

**BỘ CÔNG THƯƠNG**

**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 03:**

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

**Demo sản phẩm minh họa**

|  |  |  |
| --- | --- | --- |
| **Giảng viên hướng dẫn** | **:** | **Lê Thị Anh** |
| **Mã Lớp** | **:** | **20231IT6001001** |
| **Nhóm** | **:** | **14** |
| **Thành viên nhóm** | **:** | **1. Phạm Thùy Hương - 2021606320**  **2. Phan Thị Thu Huyền - 2021605225**  **3. Triệu Ngọc Hoa - 2021605441**  **4. Nguyễn Đăng Thành - 2021602363** |

***Hà Nội – 2023***

**LỜI CẢM ƠN**

Lời đầu tiên, nhóm chúng em xin gửi lời cảm ơn sâu sắc đến cô **Lê Thị Anh**. Trong quá trình tìm hiểu và học tập bộ môn An toàn và bảo mật thông tin, chúng em đã được cô cung cấp và truyền đạt tất cả kiến thức chuyên môn cần thiết và quý giá nhất. Ngoài ra, chúng em còn được rèn luyện một tinh thần học tập và làm việc độc lập , sáng tạo. Đây là tính cách hết sức cần thiết để có thể thành công khi bắt tay vào nghề nghiệp trong tương lai. Nhóm đã nhận được sự hướng dẫn và những chia sẻ rất tận tình, tâm huyết của cô. Từ những hướng dẫn tận tình của cô cùng với kiến thức mà nhóm đã học tập, tìm hiểu, chúng em đã hoàn thành báo cáo đề tài “**Ứng dụng RSA trong chữ ký số điện tử. Demo sản phẩm minh họa**”. Đây là cơ hội để nhóm em có thể áp dụng, tìm hiểu thêm và tổng kết lại những kiến thức mà mình đã học. Đồng thời, rút ra được những kinh nghiệm thực tế và quý giá trong suốt quá trình thực hiện đề tài.

Với tất cả sự cố gắng, nỗ lực của mình, nhóm em đã hoàn thành tốt nhất bài báo cáo này.Trong quá trình thực hiện đề tài, do kiến thức còn nhiều hạn chế và thiếu sót, nhóm chúng em chắc chắn không tránh khỏi những thiếu sót khi thực hiện . Nhóm chúng em mong nhận được sự góp ý của cô để đề tài cũng như ứng dụng demo của các thành viên trong nhóm được đầy đủ và hoàn thiện hơn về kiến thức cũng như các chức năng của ứng dụng đề mô. Sự phê bình, góp ý của cô sẽ là những bài học kinh nghiệm rất quý báu cho công việc thực tế của chúng em sau này .

Kính chúc cô thật nhiều sức khoẻ, hạnh phúc và thành công trong cuộc sống.

Nhóm chúng em xin chân thành cảm ơn!

**MỤC LỤC**

[PHẦN MỞ ĐẦU 4](#_Toc154279492)

[1.Lí do chọn đề tài 4](#_Toc154279493)

[2.Mục tiêu nghiên cứu 4](#_Toc154279494)

[3.Phương pháp nghiên cứu 4](#_Toc154279495)

[4.Đối tượng nghiên cứu 5](#_Toc154279496)

[5.Ý nghĩa của nghiên cứu 5](#_Toc154279497)

[6.Bố cục nghiên cứu 5](#_Toc154279498)

[Chương 1. Tổng quan đề tài 6](#_Toc154279499)

[1.1.Tổng quan về an toàn và bảo mật thông tin 7](#_Toc154279500)

[1.2.Sự cần thiết của An toàn và bảo mật thông tin 8](#_Toc154279501)

[1.3.Mục đích của An toàn và bảo mật thông tin 9](#_Toc154279502)

[1.4.Chữ kí số 10](#_Toc154279503)

[Chương 2. Kết quả nghiên cứu 14](#_Toc154279504)

[2.1.Giới thiệu 14](#_Toc154279505)

[2.2.Tổng quan về chữ ký số RSA 15](#_Toc154279506)

[2.2.1 Kiến trúc tổng quan về chữ kí số RSA 15](#_Toc154279507)

[2.2.2 Giải thuật RSA và hàm băm mật mã MD5 17](#_Toc154279508)

[2.2.3 Các điểm yếu của chữ ký số RSA 20](#_Toc154279509)

[2.2.4 Các dạng tấn công 22](#_Toc154279510)

[2.3.Ứng dụng của RSA trong chữ ký số 23](#_Toc154279511)

[2.4.Thiết kế, cài đặt chương trình demo thuật toán 25](#_Toc154279512)

[Chương 3. Bài học kinh nghiệm 29](#_Toc154279513)

[3.1.Bài học kinh nghiệm 29](#_Toc154279514)

[3.2.Kết luận 29](#_Toc154279515)

[TÀI LIỆU THAM KHẢO 31](#_Toc154279516)

# PHẦN MỞ ĐẦU

## 1.Lí do chọn đề tài

Trong thời đại bùng nổ công nghệ thông tin như hiện nay, dữ liệu cá nhân trên không gian mạng trở thành một kho lưu trữ khổng lồ mà nếu chúng ta không có biện pháp bảo vệ tương xứng, đúng cách thì sẽ tạo ra điều kiện thuận lợi để tội phạm hay các phần tử xấu lợi dụng thực hiện các hành vi vi phạm pháp luật tiềm ẩn nguy cơ mất an ninh thông tin.

Lợi dụng sự chủ quan, lơ là và đánh vào tâm lý “hám lời” của người dân, đề nghị cung cấp thông tin và sau đó chiếm đoạt dưới hình thức các chương trình khuyến mãi, bốc thăm trúng thưởng, mua hàng online, mini game có thưởng…

Trong thực tế các hacker, các dạng virus luôn tấn công và là mối đe dọa của các nguồn tài nguyên thông tin. Những vấn đề đảm bảo an toàn thông tin trong các hệ thống máy tính là rất quan trọng.

Hiểu được điều đó, nhóm 14 chúng em đã cùng nhau tìm hiểu về ứng dụng RSA trong chữ ký số điện tử và thực hiện xây dựng chương trình chữ ký RSA.

## 2.Mục tiêu nghiên cứu

Nghiên cứu về lý thuyết mật mã hoá khoá công khai RSA, chữ ký số và ứng dụng thuật toán RSA trong chữ ký số điện tử. Từ đó xây dựng hệ thống cho phép tạo và kiểm tra chữ ký số đối với các tài liệu: công văn, giấy tờ hành chính điện tử để bảo mật nội dung thông tin cũng như xác thực nguồn gốc của thông tin.

## 3.Phương pháp nghiên cứu

Nghiên cứu, thu thập các tài liệu đã xuất bản, các bài báo trên các tạp chí khoa học và các tài liệu trên mạng liên quan đến vấn đề đang nghiên cứu của các tác giả trong và ngoài nước. Từ đó chọn lọc và sắp xếp lại theo ý tưởng của bản thân.

## 4.Đối tượng nghiên cứu

Hệ mật mã khóa công khai RSA

Mô hình chung về chữ ký số và chữ ký số RSA

Ứng dụng của RSA trong chữ ký số điện tử

## 5.Ý nghĩa của nghiên cứu

Biết thêm được nhiều ứng dụng hữu ích của RSA trong chữ ký số điện tử với mục đích bảo vệ dữ liệu.

Xây dựng được chương trình ứng dụng dựa vào hệ mật mã RSA có chức năng bảo mật nội dung cho các tập tin, các dữ liệu hoặc các tài liệu, tạo và kiểm tra chữ ký số cho các tập tin đó để xác định toàn vẹn nội dung và người sửa hữu của tập tin khi thực hiện trao đổi qua Internet.

## 6.Bố cục nghiên cứu

Ngoài phần mở đầu, danh mục tài liệu tham khảo và các phụ lục thì nội dung chính của nghiên cứu bao gồm 03 chương chính cụ thể như sau:

Chương 1: Tổng quan đề tài

Chương 2: Kết quả nghiên cứu

Chương 3: Bài học kinh nghiệm

# Chương 1. Tổng quan đề tài

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 bảm 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.

