TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI

VIỆN ĐIỆN TỬ - VIỄN THÔNG

BÁO CÁO BÀI TẬP LỚN
LÝ THUYẾT MẬT MÃ

Đề tài:

ỨNG DỤNG HỆ MẬT ELGAMAL TRONG MÃ HÓA VÀ TẠO CHỮ KÝ SỐ

Nhóm thực hiện: Nhóm 14

Mã lớp: 105181

Lương Văn Mạnh	MSSV: 20162645
Lê Viết Khánh	MSSV: 20162137
Trịnh Quốc Cường	MSSV: 20160590
Nguyễn Văn Thuận	MSSV: 20163958

Giảng viên hướng dẫn: TS. Hán Trọng Thanh

Hà Nội, tháng 05 năm 2019

MỤC LỤC

DANH MỤC HÌNH ẢNH

DANH SÁCH BẢNG BIỂU

NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN

……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……

Ngày tháng năm

Giảng viên hướng dẫn

LỜI MỞ ĐẦU

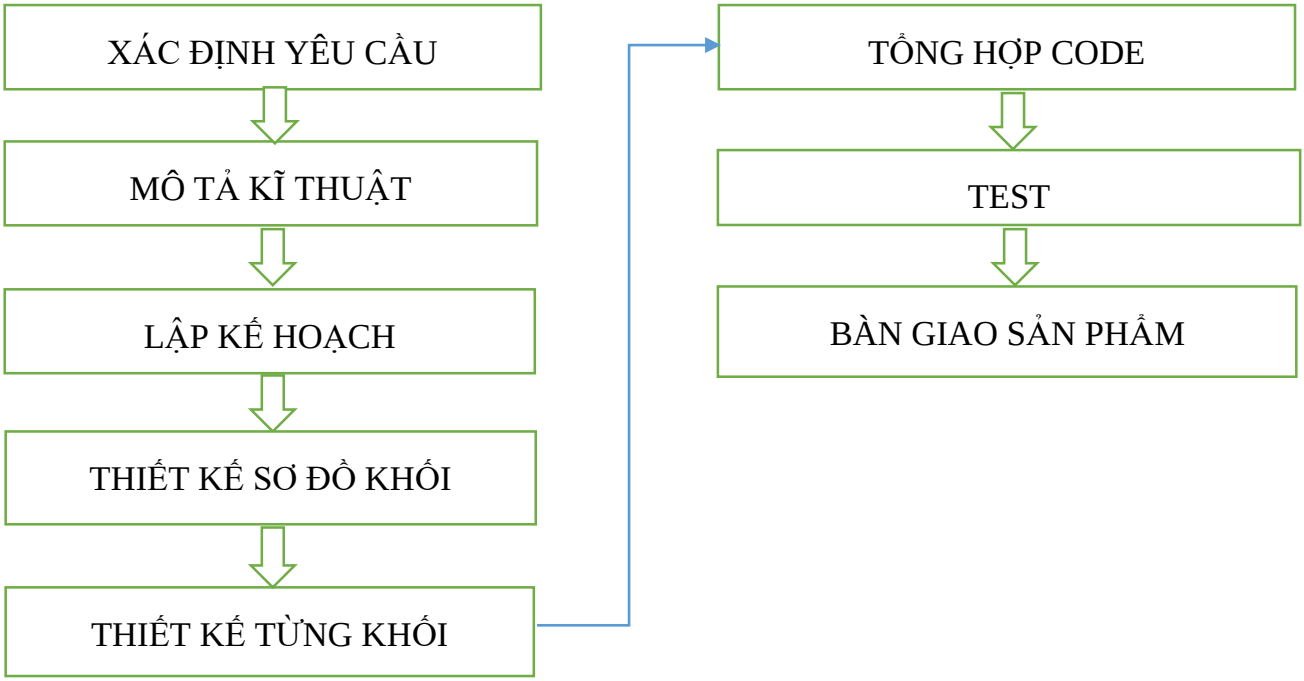
Trong mọi thời đại xã hội loài người, vấn đề bảo mật thông tin luôn được quan tâm lớn. Từ xa xưa, con người đã sáng tạo ra các hệ mật mã cổ điển để đáp ứng nhu cầu bảo mật thông tin. Mật mã học là một ngành có lịch sử từ hàng nghìn năm nay. Trong phần lớn thời gian phát triển của mình (ngoại trừ vài thập kỷ trở lại đây), lịch sử mật mã học chính là lịch sử của những phương pháp mật mã học cổ điển - các phương pháp mật mã hóa với bút và giấy, đôi khi có hỗ trợ từ những dụng cụ cơ khí đơn giản.

Vào đầu thế kỷ 20, sự xuất hiện của các cơ cấu cơ khí và điện cơ, chẳng hạn như máy Enigma, đã cung cấp những cơ chế phức tạp và hiệu quả hơn cho việc mật mã hóa. Sự ra đời và phát triển mạnh mẽ của ngành điện tử và máy tính trong những thập kỷ gần đây đã tạo điều kiện để mật mã học phát triển nhảy vọt lên một tầm cao mới. Rất nhiều hệ mật mã hiện đại đã lần lượt ra đời dựa trên cơ sở đại số Modulo và các thuật toán logarithm rời rạc… Năm 1975, IBM công bố Hệ mật DES, khởi đầu cho các hệ mật mã hiện đại. Tiếp theo đó là sự ra đời của các hệ mật mã AES, RSA, DSA, Elgamal… Hệ mật Elgamal được đề xuất vào năm 1984 trên cơ sở của bài toàn Logarit rời rạc, là một hệ mật mã rất khó thám mã.

