

## **Môn học Thực tập cơ sở**

### **Bài 16: Lập trình thuật toán mật mã học**

#### ***1.1 Mục đích***

Sinh viên tìm hiểu một giải thuật mã hóa phổ biến và lập trình được chương trình mã hóa và giải mã sử dụng ngôn ngữ lập trình phổ biến như C/C++/Python/Java, đáp ứng chạy được với số lớn.

#### ***1.2 Nội dung thực hành***

##### ***1.2.1 Tìm hiểu lý thuyết***

- Tìm hiểu về lập trình số lớn với các phép toán cơ bản
- Tìm hiểu về giải thuật mật mã khóa công khai RSA

##### ***1.2.2 Chuẩn bị môi trường***

- Môi trường lập trình theo mong muốn.

##### ***1.2.3 Các bước thực hiện và kết quả cần đạt***

#### ***a) Các bước thực hiện***

- Lập trình thư viện số lớn với các phép toán cơ bản để sử dụng trong giải thuật mã hóa/giải mã RSA
- Thử nghiệm chứng minh thư viện hoạt động tốt với các ví dụ phép toán cho số lớn
- Lập trình giải thuật mã hóa và giải mã
- Thử nghiệm mã hóa và giải mã chuỗi ký tự: “I am <mã sinh viên>” (thay bằng mã sinh viên của mình vào)

#### ***b) Kết quả cần đạt được***

- Chạy thành công các bước
- Minh chứng
  - Chụp lại các ảnh trong các kết quả cần đạt được

- Chụp lại code các phần đã lập trình (cho vào phụ lục)
- Các minh ảnh chứng cần có thông tin Mã sinh viên và họ tên sinh viên xuất hiện trong trang quản lý đào tạo.

### ***1.3 Yêu cầu đối với file báo cáo***

- File báo cáo dưới dạng pdf được trình bày rõ ràng theo cấu trúc: trang bìa, mục lục, các phần lý thuyết và thực hành riêng, tài liệu tham khảo nếu có. Báo cáo được đánh số trang trừ trang bìa.
- Đặt tên file theo định dạng kiểu như sau: *Bài thực hành 16\_Họ tên SV\_Mã SV*