哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY
立足航天，服务国防，面向国民经济主战场

计算机网络之危机四伏

主讲人：李全龙

本讲主题

身份认证

身份认证(Authentication)

目标: Bob希望Alice“证明”她的身份

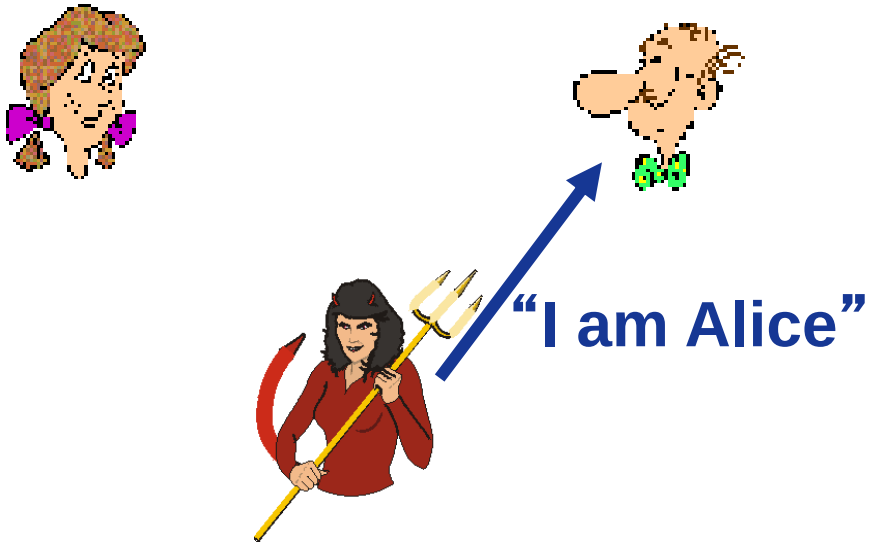
协议ap1.0: Alice声明“I am Alice”

失效场景??

身份认证

目标: Bob希望Alice“证明”她的身份

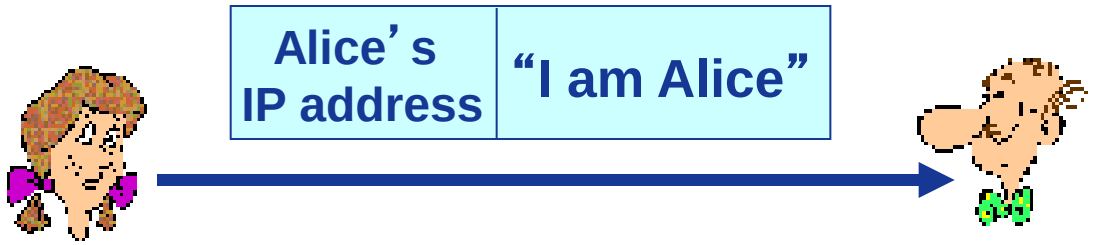
协议ap1.0: Alice声明“I am Alice”



