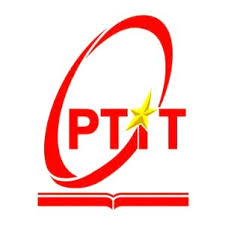
**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA VIỄN THÔNG 1**

-----🙞🙜🕮🙞🙜-----



**BÀI TIỂU LUẬN**

**ĐỀ TÀI: HỆ MẬT MÃ ELGAMAL**

**Giảng viên: TS. PHẠM ANH THƯ**

**Sinh viên: Nhóm 1**

**Lớp: AN NINH MẠNG THÔNG TIN NHÓM 3**

|  |  |
| --- | --- |
| Nguyền Hữu Phi | B17DCVT276 |
| Nguyễn Tiến Giáp | B17DCVT107 |
| Phùng Quốc Duy | B17DCVT100 |
| Vũ Chí Hiếu | B17DCVT137 |
| Phạm Đình Huấn | B17DCVT153 |

*Hà Nội, ngày 18 tháng 04 năm 2021*

**MỤC LỤC**

[**PHẦN 1: GIỚI THIỆU HỆ MẬT MÃ ELGAMAL** 4](#_Toc69676455)

[**1.1 Giới thiệu chung về hệ mật mã** 4](#_Toc69676456)

[**1.2 Hệ mật mã Elgamal** 5](#_Toc69676457)

[**PHẦN 2: TẠO KHÓA TRONG ELGAMAL** 6](#_Toc69676458)

[**2.1 Quá trình tạo khóa** 6](#_Toc69676459)

[**2.2 Mã hóa thông điệp** 6](#_Toc69676460)

[**PHẦN 3: MÃ HÓA VÀ GIẢI MÃ ELGAMAL** 7](#_Toc69676461)

[**3.1 Mã hóa** 7](#_Toc69676462)

[**3.2 Giải mã** 7](#_Toc69676463)

[**3.3 Ví dụ** 7](#_Toc69676464)

[**PHẦN 4: THÁM MÃ ELGAMAL** 9](#_Toc69676465)

[**4.1 Tìm hiểu về thám mã** 9](#_Toc69676466)

[**4.1.1 Thám mã là gì?** 9](#_Toc69676467)

[**4.1.2 Để thám mã hệ Egamal ta cần phải giải bài toán Logarit rời rạc** 9](#_Toc69676468)

[**4.2 Thuật toán Shank trong thám mã hệ Elgamal** 9](#_Toc69676469)

[**4.3 Ví dụ** 9](#_Toc69676470)

[**PHẦN 5: ỨNG DỤNG CỦA HỆ MẬT MÃ ELGAMAL** 11](#_Toc69676471)

[**5.1. Một số ứng dụng điển hình.** 11](#_Toc69676472)

[**5.2. Ứng dụng Email an toàn sử dụng hệ mật mã Elgamal** 11](#_Toc69676473)

[**5.2.2. Những tin nhắn nhận.** 11](#_Toc69676474)

[**5.2.3. Gửi tin nhắn** 13](#_Toc69676475)

[**5.3. Một số ứng dụng khác.** 14](#_Toc69676476)

[**Tài liệu tham khảo** 15](#_Toc69676477)

**Mục lục hình ảnh**.............................................................................................................................15

# **PHẦN 1: GIỚI THIỆU HỆ MẬT MÃ ELGAMAL**

## **1.1 Giới thiệu chung về hệ mật mã**

- Để đảm bảo việc truyền tin được an toàn, người ta thường mã hóa thông tin trước khi truyền đi .

