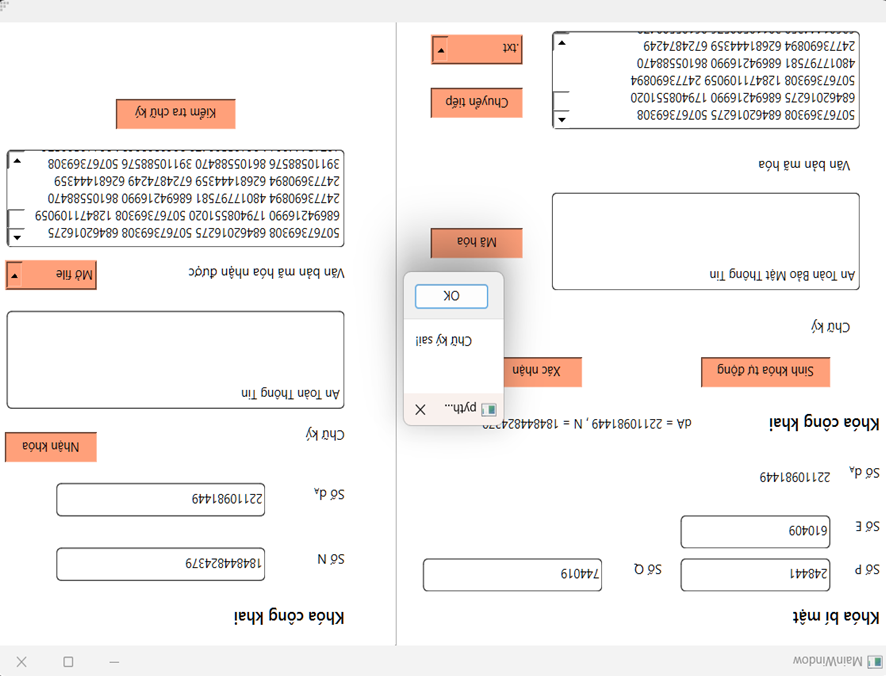
Hình ảnh 18: Mở văn bản đã được mã hóa

* Kiểm tra chữ ký:
* Bước 1: Nhập chữ ký cần kiểm tra.
* Bước 2: Click vào kiểm tra chữ ký để kiểm tra.

