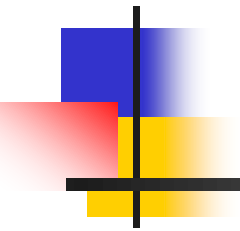


计算机网络（第 6 版）

第 7 章 网络安全

课件制作人：谢希仁

第 7 章 网络安全

课件制作人：谢希仁

第 7 章 网络安全（续）

7.3 数字签名

7.4 鉴别

7.4.1 报文鉴别

7.4.2 实体鉴别

7.5 密钥分配

7.5.1 对称密钥的分配

7.5,2 公钥的分配

课件制作人：谢希仁

第 7 章 网络安全（续）

7.6 因特网使用的安全协议

7.6.1 网络层安全协议

7.6.2 运输层安全协议

7.6.3 应用层的安全协议破

7.7 系统安全：防火墙与入侵检测

7.7.1 防火墙

7.7.2 入侵检测系统

课件制作人：谢希仁

7.1 网络安全问题概述

7.1.1 计算机网络面临的安全性威胁

计算机网络上的通信面临以下两大类威胁：

一、被动攻击。主要是截获，即从网络上窃听他人的通信内容。

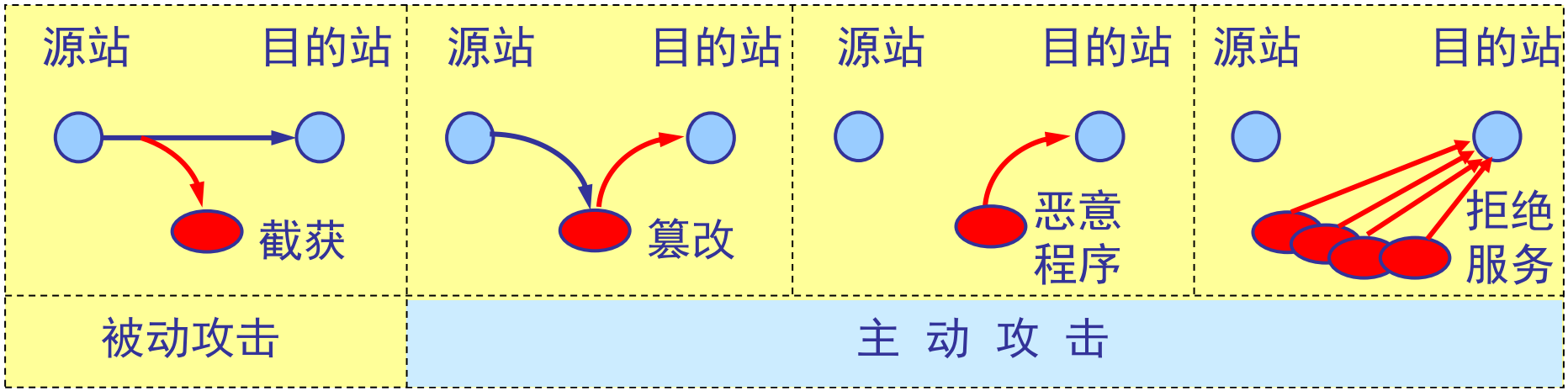
二、主动攻击，主要有：

(1) 篡改——故意篡改网络上传送的报文。

(2) 恶意程序—— 包括计算机病毒、计算机蠕虫、特洛伊木马和逻辑炸弹等。

(3) 拒绝服务——包括分布式拒绝服务。

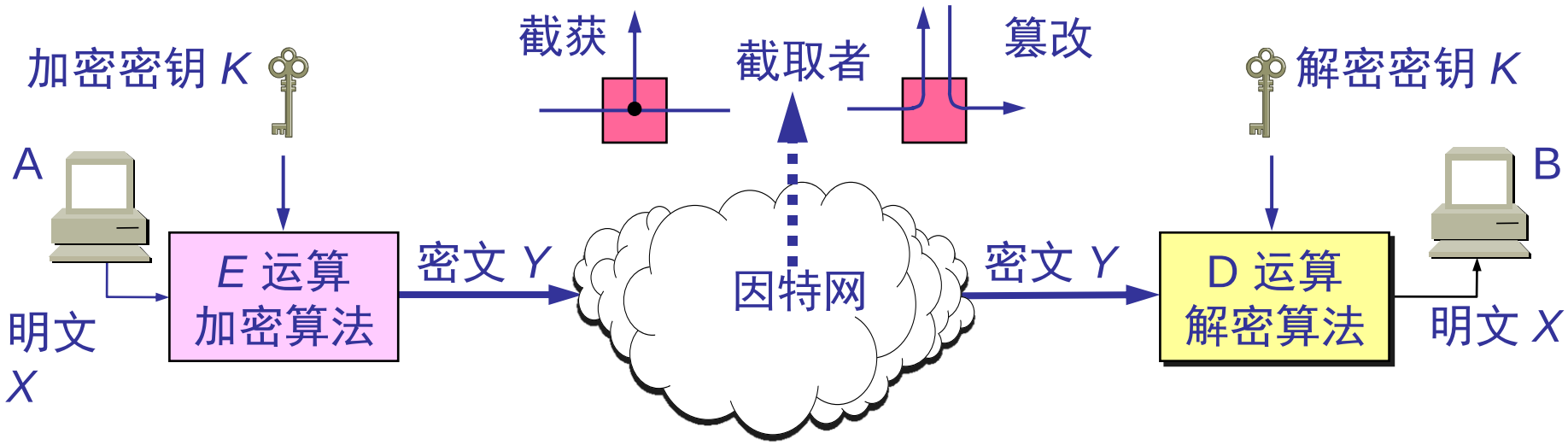
对网络的被动攻击和主动攻击



7.1.2 计算机网络安全的内容

- 保密性
- 安全协议的设计
- 访问控制

7.1.3 一般的数据加密模型



课件制作人：谢希仁

一些重要概念

- 密码编码学(cryptography)是密码体制的设计学，而密码分析学(cryptanalysis)则是在未知密钥的情况下从密文推演出明文或密钥的技术。密码编码学与密码分析学合起来即为密码学(cryptology)。
- 如果不论截取者获得了多少密文，但在密文中都没有足够的信息来唯一地确定出对应的明文，则这一密码体制称为无条件安全的，或称为理论上是不可破的。
