ISSN 2354-0575

ỨNG DỤNG MÃ HÓA VÀ CHỮ KÝ SỐ TRONG TRAO ĐỔI VĂN BẢN

Phạm Xuân Đạo[1], **Lê Văn Vịnh**[2], **Nguyễn Gia Ba**[2]
1 Trường Cao đẳng Kinh tế - Kỹ thuật Điện Biên
2 Trường Đại học Sư phạm Kỹ thuật Hưng Yên

Ngày nhận: 10/01/2017
Ngày sửa chữa: 20/02/2017
Ngày xét duyệt: 02/03/2017

Tóm tắt:

Trong các giao dịch điện tử (Chính phủ điện tử, Thương mại điện tử,...), chữ ký số được sử dụng nhằm đáp ứng yêu cầu chứng thực về nguồn gốc và tính toàn vẹn của thông tin. Hiện nay chữ ký số đã được ứng dụng rộng rãi trong các lĩnh vực Chính phủ điện tử, Thương mại điện tử,... trên thế giới cũng như đã bước đầu được triển khai ở Việt Nam. Do đó, việc nghiên cứu ứng dụng mã hóa và chữ ký số trong trao đổi văn bản dùng trong các cơ quan cấp nhà nước và các cấp là rất cần thiết.

Từ khóa: *Chữ ký số, ứng dụng chữ ký số trong văn bản.*

1. Đặt vấn đề

Với sự phát triển mạnh mẽ của CNTT và mạng Internet hiện nay đã làm thay đổi căn bản các hoạt động trong đời sống xã hội. Trong đó, việc ứng dụng chữ ký số, chữ ký điện tử trong các cơ quan nhà nước là nhu cầu cần thiết trong các giao dịch trên môi trường mạng, nhằm phục vụ công tác cải cách hành chính, từng bước xây dựng chính quyền điện tử. Bên cạnh đó, việc triển khai ứng dụng chữ ký số, chứng thực số có hiệu quả còn đảm bảo an toàn tin cậy cho các giao dịch điện tử phục vụ hoạt động chỉ đạo, điều hành, tác nghiệp của các cơ quan nhà nước.

Chữ ký số là thông tin đi kèm theo tài liệu để xác định người chủ của tài liệu. Hiện tại, chữ ký số khóa công khai kiểu RSA đang được sử dụng khá rộng rãi. Đây 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 số cũng như trao đổi các thông tin mật. Người sử dụng có thể tự sinh ra hoặc yêu cầu một tổ chức có uy tín được nhà nước giao trách nhiệm cung cấp cặp khóa này. Quá trình sử dụng chữ ký số bao gồm 2 giai đoạn, tạo chữ ký và kiểm tra chữ ký.

Để tạo ra chữ kí cho một tài liệu, người sử dụng dùng một hàm băm để trích rút đặc trưng ngắn gọn của tài liệu. Đặc trưng này được gọi là bản tóm lược. Sau đó, người sử dụng dùng khóa bí mật của mình để mã hóa bản tóm lược này và gửi kèm theo tài liệu cho người nhận. Để kiểm tra chữ ký số, bên nhận dùng khóa công khai của người gửi để giải mã ra bản tóm lược đã mã hóa. Sau đó, người nhận lại tự mình băm tài liệu đính kèm để lấy bản tóm lược rồi so với bản tóm lược vừa giải mã. Nếu hai bản này bằng nhau thì bên nhận có thể tin tưởng rằng văn bản đó là do người sở hữu khóa công khai sinh ra và đã ký vào nó.

Tuy vậy, việc ứng dụng chữ kí số trong trao đổi văn bản dùng trong cơ quan cấp tỉnh hiện đang triển khai sử dụng phần mềm để trao đổi, tuy nhiên phần mềm sử dụng chưa đơn giản và thuận tiện cho người sử dụng.

Với lý do trên, bài báo nghiên cứu phát triển ứng dụng mã hóa và chữ kí số trong trao đổi văn bản có ý nghĩa rất quan trọng cả về lý thuyết và thực tiễn.

