迪菲-赫尔曼密钥交换

Diffie-Hellman Key Exchange
刘卓

迪菲-赫尔曼密钥交换 (Diffie-Hellman Key Exchange) 可以让双方在完全没有对方任何预先信息的条件下通过不安全信道创建起一个密钥。这个密钥可以在后续的通讯中作为对称密钥来加密通讯内容。公钥交换的概念最早由瑞夫 · 墨克（Ralph C. Merkle）提出，而这个密钥交换方法，由惠特菲尔德 · 迪菲（Bailey Whitfield Diffie）和马丁 · 赫尔曼（Martin Edward Hellman）在 1976 年首次发表。

换句话说，*Alice* 和 *Bob* 想要共享一个用于对称密码的密钥分享给对方，但是他们交流渠道是不安全的，很容易被拦截或者窃听。使用迪菲-赫尔曼密钥交换就可以在这种条件下把密钥交换给对方。

1 密钥交换步骤

1. *Alice* 和 *Bob* 决定一个大质数 p 和一个非零的整数 $r \bmod p$。即 r 是一个 primitive root mod p。*Alice* 和 *Bob* 公开 r 和 p，所有人都知道他们的值；
2. *Alice* 选择一个整数 x 使得 $x \pmod p$；*Bob* 选择一个整数 y 使得 $y \pmod p$；
3. *Alice* 计算 $A \equiv r^x \pmod p$；*Bob* 计算 $B \equiv r^y \pmod p$；
4. *Alice* 和 *Bob* 公开交换 A, B
5. *Alice* 计算 $B^x \pmod p$；*Bob* 计算 $A^y \pmod p$；
6. *Alice* 和 *Bob* 算出这两个值是于 $k \equiv r^{xy} \pmod p$ 相等的，这也是他们的私钥。

因为 $\underbrace{B^x = (r^y)^x = r^{xy} = (r^x)^y = A^y}_{\pmod p}$, 所以他们的密钥是一样的。

值得注意的是：公开的信息是 p,r, A,B;

私密信息是 x, y, k;

如果 *Eve* 能够解决离散对数问题 (即给定 A 和 B 找到 x 和 y)，那么她就能够找到 k。这并不简单，但确实如此，即在给定 A、B、r 和 p 的情况下找到 k 与解决 DLP(Data loss prevention software) 一样困难。

例 1

假设 $p = 37$,$r = 17$,*Alice* 选择整数 9，*Bob* 选择整数 10

$$A = r^x \pmod p = 17^9 \pmod{37} = 6 \pmod{37}$$

$$B = r^y \pmod{p} = 17^{10} \pmod{37} = 28 \pmod{37}$$

$$k = \underbrace{B^x = 28^9 = 36 = 6^{10} = A^y}_{(\mathrm{mod}\ 37)}$$

还有验证签名的方法，具体方法是 Zero Knowledge Protocol。