7　网络安全

7.1　网络安全问题概述

7.2　两类密码体制

7.3　数字签名

7.4　鉴别

7.5　密钥分配

7.6　因特网使用的安全协议

7.7　链路加密与端到端加密

7.8　防火墙

7　网络安全

7.1　概述

一．计算机网络面临的威胁：
截获，中断，篡改，伪造

网络安全面临的威胁

1．被动攻击

（1） 定义：截获网络上信息的攻击方式

（2） 原理：又叫通信量分析，攻击者不干扰信息流，通过观察某一个PDU的长度和传输的频度，掌握所交换数据的性质，了解正在通信的协议实体的地址和身份

（3） 解决：采用各种的数据加密技术：例如压缩等

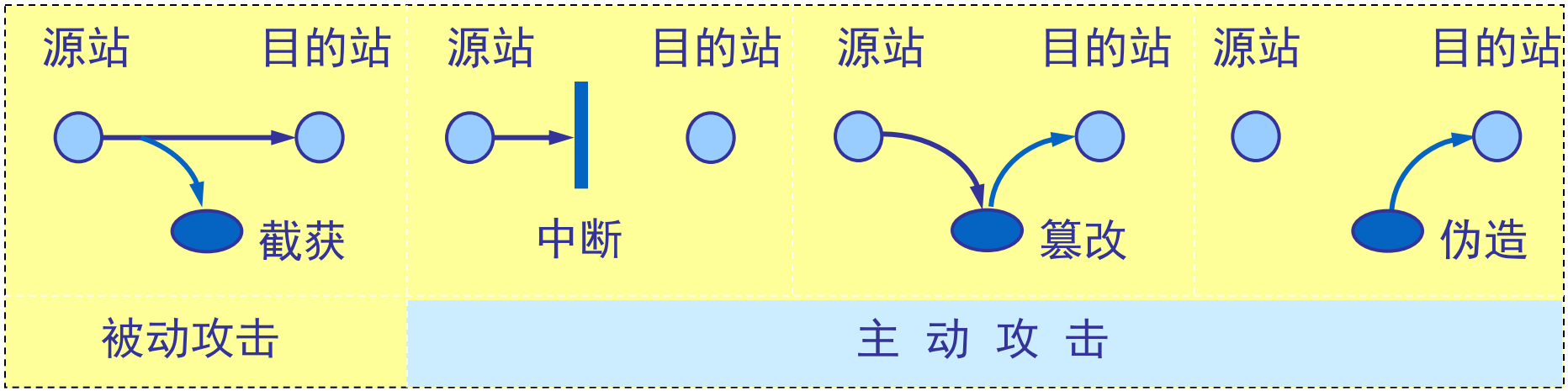
2．主动攻击

（1）　定义：更改或拒绝用户使用资源的攻击方式，中断、篡改、伪造等

（2）　原理：攻击者对某一个连接中通过的PDU进行处理，如：有选择地删改、延迟、插入、一些伪造的PDU

（3）　解决：加密技术与适当的鉴别技术相结合

对网络的被动攻击和主动攻击



二．网络安全的内容

1．保密性：为用户提供保密通信，
包括：存取控制中的登录口令，安全通信协议的设计、数字签名等

2．安全协议的设计：主要是针对具体的攻击设计安全的通信协议

如何保证设计出的协议是安全的？

协议安全性保证的方法

（1） 用形式化的方法来证明，由于协议的安全性是不可判定的，只能针对某种特定类型的攻击讨论其安全性，对复杂的通信协议，形式化的证明比较困难

（2） 用经验来分析

二．网络安全的内容

1．保密性：为用户提供保密通信，
包括：存取控制中的登录口令，安全通信协议的设计、数字签名等

2．安全协议的设计：主要是针对具体的攻击设计安全的通信协议

3．存取控制：对接入网络的权限加以控制，规定每个用户的接入权限（能读、能写）

计算机网络通信安全的目标

(1) 防止析出报文内容;

(2) 防止通信量分析;

(3) 检测更改报文流;

(4) 检测拒绝报文服务;

(5) 检测伪造初始化连接。

恶意程序(rogue program)

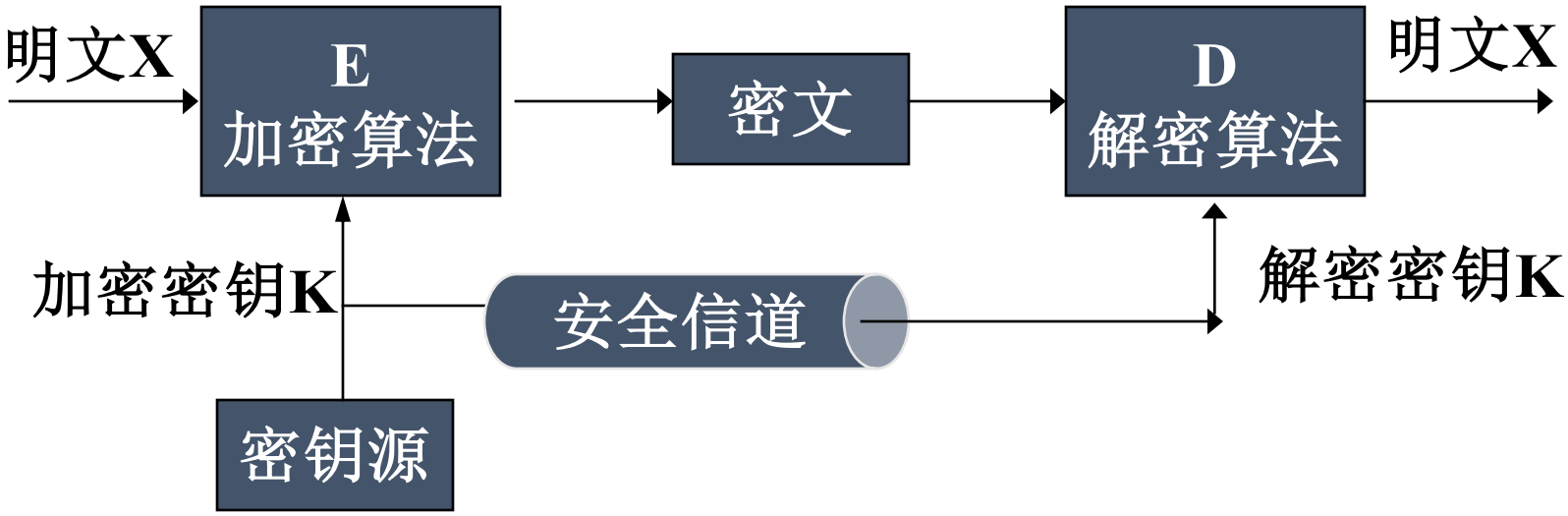
(1) 计算机病毒——会“传染”其他程序的程序，“传染”是通过修改其他程序来把自身或其变种复制进去完成的。

(2) 计算机蠕虫——通过网络的通信功能将自身从一个结点发送到另一个结点并启动运行的程序。

(3) 特洛伊木马——一种程序，它执行的功能超出所声称的功能。

(4) 逻辑炸弹——一种当运行环境满足某种特定条件时执行其他特殊功能的程序。

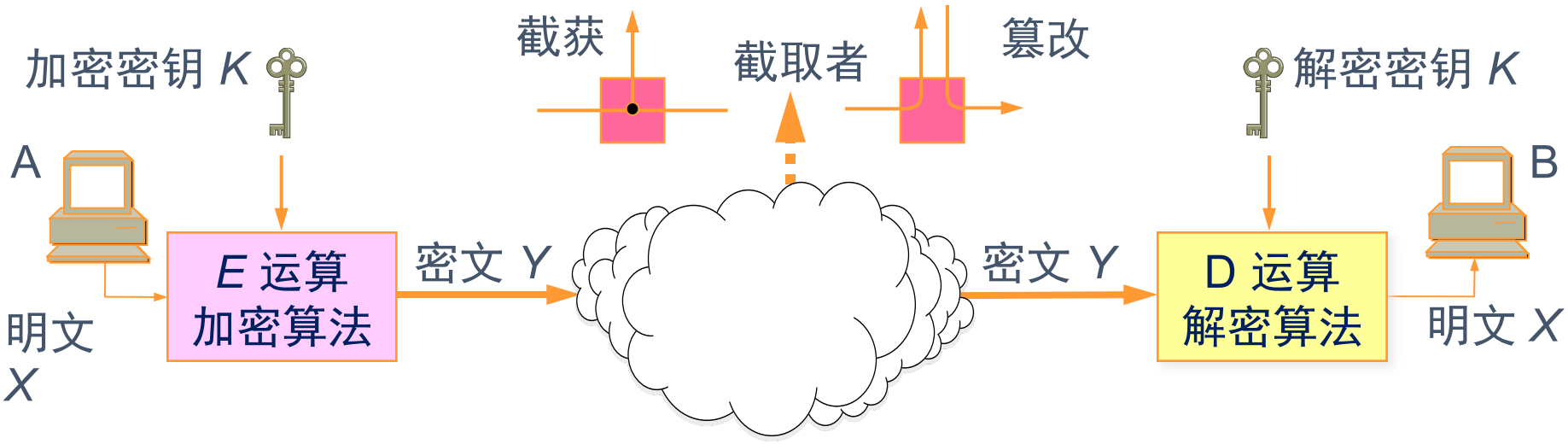
三．一般数据的加密模型
常规、公开密码密钥体制



发送端：明文X用加密算法和密钥源产生的加密密钥得到密文：

$Y=E_K（X）$

接收端：利用解密算法和通过安全信道传送过来的解密密钥K解出明文为$D_K（Y）=D_K（E_K（X））=X$


截获
截取者
篡改
加密密钥 K
解密密钥 K
A
B
E 运算
加密算法
密文 Y
密文 Y
D 运算
解密算法
明文
X
明文 X

7　网络安全

7.2　两类密码体制

一．对称密钥密码体制

加密密钥和解密密钥是相同的密码体制

1．替代密码和置换密码:

替代密码：A，B，C，D，…用D，E，F，G，…来替代（顺序不变）：例如：HAPPY用KDSSB来表示，缺点：容易被破译

置换密码：按照某一规则重新排列消息中的比特或字符。

例如：

密钥	C	L	P	H	E	R
顺序	1	4	5	3	2	6
明文	A	T	T	A	C	K
	B	E	G	I	N	S
	A	T		T	W	O

密文： ABACNWAITTETTG KSO

缺点：容易破译

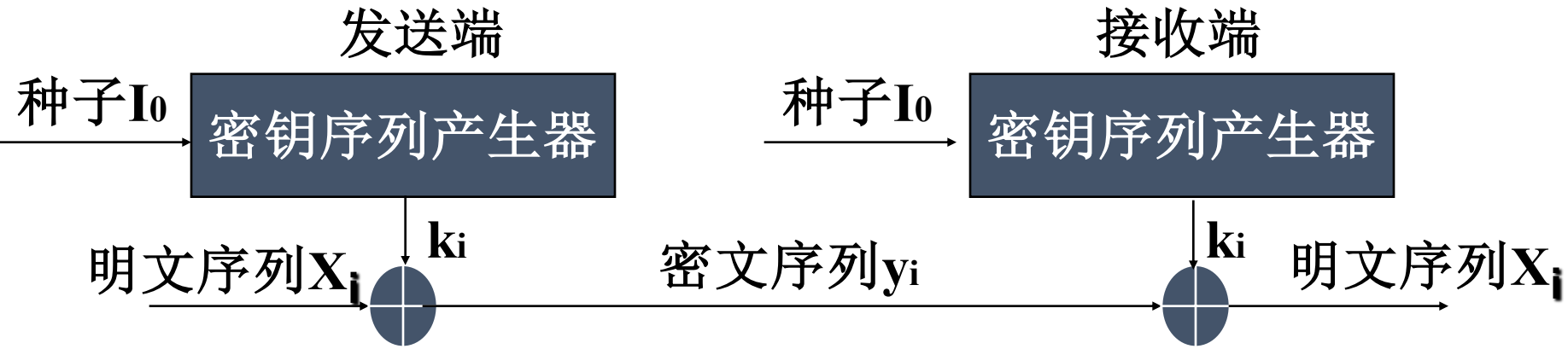
2．从得到的密文序列的结构来划分，密码分成两个不同的体制

（1） 序列密码原理

发送端：将明文X看成是连续的比特流：$X_1\ X_2\ \cdots$，且密钥序列$K=K_1\ K_2\ \cdots$中的第i个元素K_i对明文中的X_i进行加密：

$y_i=E_{ki}(x_i)=x_i \oplus k_i$

接收端解密算法为:$D_{ki}(y_i)=y_i \oplus k_i=(x_i \oplus k_i) \oplus k_i=x_i$



- 说明：如果密钥是真正的随机数，则在理论上是无法破译的，所以，实际上是用伪随机序列，该随机序列要足够的长，要有很好的随机性，周期可长达10^{50}

数据加密标准 DES

- 数据加密标准 DES 属于常规密钥密码体制，是一种分组密码。
- 在加密前，先对整个明文进行分组。每一个组长为 64 位。
- 然后对每一个 64 位 二进制数据进行加密处理，产生一组 64 位密文数据。
- 最后将各组密文串接起来，即得出整个的密文。
- 使用的密钥为 64 位（实际密钥长度为 56 位，有 8 位用于奇偶校验)。

DES 的保密性

- DES 的保密性仅取决于对密钥的保密，而算法是公开的。尽管人们在破译 DES 方面取得了许多进展，但至今仍未能找到比穷举搜索密钥更有效的方法。
- DES 是世界上第一个公认的实用密码算法标准，它曾对密码学的发展做出了重大贡献。
- 目前较为严重的问题是 DES 密钥的长度。
- 现在已经设计出来搜索 DES 密钥的专用芯片。

（2） 分组密码

A.原理：将明文划分成固定的**n**比特的数据组,以组为单位,在密钥的控制下进行一系列的线性或非线性的变化而得到的密文

B.特点**:**当给定一个密钥后，若明文分组相同,经变换得到的密文分组也相同

C.实例：美国的数据加密标准DES和国际数据加密算法IDEA，

三　公开密钥密码体制

3.1 概述

1．产生原因:

（1）由于常规密钥密码体制，加密和解密都使用相同的密钥，如何作到这一点，一是用信使来传送（不安全），二是事先约定（不好管理）

（2）对数字签名的强烈要求也是公开密钥密码体制产生的一个原因

- 公钥密码体制使用不同的加密密钥与解密密钥，是一种“由已知加密密钥推导出解密密钥在计算上是不可行的”密码体制。
- 现有最著名的公钥密码体制是RSA 体制，它基于数论中大数分解问题的体制，由美国三位科学家 Rivest, Shamir 和 Adleman 于 1976 年提出并在 1978 年正式发表的。

加密密钥与解密密钥

- 在公钥密码体制中，加密密钥(即公钥) *PK* 是公开信息，而解密密钥(即私钥或秘钥) *SK* 是需要保密的。
- 加密算法 *E* 和解密算法 *D* 也都是公开的。
- 虽然秘钥 *SK* 是由公钥 *PK* 决定的，但却不能根据 *PK* 计算出 *SK*。

应当注意

- 任何加密方法的安全性取决于密钥的长度，以及攻破密文所需的计算量。在这方面，公钥密码体制并不具有比传统加密体制更加优越之处。
- 由于目前公钥加密算法的开销较大，在可见的将来还看不出来要放弃传统的加密方法。公钥还需要密钥分配协议，具体的分配过程并不比采用传统加密方法时更简单。

2．特点：

(1)发送者用加密算法**E**和加密密钥**PK**对明文**X**加密后，接收者用解密算法**D**和解密密钥**SK**解密：$D_{SK}(E_{PK}(X))=X$，解密密钥为接收者专用（为保密的）；另：$E_{PK}(D_{SK}(X))=X$

