Diffie-Hellman 密钥交换方案
公钥密码的基本思想
利用公钥密码的密码分发过程
RSA 公钥密码的简评
公钥密码的优缺点
对称密码的优缺点

加密密钥公开，解密密钥私有
公钥密码的思想：加解密密钥不同，加密密钥公开，解密密钥私密保存
AB 各选择私钥，将计算结果交换，后计算出会话密钥（一样的）
RSA 公钥密码的简评：
1. 第一个实用的公开密钥算法
2. 目前使用最多
3. 理论基础事故数论的欧拉定理
4. 安全性依赖于大数的素因子分解的困难行
5. 既能用于加密也能用于数字签名
6. 目前密钥长度 1024 位是安全的

公钥密码的优点：
1. 密钥分发简单 2.要秘密保存的密钥量少 3.可实现数字签名和认证的功能
缺点：
1.慢 2.密钥较长 3.有数据扩展