

Tên: Nguyễn Việt Thanh Duy

MSSV: 19127378

## **Báo cáo cài đặt chương trình tạo mã RSA**

### **1. Thông tin chung:**

- Chương trình được viết bằng ngôn ngữ C++14, lập trình trên VS Code, sử dụng hệ điều hành Windows 10.
- Chương trình chạy tốt ( $\leq 60s$ ) cho **length(N) = 128** bit, với  $N = p \times q$  ( $p, q$  là số nguyên tố 64 bit).
- Các input và output của chương trình là số nguyên dưới dạng Hex.

### **2. Mô tả 1 số hàm quan trọng trong RSA:**

#### ❖ Hàm genKey:

- Đầu vào: truyền tham chiếu các biến chứa khoá công khai  $e$ , khoá bí mật  $d$  và số nguyên  $n$ .
- Đầu ra: không có.
- Chức năng: Tìm và gán giá trị tương ứng cho các biến được truyền vào.
- Lưu ý: có thể điều chỉnh số bit của  $p$  và  $q$  thông qua giá trị khởi tạo của biến bits được khai báo trong hàm.

#### ❖ Hàm Encrypt:

- Đầu vào: bản rõ  $m$ , khoá công khai  $e$  và số nguyên  $n$ .
- Đầu ra: bản mã  $c$ .
- Chức năng: mã hoá.

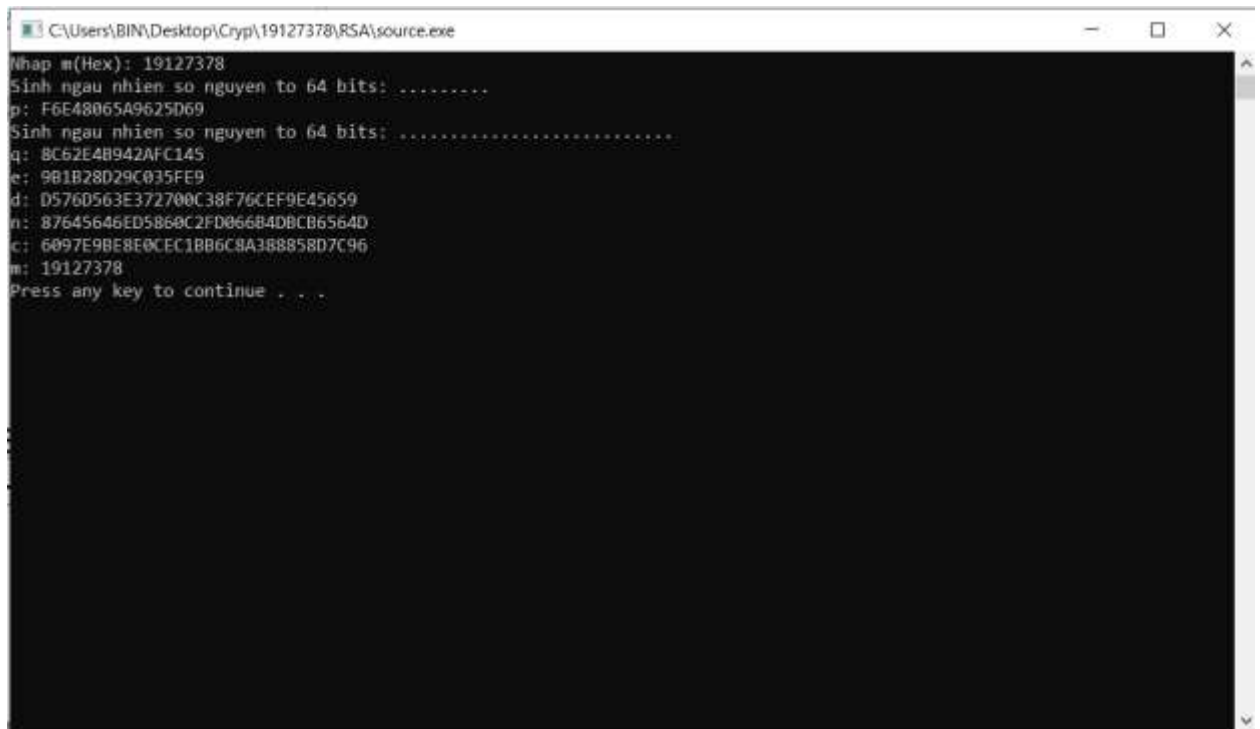
#### ❖ Hàm Decrypt:

- Đầu vào: bản mã  $c$ , khoá bí mật  $d$  và số nguyên  $n$ .
- Đầu ra: bản rõ  $m$ .
- Chức năng: giải mã.

### **3. Hướng dẫn chạy chương trình:**

- Bước 1: Nhập bản rõ  $m$  cần mã hoá dưới dạng Hex:
  - Chỉ bao gồm các kí tự: 0...9, A...F
  - $m < n$  ( $\text{length}(m) < 128$  bit)
- Bước 2: Đợi chương trình xử lý và xuất ra các thông số của mã RSA luân lượt theo thứ tự:
  - Số nguyên tố  $p$
  - Số nguyên tố  $q$
  - Khoá công khai  $e$
  - Khoá bí mật  $d$
  - Số tự nhiên  $n$
  - Bản mã  $c$
  - Bản rõ  $m$  (để kiểm tra xem mã RSA sinh ra có hoạt động đúng hay không)

- Bước 3: Nhấn nút bất kì để kết thúc chương trình.
- Hình ảnh ví dụ:



```
C:\Users\BIN\Desktop\Cryp\19127378\RSA\source.exe
Nhap m(Hex): 19127378
Sinh ngau nhien so nguyen to 64 bits: .....
p: F6E48065A9625D69
Sinh ngau nhien so nguyen to 64 bits: .....
q: 8C62E4B942AFC145
e: 9B1B28D29C035FE9
d: D576D563E372700C38F76CEF9E45659
n: 87645646ED5860C2FD06684DBC6564D
c: 6097E9BE8E0CEC1BB6C8A388858D7C96
m: 19127378
Press any key to continue . . .
```