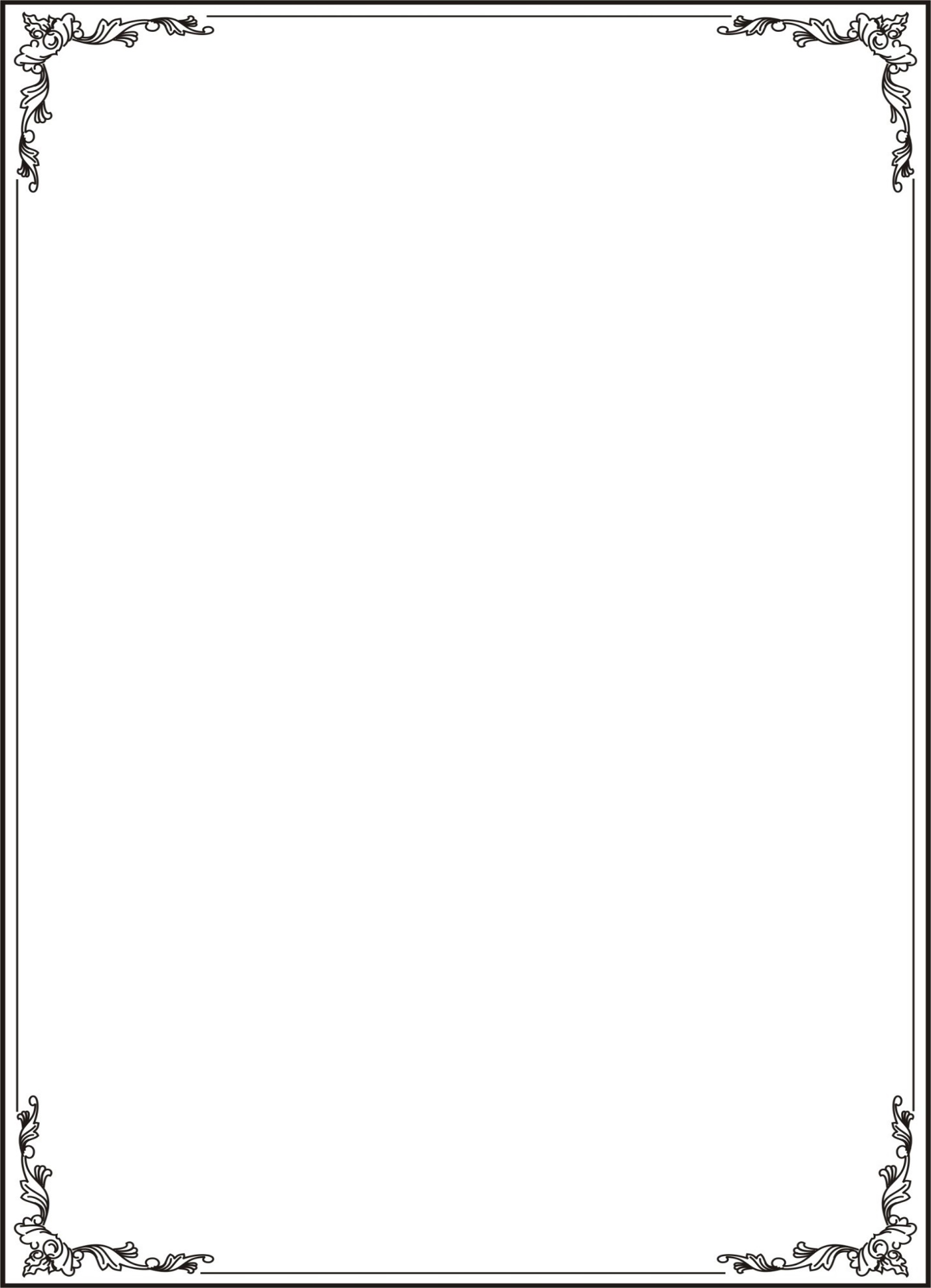
**BỘ CÔNG THƯƠNG**

**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**

∙∙∙🙞🙜🕮🙞🙜∙∙∙

****

**BÀI TẬP LỚN**

**MÔN HỌC: AN TOÀN BẢO MẬT THÔNG TIN**

**Đề tài: “Xây dựng chương trình mã hóa và giải mã Elgammal”**

**CBHD: ThS. Trần Phương Nhung**

**Nhóm: 6**

**Thành viên nhóm: Hoàng Trung Hiếu – 2020602568**

**Bùi Lê Hiếu – 2019605753**

**Nguyễn Huy Hoàng – 2019608191**

**Hoàng Trung Hiếu – 2019607984**

**Bùi Việt Hoàng – 2019603179**

**Hà Nội, 2022**

**MỤC LỤC**

[**DANH MỤC HÌNH ẢNH 4**](#_Toc113475517)

[**LỜI CẢM ƠN 5**](#_Toc113475518)

[**LỜI MỞ ĐẦU 6**](#_Toc113475519)

[**CHƯƠNG 1: TỔNG QUAN 7**](#_Toc113475520)

[**1.1 Giới thiệu an toàn bảo mật thông tin 7**](#_Toc113475521)

[**1.1.1 Sự cần thiết của việc đảm bảo an toàn thông tin 7**](#_Toc113475522)

[**1.1.2 Khái niệm an toàn thông tin 7**](#_Toc113475523)

[**1.1.3 Các phương pháp bảo vệ thông tin 9**](#_Toc113475524)

[**1.2 Giới thiệu về Hệ mã Elgammal 10**](#_Toc113475525)

[**1.2.1 Giới thiệu chung 10**](#_Toc113475526)

[**1.2.2 Mô tả hoạt động 10**](#_Toc113475527)

[**1.3 Mục đích nghiên cứu 11**](#_Toc113475528)

[**1.4 Phương pháp nghiên cứu 11**](#_Toc113475529)

[**1.5 Đối tượng nghiên cứu 11**](#_Toc113475530)

[**1.6 Ý nghĩa khoa học và thực tiễn 11**](#_Toc113475531)

[**CHƯƠNG 2: KẾT QUẢ NGHIÊN CỨU ...13**](#_Toc113475532)

[**2.1 Giới thiệu 13**](#_Toc113475533)

[**2.2 Nội dung thuật toán 13**](#_Toc113475534)

[**2.2.1 Tìm hiểu về hệ mã hóa công khai Elgammal 13**](#_Toc113475535)

[**2.2.2 Các thuật toán để xây dựng chương trình 16**](#_Toc113475536)

[**2.3 Thiết kế, cài đặt chương trình đề mô thuật toán 18**](#_Toc113475537)

[**2.3.1 Giao diện chương trình demo 19**](#_Toc113475538)

[**2.4 Cài đặt và triển khai 19**](#_Toc113475539)

[**2.4.1 Công cụ Apache Netbeans IDE 13 19**](#_Toc113475540)

[**2.4.2 Công cụ Visual Studio 20**](#_Toc113475541)

[**2.4.3 Hướng dẫn chạy chương trình đề mô 21**](#_Toc113475542)

[**2.5 Thực hiện bài toán 24**](#_Toc113475543)

[**2.5.1 Phân công công việc 24**](#_Toc113475544)

[**2.5.2 Bùi Lê Hiếu - 2019605753 26**](#_Toc113475545)

[**2.5.3 Hoàng Trung Hiếu - 2019607984 30**](#_Toc113475546)

[**2.5.4 Hoàng Trung Hiếu - 2020602568 37**](#_Toc113475547)

[**2.5.5 Nguyễn Huy Hoàng – 2019608191 39**](#_Toc113475548)

[**2.5.6 Bùi Việt Hoàng – 2019603179 42**](#_Toc113475549)

[**CHƯƠNG 3: PHẦN KIẾN THỨC LĨNH HỘI VÀ BÀI HỌC KINH NGHIỆM 43**](#_Toc113475550)

[**3.1 Nội dung đã thực hiện 43**](#_Toc113475551)

[**3.2 Hướng phát triển 44**](#_Toc113475552)

[**TÀI LIỆU THAM KHẢO 45**](#_Toc113475553)

# **DANH MỤC HÌNH ẢNH**

[*Hình 2. 1 Thiết kế sơ đồ khối 14*](#_Toc112551715)

[*Hình 2. 2 Cách làm việc của thuật toán 14*](#_Toc112551716)

[*Hình 2. 3 Giao diện chương trình demo 19*](#_Toc112551717)

[*Hình 2. 4 Tạo khóa 21*](#_Toc112551718)

[*Hình 2. 5 Nhập nội dung bản rõ 22*](#_Toc112551719)

[*Hình 2. 6 Mã hóa bản rõ 22*](#_Toc112551720)

[*Hình 2. 7 Bản mã 23*](#_Toc112551721)

[*Hình 2. 8 Bản mã sau khi giải mã 23*](#_Toc112551722)

[*Hình 2. 9 Xóa dữ liệu 24*](#_Toc112551723)

# **LỜI CẢM ƠN**

*Đầu tiên, chúng e*m xin gửi lời cảm ơn chân thành và sự tri ân sâu sắc đối với các thầy cô của trường Đại học Công Nghiệp Hà Nội, khoa Công Nghệ Thông Tin *đã đóng góp ý kiến và cho chúng em những lời khuyên vô cùng bổ ích*. Và đặc biệt chúng em xin chân thành cám ơn cô giáo Th.S Trần Phương Nhung đã nhiệt tình hướng dẫn chúng em hoàn thành bài tập lớn này.

Trong quá trình làm bài, khó tránh khỏi những sai sót, rất mong các thầy, cô bỏ qua cho chúng em. Đồng thời do trình độ lý luận cũng như kinh nghiệm thực tiễn còn hạn chế nên bài báo cáo không thể tránh khỏi những thiếu sót, chúng em rất mong nhận được ý kiến đóng góp thầy, cô. *Những ý kiến đóng góp của các thầy,cô và các bạn chính là yếu tố, động lực giúp chúng em hoàn thành bài tập lớn này một cách tốt nhất.*

*Chúng em xin chân thành cảm ơn!*

# **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 cô, các thành viên trong nhóm đã tiến hành tìm hiểu về các thuật toán mã hóa và giải mã hệ mật mã Elgamal, nhóm em tiến hành xây dựng mô phỏng hệ mật Elgamal trên các ngôn ngữ khác nhau.

# **CHƯƠNG 1: TỔNG QUAN**

## Giới thiệu an toàn bảo mật thông tin

* + 1. **Sự cần thiết của việc đảm bảo an toàn thông tin**

Ngày nay sự xuất hiện của internet toàn cầu đã giúp cho việc trao đổi thông tin trở nên nhanh gọn, dễ dàng. Các phương thức chia sẻ dữ liệu qua mạng làm cho việc trao đổi, mua bán, chuyển tiền, … diễn ra mỗi ngày trên nền tảng số.

Tuy nhiên vấn đề mới lại phát sinh. Những thông tin đang nằm ở kho dữ liệu hay đang được truyền đi có thể bị trộm cắp, bị làm sai lệch, giả mạo. Điều này làm ảnh hưởng đến độ an toàn của thông tin nhạy cảm, tin mật, … có thể tác động lớn đến nhiều cá nhân, tổ chức, hay ác động đến an ninh quốc gia.

### **Khái niệm an toàn thông tin**

#### **Khái niệm**

Định nghĩa của an toàn thông tin được nêu ra từ nhiều nguồn khác nhau, chúng ta có thể hiểu theo nhiều cách sau: “An toàn thông tin nghĩa là thông tin được bảo vệ, các hệ thống và dịch vụ có khả năng chống lại những sự can thiệp, lỗi và những tai họa không mong đợi, các thay đổi tác động đến độ an toàn của hệ thống là nhỏ nhất. Hệ thống không an toàn là hệ thống tồn tại những điểm: thông tin bị rò rỉ ra ngoài, thông tin bị thay đổi, ...”

