Diffie-Hellman密钥交换

另一种解决密钥交换的方法：Diffie-Hellman密钥交换

步骤：

1. Alice向Bob发送两个质数P和G

P必须是一个非常大的质数，而G则是一个和P相关的数，称为**生成元**。G可以是一个较小的数。

**P和G不需要保密**，被窃听者Eve获取也无所谓。

此外，P和G可以有Alice和Bob中的任意一方生成。

1. Alice和Bob各自生成一个随机数A和B。

A和B是1~P-2之间的整数，且由各自**秘密保存。**

1. Alice将这个数发给Bob，Bob将这个数发给Alice。
2. Alice用Bob发过来的书计算A次方并求 mod P

Alice的密钥=

=

Bob用Alice发过来的书计算B次方并求 mod P

Bob的密钥=

=

最终Alice计算的密钥=Bob计算的密钥

**Eve能计算出密钥吗？**

在以上的各个步骤中公开的信息有：P、G、、在知道以上信息的情况下能计算出A吗？如果是的话计算A并不难但是根据计算出A的有效算法到现在还没有出现。

**生成元的意义**

举个栗子：已知P是质数，我们假设以13为栗。计算

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| G  A | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 2 | 4 | 8 | 3 | 6 | 12 | 11 | 9 | 5 | 10 | 7 | 1 |
| 3 | 3 | 9 | 1 | 3 | 9 | 1 | 3 | 9 | 1 | 3 | 9 | 1 |
| 4 | 4 | 3 | 12 | 9 | 10 | 1 | 4 | 3 | 12 | 9 | 10 | 1 |
| 5 | 5 | 12 | 8 | 1 | 5 | 12 | 8 | 1 | 5 | 12 | 8 | 1 |
| 6 | 6 | 10 | 8 | 9 | 2 | 12 | 7 | 3 | 5 | 4 | 11 | 1 |
| 7 | 7 | 10 | 5 | 9 | 11 | 12 | 6 | 3 | 8 | 4 | 2 | 1 |
| 8 | 8 | 12 | 5 | 1 | 8 | 12 | 5 | 1 | 8 | 12 | 5 | 1 |
| 9 | 9 | 3 | 1 | 9 | 3 | 1 | 9 | 3 | 1 | 9 | 3 | 1 |
| 10 | 10 | 9 | 12 | 3 | 4 | 1 | 10 | 9 | 12 | 3 | 4 | 1 |
| 11 | 11 | 4 | 5 | 3 | 7 | 12 | 2 | 9 | 8 | 10 | 6 | 1 |
| 12 | 12 | 1 | 12 | 1 | 12 | 1 | 12 | 1 | 12 | 1 | 12 | 1 |

（2为生成元）

（6为生成元）

（7为生成元）

（11为生成元）

我们发现2的乘方对应的值（共12个）都是不一样的。也就是说2的乘方的结果出现了1到12的全部整数。具有这种性质的数称为13的**生成元**。