2. Đối tượng và phương pháp nghiên cứu

Đối tượng nghiên cứu:

- Sử dụng hệ thống chữ ký số để chuyển các giao dịch hành chính từ dạng cổ điển sang dạng điện tử.
- Nghiên cứu giải pháp xây dựng và phát triển chữ ký số để sử dụng trong các hoạt động hành chính ở cấp tỉnh.

Phương pháp nghiên cứu:

- Xác định các yêu cầu về mật hóa và xác thực thông tin
- Nghiên cứu về mật hóa, khóa công khai, chữ ký số
- Đề xuất giải pháp sử dụng chữ ký số trong các cơ quan hành chính
- Phân tích và thiết kế phần mềm thử nghiệm hệ thống chữ ký số ở các cơ quan cấp tỉnh.
- Phân tích tổng hợp mô hình hóa thử nghiệm, thực nghiệm.

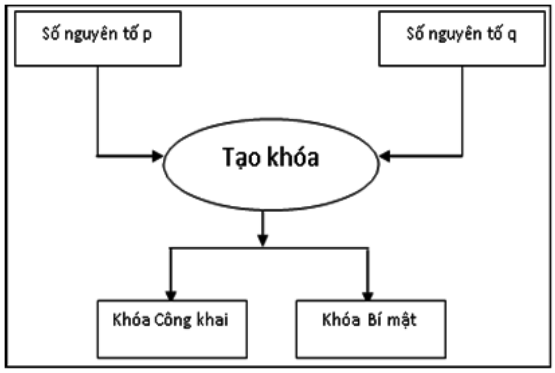
3. Các kết quả

3.1 Tạo khóa

Nhiệm vụ của là tạo ra cặp khóa bí mật - công khai cho người dùng từ hai số nguyên tố đã chọn trước.

Mỗi người sử dụng phải có một cặp khóa: Khóa bí mật dùng để ký, để giải mã thông tin nhận được và một khóa công khai tương ứng để người

khác dùng trong xác minh chữ ký và mã hóa văn bản gửi đến, khóa công khai được thông báo rộng rãi, khóa bí mật được người sử dụng lưu giữ bí mật. Quá trình tạo khóa được mô phỏng như Hình 1.



Hình 1. *Sơ đồ quá trình tạo khóa và các bước được thực hiện*

Các bước thực hiện như sau:

Bước 1: Chọn 2 số nguyên tố p và q đủ lớn.

Bước 2: Tạo cặp khóa công khai và bí mật:

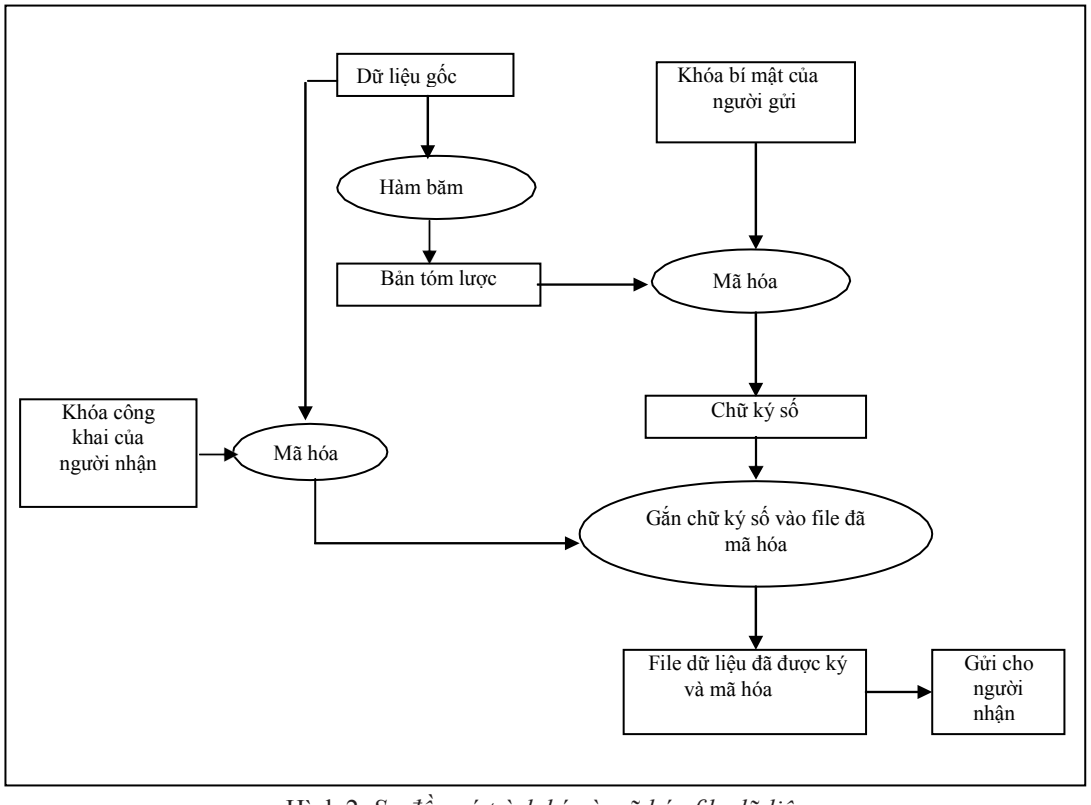
- Đặt N = p * q và n = (p-1)*(q-1)
- Chọn một số tự nhiên *e* sao cho 1 < *e* < n và nguyên tố cùng nhau với n tức là GCD(e, n) = 1.
- Tìm số tự nhiên d thỏa mãn điều kiện 1 < d < n và e*d mod n = 1. Nghĩa là d là nghịch đảo của e theo modulo n. Để tìm d có thể sử dụng thuật toán Euclid mở rộng.
- Xóa p, q và n và lấy khóa công khai là (e, n) và khóa bí mật (riêng) là (d, n).

