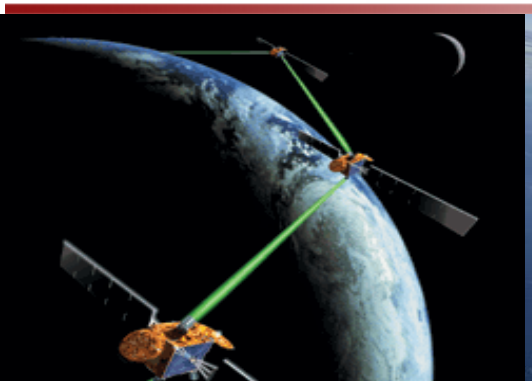
普通高等教育“十一五”国家级规划教材
教育部2011年精品教材

网络安全—技术与实践（第2版）

刘建伟 王育民 编著

清华大学出版社




课件制作人声明

- 本课件总共有17个文件，版权属于刘建伟所有，仅供选用此教材的教师和学生参考。
- 本课件严禁其他人员自行出版销售，或未经作者允许用作其他社会上的培训课程。
- 对于课件中出现的缺点和错误，欢迎读者提出宝贵意见，以便及时修订。

课件制作人：刘建伟

2016年10月27日

第8章 密码协议

一 协议的基本概念

二 安全协议分类及基本密码协议

三 秘密分拆协议

四 秘密广播协议和会议密钥分配

五 密码协议的安全性

一、协议的基本概念

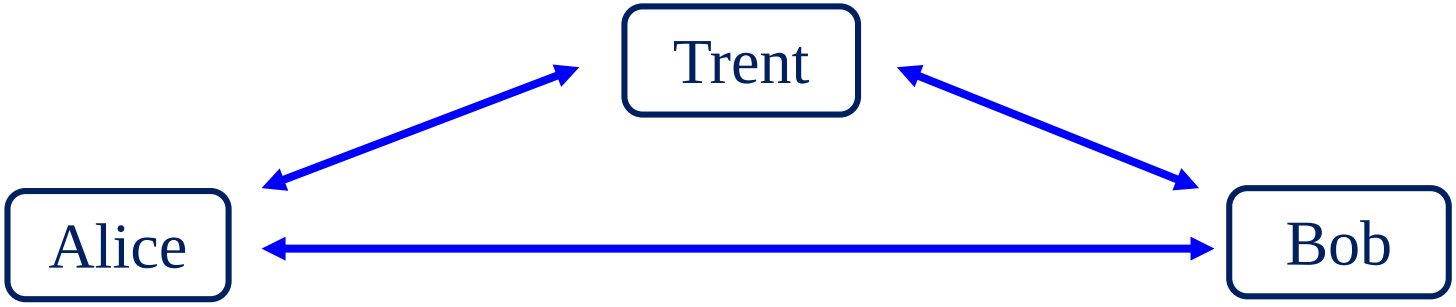
协议的定义

是指两个或两个以上的参与者为完成某项特定的任务而采取的一系列步骤。

协议三要素

1. 协议自始至终是有序的过程，每一步骤必须依次执行。
2. 协议至少需要两个参与者。一个人可以通过执行一系列步骤来完成某项任务，但它不构成协议。
3. 通过执行协议必须能够完成某项任务。即使某些东西看似协议，但没有完成任何任务，也不能成为协议。

1.1 仲裁协议



Trent为仲裁者(arbitrator)，是公正的第三方，其他各方均信赖他。

- “公正”意味着仲裁者对参与协议的任何一方没有偏向
- “可信赖”意味着他所说的话、做的事是正确的
- 仲裁者将帮助两个互不信赖的实体完成任务

仲裁协议举例说明

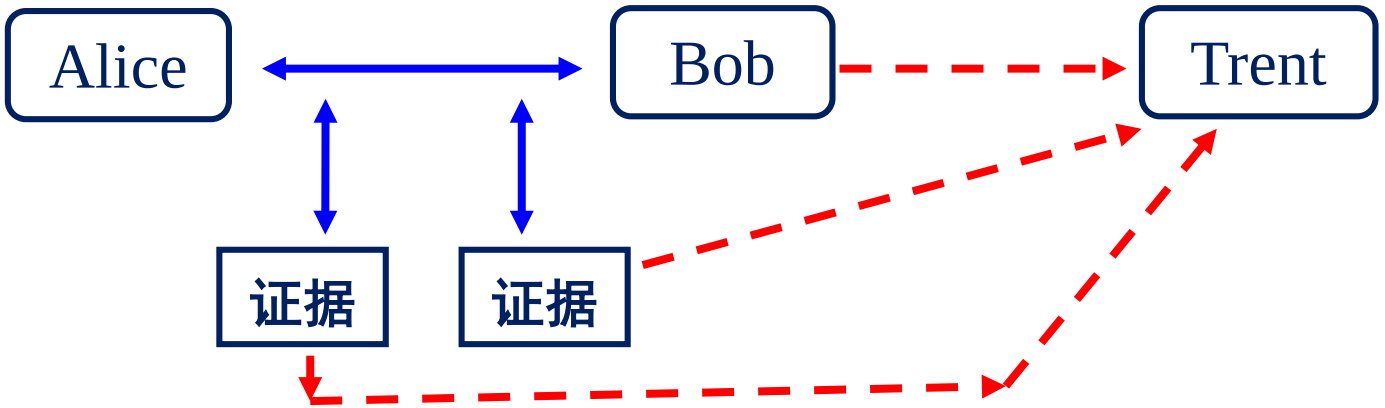
例如：在汽车交易中，Trent可以是律师，双方共同信任他：

1. Alice将车主权和钥匙交给律师；
2. Bob将支票交给Alice；
3. Alice在银行兑现支票；
4. 在规定的时间内，若证明支票是真的，律师将车主权和钥匙交给Bob；若支票是假的，Alice向律师提供证据，此后律师将车主权和钥匙归还Alice。

仲裁协议的特点

- 在计算机网络通信中，彼此互不信任的通信双方在通信时，通常需要某台计算机充当仲裁者。
- 在计算机网络中，要设立一个仲裁者，就要象平请律师一样付出一定的费用。然而在开放网络环境下，没有人愿意承担这种额外的开销。
- 协议中引入仲裁时，由于仲裁者需要对每次对话加以处理，会增加时延。当用户量很大时，它有可能成为系统的瓶颈。
- 仲裁者的服务器会成为黑客攻击的目标。一旦仲裁服务器被攻破，通信双方的信息就会泄露。在此类协议中，对仲裁服务器的安全保护是重点。

