TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**ĐỒ ÁN CUỐI KỲ MÔN BẢO MẬT THÔNG TIN**

**DIGITAL SIGNATURE AND ITS APPLICATIONS**

*Người hướng dẫn*: **TS. HUỲNH NGỌC TÚ**

*Người thực hiện*: **LÊ KHẮC THANH TÙNG – 52100943**

**TRẦN HỮU TÀI – 52100997**

**NGUYỄN QUANG LỢI – 52100909**

Lớp **: 21050301**

Khoá  **: 25**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2023**

TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**ĐỒ ÁN CUỐI KỲ MÔN BẢO MẬT THÔNG TIN**

**DIGITAL SIGNATURE AND ITS APPLICATIONS**

*Người hướng dẫn*: **TS. HUỲNH NGỌC TÚ**

*Người thực hiện*: **LÊ KHẮC THANH TÙNG – 52100943**

**TRẦN HỮU TÀI – 52100997**

**NGUYỄN QUANG LỢI – 52100909**

Lớp **: 21050301**

Khoá  **: 25**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2023**

**LỜI CẢM ƠN**

Lời đầu tiên, em xin gửi lời cảm ơn chân thành và sự tri ân sâu sắc đến với các thầy cô, giảng viên của khoa Công nghệ thông tin nói chung và các thầy cô giảng dạy môn Nhập môn Bảo mật thông tin nói riêng. Trong suốt quá trình học tập và rèn luyện, em đã nhận được rất nhiều sự giúp đỡ tận tình, sự quan tâm, chăm sóc của các thầy cô. Đặc biết là cô Huỳnh Ngọc Tú đã truyền đạt những kiến thức vô cùng bổ ích về môn học cho em.

Bởi lượng kiến thức của em còn hạn hẹp và gặp nhiều vấn đề trong quá trình học nên báo cáo bài tập lớn này sẽ còn nhiều thiếu sót và cần được học hỏi thêm. Em rất mong sẽ nhận được sự góp ý của quý thầy cô về bài báo cáo này của em để em rút kinh nghiệm trong những môn học sắp tới. Cuối cùng, em xin chân thành cảm ơn quý thầy cô.

TP Hồ Chí Minh, ngày tháng năm 2023

Sinh viên: Lê Khắc Thanh Tùng

Sinh viên: Trần Hữu Tài

Sinh viên: Nguyễn Quang Lợi

**ĐỒ ÁN ĐƯỢC HOÀN THÀNH**

**TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

Tôi xin cam đoan đây là sản phẩm đồ án của riêng tôi và được sự hướng dẫn của TS. Huỳnh Ngọc Tú. Các nội dung nghiên cứu, kết quả trong đề tài này là trung thực và chưa công bố dưới bất kỳ hình thức nào trước đây. Những số liệu trong các bảng biểu phục vụ cho việc phân tích, nhận xét, đánh giá được chính tác giả thu thập từ các nguồn khác nhau có ghi rõ trong phần tài liệu tham khảo.

Ngoài ra, trong đồ án còn sử dụng một số nhận xét, đánh giá cũng như số liệu của các tác giả khác, cơ quan tổ chức khác đều có trích dẫn và chú thích nguồn gốc.

**Nếu phát hiện có bất kỳ sự gian lận nào tôi xin hoàn toàn chịu trách nhiệm về nội dung đồ án của mình.** Trường đại học Tôn Đức Thắng không liên quan đến những vi phạm tác quyền, bản quyền do tôi gây ra trong quá trình thực hiện (nếu có).

*TP. Hồ Chí Minh, ngày tháng năm 2023*

*Tác giả*

*(ký tên và ghi rõ họ tên)*

*Lê Khắc Thanh Tùng*

*Trần Hữu Tài*

*Nguyễn Quang Lợi*

**PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN**

**Phần xác nhận của GV hướng dẫn**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tp. Hồ Chí Minh, ngày tháng năm

(kí và ghi họ tên)

**Phần đánh giá của GV chấm bài**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tp. Hồ Chí Minh, ngày tháng năm

(kí và ghi họ tên)

**TÓM TẮT**

Bài báo cáo tìm hiểu về cơ sở lý thuyết của việc tạo chữ ký số, trình bày chương trình demo và các kết quả đạt được.

**MỤC LỤC**

[LỜI CẢM ƠN i](#_heading=h.gjdgxs)

[PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN iii](#_heading=h.30j0zll)

[TÓM TẮT iv](#_heading=h.1fob9te)

[MỤC LỤC 1](#_heading=h.3znysh7)

[DANH MỤC CÁC BẢNG BIỂU, HÌNH VẼ, ĐỒ THỊ 3](#_heading=h.2et92p0)

