**信息与网络安全**

**课程设计报告**

学院：信息科学与技术学院

班级：计科1403

姓名：杨磊

学号：2013011013

2017年6月17日

## 说明

5个算法全部实现，其中 Vigenere和RSA算法未借助第三方库手工完成！

编程语言：

Python 2.7

需要使用pip安装的库

pycrypto==2.6.1

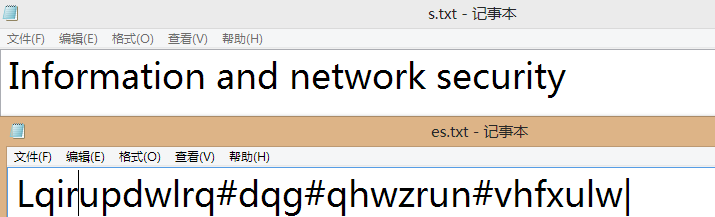
pyDes==2.0.1

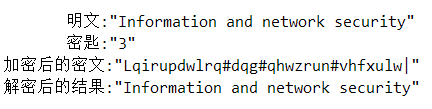
## Vigenere密码算法

#### 代码



#### 结果



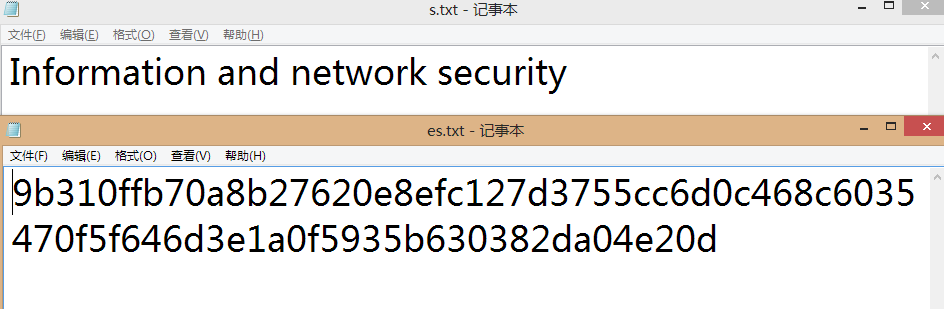


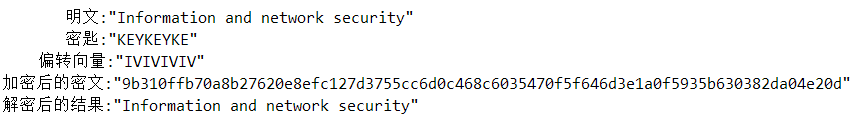
## DES对称密码算法

#### 代码



#### 结果



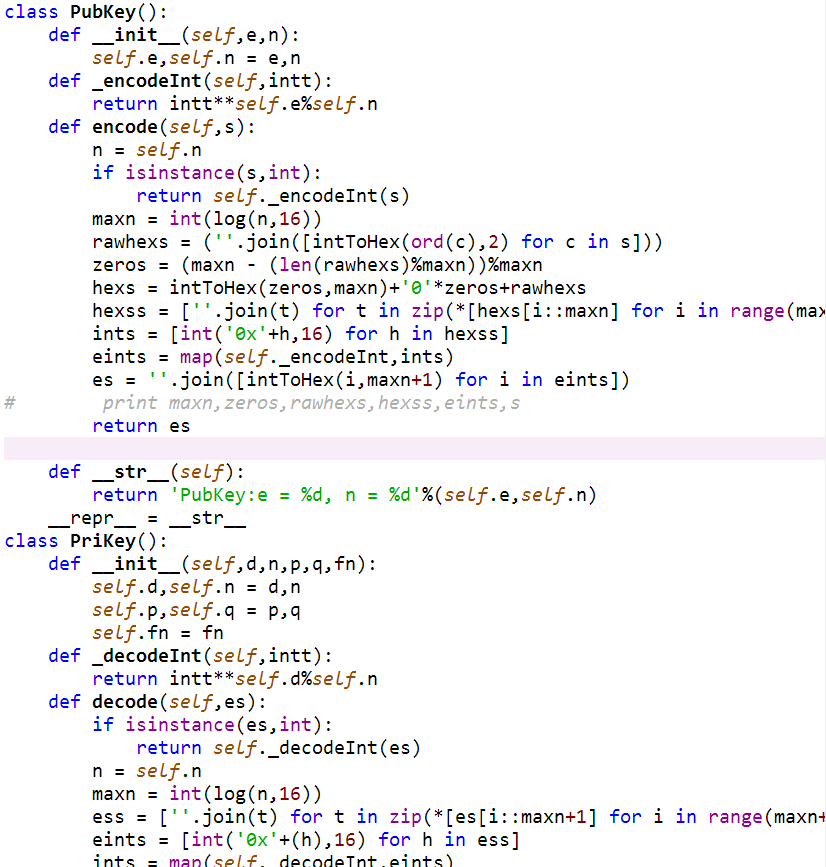


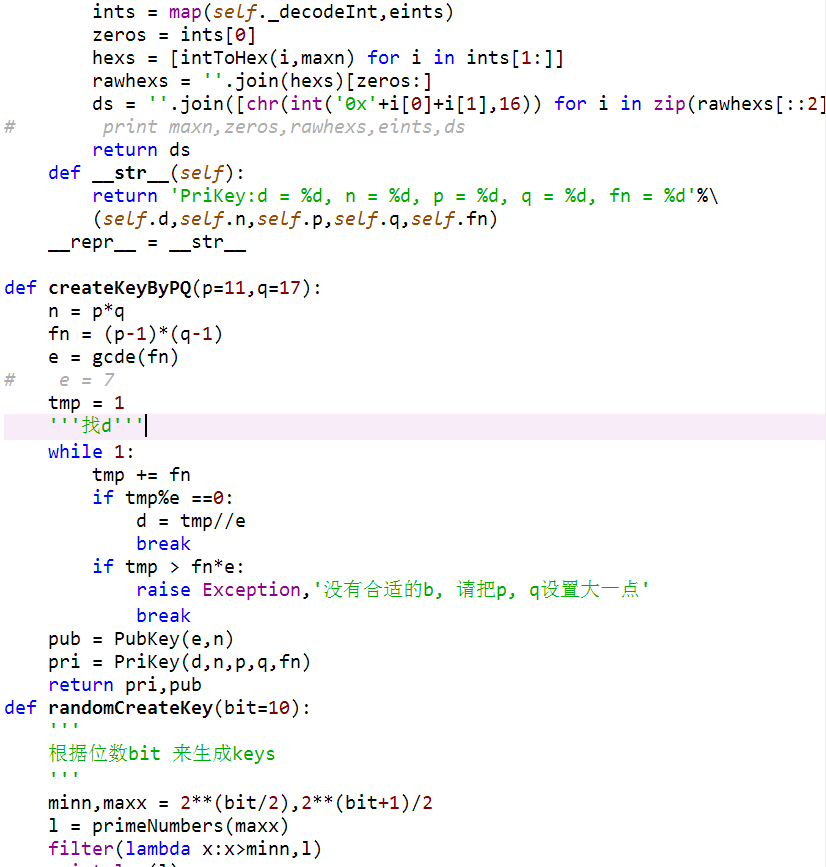
## RSA密码算法

RSA算法是自己使用Python手工完成的，密文的第一个单位加密长度是描述用于补全的多于信息，类似base64转码中末尾加“=”号的作用

#### 代码

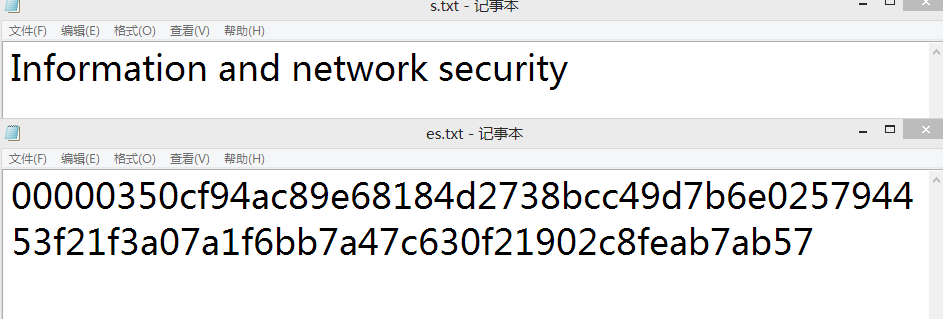


