3. 认证

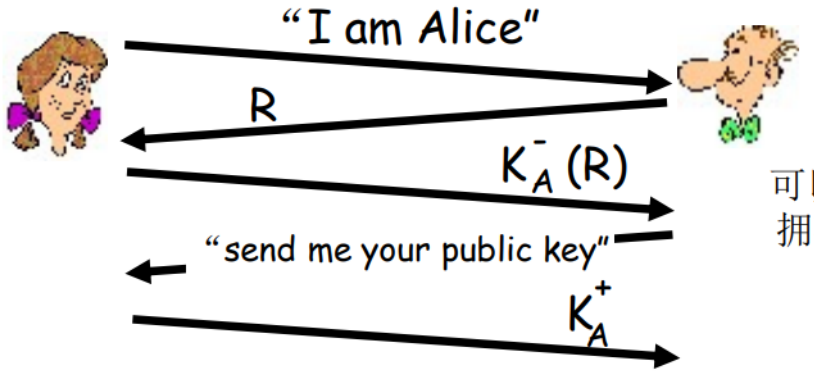
```
1.  Alice 说 “I am Alice”
        在网络上Bob看不到Alice, 因此Trudy可以简单地声称她是 Alice

2.  Alice 说 “I am Alice” , 在她发送的IP数据包中包括了她的IP地址
        Trudy可以生成一个分组，包括伪造Alice的IP地址

3.  Alice 说 “I am Alice” , 而且传送她的密码来证明.
        重放攻击playback attack:
            Trudy记录 Alice的 分组，事后向Bob重放

3.1 Alice 说 “I am Alice” , 而且传送她的加密之后的密码来证明
        记录，重放仍然有效

4.0 需要双方共享一个对称式的密钥
        有效

5.0 使用nonce,公开密钥加密技术
        有效

        安全漏洞：
            中间攻击：Trudy 在 Alice (to Bob)和 Bob之间 (to Alice)
                问题的本质：
                    1.如何拿到可靠实体的公钥
                    2.拿到公钥后如何认证
```

认证: ap5.0

ap4.0 需要双方共享一个对称式的密钥

- 是否可以通过公开密钥技术进行认证呢?

ap5.0: 使用nonce,公开密钥加密技术



Bob 计算

$K_A^+(K_A^-(R)) = R$

可以知道只有 Alice 能够拥有这个私钥, 因此才能够得到

$K_A^+(K_A^-(R)) = R$

ap5.0: 安全漏洞

中间攻击: Trudy 在 Alice (to Bob)和 Bob之间 (to Alice)