Dựa trên sự hướng dẫn của thầy, các thành viên trong nhóm đã tiến hành tìm hiểu về các thuật toán thám mã và giải mã hệ mật mã hóa Elgamal, nhóm tiến hành xây dựng mô phỏng hệ mật Elgamal trên phần mềm Matlab. Báo cáo cũng như phần mô phỏng của nhóm sẽ không tránh khỏi những thiếu sót, rất mong được sự góp ý chỉ dẫn của thầy!

NỘI DUNG

1 Quy trình kỹ thuật



Hình 1. 1 Quy trình kỹ thuật

2 Xác định yêu cầu

2.1 Yêu cầu phi chức năng

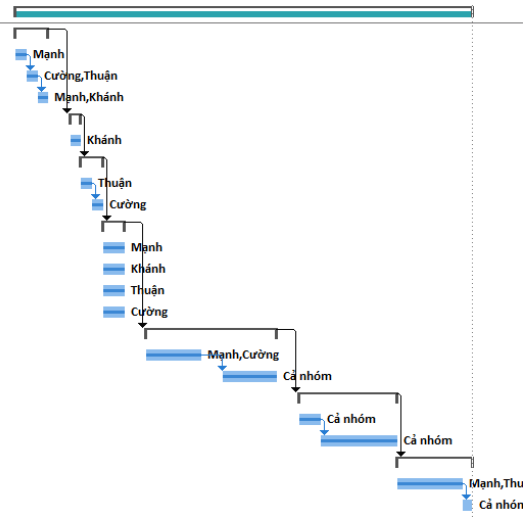
- Có lập trình giao diện
- Có chức năng tự chọn khóa, và tự động chọn khóa
- Có chức năng tạo mới

2.2 Yêu cầu chức năng

- Lập mã và giải mã một bản tin rõ
- Có ứng dụng vào chữ ký số: kiểm tra tính toàn vẹn của thông tin

3 Lập kế hoạch

Hệ mật ELGAMAL	**30 days**	**Wed 03-04-19**	**Tue 14-05-19**	
1. Khái quát hệ mật	**3 days**	**Wed 03-04-19**	**Fri 05-04-19**	
Tổng quan	1 day	Wed 03-04-19	Wed 03-04-19	Mạnh
Mô tả giải thuật	1 day	Thu 04-04-19	Thu 04-04-19	Cường,Thuận
Tính bảo mật	1 day	Fri 05-04-19	Fri 05-04-19	Mạnh,Khánh
2. Lập kế hoạch	**1 day**	**Mon 08-04-19**	**Mon 08-04-19**	
Bảng phân công công việc	1 day	Mon 08-04-19	Mon 08-04-19	Khánh
3. Thiết kế sơ đồ khối	**2 days**	**Tue 09-04-19**	**Wed 10-04-19**	
Xác định các khối	1 day	Tue 09-04-19	Tue 09-04-19	Thuận
Xác định quan hệ các khối	1 day	Wed 10-04-19	Wed 10-04-19	Cường
4. Thiết kế từng khối	**2 days**	**Thu 11-04-19**	**Fri 12-04-19**	
Khối tạo khóa	2 days	Thu 11-04-19	Fri 12-04-19	Mạnh
Khối mã khóa	2 days	Thu 11-04-19	Fri 12-04-19	Khánh
Khối giải mã	2 days	Thu 11-04-19	Fri 12-04-19	Thuận
Khối tạo chữ ký số	2 days	Thu 11-04-19	Fri 12-04-19	Cường
5. Xây dựng phần mềm	**10 days**	**Mon 15-04-19**	**Fri 26-04-19**	
Thiết kế giao diện	5 days	Mon 15-04-19	Fri 19-04-19	Mạnh,Cường
Xây dựng các chức năng	5 days	Mon 22-04-19	Fri 26-04-19	Cả nhóm
6. Test	**7 days**	**Mon 29-04-19**	**Tue 07-05-19**	
Test phần mềm	2 days	Mon 29-04-19	Tue 30-04-19	Cả nhóm
Phản hồi và đóng góp	5 days	Wed 01-05-19	Tue 07-05-19	Cả nhóm
7. Bảo vệ	**5 days**	**Wed 08-05-19**	**Tue 14-05-19**	
Hoàn thành báo cáo	4 days	Wed 08-05-19	Mon 13-05-19	Mạnh,Thuận
Bảo vệ báo cáo	1 day	Tue 14-05-19	Tue 14-05-19	Cả nhóm



