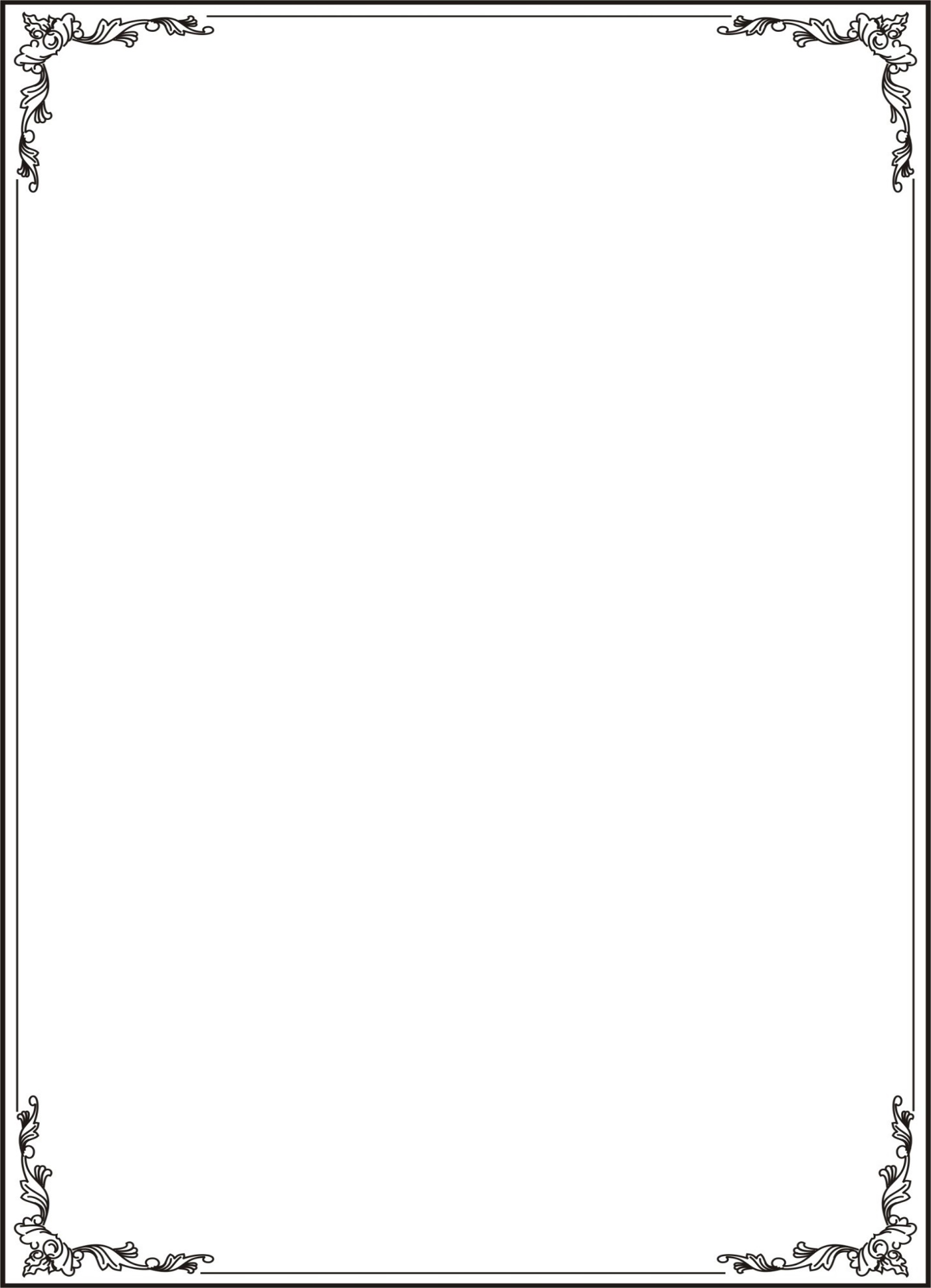
**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**