[1.](#_heading=h.4d34og8) CHƯƠNG 4

[1.1.](#_heading=h.tyjcwt) Tiểu mục cấp 1 4

[1.1.1.](#_heading=h.2s8eyo1) Tiểu mục cấp 2 4

[1.1.2.](#_heading=h.17dp8vu) Tiểu mục cấp 2 4

[1.2.](#_heading=h.3dy6vkm) Tiểu mục cấp 1 4

[1.2.1.](#_heading=h.3rdcrjn) Tiểu mục cấp 2 4

[1.2.2.](#_heading=h.26in1rg) Tiểu mục cấp 2 4

[1.3.](#_heading=h.1t3h5sf) Tiểu mục cấp 1 4

[1.3.1.](#_heading=h.lnxbz9) Tiểu mục cấp 2 4

[1.3.2.](#_heading=h.35nkun2) Tiểu mục cấp 2 4

[2.](#_heading=h.1ksv4uv) CHƯƠNG 5

[2.1.](#_heading=h.44sinio) Tiểu mục cấp 1 5

[2.1.1.](#_heading=h.2jxsxqh) Tiểu mục cấp 2 5

[2.1.2.](#_heading=h.z337ya) Tiểu mục cấp 2 5

[2.2.](#_heading=h.3j2qqm3) Tiểu mục cấp 1 5

[2.2.1.](#_heading=h.1y810tw) Tiểu mục cấp 2 5

[2.2.2.](#_heading=h.4i7ojhp) Tiểu mục cấp 2 5

**DANH MỤC KÍ HIỆU VÀ CHỮ VIẾT TẮT**

**CÁC KÝ HIỆU**

**CÁC CHỮ VIẾT TẮT**

**DANH MỤC CÁC BẢNG BIỂU, HÌNH VẼ, ĐỒ THỊ**

**DANH MỤC HÌNH**

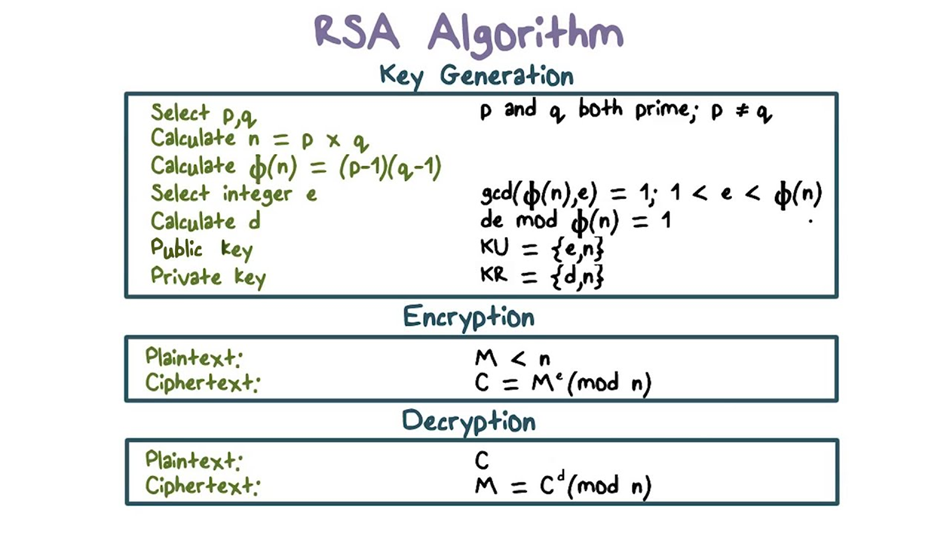
**No table of figures entries found.**

**DANH MỤC BẢNG**

**No table of figures entries found.**

1. **Cơ sở lý thuyết**
   1. **RSA**
      1. **Tổng quan**

* RSA là một thuật toán mã hóa công khai
* Phương pháp mã hóa công khai RSA là một dạng mã hóa cho phép người sử dụng trao đổi các thông tin mật mà không cần phải trao đổi các khóa chung bí mật trước đó. Điều này được thực hiện bằng cách sử dụng cặp khóa có quan hệ toán học với nhau. Một hệ mã hóa công khai sử dụng hai loại khóa: **public key** được công bố rộng rãi và được sử dụng trong việc mã hóa, **private key** chỉ do một người nắm giữ và được sử dụng để giải mã thông tin đã được mã hóa bằng khóa công khai
  + 1. **Thuật toán**

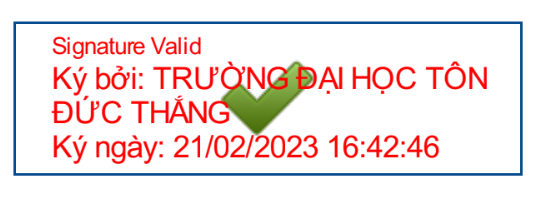
****

* 1. **Chữ ký số**
     1. **Giới thiệu**

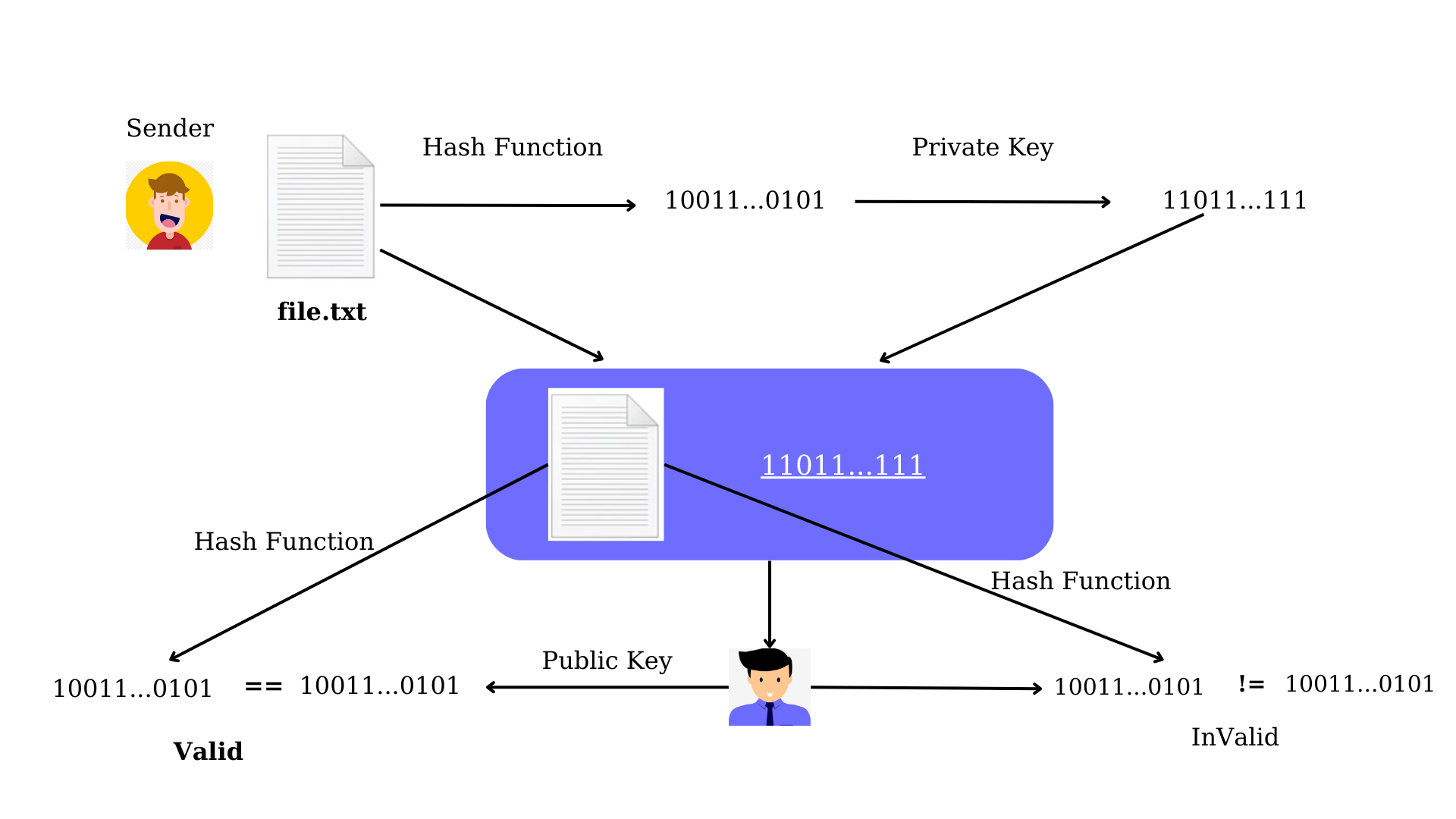
Digital signature (chữ ký số) là một phương tiện để xác thực tính toàn vẹn và nguồn gốc của một tài liệu điện tử (email, tài liệu văn bản, hợp đồng,...) thông qua việc sử dụng các thuật toán mã hóa và băm.

Nó là một loại chữ ký điện tử và cung cấp một cách để xác nhận rằng tài liệu không bị sửa đổi hoặc giả mạo kể từ khi nó được ký.

****

****

* + 1. **Nguyên lý hoạt động**

****

Người gửi gửi file.txt và nội dung của file được qua hàm băm thành mã nhị phân sau đó mã nhị phân kết hợp với private key tạo thành digital signature.

