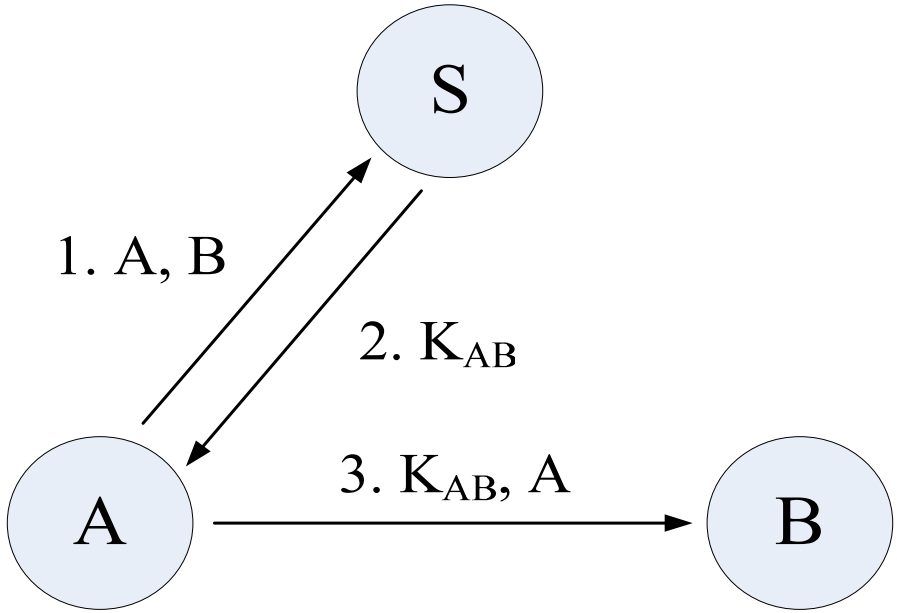
安全协议分析
(密码协议)

协议目标

- 在协议结束时，**K_{AB}**应该为**A**和**B**所知，但是除了**S**之外的其它主体应该无法知道**K_{AB}**
- **A**和**B**应该知道**K_{AB}**时最新产生的

第一次尝试协议



Alice-Bob 记号（Notation）

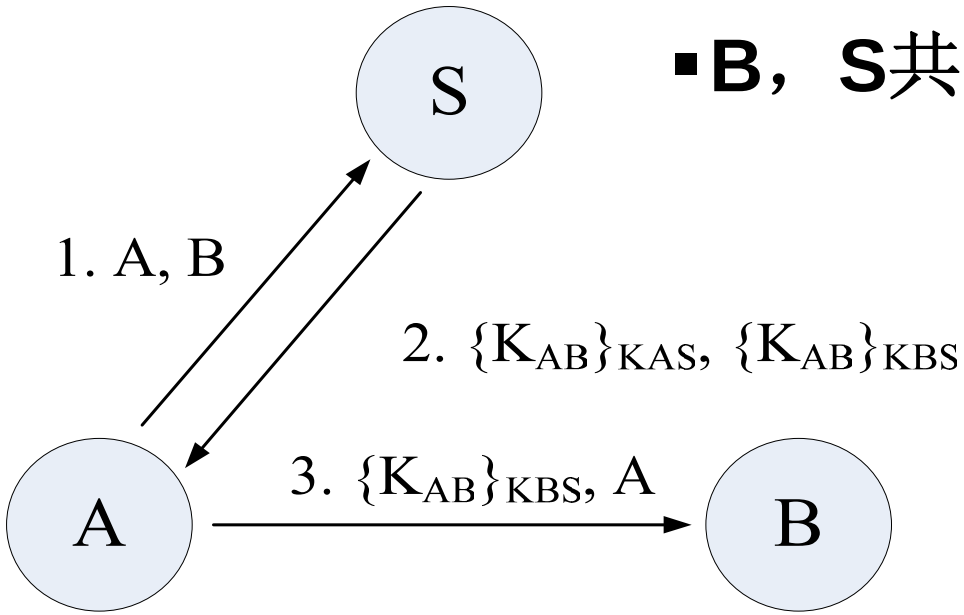
- **1. A → S : A, B　　→**
- **2. S → A : K_{AB}**
- **3. A → B : K_{AB}, A**
- 这种记法虽然简洁但是有很多局限

1.4.1 机密性(Confidentiality)

- 安全假设1:敌手能够窃听密码协议中传送的所有消息.

