**2022年秋季密码学大作业**

设计一个保密通信的协议，具体要求为：利用RSA公钥密码算法，为双方分配一个 AES算法的会话密钥，然后利用AES加密算法和分配的会话密钥，加解密传送的信息。

假设条件：假设通讯双方为A和B，并假设发方拥有自己的RSA公钥PKA和私钥SKA ，同时收方拥有自己的RSA公钥PKB和私钥SKB ，同时收发双方已经通过某种方式知道了双方的公钥。

大作业的要求：

1. 作业需要先设计出保密通讯协议的过程和具体步骤；
2. 分别编写A，B两个用户端的程序，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；
3. 对AES加密的保密信息，要求采用CBC模式进行加密；
4. 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。

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！！！！