Giá trị thực sự của thông tin chỉ đạt được khi thông tin được cung cấp chính xác và kịp thời, hệ thống phải hoạt động chuẩn xác thì mới có thể đưa ra những thông tin có giá trị cao. Mục tiêu của an toàn bảo mật trong công nghệ thông tin là đưa ra một số tiêu chuẩn an toàn và áp dụng các tiêu chuẩn an toàn này vào chỗ thích hợp để giảm bớt và loại trừ những nguy hiểm có thể xảy ra. Ngày nay với kỹ thuật truyền nhận và xử lý thông tin ngày càng phát triển và phức tạp nên hệ thống chỉ có thể đạt tới một mức độ an toàn nào đó và không có một hệ thống an toàn tuyệt đối.

#### **Các yêu cầu an toàn bảo mật thông tin**

Ngày nay, với sự phát triển rất nhanh của khoa học công nghệ, các biện pháp tấn công ngày càng tinh xảo hơn, độ an toàn của thông tin có thể bị đe dọa từ nhiều nơi, theo nhiều cách khác nhau, chúng ta cần phải đưa ra các chính sách đề phòng thích hợp. Các yêu cầu cần thiết của việc bảo vệ thông tin và tài nguyên:

* Đảm bảo bí mật (Bảo mật): thông tin không bị lộ đối với người không được phép.
* Đảm bảo tính tin cậy (Confidentiality): Thông tin và tài nguyên không thể bị truy cập trái phép bởi những người không có quyền hạn.
* Đảm bảo tính toàn vẹn (Integrity): Thông tin và tài nguyên không thể bị sửa đổi, bị thay thế bởi những người không có quyền hạn.
* Đảm bảo tính sẵn sàng (Availability): Thông tin và tài nguyên luôn sẵn sàng để đáp ứng sử dụng cho người có quyền hạn.
* Đảm bảo tính không thể chối bỏ (Non-repudiation): Thông tin và tài nguyên được xác nhận về mặt pháp luật của người cung cấp.

#### **Các nội dung an toàn thông tin**

+ Nội dung chính:

* An toàn máy tính: là sự bảo vệ các thông tin cố định bên trong máy tính, là khoa học về bảo đảm an toàn thông tin trong máy tính.
* An toàn truyền tin: là sự bảo vệ thông tin trên đường truyền tin(thông tin được truyền từ hệ thống này sang hệ thống khác), là khoa học bảo đảm an toàn thông tin trên đường truyền tin.

+ Nội dung chuyên ngành:

* An toàn dữ liệu (data security).
* An toàn cơ sở dữ liệu (database security).
* An toàn hệ điều hành (operation system security).
* An toàn mạng máy tính (network security).

#### **Các chiến lược bảo đảm an toàn thông tin**

* Giới hạn quyền hạn tối thiểu (Last Privilege): theo nguyên tắc này bất kỳ một đối tượng nào cùng chỉ có những quyền hạn nhất định đối với tài nguyên mạng.
* Bảo vệ theo chiều sâu (Defence In Depth): Không nên dựa vào một chế độ an toàn nào dù cho chúng rất mạnh, mà nên tạo nhiều cơ chế an toàn để tương hỗ lẫn nhau.
* Nút thắt (Choke Point): Tạo ra một “cửa khẩu” hẹp, và chỉ cho phép thông tin đi vào hệ thống của mình bằng con đường duy nhất chính là “cửa khẩu” này.
* Điểm nối yếu nhất (Weakest Link): Chiến lược này dựa trên nguyên tắc: “ Một dây xích chỉ chắc tại mắt duy nhất, một bức tường chỉ cứng tại điểm yếu nhất”.
* Tính toàn cục: Các hệ thống an toàn đòi hỏi phải có tính toàn cục của các hệ thống cục bộ.
* Tính đa dạng bảo vệ: Cần phải sử dụng nhiều biện pháp bảo vệ khác nhau cho hệ thống khác nhau, nếu không có kẻ tấn công vào được một hệ thống thì chúng cũng dễ dàng tấn công vào các hệ thống khác.

**1.1.3 Các phương pháp bảo vệ thông tin**

- Quyền truy nhập: Là lớp bảo vệ trong cùng nhằm kiểm soát các tài nguyên của mạng và quyền hạn trên tài nguyên đó.

- Đăng ký tên /mật khẩu: Thực ra đây cũng là kiểm soát quyền truy nhập, nhưng không phải truy nhập ở mức thông tin mà ở mức hệ thống.

- Mã hoá dữ liệu: Dữ liệu bị biến đổi từ dạng nhận thức được sang dạng không nhận thức được theo một thuật toán nào đó và sẽ được biến đổi ngược lại ở trạm nhận (giải mã).

- Bảo vệ vật lý: Ngăn cản các truy nhập vật lý vào hệ thống.

- Tường lửa: Ngăn chặn thâm nhập trái phép và lọc bỏ các gói tin không muốn gửi hoặc nhận vì các lý do nào đó để bảo vệ một máy tính hoặc cả mạng nội bộ (intranet).

- Quản trị mạng: Công tác quản trị mạng máy tính phải được thực hiện một cách khoa học. Toàn bộ hệ thống hoạt động bình thường trong giờ làm việc. Backup dữ liệu quan trọng theo định kỳ, có kế hoạch bảo trì định kỳ, bảo mật dữ liệu, phân quyền, …

## Giới thiệu về Hệ mã Elgammal

### **Giới thiệu chung**

Hệ mật mã Elgammal dựa trên độ khó của bài toán logarit rời rạc, hệ này về sau được mở rộng để phát triển nhiều hệ tương tự dựa trên độ khó của các bài toán tương tự logarit rời rạc trên cấu trúc nhóm cyclic hữu hạn, nhóm các điểm nguyên trên đường cong eliptic,... Để tăng độ bảo mật, hệ mật mã Elgammal còn dùng với tư cách đầu vào cho thuật toán lập mật mã của mình ngoài khóa công khai và bản rõ, một yếu tố ngẫu nhiên được chọn tùy ý, điều đó làm cho hệ mật mã trở thành một hệ mật mã xác suất khóa công khai. Một số hệ mật mã xác suất khóa công khai cũng được phát triển sau đó bởi Goldwasser-Micali và Bulm-Goldwasser.

1. **Mô tả hoạt động**

Hệ mật ElGammal là một hệ mật khóa bất đối xứng cho khóa công khai, dựa trên trao đổi khóa Diffie – Hellan. Thuật toán do Taher Elgammal 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 Private key mới có thể giải mã.

## Mục đích nghiên cứu

Nghiên cứu về lý thuyết mật mã, mật mã hoá khoá công khai Elgammal, ứng dụng thuật toán Elgammal trong mã hoá dữ liệu. Từ đó xây dựng hệ thống cho phép tạo mã hóa và giải mã để bảo mật nội dung thông tin cũng như xác thực nguồn gốc của thông tin.

## 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 chính thống, đáng tin cậy trên mạng Internet liên quan đến vấn đề đang nghiên cứu.

Các công cụ sử dụng:

* Microsoft word: Viết báo cáo.
* Google meet, Zoom: Họp nhóm.
* Netbeans, Visual Studio, VsCode: Thực hiện viết các chương trình.

## Đối tượng nghiên cứu

* Hệ mật mã Elgammal.
* Tìm hiểu về phương pháp mã hóa và giải mã.
* Tìm hiểu cách xây dựng hệ mã hóa Elgammal trên các ngôn ngữ khác nhau.

## Ý nghĩa khoa học và thực tiễn

*Về mặt lý thuyết:*

* Trình bày trình bày khát quát về mật mã, khái niệm về hệ mật mã  khoá bí mật và hệ mật mã khoá công khai.
* Trình bày lý thuyết chung về các phương pháp mã hoá: phương  pháp mã hoá khóa bí mật và phương pháp mã hoá khóa công  khai, nêu được các ưu điểm và nhược điểm của hai phương pháp  này. Trình bày chi tiết hệ mật mã khóa công khai Elgammal.

*Về mặt thực tiễn:*

* Xây dựng được chương trình ứng dụng dựa vào hệ mật mã Elgammal  có chức năng bảo mật nội dung cho các tập tin là các dữ liệu hoặc các tài liệu, mã hóa và gải mã nội dung thông điệp, tập tin để xác  định tính toàn vẹn nội dung và chủ nhân của tập tin khi thực hiện trao đổi.

# **CHƯƠNG 2: KẾT QUẢ NGHIÊN CỨU**

## Giới thiệu

- Đề tài: “Xây dựng chương trình mã hóa và giải mã Elgammal”.

- Các bước thực hiện triển khai đề tài:

* Tìm hiểu về hệ mã Elgammal.
* Nghiên cứu các thuật toán trong hệ mã.
* Thiết kế giao diện tổng quan và cài đặt chương trình theo thuật toán demo.

- Kết quả đạt được: Xây dựng được chương trình đề mô mã hóa và giải mã Elgammal.

## Nội dung thuật toán

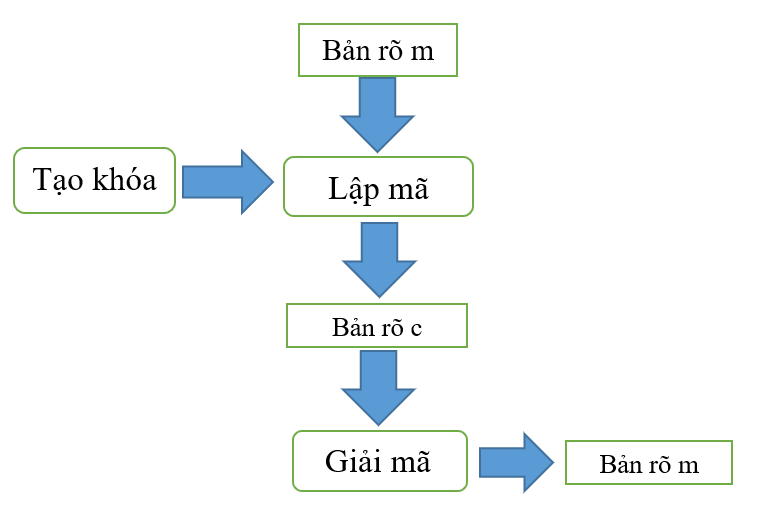
1. **Tìm hiểu về hệ mã hóa công khai Elgammal**

#### **Tổng quan hệ mã**

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.

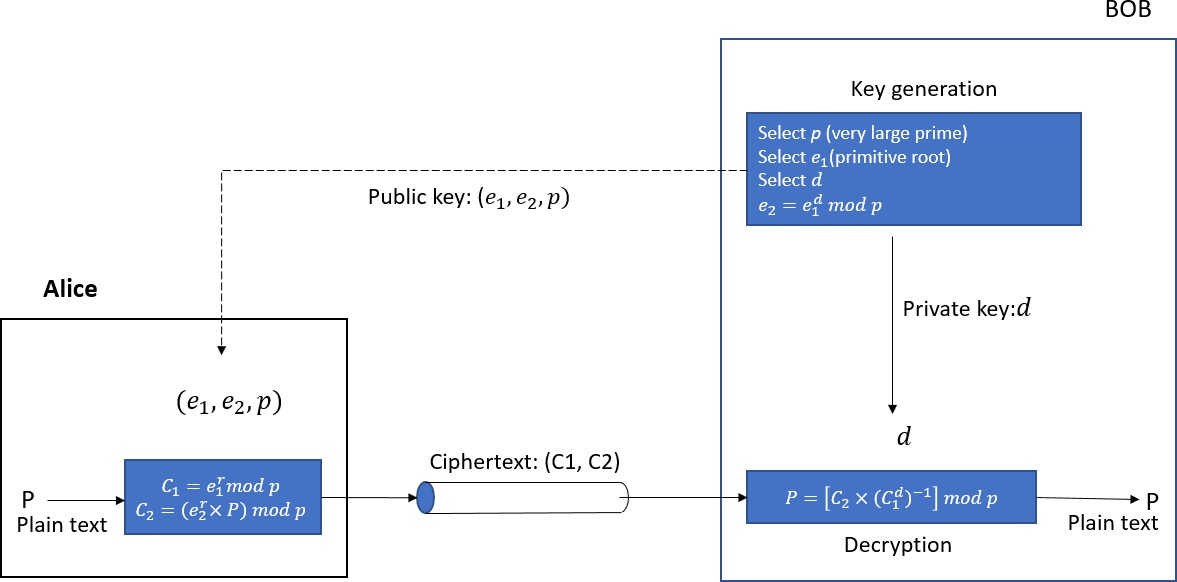
#### **Thiết kế sơ đồ khối**



Hình 2. 1 Thiết kế sơ đồ khối

#### **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 2. 2 Cách làm việc của thuật toán

#### **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 a thuộc nhóm 𝐺 = <Zp\*, X>sao cho 1 ≤ a ≤ 𝑝 −2.

3. Chọn d1 là phần tử nguyên tử của nhóm 𝐺 = <Zp \*, X>.

4. Tính d2 = d1d 𝑚𝑜𝑑 𝑝.

5. Khóa công khai sẽ là (d1, d2, 𝑝).

6. Khóa bị mật sẽ là 𝑑.

#### **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 = <𝑍p\*, X>.
2. Khí đó tính được bản mật C1 = d1r mod p.
3. Sử dụng khóa công khai để tính bản mật C2 = (M \* d2r mod p) mod p.
4. Alice sẽ có bản mã gồm (𝐶1, 𝐶2) để gửi đến cho Bob.