Việc mã hóa được tuân theo quy tắc được gọi là hệ thống mã hóa

* Một hệ thống mật mã gồm ***5 thành phần (P,C,K,E,D)*** thỏa mãn tính chất

+, ***P (Plaintext)*** là tập hợp hữu hạn các bản rõ có thể

+, ***C (Ciphertext)*** là tập hợp hữu hạn các bản mã có thể

+, ***K (Key)*** là tập hợp các bản khóa có thể

+, ***E (Encrytion)*** là tập hợp các quy tắc mã hóa có thể

+, ***D (Decrytion)*** là tập hợp các quy tắc bản giải mã có thể

* ***Quá trình mã hóa***được tiến hành bằng cách áp dụng hàm toán học E lên thông tin P, được biểu diễn ban đầu dưới dạng số, được mã hóa thành bản mã C .
* ***Quá trình giải mã***được tiến hành ngược lại: sử dụng hàm D lên bản mã C để thu được thông tin đã giải mã
* ***Thám mã (phá mã )*** là tìm những điểm yếu hoặc không an toàn trong phương thức mật mã hóa. Thám mã có thể được thực hiện bởi những kẻ tấn công ác ý, nhằm làm hỏng hệ thống hoặc những người thiết kế ra hệ thống với mục đích đánh giá độ an toàn của hệ thống
* ***Hệ mật mã gồm*** :

***Hệ mật mã đối xứng (hay còn gọi là mật mã khóa bí mật)*** : là những hệ mật mã dùng chung một khóa trong quá trình mã hóa dữ liệu và giải mã dữ liệu

***Hệ mật mã bất đối xứng (hay còn gọi là khóa công khai )*** : Các hệ mật mã này dùng một khóa để mã hóa sau đó dùng một khóa khác để giải mã . Các khóa này tạo nên từng cặp chuyển đổi ngược nhau và không khoá nào có thể suy ngược lại khóa kia .

## **1.2 Hệ mật mã Elgamal**

*-* ***Mã hóa Elgamal được đưa ra bởi Taher Elgamal năm 1985***

*-* ***Mã hóa gồm 3 thuật toán:***

+ Thuật toán khởi tạo bộ khóa

+ Thuật toán mã hóa Elgamal

+ Thuật toán giải mã Elgamal

* ***Hệ Elgamal là:***

+ Hệ mật mã hóa công khai (hệ mật mã hóa bất đối xứng)

+ Dựa trên bài toán logarithm rời rạc và tính an toàn phụ thuộc vào độ phức tạp của bài toán

+ Là một biến thể của phân phối khóa Diffie-Hellmal

+ So với RSA, Hệ Elgamal không có nhiều rắc rối về vấn đề sử dụng

* ***Ý tưởng :***

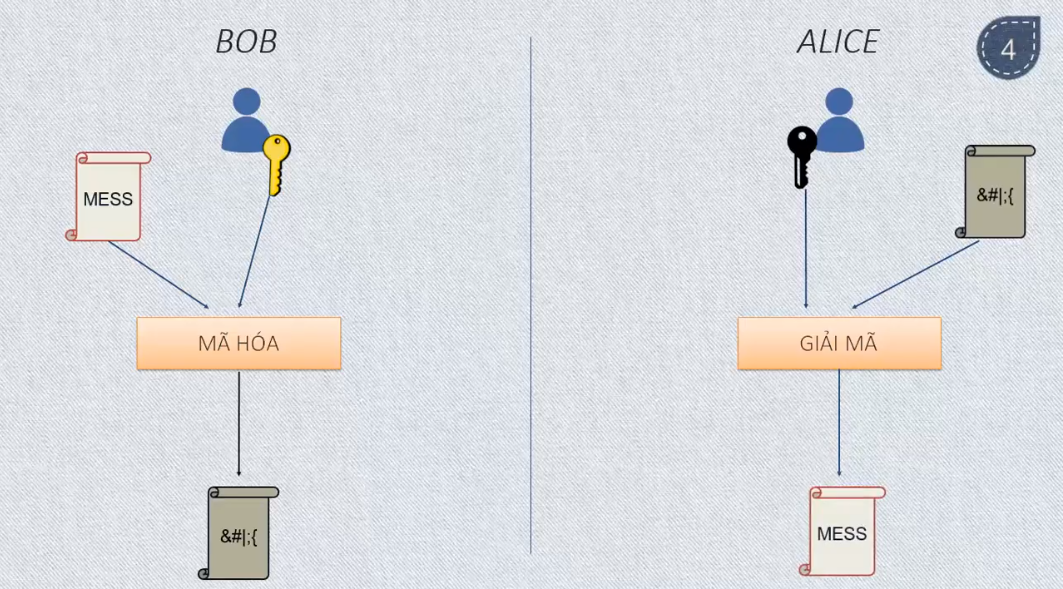
+ ***Tạo khóa***: Alice tạo 2 khóa bao gồm Public Key và Private Key