Sau đó digital signature này được đính kèm với file.txt và gửi đến người nhận. Người nhận nhận được cả file.txt và digital signature trên file đó. Sau đó người nhận sẽ giải mã digital signature thông qua public key thành mã nhị phân và file.txt cũng thông qua hàm băm ban đầu đã có được mã nhị phân. Sau đó ta so sánh 2 mã nhị phân này. Nếu giống nhau thì file này được gửi bởi chính người gửi, nếu khác nhau tức là đã có nội dung bị chỉnh sửa trong file.txt này và không phải do người gửi ban đầu gửi.

1. **Ngữ cảnh và kịch bản bảo mật**

Một user1 muốn gửi một tài liệu quan trọng cho user2 khác và sử dụng digital signature để xác thực tính toàn vẹn của tài liệu này.

Để đảm bảo an toàn cho quá trình này, user1 và user2 có thể thực hiện các bước sau:

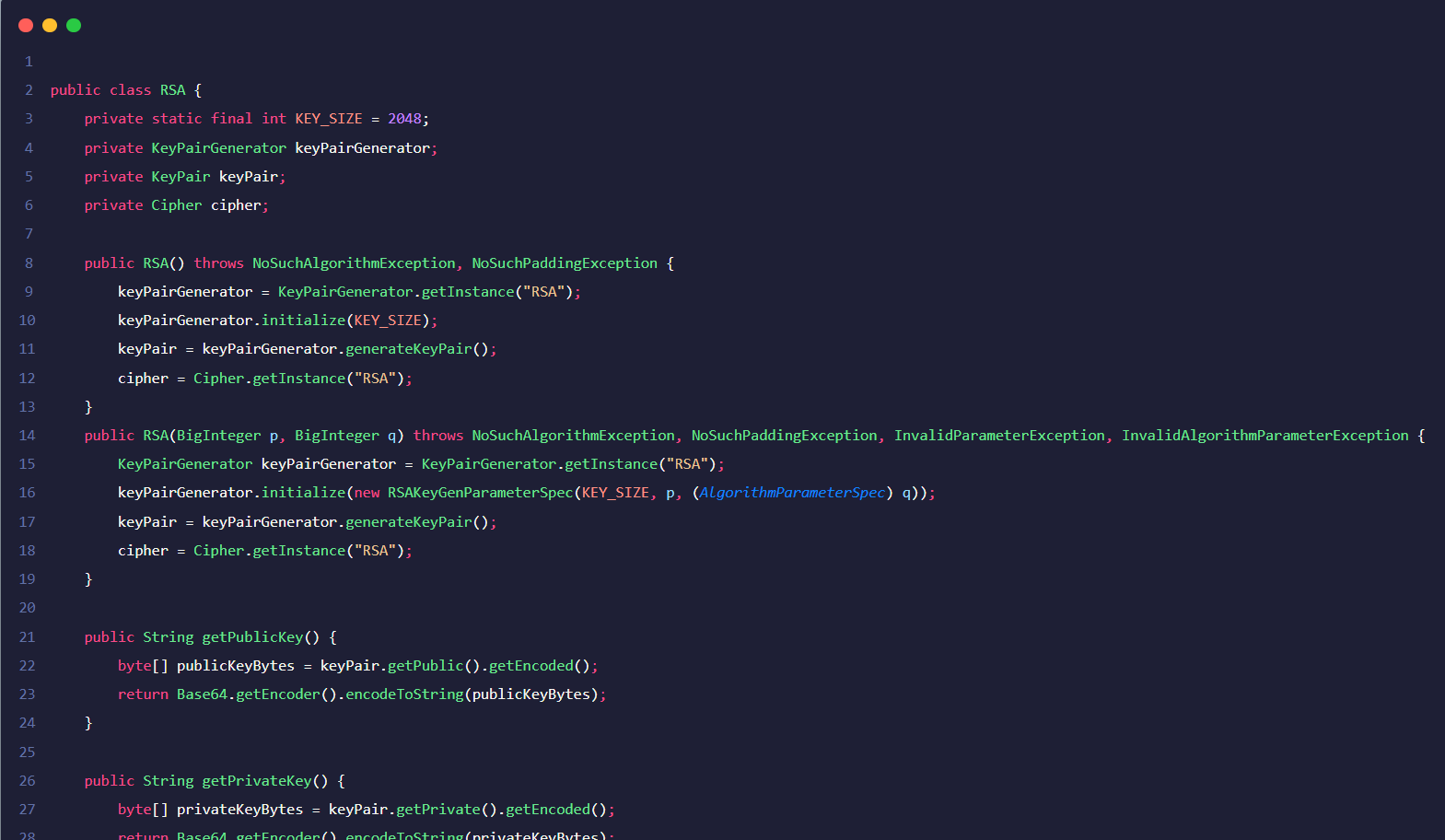
* User1 sử dụng một phần mềm digital signature để tạo ra một cặp khoá (public key và private key).
* Sau đó, cô lưu trữ private key của mình một cách an toàn. user1 sử dụng private key để tạo ra một chữ ký số (digital signature) cho tài liệu của mình.
* User1 gửi tài liệu cùng với chữ ký số đến user2 . Bob sử dụng public key của user1 để xác thực chữ ký số.
* Nếu chữ ký số được xác thực thành công, user2 có thể tin tưởng tính toàn vẹn và chính xác của tài liệu

Để đảm bảo an toàn cho quá trình này, user1 và user2 có thể thực hiện các biện pháp bảo mật sau:

* User1 chỉ sử dụng private key của mình để tạo ra chữ ký số. Cô không được chia sẻ private key với bất kỳ ai khác.
* User1 và User2 nên sử dụng các phần mềm digital signature được đáng tin cậy và được bảo vệ bởi các cơ quan bảo mật.
* User1 và User2 nên sử dụng kênh truyền thông an toàn để truyền tài liệu và chữ ký số.
* Ví dụ: sử dụng giao thức HTTPS hoặc sử dụng mã hóa PGP. user2 nên xác thực public key của user1 để đảm bảo rằng public key này thật sự thuộc về user1. User2 có thể sử dụng các cơ quan chứng thực để xác thực public key của user1.
* User2 nên kiểm tra lại tính toàn vẹn và chính xác của tài liệu sau khi đã xác thực chữ ký số của user1.

1. **CHƯƠNG 3: ỨNG DỤNG VỀ DIGITAL SIGNATURE**
   1. **Tổng quan**
      1. **Giới thiệu về chương trình  
         - Thực hiện chương trình java để làm ứng dụng desktop demo về hệ mật mã RSA mã hóa và giải mã như thế nào và áp dụng nó vào xác thực chữ ký số.**
      2. **Các chức năng của ứng dụng**

* Tạo cặp khóa tự động bằng thuật toán RSA .