#### **Giải mã**

Bob nhận được bản mã (𝐶1, 𝐶2) và có khóa bị mật 𝑑 khi đó Bob sẽ tìm được bản rõ theo công thức: [𝐶2 \* (𝐶a) − 1] 𝑚𝑜𝑑 𝑝.

#### **Tính bảo mật của hệ Elgammal**

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.

#### **Ưu điểm và nhược điểm của hệ mã Elgammal**

**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.

1. **Các thuật toán để xây dựng chương trình**

#### **2.2.2.1 Kiểm tra số nguyên tố**

* Nếu n (số kiểm tra) < 2 thì không phải là số nguyên tố.
* Sử dụng vòng lặp chạy từ i = 2 cho tới <= √n, nếu n chia hết cho i thì không phải là số nguyên tố, ngược lại n là số nguyên tố.

#### **2.2.2.2 Bình phương và nhân**

* Ta có công thức: xk mod n.
* Đổi số k về hệ nhị phân.
* Khởi tạo p = 1 và chuyển k ở dạng nhị phân thành một chuỗi để dễ so sánh.
* Sử dụng vòng for duyệt đến hết chuỗi nhị phân, nếu kí tự trong chuỗi là 1 thì tính theo công thức: p = p \* p, p = p % n, p = p \* x, p = p mod n; ngược lại thì tính theo công thức: p = p \* p, p = p % n.
* Sau khi duyệt hết vòng lặp thì trả về p là số cần tìm.

#### **2.2.2.3 Euclide tìm modulo nghịch đảo**

* Ta có công thức: x-1 mod n (r0 = n, r1 = x).
* Tạo một hàm với 2 tham số truyền vào là r0 và r1.
* Khai báo các biến q[100], r2 = -1, s[100], t[100], i = 0 để thực hiện lưu trữ các giá trị được tính.
* Sử dụng vòng lặp while với điều kiện r2 khác 0 thì ta tính:
* q[i+1] = r0 / r1; r2 = r0 % r1;
* Nếu i = 0 thì s[i] = 1; t[i] = 0;
* Nếu i = 1 thì s[i] = 0; t[i] = 1;
* Nếu i != 0 và 1: s[i] = s[i-2] – q[i-1] \* s[i-1]; t[i] = t[i-2] – q[i-1] \* t[i-1];
* r0 = r1; r1 = r2;
* Biến i tăng giá trị lên 1;

+ Thoát khỏi vòng lặp: s[i] = s[i-2] – q[i-1]\*s[i-1]; t[i] = t[i-2] – q[i-1]\*t[i-1];

+ Giá trị nghịch đảo cần tìm: nếu t[i] > 0 thì trả về t[i] ngược lại sẽ trả về n+t[i].

#### **2.2.2.4 Kí tự mã hóa**

Ở đây, nhóm em sử dụng bảng mã kí tự Unicode để mã hóa và giải mã.

#### **2.2.2.5 Xây dựng thuật toán với C++**

**Kiểm tra số nguyên tố**

#include <bits/stdc++.h>

using namespace std;

bool kiemTraSNT(int n) {

if(n < 2)

return false;

for(int i = 2; i <= sqrt(n); i++)

if(n % i == 0)

return false;

return true;

}

int main() {

cout <<kiemTraSNT(7);

}

**Bình phương và nhân**

#include <bits/stdc++.h>

using namespace std;

int soNhiPhan(int n) {

if(n == 0) return n/10;

return (n%2) + soNhiPhan(n/2)\*10;

}

int binhPhuongVaNhan(int x, int n, int k) {

int p = 1, k\_nhiPhan = soNhiPhan(k);

char s[100];

sprintf(s, "%d", k\_nhiPhan);

for(int i = 0; i < strlen(s); i++) {

if(s[i] == '1') {

p = p \* p;

p = p % n;

p = p \* x;

p = p % n;

} else {

p = p \* p;

p = p % n;

}

}

return p;

}

int main() {

cout <<binhPhuongVaNhan(37, 101, 27);

}

**Euclide tìm modulo nghịch đảo**

#include <bits/stdc++.h>

using namespace std;

int ocolitMoRong(int ri, int ri1) {

int q[100], ri2 = -1, s[100], t[100], i = 0;

while(ri2 != 0) {

q[i+1] = ri / ri1;

ri2 = ri % ri1;

if(i == 0) {

s[i] = 1;

t[i] = 0;

} else if(i == 1) {

s[i] = 0;

t[i] = 1;

} else {

s[i] = s[i-2] - q[i-1] \* s[i-1];

t[i] = t[i-2] - q[i-1] \* t[i-1];

}

ri = ri1;

ri1 = ri2;

i++;

}

s[i] = s[i-2] - q[i-1] \* s[i-1];

t[i] = t[i-2] - q[i-1] \* t[i-1];

return t[i];

}

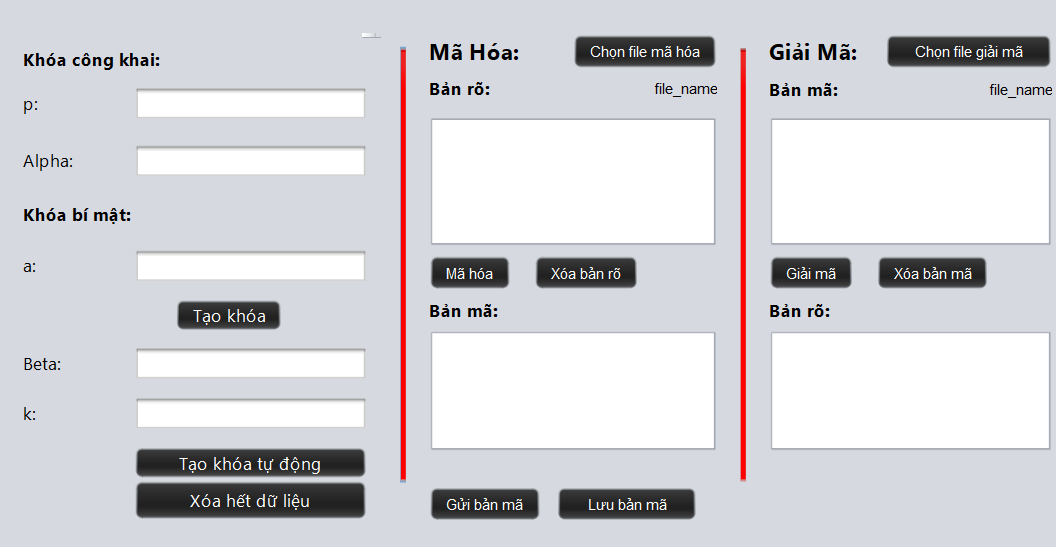
int main() {

cout <<ocolitMoRong(1200, 71);

}

## Thiết kế, cài đặt chương trình đề mô thuật toán

1. **Giao diện chương trình demo**



Hình 2. 3 Giao diện chương trình demo

1. **Cài đặt và triển khai**

Công cụ sử dụng để triển khai chương trình đề mô của các thành viên:

* Ngôn ngữ Java: Apache Netbeans IDE 13.
* Ngôn ngữ C#: Visual Studio.
* Ngôn ngữ JavaScript: Visual Studio Code.
* Ngôn ngữ Python: Visual Studio Code.
* Ngôn ngữ PHP: Visual Studio Code.

1. **Công cụ Apache Netbeans IDE 13**

NetBeans là một môi trường phát triển tích hợp (IDE) cho Java. NetBeans cho phép các ứng dụng được phát triển từ một tập hợp các thành phần phần mềm được gọi là modules. NetBeans chạy trên Windows, macOS, Linux và Solaris. Ngoài việc phát triển Java, nó còn có các phần mở rộng cho các ngôn ngữ khác như PHP, C, C++, HTML5, và JavaScript. Các ứng dụng dựa trên NetBeans, bao gồm NetBeans IDE, có thể được mở rộng bởi các nhà phát triển bên thứ ba.

NetBeans IDE là một IDE nguồn mở. NetBeans IDE hỗ trợ phát triển tất cả các loại ứng dụng Java (Java SE (bao gồm JavaFX), Java ME, web, EJB và ứng dụng mobile). Trong số các tính năng khác là hệ thống dự án dựa trên Ant, hỗ trợ Maven, cải tiến mã nguồn, quản lý phiên bản (hỗ trợ CVS, Subversion, Git, Mercurial và Clearcase).

1. **Công cụ Visual Studio**

Microsoft Visual Studio là một môi trường phát triển tích hợp (IDE) từ Microsoft. Microsoft Visual Studio còn được gọi là "Trình soạn thảo mã nhiều người sử dụng nhất thế giới ", được dùng để lập trình C++ và C# là chính. Nó được sử dụng để phát triển chương trình máy tính cho Microsoft Windows, cũng như các trang web, các ứng dụng web và các dịch vụ web. Visual Studio sử dụng nền tảng phát triển phần mềm của Microsoft như Windows API, Windows Forms, Windows Presentation Foundation, …

Visual Studio bao gồm một trình soạn thảo mã hỗ trợ IntelliSense cũng như cải tiến mã nguồn. Trình gỡ lỗi tích hợp hoạt động cả về trình gỡ lỗi mức độ mã nguồn và gỡ lỗi mức độ máy. Công cụ tích hợp khác bao gồm một mẫu thiết kế các hình thức xây dựng giao diện ứng dụng, thiết kế web, thiết kế lớp và thiết kế giản đồ cơ sở dữ liệu. Nó chấp nhận các plug-in nâng cao các chức năng ở hầu hết các cấp bao gồm thêm hỗ trợ cho các hệ thống quản lý phiên bản (như Subversion).

