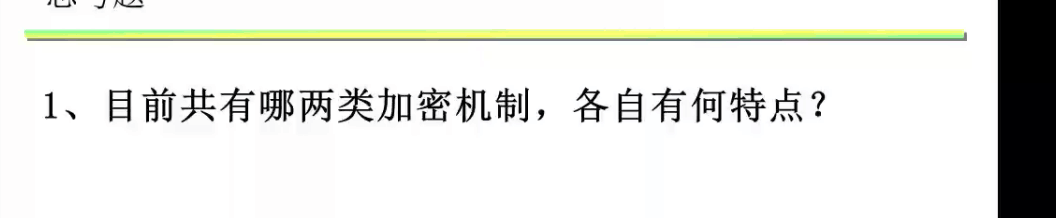
**计算机网络作业**

71118415 叶宏庭

题目：



解答：

1. 对称密钥加密体制（DES）

通信双方采用相同的密钥(静态分配)；

对于每个通信伙伴都需要维护一个密钥，所以N个伙伴就应维护N个密钥，维护信息量大；

无法应用到群组内的安全通信；

该算法主要执行置换，代换，微操作等，加密/解密速度快；

常用于批量数据的加密；

1. 非对称密钥加密体制（RSA）

总的密钥数量与用户数成线性关系，N个通信伙伴对应2N个密钥；

每个人有自己独特的密钥，一个公钥，一个私钥；

用户只需要维护自己的私钥即可，维护量小；

可用于群组内的安全通信；

采用乘法运算，加密/解密速度慢，常用于少量数据的加密；