# MỤC LỤC

*Trang*

[MỤC LỤC 1](#_Toc39746896)

[LỜI NÓI ĐẦU 3](#_Toc39746897)

[CHƯƠNG I: GIỚI THIỆU CHUNG VỀ MẬT MÃ VÀ CHỮ KÝ ĐIỆN TỬ 4](#_Toc39746898)

[1.1. Giới thiệu chung về mật mã 4](#_Toc39746899)

[1.1.1. Hệ mã hoá khoá đối xứng 5](#_Toc39746900)

[1.1.2. Hệ mã hoá khoá công khai 5](#_Toc39746901)

[1.1.3. Hệ mã hoá lai 5](#_Toc39746902)

[1.2. Giới thiệu chung về chữ ký điện tử 6](#_Toc39746903)

[CHƯƠNG II: MỘT SỐ LÝ THUYẾT TOÁN HỌC VÀ THUẬT TOÁN 7](#_Toc39746904)

[2.1. Một số lý thuyết toán học 7](#_Toc39746905)

[2.1.1. Số nguyên tố 7](#_Toc39746906)

[2.1.2. Nhóm vòng 7](#_Toc39746907)

[2.1.3. Phép tính đồng dư 7](#_Toc39746908)

[2.1.4. Định lý Fermat 7](#_Toc39746909)

[2.2. Một số thuật toán 7](#_Toc39746910)

[2.2.1. Thuật toán Miller-Rabin 7](#_Toc39746911)

[2.2.2. Thuật toán bình phương và nhân 8](#_Toc39746912)

[2.2.3. Thuật toán Euclid mở rộng 8](#_Toc39746913)

[CHƯƠNG III: HỆ MÃ HOÁ ELGAMAL 9](#_Toc39746914)

[3.1. Giới thiệu về hệ mã hoá Elgamal 9](#_Toc39746915)

[3.2. Hệ mã hoá Elgamal 9](#_Toc39746916)

[3.2.1. Quá trình sinh khoá 9](#_Toc39746917)

[3.2.2. Quá trình mã hoá 9](#_Toc39746918)

[3.2.3. Quá trình giải mã 9](#_Toc39746919)

[3.3. Độ an toàn của hệ mã hoá Elgamal 9](#_Toc39746920)

[3.4. Đánh giá hệ mã hoá Elgamal 10](#_Toc39746921)

[3.4.1. Ưu điểm 10](#_Toc39746922)

[3.4.2. Nhược điểm 10](#_Toc39746923)

[CHƯƠNG IV: CHỮ KÝ ĐIỆN TỬ ELGAMAL 11](#_Toc39746924)

[4.1. Sơ đồ ký Elgamal 11](#_Toc39746925)

[4.1.1. Quá trình tạo khoá 11](#_Toc39746926)

[4.1.2. Quá trình ký 11](#_Toc39746927)

[4.1.3. Quá trình xác nhận chữ ký 11](#_Toc39746928)

[4.2. Độ an toàn của chữ ký Elgamal 11](#_Toc39746929)

[CHƯƠNG V: DEMO 12](#_Toc39746930)

[6.1. Công cụ 12](#_Toc39746931)

[6.2. Chương trình 12](#_Toc39746932)

[6.3. Kết quả 12](#_Toc39746933)

[6.4. Demo 12](#_Toc39746934)

[CHƯƠNG VI: KẾT LUẬN 14](#_Toc39746935)

[CHƯƠNG VII: TÀI LIỆU THAM KHẢO 15](#_Toc39746936)

# LỜI NÓI ĐẦU

Từ xa xưa, nhu cầu sử dụng mật mã đã xuất hiện từ rất sớm, khi con người biết trao đổi và gửi thông tin qua lại cho nhau, đặc biệt là thông tin được thể hiện bằng ngôn ngữ, thư từ. Bắt đầu từ những hệ mã hoá cổ điển như Shift Cipher, Substitution Cipher, … Tuy nhiên, những hệ mã hoá này rất dễ bị phá và không an toàn.