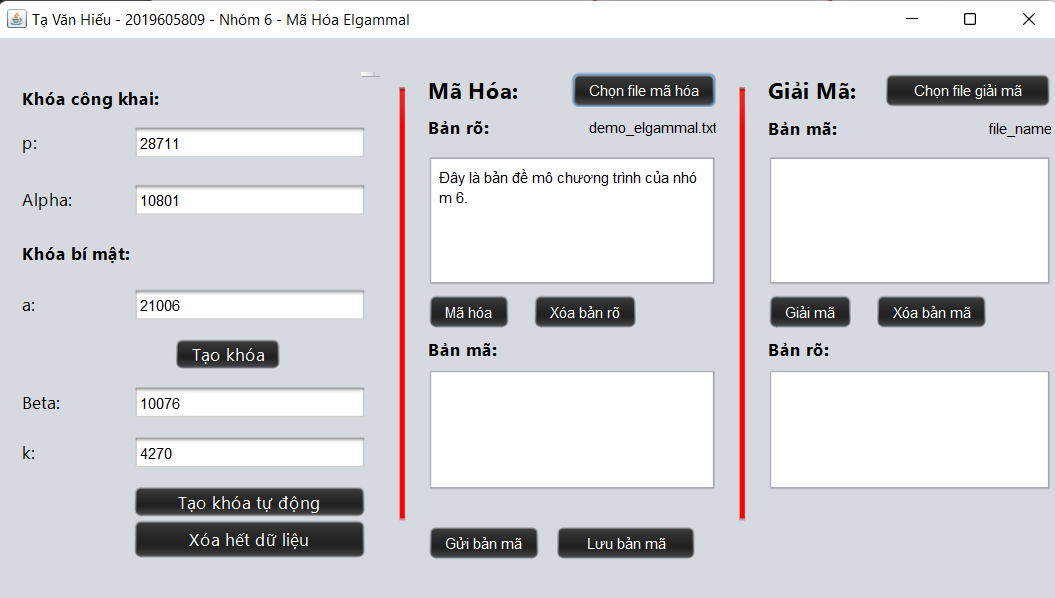
1. **Hướng dẫn chạy chương trình đề mô**

Khi người dùng thực hiện chạy chương trình, giao diện chương trình sẽ được hiện lên và người dùng phải nhập vào các tham số: p, alpha và a. Sau đó người dùng nhấn vào tạo khóa để thực hiện tạo ra các tham số: beta và k. Hay người dùng có thể tạo khóa nhanh bằng nút “Tạo khóa tự động” và giao diện sau khi tạo khóa sẽ được hiển thị như sau:



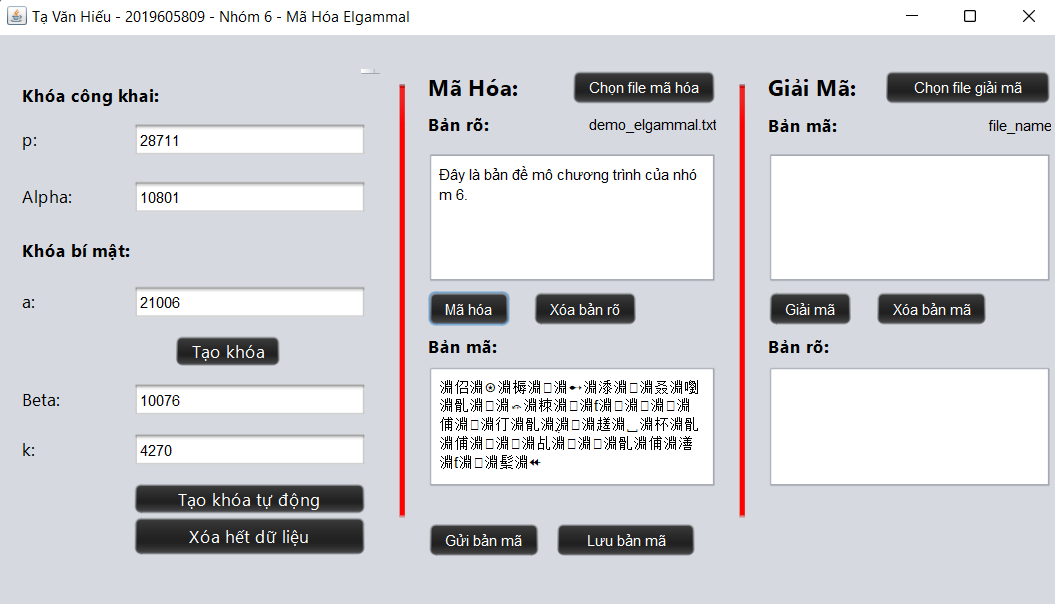
Hình 2. 4 Tạo khóa

Sau khi đã tạo khóa, người dùng có thể thực hiện nhập vào nội dung của bản rõ phần mã hóa thông qua bàn phím hay đọc trực tiếp nội dung từ file thông qua nút “Chọn file mã hóa” và giao diện khi đọc nội dung bản rõ từ file như sau:



Hình 2. 5 Nhập nội dung bản rõ

Khi đã nhập xong nội dung bản rõ, người dùng có thể nhấn nút: “Mã hóa” để thực hiện mã hóa bản rõ, “Xóa bản rõ” để thực hiện xóa nội dung của bản rõ trên TextBox. Và màn hình sau khi mã hóa bản rõ được thể hiện như sau:



Hình 2. 6 Mã hóa bản rõ

Người dùng có thể thực hiện gửi bản mã cho người nhận thông qua nút “Gửi bản mã” và có thể lưu nội dung bản mã lại thông nút “Lưu bản mã”. Và giao diện sau khi người dùng gửi bản mã như sau:



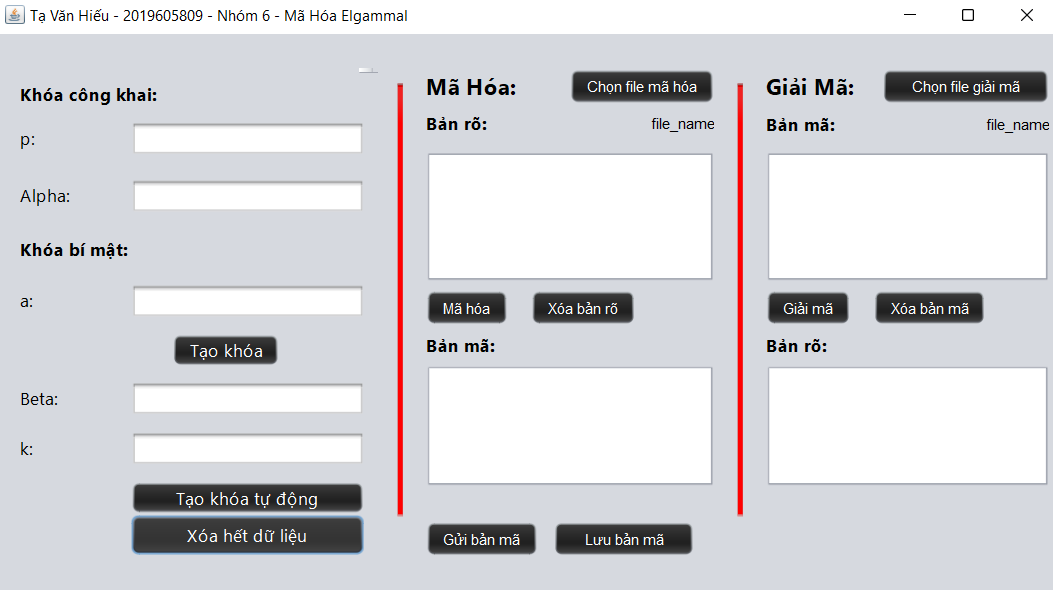
Hình 2. 7 Bản mã

Sau khi đã có bản mã, người dùng có thể thực hiện xóa bản mã thông qua nút “Xóa bản mã” và giải mã bản mã thông qua nút “Giải mã” và giao diện sau khi giải mã bản mã được thể hiện như sau:



Hình 2. 8 Bản mã sau khi giải mã

Sau khi người dùng hoàn tất mã hóa và giải mã, để xóa hết dữ liệu các ô văn bản người dùng có thể nhấn vào nút “Xóa hết dữ liệu” và giao diện sau khi xóa hết dữ liệu như sau:



Hình 2. 9 Xóa dữ liệu

1. **Thực hiện bài toán**
2. **Phân công công việc**

Các chức năng sẽ cài đặt trong chương trình:

* Tạo khóa cho hệ mã.
* Mã hóa bản rõ.
* Giải mã bản mã.
* Đọc file bản rõ và bản mã.
* Lưu file bản mã.

Bảng phân công nội dung công việc cho từng thành viên:

|  |  |
| --- | --- |
| **Tên sinh viên** | **Tên công việc** |
| Bùi Lê Hiếu | + Viết nội dung chương 2: Các thuật toán để xây dựng chương trình.  + Viết nội dung chương 2: Cài đặt và triển khai.  + Tìm hiểu công cụ Netbeans.  + Viết chương trình đề mô với ngôn ngữ Java.  + Hoàn thiện cuốn báo cáo. |
| Hoàng Trung Hiếu - 2019607984 | + Viết nội dung chương 1: Tổng quan  + Viết nội dung chương 3: Kiến thức lĩnh hội và bài học kinh nghiệm.  + Viết chương trình đề mô với ngôn ngữ C#. |
| Hoàng Trung Hiếu - 2020602568 | + Viết nội dung chương 2: Tìm hiểu về hệ mã hóa công khai Elgammal.  + Tìm hiểu công cụ Visual Studio.  + Viết chương trình đề mô với ngôn ngữ JavaScript. |
| Nguyễn Huy Hoàng | + Viết nội dung chương 2: Tìm hiểu về hệ mã hóa công khai Elgammal.  + Tìm hiểu công cụ Visual Studio.  + Viết chương trình đề mô với ngôn ngữ PHP. |
| Bùi Việt Hoàng | + Viết nội dung báo cáo: Các thuật toán để xây dựng chương trình.  + Viết nội dung : Cài đặt và triển khai.  + Viết chương trình đề mô với ngôn ngữ python.  + Hoàn thiện cuốn báo cáo. |

### **Bùi Lê Hiếu - 2019605753**

* Viết nội dung chương 2: Các thuật toán để xây dựng chương trình.
* Viết nội dung chương 2: Cài đặt và triển khai.
* Tìm hiểu công cụ Netbeans.
* Hoàn thiện cuốn báo cáo.
* Viết chương trình đề mô với ngôn ngữ Java trên công cụ Apache Netbeans IDE 13.

**Hàm tạo khóa:**

private void btnTaoKhoaActionPerformed(java.awt.event.ActionEvent evt) {                                             
        int beta;  
        if (textInputP.getText().isEmpty())  
            JOptionPane.showMessageDialog(this, "Chưa nhập số P!", "Error", JOptionPane.OK\_OPTION);  
        else if (textInputAlpha.getText().isEmpty())  
            JOptionPane.showMessageDialog(this, "Chưa nhập số Alpha!", "Error", JOptionPane.OK\_OPTION);  
        else if (textInputA.getText().isEmpty())  
            JOptionPane.showMessageDialog(this, "Chưa nhập số A!", "Error", JOptionPane.OK\_OPTION);  
        else {  
            int p = Integer.valueOf(textInputP.getText().trim());  
            int alpha = Integer.valueOf(textInputAlpha.getText().trim());  
            int a = Integer.valueOf(textInputA.getText().trim());  
            if (p < 50) {  
                JOptionPane.showMessageDialog(this, "Nhập P >= 50!", "Error", JOptionPane.OK\_OPTION);  
            } else if (!checkSNT(p)) {  
                JOptionPane.showMessageDialog(this, "P không phải số nguyên tố. Vui lòng nhập lại!", "Error", JOptionPane.OK\_OPTION);  
            } else {  
                beta = binhPhuongNhan(alpha, p, a);  
                textInputBeta.setText("" + beta);  
                Random rd = new Random();  
                int k = rd.nextInt((p - 2) + 1);  
                textInputK.setText("" + k);  
            }  
        }  
    }

**Hàm tạo khóa tự động:**

private void btnTaoKhoaTuDongActionPerformed(java.awt.event.ActionEvent evt) {                                                   
        int max = 45000, min = 8000;  
        int p, a, alpha, beta, k;  
        Random random = new Random();  
        do {  
            p = random.nextInt((max - min) + 1) + min;  
        } while (checkSNT(p) == false);  
        textInputP.setText("" + p);  
        //set a  
        a = random.nextInt((p - 2) + 1) + 2;  
        textInputA.setText("" + a);  
        //set alpha   
        alpha = random.nextInt((p - 1) + 1) + 1;  
        textInputAlpha.setText("" + alpha);  
        //set K  
        k = random.nextInt((p - 2) + 1);  
        textInputK.setText("" + k);  
        //set beta   
        beta = binhPhuongNhan(alpha, p, a);  
        textInputBeta.setText("" + beta);  
    }