Hình 3. 1 Lập kế hoạch

4 Mô tả kĩ thuật

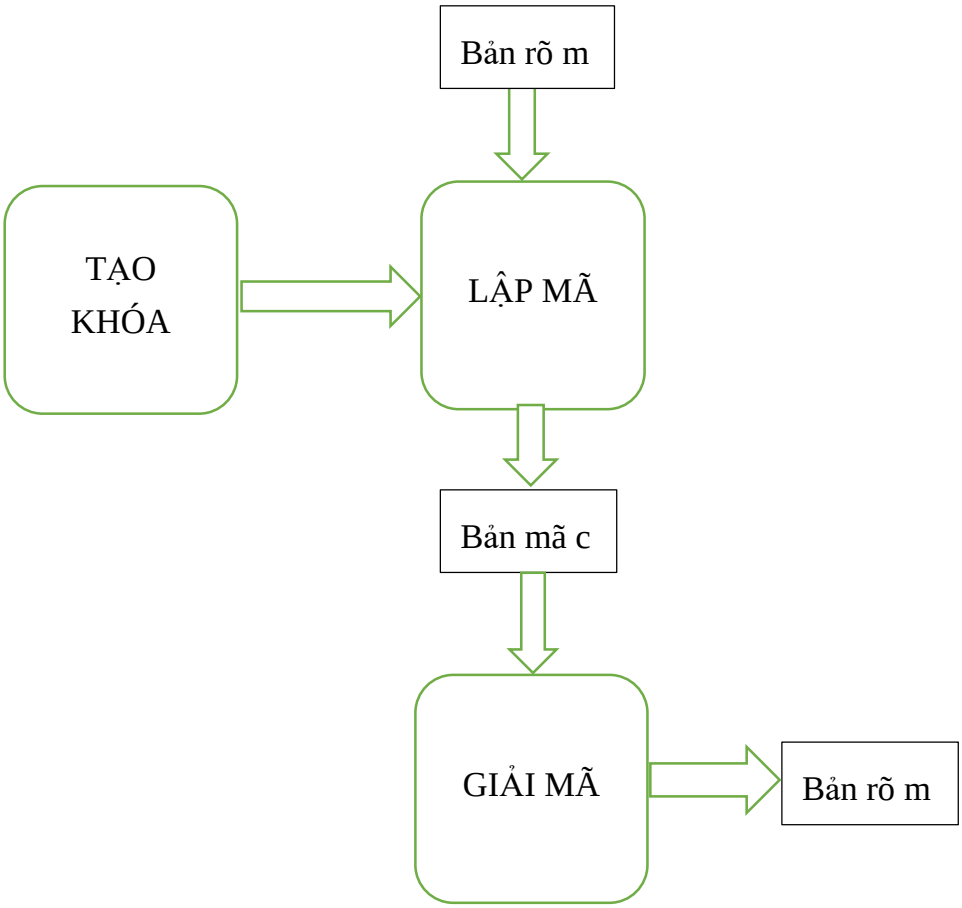
4.1 Hệ mật Elgamal

4.1.1 Tổng quan

Hệ mật ElGamal là một hệ mật khóa bất đối xứng cho khóa công khai, dựa trên trao đổi khóa Diffie – Hellan. Thuật toán do Taher Elgamal tạo ra vào năm 1985 lấy mô hình bài toán logarit rời rạc.

Thuật toán ElGamal có hai khóa: Public key (khóa công khai) và Private key (khóa bí mật). Public key sẽ được công bố và mọi người đều có thể mã hóa bản tin Nhưng chỉ có Pravate key mới cả thể giải mã.

4.1.2 Thiết kế sơ đồ khối

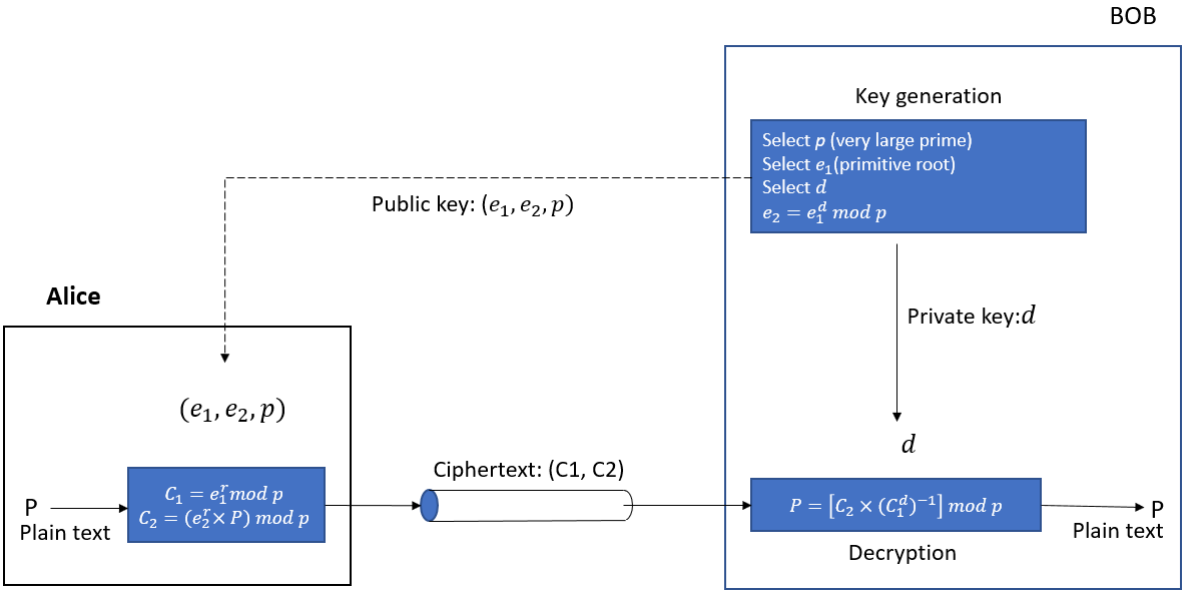


Hình 4. 1 Sơ đồ khối

4.1.3 Mô tả

Cách làm việc của giải thuật này khi áp dụng thuật toán là khi mã hóa một bản tin bất kì, Alice tạo ra một số ngẫu nhiên kết hợp với bản rõ để tạo ra bản mã. Sau đó Alice truyền bản mã cho Bob, để giải mã Bob cần có khóa bí mật để giải mã bản tin.