## 1.1.Tổng quan về an toàn và bảo mật thông tin

An toàn thông tin là các hoạt động bảo vệ tài sản thông tin và là một lĩnh vực rộng lớn. Nó bao gồm cả những sản phẩm và những quy trình nhằm ngăn chặn truy cập trái phép, hiệu chỉnh, xóa thông tin,…

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.

An toàn thông tin liên quan đến hai khía cạnh đó là an toàn về mặt vật lý và an toàn về mặt kỹ thuật.

Mục tiêu cơ bản của an toàn thông tin:

+ Đảm bảo tính bảo mật.

+ Đảm bảo tính toàn vẹn.

+ Đảm bảo tính xác thực.

+ Đảm bảo tính sẵn sàng.

Phương thức, thủ đoạn đánh cấp dữ liệu cá nhân:

- Sử dụng mã độc, phần mềm có tính năng gián điệp hay tấn công, xâm nhập hệ thống máy tính, làm gián đoạn, tổn hại tới tính bí mật, tính toàn vẹn và sẵn sàng của máy tính người sử dụng để chiếm đoạt thông tin dữ liệu cá nhân. Chẳng hạn, vụ tin tặc (hacker) rao bán khối lượng dữ liệu khách hàng của các nhà mạng, điện lực, ngân hàng và doanh nghiệp Việt Nam trên 01 diễn đàn cho hacker là một vấn đề đáng báo động và tiềm ẩn nguy cơ bị các đối tượng xấu lợi dụng để lừa đảo chiếm đoạt tài sản khách hàng.

- Tấn công vào hệ thống lưu trữ dữ liệu cá nhân, thông tin khách hàng để bán cho đối thủ của họ, ăn cắp mật khẩu của các tài khoản nhằm mục đích biển thủ tiền...

## 1.2.Sự cần thiết của An toàn và bảo mật thông tin

Hệ thống thông tin là thành phần thiết yếu trong mọi cơ quan, tổ chức và đem lại khả năng xử lý thông tin, là tài sản quan trọng nhưng hệ thống thông tin cũng chứa rất nhiều điểm yếu và rủi do. Do máy tính được phát triển với tốc độ rất nhanh để đáp ứng nhiều yêu cầu của người dùng, các phiên bản được phát hành liên tục với các tính năng mới được thêm vào ngày càng nhiều, điều này làm cho các phần mềm không được kiểm tra kỹ trước khi phát hành và bên trong chúng chứa rất nhiều lỗ hổng có thể dễ dàng bị lợi dụng. Thêm vào đó là việc phát triển của hệ thống mạng, cũng như sự phân tán của hệ thống thông tin, làm cho người dùng truy cập thông tin dễ dàng hơn và tin tặc cũng có nhiều mục tiêu tấn công dễ dàng hơn.



Việc bảo mật dữ liệu cá nhân là có ý nghĩa hết sức quan trọng bởi nếu dữ liệu bị đánh cắp có thể gây ra những tổn thất tài chính nghiêm trọng, nguy cơ bị tống tiền, lừa đảo, chiếm đoạt tài sản, bôi nhọ, xâm phạm danh dự, nhân phẩm, xâm hại tình dục..., gây hậu quả cả về vật chất và tinh thần, ảnh hưởng trực tiếp đến quyền và lợi ích hợp pháp của các cơ quan, tổ chức, doanh nghiệp và mỗi cá nhân. Vì vậy, trước hết là mỗi cá nhân cần thực hiện tốt bảo mật dữ liệu của mình để ngăn chặn hành vi trộm cắp dữ liệu, đảm bảo tính toàn vẹn của các thông tin cá nhân; bảo vệ quyền riêng tư và tránh được những hệ lụy, rủi ro phát sinh khi bị lộ, lọt, đánh cắp dữ liệu cá nhân.

## 1.3.Mục đích của An toàn và bảo mật thông tin

*+ Bảo vệ tài nguyên của hệ thống*

Các hệ thống máy tính lưu giữ rất nhiều thông tin và tài nguyên cần được bảo vệ. Trong một tổ chức, những thông tin và tài nguyên này có thể là dữ liệu kế toán, thông tin nguồn nhân lực, thông tin quản lý, bán hàng, nghiên cứu, sáng chế, phân phối, thông tin về tổ chức và thông tin về các hệ thống nghiên cứu. Đối với rất nhiều tổ chức, toàn bộ dữ liệu quan trọng của họ thường được lưu trong một cơ sở dữ liệu và được quản lý và sử dụng bởi các chương trình phần mềm.

Các tấn công vào hệ thống có thể xuất phát từ những đối thủ của tổ chức hoặc cá nhân do đó, các phương pháp để bảo đảm an toàn cho những thông tin này có thể rất phức tạp và nhạy cảm. Các tấn công có thể xuất phát từ nhiều nguồn khác nhau, cả từ bên trong và bên ngoài tổ chức. Hậu quả mà những tấn công thành công để lại sẽ rất nghiêm trọng.

*+ Bảo đảm tính riêng tư*

Các hệ thống máy tính lưu giữ rất nhiều thông tin cá nhân cần được giữ bí mật. Những thông tin này bao gồm: Số thẻ bảo hiểm xã hội, số thẻ ngân hàng, số thẻ tín dụng, thông tin về gia đình,...

Tính riêng tư là yêu cầu rất quan trọng mà các ngân hàng, các công ty tín dụng, các công ty đầu tư và các hãng khác cần phải đảm bảo để gửi đi các tài liệu thông tin chi tiết về cách họ sử dụng và chia sẻ thông tin về khách hàng. Các hãng này có những quy định bắt buộc để bảo đảm những thông tin cá nhân được bí mật và bắt buộc phải thực hiện những quy định đó để bảo đảm tính riêng tư. Hậu quả nghiêm trọng sẽ xảy ra nếu một kẻ giả mạo truy nhập được những thông tin cá nhân.

***=>*** 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, nhóm 14 chúng em đã nghiên cứu về ứng dụng RSA trong chữ ký số điện tử, đồng thời có viết được chương trình nhằm mục đích demo về vấn đề trên.

## 1.4.Chữ kí số

Chữ ký điện tử không phải là hình thức số hóa chữ ký viết tay rồi gửi kèm theo một thông điệp mà là một phương thức để chứng thực nguồn gốc và nội dung của một thông điệp thông qua kỹ thuật mã hóa.

Chữ ký số là một dạng chữ ký điện tử (là tập hợp con của chữ ký điện tử) được tạo ra bằng sự biến đổi một thông điệp dữ liệu ban đầu và khóa công khai của người ký có thể xác định chính xác.

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

Khóa công khai thường được phân phối thông qua chứng thực khóa công khai.

****

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

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

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

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

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

+ Giải thuật tạo chữ ký số.

+ Phương pháp chuyển dữ liệu thông điệp thành dạng có thể ký được.

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

+ Giải thuật kiểm tra chữ ký số.

+ Phương pháp khôi phục dữ liệu từ thông điệp.

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

Ví dụ : Ta có thể mô phỏng trực quan một hệ mật mã khoá 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 khoá 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.

* 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 (Priavte key) của người gửi và 1 giải thuật tạo chữ ký (Signature/ Encryption algorithm). Kết quả chữ ký số (Digital signature) của thông điệp hay còn gọi là chuỗi đại diện được mã hóa (Encryted message digest)

Thông điệp ban đầu (message) được ghép với chữ ký số (Digital signature) tạo thành thông điệp đã được ký (Signed message)

Thông điệp đã được ký (Signed message) được gửi cho người nhận

* Quá trình kiểm tra chữ kí (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 < hoặc >MD2 => chữ ký không hợp lệ. Thông điệp có thể đã bị sửa đổi hoặc không thực sự xuất phát từ người gửi.