Bước 3: Lưu khóa công khai với tên file là Keypublic.txt và khóa bí mật với tên file là Keyprivate.txt. Công bố khóa công khai và giữ bí mật khóa riêng.

3.2. Ký và mã hóa tài liệu

Để có thể trao đổi các văn bản số có chữ ký và những văn bản mật giữa những người có nhu cầu thì những người này đều phải có cặp khóa của riêng mình. Khi một người muốn gửi cho ai đó một văn bản quan trọng, đòi hỏi phải được ký xác nhận chính danh người gửi và nếu muốn giữ bí mật thì phải thực hiện mã hóa file tài liệu cần gửi. Người gửi sẽ thực hiện ký và mã hóa văn bản đã ký. Quy trình ký và mã hóa được mô phỏng như Hình 2.

Quy trình này sẽ tạo ra một file chữ ký (DigitalSignature.txt), gồm chữ ký và file tài liệu đã được mã hóa.



Hình 2. *Sơ đồ quá trình ký và mã hóa file dữ liệu*

Các Bước thực hiện như sau:

Bước 1:

- Chọn khóa công khai của người nhận
- Chọn khóa bí mật của người gửi
- Chọn file tài liệu để mã hóa và ký

Bước 2: Dùng hàm SHA-1 băm file tài liệu

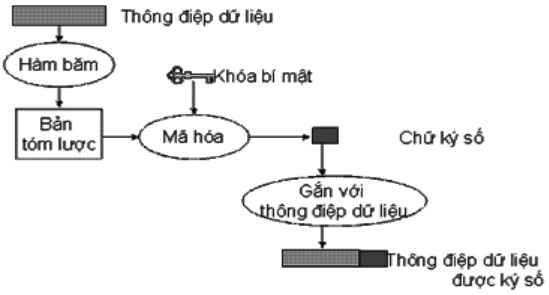
đã chọn để thu được bản tóm lược. Sử dụng thuật toán RSA với khóa bí mật của người gửi mã hóa bản tóm lược để có chữ ký số.

Bước 3: Mã hóa file tài liệu bằng thuật toán RSA với khóa công khai của người nhận.

Bước 4: Gộp chữ ký số vào bản tin đã mã hóa.

Bước 5: Gửi file đã gộp cho người nhận.