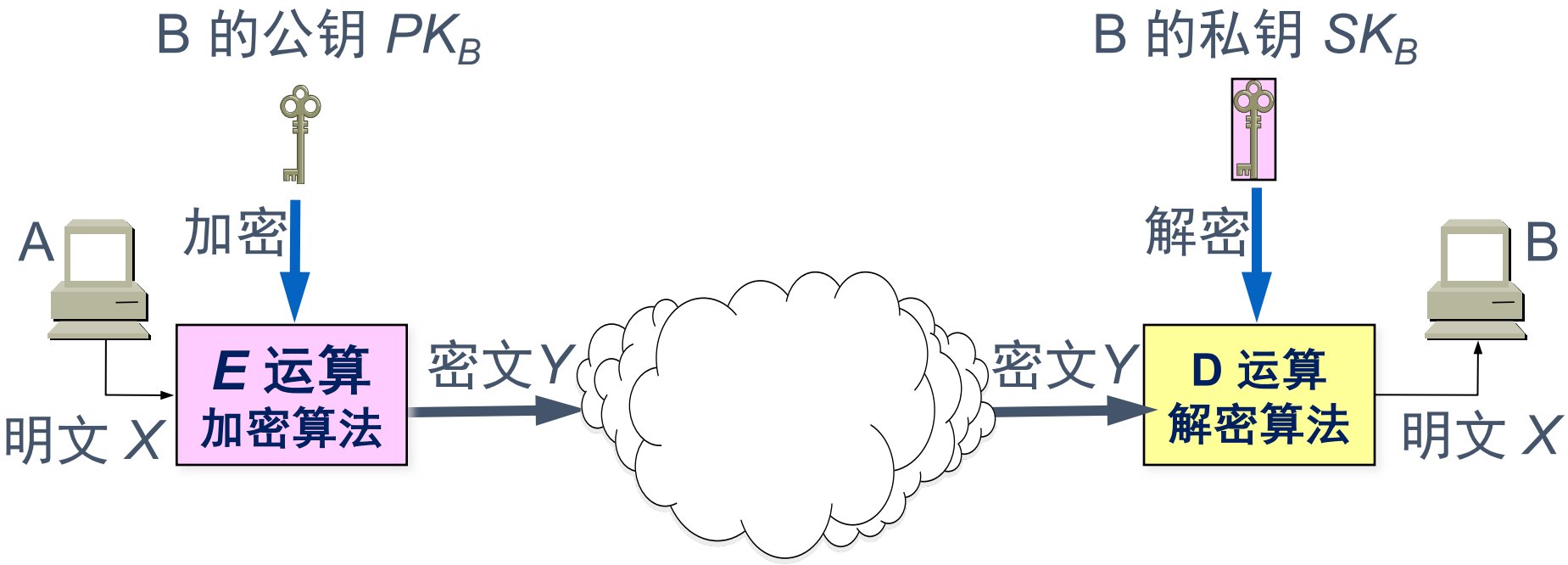
（2）加密密钥公开，但利用加密密钥不能解密

（3）在计算机上容易生成一对PK和SK

（4）从已知的PK不能推导出SK

（5）加密和解密算法公开

公钥密码体制



7　网络安全

书信或文件是根据亲笔签名来验证其真实性，但在计算机网络中传送的文电是如何实现身份验证?

通过数字签名

1．目的

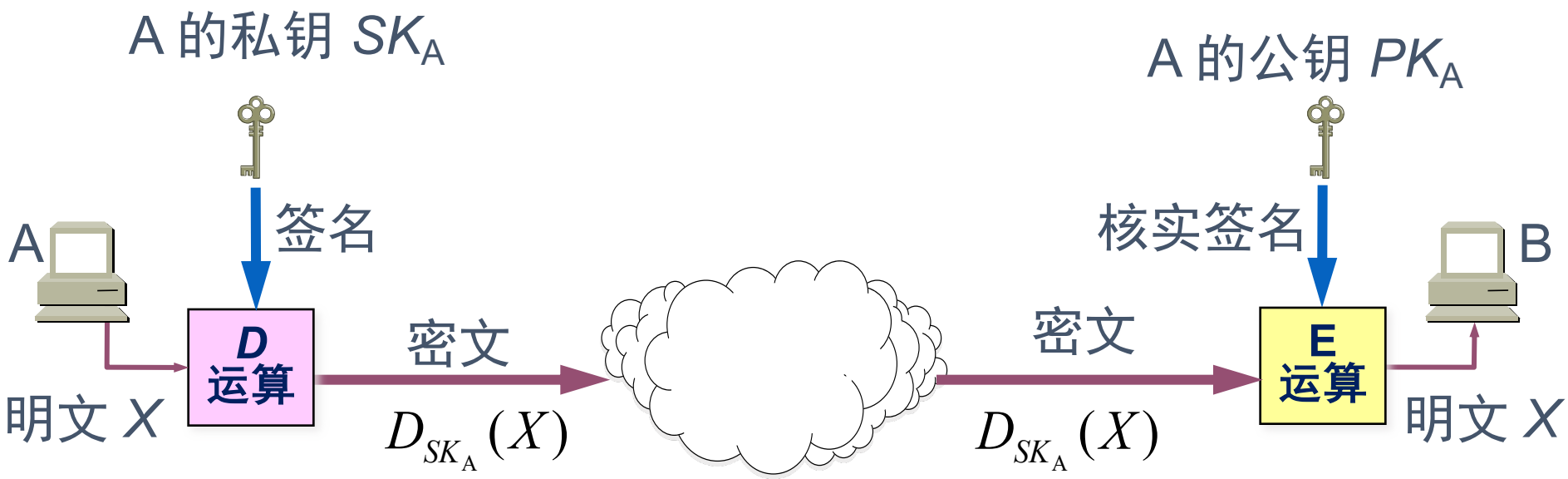
- （1）接收者能够核实发送者对报文的签名
- （2）发送者事后不能抵赖对报文的签名
- （3）接收者不能伪造对报文的签名

2．实现

发送者A用秘密解密密钥SK_A对报文X进行运算，将结果D_{SKA}（X）传送给接收者B（解密和加密仅仅是一种算法），B用已知A的公开加密密钥得出X

$$E_{PKA}（D_{SKA}（X））=X$$

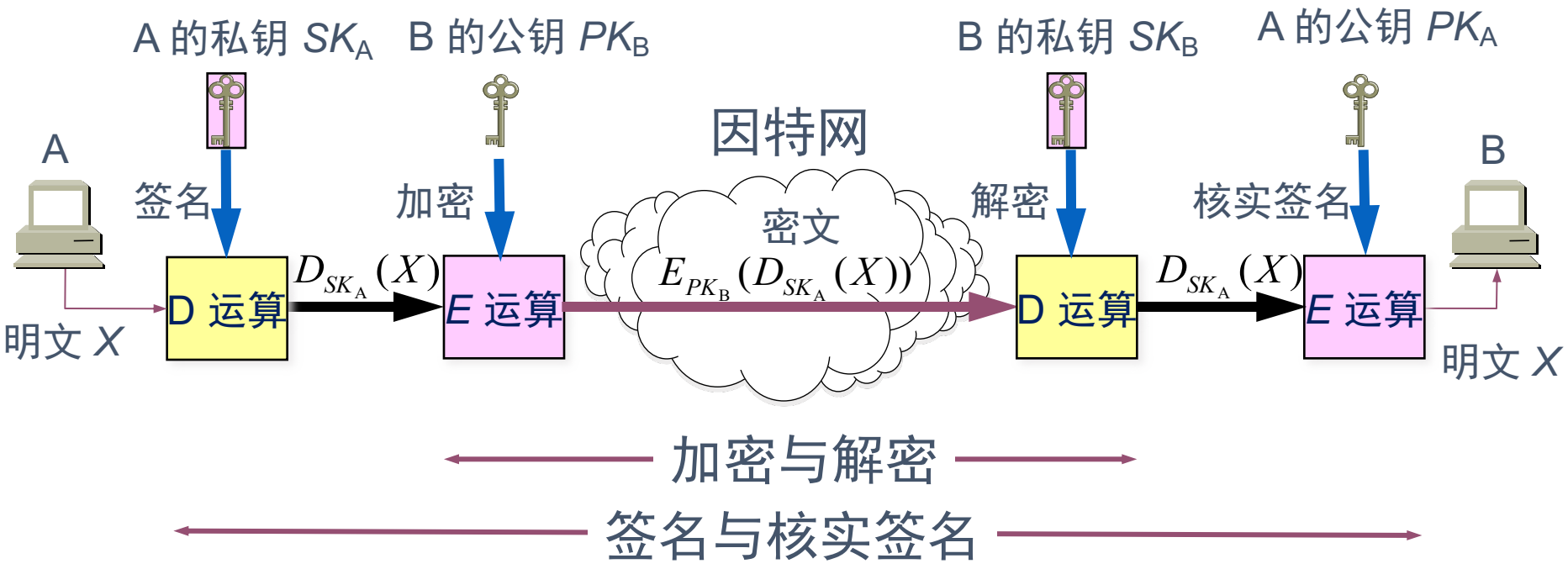
数字签名的实现



- 3.说明
- (1)实现数字签名:因为只有A才有解密密钥,所以，只有A才能做出密文
- (2)若发送者抵赖,B可以将X及D_{SKA}（X）出示给第三者,第三者可以用PK_A去验证A确实发送X给B

  (3)若B将X伪造成X',则B不能在第三者面前出示可以使用PKA还原出明文X的D_{SKA}（X'）,因为B没有SKA
- 下面介绍对付主动攻击采用的方法

具有保密性的数字签名


A 的私钥 SK_A
B 的公钥 PK_B
B 的私钥 SK_B
A 的公钥 PK_A
A
签名
加密
因特网
解密
核实签名
B
密文
$E_{PK_B}(D_{SK_A}(X))$
D 运算
$D_{SK_A}(X)$
E 运算
D 运算
$D_{SK_A}(X)$
E 运算
明文 X
明文 X
加密与解密
签名与核实签名

7　网络安全

7.4　　报文鉴别

一．定义：使通信的接收方能够验证所收到的报文的真伪

二．进行报文鉴别常用的方法是

使用报文摘要

报文摘要

1．原理:

S1: 发送方将可变长度报文m经过报文摘要算法运算后得出固定长度的报文摘要H(m);

S2: 对H(m) 进行加密得出E_K(H(m) ;

S3: 将报文m + E_K(H(m) 一起发送;

S4: 接收方将 E_K(H(m)解密还原为 H(m)；

S5: 将收到的报文m进行报文摘要运算,判断结果为H(m)?