**KHOA CÔNG NGHỆ THÔNG TIN**

∙∙∙🙞🙜🕮🙞🙜∙∙∙

**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**

****

**BÁO CÁO THỰC NGHIỆM**

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

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

**Giảng viên: Trần Phương Nhung**

**Nhóm sinh viên thực hiện: Nhóm 6**

**1.**

**2.**

**3.**

**4.**

**5.**

**Hà Nội, 2021**

# **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 cô!

Mục lục

[**LỜI MỞ ĐẦU** 2](#_Toc104504661)

[**Chương 1:Tổng quan hệ mã hóa ElGamal** 4](#_Toc104504662)

[1.1 Tổng quan hệ mã 4](#_Toc104504663)

[1.2 Thiết kế sơ đồ khối 4](#_Toc104504664)

[1.3 Mô tả 5](#_Toc104504665)

[1.4 Tạo khóa 5](#_Toc104504666)

[1.5 Mã hóa 5](#_Toc104504667)

[1.6 Giải mã 5](#_Toc104504668)

[1.7 Tính bảo mật của hệ mật mã Elgamal 6](#_Toc104504669)

[1.8 Ưu điểm và nhược điểm của hệ mã Elgamal 6](#_Toc104504670)

# **Chương 1:Tổng quan hệ mã hóa ElGamal**

## 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

Bản rõ m

Tạo khóa

Lập mã

Bản rõ c

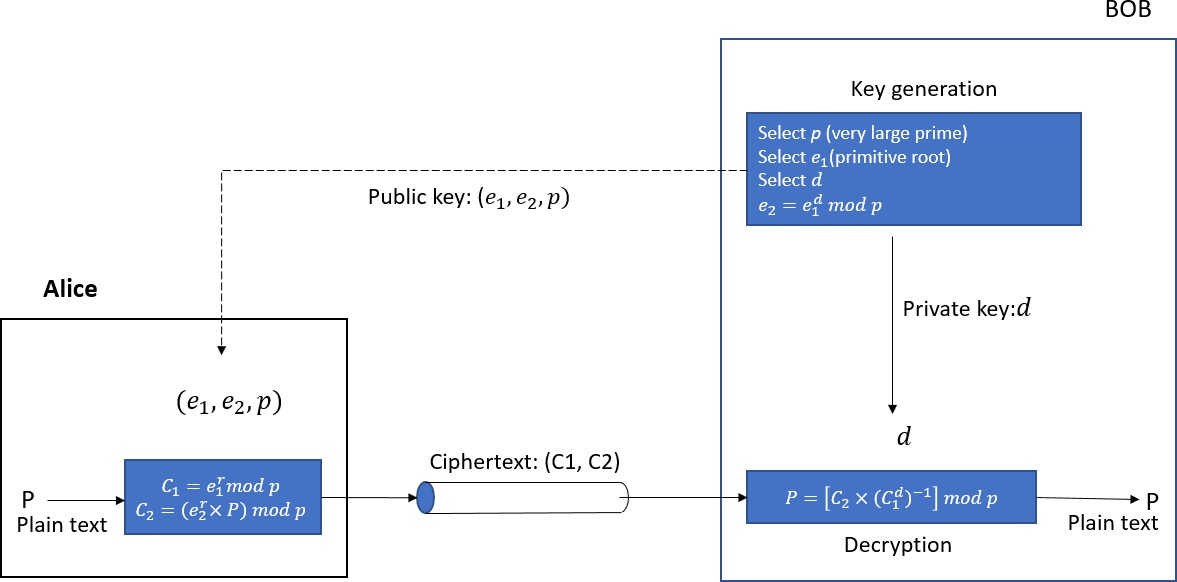
Giải mã

Bản rõ m

## 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:



## 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>

Tính d2 =d1d 𝑚𝑜𝑑 𝑝

1. Khóa công khai sẽ là (d1,d2,𝑝)

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

Alice sẽ có bản mã gồm (𝐶1,𝐶 2) để gửi đến cho Bob.

## Giải mã

Bob nhận được bản mã (𝐶1,𝐶 2) và có khóa bị mật 𝑑 khi đó Bob sẽ tìm được bản rõ theo công thức: [𝐶2 \* (𝐶a)−1] 𝑚𝑜𝑑 𝑝 .

1

## 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.

## 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