Quy trình tạo chữ kí số được mô phỏng trong Hình 3

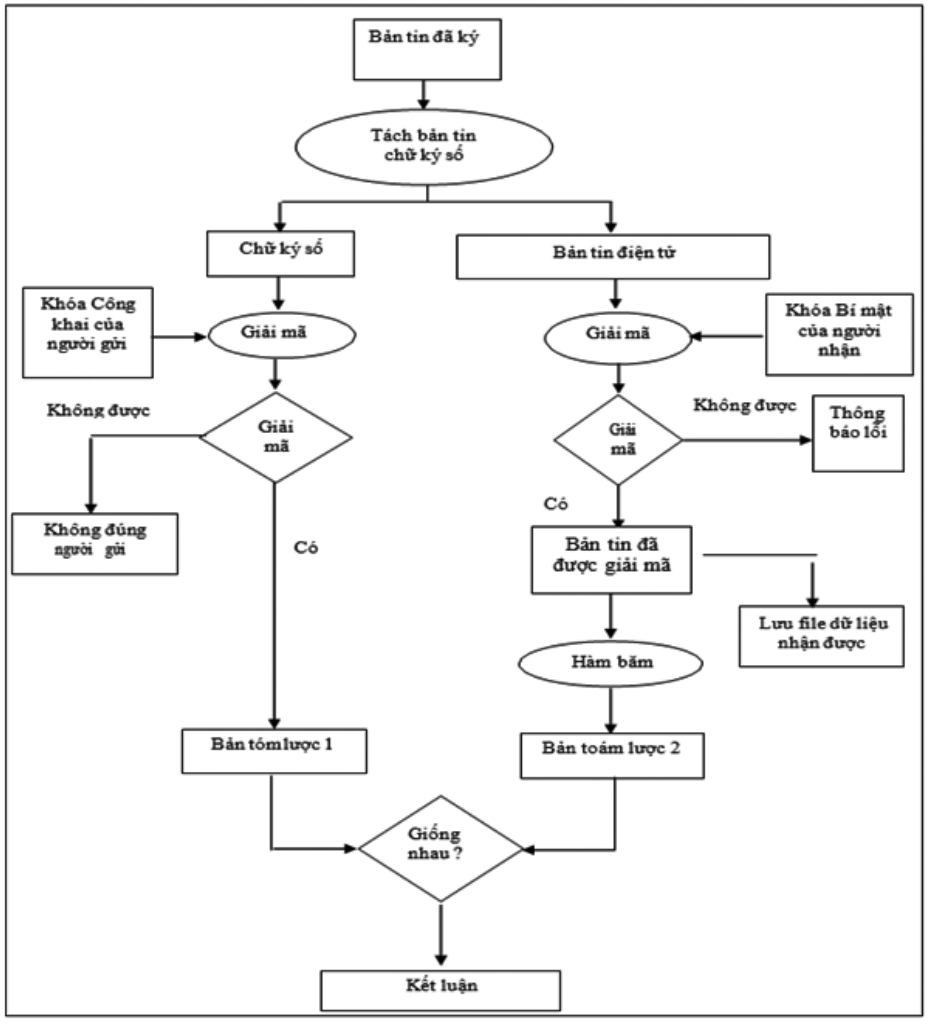


Hình 3. *Quy trình tạo chữ ký số*

3.3. Giải mã và xác thực chữ ký

Nhiệm vụ của modul này chính là kiểm tra tính đúng đắn của chữ ký số, đồng thời giải mã file dữ liệu nhận được để thu được bản tin ban đầu.

Sau khi nhận được một file dữ liệu nào đó có đính kèm chữ ký của người gửi, người nhận phải giải mã file dữ liệu này để thu được bản tin ban đầu và xác thực chữ ký đính kèm có đúng của người gửi đã biết trước. Quy trình xác thực chữ ký và giải mã được thể hiện ở Hình 4.