在网络中,Bob“看”不到 Alice, 因此Trudy可以简单地声明她就是Alice！

身份认证

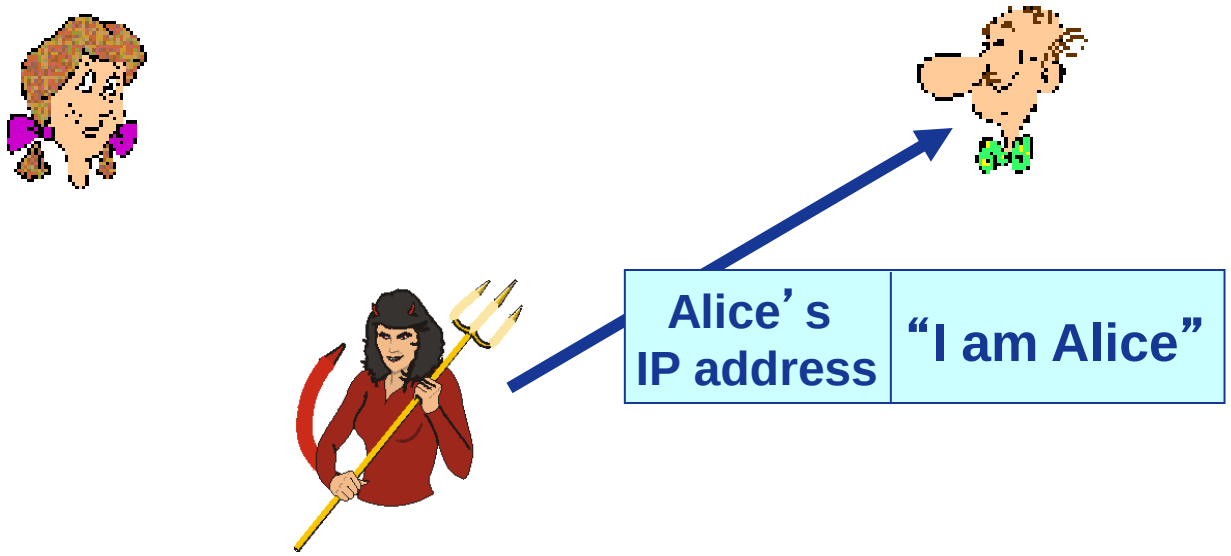
协议ap2.0: Alice在IP分组中声明“I am Alice”，IP分组包含Alice的源IP地址



失效场景??

身份认证

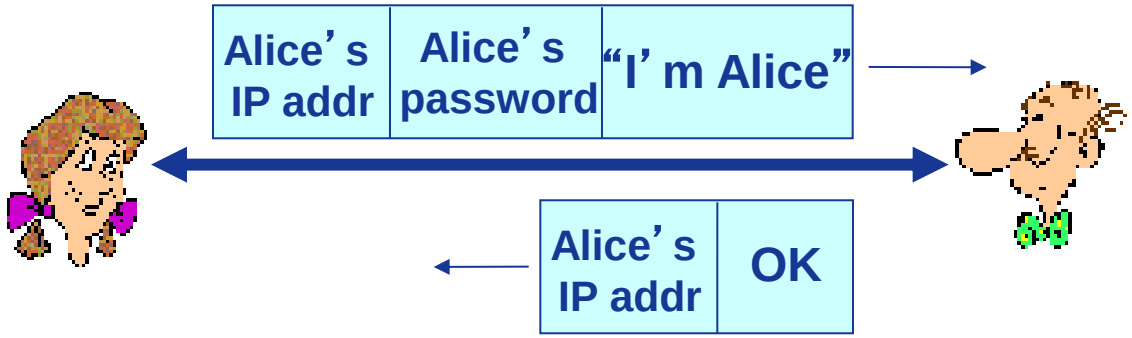
协议ap2.0: Alice在IP分组中声明“I am Alice”，IP分组包含Alice的源IP地址