Vào đầu thế kỉ 20, với những tiến bộ liên tục của kỹ thuật tính toán và truyền thông, ngành mật mã cũng đã có những tiến bộ to lớn. Vào những thập niên đầu của thế kỉ, sự phát triển của các kĩ thuật biểu diễn, truyền và xử lý tín hiệu đã có tác động giúp cho các hoạt động lập và giải mật mã từ thủ công chuyển sang cơ giới hoá rồi điện tử hoá.

Ngày nay, các tài liệu văn bản, giấy tờ và các thông tin quan trọng đều được xử lý trên máy tính và được truyền đi trong một môi trường mà mặc định là không an toàn. Do đó, yêu cầu về một cơ chế để đảm bảo tính an toàn và bí mật của thông tin ngày cang trở nên cấp thiết.

Chính vì vậy, nhóm chúng em với sự hướng dẫn của giảng viên TS. Trịnh Viết Cường đã tìm hiểu về “Hệ mã hoá và chữ ký điện tử Elgamal”. Báo cáo cũng như chương trình mô phỏng sẽ không tránh khỏi những thiếu sót, rất mong được sự góp ý chỉ dẫn của thầy!

Chúng em xin chân thành cảm ơn!

# CHƯƠNG I: GIỚI THIỆU CHUNG VỀ MẬT MÃ VÀ CHỮ KÝ ĐIỆN TỬ

## Giới thiệu chung về mật mã

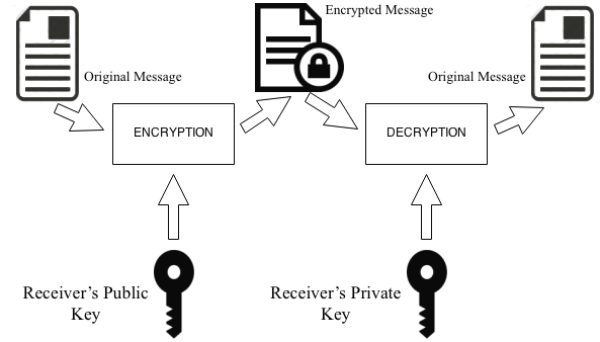
Ta biết rằng tin truyền trên môi trường mạng rất dễ bị lấy cắp. Để đảm bảo việc truyền tin an toàn, người ta thường mã hoá thông tin trước khi truyền đi. Việc mã hoá thường theo quy tắc nhất định gọi là hệ thống mật mã.

Một hệ thống mật mã bao gồm 5 thành phần (P, C, K, E, D) thoả mãn các tính chất sau:

* P – Plain Text: Là tập hợp hữu hạn các bản rõ có thể.
* C – Cipher Text:  Là tập hợp hữu hạn các bản mã có thể.
* K – Key: Là tập hợp các bản khoá có thể.
* E – Encryption:  Là tập hợp các qui tắc mã hoá có thể.
* D – Decryption:  Là tập hợp các qui tắc giải mã có thể.

Quá trình mã hoá được tiến hành bằng cách áp dụng hàm toán học E lên thông tin P, vốn được biểu diễn dưới dạng số để trở thành thông tin mã hoá C.

Quá trình giải mã được tiến hành ngược lại, áp dụng hàm toán học D lên thông tin C để được thông tin đã giải mã P.



*Hình 1: Quá trình mã hoá và giải mã*

### Hệ mã hoá khoá đối xứng

Hệ mã hoá khoá đối xứng – hay còn gọi là hệ mã hoá khoá bí mật: là những hệ mật mã dùng chung một khoá trong cả quá trình mã hoá và giải mã giữ liệu. Do đó khoá phải được giữ bí mật tuyện đối.

Một số hệ mã hoá khoá đối xứng:

* A5/1
* RC4
* DES
* AES
* …

|  |  |
| --- | --- |
| Ưu điểm | Nhược điểm |
| * Tốc độ mã hoá, giải mã nhanh | * Phải thống nhất khoá trước khi sử dụng * Phải lưu trữ nhiều khoá nếu làm việc với nhiều đối tượng |

### Hệ mã hoá khoá công khai

Hệ mã hoá khoá công khai sử dụng một khoá để mã hoá và một khoá khác để giải mã, nghĩa là hai khoá dùng để mã hoá và giải mã là hai khoá khác nhau. Không có khoá nào có thể suy được từ khoá kia. Khoá dùng để mã hoá có thể công khai nhưng khoá dùng để giải mã phải giữ bí mật.