Giả sử Bob nhận được bản tin được mã hóa như hình:



Hình 4. 2 Mô hình hệ mật Elgamal

4.1.4 Tạo khóa

Để Alice và Bob có thể trao đổi thông tin với nhau bằng thuật toán mã Elgamal thì cần phải tạo khóa trước tiên:

1. Chọn số nguyên tố p đủ lớn sao cho bài toán logarit trong Z_p là khó giải.
2. Chọn một số d thuộc nhóm $G = < Z_p^*, \times >$ sao cho $1 \leq d \leq p - 2$

   Chọn e_1 là phần tủ nguyên tử của nhóm $G = < Z_p^*, \times >$
3. Tính $e_2 = e_1^d \ mod \ p$
4. Khóa công khai sẽ là $(e_1, \ e_2, \ p)$

   Khóa bị mật sẽ là d.

4.1.5 Mã hóa

Giả sử Alice gửi một bản tin M cho Bob, khi đó Alice sẽ thực hiện các bước:

1. Chọn một số nguyên ngẫu nhiên r nằm trong nhóm $G = < Z_p^*, \times >$

   Khí đó tính được bản mật $C_1 = e_1^r \ mod \ p$
2. Sử dụng khóa công khai để tính bản mật $C_2 = (e_2^r \times P) \ mod \ p$
3. Alice sẽ có bản mã gồm (C_1, C_2) để gửi đến cho Bob.

4.1.6 Giải mã

Bob nhận được bản mã (C_1, C_2) và có khóa bị mật d khi đó Bob sẽ tìm được bản rõ theo công thức: $[C_2(C_1^d)^{-1}]\ mod\ p$.

4.1.7 Tính bảo mật của hệ mật mã Elgamal

Hệ mật ElGamal sẽ bị phá vỡ nếu khóa bị mật d hoặc r có thể tính được trong bài toán logarit rời rạc.

Tuy nhiên bài toán logarit rời rạc chưa có phương pháp tính hiệu quả nên độ an toàn của hệ mật là rất lớn, với một số p đủ lớn thì thuật toán ElGamal không có phương pháp thám mã hiệu quả.

4.1.8 Ưu điểm và nhược điểm của hệ mã Elgamal

- Ưu điểm:
    - Do được xây dựng từ bài toán logarit rời rạc, độ phức tạp của bài toán logarithm lớn nên có độ an toàn cao.
    - Bản mã phụ thuộc vào bản rõ và giá trị ngẫu nhiên nên từ một bản rõ ta có thể có nhiều bản mã khác nhau.
- Nhược điểm:
    - Tốc độ chậm (do phải xử lý số nguyên lớn).
    - Dung lượng bộ nhớ dành để lưu trữ các bản mã lớn gấp đôi so với các hệ mã khác.
    - Do việc sử dụng các số nguyên tố nên việc sinh khóa và quản lý khóa cũng khó khan hơn các hệ mã khối.

4.2 Ứng dụng chữ ký số

4.2.1 Chữ ký số

Chữ ký số là một dạng của chữ ký điện tử. Nó là một dạng dữ liệu dùng để chứng thực cho các dữ liệu khác.

Chữ ký số sử dụng một hệ mã hóa bất đối xứng. Trong phần lớn các trường hợp, nó còn có thể kiểm tra cả tính toàn vẹn của dữ liệu nữa. Chữ ký số tương tự như chữ ký tay trên nhiều phương diện, nhưng việc cài đặt và sử dụng chữ ký số khó khăn hơn rất nhiều.

4.2.2 Chữ ký số sử dụng hệ mật mã Elgamal

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

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

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

Các hàm hash là hàm 1 chiều, vì vậy dù có được hash cũng không thể biết được bản tin gốc như thế nào.

Độ dài hash là cố định và thường rất nhỏ, vì vậy chữ số sẽ không chiếm quá nhiều dung lượng.

Giá trị hash còn có thể dùng để kiểm tra lại bản tin nhận được có nguyên vẹn hay không?

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

4.2.3 Ưu điểm

- Khả năng nhận thực:

Các hệ thống mật mã khóa công khai cho phép mật mã hóa văn bản với khóa bí mật mà chỉ có người chủ của khóa biết. Để sử dụng chữ ký số thì văn bản không cần phải được mã hóa mà chỉ cần mã hóa hàm băm của văn bản đó. Khi cần kiểm tra, bên nhận giải mã để lấy lại hàm băm và kiểm tra với hàm băm của văn bản nhận được. Nếu hai giá trị này khớp nhau thì bên nhận có thể tin tưởng rằng văn bản xuất phát từ người sở hữu khóa bí mật. Tất nhiên là chúng ta không thể đảm bảo 100% là văn bản không bị giả mạo vì hệ thống vẫn có thể bị phá vỡ

- Tính toàn vẹn:

  Cả hai bên tham gia vào quá trình thông tin đều có thể tin tưởng là văn bản không bị sửa lỗi trong khi truyền vì nếu văn bản bị thay đổi thì hàm băm cũng thay đổi và lập tức bị phát hiện. Quá trình mã hóa sẽ ẩn nội dung của gói tin đối với bên thứ ba nhưng không ngăn cản được việc thay đổi nội dung của nó.