1.2 裁决协议



- 裁决人(adjudicator)也是公正的可信赖的第三方，但他不直接参与协议。这是区别于仲裁协议的情况。
- 一旦通信双方发生纠纷，则需要双方向裁决人提供各自掌握的证据，由裁决人来加以裁决。

裁决协议举例说明

- 无仲裁子协议
  1. **Alice和Bob协商协议条款；**
  2. **Alice签署这个合同；**
  3. **Bob签署这个合同；**
- 裁决子协议
  1. **Alice和Bob 出现在法官面前；**
  2. **Alice向法官提供他的证据；**
  3. **Bob向法官提供他的证据；**
  4. **法官根据双方提供的证据进行裁决。**

裁决协议的特点

- 裁决协议建立在通信双方均是诚实的基础上。
- 当有人怀疑发生欺骗时，可信赖的第三方就可以根据所提供的证据判定是否存在欺骗。
- 一个好的裁决协议应当能够确定欺骗者的身份；
- 裁决协议只能检测欺骗是否存在，但是不能防止欺骗的发生。

1.3 自执行协议

- 自执行协议(self-enforcing)协议是最好的协议。协议本身就保证了公平性。
- 这种协议不需要仲裁者的参与，也不需要仲裁者解决争端。
- 如果协议中的一方试图欺骗另一方，那么另一方会立刻检测到该欺骗的发生，并停止执行协议。

好的协议应具备的特点

- 协议涉及的各方必须知道此协议的所有步骤。
- 协议涉及的各方必须同意遵守协议。
- 协议必须是非模糊的。对协议的每一步都必须确切定义，力求避免产生误解。
- 协议必须是完整的。对每一种可能发生的情况都要作出反应。
- 每一步操作要么是由一方或多方进行计算，要么是在各方之间进行消息传递，二者必居其一。

二、安全协议分类及基本密码协议

根据安全协议的功能分类

- 认证协议 (authentication protocol)；
- 密钥建立（或者密钥交换、密钥分配）协议 (key agreement/ exchange/distribution protocol)；
- 认证的密钥建立（交换、分配）协议 (authenticated key agreement/exchange/distribution protocol)。

根据ISO的七层参考模型分类

- 高层协议 (higher layer protocol)
- 低层协议 (lower layer protocol)。

安全协议分类及基本密码协议（续）

根据协议中采用的算法分类

- 双钥（或公钥）协议 (public-key protocol)
- 单钥协议 (secret-key protocol)
- 混合协议 (hybrid protocol)

安全协议分类及基本密码协议（续）

比较科学的分类方法是：

- 认证协议 (authentication protocol)——向一个实体提供关于另外一个实体身份的确信度；
- 密钥建立协议 (key establishment protocol)—— 在两个通信实体之间建立共享密钥；
- 认证的密钥建立协议(authenticated key establishment protocol) ——在另一实体的身份已被证实的基础之上，两个通信实体之间建立共享密钥。

2.1 密钥建立协议

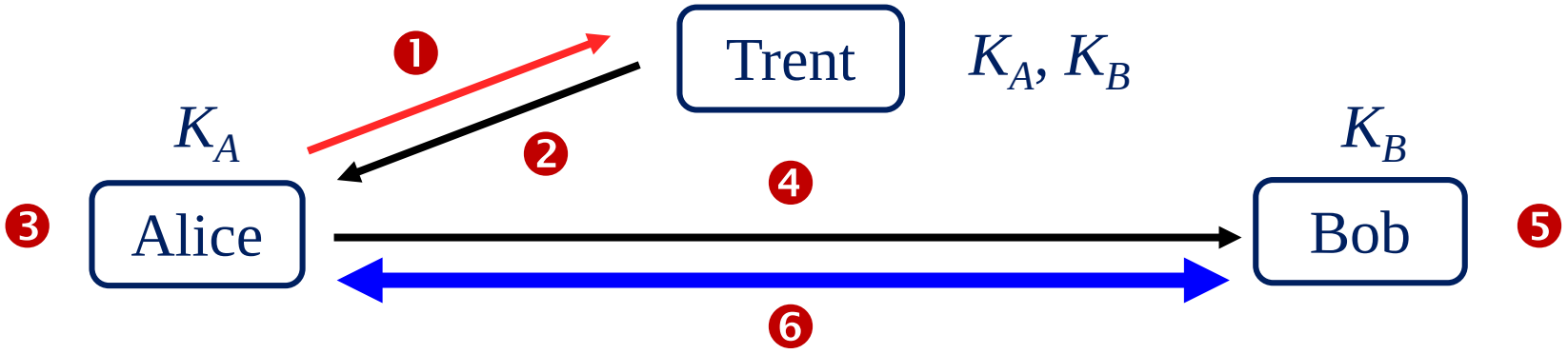
密钥建立协议可在实体之间建立会话密钥

- 该会话密钥（共享秘密）通常用作通信双方一次性通信的密钥；它也可以扩展到多方共享密钥建立，如会议密钥建立。
- 协议可以采用单钥、双钥体制实现，有时要借助于可信赖的第三方实现；
- 密钥传输协议：密钥从一个实体传给另一个实体
- 密钥协商协议：由双方或多方共同提供信息建立起共享密钥。

什么是会话密钥？

- 在保密通信中，通常对每次会话都采用不同的密钥进行加密，所以叫做会话密钥。会话密钥只在通信的持续范围内有效。通信结束后，会话密钥会被清除。

（1）采用单钥体制的密钥建立协议



① **Alice → Trent：请求得到与Bob的会话密钥；**

② **Trent → Alice：** $E_{K_A}(Key)$, $E_{K_B}(Key)$

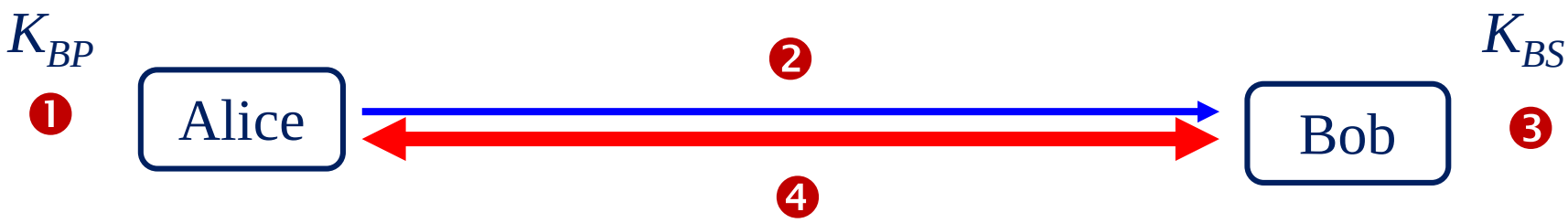
③ **Alice解密：** $D_{K_A}[E_{K_A}(Key)]=Key$

