2022年秋季学期《物联网安全》（无军籍）

课程实验随堂验收考核要求

实验1：加解密算法与加密通信设计与实现

1. 考核方式

采取全阶段考核，即现场验收和实验报告考核结合的方式，两者成绩都为百分制。本文说明实验随堂验收的考核要求，实验报告的考核要求请参考《2022年秋季学期“物联网安全”课程实验报告考核要求》。

随堂验收主要查看学生根据实验指导书的步骤对于实验的完成情况，验收主要检查两个部分：实验基本目标的完成情况和实验加分项的完成情况。在验收过程中针对两个检查部分还会根据实际情况进行提问，以检验学生对于实验考察知识的掌握程度和对于实验的深入理解情况。

随堂验收的成绩由实验内容评分、实验质量评分以及完成速度评分这三个部分构成，实验三的具体评分细则由下面三个部分分别阐述。

1. 实验完成内容评分细则
2. 检查实验初始步骤：

客户端和服务端能够ping通。

**该步骤完成且截图完整得5分。**

1. 查看以下验证性实验步骤的截图

1）查看所设计的程序。

运行程序，客户端和服务端成功通信，截图。

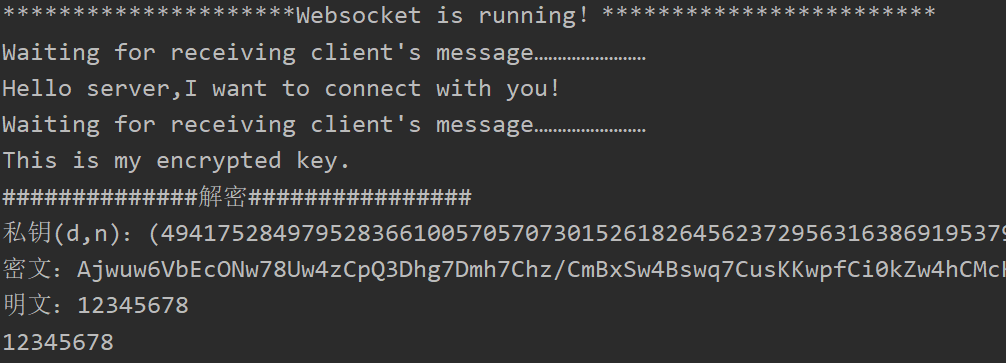
**该步骤完成且截图完整得15分。**

2）启动程序；

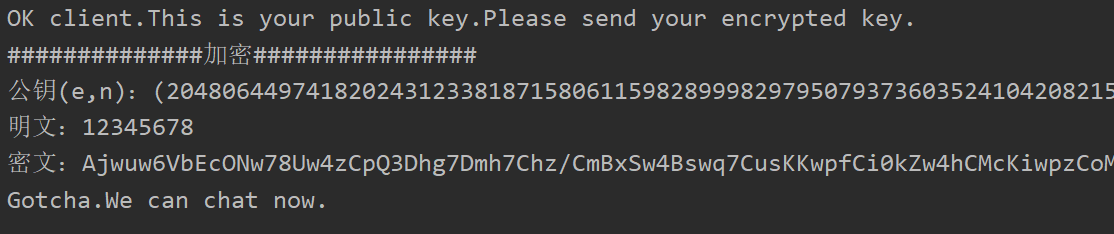
3）客户端与服务端通信，并输出密钥交换过程中间结果；

**截图类似于：**

服务端：



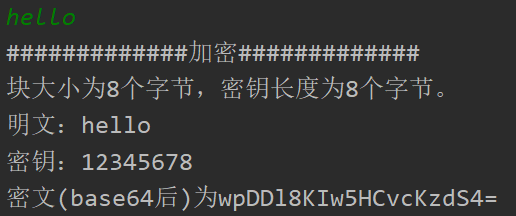