- Tính không thể phủ nhận:

  Trong giao dịch, một bên có thể từ chối nhận một văn bản nào đó do mình gửi. Để ngăn ngừa khả năng này, bên nhận có thể yêu cầu bên gửi phải gửi kèm chữ ký số và văn bản. Khi có tranh chấp, bên nhận sẽ dùng chữ ký này như một chứng cứ để bên thứ ba giải quyết. Tuy nhiên, khóa bí mật vẫn có thể bị lộ và tính không thể phủ nhận cũng không thể đạt được hoàn toàn.

4.2.4 Ý nghĩa

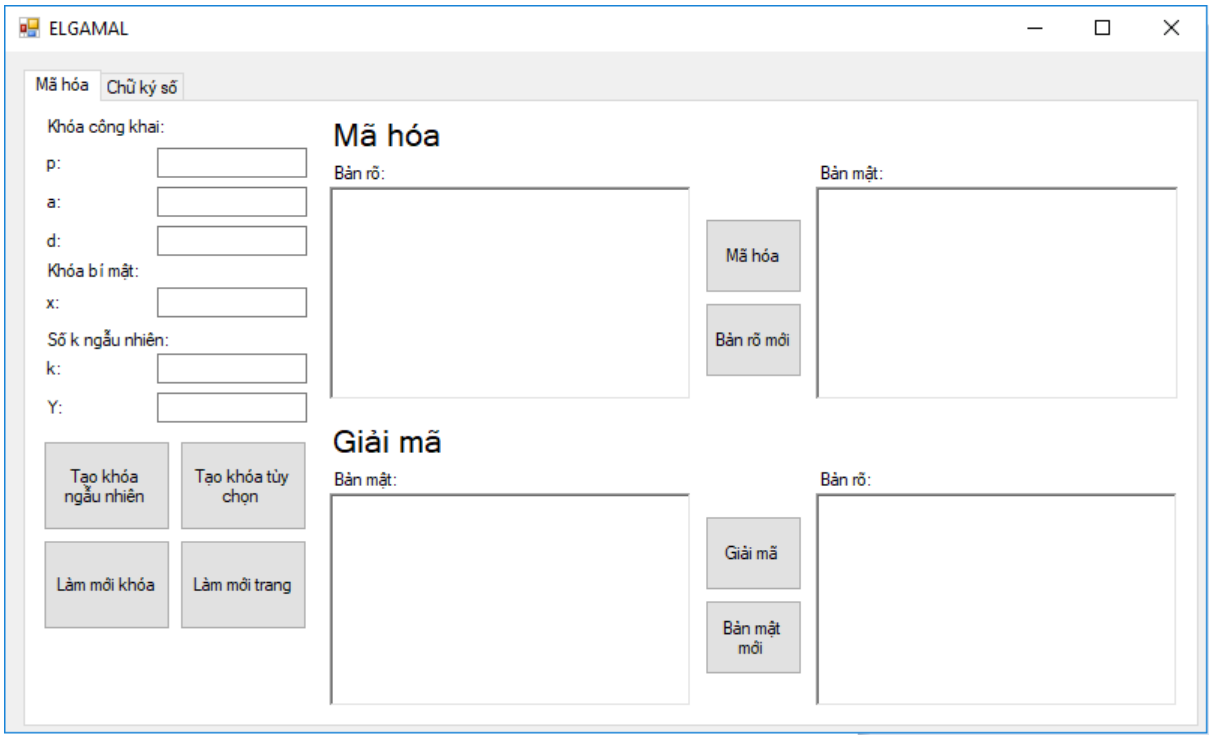
- Được sử dụng rộng rãi trong thương mại điện tử để thực hiện các giao dịch điện tử nhằm xác định rõ người kí văn bản
- Chống chối bỏ khi người ký đã ký vào văn bản thì họ không thể phủ nhận là chữ ký đó không phải của họ.
- Xác thực nội dung của văn bản ký: nhằm kiểm tra tính toàn vẹn của văn bản xem nó có bị thay đổi thông tin trong quá trình vận chuyển.
- Độ an toàn của chữ ký số rất là cao, hiện nay được sử dụng rất phổ biến trong giao dịch điện tử.

Để đảm bảo an toàn, và tăng hiệu quả của chữ ký số cần có các tổ chức chứng thực điện tử nhằm cung cấp và đảm bảo độ tin cậy cho chữ ký số. Đó là các tổ chức công an.