Hình 4. *Sơ đồ quá trình giải mã và xác thực chữ ký*

Các Bước thực hiện như sau:

Bước 1:

- Chọn khóa công khai của người gửi
- Chọn khóa bí mật của người nhận
- Chọn file cần giải mã và xác thực chữ ký

Bước 2: Bản tin điện tử có đính kèm chữ ký của người gửi, sau khi nhận được sẽ tách riêng phần chữ ký và phần văn bản (đã được mã hoá)

Bước 3: Dùng khóa công khai (public key) của người gửi để giải mã chữ ký số của thông điệp, kết quả thu được bản tóm lược 1 (nếu không giải mã được thông báo "không đúng người gửi")

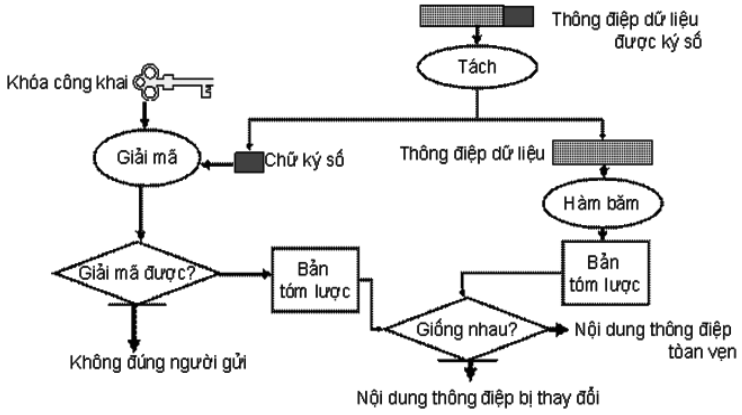
Bước 4: Người nhận dùng khoá bí mật của mình để giải mã phần văn bản đã được mã hoá, kết quả thu được bản tin điện tử ban đầu và lưu dưới dạng file txt (nếu không giải mã được thông báo lỗi).

Bước 5: Xác nhận chữ ký bằng cách sau:

Bước 5.1: Dùng giải thuật băm SHA-1 để mã hóa văn bản thu được ở Bước 4, kết quả thu được là bản tin tóm lược thứ 2.

Bước 5.2: So sánh 2 bản tin tóm lược thu được ở Bước 3 và Bước 5.1, ta kết luận thông điệp này là của người gửi (nếu không giống nhau kết luận không đúng người gửi).

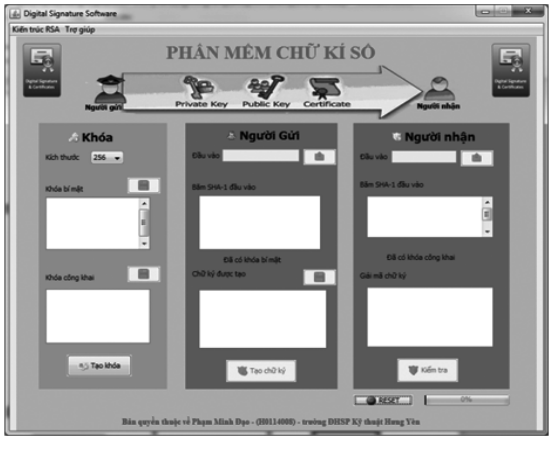
Quy trình thẩm định chữ kí số được mô phỏng trong Hình 5



Hình 5. *Quy trình thẩm định chữ ký số*

3.4. Giao diện và số chức năng chính của chương trình

Màn hình giao diện của chương trình

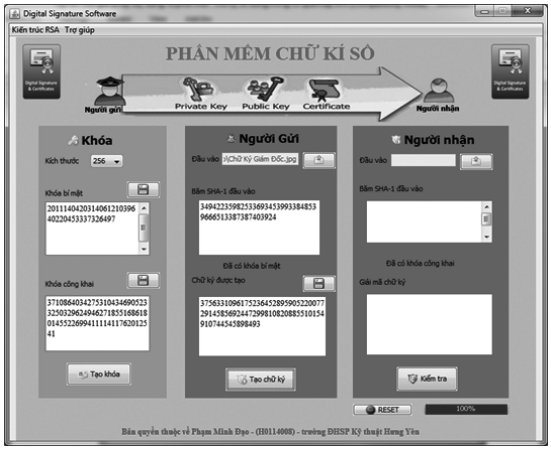


Hình 6. *Giao diện chương trình chính*

Chọn 2 số nguyên tố p và q, người sử dụng chọn **Khóa công khai** và **Khóa bí mật** để tạo khóa công khai và khóa bí mật, đặt tên cho 2 cặp khóa này, chương trình được lưu trữ bằng đường dẫn của người dùng lựa chọn cộng với tên file mặc định là Keyprivate.txt đối với khóa bí mật, Keypublic.txt đối với khóa công khai. Người sử dụng công bố khóa công khai và lưu giữ khóa bí mật vừa tạo được.

