实验十-数字签名

【实验目的及要求】

1、 了解并掌握常用的数字签名方法并编程实现；

2、 感受不同数字签名方案的优缺点及适用场景。

【实验步骤】

【注】本地实现验证算法时要考虑验证成功与失败两种情况，例随机更改签名中的某几位尝试验证是否能通过，不能通过需要给出报错信息。

（一）必做

（1）实现ElGamal数字签名方案，并给出签名、验证算法的流程图和伪代码。

（2）实现Schnorr数字签名方案，并给出签名、验证算法的流程图和伪代码。

（3）实现SM2数字签名方案。

（二）选做

1、难度：中等

实现RSA-PSS数字签名算法，并且给出签名验证算法的流程图和伪代码（可参考第七版教材13.6）。

【实验报告】

1、 实验布置两周内，请同学们将实验报告提交至OJ平台对应位置，逾期者酌情扣分。

2、 对于每个算法，报告中应含有函数调用关系图、测试样例及运行结果截图，并且记录自己本次实验的收获感想，和对实验不足之处的建议，部分算法需要流程图**和**伪代码。

3、 报告格式见附件二；且该格式仅供参考，同学们可酌情更改。

**4、 请注意：所有实验中，**并不是做困难难度的实验的难度系数一定高于难度为中等；**难度系数由实验自身难度和具体实现情况以及程度决定；**如果只能敷衍完成，同学们不如选择在更简单的选做题上创新。