Trudy可以构造一个分组，“欺骗”为Alice的IP地址

身份认证

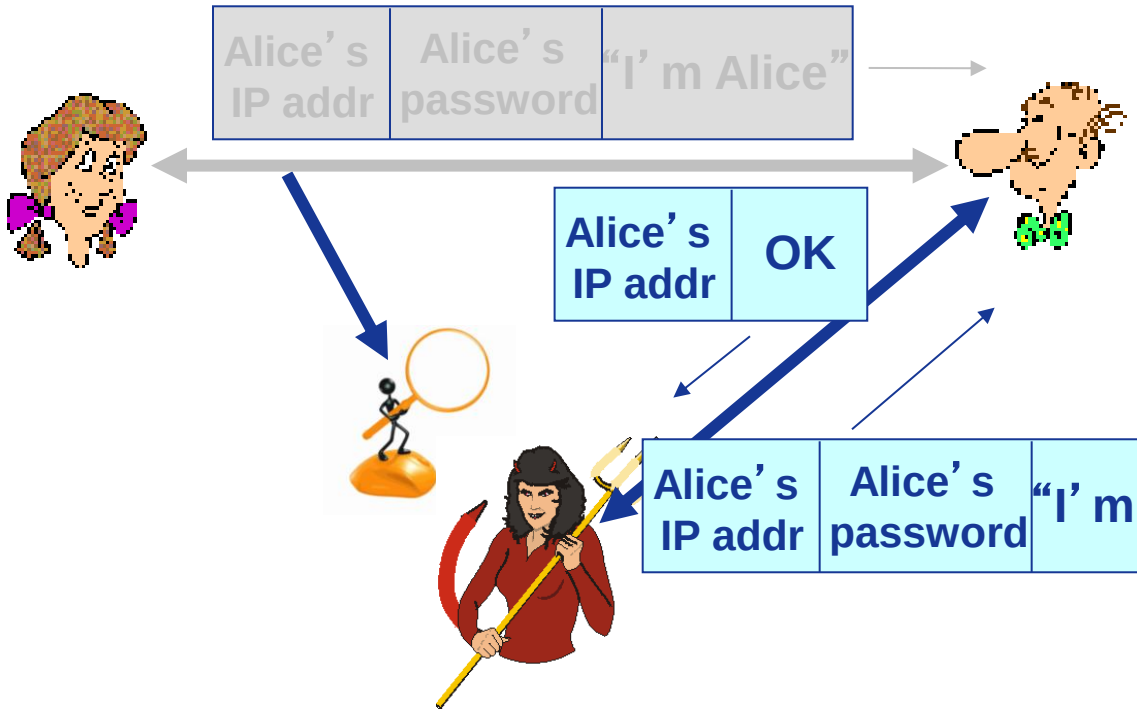
协议ap3.0： **Alice声明“I am Alice”的同时，发送她的秘密口令进行“证明”.**



失效场景??

身份认证

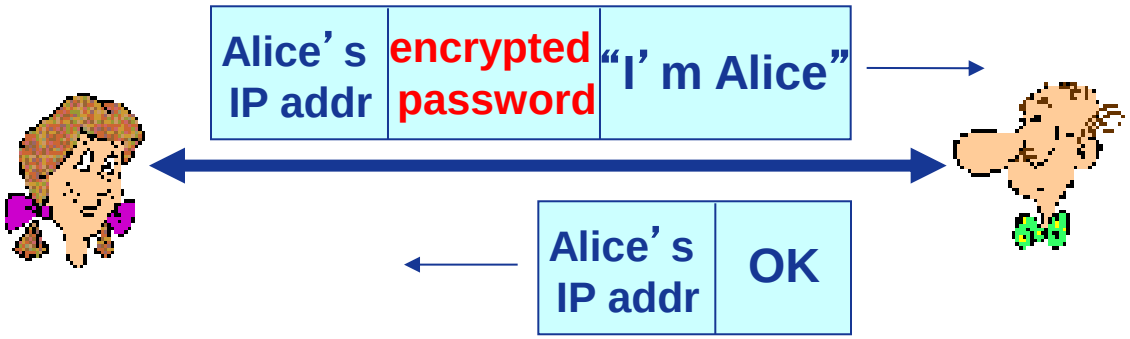
协议ap3.0： **Alice声明“I am Alice”的同时，发送她的秘密口令进行“证明”.**



