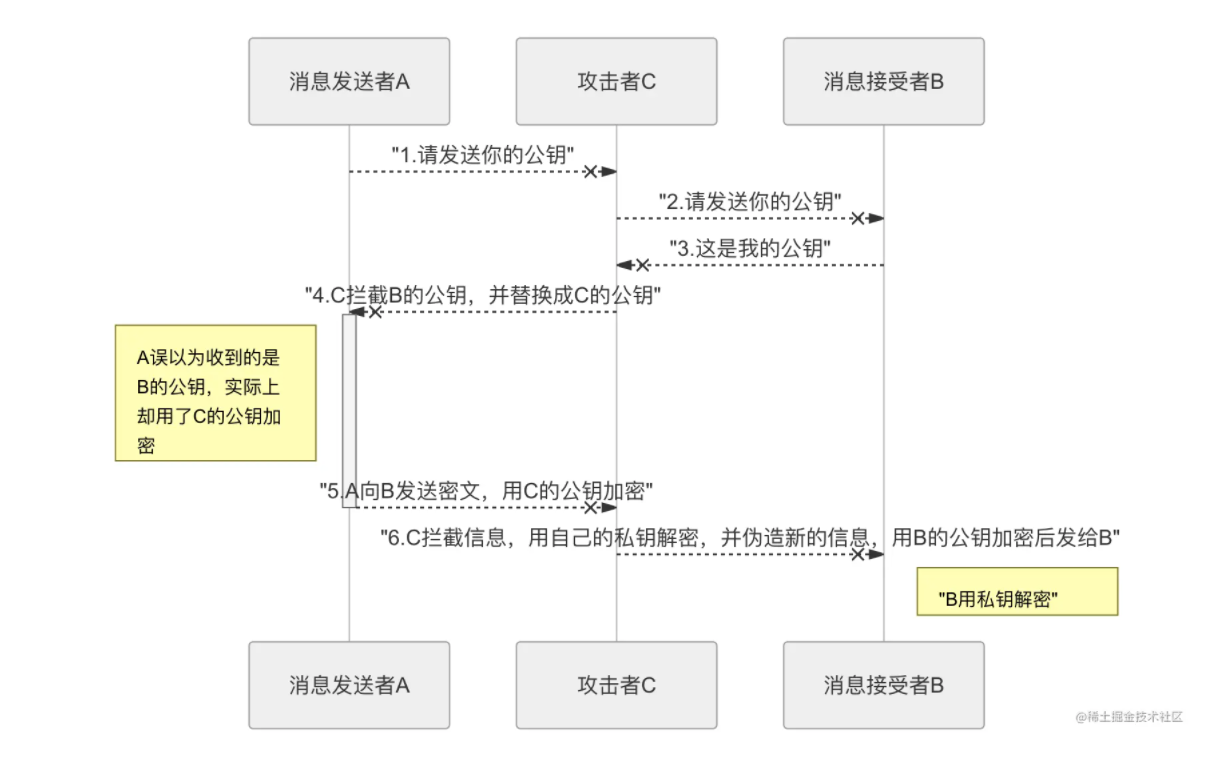
中间人攻击是什么？

所谓中间人攻击就是在A和B通信的过程中加入了恶意攻击者C。C作为中间人转发两者的请求。

示意图如下：



上面是一个完整的中间人攻击流程：

A向B请求公钥，但是却被C截获。

C向B发送公钥请求。

B将公钥发给C。

C截获了B的公钥，然后替换成自己的公钥发给A。

A将C的公钥当成了B的公钥，并用其加密信息，发给B。

C截获了加密信息，用自己的私钥解密，获得明文。同时伪造新的信息，再用B的公钥加密，发给B。

B获得加密信息，用自己的私钥解密。

中间人攻击不仅仅针对于RSA算法，任何公钥算法都可能受到中间人攻击的影响。

只靠公钥本身是无法防御中间人攻击的。这时候，我们就需要一个第三方的可信任的机构来解决这个公钥传递的问题，那就是证书。