+ ***Gửi Public Key***: Alice gửi Public Key cho Bob

+ ***Mã hóa thông điệp***: Bob nhận Public Key và mã hóa thông điệp

+ ***Gửi thông điệp***: Bob gửi thông điệp đã mã hóa cho Alice

+ ***Giải mã thông điệp***: Alice nhận thông điệp và giải mã bằng Private Key



# **PHẦN 2: TẠO KHÓA TRONG ELGAMAL**

## **2.1 Quá trình tạo khóa**

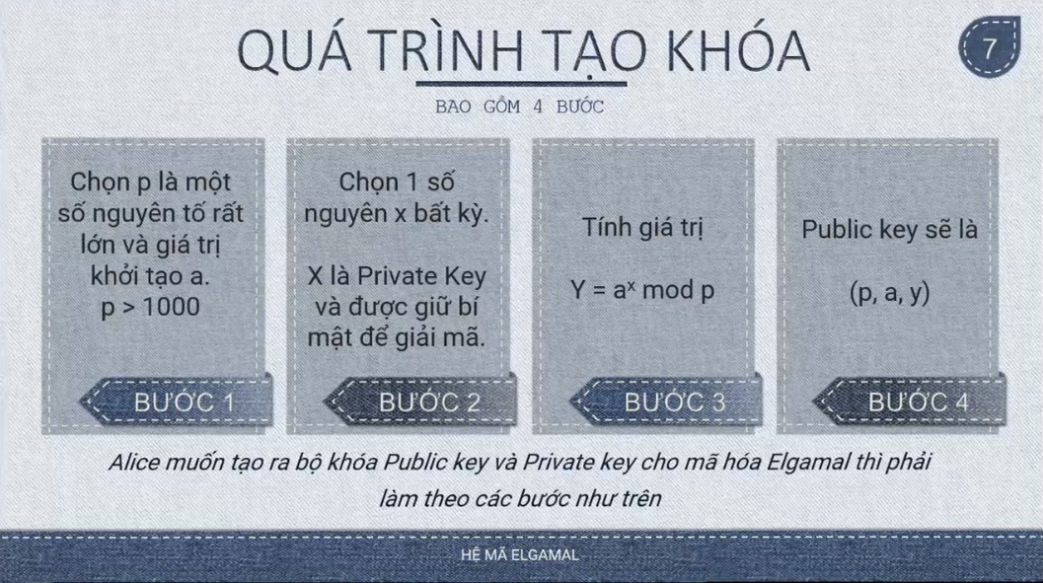
- ***Bao gồm 4 bước:***

+ Chọn p là một số nguyên tố rất lớn và giá trị khởi tạo a

+ Chọn x là một số nguyên bất kì, x là private key và được giữ bí mật để giải mã

+ Tính y = a^x mod p

+ ***Public Key*** sẽ là (p,a,y)



**2.2 Mã hóa thông điệp**

***Sau khi tạo khóa, Alice gửi public key cho Bob. Bob dùng khóa này để mã hóa thông điệp gửi cho Alice***

****

# **PHẦN 3: MÃ HÓA VÀ GIẢI MÃ ELGAMAL**

## **3.1 Mã hóa**

Ban đầu người ta sẽ lựa chọn **một số nguyên tố lớn p** và **hai số nguyên tố nhỏ hơn p là a và x (khóa bí mật của người nhận)** sau đó tính khóa công khai :

Để mã hóa **một thông điệp M (một số nguyên tố trên Zp)** thành **bản mã C** người gửi chọn **một số ngẫu nhiên k nhỏ hơn p** và tính cặp mã:

Bản mã **E(** được gửi đi với:

Sau đó k sẽ bị hủy đi

## 

## **3.2 Giải mã**

* Thành phần khóa công khai:
* Thành phần khóa bí mật:

## **3.3. Ví dụ**

Cho hệ Elgamal có **p = 2579, a = 2, x= 765**; chọn **k** ngẫu nhiên là **853**. Bản rõ **M = 1299**. Tìm khóa của hệ mật mã trên?