Một số hệ mã hoá khoá công khai:

* RSA
* Elgamal
* Rabin
* …

|  |  |
| --- | --- |
| Ưu điểm | Nhược điểm |
| * Khắc phục được những nhược điểm của hệ mã hoá khoá đối xứng | * Tốc độ mã hoá, giải mã chậm hơn |

### Hệ mã hoá lai

Mô hình của hệ mã hoá lai:

* Dùng hệ mã hoá khoá công khai để mã hoá và giải mã khoá phiên, khoá phiên rất ngắn.
* Dùng hệ mã hoá khoá đối xứng để giải mã dữ liệu cần gửi dưới khoá phiên.
* Ưu điểm:
* Tận dụng ưu điểm của hệ mã hoá khoá công khai và hệ mã hoá khoá đối xứng.
* Dùng hệ mã hoá khoá công khai để mã hoá và giải mã khoá phiên -> dữ liệu bé.
* Dùng hệ mã hoá khoá đối xứng để mã hoá dữ liệu lớn.

## Giới thiệu chung về chữ ký điện tử

Trong cách thức truyền thống, thông báo được truyền đi trong giao dịch thường dưới dạng các văn bản viết tay hoặc đánh máy kèm theo chữ ký tay của người gửi ở bên dưới văn bản. Chữ ký đó dùng để xác thực đúng là của người ký, tức là của chủ thể giao dịch, và nếu tờ giấy mang văn bản không bị cắt, dán, tẩy, xoá thì tính toàn vẹn của thông báo cũng được chứng thực bởi chữ ký đó.

Khi chuyển sang cách thức truyền tin bằng phương tiện hiện đại, các thông báo được truyền đi trên các mạng truyền tin số hoá, bản thân các thông báo cũng được biểu diễn dưới dạng số hoá, tức các dãy nhị phân, “chữ ký” nếu có cũng ở dưới dạng các dãy bit. Chữ ký tay có thể được kiểm thử bằng cách so sánh các bản nguyên mẫu, nhưng chữ ký điện tử thì phải sử dụng những thuật toán đặc biệt để kiểm tra.

Chữ ký điện tử cũng cần đảm bảo các chức năng: xác định được người chủ của một dữ liệu nào đó: văn bản, ảnh, video, ... dữ liệu đó có bị thay đổi hay không.

Một sơ đồ chữ ký gồm có 5 thành phần (P, A, K, S, V):

* P – Tập hữu hạn các bức điện (thông điệp) có thể
* A– Tập hữu hạn các chữ ký có thể
* K – Tập hữu hạn các khóa có thể (không gian khóa)
* S – Tập các thuật toán ký dạng – Sigk : P A
* V – Tập các thuật toán kiểm tra chữ ký dạng – Verk : P x A {true, false}

# CHƯƠNG II: MỘT SỐ LÝ THUYẾT TOÁN HỌC VÀ THUẬT TOÁN

## Một số lý thuyết toán học

### Số nguyên tố

* Số nguyên tố là số nguyên dương lớn hơn một và chỉ có hai ước là một và chính nó.

### Nhóm vòng

* Với số nguyên tố p, xét nhóm Z\*p = {1, 2, …, p - 1}
* Xét 1 < g < p – 1, nếu {g0, g1, …, gp-2} mod p = {1, 2, …, p - 1} thì g được gọi là phần tử sinh của nhóm Z\*p.
* Nhóm Z\*p được gọi là nhóm vòng.

### Phép tính đồng dư

* Cho số nguyên dương n, hai số nguyên: a, b được gọi là đồng dư theo modul n nếu chúng có cùng số dư khi chia cho n.

### Định lý Fermat

* Nếu p là một số nguyên tố và a là một số nguyên tố thì ap ≡ a (mod p).
* Nếu p là một số nguyên tố và a là một số nguyên không chia hết cho p thì ap-1 ≡ 1 (mod p).

