Diffie-Hellman密钥交换算法实现

1. 实现DH密钥交换协议（算法参数，p是128bit的任意一个素数 ， g 为 2）
2. 利用1.实现的算法，设计一个服务端和客户端，进行通信，在通信的过程中，消息要使用协商好的密钥加密消息。（加密算法是AES的cbc模式, 密钥长度为128）

实验格式命名：

学号\_姓名\_实验

注意，如果不按实验格式命名，一概不收。同时记得打包为一个压缩包。