嗅探(sniffing): Trudy嗅探Alice 的分组，提取口令

身份认证

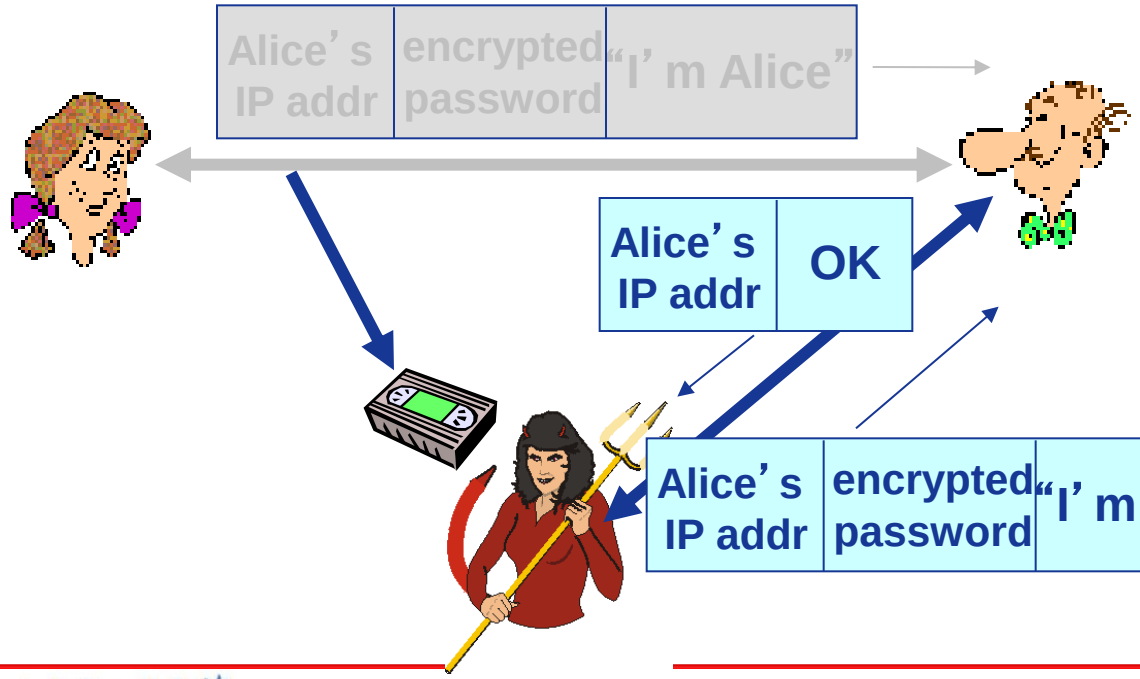
协议ap3.1: Alice声明“I am Alice”的同时，发送她的加密的秘密口令进行“证明”.



失效场景??

身份认证

协议ap3.1: Alice声明“I am Alice”的同时，发送她的加密的秘密口令进行“证明”.



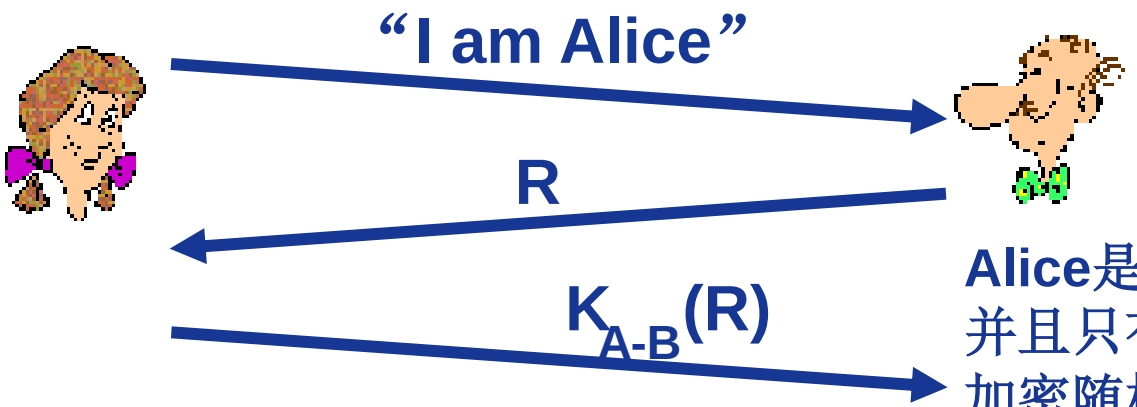
回放攻击(playback attack): Trudy记录Alice 的分组，稍后“回放”给Bob