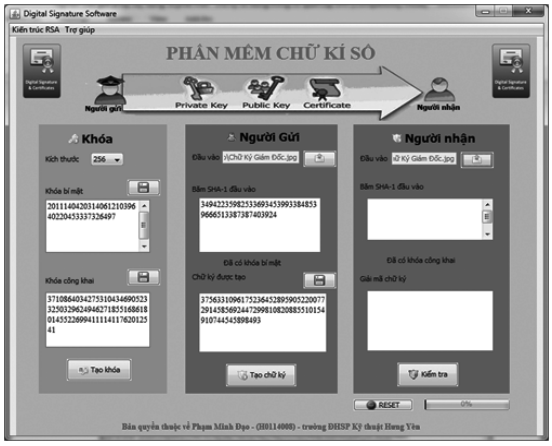
Tạo chữ ký cho file tài liệu (Người gửi)

Người gửi chọn khóa bí mật của mình để thực hiện ký và chọn khóa công khai của người nhận để thực hiện mã hóa, sau đó chọn **Kí tên**, kết quả thu được file dữ liệu đã được ký và mã hóa.



Hình 7. *Giao diện màn hình thực hiện mã hóa và ký*

Mở văn bản (Người nhận)

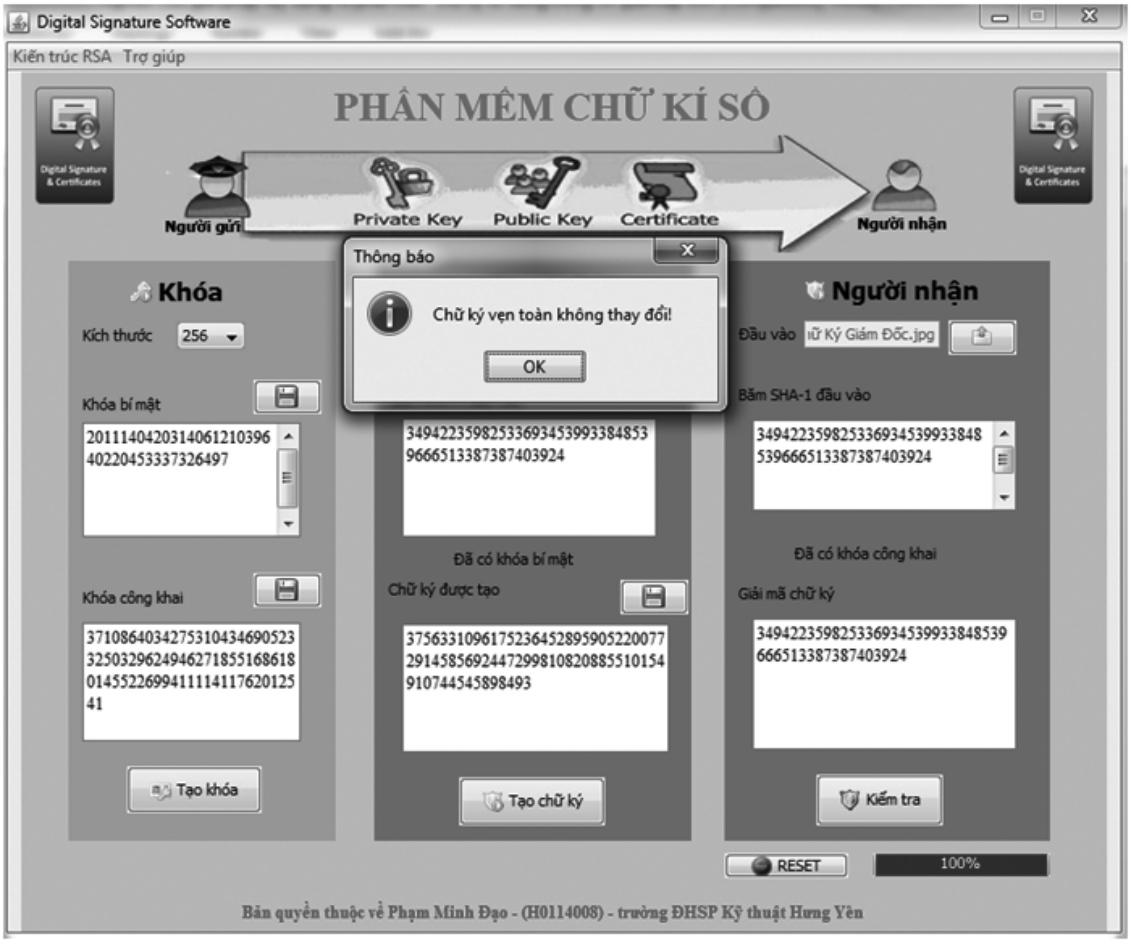


Hình 8. *Giao màn hình thực hiện mở văn bản*

Thực hiện việc mở văn bản bằng cách: file dữ liệu đã được ký và mã hóa có tên là DigitalSignature.txt trong thư mục người dùng chọn.

Kiểm tra (Giải khóa)

Tiến hành giải mã và xác thực chữ ký số. Người sử dụng chọn khóa công khai của người gửi để xác minh chữ ký và chọn khóa bí mật của mình để giải mã file dữ liệu nhận được, chọn **Kiểm tra**, chọn file dữ liệu cần giải mã và xác minh chữ ký, chương trình sẽ thông báo kết quả sau khi thực hiện.



Hình 9. *Giao diện màn hình thực hiện giải mã và xác minh chữ ký*

4. Kết luận

Bài báo đã đưa ra được sơ đồ tạo khóa, tạo chữ ký, giải mã và xác thực chữ ký và các bước thực hiện và phát triển ứng dụng bằng ngôn ngữ Java được cài đặt trên hệ mã RSA trong việc xây dựng lược đồ chữ ký số và cài đặt ứng dụng chữ ký số trong trao đổi văn bản vì có nhiều ưu điểm và đang được ứng dụng rộng rãi hiện nay.

Tài liệu tham khảo

[1]. Phan Đình Diệu (202), *Lý thuyết mật mã và an toàn thông tin*, NXB Đại học Quốc gia Hà Nội.
