**BÁO CÁO BÀI TẬP LỚN**

**Chương trình chữ ký điện tử Elgama (Sử dụng ngôn ngữ C++, C#)**

**CHƯƠNG 1: GIỚI THIỆU**

**1.1 Đặt vấn đề**

Chữ ký điện tử là một công cụ quan trọng trong lĩnh vực bảo mật và an toàn thông tin, giúp xác thực nguồn gốc, đảm bảo tính toàn vẹn và chống chối bỏ trong giao dịch điện tử. Trong thời đại số hóa, nhu cầu sử dụng chữ ký điện tử ngày càng trở nên phổ biến trong các lĩnh vực như tài chính, thương mại, y tế, và giáo dục.

Elgama là một thuật toán chữ ký số dựa trên các nguyên lý của toán học và mật mã học, đặc biệt là các khái niệm về số nguyên tố và tính modulo. Khác với các hệ mã như RSA, Elgama có những đặc điểm vượt trội về tốc độ tính toán và bảo mật trong nhiều trường hợp.

**1.2 Mục tiêu đề tài**

* Xây dựng chương trình chữ ký điện tử Elgama bằng ngôn ngữ lập trình C++ và C#.
* Tìm hiểu các khái niệm liên quan đến chữ ký điện tử và thuật toán Elgama.
* Ứng dụng thuật toán trong việc tạo, ký và xác minh chữ ký điện tử.
* Đánh giá hiệu năng và độ bảo mật của hệ thống.

**1.3 Phạm vi nghiên cứu**

* Tìm hiểu các khái niệm cơ bản: số nguyên tố, modulo, hàm Euler, và các định lý cơ bản trong mật mã.
* Xây dựng chương trình mẫu mô phỏng chữ ký điện tử Elgama.
* Thực hiện kiểm thử chương trình trên các bộ dữ liệu khác nhau để đánh giá hiệu quả hoạt động.

**1.4 Phương pháp thực hiện**

* Nghiên cứu tài liệu lý thuyết về mật mã học và chữ ký điện tử.
* Thiết kế và lập trình chương trình chữ ký điện tử Elgama.
* Tiến hành kiểm thử và phân tích kết quả.
* Tổng hợp và viết báo cáo hoàn chỉnh.

**CHƯƠNG 2: CƠ SỞ LÝ THUYẾT**

**2.1 Tổng quan về chữ ký điện tử**

* **Khái niệm:**  
  Chữ ký điện tử là một chuỗi dữ liệu điện tử được tạo ra để xác thực danh tính của người ký và bảo vệ tính toàn vẹn của tài liệu số.
* **Chức năng:**
  + Xác thực nguồn gốc: Đảm bảo tài liệu được gửi từ đúng người ký.
  + Bảo vệ tính toàn vẹn: Phát hiện mọi thay đổi trái phép trong tài liệu.
  + Chống chối bỏ: Ngăn người ký phủ nhận việc ký tài liệu.

**2.2 Thuật toán Elgama**

* **Nguyên lý hoạt động:**  
  Thuật toán Elgama dựa trên bài toán logarit rời rạc, một bài toán khó giải trong mật mã học.
* **Các bước chính:**
  1. **Tạo khóa:**
     + Chọn một số nguyên tố lớn ppp.
     + Chọn một số nguyên ggg thỏa mãn 1<g<p1 < g < p1<g<p.
     + Chọn một số nguyên xxx (khóa bí mật), 1<x<p−11 < x < p-11<x<p−1.
     + Tính y=gxmod  py = g^x \mod py=gxmodp (khóa công khai).
  2. **Ký tài liệu:**
     + Chọn một số nguyên kkk ngẫu nhiên thỏa mãn 1<k<p−11 < k < p-11<k<p−1 và gcd(k,p−1)=1\text{gcd}(k, p-1) = 1gcd(k,p−1)=1.
     + Tính r=gkmod  pr = g^k \mod pr=gkmodp.
     + Tính s=k−1(H(m)−xr)mod  (p−1)s = k^{-1}(H(m) - xr) \mod (p-1)s=k−1(H(m)−xr)mod(p−1), trong đó H(m)H(m)H(m) là hàm băm của tài liệu mmm.
  3. **Xác minh chữ ký:**
     + Kiểm tra tính đúng đắn: gH(m)mod  p=yr⋅rsmod  pg^{H(m)} \mod p = y^r \cdot r^s \mod pgH(m)modp=yr⋅rsmodp.

**2.3 Đặc điểm của Elgama**

* **Ưu điểm:**
  + Dựa trên bài toán khó giải, đảm bảo độ bảo mật cao.
  + Hiệu quả trong việc tạo và xác minh chữ ký.
* **Nhược điểm:**
  + Cần số nguyên tố lớn để đảm bảo an toàn.
  + Cần tính toán số mũ lớn, dẫn đến tiêu tốn tài nguyên trong một số trường hợp.

**2.4 So sánh Elgama và RSA**