④ **Alice → Bob：** $E_{K_B}(Key)$

⑤ **Bob解密：** $D_{K_B}[E_{K_B}(Key)]=Key$

⑥ **Alice和Bob：采用会话密钥*Key*进行保密通信。**

（2）采用双钥体制的密钥建立协议



① **Alice从数据库中得到Bob的公钥；**

② **Alice → Bob：** $E_{K_{BP}}(Key)$

③ **Bob解密：** $D_{K_{BS}}[E_{K_{BP}}(Key)] = Key$

④ **Alice和Bob：采用会话密钥*Key*进行保密通信。**

注意：

- 此协议没有对公钥的合法性进行验证，所以不能抵抗中间人攻击。
- 要解决公钥合法性的问题，必须采用**PKI/CA**数字证书技术。

（3）中间人攻击

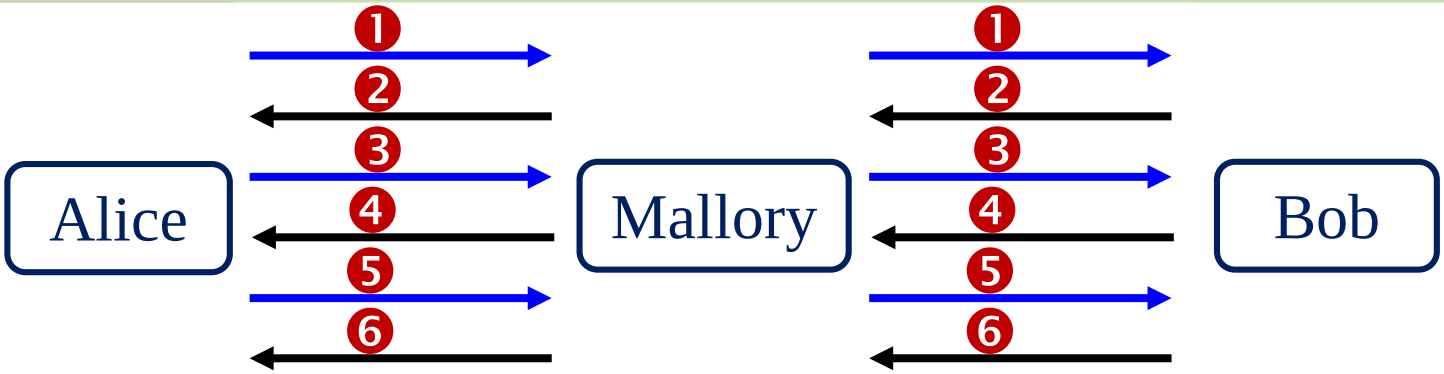
① Alice → Bob：Alice发送其公钥K_{AP}给Bob；Mallory截获这一公钥，并将自己的公钥K_{MP}发送给Bob；