**Giải**

**Mã hóa:**

Trước hết ta tính được:

Để mã hóa thông điệp **M = 1299 ta tính theo k = 853:**

Vậy bản mã được gửi đi sẽ là **C = (435, 2396)**

**Giải mã:**

Với khóa bí mật **x = 765**:

**Kết luận:**

Xây dựng được hệ mã Elgamal bộ khóa:

Thành phần khóa công khai:

Thành phần khóa bí mật:

Mã hóa **M = 1299** với **E( = (435, 2396)**

# **PHẦN 4: THÁM MÃ ELGAMAL**

## **4.1 Tìm hiểu về thám mã**

### **4.1.1 Thám mã là gì?**

Thám mã (phá mã) là tìm những điểm yếu trong phương thức mật mã hóa, được thực hiện bởi những kẻ tấn công

### **4.1.2 Để thám mã hệ Egamal ta cần phải giải bài toán Logarit rời rạc**

*Bài toán: Tìm 1 số mũ x duy nhất (0<=x<=p-2) sao cho y=a^x mod p*

Có 2 thuật toán để giải bài toán này

* Thuật toán Shank
* Thuật toán Pohlig Hellman

Trong nội dung bài thuyết trình, nhóm trình bày về thuật toán Shank.

### **4.2 Thuật toán Shank trong thám mã hệ Elgamal**

* Người thám mã chỉ có khóa công khai Ku (p,a,y)
* Cần tìm ra giá trị x (khóa bí mật) thỏa mãn y = a^x mod p (0<=x<=p-2)
* Các bước của thuật toán:

Tính m = [(p-1)1/2]

B1: Tính a­mjmod p với 0<=j<=m-1

B2: Sắp xếp các cặp (j, amj mod p) và lưu vào danh sách L1

B3: Tính y\*a-i mod p với 0<=i<=m-1

B4: Sắp xếp các cặp (i, y\*a-i mod p) và lưu vào danh sách L2

B5: Tìm cặp thỏa mãn **amj mod p = y\*a-i mod p** danh sách L1, L2 để lấy giá trị i,j

B6: Tính x=log­ay=(mj+i) mod (p-1)

## **4.3 Ví dụ**

**- Khi biết giá trị khóa công khai**

**(p,a,y) = (17,3,13)**

**m=4**

* **Ta tính được giá trị trong 2 bảng L1, L2**

Bảng L1

|  |  |
| --- | --- |
| j | a­mjmod p |
| 0 | 1 |
| 1 | 13 |
| 2 | 16 |
| 3 | 4 |

Bảng L2

|  |  |
| --- | --- |
| i | y\*a-i mod p |
| 0 | 13 |
| 1 | 13/3 |
| 2 | 13/9 |
| 3 | 13/27 |

Từ bảng L1, L2 ta có **a­mjmod p** = **y\*a-i mod p** = 13 tại **j=1** và **i=0**

* **x = (mj+i) mod (p-1) = 4**
* Nhận xét:
* Tính an toàn của hệ Elgamal phụ thuộc vào độ phức tạp của bài toán Logarit
* Bài toán Logarit chưa có phương pháp hiệu quả => Hệ Elgamal có độ an toàn cao
* Với 1 số p đủ lớn gần như không có phương pháp thám mã hiệu quả

Ngoài ra, nếu dùng phương pháp vét cạn (tức là duyệt tất cả các phần tử x) để tìm x thỏa mãn) thì độ phức tạp của bài toán là O(p) => mất thời gian lớn => không khả thi (nếu dùng thuật toán Shank thì độ phức tạp của bài toán là O ([p-1]^0.5]), với p lớn thì cũng không có hiệu quả)

# **PHẦN 5: ỨNG DỤNG CỦA HỆ MẬT MÃ ELGAMAL**

## **5.1 Một số ứng dụng điển hình**

* Chữ kí điện tử.

Đối với các thông tin có bản quyền, hoặc trong vấn đề xác nhận chủ thể, tác giả thường ký số bằng **chữ ký điện tử** lên đó. Mục đích của chữ ký điện tử không phải là che dấu dữ liệu, mà nó quan tâm đến nguồn gốc dữ liệu. Phải nói thêm là **chữ ký số** chỉ là một trường hợp riêng của chữ ký điện tử, tuy nhiên trong thực tế chúng thường được dùng với cùng một ý nghĩa. Đảm bảo bản quyền phần mềm, đảm bảo giao dịch liên ngân hàng,...