# Chương 2. Kết quả nghiên cứu

## 2.1.Giới thiệu

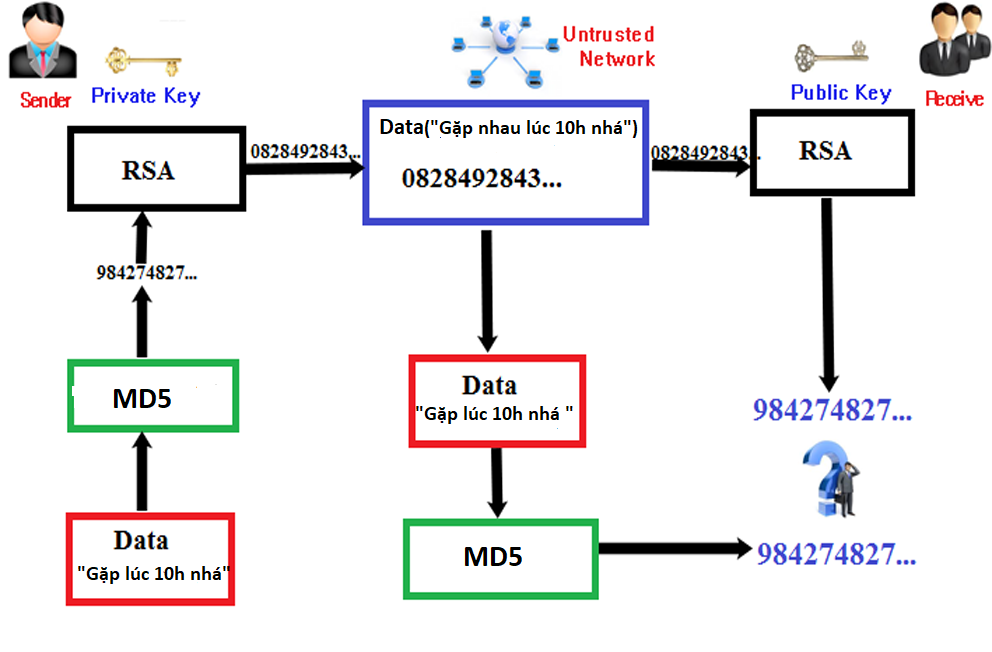
Tên đề tài nghiên cứu: Ứng dụng RSA trong chữ ký số điện tử. Demo sản phẩm minh họa

|  |  |  |
| --- | --- | --- |
| STT | Nhiệm vụ, công việc chính | Kết quả đạt được |
| 1 | Kiến trúc tổng quan về chữ ký số RSA | Đã tìm hiểu được kiến trúc tổng quan của chữ ký điện tử nói chung cũng như chữ ký điện tử RSA nói riêng |
| 2 | Giải thuật RSA và hàm băm mật mã MD5 | Nắm được giải thuật RSA trong chữ ký điện tử RSA và hàm băm mật mã MD5 |
| 3 | Các điểm yếu của chữ ký số RSA | Tìm hiều được một vài điểm yếu của chữ ký số RSA |
| 4 | Các dạng tấn công của chữ ký số RSA | Hiểu hơn được về các phương pháp tấn công đối với chữ ký số RSA |
| 5 | Ứng dụng chữ ký và sử dụng giải thuật RSA | Ứng dụng được chứ ký số RSA và viết được chương trình demo |

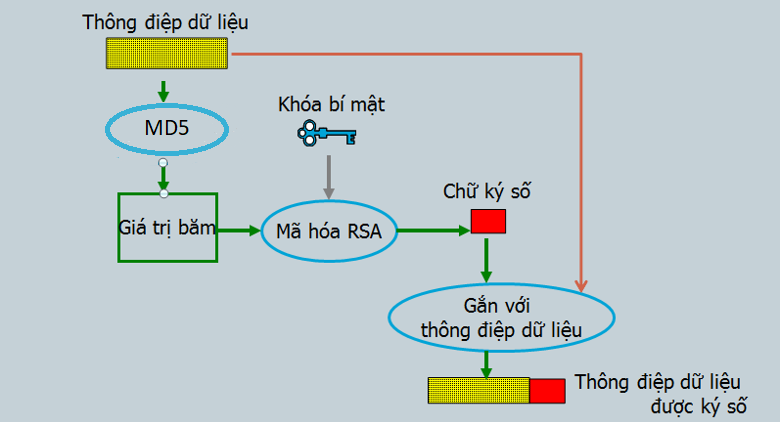
Nhằm minh họa phần nội dung kiến thức về chữ kí điện tử RSA, nhóm 14 đã xây dựng chương trình đề mô trên nền ngôn ngữ lập trình Python

## 2.2.Tổng quan về chữ ký số RSA

### 2.2.1 Kiến trúc tổng quan về chữ kí số RSA



* Quá trình ký (Bên gửi)



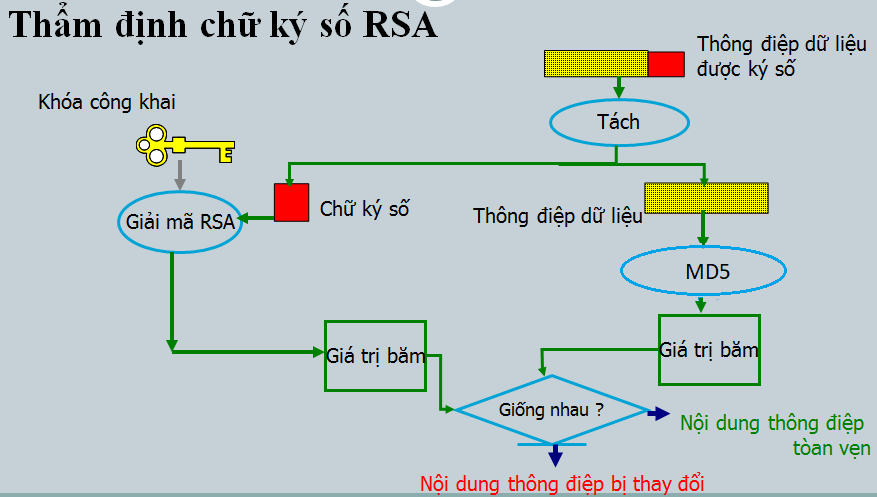
Tính toán chuỗi đại diện (message digest/ hash value) của thông điệp sử dụng một giải thuật băm (Hashing algorithm) MD5

Chuỗi đại diện được ký sử dụng khóa riêng (Priavte key) của người gửi và giải thuật tạo chữ ký (Signature/ Encryption algorithm) RSA. Kết quả chữ ký số (Digital signature) của thông điệp hay còn gọi là chuỗi đại diện được mã hóa bởi giải thuật RSA (Encryted message digest).

Thông điệp ban đầu (message) được ghép với chữ ký số( Digital signature) tạo thành thông điệp đã được ký (Signed message).

Thông điệp đã được ký (Signed message) được gửi cho người nhận.

* Quá trình kiểm tra chữ ký (Bên nhận)



Tách chữ ký số RSA 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 (giải thuật sử dụng trong quá trình ký là MD5)

Sử dụng khóa công khai (Public key) của người gửi để giải mã chữ ký số RSA=> 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 < hoặc >MD2 => chữ ký không hợp lệ. Thông điệp có thể đã bị sửa đổi hoặc không thực sự xuất phát từ người gửi.

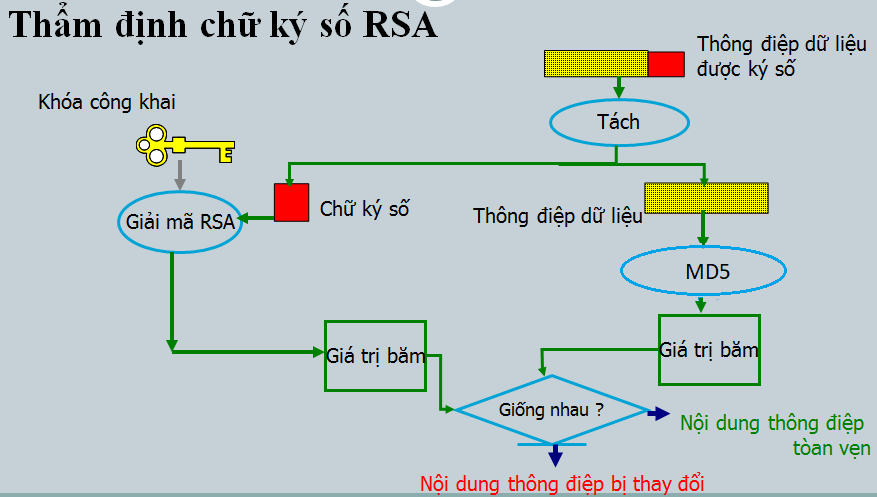
### 2.2.2 Giải thuật RSA và hàm băm mật mã MD5