## Một số thuật toán

1. Thuật toán Miller-Rabin

* Giả mã:

|  |
| --- |
| Input: n > 2, an odd integer to be tested for primality;  k, a parameter that determines the accuracy of the test  Output: *composite* if n is composite, otherwise *probably* *prime*  write n − 1 as 2s.d with d odd by factoring powers of 2 from n − 1  LOOP: repeat k times:  pick a randomly in the range [2, n − 1]  x ← ad mod n  if x = 1 or x = n − 1 then do next LOOP  for r = 1 ... s − 1  x ← x2 mod n  if x = 1 then return composite  if x = n − 1 then do next LOOP  return *composite*  return *probably prime* |

1. Thuật toán bình phương và nhân

* Giả mã:

|  |
| --- |
| Function Power\_Modulo(Int x,n,m){  Var Int Power:=1  For i=1 to k do  Power:=(Power^2) mod m  If b[i]=1 then  Power:=(Power\*x) mod m  Return Power  } |

1. Thuật toán Euclid mở rộng

* Giả mã:

|  |
| --- |
| Procedure Euclid\_Extended (a,m)  int, y0=0,y1:=1;  While a>0 do {  r:= m mod a  if r=0 then Break  q:= m div a  y:= y0-y1\*q  y0:=y1  y1:=y  m:=a  a:=r  }  If a>1 Then Return "A không khả nghịch theo mođun m"  else Return " Nghịch đảo modulo m của a là y" |

# CHƯƠNG III: HỆ MÃ HOÁ ELGAMAL

## Giới thiệu về hệ mã hoá Elgamal

* Hệ mã hoá Elgamal là một hệ mã hoá khoá công khai.
* Hệ mã hoá Elgamal dựa trên bài toán logarithm rời rạc. Độ an toàn của nó phụ thuộc vào độ phức tạp của bài toán logarithm rời rạc.
* Hệ mã hoá Elgamal là một biến thể của sơ đồ phân phối khoá Diffie-Hellman, được T. Elgamal đề xuất vào năm 1985.

## Hệ mã hoá Elgamal

1. Quá trình sinh khoá

* Chọn p là số nguyên tố lớn sao cho bài toán logarit rời rạc trong Z\*p là “khó giải”.
* Chọn ngẫu nhiên một giá trị 1 ≤ a ≤ p – 2, a là khoá bí mật của người dùng.
* Tìm phần tử sinh g, tính khoá công khai: h ≡ ga mod p.
* Định nghĩa tập khoá: K = {(p, g, a, h): h ≡ ga mod p}. Các giá trị p, g, h được công khai, phải giữ bí mật a.

1. Quá trình mã hoá

* Để mã hoá một thông điệp M (là một số nguyên) thành bản mã C, người gửi sẽ chọn ngẫu nhiên một giá trị k với 1 ≤ k ≤ p – 2 và tính cặp bản mã:

C1

C2

* Bản mã gửi đi gồm C = (C1, C2­).
* Sau khi quá trình mã hoá kết thúc, k sẽ bị huỷ đi.

1. Quá trình giải mã

* Để giải mã bản mã C, sử dụng khoá bí mật của người dùng và giải mã theo công thức:

X

## Độ an toàn của hệ mã hoá Elgamal

* Hệ mã hoá Elgamal áp dụng bài toán logarit rời rạc vì vậy độ an toàn của hệ mã hoá là rất lớn, vì bài toán logarit rời rạc chưa có phương pháp hiệu quả để tính.
* Với một số p đủ lớn, thuật toán mã hoá Elgamal không có phương pháp thám mã hiệu quả.

## Đánh giá hệ mã hoá Elgamal

1. Ưu điểm

* Độ phức tạp của bài toán logarith rời rạc lớn nên độ an toàn cao.
* Bản mã phụ thuộc vào bản rõ M và giá trị ngẫu nhiên nên từ một bản rõ, ta có thể có nhiều bản mã khác nhau.

1. Nhược điểm

* Tốc độ chậm do phải xử lý số nguyên lớn.
* Dung lương bộ nhớ dành cho việc lưu trữ khoá yêu cầu phải lớn.
* Do việc sử dụng các số nguyên tố nên việc sinh khoá và quản lý khoá cũng khó khăn hơn các hệ mã khối.