是: 收到的报文正确

否: 报文被篡改

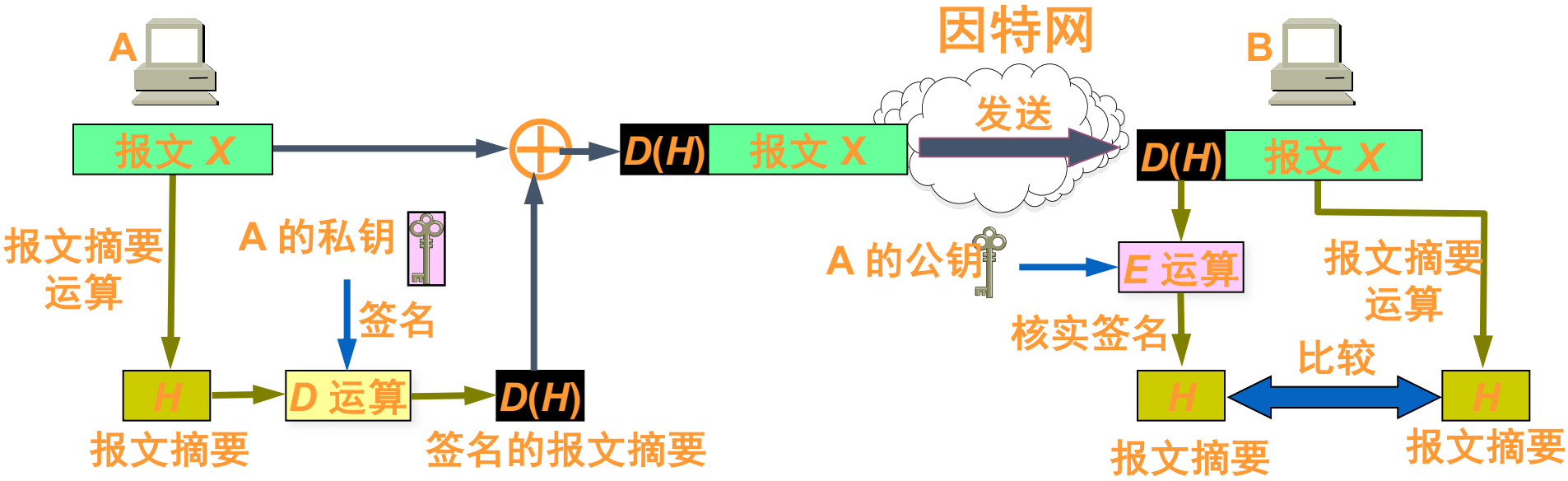
优点:仅对H(m)加密实现简单

报文摘要

2. 满足的条件:
(1)任给一个报文摘要值x,想找一个报文y使得H(y)=x,在计算上不可行（根据报文摘要推导不出报文）

(2)若想找到任意两个报文x和y,使得H(x)= H(y),在计算上不可行（没有两个具有同样摘要的报文）
这两个条件使得攻击者不能伪造出另一个报文y,使得y具有同样的报文摘要x

报文摘要的实现

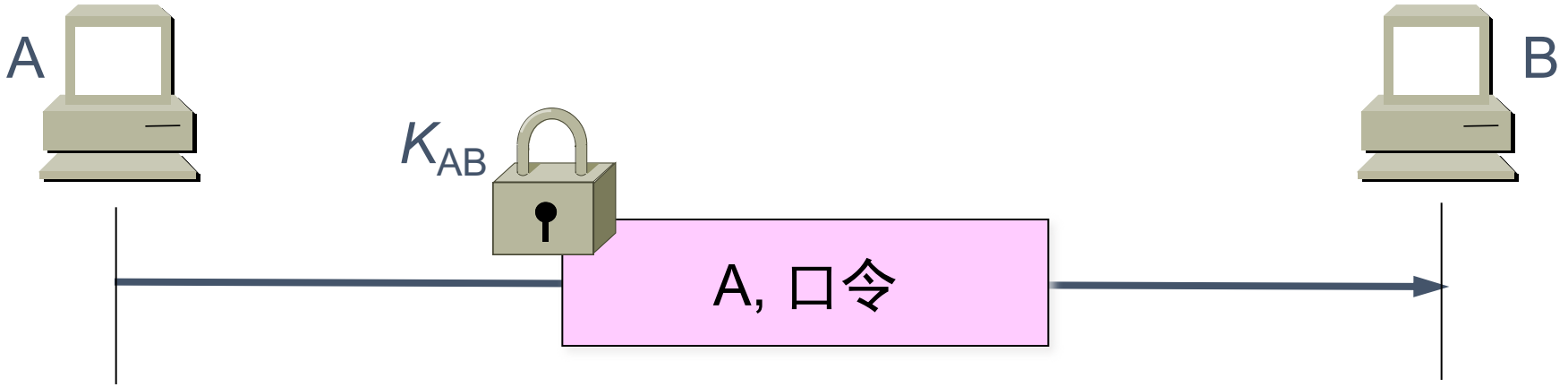

A
报文 X
报文摘要
运算
A 的私钥
签名
H
D 运算
D(H)
报文摘要
签名的报文摘要
因特网
发送
D(H)
报文 X
A 的公钥
E 运算
核实签名
H
报文摘要
B
D(H)
报文 X
报文摘要
运算
比较
H
报文摘要