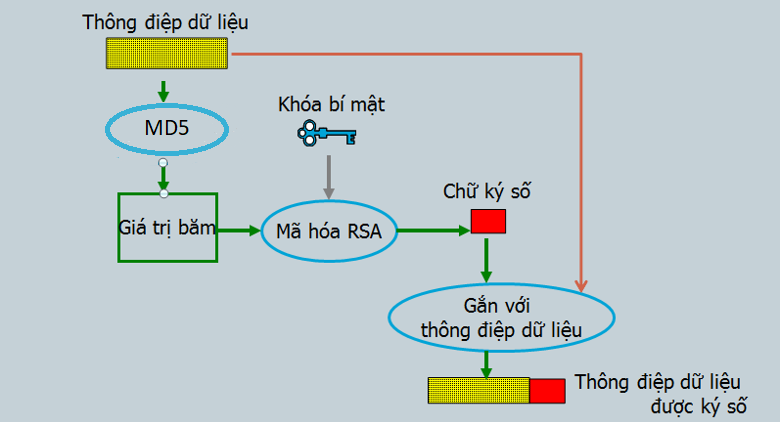
1. ***Giải thuật RSA***

* Tạo khóa:

Giải thuật RSA có hai khóa:

Khóa công khai (Public key – Kpub): được công bố rộng rãi cho mọi người và được dùng để thẩm định chữ ký số.



Khóa bí mật (Private key – Kpr ): không được chia sẻ được chia cho mọi người và được dùng để ký chữ ký số.

* Các bước tạo khóa:

B1: Đầu vào là hai SNT p và q.

B2: Tính N = p \* q và Φ(N) = (p-1)\*(q-1)

B3: Chọn ngẫu nhiên E thỏa mãn: { 1<E<Φ(N), GCD(E, Φ(N) = 1 }

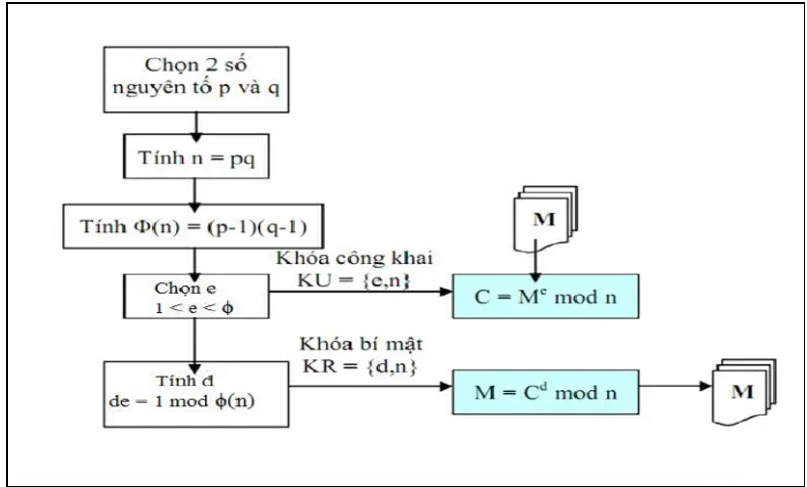
B4: Tính D = E-1 mod (Φ(N))

Kết quả: Kpub = {E, N}

Kpr = {D, N}

Hàm ký: M = sig(C) = CD mod N

Hàm kiểm tra: C = ME mod N



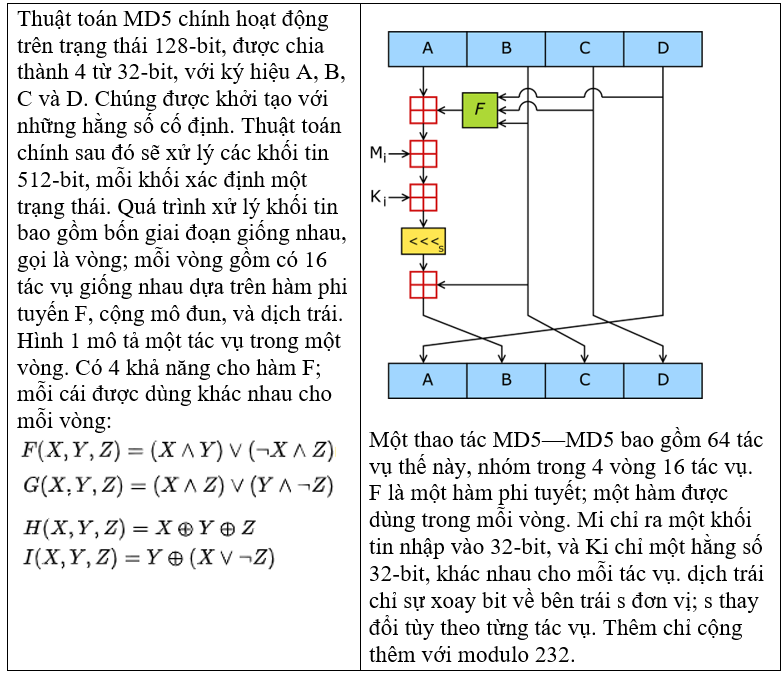
1. **Hàm băm mật mã MD5**

* Khái niệm:

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.

* Thuật toán:

MD5 chuyển một đoạn thông tin chiều dài thay đổi thành một kết quả chiều dài không đổi 128 bit. Mẩu tin đầu vào được chia thành từng đoạn 512 bit; mẩu tin sau đó được độn sao cho chiều dài của nó chia chẵn cho 512. Công việc độn vào như sau: đầu tiên một bit đơn, 1, được gắn vào cuối mẩu tin. Tiếp theo là một dãy các số zero sao cho chiều dài của mẩu tin lên tới 64 bit ít hơn so với bội số của 512. Những bit còn lại được lấp đầy bằng một số nguyên 64-bit đại diện cho chiều dài của mẩu tin gốc.



* Tính chất:

Tính xác định: cho 1 input cho ra một output duy nhất

Dễ tính toán: tính toán phải nhanh

Không thể đảo ngược: 1 output ko có một thuật toán nào cho ra input ban đầu

Chống va chạm – tránh xung đột: cho 2 input đầu thì xác suất cho ra cùng 1 output là cực kì thấp

Hiệu ứng nở tuyết: khi thay đổi 1 chút input thì output cho ra hoàn toàn khác mà không biết quy luật thay đổi

Chấp nhận tất cả dữ liệu chuyển vào

### 2.2.3 Các điểm yếu của chữ ký số RSA

1. **Điểm yếu của chữ ký số nói chung**

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.

Như vậy, với sự xuất hiện của chữ ký số, vấn đề giá trị pháp lý của tài liệu điện tử, có thể coi như đã được giải quyết. Việc sử dụng chữ ký số trong giao dịch cũng có những ưu điểm và bất cập nhất định. Dưới đây là những hạn chế của chữ ký số:

Sự lệ thuộc vào máy móc và chương trình phần mềm: chữ ký số là một chương trình phần mềm máy tính. Để kiểm tra tính xác thực của chữ ký cần có hệ thống máy tính và phần mềm tương thích.

Tính bảo mật không tuyệt đối: Nếu chữ ký bằng tay được thực hiện trên giấy, được ký trực tiếp và luôn đi kèm với vật mang tin, chữ ký tay không thể chuyển giao cho người khác, thì chữ ký số không như vậy. Chữ ký số là một bộ mật mã được cấp cho người sử dụng, đây là phần mềm máy tính không phụ thuộc vào vật mang tin. Chính vì vậy, trở ngại lớn nhất khi sử dụng chữ ký số là khả năng tách biệt khỏi chủ nhân của chữ ký. Nói cách khác, chủ nhân của chữ ký số không phải là người duy nhất có được mật mã của chữ ký. Tồn tại một số nhóm đối tượng có thể có được mật mã, đó là: bộ phận cung cấp phần mềm; bộ phận cài đặt phần mềm, những người có thể sử dụng máy tính có cài đặt phần mềm. Ngoài ra, mật mã có thể bị đánh cắp. Cũng có thể, chủ nhân chữ ký số chuyển giao cho người khác mật mã của mình. Như vậy, tính bảo mật của chữ ký số không phải là tuyệt đối.

