BÀI THỰC HÀNH SỐ 2

Bài 1. Cài đặt thuật toán mã hóa RSA

* Tạo menu hoặc giao diện để người sử dụng chọn các chức năng.
  + Nhâp thông điệp cần mã hóa
  + Tạo khóa bí mật và khóa công khai
  + Tiến hành mã hóa thông điệp đã nhập
  + Tiến hành xác thực thông điệp
  + Giải mã bản mã để thu được bản rõ ban đầu.
  + Giải mã thông điệp xác thực để thu được bản rõ ban đầu.

Bài 2. Cài đặt thuật toán trao đổi khóa Diffie Hellman

* Tạo menu hoặc giao diện để người sử dụng chọn các chức năng.
  + Nhập số nguyên tố q rồi tính căn nguyên thủy của q
  + Tính khóa công khai của bên gửi và bên nhận
  + Tính khóa bí mật của bên gửi và bên nhận
  + HIển thị khóa bí mật K lên màn hình