第二次尝试协议

- A，S共享：K_{AS}
- B，S共享：K_{BS}

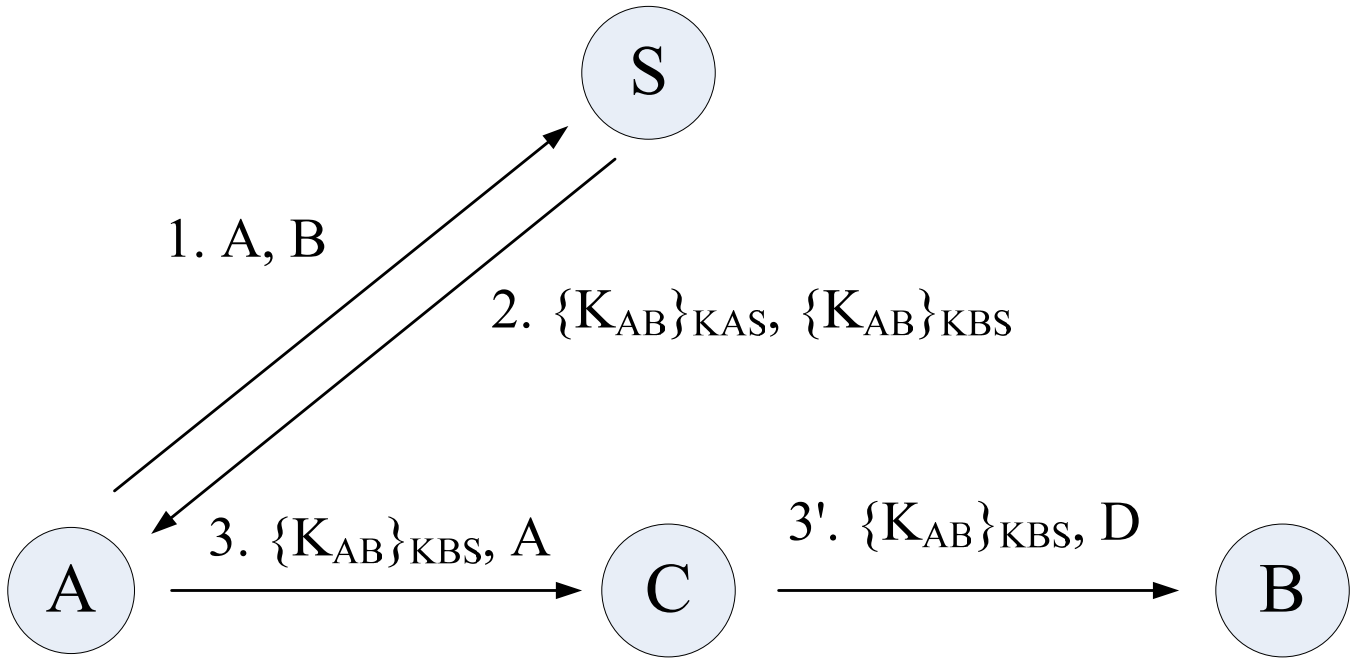


完美密码假设Perfect Cryptography

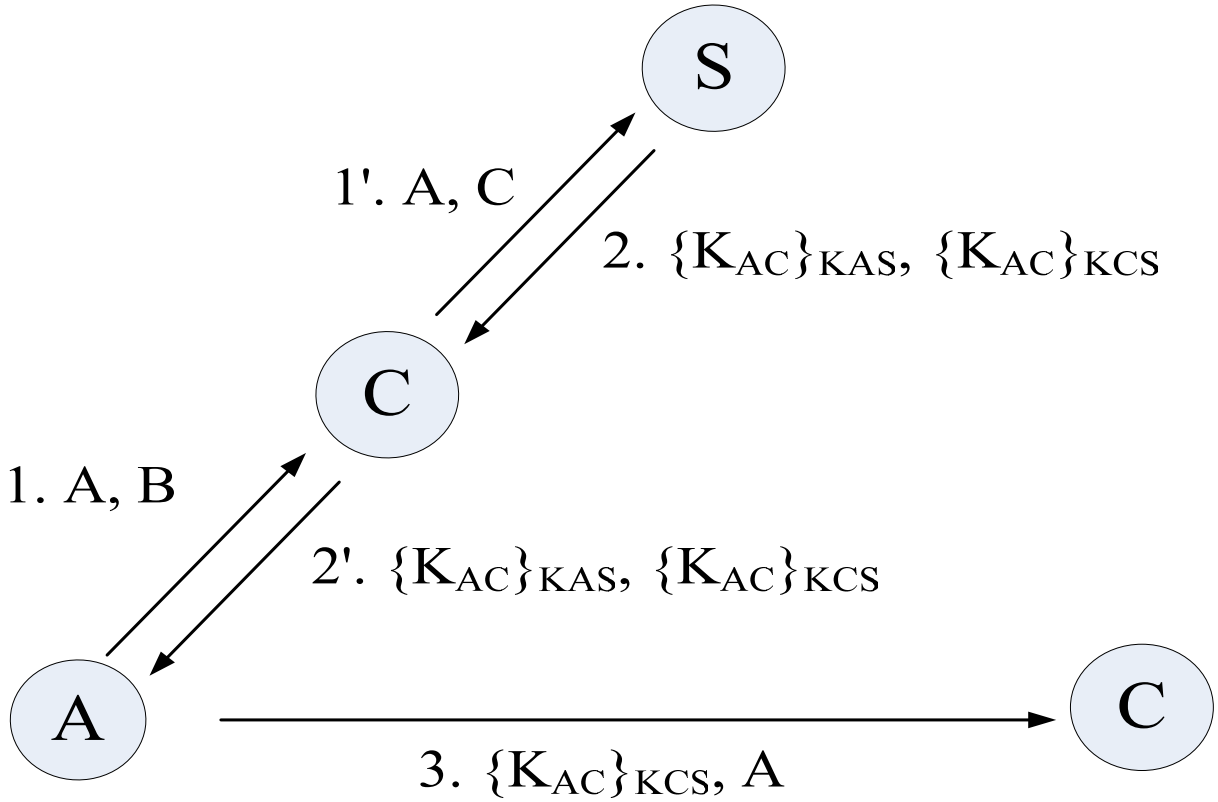
1.4.2 鉴别(Authentication)