实体鉴别

- 实体鉴别和报文鉴别不同。
- 报文鉴别是对每一个收到的报文都要鉴别报文的发送者，而实体鉴别是在系统接入的全部持续时间内对和自己通信的对方实体只需验证一次。

最简单的实体鉴别过程

- A 发送给 B 的报文被加密，使用的是对称密钥 K_{AB}。
- B 收到此报文后，用共享对称密钥 K_{AB} 进行解密，因而鉴别了实体 A 的身份。



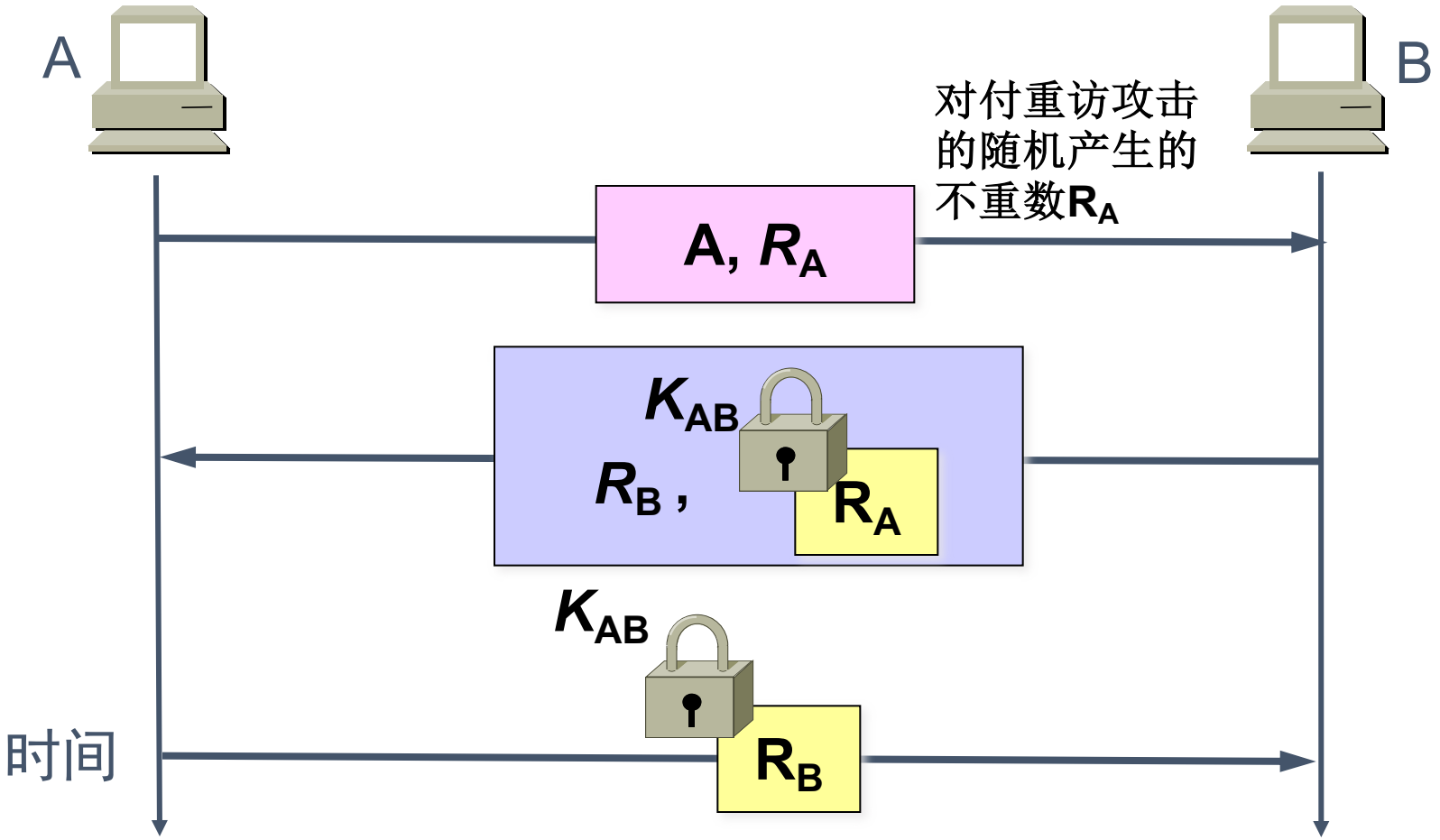
明显的漏洞

- 入侵者 C 可以从网络上截获 A 发给 B 的报文。C 并不需要破译这个报文（因为这可能花很多时间）而可以直接把这个由 A 加密的报文发送给 B，使 B 误认为 C 就是 A。然后 B 就向伪装是 A 的 C 发送应发给 A 的报文。
- 这就叫做重放攻击(replay attack)。C 甚至还可以截获 A 的 IP 地址，然后把 A 的 IP 地址冒充为自己的 IP 地址（这叫做 IP 欺骗），使 B 更加容易受骗。
- 发送方身份鉴别

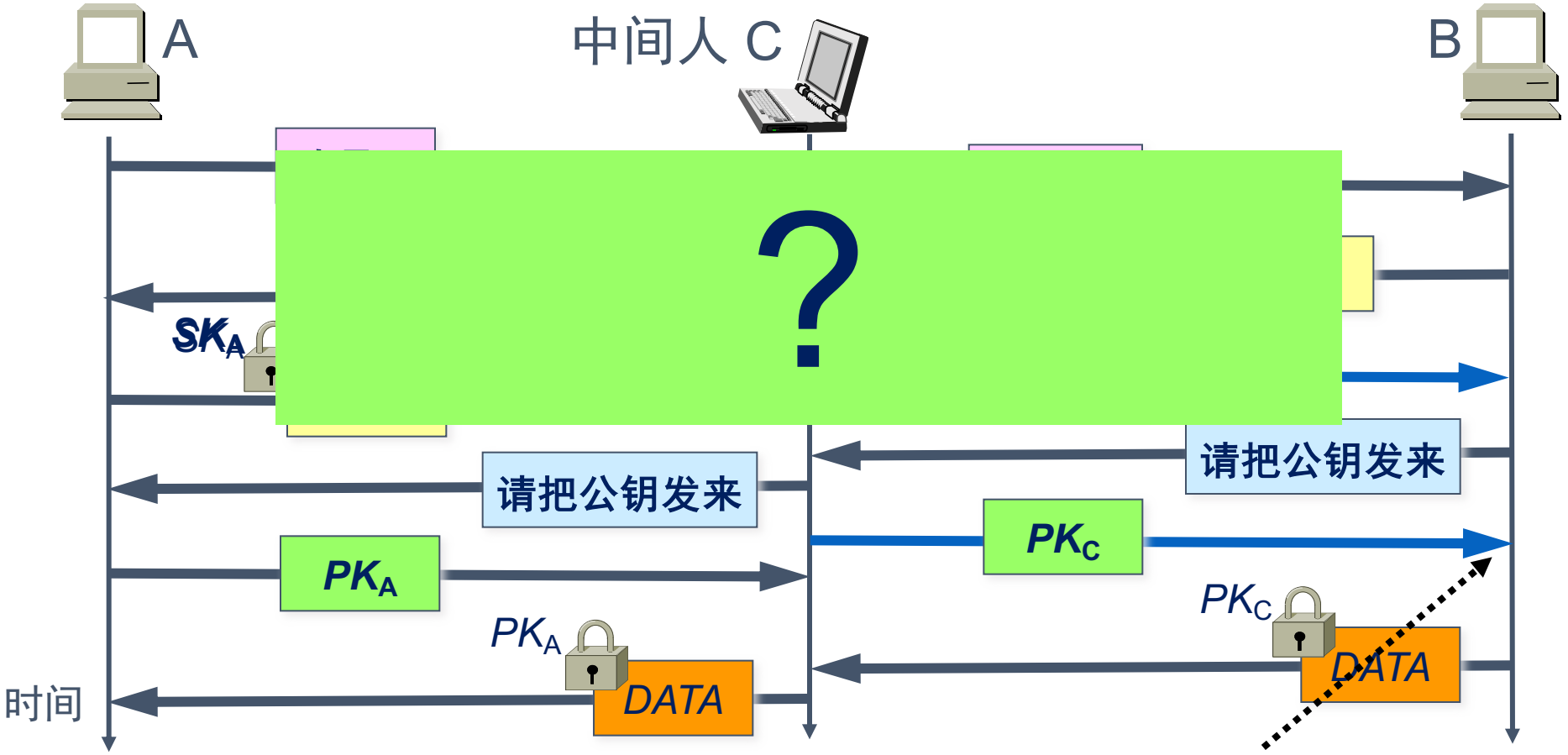
使用不重数

- 为了对付重放攻击，可以使用不重数(nonce)。不重数就是一个不重复使用的大随机数，即“一次一数”。

使用不重数进行鉴别



中间人攻击



SK_C：C的私钥; SK_A：A的私钥

PK_A：A的公钥; PK_C：C的公钥

B收到C的公钥后，使用公钥对$SK_C(R_B)$进行解密,数据准确，认为C就是A

中间人攻击说明

- B开始和C进行通信
- B使用C的公钥加密发给C，C 收到后用自己的私钥 SK_C 解密，复制一份留下，再用 A 的公钥 PK_A 对数据加密后发送给 A
- A 收到数据后，用自己的私钥 SK_A 解密，以为和B进行了保密通信。其实，B发送给A的加密数据已被中间人 C 截获并解密了一份。但 A 和 B 却都不知道。