客户端；



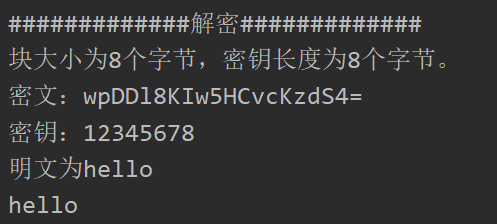
**该步骤完成且截图完整得20分**

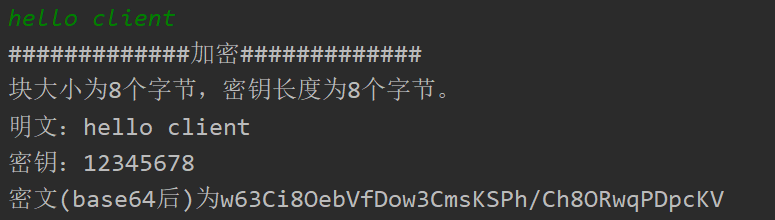
**双方开展加密聊天，截图类似于：**

client向server发送hello：

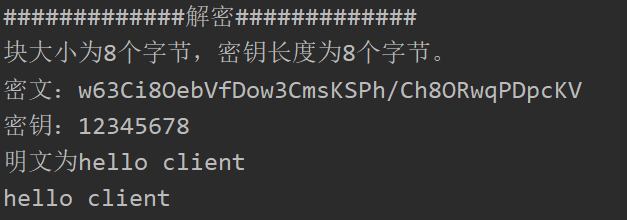


server接受到消息：



server向client发送hello client：  


client接受消息：

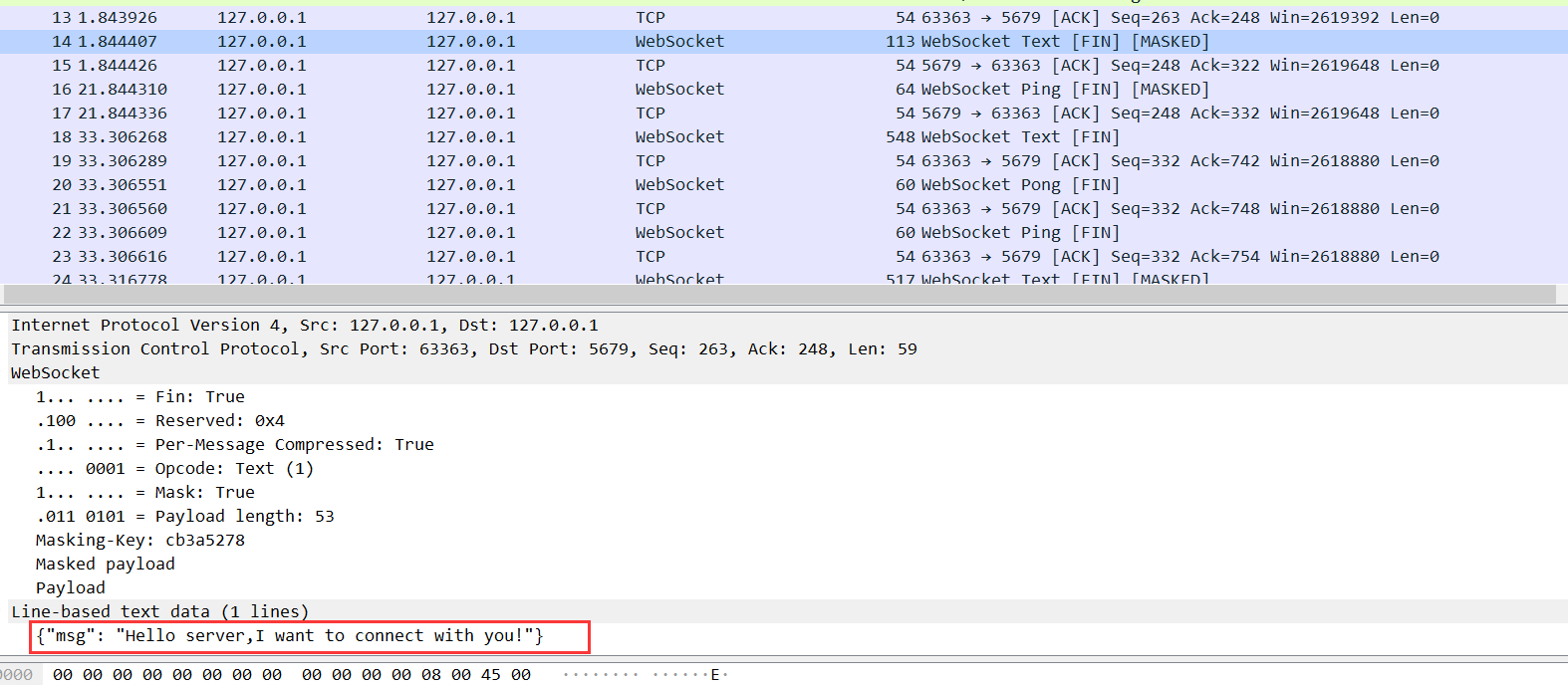


**此步骤完成且截图清晰得20分。**

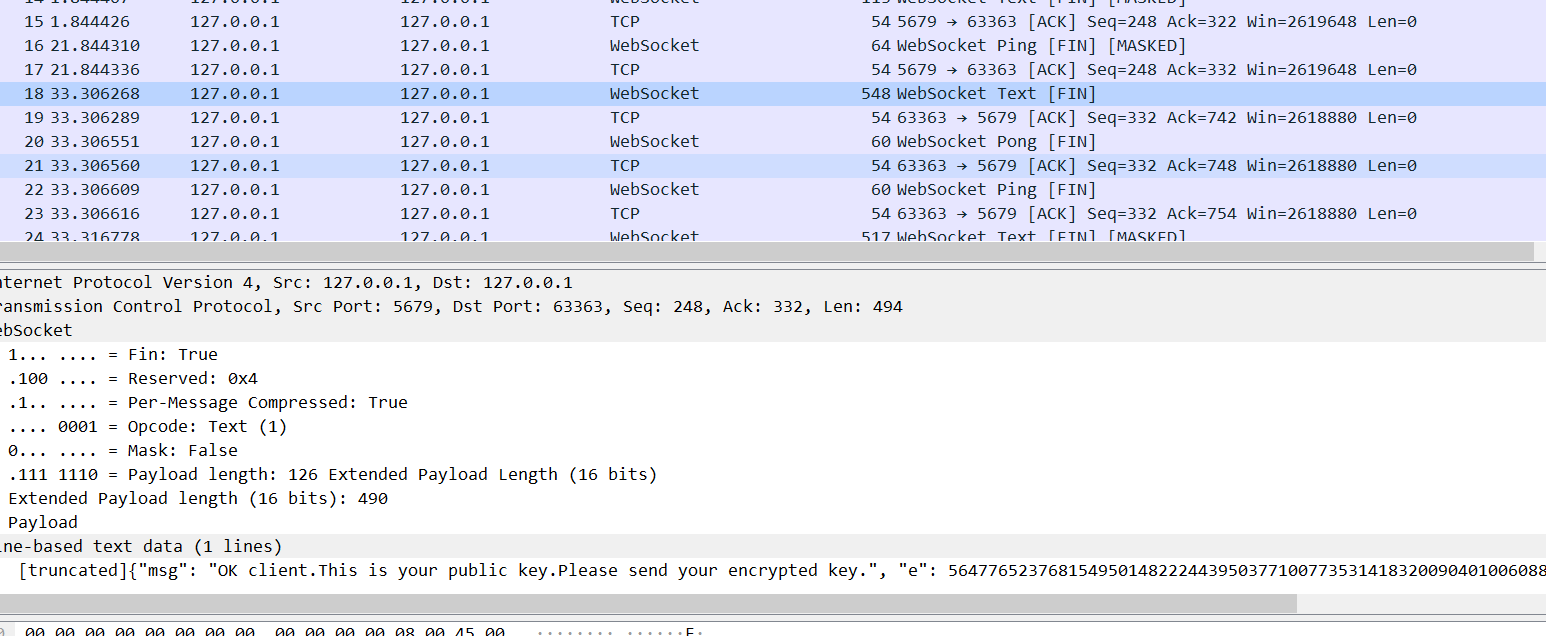