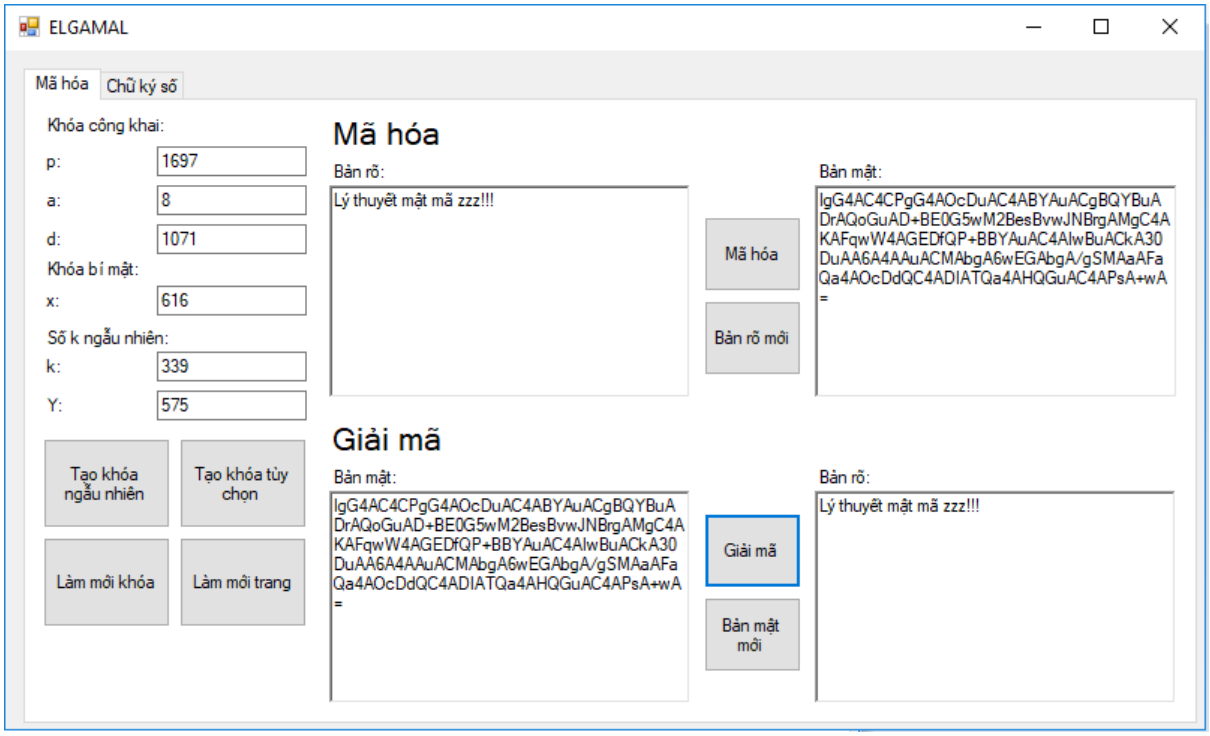
5 Tổng hợp code và demo kết quả

Phần mềm được xây dựng bằng ngôn ngữ lập trình C#, công cụ Visual Studio 2017.

