**课堂作业1**

1. **对称密钥密码系统（以DES为代表）**

对称加密是最早的加密方法之一，其特点是加密和解密使用相同的密钥。DES（数据加密标准）是一种经典的对称加密算法，尽管它已经被认为不够安全（主要是因为其密钥长度较短），但它的设计思想对后来的对称加密算法有很大影响。

**优点**

1. **高效性**：对称加密算法通常比非对称加密算法要快很多。它们对硬件要求低，能够快速加密大量数据，非常适合于需要处理大量数据的场景，如文件加密和数据库加密。
2. **简单性**：对称密钥的算法结构相对简单，容易实现，这使得它们可以在资源受限的环境中使用，例如嵌入式设备。

**缺点**

1. 密钥管理问题：最大的挑战是密钥的安全分发和管理。在双方通信之前，必须以某种安全方式共享密钥。在有大量用户需要通信的系统中，密钥管理变得复杂和不可行。
2. 安全性问题：随着计算能力的提高，短密钥的对称加密算法（如DES）容易受到暴力攻击。因此，需要定期更换密钥并使用足够长的密钥，这进一步增加了管理的复杂度。
3. **非对称密钥密码系统（以RSA为代表）**

非对称加密，也称为公开密钥加密，使用一对密钥：公钥和私钥。公钥可公开分享，用于加密信息；私钥保持私密，用于解密信息。RSA是一种广泛使用的非对称加密算法，以其创始人Rivest、Shamir和Adleman的首字母命名。

**优点**

1. **密钥共享简化**：公钥的公开性简化了密钥的分发问题。任何人都可以使用公钥来加密信息，但只有持有对应私钥的接收方可以解密，这使得安全通信更容易实现。
2. **数字签名**：非对称加密提供了数字签名功能，使得信息的接收者可以验证信息的真实来源和完整性，这对于确保网络安全和防止信息篡改至关重要。

**缺点**

1. **计算密集**：由于其加密过程的复杂性，非对称加密算法通常比对称加密慢得多。这在处理大量数据时可能成为瓶颈。
2. **密钥长度和安全性**：为了保持加密的安全性，非对称加密需要使用较长的密钥。这不仅使得算法运行更慢，还要求更高的计算资源和存储空间。
3. **受限的加密数据大小**：非对称加密算法通常有数据大小的限制，即加密的数据不能超过密钥的长度。这限制了其在某些情况下的应用。