**2022年春季密码学大作业**

在保密通信过程中，对消息完整性的检验和对消息来源的认证，是一个非常重要的问题，本次大作业的内容为：设计一个协议，利用rsa公钥加密算法和MD5哈希算法，实现对消息的完整性检验和发送者身份验证的功能，并编程实现这个协议。程序的要求是假设通讯双方为A合B，并假设发方拥有自己的RSA公钥PKA和私钥SKA ，同时收方B已经通过某种方式知道了发方的公钥PKA  。协议要求对发方A发来的消息，收方B通过检验，能够确定：

1. B收到的消息是完整的，即消息在传送过程中没有遭到非法修改；
2. B收到的消息来源是真实的，即该消息的确是由A发来的，而不是由其他人伪造的。

大作业的要求：

1. 分别编写两个程序，一个为发方程序，一个为收方程序，写清楚两个程序分别要完成的功能，并能够在两个程序间进行通讯。
2. 大作业的提交方式同实验报告的提交，也就是说既要提交程序实现的说明文档，也要提交源代码和可执行程序。
3. **模n至少1024bit,单向实现要求即可双向也可以**

补充说明：本次大作业的最终成绩，将作为我们的期末成绩，也就是说，也就是说，这次大作业的战绩，将占本门课程成绩70%，在总成绩中占比非常高，故希望大家能足够重视，努力完成这次大作业！！！！