**Hàm mã hóa:**

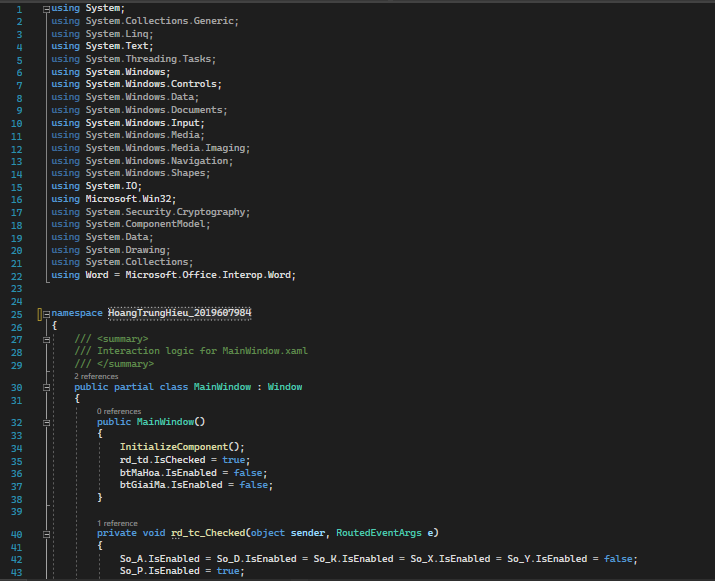
private void btnMaHoaActionPerformed(java.awt.event.ActionEvent evt) {                                           
        if (tbBanRoMaHoa.getText().isEmpty())  
            JOptionPane.showMessageDialog(this, "Không có thông điệp cần mã hóa!", "Error", JOptionPane.OK\_OPTION);  
        else {  
            if (textInputP.getText().isEmpty() || textInputAlpha.getText().isEmpty() || textInputBeta.getText().isEmpty()) {  
                JOptionPane.showMessageDialog(this, "Lỗi tạo khóa!", "Error", JOptionPane.OK\_OPTION);  
            } else {  
                Random random = new Random();  
                int p = Integer.valueOf(textInputP.getText().trim());  
                int alpha = Integer.valueOf(textInputAlpha.getText().trim());  
                int beta = Integer.valueOf(textInputBeta.getText().trim());  
                int k = random.nextInt((p - 2) + 1);  
                //Tìm y = (y1, y2).  
                int y1 = binhPhuongNhan(alpha, p, k);  
                int y2;  
                String banRo = tbBanRoMaHoa.getText();  
                ArrayList<Integer> arr\_ban\_ma = new ArrayList<>();  
                for (int i = 0; i < banRo.length(); i++) {  
                    arr\_ban\_ma.add(y1);  
                    y2 = ((banRo.charAt(i) \* binhPhuongNhan(beta, p, k)) % p);  
                    arr\_ban\_ma.add(y2);  
                }  
                //chuyển chuỗi mã hóa sang dạng chữ:  
                String banMa = "";  
                for (int j = 0; j < arr\_ban\_ma.size(); j++) {  
                    banMa += (char) (arr\_ban\_ma.get(j) % p);  
                }  
                tbBanMaMaHoa.setText(banMa);  
            }  
        }  
    }

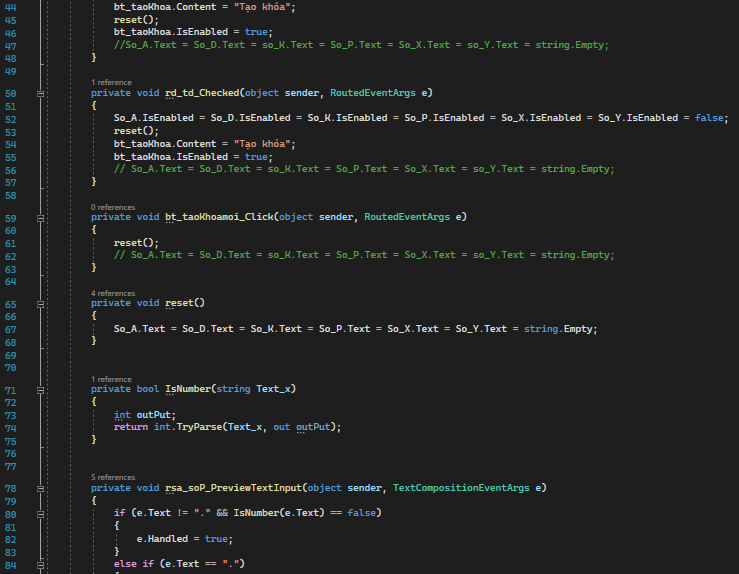
**Hàm giải mã:**

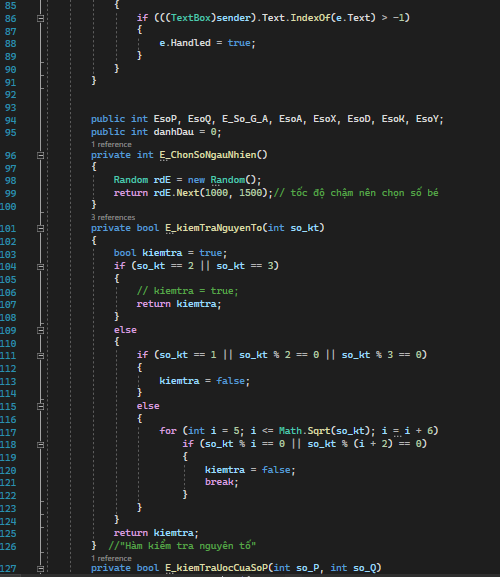
private void btnGiaiMaActionPerformed(java.awt.event.ActionEvent evt) {                                            
        if (tbBanMaGiaiMa.getText().isEmpty()) {  
            JOptionPane.showMessageDialog(this, "Không có thông điệp cần giải mã!", "Error", JOptionPane.ERROR\_MESSAGE);  
        } else {  
            ArrayList<Integer> arr\_ban\_ma = new ArrayList<>();  
            String banMa = tbBanMaGiaiMa.getText();  
            int p = Integer.parseInt(textInputP.getText().trim());  
            int a = Integer.parseInt(textInputA.getText().trim());  
            for (int i = 0; i < banMa.length(); i++) {  
                arr\_ban\_ma.add((int) banMa.charAt(i));  
            }  
            //d=y2(y1^a)^-1 mod p  
            int k = binhPhuongNhan(arr\_ban\_ma.get(0), p, a);  //k=y1^a mod p  
            String banRo = "";  
            for (int j = 1; j < arr\_ban\_ma.size(); j += 2) {  
                //d=y2(k)^-1 mod p  
                char c = (char) ((arr\_ban\_ma.get(j) \* ocolitMoRong(p, k)) % p);  
                banRo += c;  
            }  
            tbBanRoGiaiMa.setText(banRo);  
        }  
    }

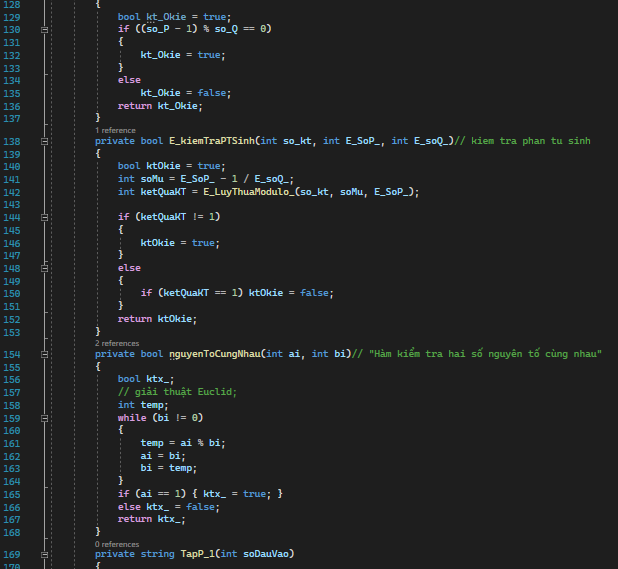
### **Hoàng Trung Hiếu - 2019607984**

* Viết nội dung chương 1: Tổng quan
* Viết nội dung chương 3: Kiến thức lĩnh hội và bài học kinh nghiệm.
* Viết chương trình đề mô với ngôn ngữ C# trên công cụ Visual Studio.

