

Vấn đề kiểm tra số nguyên tố lớn

Học viên: Trương Công Quyền
chuyên ngành Hệ thống thông tin,
khoa Công nghệ thông tin
email congquyenhv85@gmail.com

Giáo viên hướng dẫn: PGS.TS. Trịnh Nhật Tiến
Cơ quan công tác: Khoa Công nghệ thông tin – Trường
Đại học Công nghệ - Đại học Quốc gia Hà Nội
Email tientn@vnu.edu.vn

I. CHƯƠNG 1 – CÁC KHÁI NIỆM CƠ BẢN

- A. Ký hiệu và Khái niệm.
- B. Thuật toán nghịch đảo.
- C. Thuật toán phân tích một số ra thừa số nguyên tố.
- D. Số học các số nguyên, thuật toán EUCLID.
- E. E. Độ phức tạp tính toán.

II. CHƯƠNG 2 – SỐ NGUYÊN TỐ VÀ MỘT SỐ PHƯƠNG PHÁP KIỂM TRA SỐ NGUYÊN TỐ

- A. Số nguyên tố.
- B. Các số nguyên tố có dạng đặc biệt.
- C. Một số phương pháp kiểm tra số nguyên tố.

III. CHƯƠNG 3 – MỘT SỐ ỨNG DỤNG CỦA SỐ NGUYÊN TỐ

- A. Mã hóa.
- B. Ký số.

IV. CHƯƠNG 4 – THỬ NGHIỆM CHƯƠNG TRÌNH

- A. Cấu hình hệ thống cho chương trình.
- B. Chương trình.

V. KẾT LUẬN

- A. Kết quả đạt được

Tìm hiểu số nguyên tố và các phương pháp kiểm tra số nguyên tố.

Tìm hiểu các ứng dụng số nguyên tố lớn.

Xây dựng thử nghiệm chương trình với các chức năng sau: kiểm tra số nguyên tố lớn bằng phương pháp Fermat, kiểm tra số nguyên tố lớn bằng phương pháp Miller-Rabin.

B. Hướng phát triển

Cải tiến các phương pháp đã có, nghiên cứu đưa ra các phương pháp mới.

TÀI LIỆU THAM KHẢO

- [1] PGS. TS. Trịnh Nhật Tiến (2009), *Bài giảng cao học: An ninh Cơ sở dữ liệu*, ĐH Công nghệ, ĐHQG HN.
- [2] PGS. TS. Trịnh Nhật Tiến (2008), *Giáo trình: An toàn dữ liệu*, ĐH Công nghệ, ĐHQG HN.
- [3] Nguyễn Văn Ba (2006), *Lý thuyết ngôn ngữ và tính toán*, NXB ĐHQG HN.
- [4] Phan Đình Diệu (2006), *Lý thuyết mật mã và An toàn thông tin*, NXB ĐHQG HN.
- [5] Nguyễn Xuân Dũng (2007), *Bảo mật thông tin mô hình & ứng dụng*, NXB Thống kê.
- [6] Bùi Doãn Khanh, Nguyễn Đình Thúc, Trần Đan Thư (2007), *Cơ sở lý thuyết số trong an toàn - bảo mật thông tin*, NXB Giáo dục.
- [7] Hà Huy Khoái, Phạm Huy Điển (2003), *Số học thuật toán: Cơ sở lý thuyết và tính toán thực hành*, NXB ĐHQG HN.
- [8] Hà Huy Khoái, Phạm Huy Điển (2004), *Mã hóa thông tin: Cơ sở toán học và ứng dụng*, NXB ĐHQG HN.
- [9] Manindra Agrawal (2005), "Primality tests based on Fermat's little theorem", *Department of CS, Indian Institute of Technology, Kanpur*.
- [10] Manindra Agrawal, Neeraj Kayal, Nitin Saxena (2004), "PRIMES is in P", *Ann. of Math.*, (2), 160(2): 781-793.
- [11] R. Crandall, Carl Pomerance (2001), "Prime Numbers: A Computational Perspective", *Springer-Verlag*, New York, 2001.
- [12] R. Crandall and J. Papadopoulos (2003), "On the implementation of AKS-class primality tests", Technical paper, Apple Advanced Computation Group.