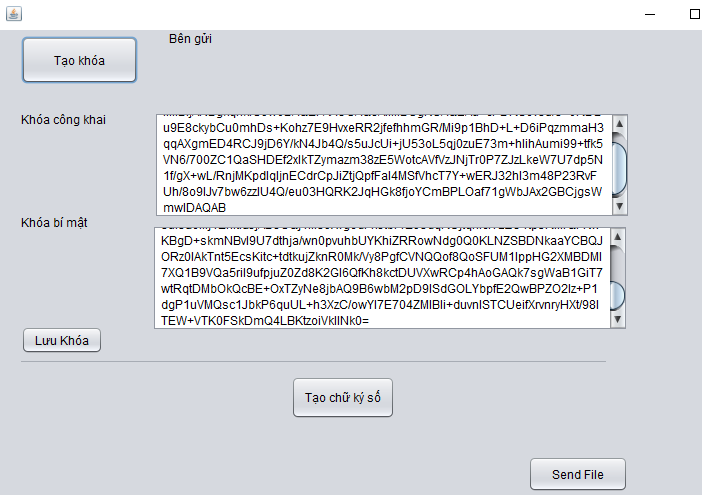
* Tạo lớp RSA chứa tất cả các method để có thể tạo khóa công khai và khóa bí mật.
* Hàm tạo khóa sẽ thực hiện tạo khóa thông qua thư viện java.security.\*; java.security.spec.AlgorithmParameterSpec ; java.security.spec.RSAKeyGenParameterSpec;
* Khóa sau khi tạo sẽ được chuyển đổi về dạng Base 64 và có thể sử dụng.
* Tạo khóa thủ công bằng thuật toán RSA.  
  + tạo khóa thủ công bằng cách người dùng có thể nhập hai biến p và q .
* Lưu trữ lại khóa vào thư mục.
* Sau khi tạo khóa , trong ứng dụng có một option để có thể lưu lại khóa vào trong thư mục mặc định là key của ứng dụng để có thể sử dụng và gửi đi cho người khác.
* Khóa được lưu dưới dạng Base 64.
* Mã hóa và giải mã sử dụng RSA.

+ Hệ mật mã RSA sẽ sử dụng khóa công khai để có thể mã hóa dữ liệu sang một dạng văn bản mã hóa.

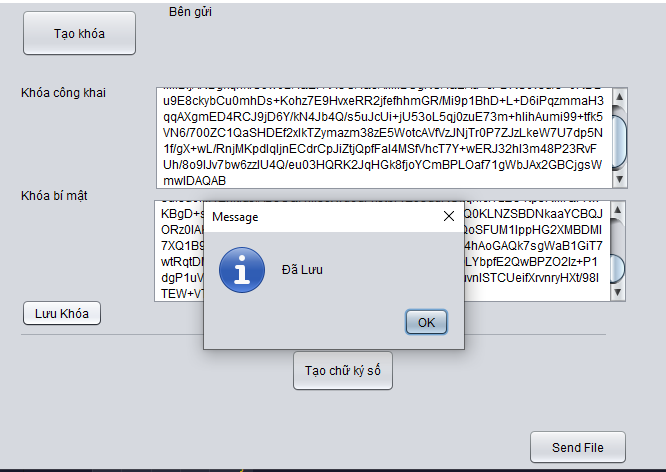
+ Hệ mật mã RSA sẽ sử dụng khóa bí mật để có thể giải mã đoạn text sau khi mã hóa về dạng ban đầu bằng khóa bí mật.

+ Bằng các giải mã phi đối xứng thì thuật toán bảo mật này có độ phức tạp cao hơn và khó có thể giải mã hơn vì thế nó được áp dụng trong chữ ký số.

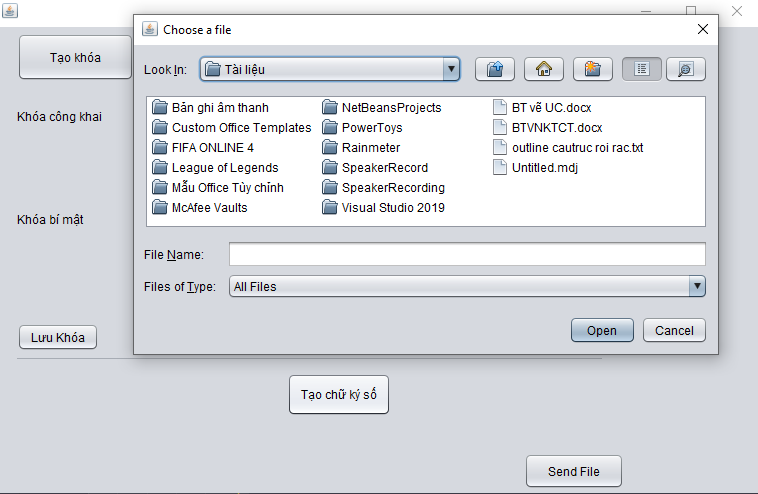
* Thực hiện ký lên đoạn văn bản và lưu đoạn văn bản được ký vào thư mục hệ thống.
* Áp dụng hệ mật mã RSA vào chữ ký số , nó giúp người dùng có thể ký vào bản tài liệu của họ và gửi đi cho bất kỳ ai .
* Ở đây chúng em làm ứng dụng để demo phần xác thực bằng chữ ký số.
* Đầu tiền tạo một cặp khóa công khai và bí mật .



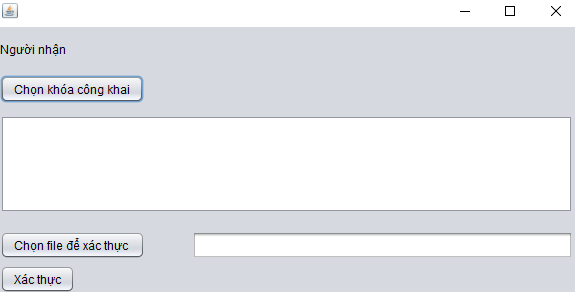
* Lưu lại lại khóa đã tạo.



* Thực hiện tạo chữ ký bằng cho một file bất kỳ bằng cách nhấn vào button tạo chữ ký số , sau đó hộp thoại sẻ hiện ra và chọn file cần tạo chữ ký số cho nó.



