## 实验5：利用MAC和数字签名实现消息认证

### 实验目的

* 掌握基于对称密码实现消息认证的MAC设计原理及应用
* 掌握基于非对称密码实现消息认证的数字签名设计原理及应用
* 了解数字证书的结构和作用

### 实验内容

1. 利用cryptography中primitives的hashes、hmac模块实现给定消息的认证码生成及验证
2. 利用cryptography中primitives的cmac和algrithms.AES实现给定消息的认证码生成及验证
3. 利用cryptography中primitives的asymmetric.rsa生成给定消息的RSA数字签名并完成验证
4. 利用cryptography中primitives.asymmetric中的ec生成给定消息的椭圆曲线数字签名并完成验证
5. 利用Crypto库中的对应功能模块编程实现消息认证码和数字签名的生成和验证
6. 熟悉代码5-6，5-7，5-8，总结数字证书的内容结构、签发方式和作用。（可以在下次实验完成）