② Bob → Alice：Bob发送其公钥K_{BP}给Alice；Mallory截获此公钥，并将自己的公钥K_{MP}发送给Alice；

③ Alice → Bob：当Alice采用“Bob”的公钥对消息加密并发送给Bob时，Mallory就会截获并解密此消息；

④ Bob → Alice：当Bob采用“Alice”的公钥对消息加密并发送给Alice时，Mallory就会截获并解密此消息。

（4）联锁协议



① Alice → Bob：Alice发送其公钥K_{AP}给Bob；

② Bob → Alice：Bob发送其公钥K_{BP}给Alice；

③ Alice → Bob：Alice采用Bob的公钥对消息加密，并发送一半密文给Bob；

④ Bob → Alice：Bob采用Alice的公钥对消息加密，并发送一半密文给Alice；

⑤ Alice → Bob：Alice将另一半密文发送给Bob；Bob将两半密文组合在一起，并采用其私钥K_{BS}解密；

⑥ Bob → Alice：Bob发送它的另一半密文给Alice；Alice将Bob的两半密文组合在一起，并采用其私钥K_{AS}解密。

联锁协议的安全性讨论

联锁协议可以有效地抵抗中间人攻击

- 当仅获得一半而未获得另一半密文时，这些数据对攻击者毫无用处，因为攻击者无法解密（见书236页）。

在实际中如何实现呢？

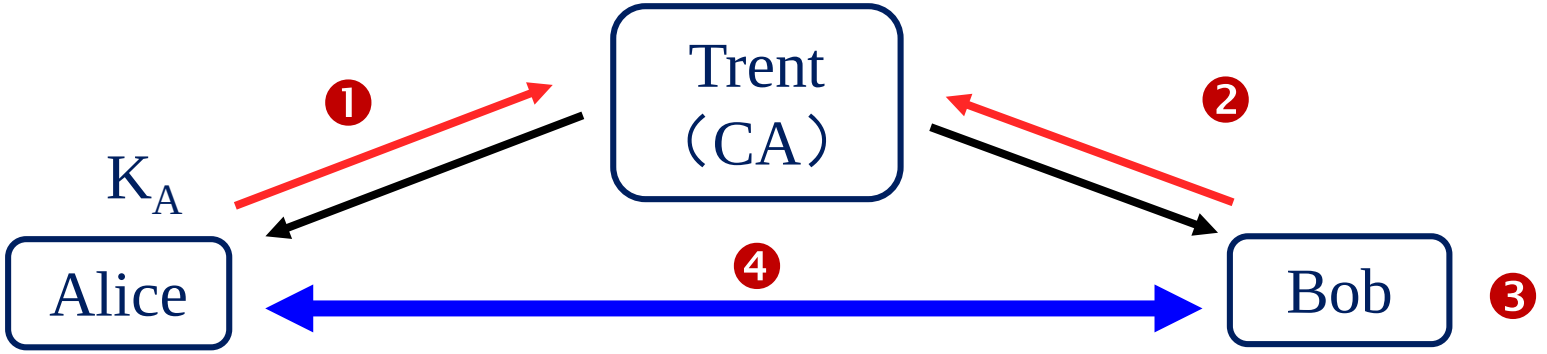
① 如果采用初始化矢量*IV*的分组加密模式（如CBC/CFB/OFB）：

- 第一半消息：密文输出
- 第二半消息：初始化矢量*IV*

② 如果收发双方可以计算杂凑函数值，

- 第一半消息：加密消息的单向杂凑函数值
- 第二半消息：密文输出

（5）采用数字签名的密钥交换



① **Alice从Trent中得到Bob的数字证书**

(CA用其私钥对Bob公钥进行签名)；

① **Bob从Trent中得到Alice的数字证书**

(CA用其私钥对Alice公钥进行签名)；

③ **Alice和Bob均可采用CA的公钥验证数字证书（CA签名）的正确性，并获得对方的可信公钥；**

④ **Alice和Bob：采用可信的公钥进行保密通信。**

（6）密钥和消息传输

①Alice生成一随机数K，并用其对消息M加密：$E_K(M)$；

②Alice从数据库中得到Bob的公钥；

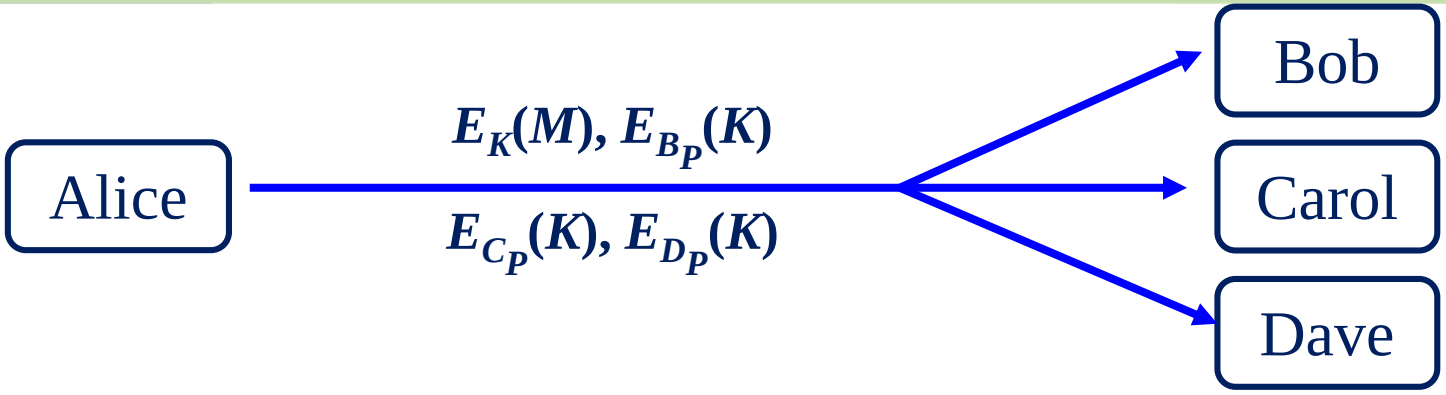
③Alice用Bob的公钥对会话密钥加密：$E_{B_P}(K)$

④Alice将加密的消息和会话密钥发送给Bob：$E_K(M), E_{B_P}(K)$

⑤Bob采用其私钥对Alice的会话密钥解密：$D_{B_S}[E_{B_P}(K)]=K$

⑥Bob采用会话密钥K对Alice的消息解密：$D_K[E_K(M)]=M$

（7）密钥和消息广播



①Alice生成一随机数K，并用其对消息M加密：$E_K(M)$；

②Alice从数据库中得到Bob, Carol, Dave的公钥；

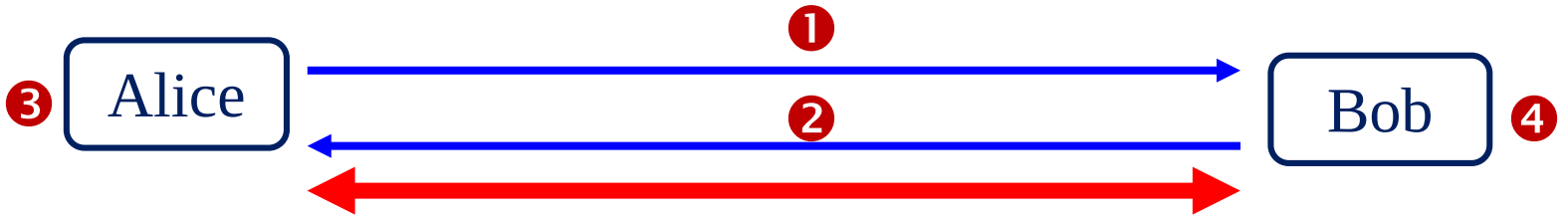
③Alice用Bob, Bob, Carol, Dave的公钥对会话密钥加密：$E_{B_P}(K)$, $E_{C_P}(K)$, $E_{D_P}(K)$

④Alice广播加密的消息和所有加密的会话密钥：$E_K(M)$, $E_{B_P}(K)$, $E_{C_P}(K)$, $E_{D_P}(K)$

⑤仅有Bob，Carol，Dave可以采用各自的私钥解密求出会话密钥K：$D_{B_S}[E_{B_P}(K)]=K$，$D_{C_S}[E_{C_P}(K)]=K$，$D_{D_S}[E_{D_P}(K)]=K$

