实验七 ECC的相关实践

一、 实验目的：

1、掌握ECC的设计思想与流程。

2、深刻理解公钥加密体制的一个重要应用——数字签名。

3、通过设计程序结构，增强程序的实用性和可扩展性，提高编程能力。

二、 实验说明：

本次实验内容按照难度不同分为三个等级，得分会以选定的实验等级为基准。

三、 实验内容：

**1、初级：**

**简单实现基于ECC的加密。要求实现第五版课本229页的例子。**

**2、中级：**

**按照“The Elliptic Curve Digital Signature Algorithm (ECDSA).pdf”,实现基于ECC的数字签名，并验证签名。可以使用文章推荐的参数。**

Pdf我加了书签，是关键的位置。(选中级不用再做初级).

python有个ecdsa的库 <https://pypi.python.org/pypi/ecdsa> 可以自己看看。实验不能用现成的库，可以试试看能不能结果一样。

**3、高级：**

**按照“Identity Based Encryption.pdf”，实现基于ECC和双线性对的加密解密算法。只需实现论文中的方案即可。**(选高级不用再做中级)

四、 实验要求：

1、请合理划分程序结构，每一部分独立为一个.sage或.sagews文件，同实验报告一起打包提交，压缩文件命名格式为：**学号\_姓名\_实验七.zip/rar**。

2、代码鼓励写注释。**实验报告**应至少含有算法原理、算法流程、测试样例及运行结果，鼓励写心得体会或感想建议。

3、截止时间为6月28日。助教会在6月28日去沙河检查最后一次。同时要求前几次作业没有检查过的、或者想提高难度的同学，要在最后一次检查时候同时检查相应的作业。检查后要把作业提交到邮箱buaa2015\_xinan@163.com。**缺交一次作业或者缺少让助教检查一次作业，对于最后的成绩影响会比较大。**