实验七-RSA

【实验目的及要求】

1、 掌握 RSA 算法原理及实现；

2、 了解常见的 RSA 攻击方法。

【实验步骤】

（一）必做

（1）实现 RSA 算法，要求使用第一次试验中实现的子函数，并在解密过程使用中国剩余定理加快解密算法。并且分析参数的生成规则及安全性。

实现以下几种常见的针对 RSA 的攻击：

（2）实现小指数广播攻击；如果选取的加密指数较低，并且使用了相同的加密指数给多名接收者发送相同的消息，则可进行广播攻击得到明文。

（3）实现共模攻击；多次加密，其中 e 不同、n 相同、m 相同，则可在不分解 n 和求 d 的前提下，解出明文 m。要求在实验报告中对共模攻击的流程进行证明。

（二）选做

1、难度：简单

实现已知 e, d 分解 n。并且在实验报告中给出原理。

2、难度：一般

参考 RSA 官方文档（附件一）实现 RSA-OAEP；其中哈希函数可直接调库使用 SHA256 算法，无需编程实现。

3、 难度：困难

查询相关资料实现维纳攻击：在 d 较小时，攻击者可以使用 Wiener's Attack 来获得私钥；并且在实验报告中给出算法原理、算法流程图和伪代码。

【思考题】

1、考虑 RSA 算法在实际应用中提高安全性的措施。
2、RSA 算法在生成密钥时为什么要选取大素数？请简要说明。

3、阐述如何利用 RSA 算法的性质进行选择密文攻击。

【实验报告】

1、 实验布置两周内，请同学们将实验报告提交至0J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。