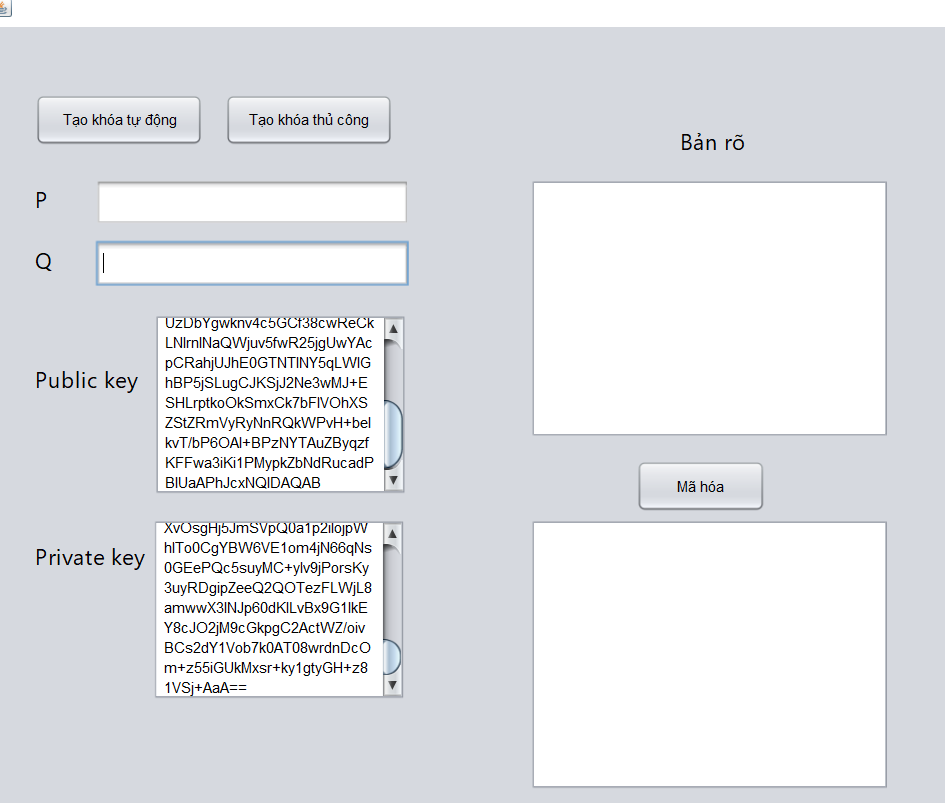
* File này sẽ được ký bằng khóa bí mật và lưu lại trong thư mục sign của hệ thống với đuôi .sign.
* Khi người dùng muốn kiểm tra tính toàn vẹn của dữ liệu không thay đổi sau khi gửi đi thì có thể chọn chức năng xác thực.



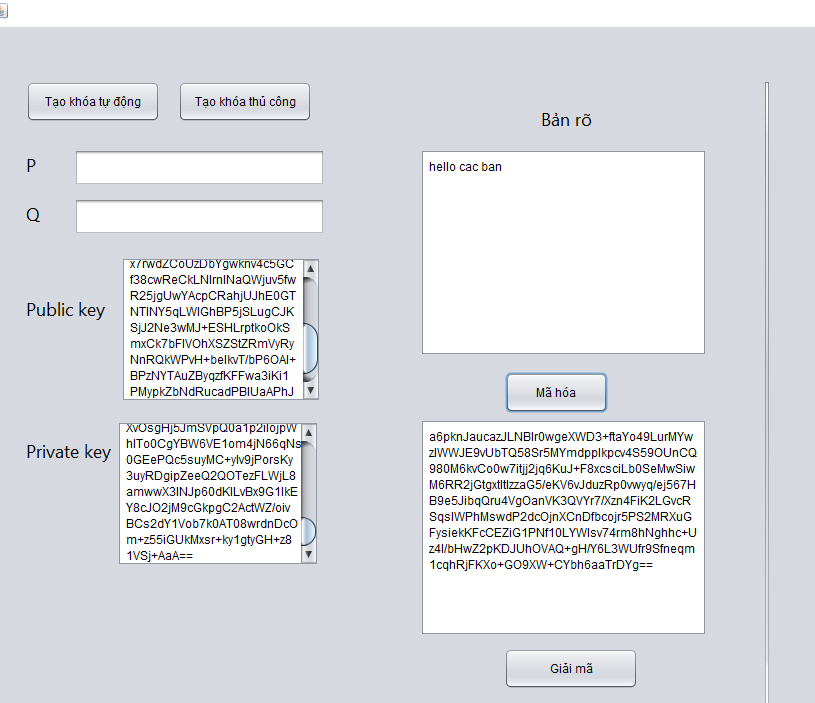
* Đầu tiên ứng dụng cho phép chọn khóa công khai mà người gửi cung cấp.
* Thực hiện chọn file để xác thực và file chữ ký số để xác thực
* Sau khi xác thực ứng dụng sẽ trả về kết quả cho người dùng.
* Xác thực đoạn văn bản được ký.
* Kiểm tra tính toàn vẹn dữ liệu của đoạn văn bản.
  1. **Demo**

**3.2.1 Thực hiện demo hệ mật mã RSA trong mã hóa và giải mã**

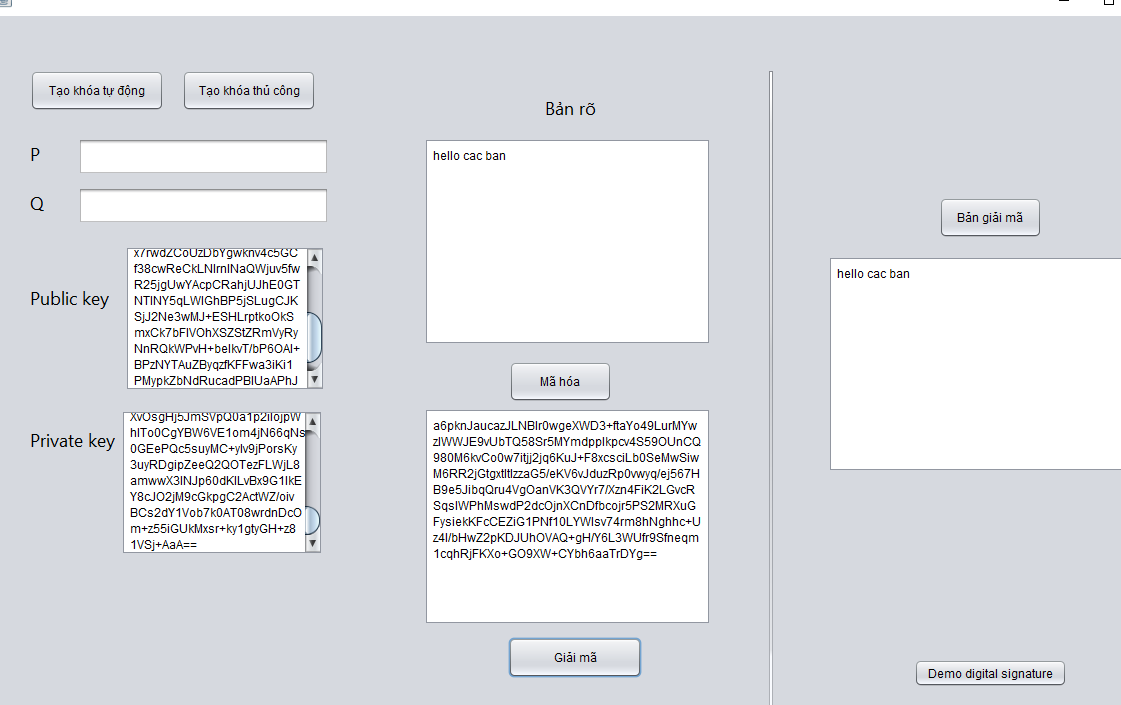
**b1 : Tạo khóa tự động , chương trình sẽ sinh ra hai cặp khóa bí mật và công khai.**

****

**-b2 : thực hiện nhập văn bản cần mã hóa và nhấn mã hóa văn bản đã được mã hóa sang một dạng khác tránh người khác đọc được thông tin bằng cách sử dụng mã hóa RSA với khóa công khai đã tạo lúc nảy.**