第五节　　密钥分配

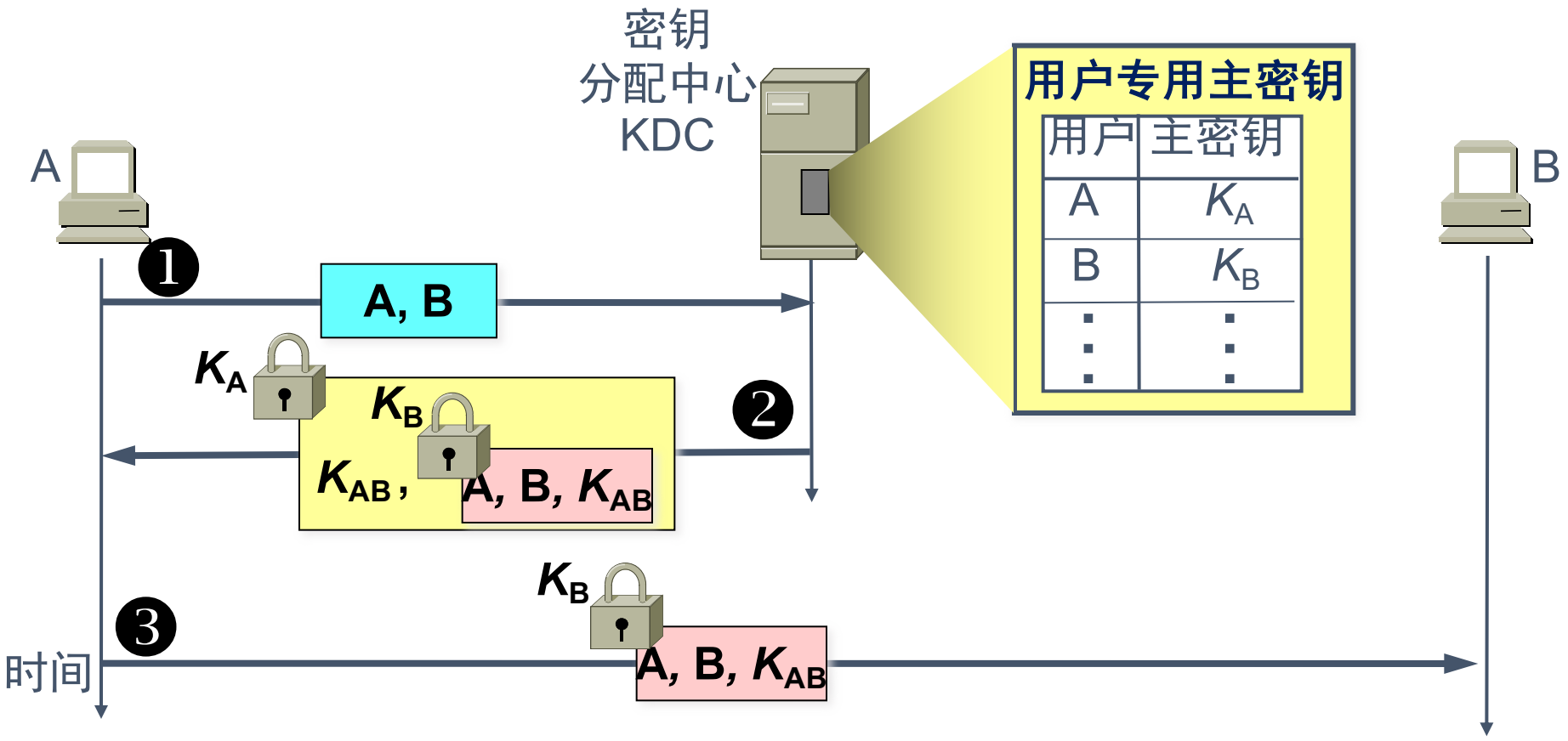
由于密码算法是公开的，所以，网络的安全性就在于密钥的安全保护，这就是密钥管理

一．密钥管理：密钥的产生、分配、注入、验证和使用

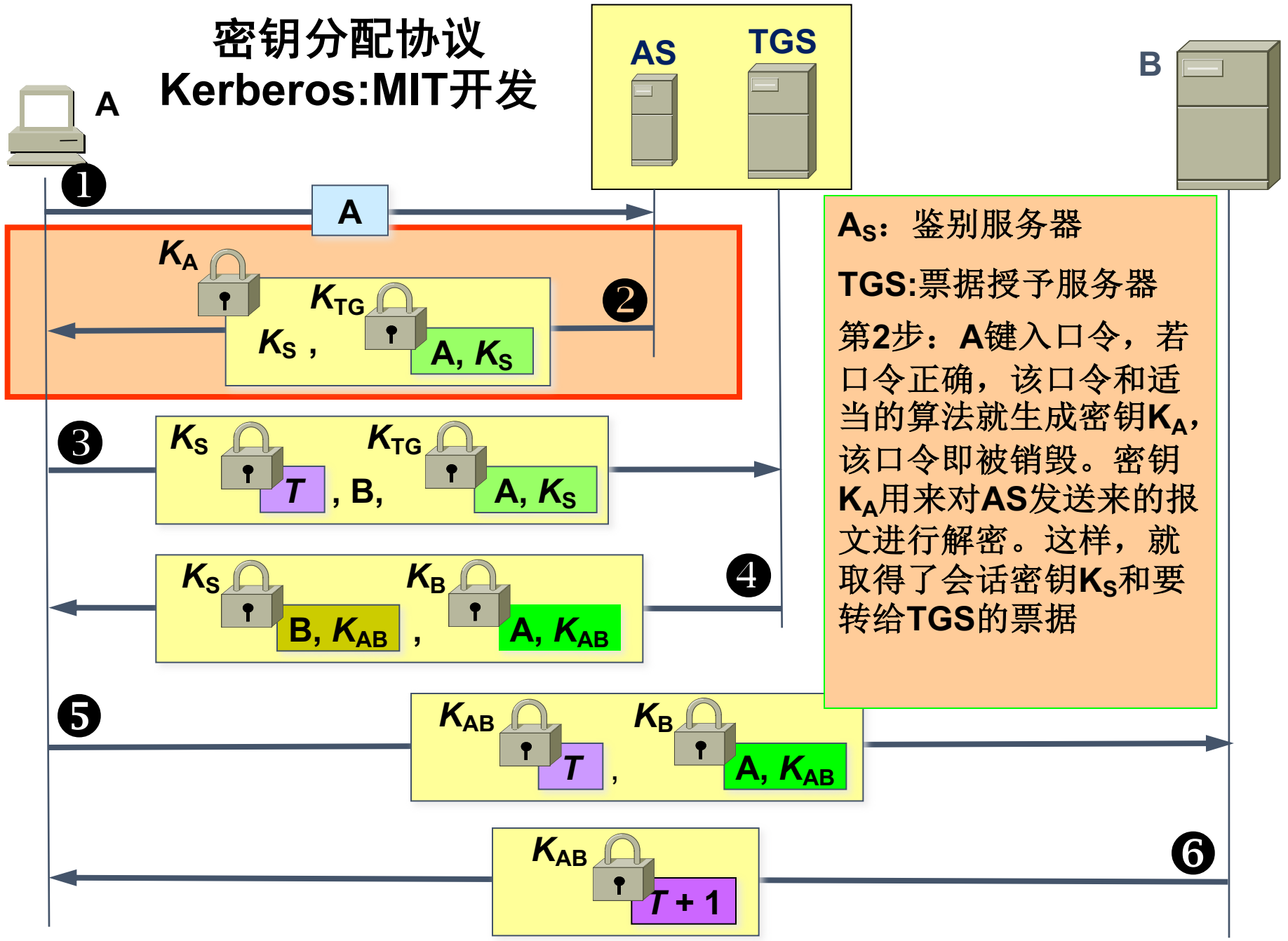
7.5.1 对称密钥的分配

- 目前常用的密钥分配方式是设立密钥分配中心 KDC (Key Distribution Center)。
- KDC 是大家都信任的机构，其任务就是给需要进行秘密通信的用户临时分配一个会话密钥（仅使用一次）。
- 用户 A 和 B 都是 KDC 的登记用户，并已经在 KDC 的服务器上安装了各自和 KDC 进行通信的主密钥（master key）K_A 和 K_B。“主密钥”可简称为“密钥”。

对称密钥的分配


密钥
分配中心
KDC
用户专用主密钥
用户
主密钥
A
K_A
B
K_B
A
B
1
A, B
K_A
K_B
K_{AB},
A, B, K_{AB}
2
K_B
A, B, K_{AB}
3
时间