身份认证

目标: 避免回放攻击

一次性随机数(nonce): 一个生命期内只用一次的数R

ap4.0: 为了证明是“真实的”Alice，Bob向Alice发送一个随机数R，Alice必须返回R，并利用共享密钥进行加密



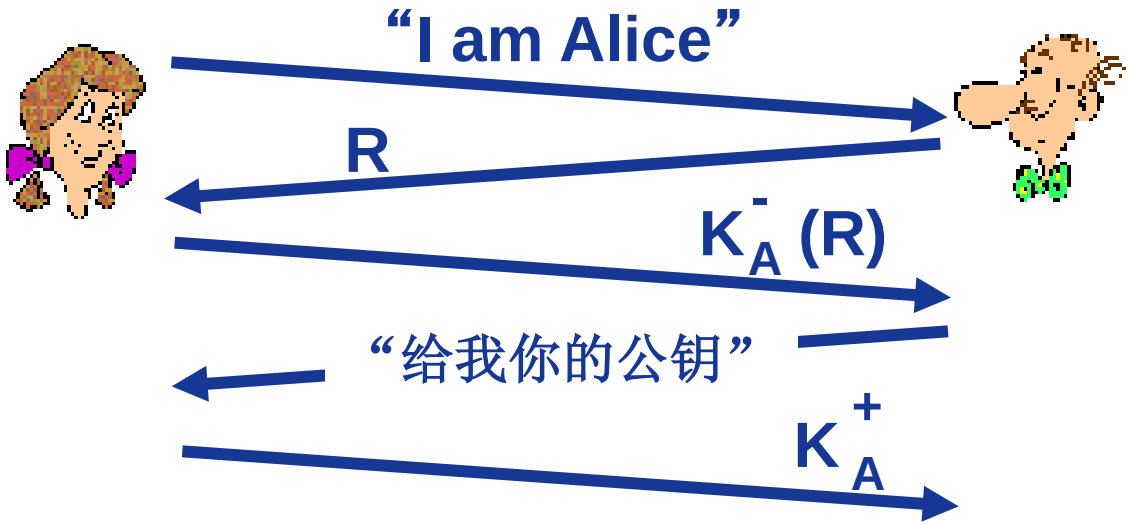
失效、缺点?

身份认证: ap5.0

ap4.0需要共享密钥!

- 是否可以利用公钥技术那?

ap5.0: 利用一次性随机数以及公钥加密技术



Bob计算:

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

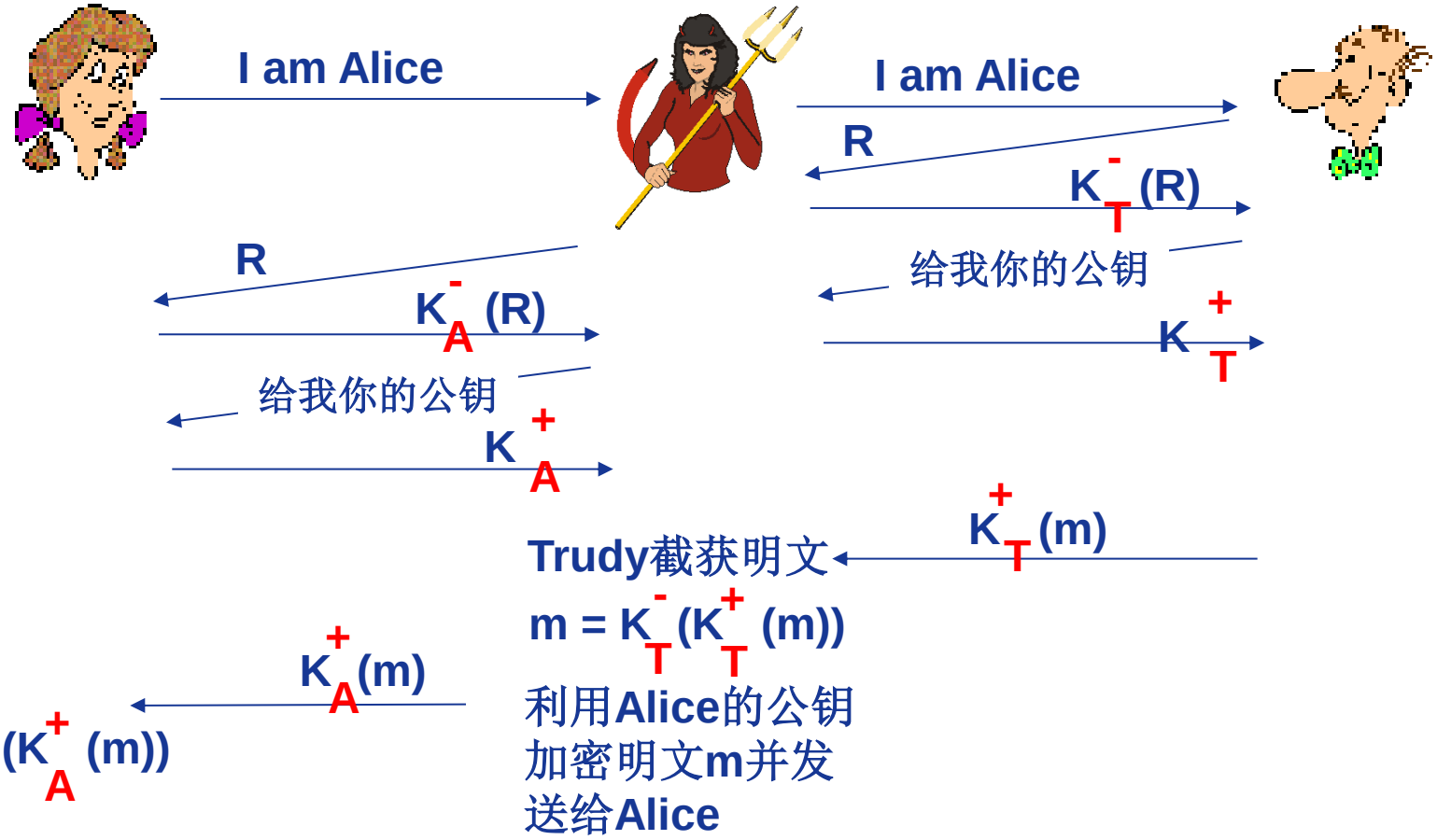
并已知只有Alice拥有加密R的私钥,因此:

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

失效?

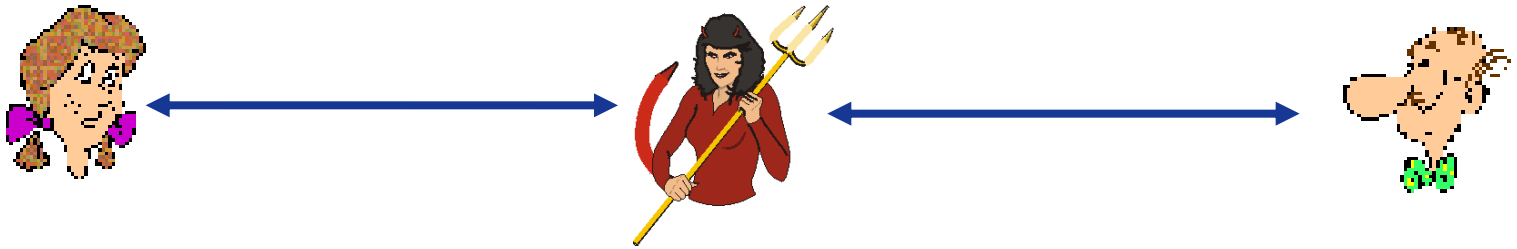
ap5.0: 安全漏洞

中间人攻击(man in the middle attack): Trudy向Bob假扮Alice，向Alice假扮Bob。



ap5.0: 安全漏洞

中间人攻击(man in the middle attack): Trudy向Bob假扮Alice，向Alice假扮Bob。



很难检测:

- **Bob与Alice可以收到彼此发送的所有信息。**
- **问题是Trudy也收到了所有信息！**

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

立足航天，服务国防，面向国民经济主战场

谢 谢！