****

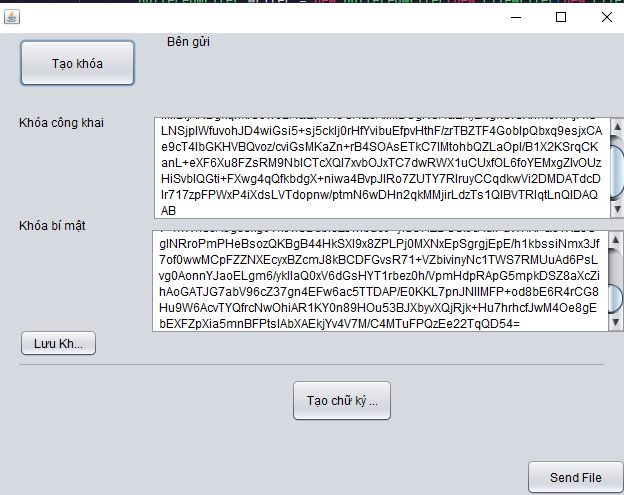
**b3: thực hiện giải mã văn bản cần giải mã , nhấn vào giải mã**

****

* **Văn bản sau khi giải mã đúng với đoạn text ban đầu.**

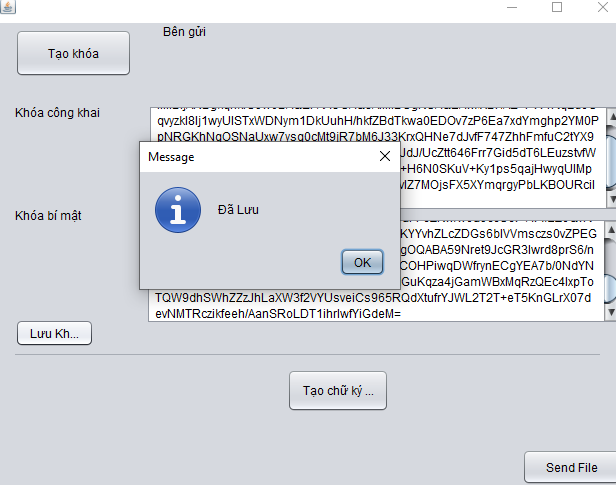
**3.2.2 Thực hiện demo hệ mật mã RSA áp dụng trong chữ ký số.**

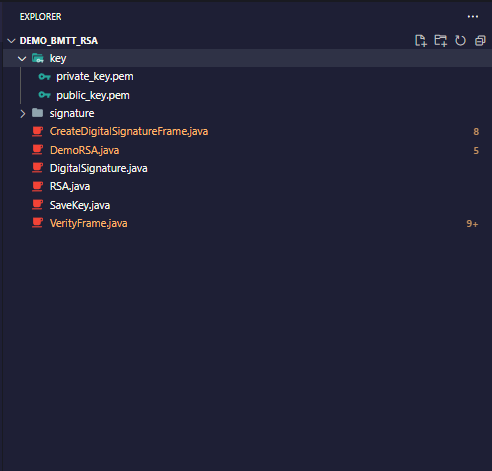
**- b1 : Thực hiện sinh khóa .**

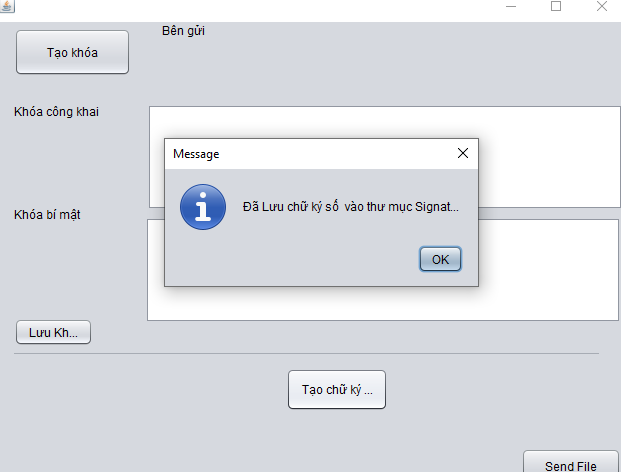
****

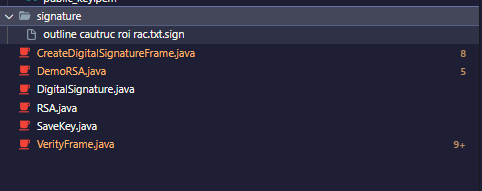
**Chương trình sẽ sinh ra cặp khóa là khóa công khai và khóa bí mật.**

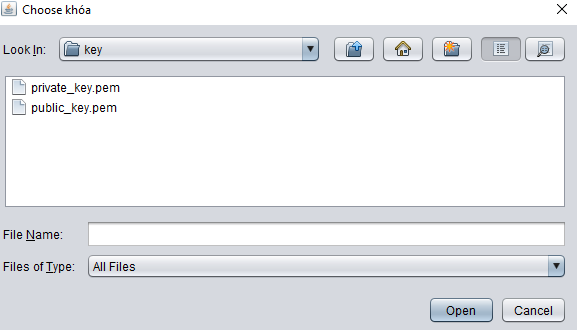
**B2: thực hiện lưu lại khóa**

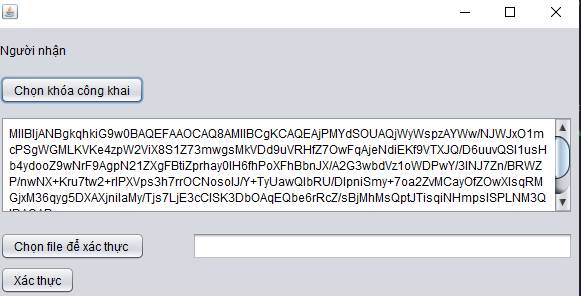
****

* **Khóa sau khi lưu sẽ được lưu đến thư mục key của hệ thống có đuôi là .pem .**
* ****

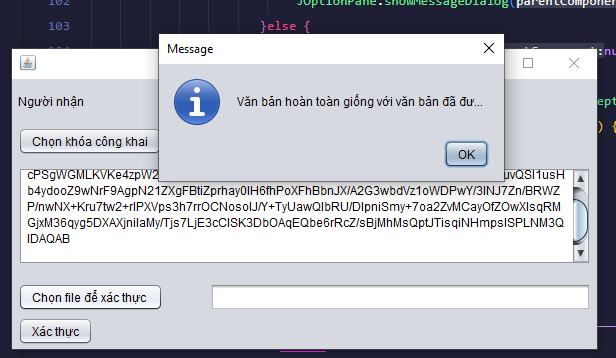
**b3 : Tạo chữ ký số và ký nó vào file bất kỳ.  
- Văn bản đã được ký và lưu trong thư mục signature vơi đuôi .sign.**

****

**b4: Sau khi đã có đoạn văn bản được ký thực hiện xác minh và kiểm tra tính bảo toàn dữ liệu của nó. Đầu tiên chọn khóa công khai đã được cung cấp từ người gửi.**