密钥分配协议
Kerberos:MIT开发

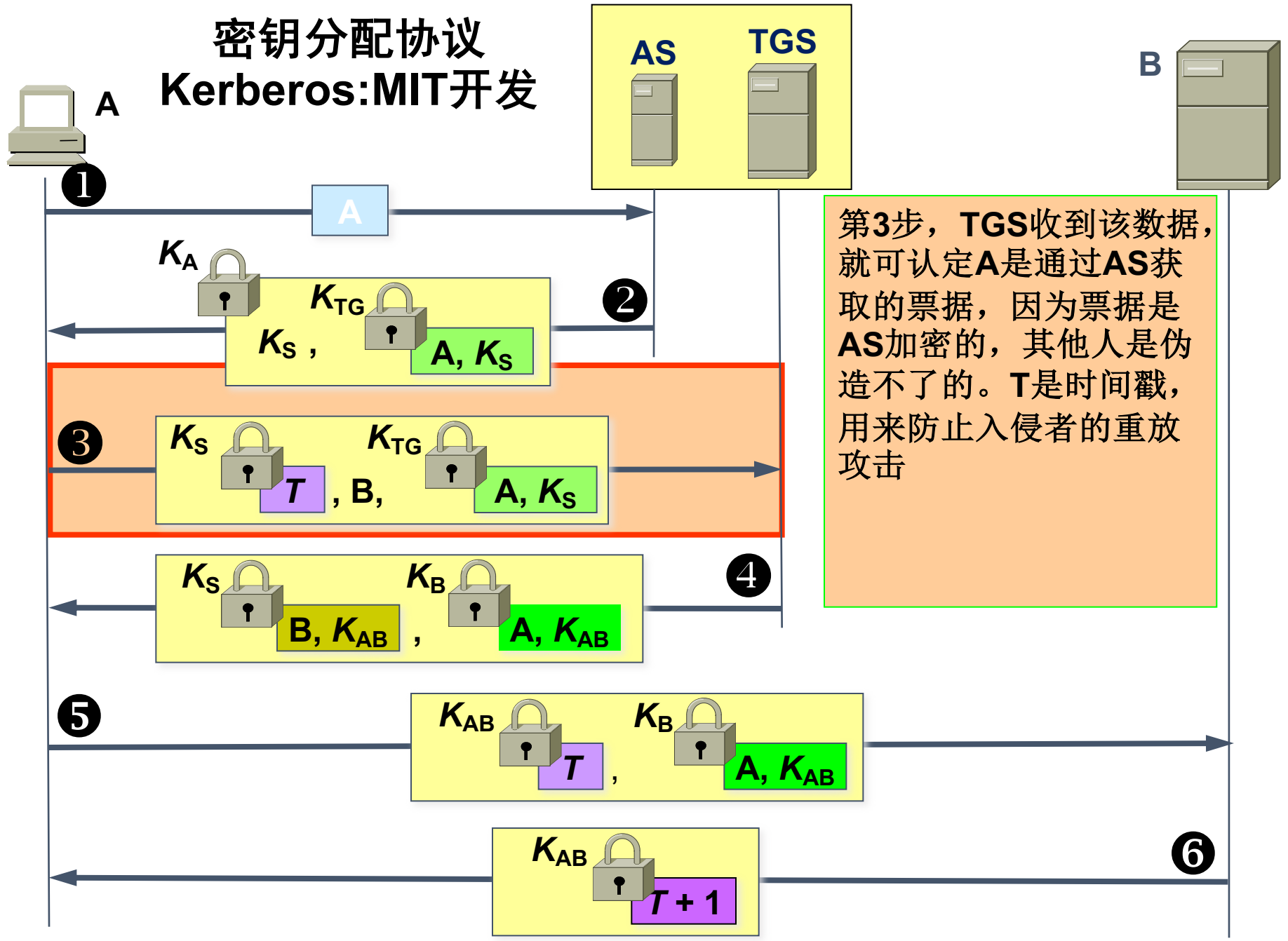


A_S：鉴别服务器

TGS:票据授予服务器

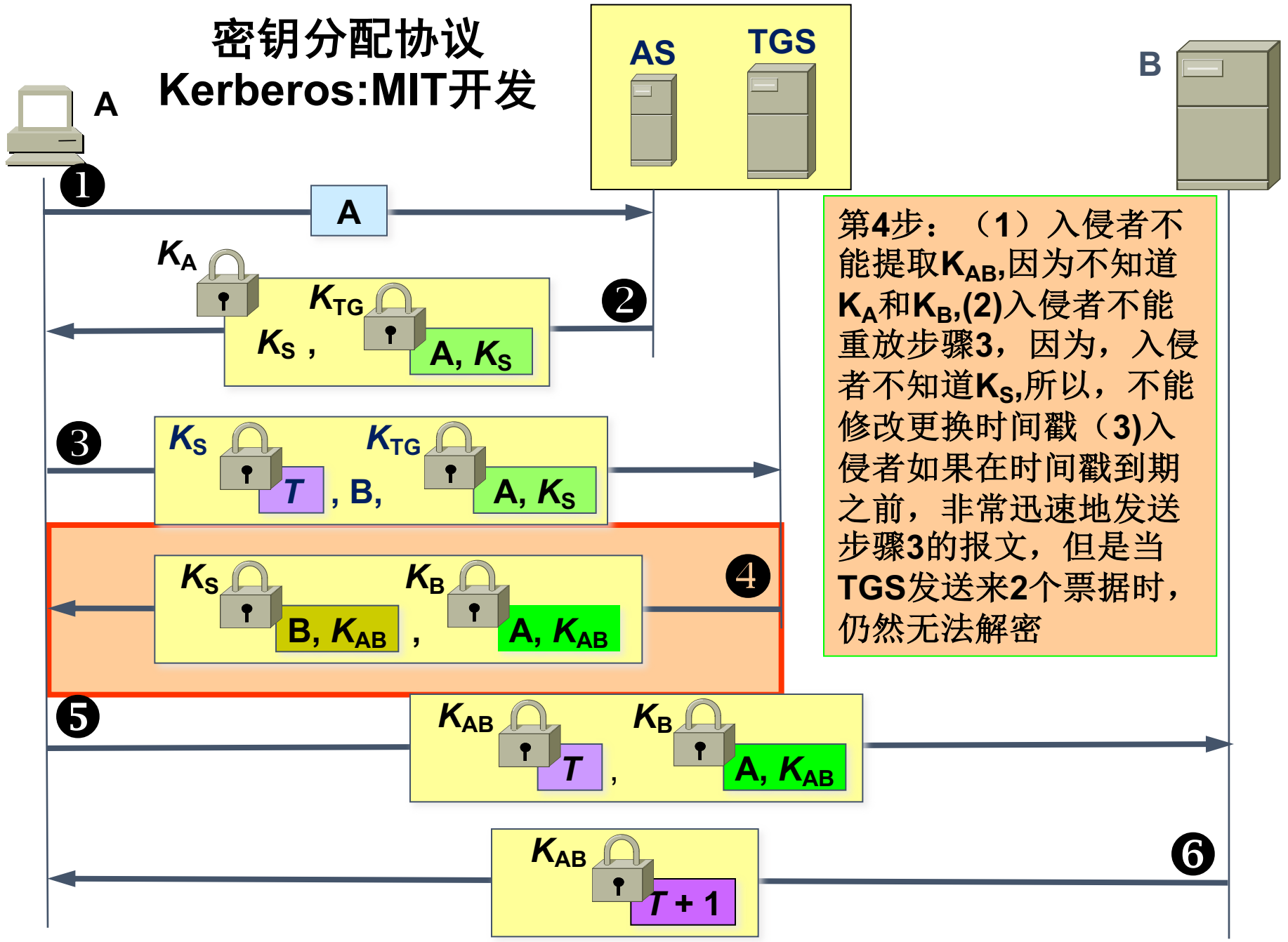
第2步：A键入口令，若口令正确，该口令和适当的算法就生成密钥K_A，该口令即被销毁。密钥K_A用来对AS发送来的报文进行解密。这样，就取得了会话密钥K_S和要转给TGS的票据

密钥分配协议
Kerberos:MIT开发



第3步，TGS收到该数据，就可认定A是通过AS获取的票据，因为票据是AS加密的，其他人是伪造不了的。T是时间戳，用来防止入侵者的重放攻击

密钥分配协议
Kerberos:MIT开发



第4步：（1）入侵者不能提取K_{AB},因为不知道K_A和K_B,(2)入侵者不能重放步骤3，因为，入侵者不知道K_S,所以，不能修改更换时间戳（3)入侵者如果在时间戳到期之前，非常迅速地发送步骤3的报文，但是当TGS发送来2个票据时，仍然无法解密

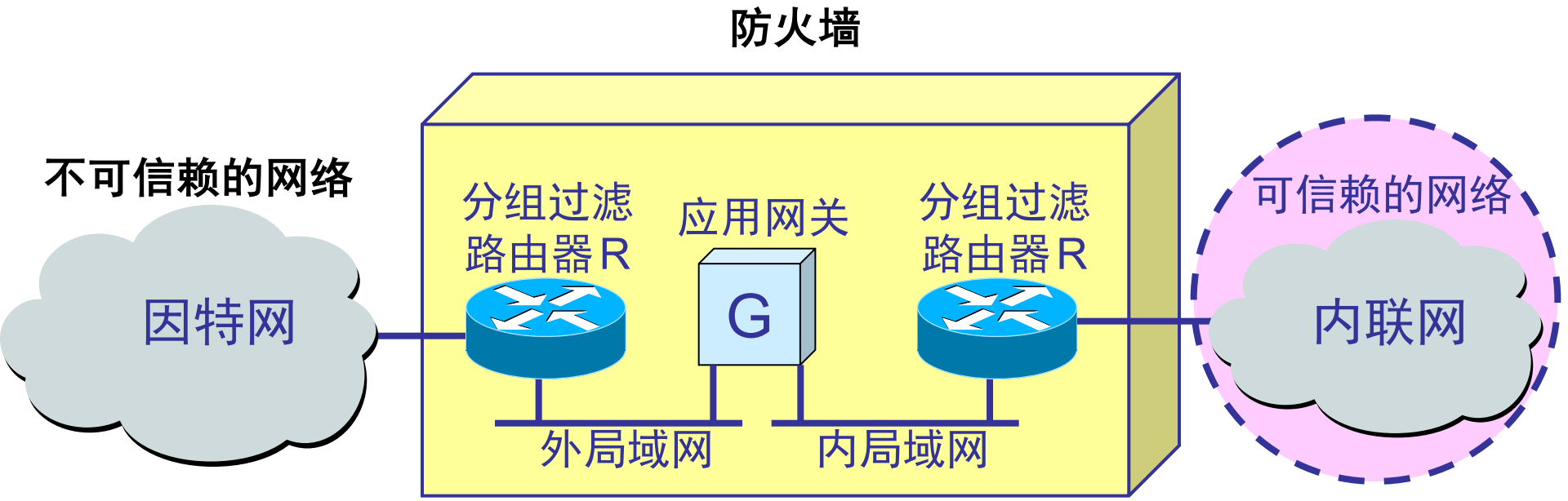
7.5.2 公钥的分配

- 需要有一个值得信赖的机构——即认证中心CA (Certification Authority)，来将公钥与其对应的实体（人或机器）进行绑定(binding)。
- 认证中心一般由政府出资建立。每个实体都有 CA 发来的证书(certificate)，里面有公钥及其拥有者的标识信息。此证书被 CA 进行了数字签名。任何用户都可从可信的地方获得认证中心 CA 的公钥，此公钥用来验证某个公钥是否为某个实体所拥有。有的大公司也提供认证中心服务。

7.8 防火墙(firewall)

- 防火墙是由软件、硬件构成的系统，是一种特殊编程的路由器，用来在两个网络之间实施接入控制策略。接入控制策略是由使用防火墙的单位自行制订的，为的是可以最适合本单位的需要。
- 防火墙内的网络称为“可信赖的网络”(trusted network)，而将外部的因特网称为“不可信赖的网络”(untrusted network)。
- 防火墙可用来解决内联网和外联网的安全问题。

