网络安全技术 —— 课堂作业1

学号：2013921
姓名：周延霖
专业：信息安全

（一）以DES为代表的对称秘钥密码系统的优缺点

DES的密钥长度为56位，使用Feistel网络进行加密。以下是DES的优缺点：

- 优点：

1. 高度安全性：DES使用的Feistel网络结构和复杂的S盒操作使得其具有较高的安全性，难以被破解
2. 加密速度快：DES算法的加密速度相对较快，适合用于大数据量的加密
3. 实现简单：DES算法的实现较为简单，计算量较小，适合用于资源受限的场景

- 缺点：

1. 密钥长度较短：DES的密钥长度只有56位，可能会被暴力破解或巨量计算攻击所攻破
2. 容易受到差分攻击：差分攻击是一种针对Feistel网络的攻击方式，DES算法容易受到此类攻击
3. 算法过时：由于DES的密钥长度过短，现代计算机的计算能力较强，所以DES算法已经逐渐被更加安全的算法所取代，如AES算法

（二）以RSA为代表的非对称秘钥密码系统的优缺点

RSA密钥由一对公钥和私钥组成，分别用于加密和解密。以下是RSA的优缺点：

- 优点：

1. 高度安全性：RSA的安全性建立在大数质因数分解问题上，即破解RSA需要计算大质数的质因数，因此其安全性较高
2. 不需要密钥交换：RSA算法不需要像对称密钥算法一样进行密钥交换，因此可以避免密钥泄露问题
3. 数字签名功能：RSA算法可以用于数字签名，确保数据的完整性和来源可信性。

- 缺点：

1. 计算复杂度高：RSA算法的加密和解密速度相对较慢，尤其是对于较长的密钥长度
2. 密钥长度需要足够长：RSA算法的安全性依赖于密钥长度，为了防止被攻击，密钥长度需要足够长，这也会增加算法的计算复杂度
3. 加密长度限制：由于RSA算法是基于模运算的，因此其加密长度受限于模数的长度，无法对大于模数长度的数据进行加密