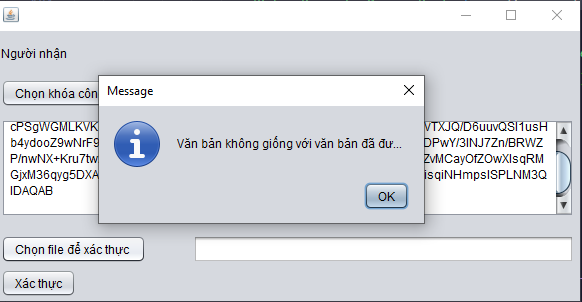
****

**b5 : tiếp theo chọn file với nội dung ban dầu và file đã được ký , giả sử nội dung ban đầu giống với nội dung của đoạn văn bản đã được ký.**

****

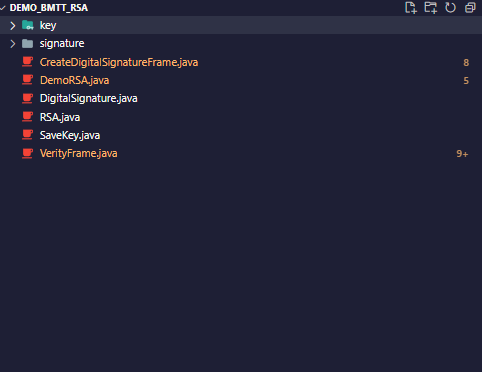
* **Văn bản hoàn toàn giống với văn bản đã được ký**

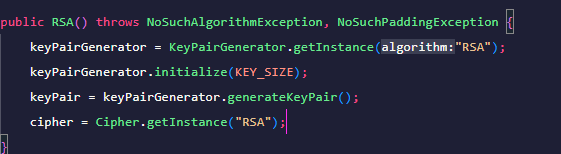
**b5 : tiếp theo chọn file với nội dung ban dầu và file đã được ký , giả sử nội dung ban đầu không giống với nội dung của đoạn văn bản đã được ký.**

****

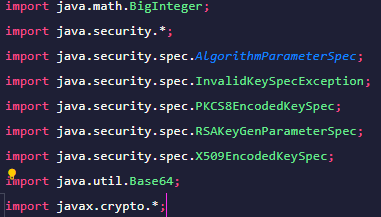
1. **CHƯƠNG 4: SOURCE CODE**

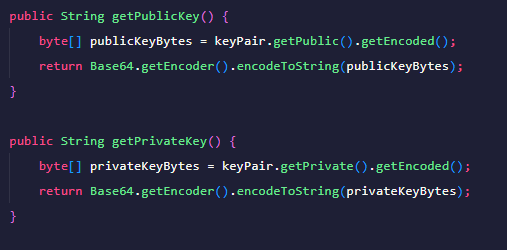
**4.1 Cấu trúc thư mục :**

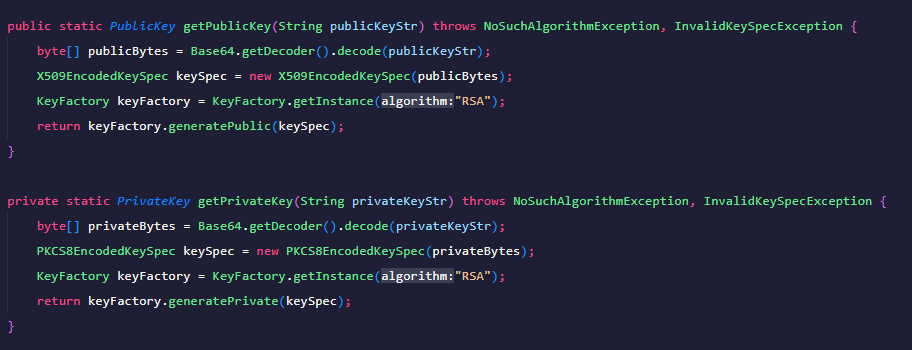
****

* **Chương trình bao gồm những lớp để phục vụ cho việc tạo khóa và tạo chữ ký số trong hệ mật mã RSA.**
* **DemoRSA.java : file này là ứng dụng demo về hệ mật mã RSA.**
* **CreateDigitalSignatureFrame.java : file này demo về phần hiện thực chữ ký số.**
* **Khởi tạo lớp RSA với nhiệm vụ chính là tạo khóa mã hóa và giải mã.**
* ****

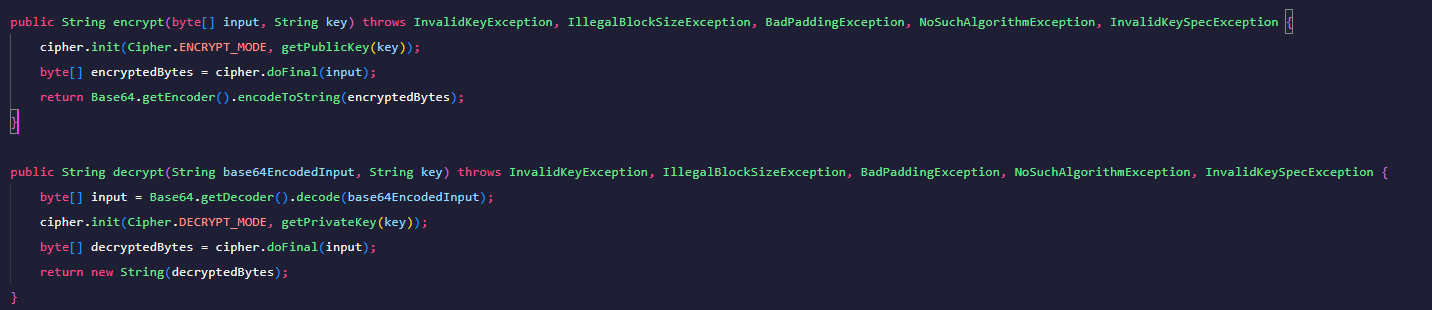
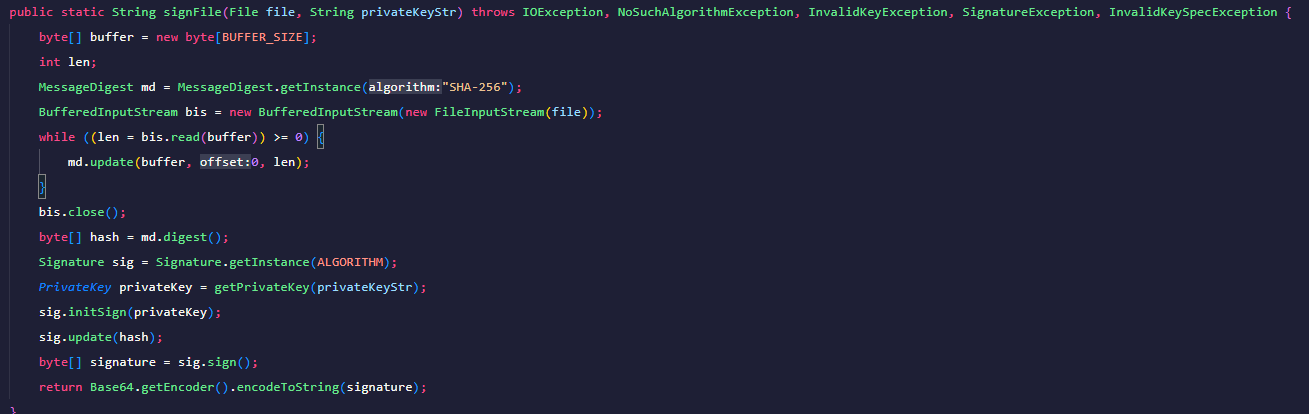
**Lớp này sử dụng thư viện java.security.\* để có thể tạo cặp khóa bí mật và công khai mà không cần tính toán phức tạp.**

