**实验1：实现 Shamir秘密共享方案**

实验时数：4学时。

**一、实验目的**

1.熟练掌握Shamir秘密共享算法的秘密分配的步骤。

2.熟练掌握恢复秘密消息的机制(矩阵或者拉格朗日插值二选一)。

**二、实验内容**

1. 配置C或Python环境。

2. 任选一种语言实现(t,n)Shamir秘密共享方案，主要步骤要有标注。

3. 令秘密消息是11，构造(3,5)门限方案，选取多项式为F(x)=(7x^2+9x+11)mod13

1) 计算5个影子

2) 从任意3个影子中恢复出消息(矩阵或者拉格朗日插值二选一)

**三、实验报告编写**

1. 实验报告文件命名规则：学号+姓名+实验n，例：201922222222张三实验1。

2. 按实验报告格式，遵从实验要求完成：

3. 请同学们每次实验记得签到，把每次上机的内容保存好，完成报告后，实验后的第二周由班长统一收齐实验报告发到老师邮箱。