## 实验4：实现非对称加密编程

### 实验目的

* 实现非对称加密密钥生成
* 实现非对称密钥对象和字节流的相互转换
* 实现RSA非对称加解密（1.RAW-RSA，2.随机padding后的安全RSA）

### 实验内容

1. 安装gmpy2（若之前没有安装）
2. 利用cryptography中的 asymmetric的rsa模块实现rsa密钥对的生成
3. 利用cryptography中的serialization模块实现rsa密钥字节数组到密钥对象的相互转换
4. 利用gmpy2库以及cryptography中的rsa实现简单Raw Rsa加密和解密
5. 利用crypto的PKCS1\_OAEP实现安全rsa加解密
6. 实现共模攻击和同态攻击（选做）
7. 通过代码4-10了解PKCS1v15攻击（选做）