⑥Bob , Carol, Dave采用会话密钥K对Alice的消息解密：$D_K[E_K(M)]=M$

（8）Diffie-Hellman密钥交换协议



约定：Alice和Bob均知道两个大素数n和g，g是群$(0,\ldots,n-1)$上的本原元。这两个整数公开，可通过不安全信道传输它们。

① Alice→Bob：Alice选择一个随机的大整数x: $X=g^x \bmod n$

② Bob→Alice：Bob选择一个随机的大整数y: $Y=g^y \bmod n$

③ Alice计算：$K=Y^x \bmod n=g^{xy} \bmod n$

④ Bob计算：$K=X^y \bmod n=g^{xy} \bmod n$

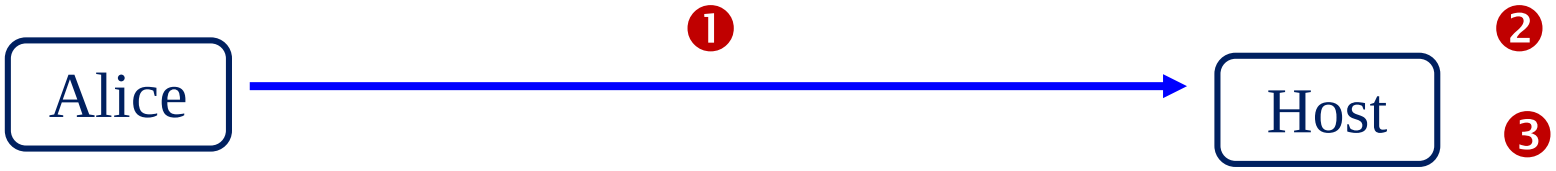
至此，Alice和Bob就可以采用密钥K进行保密通信。

注意：Diffie-Hellman攻击不能抵抗中间人攻击！要学会证明！

2.2 认证协议

- 认证包含消息认证、数据源认证和实体认证，用以防止欺骗、伪装等攻击。
- 传统的认证方法是采用口令来解决这个问题。
- 但是，口令容易被窃取。所以，采用口令认证的方式，其安全性比较脆弱。
- 要解决这个问题，必须设计安全的认证协议，以防止假冒和欺骗等攻击。
- 认证分为单向认证和双向认证。

（1）采用单向函数的认证协议



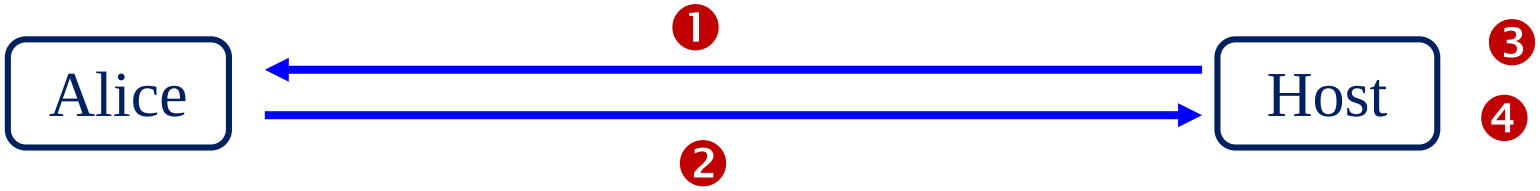
①**Alice → Host：** **Alice向主机发送它的口令：*Passwd***

②**Host计算该口令的单向（杂凑）函数值：*MD'=H(Passwd)***

③**Host将计算得到的*MD'*与预先存储的值*MD*进行比较；**

④**如果相同，则通过认证；如果不同，则拒绝Alice登录。**

（2）采用双钥体制的认证



① **Host → Alice**： 主机向Alice发送一随机数：R

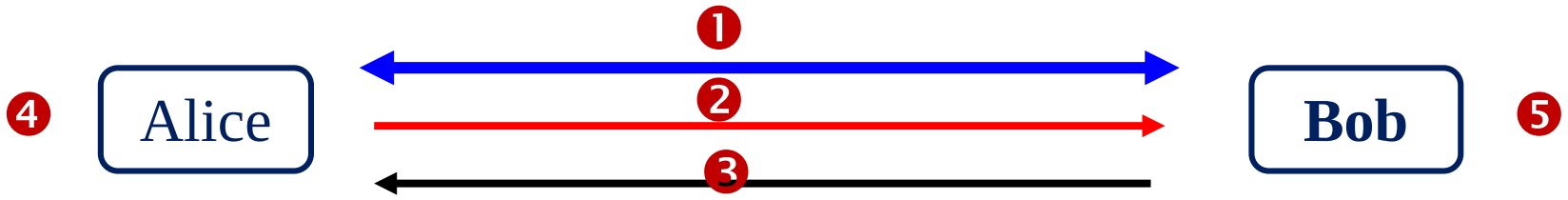
② **Alice → Host**：$E_{A_S}(R)$（实质上就是对R签名），ID_A

③ Host在其数据库中搜索Alice的公钥，并采用此公钥解密（实质是验证签名）：$D_{A_P}[E_{A_S}(R)]=R'$

④ 如果$R=R'$，则通过认证；如果$R\neq R'$，则拒绝Alice登录。

注意：此协议实现了Host对Alice 的认证，而没有实现Alice对Host 的认证，因此认证是单向的。

（3）采用联锁协议的双向认证



① Alice(口令P_A) 和Bob (口令P_B)相互交换公钥；

② Alice → Bob：$E_{B_P}(P_A)$

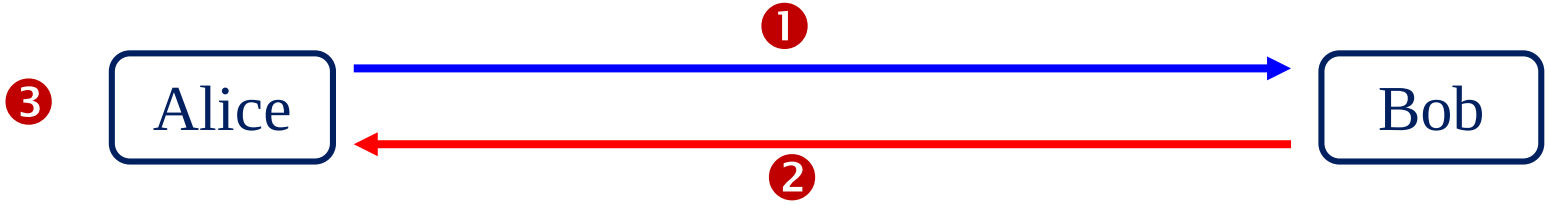
③ Bob → Alice：$E_{A_P}(P_B)$

④ Alice对③中收到的消息解密，并验证：$D_{A_S}[E_{A_P}(P_B)]=P_B$

⑤ Bob对2中收到的消息解密，并验证：$D_{B_S}[E_{B_P}(P_A)]=P_A$

注意：Mallory可以对此协议成功实施中间人攻击。

（4）SKID身份识别协议



SKID2和SKID3采用单钥体制构造(RACE的RIPE计划，MAC)