[2]. Phạm Huy Điển, Hà Huy Khoái (2004), *Mã hoá thông tin – cơ sở toán học và ứng dụng*, NXB Đại học Quốc gia Hà Nội.
[3]. Bùi Doãn Khanh, Nguyễn Đình Thúc (2004), *Mã hóa thông tin Lý thuyết và ứng dụng*, NXB Lao động.
[4]. Bùi Thế Hồng (2016), *Bảo mật máy tính và mạng*, Bộ môn Mạng và Truyền thông, Khoa CNTT, ĐH SP KT HY.
[5]. R. Rivest, A, sharmir, L. Adleman (1978), *A Method for Obtaining Digital Signatres and Public-key Cryptosystems*, Communication of theo ACM 21, pp. 120 – 126.
[6]. E. Biham, A. Shamir (1993), *Differential Cryptanalysis of the Data Encryption Standard*, Springer- Verlag.
[7]. Daniel Genkin, Yuval Ishai, Manoj Prabhakaran, Amit Sahai, and Eran Tromer (2015). *Circuits Resilient to Additive Attacks with Applications to Securecomputation*. IACR Cryptology ePrint Archive, 2015, pp. 154.

THE APPLICATION OF CODING AND DIGITAL SIGNATURES IN EXCHANGE OF DOCUMENTS

Abstract:
In the electronic trading (e-Government, e-Commerce,..), digital signatures are used to meet the request for authentication of the origin and integrity of information. Currently, digital signatures have been widely applied in the fields of e-Government, e-Commerce,... in the world as well as had initially been implemented in Vietnam. Therefore, the research of application of encryption and digital signatures used in the exchange of documents in the provincial authorities is much needed.
Keywords: *Digital signature, digital signature applications.*