**公钥密码实现程序**

**1、编程训练目的**

密码学就是研究数据加密与解密算法的学科。传统的密码学已经有很悠久的历史了，而1976年公钥密码体系的诞生使得密码学得到了迅速的发展，并在网络中获得了广泛的应用。目前，一般通过加密与解密、身份确认、数字签名等方法来保证信息存储与传输的安全。

本作业编程训练的目的，通过实现自己的加密解密程序，从而对密码学的相关知识，尤其是数据加密解密的流程有一个初步的了解。

**2、编程训练要求**

实现一个RSA加密算法。具体要求如下:

(1)能够加密指定字符串并对加密后的密文进行解密，并与源字符串进行比对，证明解密无误;

(2)必须输出加密相关的各项参数,如公钥、私钥，通过乘积构成大整数的两个素数等;

(3)图1为程序运行示意图。

**3、程序及文档提交要求**

编写《程序设计说明》，包括模块设计、核心代码的实现说明，必要的流程图，要求清晰明了，文档格式可自行设计。

提交时，将程序代码和《程序设计说明》打包压缩，命名格式：“学号-姓名-RSA程序实现”，在截止日期前提交至网盘（具体看助教要求）。

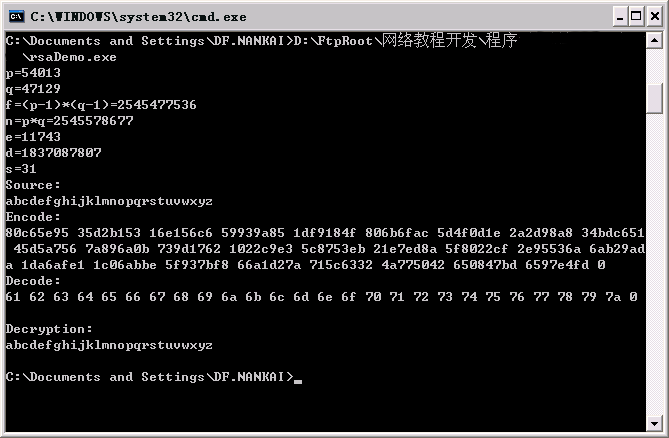


图1 程序运行示意图