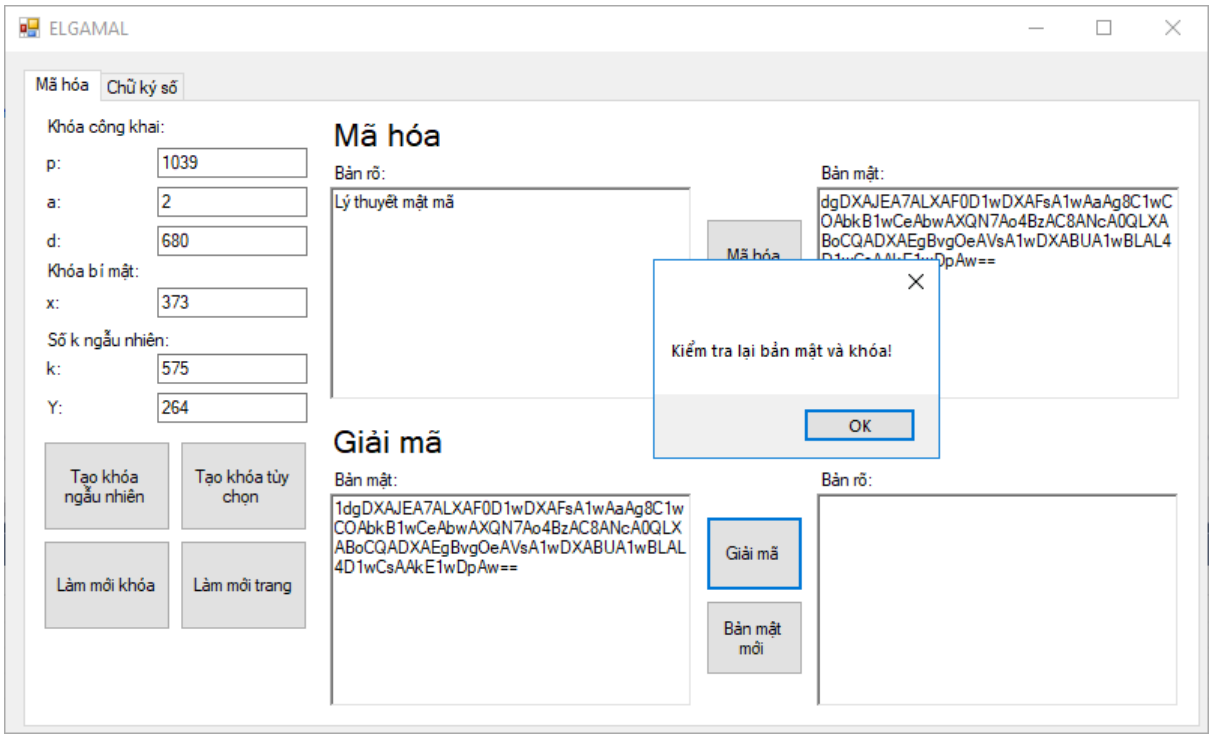
5.1 Mã hóa Elgamal



Hình 5. 1 Giao diện thực hiện chức năng mã hóa Elgamal

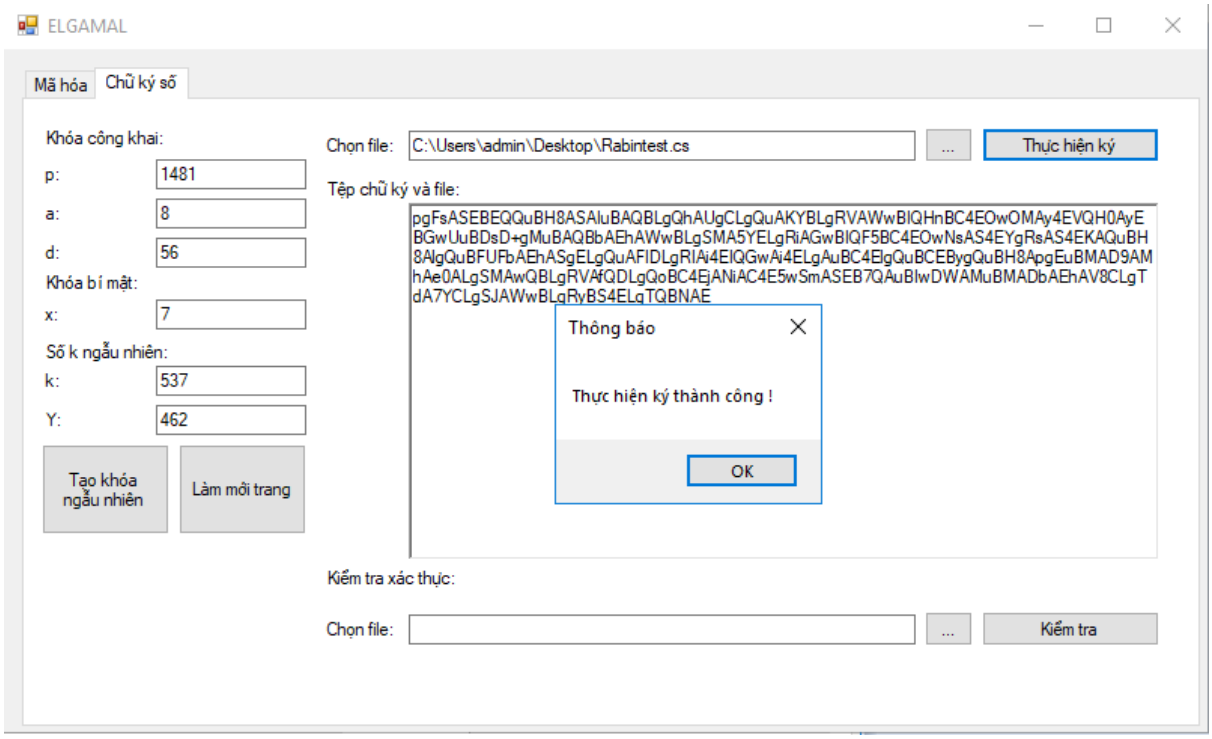


Hình 5. 2 Kết quả thử nghiệm chức năng mã hóa Elgamal

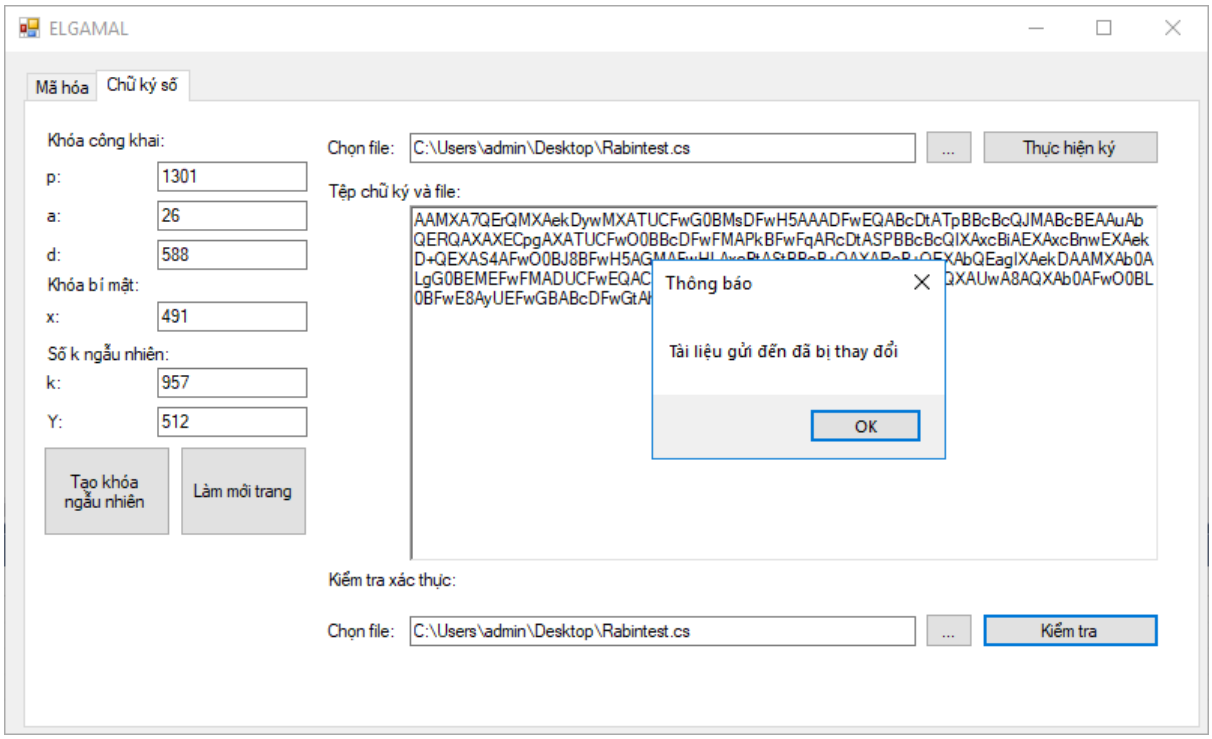


Hình 5. 3 Kiểm tra lại bản mật và khóa

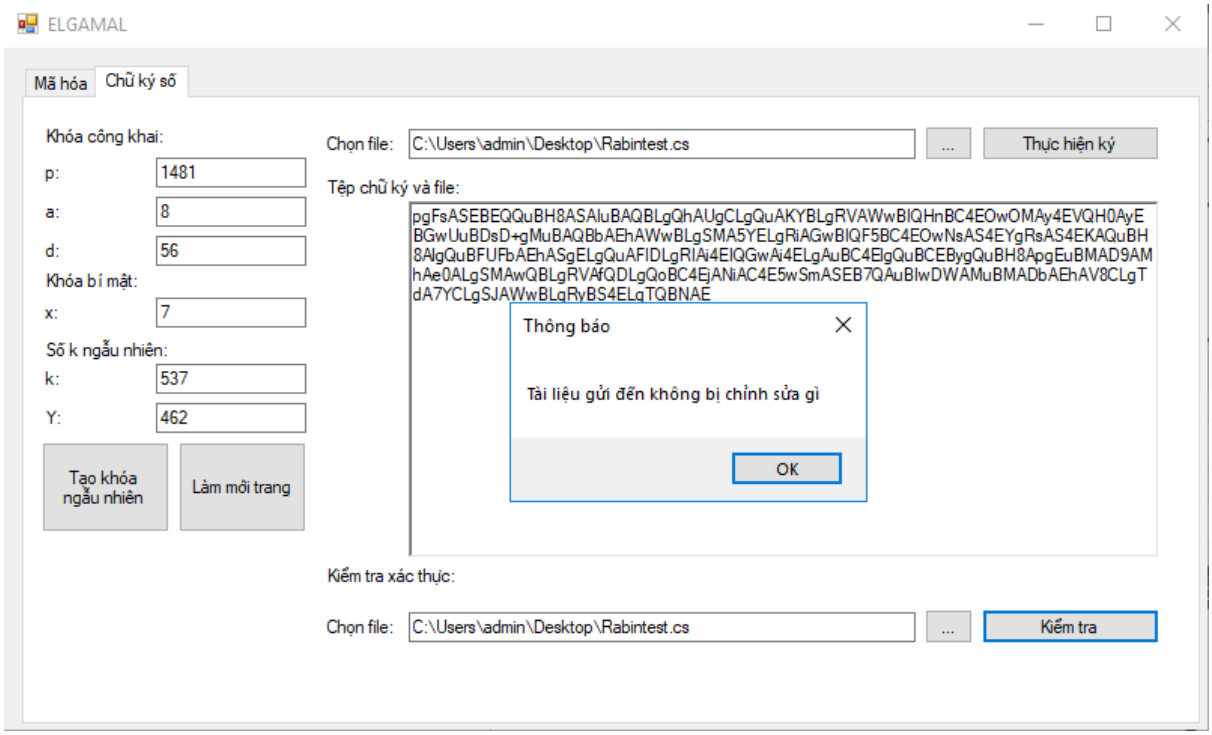
5.2 Tạo chữ ký số



Hình 5. 4 Giao diện thực hiện chức năng tạo chữ ký số



Hình 5. 5 Giao diện xác thực chữ ký số



Hình 5. 6 Kiểm tra tính toàn vẹn của tài liệu

KẾT LUẬN

Qua quá trình làm việc nhóm và làm project về hệ mật Elgamal, chúng em đã hiểu hơn về các bước, quy trình thiết kế một phần mềm. Hiểu hơn về lập trình giao diện. Chúng em đã tạo ra phần mềm giải thuật Elgamal và ứng dụng nó vào tạo chữ kí số tuy chưa hoàn chỉnh về nhiều mặt nhưng đó là những kinh nghiệm, kiến thức quy báu giúp cho chúng em hiểu rõ hơn về tính toàn vẹn của một tài liệu.

Chúng em xin cảm ơn **TS. Hán Trọng Thanh** đã giúp đỡ, giải đáp thắc mắc cho chúng em trong quá trình hoàn thành project. Chúng em xin chân thành cảm ơn thầy.

Nhóm 14

DANH MỤC TÀI LIỆU THAM KHẢO

[1] TS.Hán Trọng Thanh, *Giáo trình lý thuyết mật mã*.

[2] Wikipedia, *Elgamal encryption*.