Vấn đề bản gốc, bản chính: Nếu đối với tài liệu giấy, chữ ký được ký một lần và chỉ có một bản duy nhất (được coi là bản gốc). Bản gốc được ký bằng chữ ký sẽ không thể cùng lúc ở hai chỗ khác nhau. Có thể tin tưởng rằng, nếu bản gốc duy nhất mất đi thì sẽ không thể có bản thứ hai giống hệt như vậy. Nhưng với văn bản điện tử đã được ký bằng chữ ký số, người ra có thể copy lại và bản copy từ bản chính và bản copy từ bản copy không có gì khác biệt so với bản chính duy nhất được ký. Đây là một thách thức đối với công tác văn bản và cả nền hành chính. Khái niệm bản gốc, bản chính trong văn bản hành chính sẽ phải xem xét lại.

Sự có thời hạn của chữ ký điện tử: Chữ ký điện tử là chương trình phần mềm được cấp có thời hạn cho người sử dụng. Về lý thuyết, văn bản sẽ có hiệu lực pháp lý khi được ký trong thời hạn sử dụng của chữ ký. Tuy nhiên, thực tế hiệu lực pháp lý của văn bản hoàn toàn có thể bị nghi ngờ khi chữ ký số hết thời hạn sử dụng. Đây cũng là một hạn chế và thách thức rất lớn đối với việc sử dụng chữ ký số.

1. **Điểm yếu của chữ ký số RSA nói riêng**

* Hiệu suất thực hiện thuật toán RSA

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).

* 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

### 2.2.4 Các dạng tấn công

- Tấn công lặp

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

C1 = Ce (mod *n*)

C2 = C1e (mod *n*)

…………………

Ci = Ci-1e (mod *n*)

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

i

Cj = *C*j-1 (mod *n*)

C = Me (mod *n*)

- Tấn công module n dùng chung:

Simons và Norris cũng chỉ ra rằng hệ thống RSA có thể bị tấn công khi sử dụng module n dùng chung, thực vậy nếu một thông điệp M được mã hoá bằng hai khoá công khai e1 và e2 từ hai thành viên trong hệ thống thì được:

C1 = M e1 (mod n)

C2 = M e2 (mod n)

Sau đó người tấn công dùng thuật toán Euclide mở rộng:(e1)\*a +(e2)\*b = 1 sao cho gcd(e1, e2 ) = 1 thì M được khôi phục lại như sau:

M = mod n.

- Tấn công khi khóa công khai E nhỏ:

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

Giả sử để gửi thông điệp M đến các người dùng P1, P2 …,Pk với khoá công khai là (ei , ni). A mã hoá M bằng khoá công khai (ei , ni) và gửi các bản mã Ci đến người dùng Pi, biết M < ni với i = 1, 2,…, n.

Ta có thể nghe trộm kết nối ra ngoài của A và thu thập được k bản mã Ci.

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

Thực vậy, nếu có được C1, C2, C3 với

C1 = M3 mod n1 ; C2 = M3 mod n2 ; C3 = M3 mod n3 và gcd(ni, nj) = 1, i ≠ j. Áp dụng định lý số dư Trung Hoa với C1, C2, C3 tìm được:

C’ thuộc Zn1n2n3. Mặt khác M < ni với I =1, 2,…, n => M3 < n1n2n3

Khi đó C’ = M3 mod n1n2n3 -> M3 là số nguyên

Vậy M=

## 2.3.Ứng dụng của RSA trong chữ ký số

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.

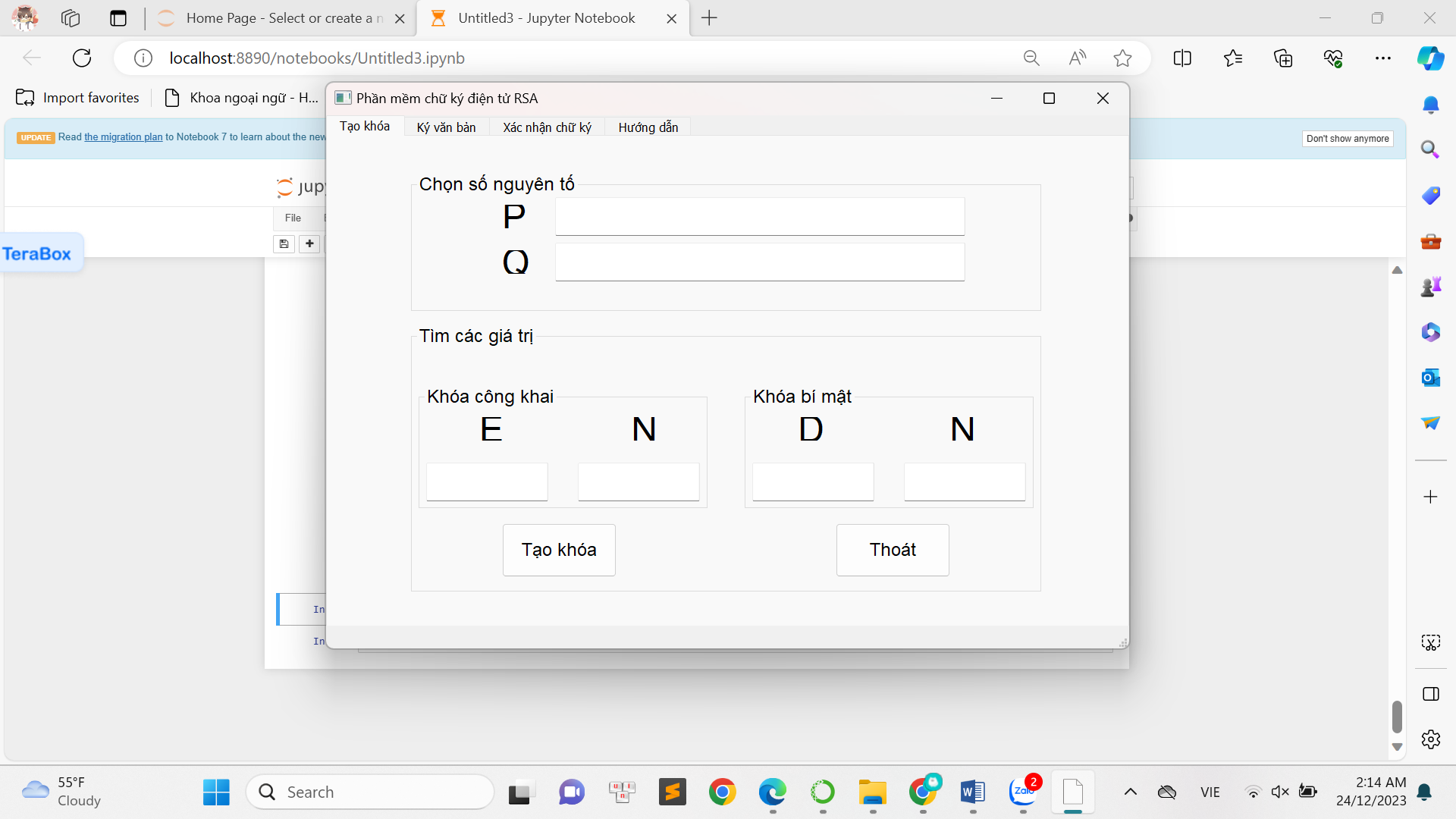


- Trong nhiều ngôn ngữ lập trình, các nhà lập trình viên thường sử dụng những đoạn code chứa RSA để tăng tính bảo mật cho trang web và ứng dụng cũng như đảm bảo an toàn cho người sử dụng.Các đoạn code RSA này có thể hoạt động dưới bất kỳ sự thay đổi nào của môi trường. Ngoài ra, các lập trình viên cũng 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.