防火墙在互连网络中的位置



防火墙的功能

- 防火墙的功能有两个：阻止和允许。
- “阻止”就是阻止某种类型的通信量通过防火墙（从外部网络到内部网络，或反过来）。
- “允许”的功能与“阻止”恰好相反。
- 防火墙必须能够识别通信量的各种类型。不过在大多数情况下防火墙的主要功能是“阻止”。

防火墙技术一般分为两类

(1) 网络级防火墙——用来防止整个网络出现外来非法的入侵。属于这类的有分组过滤和授权服务器。前者检查所有流入本网络的信息，然后拒绝不符合事先制订好的一套准则的数据，而后者则是检查用户的登录是否合法。

(2) 应用级防火墙——从应用程序来进行接入控制。通常使用应用网关或代理服务器来区分各种应用。例如，可以只允许通过访问万维网的应用，而阻止 FTP 应用的通过。

- 计算机安全的概念

1、定义：对于一个自动化的信息系统，采取保护措施确保信息系统资源（软件硬件信息数据和通信）的CIA

- 保密性Confidentiality（数据保密性-确保隐私信息不向非授权者泄露和使用；隐私性-确保个人能够控制和确定与其自身相关的哪些信息可被收集保存，这些信息可由谁来向谁公开）
- 完整性Integrity（数据完整性-确保信息程序只能以特定和授权的方式执行；确保系统以一种正常的方式来执行预定的功能而不被非法操控）
- 可用性Availability（确保系统工作迅速，对于授权用户不能拒绝服务）

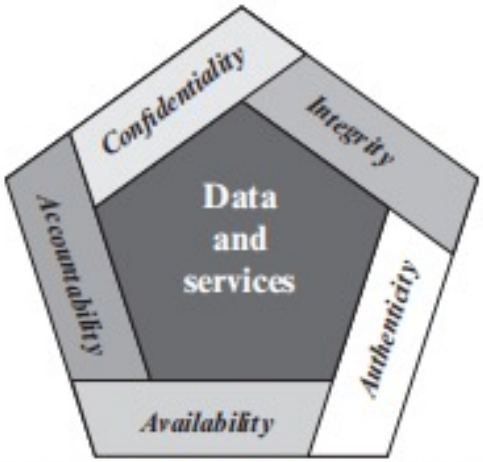


Figure 1.1 Essential Network and Computer Security Requirements

- 网络安全模型
  - 利用TCP/IP通信协议建立一条逻辑信道
  - 安全技术：安全交换所发送的信息（加密消息使信息不可非法访问，附加基于消息内容的编码用来验证发送者身份）；被两个主体共享且不被攻击者知道的一些机密信息（发送前加密消息收到消息后利用解密密钥解密）
  - 设计安全服务包含：

    1、设计算法：执行与安全相关的变换，攻击者无法攻破

    2、产生算法所使用的秘钥等信息

    3、设计分配和共享秘密信息的方法

    4、商议通信双方使用的用于实现安全算法和解密等安全服务的协议

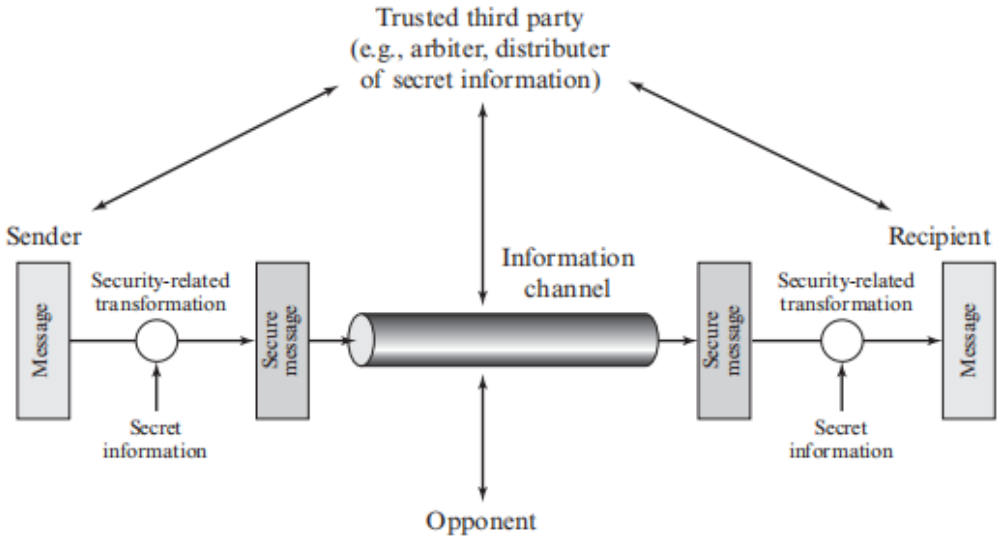
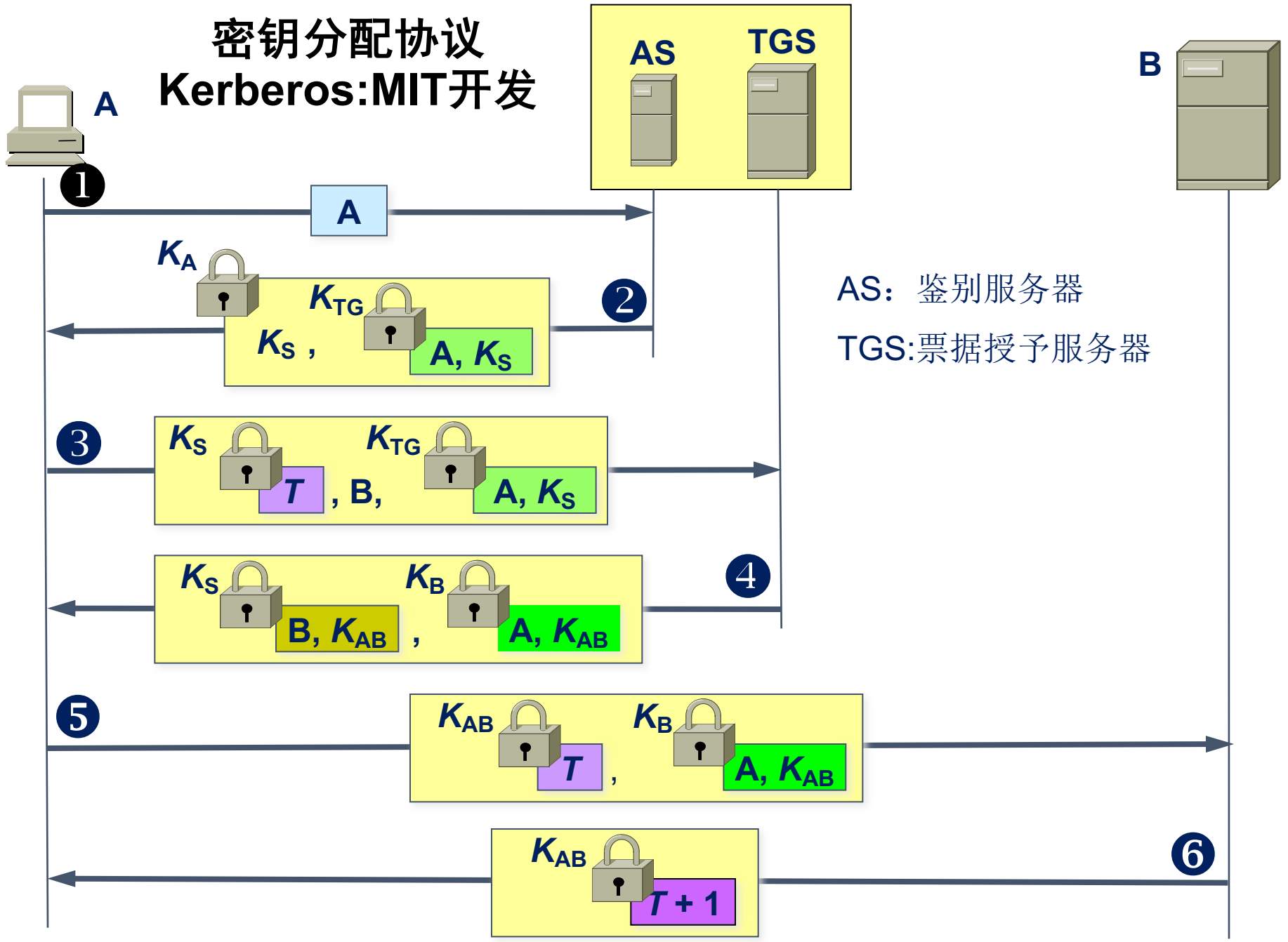


Figure 1.5 Model for Network Security

- END

密钥分配协议
Kerberos:MIT开发



AS：鉴别服务器

TGS:票据授予服务器