* Giao dịch điện tử.

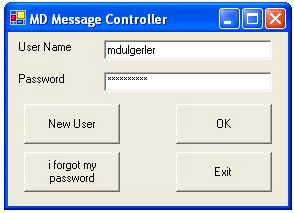
Ứng dụng quan trọng của mã hóa, ký số trong thông tin giao tiếp ngày nay là đảm bảo giao dịch trên mạng.

## **5.2 Ứng dụng Email an toàn sử dụng hệ mật mã Elgamal**

Chương trình cung cấp độ bảo mật cao trong các quy trình đăng nhập và ngăn chặn việc truy cập trái phép của những người dùng không tin cậy, sử dụng thuật toán băm trong quá trình lưu mật khẩu vào cơ sở dữ liệu.

**5.2.1 Khởi động chương trình**

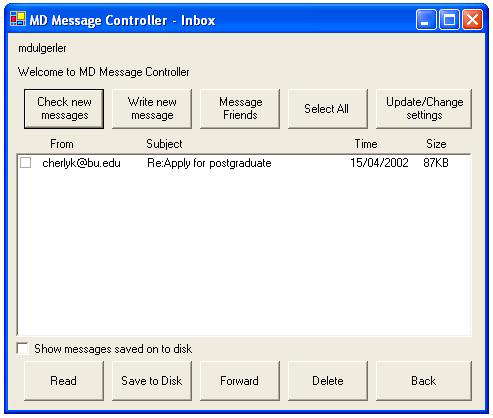
Khi chương trình được chạy, 1 cửa sổ đăng nhập của người dùng được hiện ra. Người dùng sẽ nhập username và password vào form đăng nhập A (Hình 2)



Hình 2: User Login Window

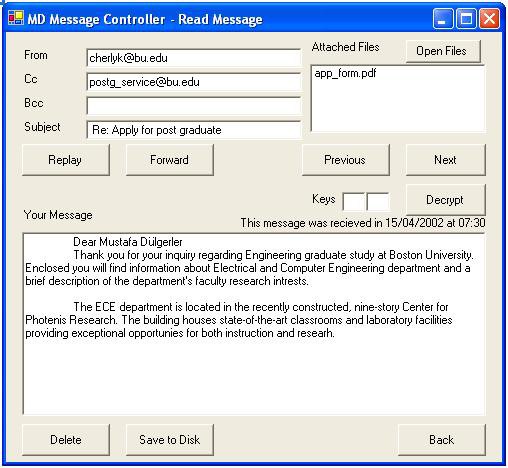
### **5.2.2 Những tin nhắn nhận**

Các email được gửi đọc từ máy chủ sau đó được liệt kê ở hình 3.



Hình 3: Cửa sổ tin nhắn nhận được

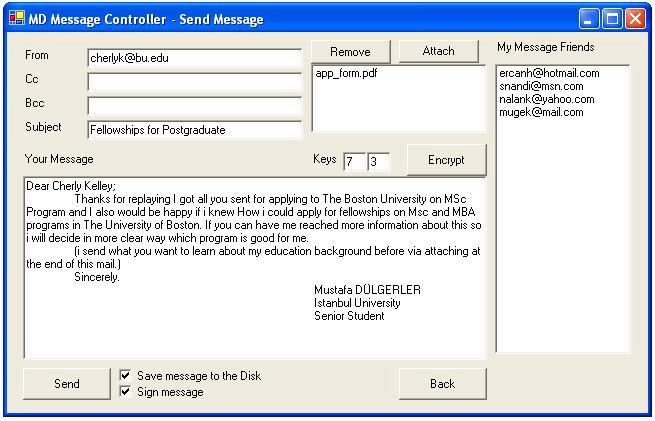
Nếu người dùng muốn đọc 1 trong các email được liệt kê, người dùng có thể nhấn nút “Read” trên biểu mẫu hoặc nhấn đúp chuột vào chủ đề của email (hình 4).