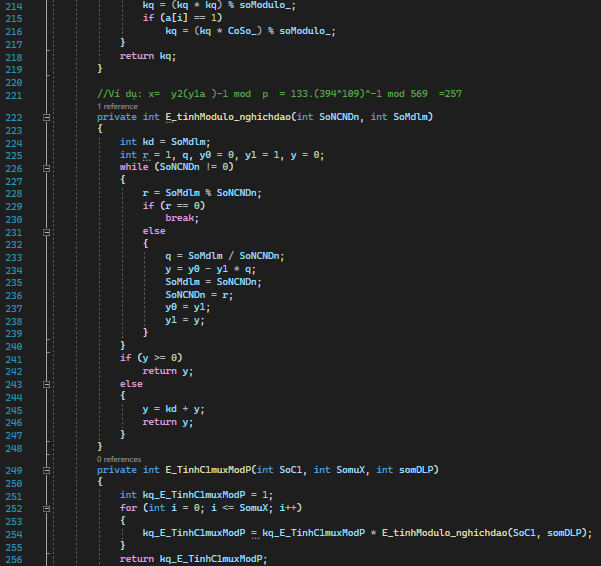


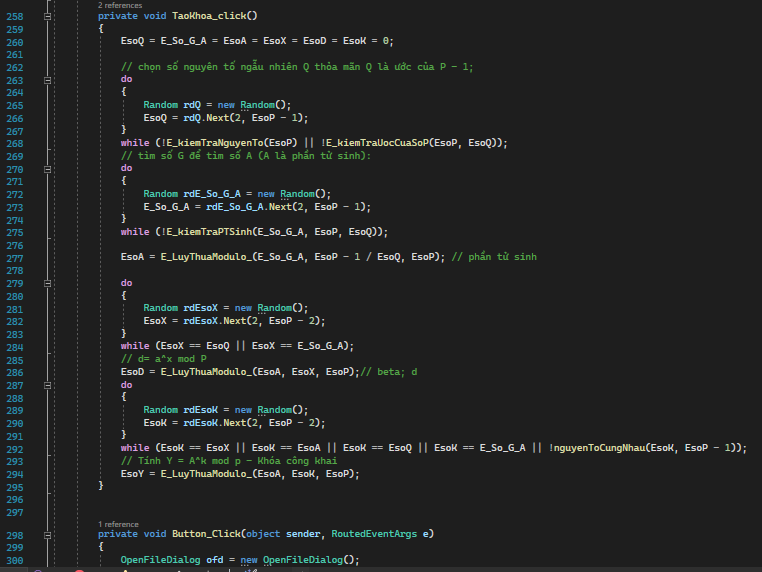


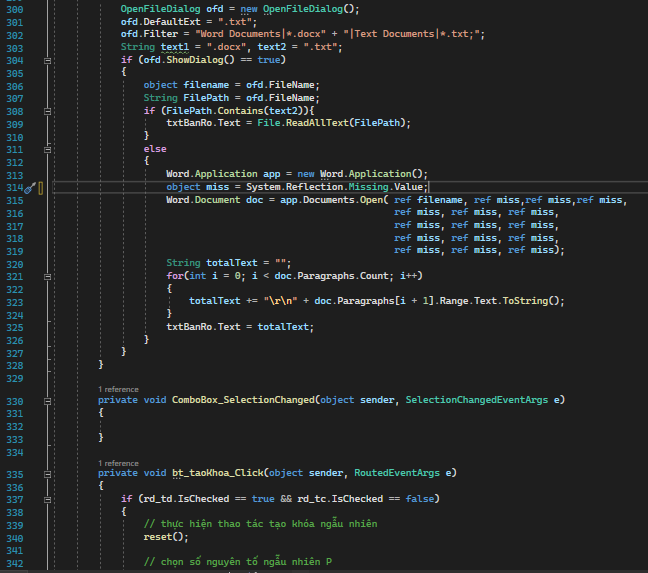


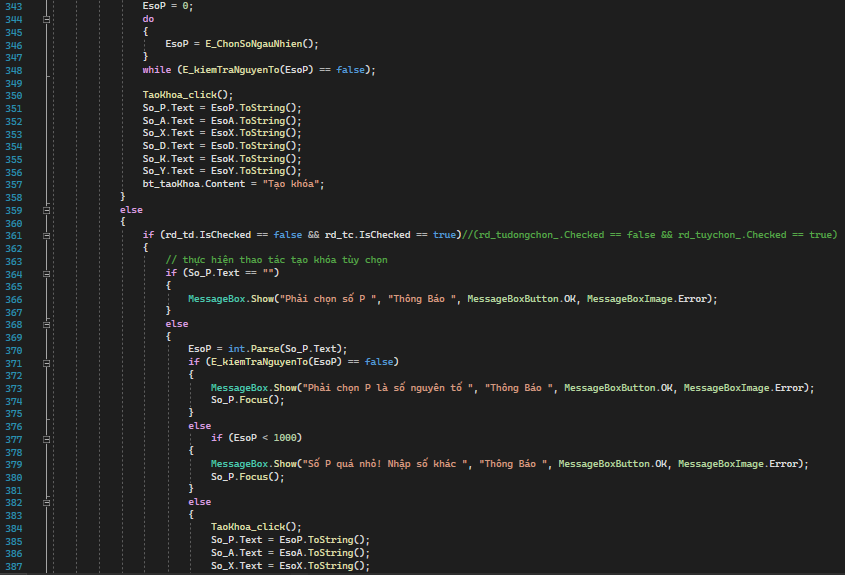


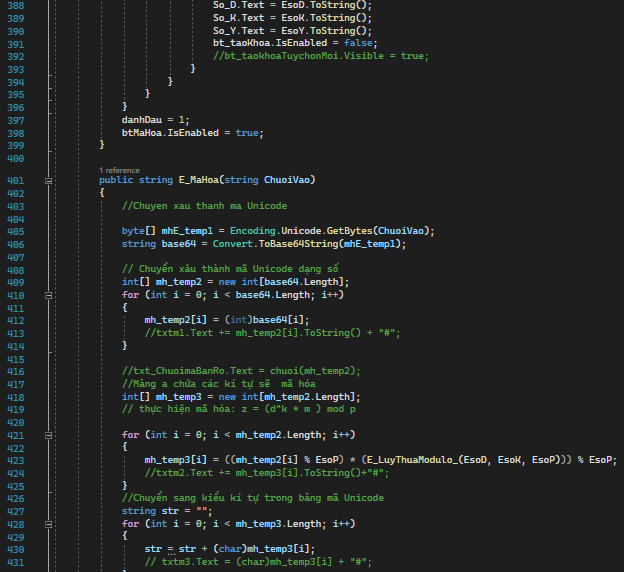


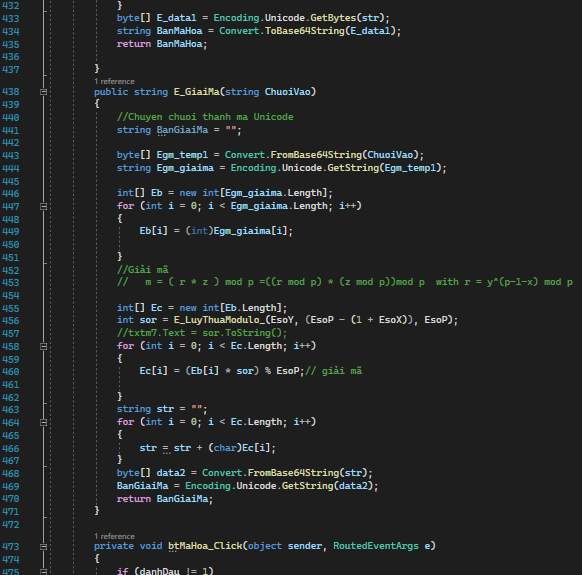


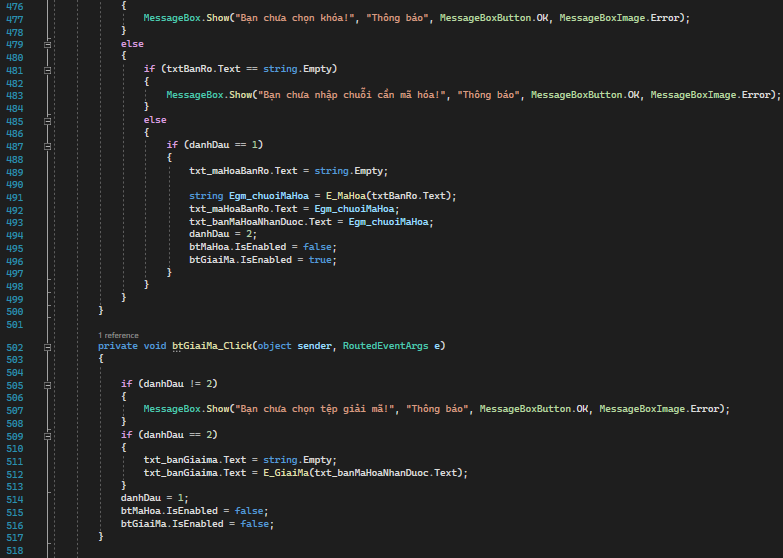


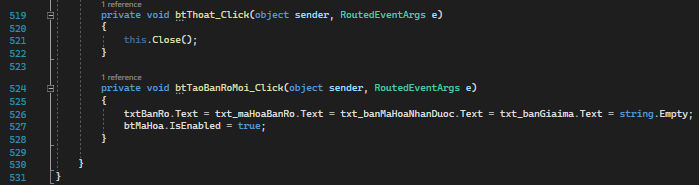






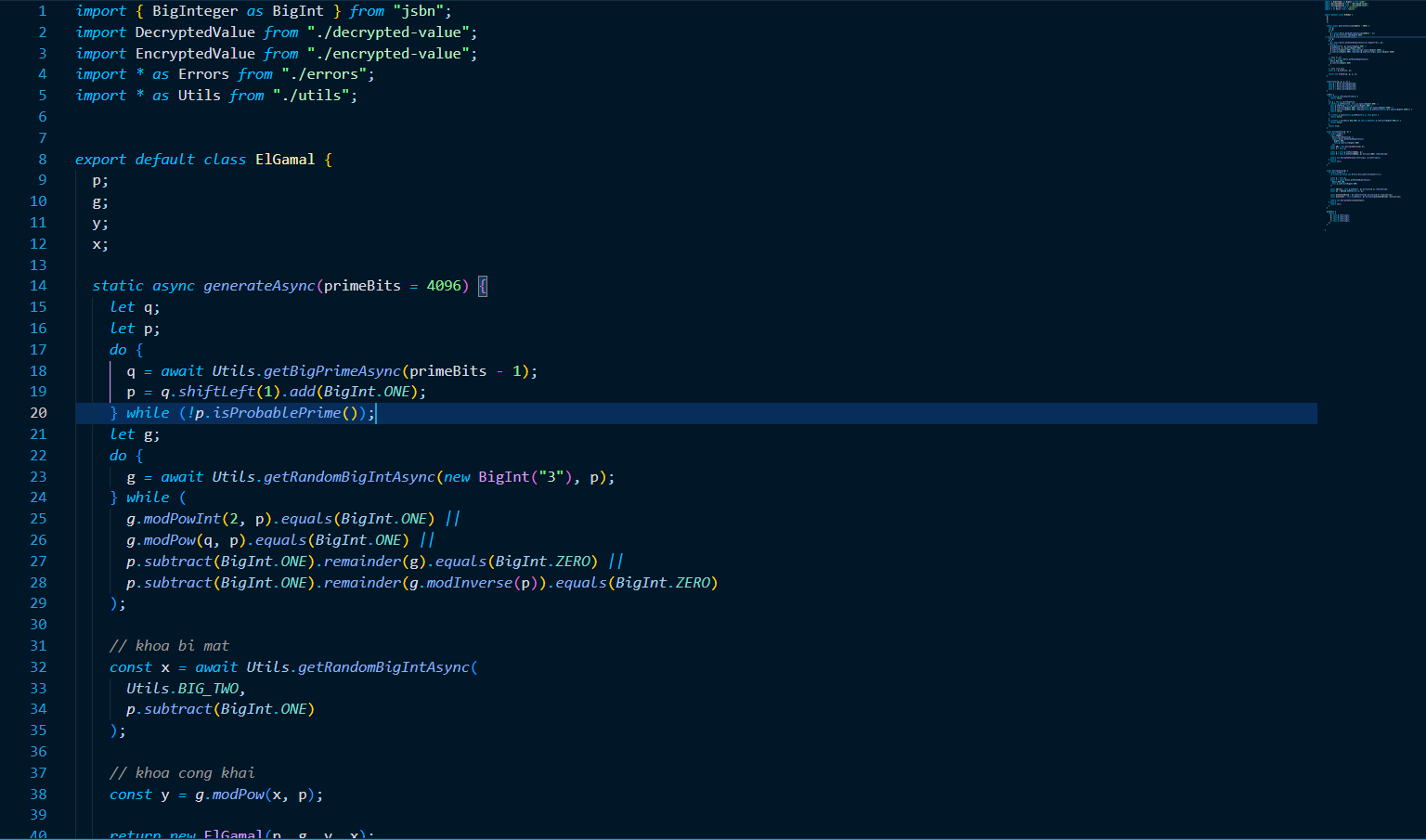