# CHƯƠNG IV: CHỮ KÝ ĐIỆN TỬ ELGAMAL

## Sơ đồ ký Elgamal

Sơ đồ chữ ký ElGamal được đề xuất năm 1985, gần như đồng thời với sơ đồ hệ mật mã ElGamal, cũng dựa trên độ khó của bài toán lôgarit rời rạc. Sơ đồ được thiết kế đặc biệt cho mục đích ký trên các văn bản điện tử, được mô tả như một hệ:

S = (P, A, K, S, V)

1. Quá trình tạo khoá

* Chọn p là số nguyên tố lớn sao cho bài toán logarit rời rạc trong Z\*p là “khó giải”.
* Chọn ngẫu nhiên một giá trị 1 ≤ a ≤ p – 2, a là khoá bí mật của người dùng và dùng để ký.
* Tìm phần tử sinh g, tính khoá công khai: h ≡ ga mod p

1. Quá trình ký

* Chọn k ngẫu nhiên sao cho: 2 < k < p – 2 và ƯCLN(k, p - 1) = 1
* Tính r = gk mod p
* Tính s = (m – a \* r) \* k-1 mod (p - 1)
* Cặp chữ ký là (r, s)

1. Quá trình xác nhận chữ ký

* Sử dụng khoá công khai h để xác nhận chữ ký.
* Chữ ký hợp lệ nếu:

gm ≡ ga \* r \* rs (mod p)

## Độ an toàn của chữ ký Elgamal

Sơ đồ chữ ký Elgamal được xem là an toàn, nếu việc ký trên một văn bản là không thể giả mạo được, nói cách khác, không thể có một người nào ngoài chủ thể hợp pháp có thể giả mạo chữ ký của chủ thể hợp pháp đó trên một văn bản bất kỳ. Vì vậy, việc giữ bí mật a khoá dùng để tạo chữ ký là có ý nghĩa quyết định đối với việc bảo đảm tính an toàn của chữ ký.

# CHƯƠNG V: DEMO

1. **Công cụ**

* Bộ Microsoft Visual Studio
* Ngôn ngữ lập trình C#
* Windows Form Application

1. **Chương trình**

* Hệ mã hoá và chữ ký Elgamal đều dựa trên số nguyên tố lớn: 1024 và 2048 bits.
* Ngoài hệ mã hoá và chữ ký Elgamal, chương trình còn có hệ mã hoá và chữ ký RSA.