Hình 4: Cửa sổ đọc tin nhắn

Nếu email được gửi từ 1 người dùng xác thực, ở dạng mã hóa, email có thể được giải mã bằng cách nhấp vào nút “DECRYPT” trên mẫu tin nhắn đã đọc.

### 5.2.3 Gửi tin nhắn

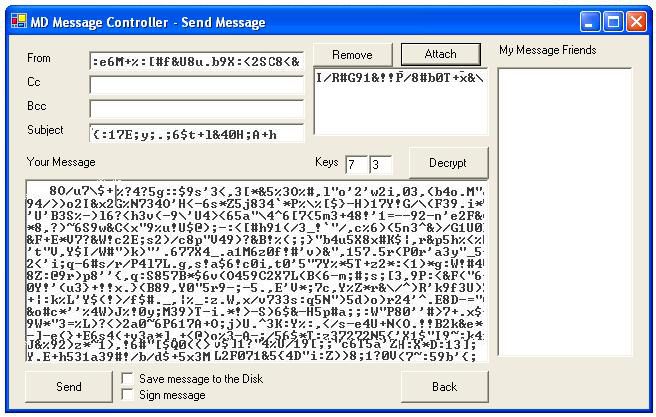


Hình 5: Cửa sổ gửi tin nhắn

Khi tin nhắn đã được gửi, nếu nút “ENCRYPT” được click, tin nhắn sẽ được mã hóa bằng thuật toán ElGamal, click tiếp tục vào nút “SENT”, tin nhắn được mã hóa được gửi đến người nhận (hình 5).

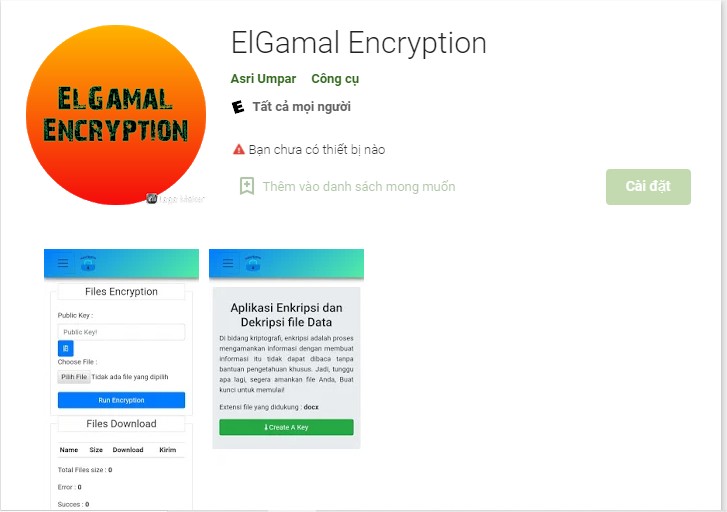
Hai giá trị của 2 chìa khóa phải được xác định để tạo mã khóa.





*Hình 6: Mật mã hóa tin nhắn*

## 5.3 Một số ứng dụng khác



Hình 7: Một số ứng dụng khác

Ứng dụng cho phép mã hóa các tập tin bằng hệ mật mã Elgamal.

Trang web mật mã hóa thông tin bằng hệ mật mã Elgamal

# **Tài liệu tham khảo**

1. Thành phố Đà Lạt, Đề tài: “Hệ thống mật mã Elgamal”, Trường đại học Đà Lạt, 21/05/2016.
2. Thơm Hồ Thị Hương, “AN TOÀN BẢO MẬT THÔNG TIN”, 14/03/2020.

# **Mục lục hình ảnh**

[Hình 1: Hệ thống mật mã elgamal 4](#_Toc69675513)

[Hình 2: User Login Window 11](#_Toc69675514)

[Hình 3: Cửa sổ tin nhắn nhận được 12](#_Toc69675515)

[Hình 4: Cửa sổ đọc tin nhắn 12](#_Toc69675516)

[Hình 5: Cửa sổ gửi tin nhắn 13](#_Toc69675517)

[Hình 6: Mật mã hóa tin nhắn 14](#_Toc69675518)

[Hình 7: Một số ứng dụng khác 14](#_Toc69675519)