下面是单向认证协议SKID2：Bob向Alice认证其身份。

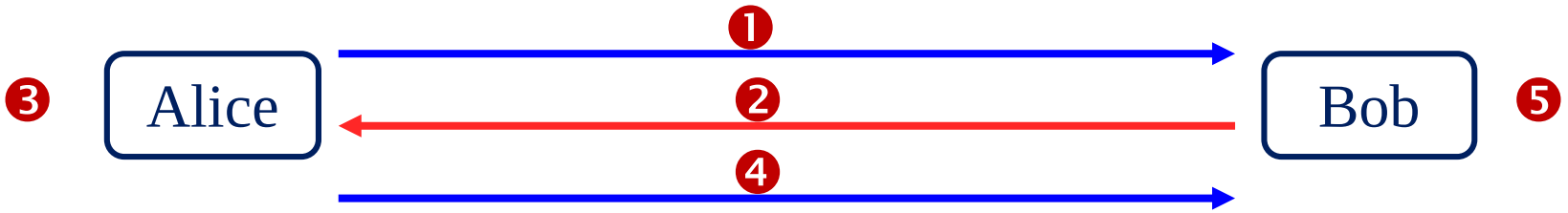
① **Alice → Bob：** 随机数R_A（RIPE规定为64b）

② **Bob → Alice：** 随机数R_B，$H_K(R_A, R_B, B)=MAC(K, R_A||R_B||B)$

③ **Alice：** 计算$H_K'(R_A, R_B, B)=MAC'(K, R_A||R_B||B)$，并与收到来自Bob的值进行比较。若相等，则Alice成功认证Bob；否则，Alice认为Bob不拥有密钥K，所以是非法的。

注意：此协议不能抵抗中间人攻击（请同学自己证明）。

双向SKID身份识别协议—SKID3



① Alice → Bob：随机数R_A（RIPE规定为64b）

② Bob → Alice：随机数R_B，$H_K(R_A, R_B, B)=MAC(K, R_A||R_B||B)$

③ Alice：计算$H_K'(R_A, R_B, B)=MAC(K, R_A||R_B||B)$，并与收到来自Bob的值进行比较。若相等，则Alice成功认证Bob；否则，Alice认为Bob不拥有密钥K，所以是非法的。

④ Alice → Bob：$H_K(R_B, A)=MAC(K, R_B||A)$

⑤ Bob：计算$H_K'(R_B, A)=MAC(K, R_B||A)$，并与收到来自Alice的值进行比较。若相等，则Bob成功认证Alice ；否则，Bob认为Alice不拥有密钥K，所以是非法的。

注意：此协议不能抵抗中间人攻击（请同学自己证明）。

（5）消息认证

当Bob收到Alice的消息*M*，它如何判断这条消息是真的？

有以下三种方法：

- Alice对消息*M*签名，并将签名发给Bob。
- Alice采用单钥体制对消息*M*加密，并将密文发给Bob。
- Alice计算消息*M*的MAC值，并将MAC发送给Bob。

注意：第一种方法可以向Trent证明此消息来自Alice；

第二、第三种方法不能向Trent证明此消息来自Alice。

2.3 认证的密钥建立协议

- 这类协议将认证和密钥建立结合在一起，使Alice和Bob确信他们正在与可信赖的对方进行保密通信。
- 密钥认证分为三种：

① 隐式密钥认证。Alice确信Bob的身份，只需验证密钥。

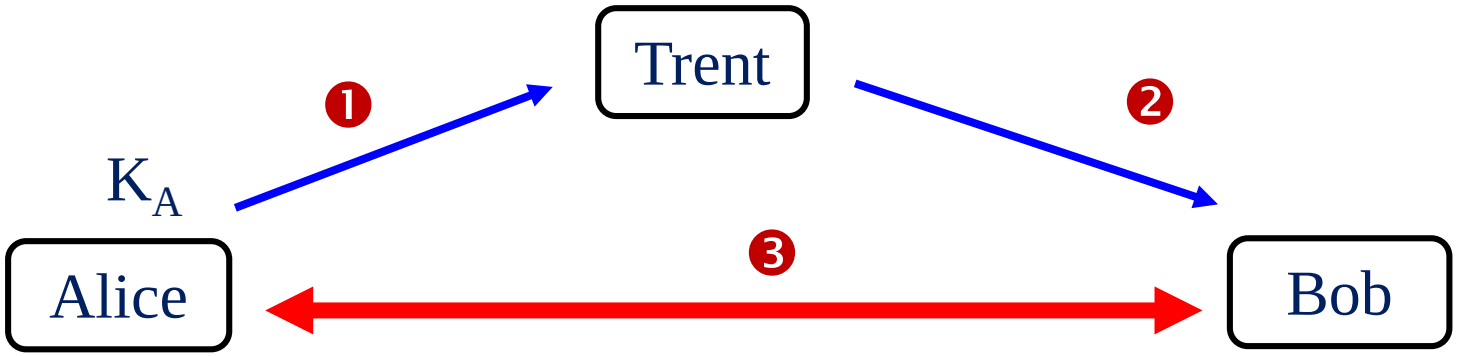
② 密钥确认：Alice确信未经身份识别的Bob确实拥有某个特定密钥。此类协议的中心问题是识别Bob的密钥值。

③ 显式密钥认证：Alice确信经过身份识别的Bob确实拥有某个特定密钥。此类协议的中心问题是识别Bob的身份。

认证和密钥交换协议中采用的符号

A	Alice的姓名识别符
B	Bob的姓名识别符
E_A	采用Trent与Alice共享的密钥加密
E_B	采用Trent与Bob共享的密钥加密
I	索引号码
K	随机会话密钥
L	有效期
T_A，T_B	时戳（Timestamp）
R_A，R_B	由Alice和Bob选择的一次随机数（nonce）
S_T	Trent的签名