- 安全假设2:敌手能够使用任何可用的信息修改一个密码协议中所传送的所有消息.敌手能够把任何消息重发给任何其他的主体.这包括产生和插入全新消息的能力.

对第二次协议的攻击

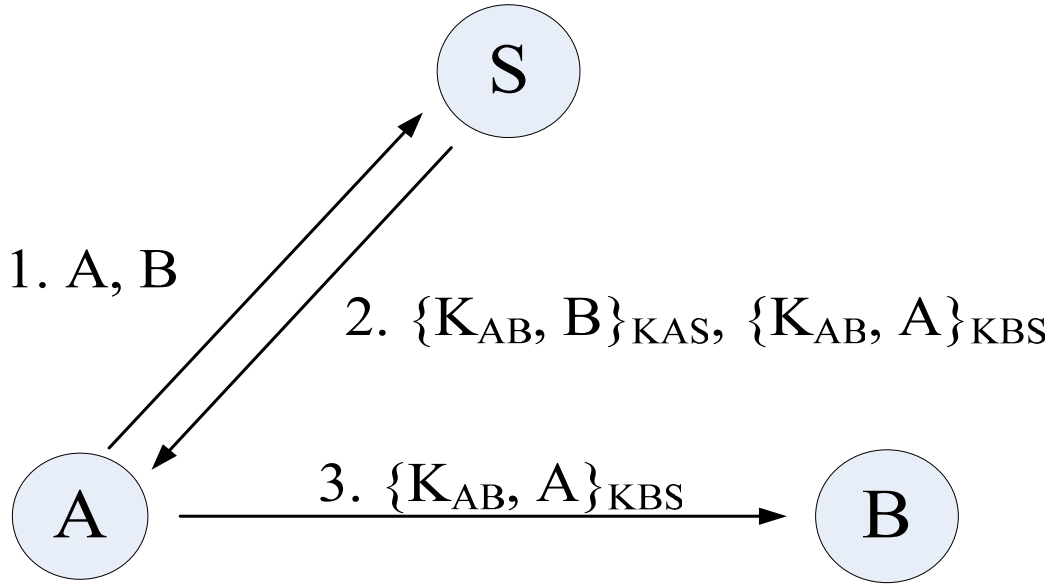


对第二次协议的另一种攻击



- 安全假设3:敌手可以是合法的协议参与者(an insider),或者一个外来者(an outsider),或者是两者的组合.