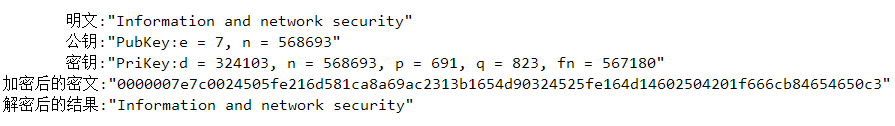






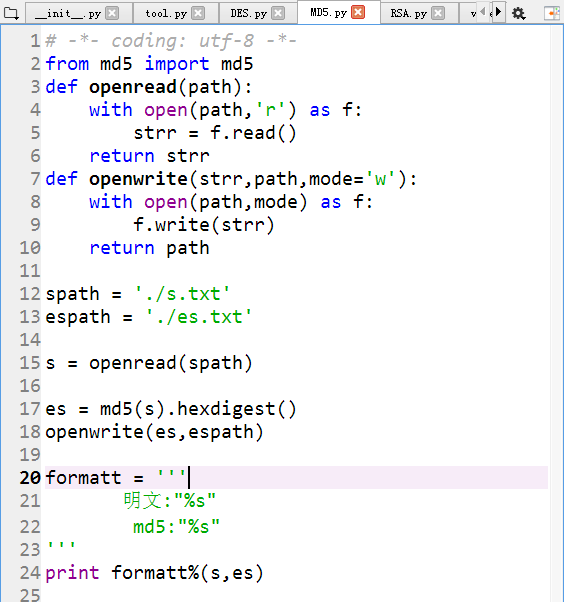
#### 结果



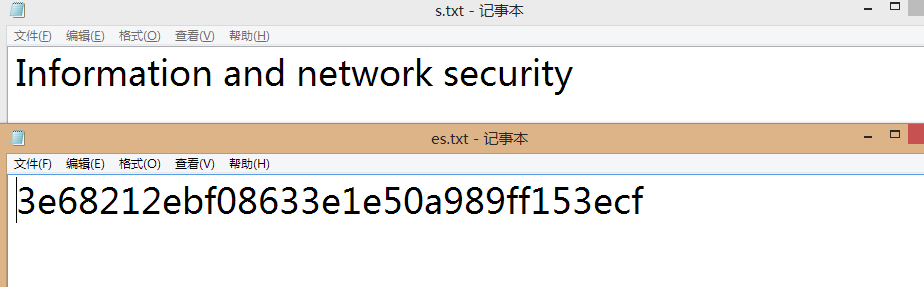


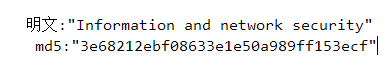
## MD5算法

#### 代码



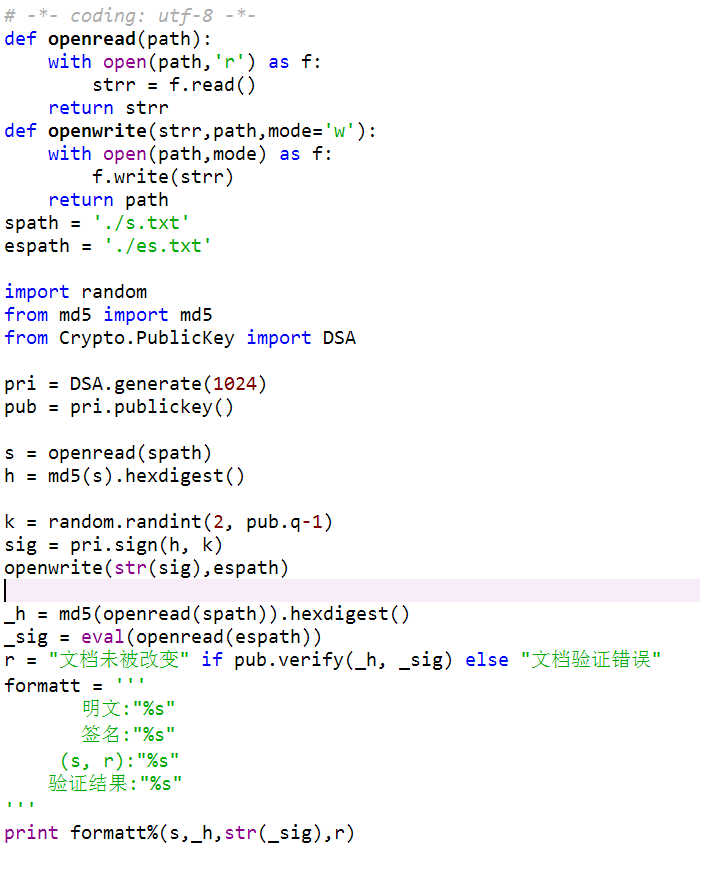
#### 结果





## DSS(DSA)算法

#### 代码



#### 结果