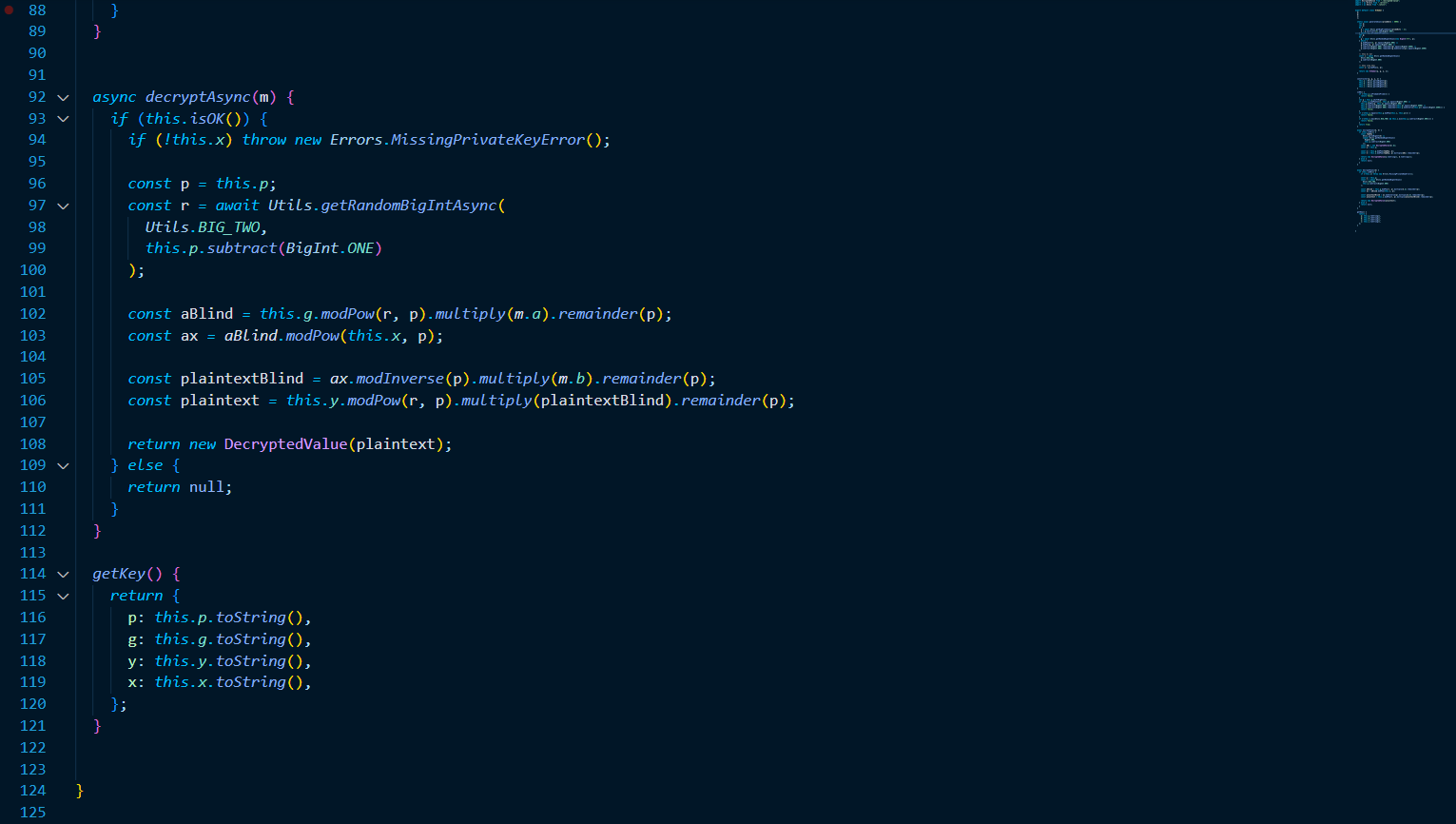


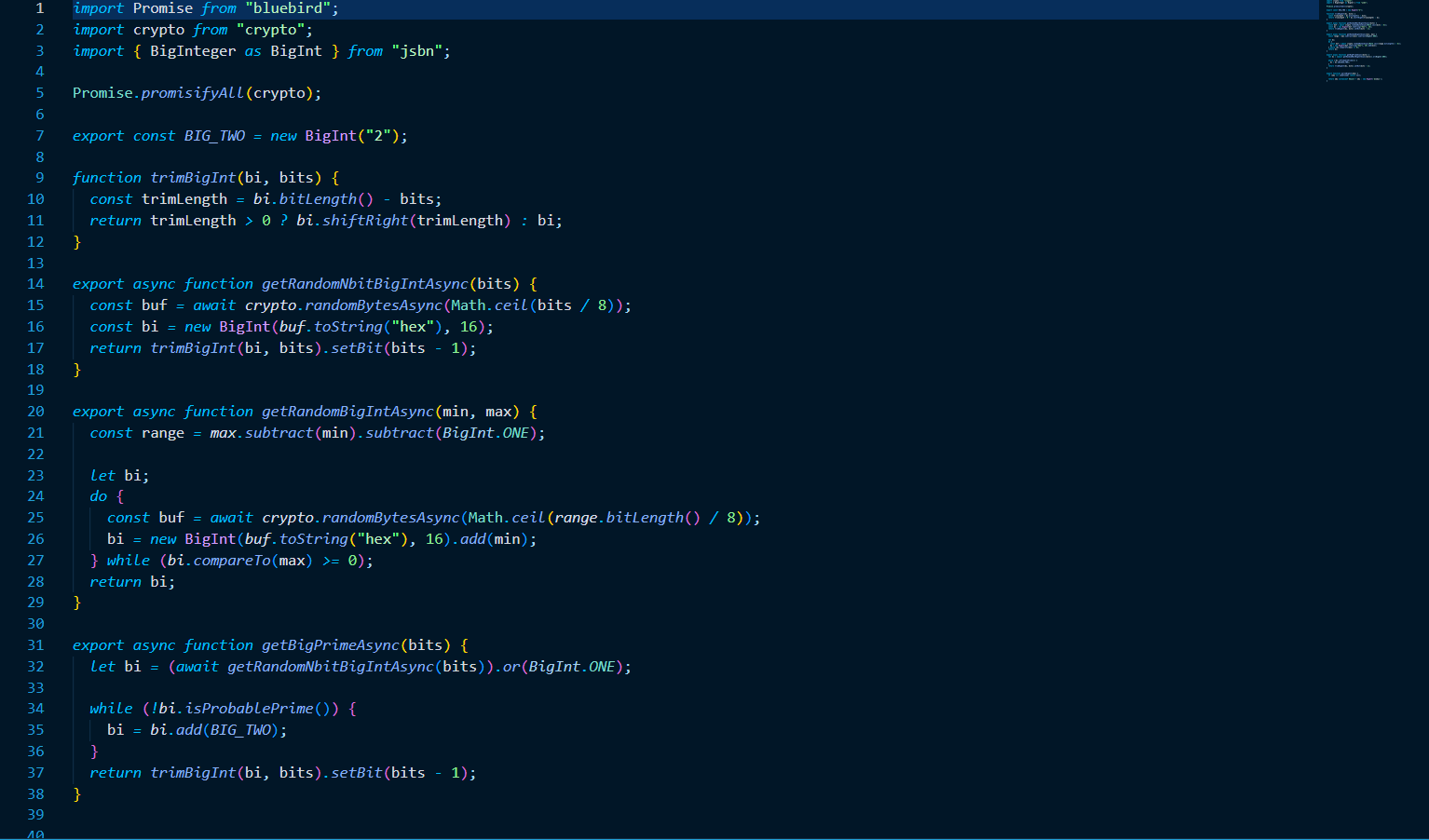
1. **Hoàng Trung Hiếu - 2020602568**

* Viết nội dung chương 2: Tìm hiểu về hệ mã hóa công khai Elgammal.
* Tìm hiểu về công cụ Visual Studio.
* Viết chương trình đề mô với ngôn ngữ JavaScript trên công cụ Visual Studio Code.



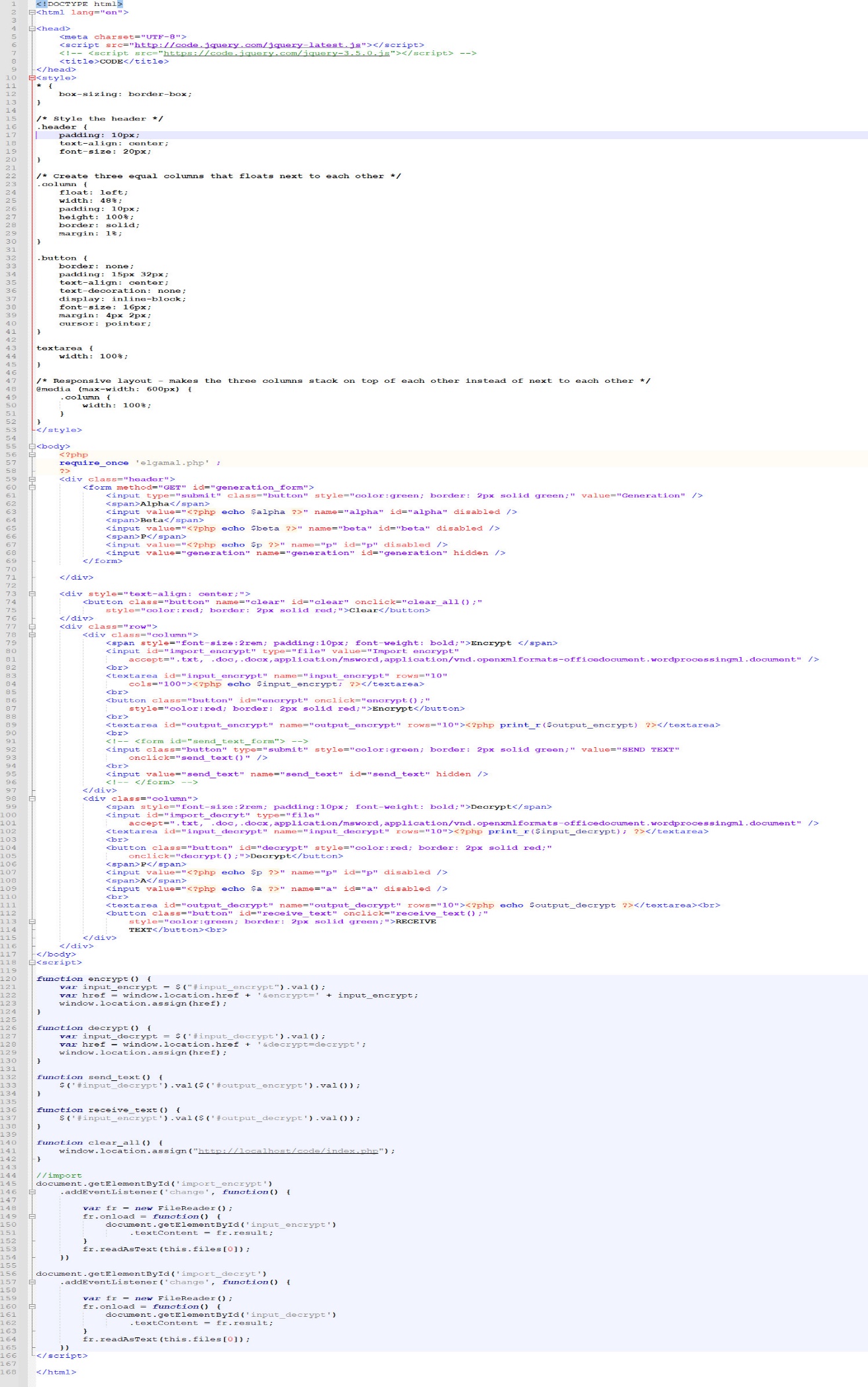
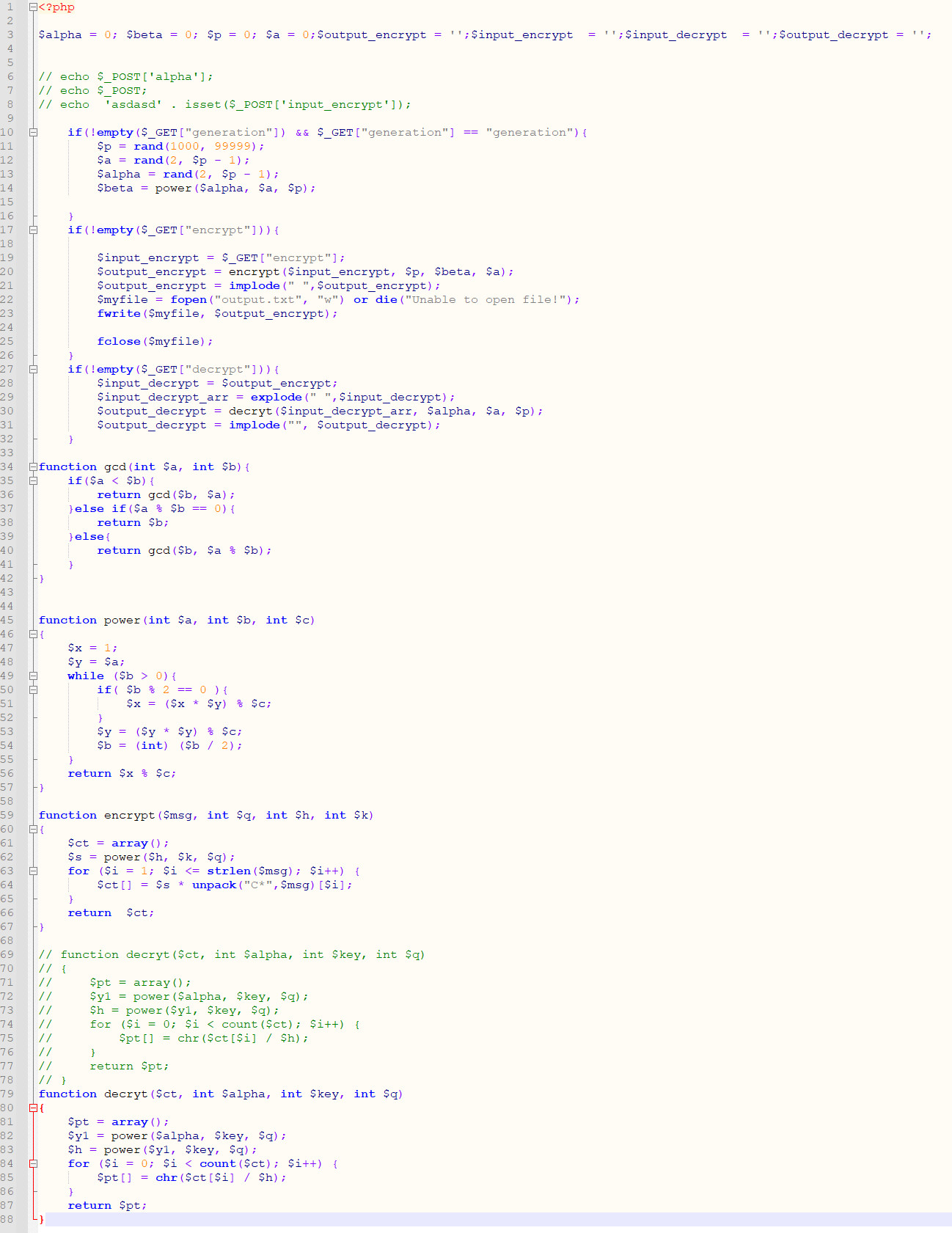