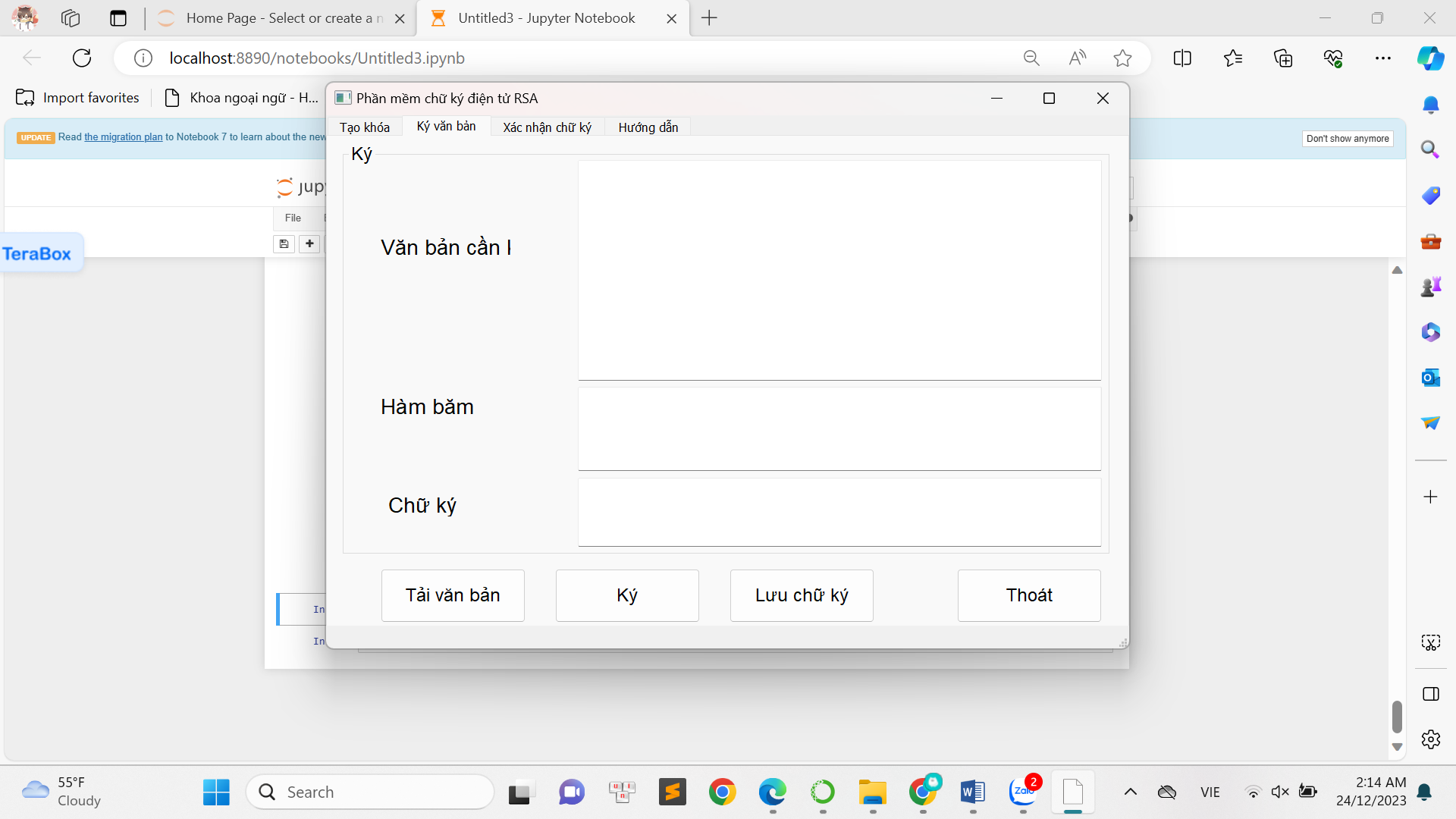
## 2.4.Thiết kế, cài đặt chương trình demo thuật toán