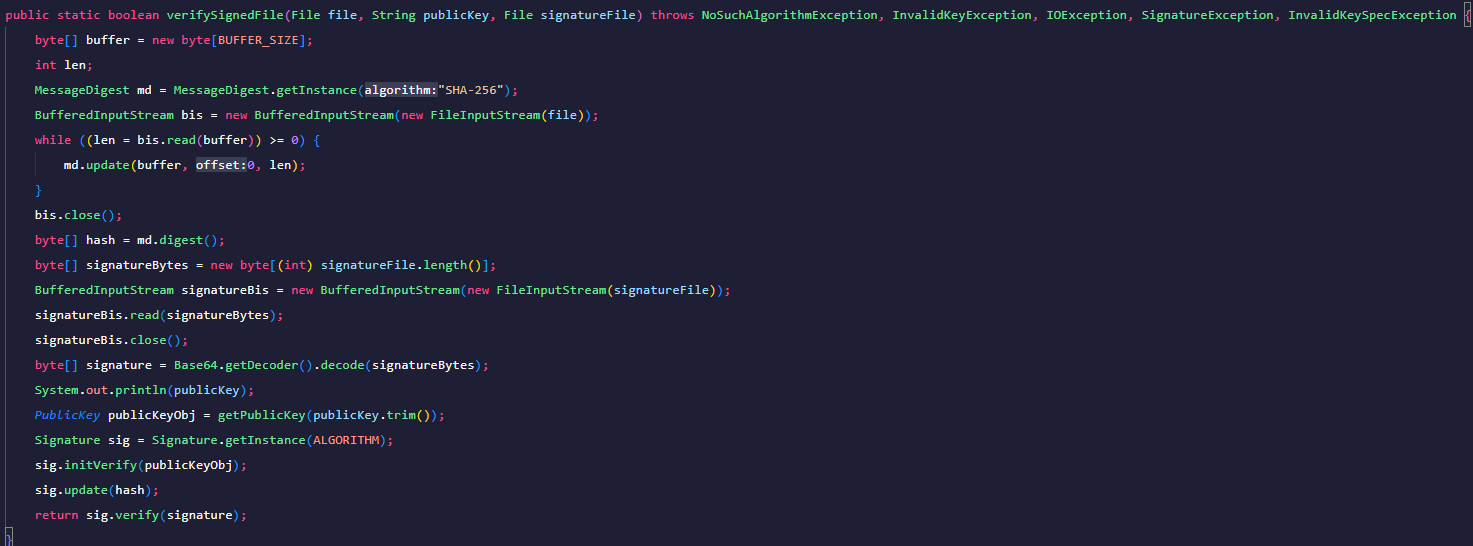
****

* **Hiện thực hai hàm lấy khóa sau khi khởi tạo đối tương RSA**
* ****
* **Hiện thực hàm lấy được khóa công khai và bí và trả về đối tượng keyFactory.generatePrivate(keySpec)**

****

**-Giải thích :**

* **Phải hiện thực hàm này bởi vì khi lưu khóa công khai và khóa bí mật thì chúng em thực hiện đưa nó về dạng string của Base 64 để dễ dàng trao đổi và có thể lấy khóa từ String thông qua hai hàm trên.**
* **Hiện thực hai hàm mã hóa và giải mã văn bản.**
* **Khởi tạo lớp DigitalSignature.java để có thể tạo chữ ký số từ một file bất kỳ .**
* ****
* **Hàm này sử dụng lại tất cả thư viện chuyển dổi chuôi , tạo khóa và tạo chữ ký số .**
* **Hiện thực hàm tạo chứ ký số**
* ****
* Giải thích :
  + Hàm nhận vào hai tham số đó là FIle cần ký và chuỗi của khóa bí mật.
  + Đầu tiên đọc dữ liệu từ file vào buffer: Hàm tạo ra một mảng byte có kích thước BUFFER\_SIZE để đọc dữ liệu từ file vào buffer.
  + Tiếp theo tính giá trị băm của dữ liệu: Hàm sử dụng thuật toán băm SHA-256 để tính toán giá trị băm của dữ liệu được đọc từ file.
  + Với mỗi lần đọc dữ liệu từ buffer vào message digest (md), hàm update() sẽ cập nhật giá trị băm md với dữ liệu đó
  + . Kết thúc quá trình tính giá trị băm: Sau khi đọc hết dữ liệu từ file, hàm digest() được gọi để lấy giá trị băm cuối cùng của dữ liệu.
  + Ký và mã hóa dữ liệu: Hàm sử dụng thuật toán ký và mã hóa RSA để ký giá trị băm vừa tính toán được ở bước trước.
  + Đầu vào của hàm là khóa riêng (private key) được truyền vào dưới dạng chuỗi, hàm sử dụng hàm getPrivateKey() để chuyển đổi chuỗi khóa riêng thành đối tượng PrivateKey có thể sử dụng được.
  + Hàm initSign() sẽ khởi tạo đối tượng Signature với khóa riêng đã truyền vào, và hàm update() sẽ cập nhật chữ ký với giá trị băm md vừa tính toán.
  + Sau đó, hàm sign() được gọi để hoàn thành quá trình ký và mã hóa dữ liệu, và trả về chữ ký dưới dạng mảng byte.
  + Trả về chữ ký dưới dạng chuỗi base64: Cuối cùng, hàm trả về chuỗi chữ ký đã được mã hóa dưới dạng chuỗi base64 sử dụng lớp Base64 của Java.

- Hiện thực hàm kiểm tra dữ liệu và xác thực cho chữ ký số 

-Giải thích :

- Tính toán giá trị băm của file đầu vào bằng thuật toán SHA-256. Đọc nội dung của file chữ ký được tạo trước đó và giải mã nó bằng Base64 để lấy được chữ ký dưới dạng mảng byte.

- Đọc khóa công khai từ chuỗi khóa công khai đầu vào. Sử dụng khóa công khai để xác thực tính hợp lệ của chữ ký bằng cách sử dụng đối tượng Signature.

- Trả về kết quả xác thực của chữ ký, đó có thể là True (hợp lệ) hoặc False (không hợp lệ).

**TÀI LIỆU THAM KHẢO**

**Tiếng Việt**

**Tiếng Anh**