《信息安全引论》选做实验一

实验： 实现 RSA 算法

实验内容

实现 RSA 算法，具有以下功能：

1. 随机生成公钥与私钥。
2. 给出明文，计算出密文。
3. 给出密文，解密出明文。

实现过程中可以参考 openssl 等实现，并使用任意的数学计算库。例如，一种可能的简单实现方式如下：

```
from Crypto.Util.number import getPrime
import gmpy2

p, q = getPrime(1024), getPrime(1024)
N = p * q
e = 0x10001

d = gmpy2.invert(e,(p-1)*(q-1))

c = int(input('c:')) # 密文

m = pow(c,d, N) # 计算明文
```

实验环境

可以使用 python 等任意高级语言编写。

实验要求

- 完整实现要求中的三个功能，并给出使用随机生成的密钥对自己学号（如"2000011111"）的加密结果。
- 需要提交源代码文件与必要的文档，简要解释说明关键的步骤。

提交方式

请把实验的内容打包成一个文件夹，压缩并命名为：学号+姓名+实验作业.zip 。