# **DH密钥交换和ECDH原理**

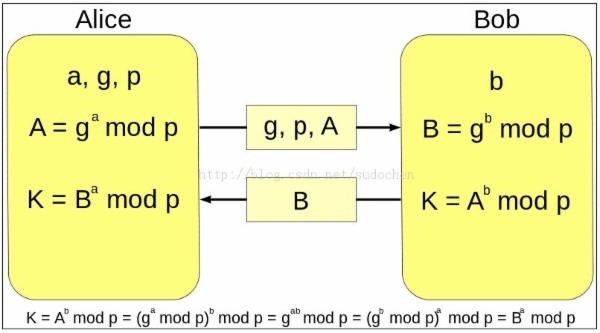
时间 2013-06-24 18:50:55 [CSDN博客](http://www.tuicool.com/sites/vQZRB3" \t "https://www.cnblogs.com/fishou/p/_blank)[相似文章](http://www.tuicool.com/articles/dup?id=em6zEb" \t "https://www.cnblogs.com/fishou/p/_blank) (*0*)*原文*  <http://blog.csdn.net/sudochen/article/details/9164427>

下面我们以Alice和Bob为例叙述Diffie-Hellman密钥交换的原理。

1,Diffie-Hellman交换过程中涉及到的所有参与者定义一个组，在这个组中定义一个大质数p，底数g。

2,Diffie-Hellman密钥交换是一个两部分的过程，Alice和Bob都需要一个私有的数字a，b。

下面是DH交换的过程图：



本图片来自wiki

下面我们进行一个实例

1.爱丽丝与鲍伯协定使用p=23以及g=5.

2.爱丽丝选择一个秘密整数a=6, 计算A = g^a mod p并发送给鲍伯。   
   A = 5^6 mod 23 = 8.

3.鲍伯选择一个秘密整数b=15, 计算B = g^b mod p并发送给爱丽丝。   
   B = 5^15 mod 23 = 19.

4.爱丽丝计算s = B a mod p   
  19^6 mod 23 = 2.

5.鲍伯计算s = A b mod p   
   8^15 mod 23 = 2.

ECDH密钥交换：

ECDH:

       ECC算法和DH结合使用，用于密钥磋商，这个密钥交换算法称为ECDH。交换双方可以在不共享任何秘密的情况下协商出一个密钥。ECC是建立在基于椭圆曲线的离散对数问题上的密码体制，给定椭圆曲线上的一个点P，一个整数k，求解Q=kP很容易；给定一个点P、Q，知道Q=kP，求整数k确是一个难题。ECDH即建立在此数学难题之上。密钥磋商过程：

假设密钥交换双方为Alice、Bob，其有共享曲线参数（椭圆曲线E、阶N、基点G）。

1) Alice生成随机整数a，计算A=a\*G。 #生成Alice公钥

2) Bob生成随机整数b，计算B=b\*G。 #生产Bob公钥

3) Alice将A传递给Bob。A的传递可以公开，即攻击者可以获取A。

    由于椭圆曲线的离散对数问题是难题，所以攻击者不可以通过A、G计算出a。

4) Bob将B传递给Alice。同理，B的传递可以公开。

5) Bob收到Alice传递的A，计算Q =b\*A  #Bob通过自己的私钥和Alice的公钥得到对称密钥Q

6) Alice收到Bob传递的B，计算Q`=a\*B  #Alice通过自己的私钥和Bob的公钥得到对称密钥Q'

Alice、Bob双方即得Q=b\*A=b\*(a\*G)=(b\*a)\*G=(a\*b)\*G=a\*(b\*G)=a\*B=Q' (交换律和结合律)，即双方得到一致的密钥Q。

        目前Openssl里面的ECC算法的套件支持是ECDSA/ECDH。在国密的SSL套件中，可以使用ECDSA/ECC(密钥加密传输)，ECDSA/ECDH(密钥磋商)两种套件

分类: [安全知识库](https://www.cnblogs.com/fishou/category/639429.html" \t "https://www.cnblogs.com/fishou/p/_blank)