Họ và tên: Lê Thị Bảo Yến

MSSV: 0850080057

Lớp: 0850080057

**BÁO CÁO CÁ NHÂN**

**ĐỘ AN TOÀN CỦA HỆ CHỮ KÝ ELGAMAL**

1. **Hệ chữ ký Elgamal là gì?**
   1. Tổng quan

* Hệ chữ ký ElGamal được xây dựng trên nền tảng hệ mã khóa công khai ElGamal và sử dụng cùng một bộ khóa công khai và khóa bí mật. Hệ mã khóa công khai ElGamal sử dụng tính toán đường cong Elliptic (ECC) để mã hóa và giải mã thông điệp.
* Hệ chữ ký ElGamal hoạt động bằng cách sử dụng một cặp khóa: khóa riêng (private key) và khóa công khai (public key). Khóa riêng được sử dụng để ký và khóa công khai được sử dụng để xác minh chữ ký. Các bước để tạo và xác minh một chữ ký ElGamal bao gồm:
* Tạo khóa: Người dùng tạo cặp khóa ElGamal (khóa riêng và khóa công khai).
* Ký thông điệp: Người dùng sử dụng khóa riêng để tạo chữ ký cho thông điệp.
* Xác minh chữ ký: Người nhận sử dụng khóa công khai của người ký để xác minh tính hợp lệ của chữ ký.
* Hệ chữ ký ElGamal được sử dụng rộng rãi trong các ứng dụng an ninh mạng để bảo vệ tính toàn vẹn và độ tin cậy của các thông điệp và giao dịch truyền qua mạng.
  1. So sánh với các hệ mã hóa khác
* RSA: là một trong những thuật toán mã hóa khóa công khai được sử dụng phổ biến. RSA có tốc độ xử lý cao hơn hệ ElGamal, tuy nhiên cùng một kích thước khóa, RSA yêu cầu số bit đầu vào lớn hơn làm tăng chi phí lưu trữ khóa.
* Diffie-Hellman: là một thuật toán trao đổi khóa được sử dụng để thiết lập một khóa chung giữa hai bên trong hệ mã hóa khóa công khai, tương tự như hệ ElGamal. Tuy nhiên, hệ ElGamal có khả năng chống lại tấn công theo kiểu sinh từ mạnh hơn hệ Diffie-Hellman.
* ECC: là một hệ mã hóa khóa công khai mới, có thể sử dụng khóa ngắn hơn so với RSA hoặc ElGamal với cùng mức độ bảo mật. Hệ mã hóa này cũng cung cấp khả năng bảo mật cao hơn khi sử dụng khóa ngắn hơn.

1. **Cách tạo chữ ký số trong hệ thống ElGamal**
   1. Tạo khóa

* Chọn p là 1 số nguyên tố rất lớn (>1024 bit) và giá trị khởi tạo g.
* Chọn một số nguyên x làm khóa bí mật, sử dụng để kí với 0<x<p
* Tính giá trị y = g^x mod p
* Ta sẽ có cặp khóa là: Public key (p, g, y) và Private key (x)

Sau khi có cặp khóa, người dùng có thể sử dụng khóa riêng để ký các thông điệp và khóa công khai để xác minh chữ ký.

* 1. Tạo chữ ký

Người dùng muốn ký một thông điệp message sẽ thực hiện các bước sau :

* Nhập thông điệp là message, chuyển đổi message về dạng chuỗi thập lục phân và sử dụng băm.
* Chọn một số ngẫu nhiên k, với 0 < k < p - 1
* Tính r = g^k mod p.
* Tính s = (message - x\*r) \* k^-1 mod (p-1).
* Chữ ký là cặp (r, s).
  1. Xác minh chữ ký

Người nhận thông điệp đã băm là message và chữ ký sẽ thực hiện các bước sau để xác minh chữ ký :

* Tính v1 = g^ message mod p.
* Tính v2 = (y^r mod p) \* ((r^s mod p) mod p).
* Nếu v1 = v2, chữ ký được xác minh là hợp lệ.

1. **DEMO**

