Nhập môn mã hóa mật mã
Bài tập nhóm 1

Ngày 21 tháng 11 năm 2022

1 Lý thuyết

Trong mật mã học, việc kiểm tra một số tự nhiên n có phải số nguyên tố hay không rất quan trọng và được sử dụng thường xuyên. Phương pháp đơn giản và dễ thực hiện nhất là kiểm tra xem n có chia hết cho các số tự nhiên từ 2 đến $n-1$ hay không, nhưng cách này lại rất tốn thời gian và không phù hợp khi n rất lớn (từ 2048 bits trở lên). Nhiều phương pháp kiểm tra số nguyên tố đã được tạo ra nhằm cải thiện thời gian kiểm thử, trong phần này, các bạn sinh viên được yêu cầu tìm hiểu và so sánh các phương pháp đó.

Yêu cầu

1. Tìm hiểu về các phương pháp sau:
   - Phép kiểm tra tính nguyên tố của Fermat.
   - Phép kiểm tra tính nguyên tố của Miller-Rabin.

   Phần tìm hiểu phải chỉ ra được các phương pháp trên thực hiện việc kiểm tra như thế nào, độ phức tạp trên lý thuyết của thuật toán, và thuật toán dựa trên các định lý nào.
2. So sánh về độ phức tạp và tính đúng đắn của các thuật toán ở trên.

2 Thực hành

Kích thước khóa đóng vai trò quan trọng trong việc đảm bảo tính an toàn của hệ mã RSA. Trong thực tế, từ 2015, NIST đã đưa ra khuyến cáo về kích thước khóa tối thiểu của RSA là 2048 bits[1]. Trong phần này, các bạn sinh viên cần cài đặt chương trình sinh khóa cho thuật toán mã hóa RSA với độ dài khóa cho trước và đưa ra đánh giá về độ phức tạp cũng như thời gian vận hành của chương trình. Ngoài ra, trong quá trình sinh số nguyên tố, cần sử dụng 1 trong 2 thuật toán kiểm tra số nguyên tố đã tìm hiểu ở trên.

Yêu cầu

1. Cài đặt: *Sử dụng ngôn ngữ C/C++, không dùng thư viện hỗ trợ lưu trữ/tính toán số nguyên lớn*
   - Cài đặt 1 trong 2 thuật toán kiểm tra số nguyên tố trong phần Lý thuyết.
   - Cài đặt chương trình sinh khóa cho thuật toán mã hóa RSA. Chương trình cần cho phép người dùng chọn 1 trong 3 độ dài khóa là 512 bits, 1024 bits và 2048 bits.
2. Báo cáo:
   - Đánh giá ưu/nhược điểm và thời gian thực hiện của thuật toán kiểm tra số nguyên tố đã cài đặt.

[1] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf

- Báo cáo chi tiết về chương trình sinh khóa đã cài đặt, bao gồm:
  - Cách chạy chương trình
  - Thiết kế chương trình, cách lưu và tính toán số nguyên lớn, các sinh số nguyên tố lớn tương ứng với từng độ dài khóa.
  - Thời gian thực hiện, ưu/nhược điểm của chương trình đã cài đặt.

3 Các quy định nộp bài

3.1 Các quy định chung

1. Sinh viên cần nộp đầy đủ các thành phần sau:
   - File báo cáo đồ án: report.pdf
   - Thư mục chứa mã nguồn chương trình: source
   - Trong thư mục source, cần có file README.TXT hướng dẫn chi tiết cách chạy chương trình.
2. Đồ án được thực hiện trong 2 tuần.
3. Đồ án làm theo nhóm đã đăng ký.
4. Phần nộp bài (do trưởng nhóm đại diện nộp) sẽ gồm có 2 phần là mã nguồn (lưu trong thư mục Source) và báo cáo (lưu trong thư mục Report), được nén thành 1 file bằng định dạng ZIP có tên dạng như sau: MSSV01_MSSV02_MSSV03_MSSV04_MSSV05.zip (với nhóm có 5 thành viên).

3.2 Mã nguồn

1. Mã nguồn không thể biên dịch (báo lỗi biên dịch như sai cú pháp) hoặc không thể chạy được (báo các lỗi như lỗi runtime, sai logic chương trình) sẽ không được tính điểm.
2. Các hành vi gian lận liên quan đến mã nguồn (sao chép mã nguồn giữa các nhóm, sao chép mã nguồn trên Internet, ...) sẽ bị 0 điểm cả bài tập.

3.3 Báo cáo

Phần báo cáo tối thiểu cần có các câu trả lời cho những yêu cầu đã nêu trong đề bài. Các hành vi sao chép giữa các nhóm, sao chép nội dung trên mạng hoặc sao chép nội dung tiếng Anh rồi dịch sang tiếng Việt đều không được phép, trừ những nội dung lý thuyết như mã giả thuật toán được yêu cầu tìm hiểu, định lý, hệ quả liên quan.

Hết