4）利用Wireshark验证加密通信

利用Wireshark对双方通信流量进行抓包分析，截图类似于：

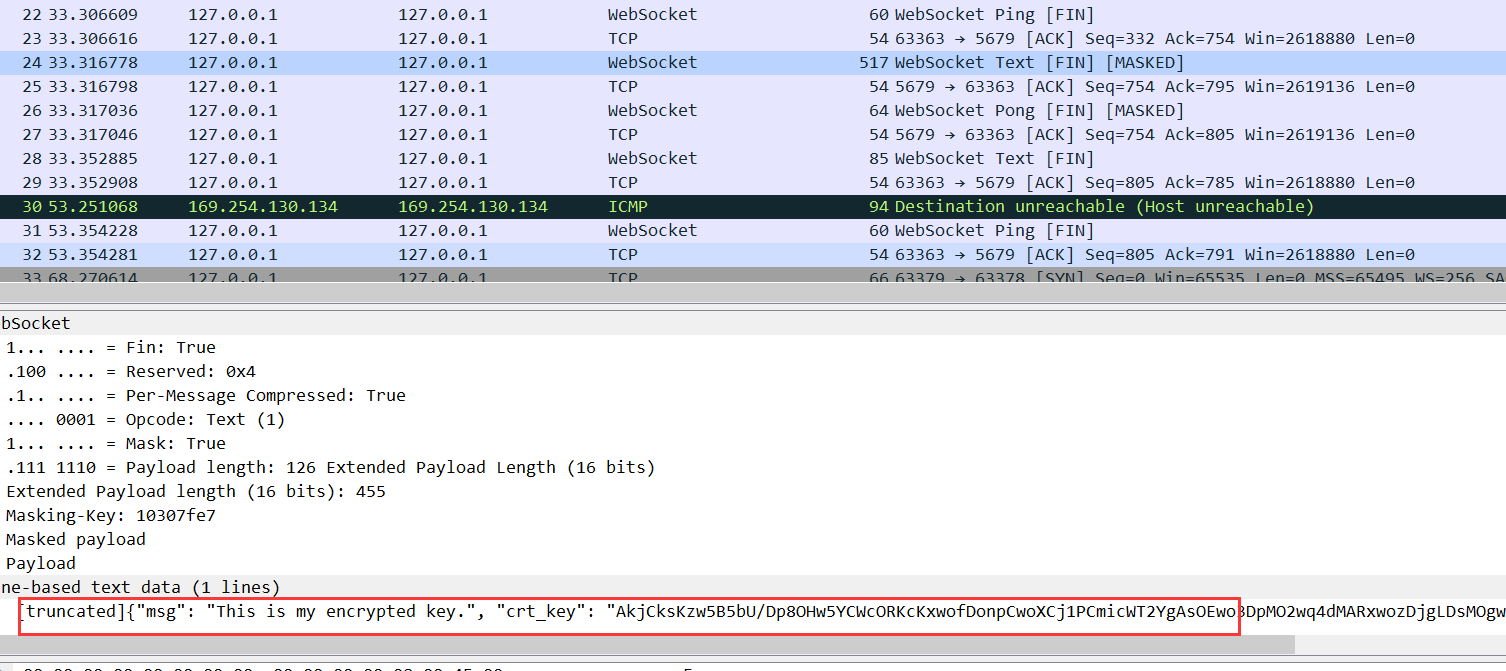
发起会话：



密钥交换：



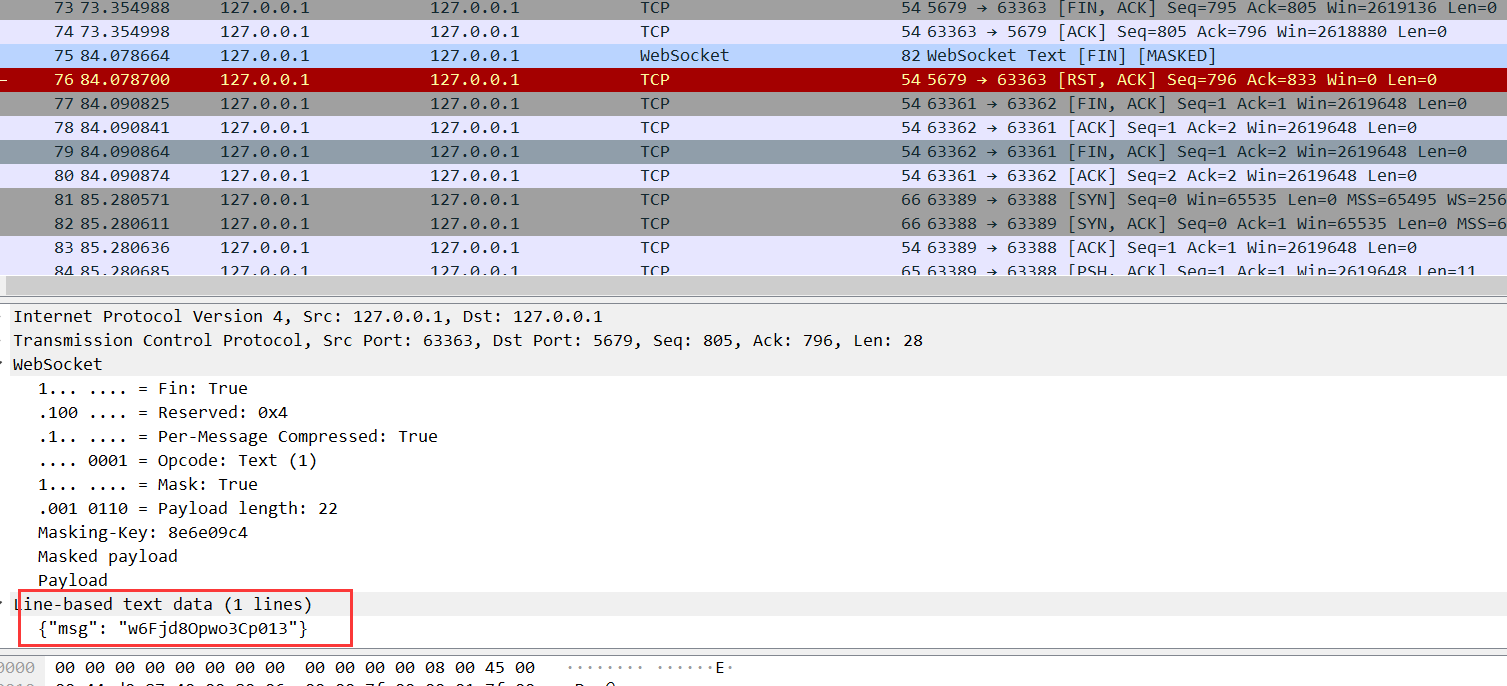
加密会话密钥：



**该步骤完成且截图完整得25分**

Wireshark抓取会话聊天流量，查看被加密的通信消息：

**截图类似于：**



**该步骤完成且截图完整得15分**

1. 实验完成质量评分细则

1.完成Wireshark之前的基本验证性步骤，为60分，若这个最基本的都没有完成，直接不及格；

2.在完成基本验证性步骤的基础上，Wireshark验证密钥交换但过于简单，得70分；

3.完成以上步骤，Wireshark验证完整，有说服力，得80分；

4.程序界面设计合理得85分；

5.随堂验收时能够清晰、流畅的叙述实验流程、回答问题得90分

6.密钥交换过程设计合理、清晰得95分；

7.在前面的基础上，实验、验证、分析过程完整清晰且具备较强说服力得100分。

1. 实验完成速度评分细则

没完成的0分。比大多数人花的时间都长很多，另外验收的60分；比大多数人花的时间长一些，在快下课时最后5人验收的得70分；中间的大多数人80分；前8个验收的，完成基本要求的得90分；前8个验收的中，完成情况极好的得100分。（具体人数根据选课人数确定）