DH算法

DH算法的出现就是用来进行密钥传输的。DH算法是基于离散对数实现的。用户A和B如何利用RSA算法来传输密钥？

在通信前，用户A和B双方约定2个大整数n和g,其中1，这两个整数可以公开

1) A随机产生一个大整数a，然后计算Ka=ga mod n。（a需要保密）

2) B随机产生一个大整数b，然后计算Kb=gb mod n。（b需要保密）

3) A把Ka发送给B,B把Kb发送给A

4) A计算K=Kba mod n

5) B计算K=Kab mod n

由于Kba mod n= （gb mod n）a mod n= （ga mod n）b mod n，因此可以保证双方得到的K是相同的，K即是共享的密钥。