**\* Giao diện chương trình demo**

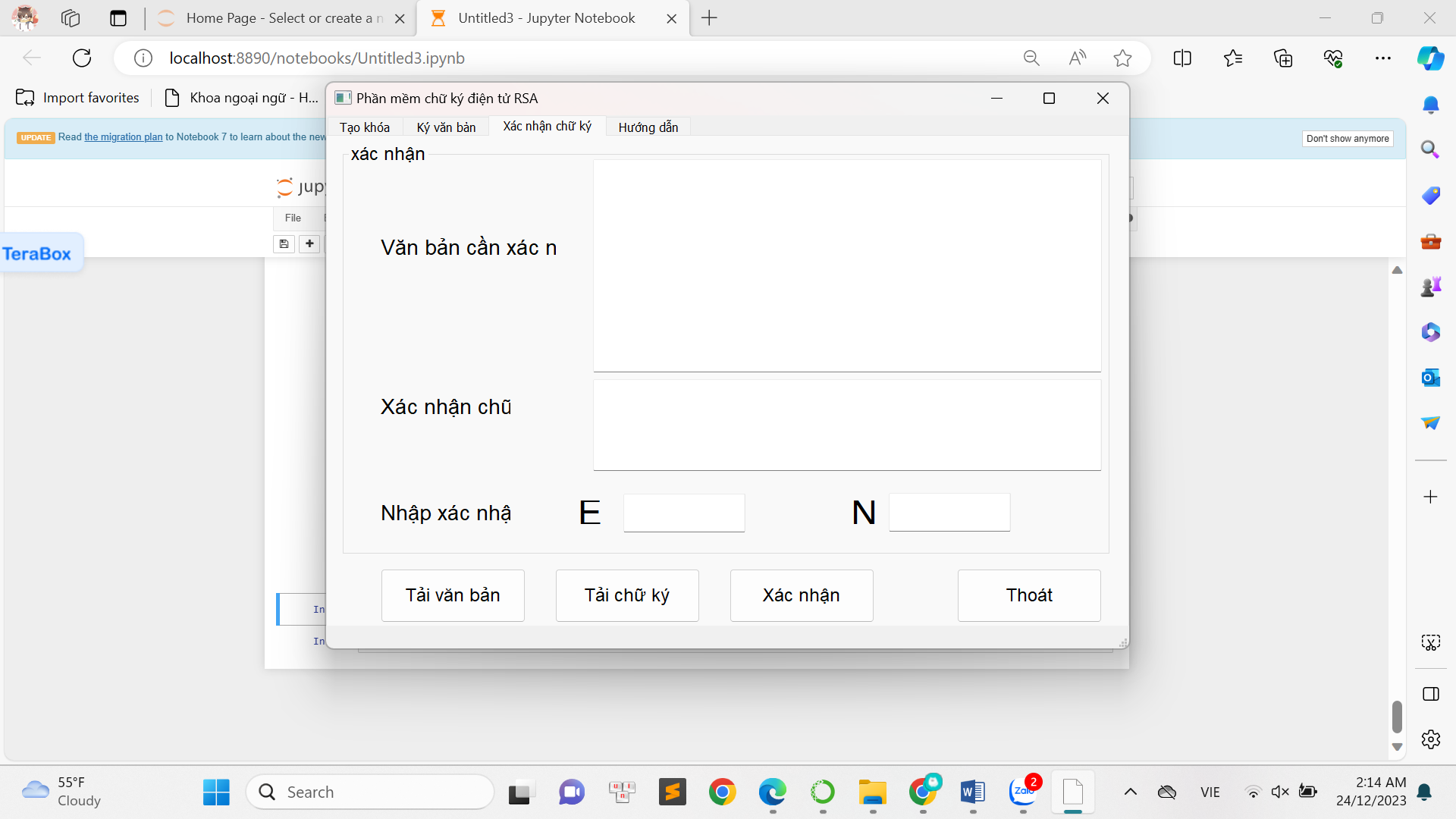
* Giao diện tạo khóa



* Giao diện ký văn bản

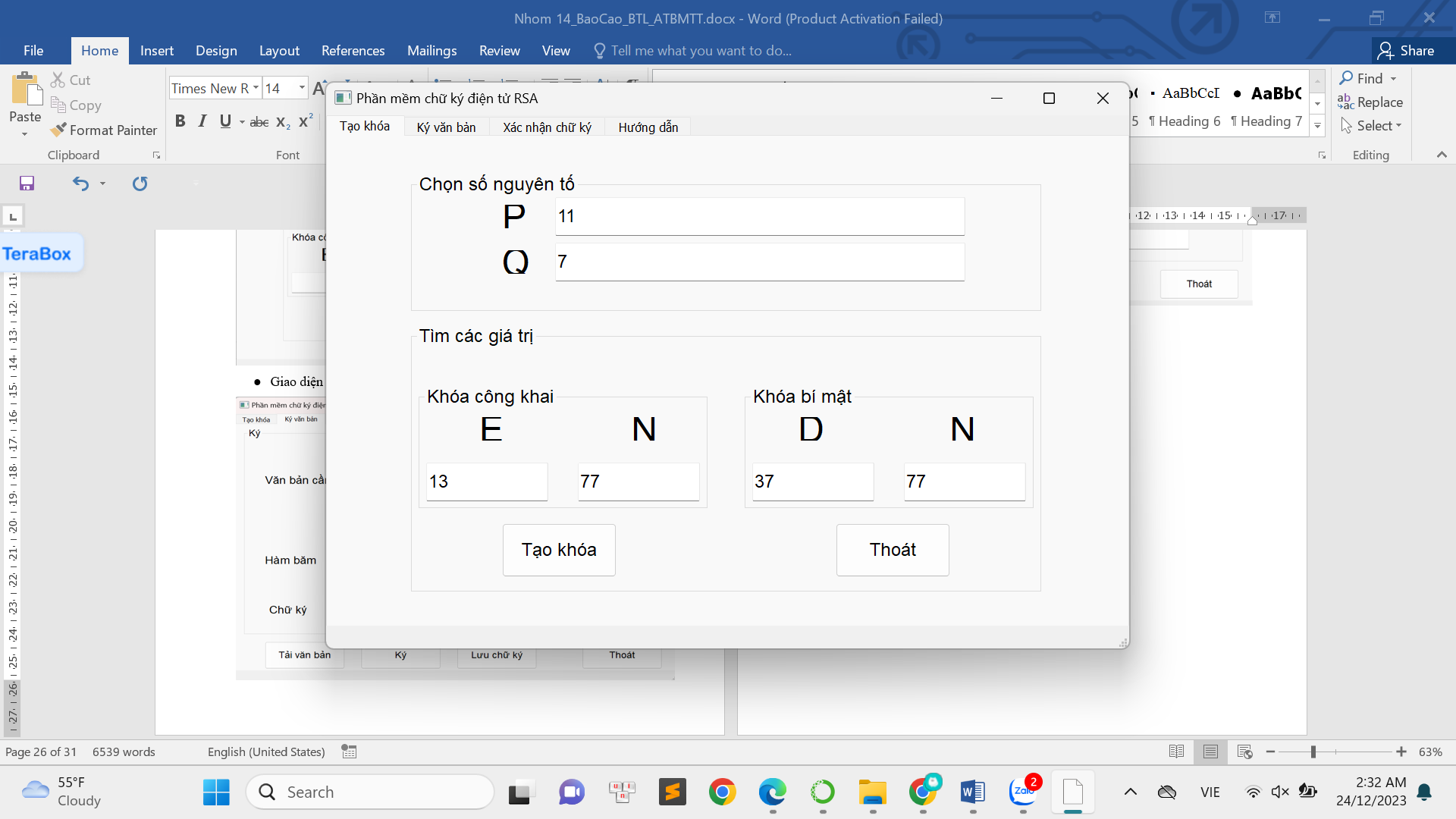


* Giao diện xác nhận chữ ký

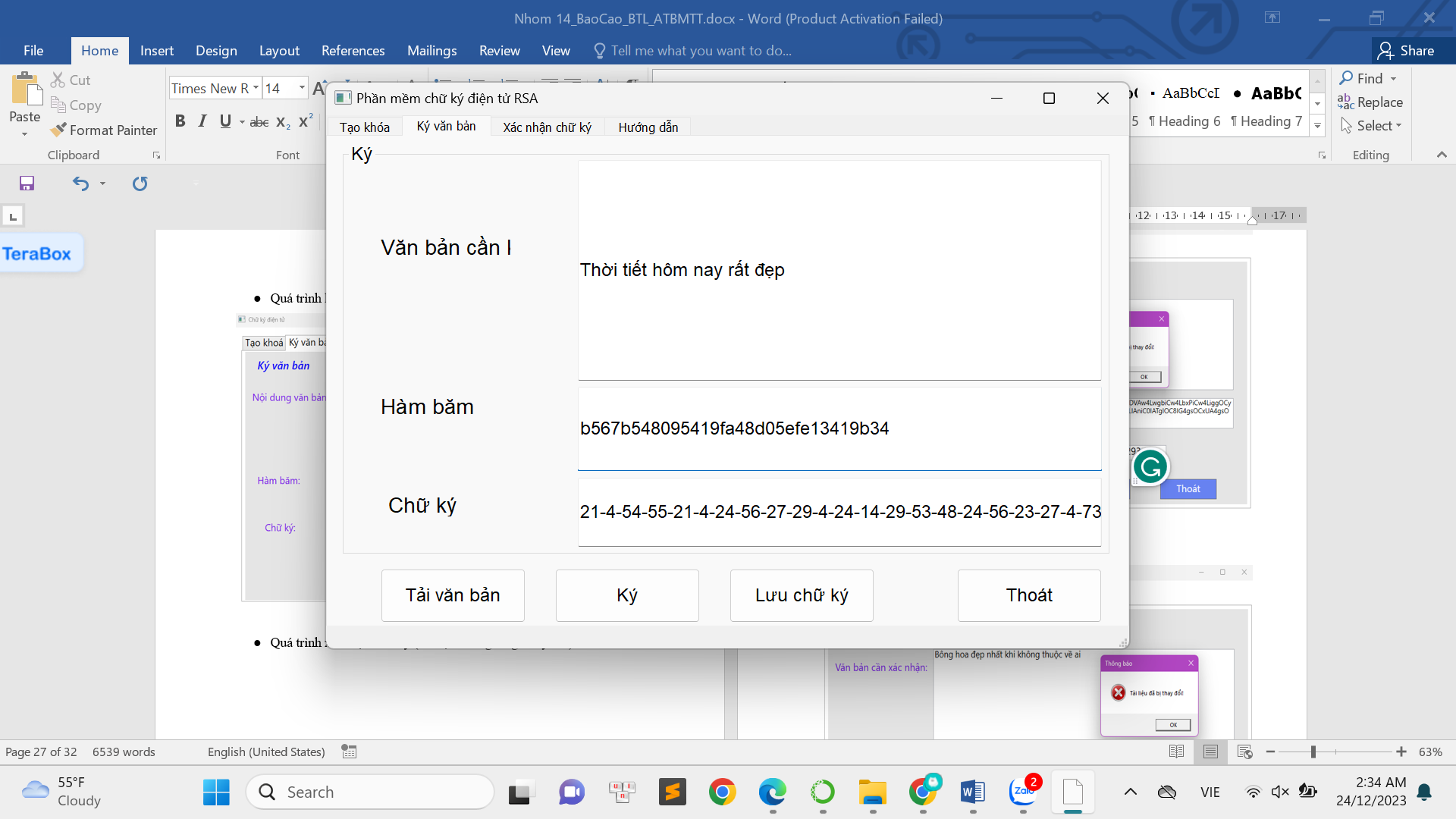


**\* Chạy chương trình demo**

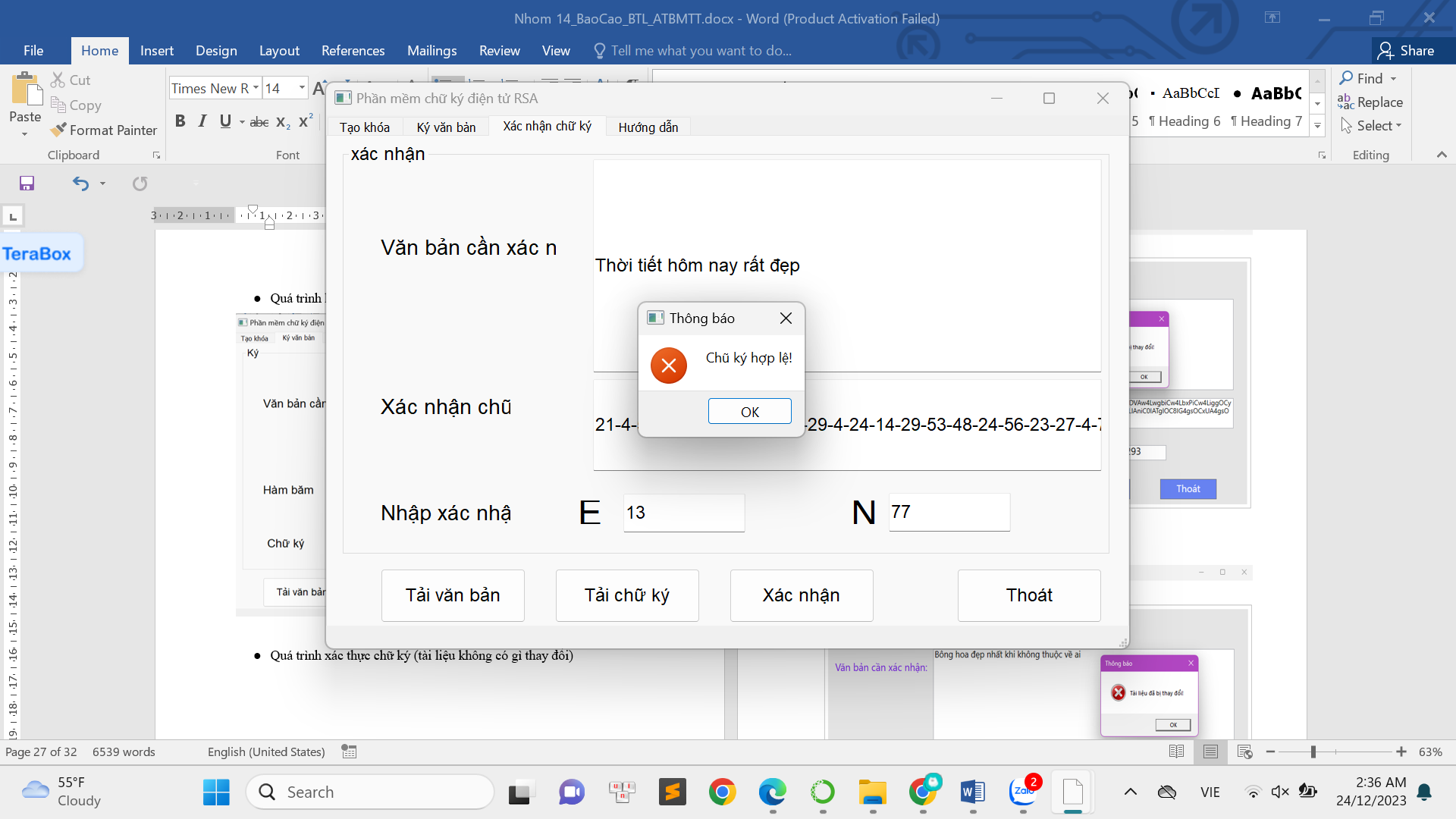
* Quá trình tạo khóa



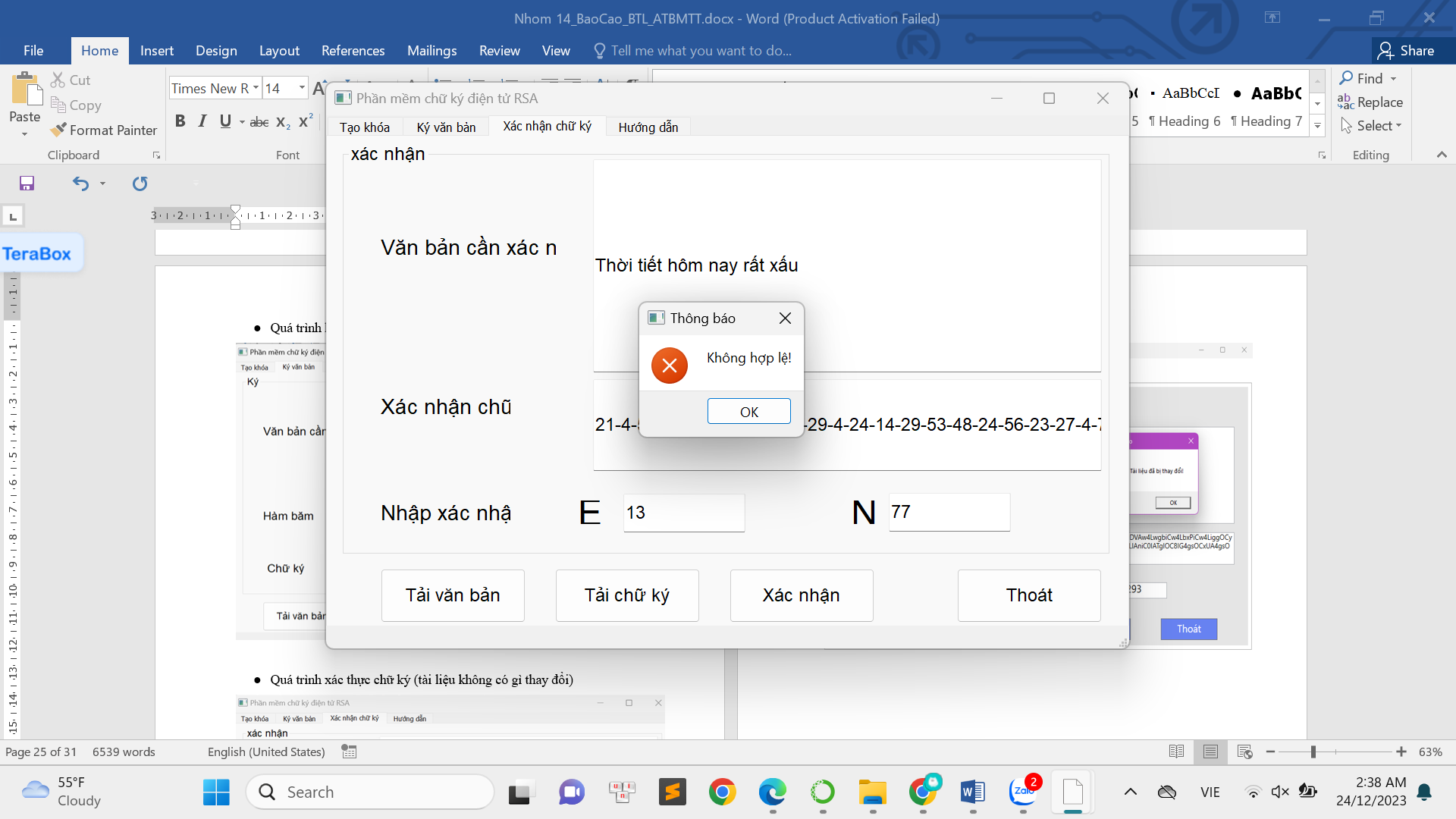
* Quá trình ký



* Quá trình xác thực chữ ký (tài liệu không có gì thay đổi)



* Quá trình xác thực chữ ký (tài liệu có thay đổi)



# Chương 3. Bài học kinh nghiệm

## 3.1.Bài học kinh nghiệm

* Các kỹ năng cần phải 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 mã hoá RSA.
* Kiến thức chuyên sâu :
* 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 (như Java, C#, C++, Python...).
* Hiểu và vận hành quy trình phát triển phần mềm.
* Phân tích lỗ hổng, virus, mã độc, phân tích đánh giá hệ thống.
* 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.