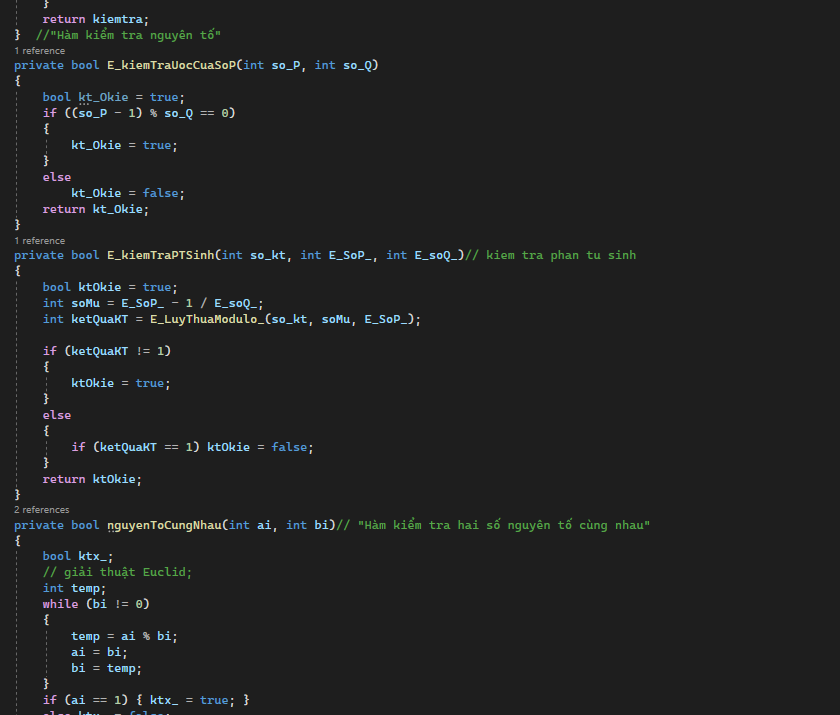
1. **Nguyễn Huy Hoàng – 2019608191**

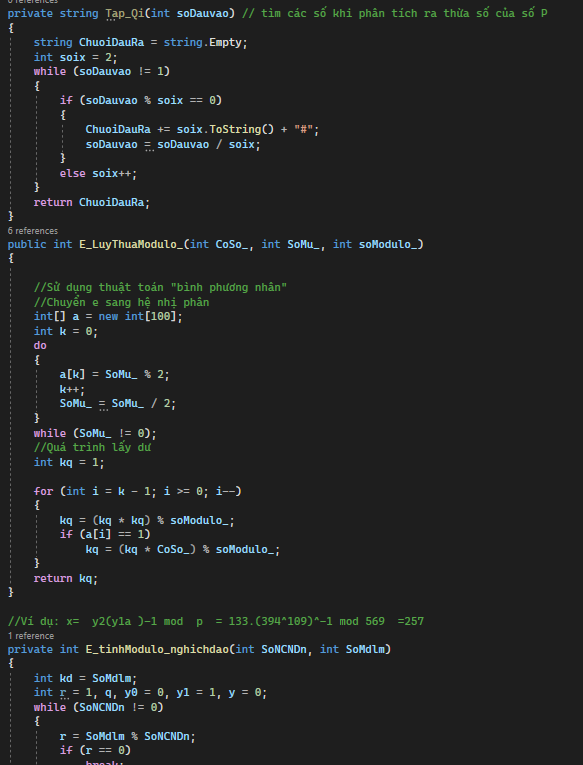
* Viết nội dung chương 2: Tìm hiểu về hệ mã hóa công khai Elgammal.
* Viết chương trình đề mô với ngôn ngữ PHP trên công cụ Visual Studio Code.



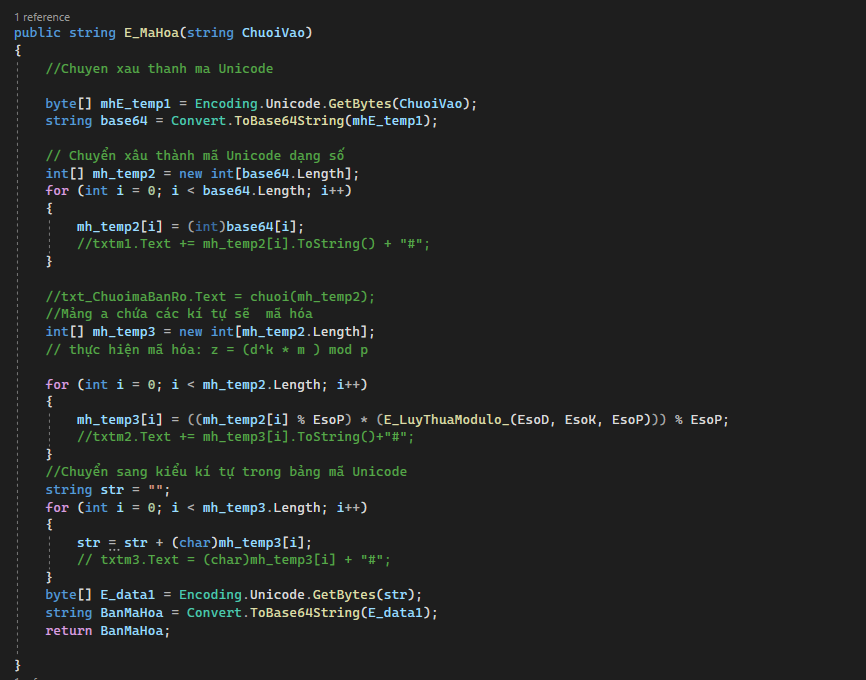
### **Bùi Việt Hoàng – 2019603179**

* Viết nội dung chương 2: Tìm hiểu về hệ mã hóa công khai Elgammal.
* Viết chương trình đề mô với ngôn ngữ Python trên công cụ Visual Studio Code.

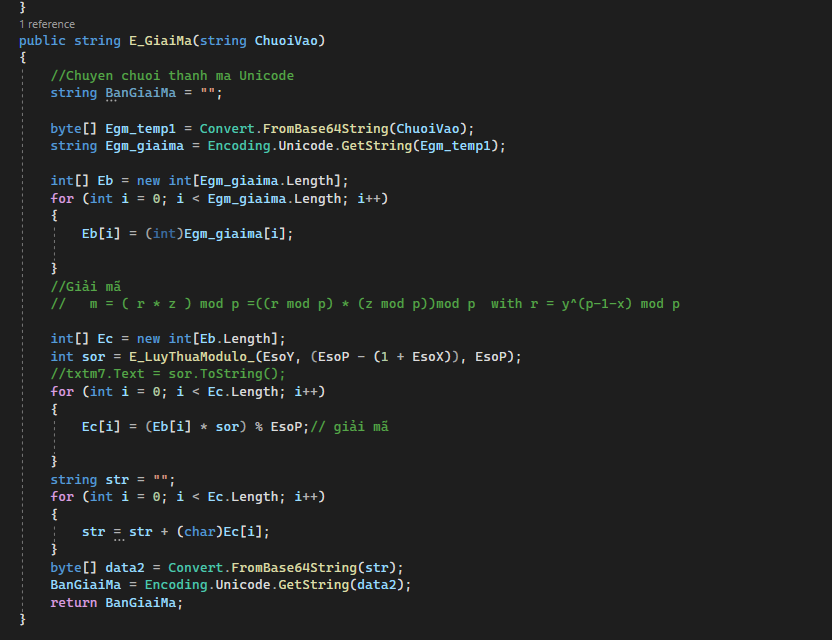




Mã Hóa



Giải mã:



# **CHƯƠNG 3: PHẦN KIẾN THỨC LĨNH HỘI VÀ BÀI HỌC KINH NGHIỆM**

1. **Nội dung đã thực hiện**

Đề tài nghiên cứu về thuật toán mã hóa và giải mã Elgammal và viết ví dụ minh họa, trong đó hệ mã Elgammal được tập trung tìm hiểu bao gồm: cách thức hoạt động, quy trình tạo khóa, quy trình mã hóa, giải mã. Bên cạnh đó, nghiên cứu tìm hiểu về thuật toán eculid mở rộng, thuật toán kiểm tra số nguyên tố, thuật toán bình phương và nhân, đưa ra được những ưu điểm/ nhược điểm của hệ mã hóa khi ứng dụng vào bài toán.

Từ đó có được những kiến thức cần thiết để xây dựng chương trình ứng dụng mã hóa và giải mã Elgammal: Giới thiệu một cách khái quát ứng dụng của thuật toán Elgammal, phương pháp tạo khóa, phương pháp mã hóa, phương pháp giải mã. “Mã hóa và giải mã Elgammal” để thực hiện các quá trình mã hóa và giải mã văn bản.

**Những bài học kinh nghiệm được rút ra sau khi kết thúc bài tập lớn:**

* Nắm được phương pháp mã hóa và giải mã Elgammal.
* Nắm được cách triển khai Elgammal với một số ngôn ngữ: C#, Java, Python, JavaScript, …
* Nắm rõ kỹ năng xác định vấn đề, kĩ năng phân tích vấn đề và sàng lọc ý kiến.
* Nhóm trưởng cần xác định vai trò của từng thành viên, kiểm soát công việc tối ưu nhất và đưa ra những quyết định đúng đắn.
* Xây dựng tiêu chí đánh giá công việc và thái độ làm việc của từng thành viên trong nhóm. Vừa đảm bảo tính khích lệ động viên, vừa đảm bảo tính ràng buộc về trách nhiệm đối với từng thành viên.
* Biết lắng nghe, tôn trọng ý kiến của từng thành viên.
* Đặt tinh thần trách nhiệm trong công việc thành ưu tiên hàng đầu.
* Phát huy sự gắn kết, tạo sự đồng thuận, phân chia công việc hiệu quả, đưa ra cơ chế giải quyết những mâu thuẫn phát sinh trong nhóm.

1. **Hướng phát triển**

Do thời gian nghiên cứu có hạn, nên chương trình đề mô của nhóm em chưa được đầy đủ các chức năng nên mới chỉ thực hiện được các chức năng như: tạo khóa, tạo khóa tự động, mã hóa và giải mã văn bản, đọc file bản rõ/ bản mã và lưu file bản mã mà chưa thiết kế được các chức năng như: đọc file doc, … Nhóm em sẽ tiếp tục nghiên cứu và phát triển các chức năng còn thiếu để hoàn thiện chương trình đề mô của nhóm.

Cuối cùng, với những kết quả đạt được của đề tài nghiên cứu, tuy còn có những hạn chế, nhưng đã giúp chúng em có được khả năng nghiên cứu cơ bản về bảo mật và xác thực thông tin. Từ đó có thể xây dựng các ứng dụng về bảo mật và xác thực thông tin ở những cấp độ an toàn khác nhau.

# **TÀI LIỆU THAM KHẢO**

1. <https://vi.wikipedia.org/wiki/NetBeans>
2. <https://vi.wikipedia.org/wiki/Microsoft_Visual_Studio>