（1）大嘴青蛙协议



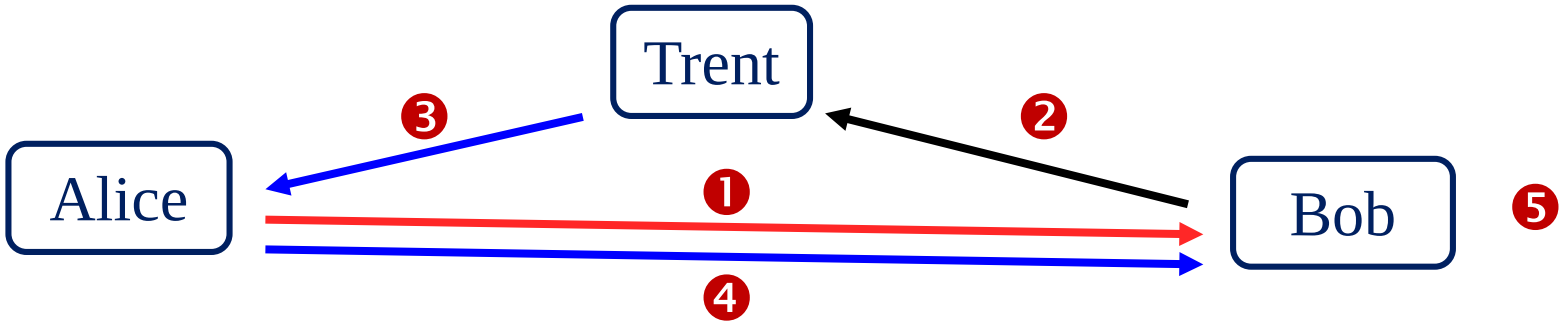
该协议是最简单的三方协议，采用单钥体制构造：

① **Alice → Trent：** $A, E_A(T_A, B, K)$

② **Trent → Bob：** $E_B(T_T, A, K)$

③ **Alice与Bob：** 共享密钥K。此后，双方将采用密钥K进行保密通信。

（2）Yahalom协议



① **Alice → Bob：** A, R_A

② **Bob → Trent：** B, $E_B(A, R_A, R_B)$

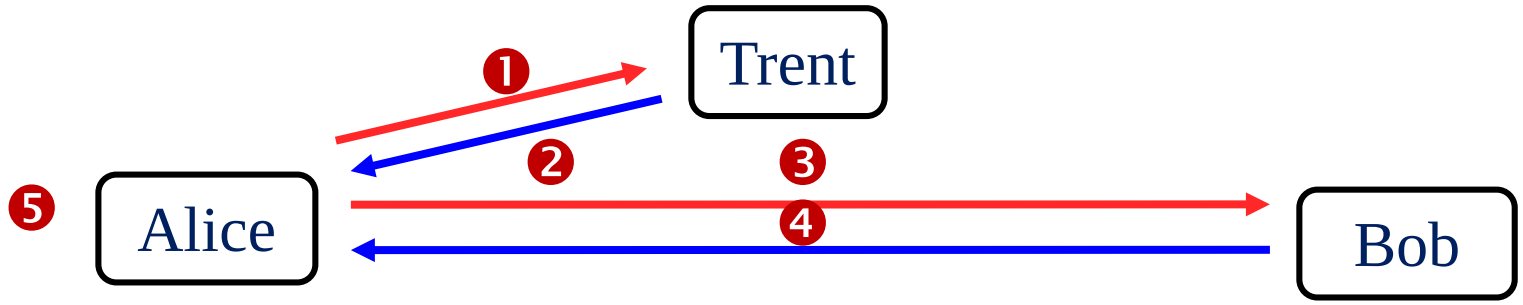
③ **Trent → Alice：** $E_A(B, K, R_A, R_B)$, $E_B(A, K)$

④ **Alice：** 解密第1条消息，提取K，并验证R_A与①中相等；然后，发送给Bob： $E_B(A, K)$, $E_K(R_B)$

⑤ **Bob：** 用它的共享密钥对第1条消息解密，求出K；然后，采用K，求出R_B。验证是否与②中的值相同。

（3）Kerberos协议

（3）Kerberos协议



① **Alice → Trent：** A, B

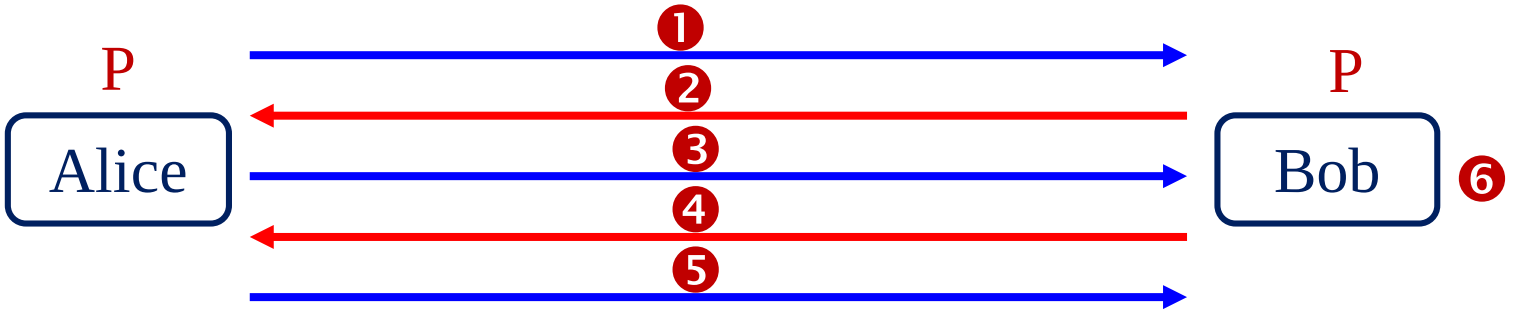
② **Trent → Alice：** $E_A(T, L, K, B)$， $E_B(T, L, K, A)$