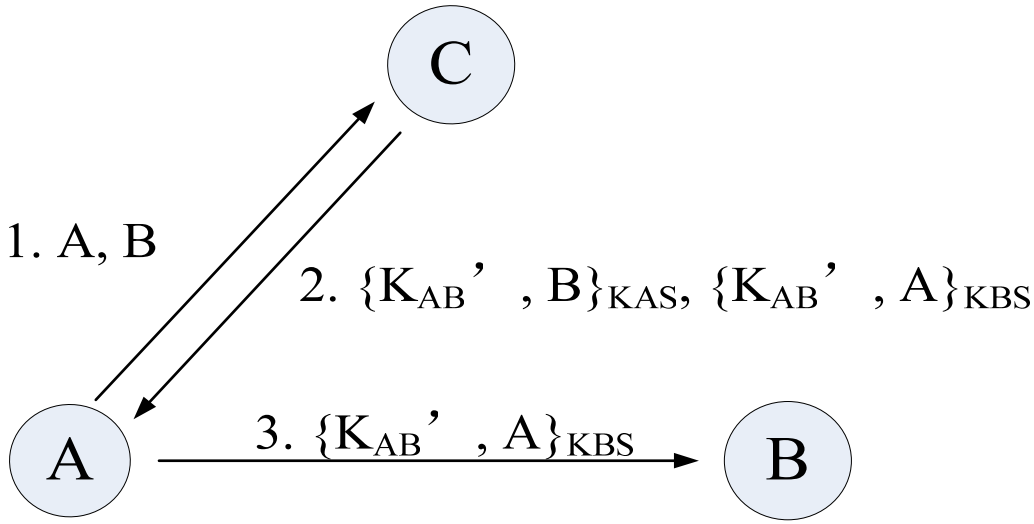
第三次尝试协议



1.4.3 重放(Replay)

- 安全假设4:敌手能够从以前协议运行中通过密码分析获取会话密钥K_{AB}.

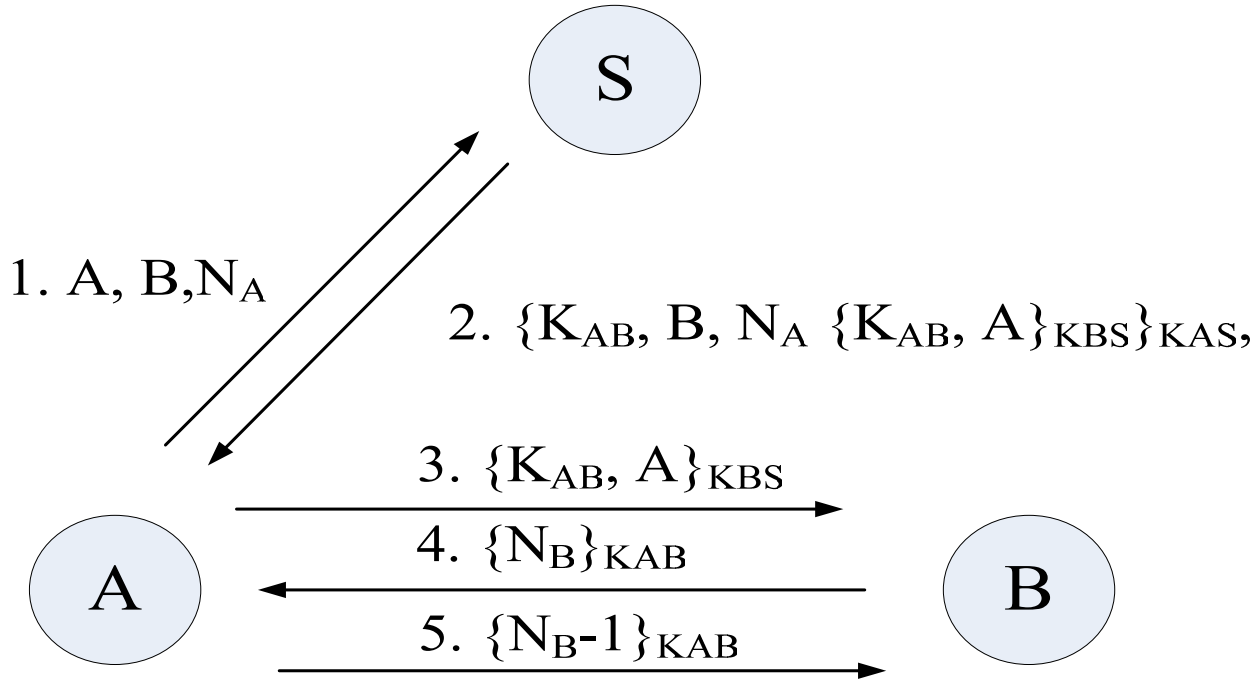
对第三次尝试协议的攻击



- 定义:一个临时值(Nonce)是一个主体产生的随机数并且在协议的一条消息中回传给该主体以表明此条消息是最新产生的.