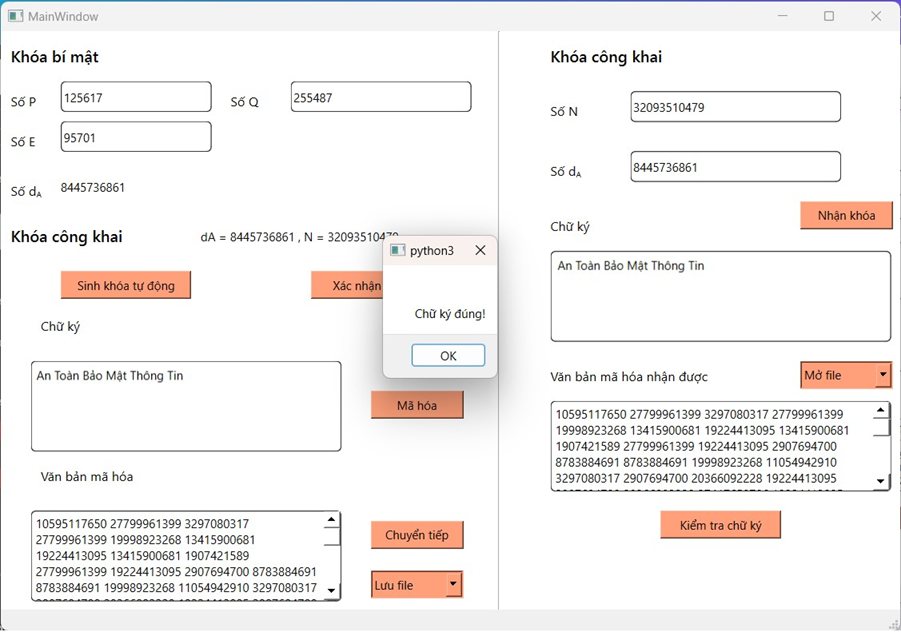


Hình ảnh 19: Kiểm tra tính đúng sai của mã hóa chữ ký

* Kết quả sau khi kiểm tra



Hình ảnh 17: Kêt quả sai sau khi mã hóa



Hình ảnh 16: Kết quả đúng sau khi mã hóa chữ ký

# Kiến thức lĩnh hội và bài học kinh nghiệm

## Kiến thức lĩnh hội

* 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 như: Chữ ký số, Chữ ký số RSA, phương pháp mã hóa bất đối xứng, hàm băm nói chung và hàm băm MD5 nói riêng
* Tìm hiểu chữ ký số và chữ ký số RSA về các nội dung:
* Ưu, nhược điểm
* Nguyên lý hoạt động của chữ ký số
* Cấu tạo của chữ ký số RSA
* Nội dung thuật toán của chữ ký số RSA: sinh khóa, mã hóa và giải mã, ký và xác thực chữ ký
* Tìm hiểu về hàm băm về các nội dung: Một số hàm băm phổ biến, ưu nhược điểm.
* Tìm hiểu về cách hoạt động cũng như lập trình được giao diện của ngôn ngữ lập trình Python.
* Tìm hiểu về cách triển khai những thuật toán của đề tài được giao vào trong ngôn ngữ lập trình Python.
* Demo chương trình và viết báo cáo

## Bài học kinh nghiệm

* Các kỹ năng cần có như:
* Kỹ năng làm việc nhóm.
* Kỹ năng tóm tắt, phân tích và giải quyết vấn đề.
* Kỹ năng nghiên cứu, tìm tòi và học hỏi.
* Kiến thức bắt buộc:
* Các môn toán học và lập trình.
* Cách thức hoạt động của chữ ký RSA, hệ mật RSA.
* Kiến thức chuyên sâu về:
* Có kiến thức nền tảng về máy tính (phần cứng, phần mềm) và hệ thống mạng.
* Hiểu và nắm bắt về luật an toàn thông tin.
* Vận dụng tốt ngôn ngữ lập trình Python.
* Có chuyên môn về mã hóa thông tin, an toàn cơ sở dữ liệu.
* Có ý thức nâng cao hiểu biết, nhận thức bản thân về an toàn thông tin. Tự trau dồi kinh nghiệm ứng phó sự cố bảo mật cũng như vận hành các quy trình bảo mật mới.
* Thường xuyên cập nhật phần mềm, hệ điều hành máy tính cá nhân lên phiên bản mới nhất. Không sử dụng phần mềm crack.
* Đề cao cảnh giác khi duyệt Email, kiểm tra kỹ tên người gửi để phòng tránh lừa đảo. Tuyệt đối không tải các file đính kèm hoặc nhấp vào đường link không rõ nguồn gốc.

## 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.
* Giao tiếp, trao đổi giữa các thành viên trong nhóm rất tốt.
* Khó khăn:
* Cần học thêm nhiều kiến thức bên ngoài để xây dựng được một chương trình với giao diện hoàn chỉnh.
* 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
* 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.
* 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.
* Xây dựng cổng thông tin trao đổi thông tin giữa các cơ quan, tổ chức với nhau.
* 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 hàng; giao dịch email; …

# Tài liệu tham khảo

1. TENTEN,(2022).Chữ ký số RSA là gì? Giải thích thuật ngữ RSA dễ hiểu nhất, <https://tenten.vn/tin-tuc/chu-ky-so-rsa/> , truy cập 12/202.
2. AITHIETKE, (2021), Cơ chế hoạt động và ứng dụng của RSA, AI Design, <https://aithietke.com/co-che-hoat-dong-va-ung-dung-cua-rsa/>, truy cập 12/2023.
3. Chu Ngọc Long, (2020), Tìm hiểu về chữ ký số và ứng dụng, VIBLO, <https://viblo.asia/p/tim-hieu-ve-chu-ky-so-va-ung-dung-jvElay0Nlkw> , Truy cập 12/2023.
4. Khoainv, (2015), Ứng dụng chữ ký số trong các dự án Chính phủ điện tử, Kiến trúc phần mềm Việt, <https://kientrucphanmemviet.wordpress.com/2015/10/16/ung-dung-chu-ky-so-trong-cac-du-an-chinh-phu-dien-tu/>, truy cập 12/2023.
5. Shashank, (2023), Digital Signatures and Certificates, Geeksforgeeks, <https://www.geeksforgeeks.org/digital-signatures-certificates/>, truy cập 12/2023.
6. ThS. Nguyễn Thanh Sơn, (2020), Giới thiệu về một số hàm băm và ứng dụng trong một số sản phẩm mật mã dân sự, Ban cơ yếu chính phủ Cục quản lý mật mã dân sự và kiểm định sản phẩm mật mã, <https://nacis.gov.vn/nghien-cuu-trao-doi/-/view-content/213743/gioi-thieu-ve-mot-so-ham-bam-va-ung-dung-trong-mot-so-san-pham-mat-ma-dan-su>, truy cập 12/2023.
7. Tanvi Bugdani, (2023), RSA Algorithm: Theory and Implementation in Python, AskPython, <https://www.askpython.com/python/examples/rsa-algorithm-in-python>, truy cập 12/2023.