③ **Alice → Bob：** 对第一条消息解密得到K；然后，向Bob发送消息： $E_K(A, T)$， $E_B(T, L, K, A)$

④ **Bob → Alice：** 对收到的消息解密，得到K；然后，将T加1，采用K加密后发送给Alice： $E_K(T+1)$

⑤ **Alice：** 对收到的消息解密求出$T+1$，并验证其正确性。

（4）EKE协议



此协议假设：Alice和Bob共享一个秘密口令P

① Alice → Bob：$A, E_P(K')$

② Bob → Alice：$E_P[E_{K'}(K)]$

③ Alice → Bob：$E_K(R_A)$

④ Bob → Alice：$E_K(R_A, R_B)$

⑤ Alice → Bob：$E_K(R_B)$

⑥ Bob：采用K对消息解密得到R_B，并验证是否被篡改。如果R_B没有被篡改，说明Alice是知道口令P。此后，双方用K进行保密通信。

三、秘密分拆协议

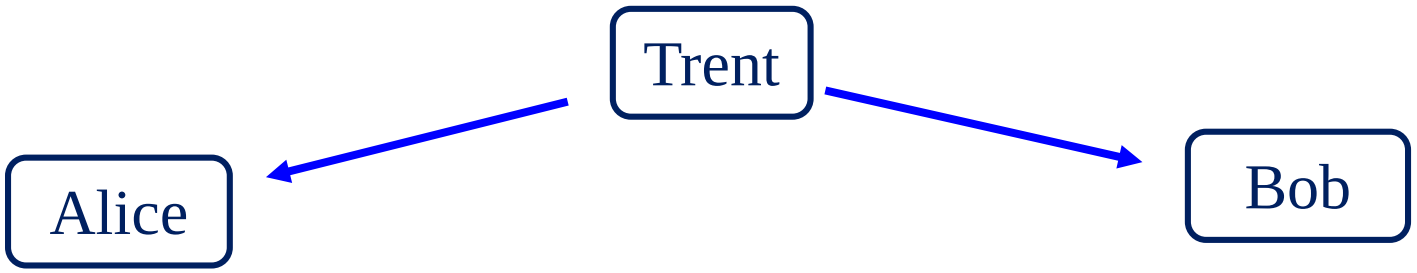
问题提出

- 假如你有一种饮料的配方，但出于保密考虑，只能将配方让最亲密的人知道；
- 如果任何一个人背叛了你，就会将配方出卖给竞争对手。

解决方案

- 将秘密配方分拆，一个人只能掌握配方中一种成分的比例；
- 一个人出卖配方，将毫无用处；
- 只有所有的人组合在一起，才能恢复配方。

秘密分拆协议（2方）



① Trent生成一随机比特串R，它与消息M具有相同的长度；

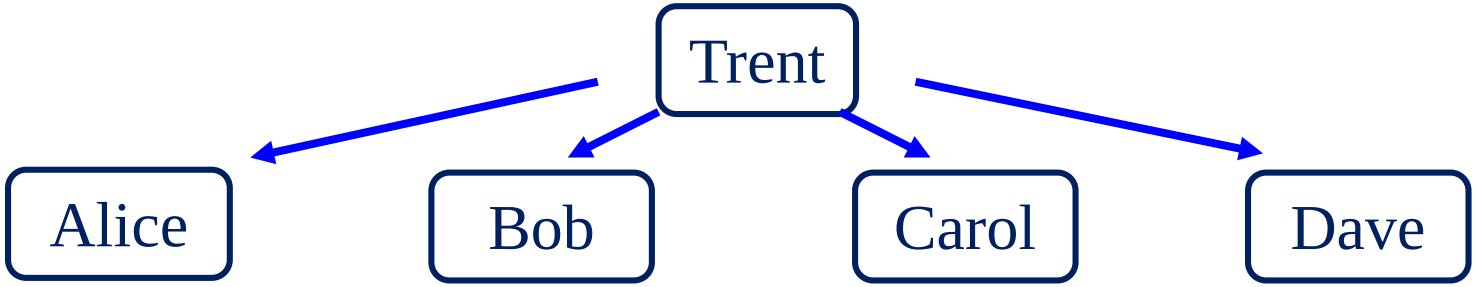
② Trent将M与R进行异或运算，得到S：$S=M\oplus R$

③ Trent将R分给Alice，而将S分给Bob。

若想重组这条消息，Alice和Bob仅需执行：

④ Alice和Bob将各自得到的比特串进行异或运算，就会得到消息M：$M=S\oplus R$

秘密分拆协议（4方）



① Trent生成3个随机数R, S, T，它们与消息M具有相同的长度；

② Trent将M与3个随机数进行异或运算，得到$U=M\oplus R\oplus S\oplus T$

③ Trent将R分给Alice，S分给Bob，T分给Carol，U分给Dave。

④ Alice、Bob、Carol和Dave将各自得到的比特串进行异或运算，就会得到消息M：$M=U\oplus R\oplus S\oplus T$

五、密码协议的安全性

问题提出

- 认证协议是许多分布式系统安全的基础。虽然密码协议中仅仅进行很少的几组消息传输，但是其中每一消息的组成都是经过巧妙设计的，而且这些协议之间有着复杂的相互作用和制约。
- 但是，因为设计上的漏洞，很多协议都存在严重的安全缺陷。

存在缺陷的原因

- 协议设计者有可能误用了所采用的密码技术
- 协议不恰当地照搬了其他协议的某些特性
- 对某一特定的通信环境及其安全需求研究不够

5.1 对密码协议的攻击

1. 已知明文攻击
   - 攻击者通过搭线窃听，收集明文/密文对。通过长期窃听，攻击者可以建立一个加密表。有可能进一步发现密钥。
2. 选择密文攻击
   - 攻击者选择特定的密文比特串如全0和全1，来更快地解出密钥。这种攻击是主动攻击，因此更危险。
3. 预言者会话攻击
   - （详见书259页）
4. 并行会话攻击
   - （详见书260页）

5.2 密码协议的安全性分析

攻击检验法

这种方法就是采用现有的一些有效的协议攻击方法，逐个对协议进行攻击，检验其是否具有抵御这些攻击的能力。分析时，主要采用语言描述的形式，对协议所交换的密码消息的功能进行剖析。

形式语言逻辑分析法

- 采用非专门语言和验证工具对协议建立模型并加以验证。
- 通过开发专家系统，对密码协议进行开发研究。
- 采用基于知识和信任的逻辑，对协议进行安全性研究。
- 基于密码系统的代数特点，开发某种形式方法对协议进行分析和验证。

5.2 密码协议的安全性分析

可证安全性分析法

- 针对密码协议运行环境，定义协议安全目标，攻击者能获得服务
- 虚构一个仿真器，利用已知的困难问题参数，模拟协议提供的所有服务，包括协议的公开参数和真实协议运行中攻击者能够获得所有数据
- 虚构一个成功的攻击者，从仿真器那儿获得所有现实攻击者能够的服务，攻击者最终能使协议目标失效
- 仿真器将攻击者证明自己能使得协议失效的证据转化为前述困难问题的解
- 由于上述已知的困难问题没有有效的解法，所以这样的攻击者就不可能存在，即协议是安全的，否则该攻击者可以作为一个子程序加以调用从而表明该问题有有效算法求解，引出矛盾。

谢谢！