1. 名词解释（10\*4）
2. 链路加密和端对端加密
3. 一次一密
4. Diffla-helman算法简述
5. 伪随机数
6. 主动攻击和被动攻击
7. 雪崩效应

还有三个忘了，应该是很基础

二：简答题（10\*7）最后一个是附加题

1. 什么是2-DES,为什么使用2-DES不安全，以及3DES构造有哪些特点
2. OSI安全框架的主要内容叙述
3. 比较对称加密，hash算法，mac算法的区别和联系（从设计，构造，功能等方面来谈）
4. 论证RSA算法的正确性，说明安全性；给一个具体例子来做
5. Kerberos要实现的主要目标是什么？通过什么样的方法实现了用户的安全性和可靠性
6. 简述c/s或b/s架构的一些安全问题，设计一个算法来解决这些问题
7. 简述欧拉定理的主要内容，并证明；简述其在miller-Rabin算法中起到的作用