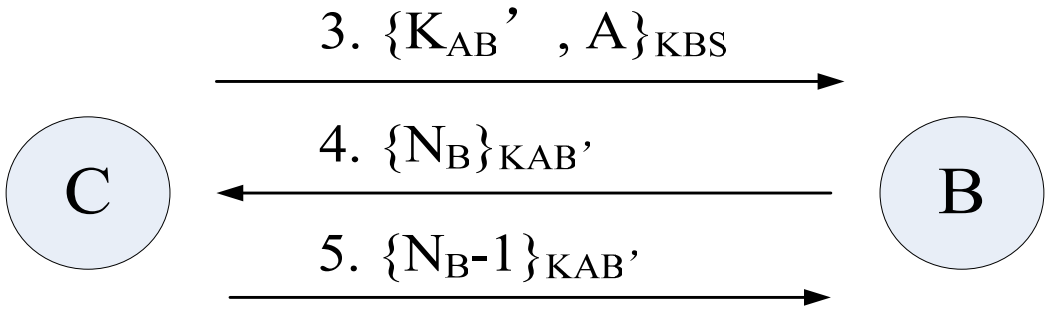
- 即挑战－应答（challenge-response）

第四次尝试协议（Needham-Schroeder）

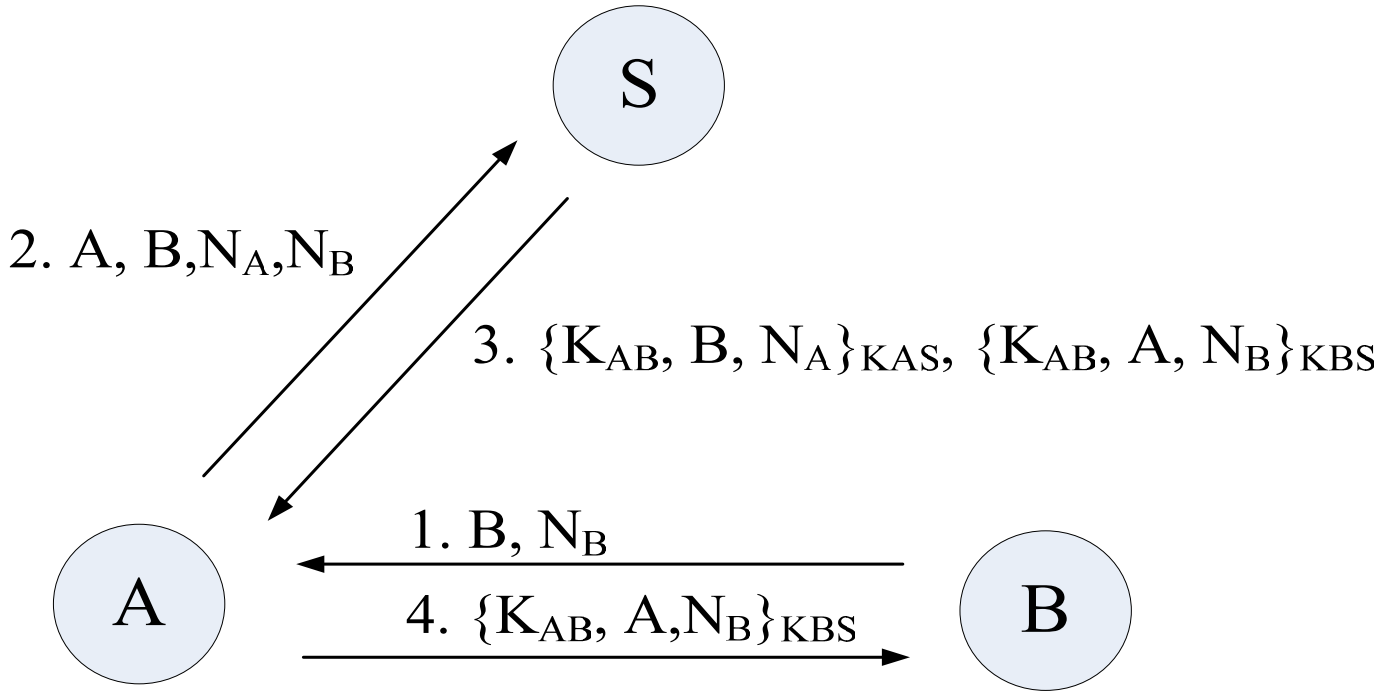


NSSK

对第四次尝试协议的攻击



第五次尝试协议（final）



- 对比最终协议和第四次尝试协议
- **Key Confirmation**