## 3.2.Kết luận

**\* Ưu điểm:**

**-** Chữ kí số RSA sử dụng thuật toán RSA là một thuật toán phù hợp cho việc phát triển các hệ thống bảo mật tương lai.

- Có thể dễ dàng thuận lợi trong việc triển khai bảo mật dữ liệu.

- Hoàn toàn có thể áp dụng vào những hệ thống bảo mật lớn với độ an toàn rẩt cao.

**\* Nhược điểm:**

**-** Tốc độ chậm (mất nhiều thời gian trong việc mã hóa do phải tính toán một số tài nguyên lớn).

- Dung lượng lưu trữ khóa yêu cầu cần phải lớn.

# TÀI LIỆU THAM KHẢO

[1] Phan Đình Diệu (2002). Lý thuyết mật mã và an toàn thông tin. NXB Đại học quốc gia Hà Nội.

[2] Secure Communicating Systems: Design, Analysis, and Implementation, Tác giả Michael Huth, Michael R. A. Huth

[3]<https://vi.wikipedia.org/wiki/Ch%E1%BB%AF_k%C3%BD_s%E1%BB%91>

[4][https://vi.wikipedia.org/wiki/RSA\_(m%C3%A3\_h%C3%B3a)](https://vi.wikipedia.org/wiki/RSA_(m%C3%A3_h%C3%B3a)%20)

[5]<https://www.educba.com/rsa-algorithm/>

[6]<https://www.geeksforgeeks.org/rsa-and-digital-signatures/>