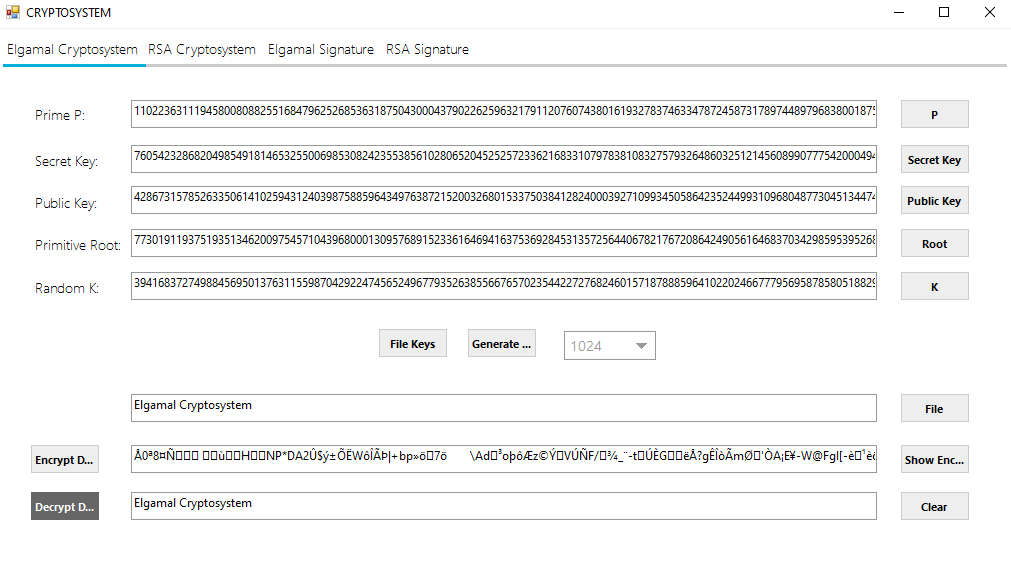
1. **Kết quả**

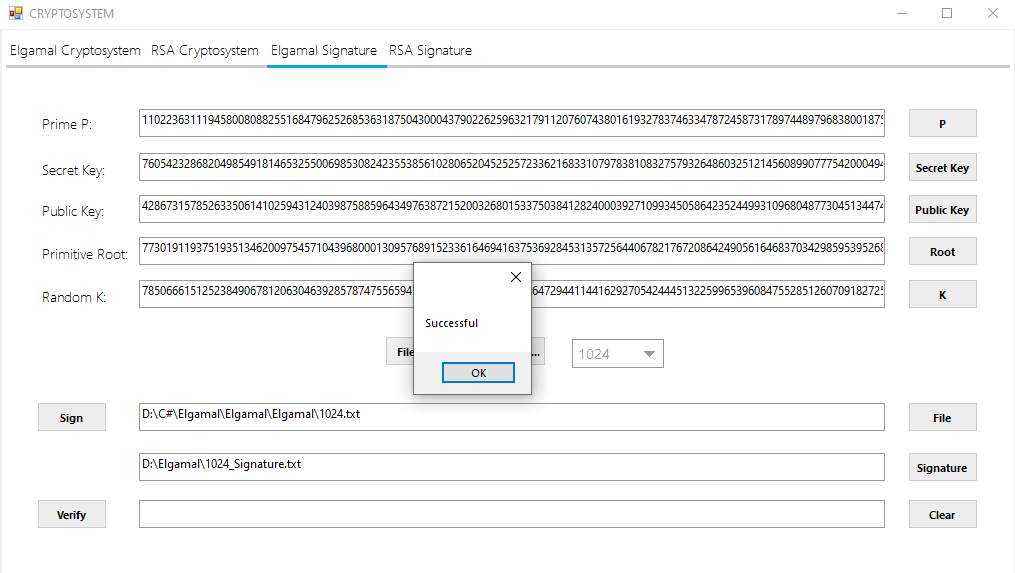
* Đạt được:
* Xây dựng thành công hệ mã hoá và chữ ký Elgamal với số lớn.
* Thao tác với file.
* Chưa đạt được:
* Tốc độ mã hoá và ký những file với kích thước lớn chậm.
* Chưa tối ưu được thuật toán tìm phần tử sinh.

1. **Demo**



*Hình 2. Giao diện chương trình*

*Hình 3. Mã hoá và giải mã*

**

*Hình 4. Ký và kiểm tra chữ ký*

# CHƯƠNG VI: KẾT LUẬN

Bảo mật an toàn thông tin là điều mà con người luôn mong muốn từ khi mà công nghệ đã phát triển một cách vượt bậc ở nước ta và trên cả toàn thế giới. Cho đến hiện nay thì nhờ có hệ mã hóa mà các thông tin và các dữ liệu của chúng ta có thể trao đổi với mọi người một cách an toàn nhất.

Qua lần làm bài tập và dựa trên mục đích của lần làm bài tập này, đã giúp chúng em hiểu được phần kiến thức sâu hơn về các hệ mã hóa, đặc biệt là hệ mã hoá và chữ ký điện tử Elgamal. Rõ hơn về các mục đích sử dụng của hệ mã và ký, quá trình mã hoá một file và quá trình thực hiện ký một chữ ký.

Trong thời gian làm bài tập nhóm cùng thầy và các bạn, chúng em đã học hỏi được nhiều rất nhiều kinh nghiệm để giúp cải thiện kỹ năng lập trình cho từng cá nhân. Nắm vững và sâu hơn về hệ mã hóa nói riêng và bảo mật thông tin nói chung; Bước đầu cũng được làm quen với công việc nghiên cứu. Chúng em cũng hiểu rằng đây là nền tảng ban đầu để giúp chúng em rất nhiều trên con đường học tập và nghiên cứu sau này.

# CHƯƠNG VII: TÀI LIỆU THAM KHẢO

[1] Bài giảng an toàn và bảo mật thông tin - Trần Minh Văn – Đại học Nha Trang

[2] Elgamal Encryption - Wikipedia

[3] Elgamal Signature Scheme - Wikipedia

[4] Digital Signatures: ElGamal Signature Scheme and Digital Signature Algorithm (and Birthday Attacks). Link: <https://www.commonlounge.com/discussion/35a1c2baa00b447f9275e8f71b02ef29>