- 如果密码体制中的密码不能被可使用的计算资源破译，则这一密码体制称为在计算上是安全的。

7.2 两类密码体制

7.2.1 对称密钥密码体制

- 所谓常规密钥密码体制，即加密密钥与解密密钥是相同的密码体制。
- 这种加密系统又称为对称密钥系统。

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 的密钥的长度。
- 现在已经设计出来搜索 DES 密钥的专用芯片。

7.2.2 公钥密码体制

- 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。
- 公钥密码体制的产生主要是因为两个方面的原因，一是由于常规密钥密码体制的密钥分配问题，另一是由于对数字签名的需求。
- 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。

公钥算法的特点

- 发送者 A 用 B 的公钥 PK_B 对明文 X 加密（E 运算）后，在接收者 B 用自己的私钥 SK_B 解密（D 运算），即可恢复出明文：

$$D_{SK_B}(Y) = D_{SK_B}(E_{PK_B}(X)) = X \qquad (7\text{-}4)$$

- 解密密钥是接收者专用的秘钥，对其他人都保密。
- 加密密钥是公开的，但不能用它来解密，即

$$D_{PK_B}(E_{PK_B}(X)) \neq X \qquad (7\text{-}5)$$

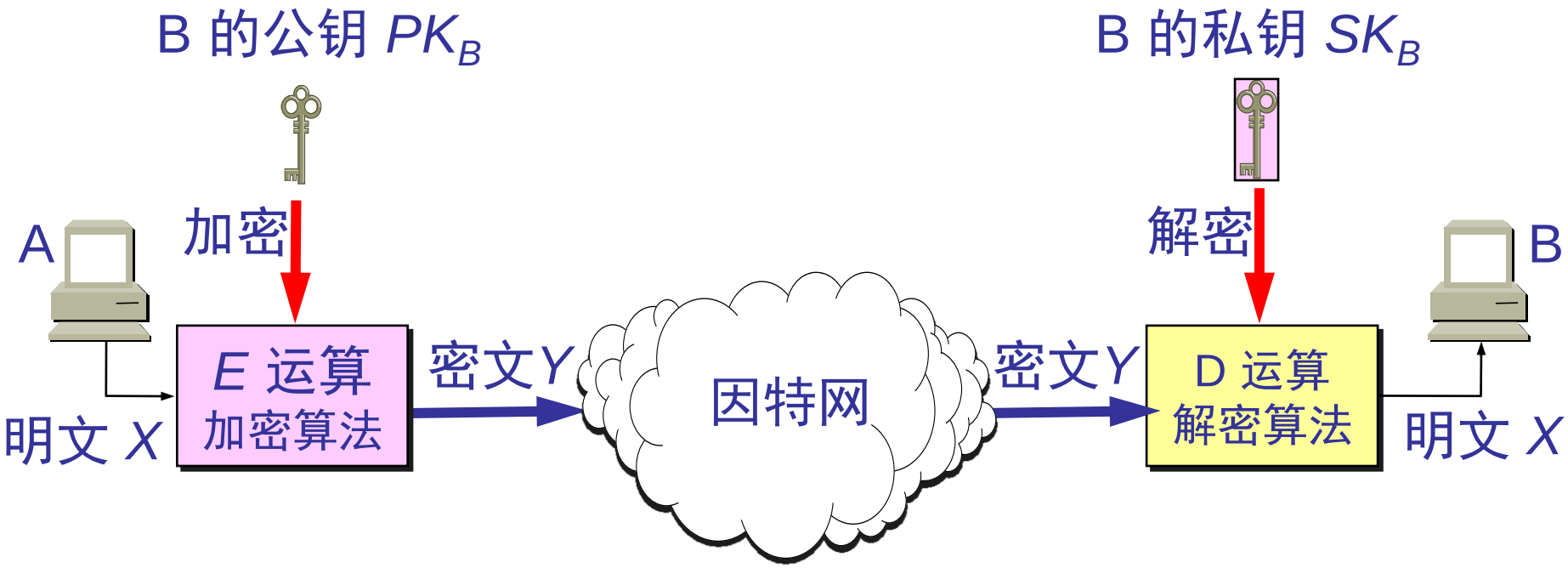
公钥算法的特点（续）

- 加密和解密的运算可以对调，即

$$E_{PK_B}(D_{SK_B}(X)) = D_{SK_B}(E_{PK_B}(X)) = X \quad （7\text{-}6）$$

- 在计算机上可容易地产生成对的 *PK* 和 *SK*。
- 从已知的 *PK* 实际上不可能推导出 *SK*，即从 *PK* 到 *SK* 是“计算上不可能的”。
- 加密和解密算法都是公开的。

公钥密码体制



7.3 数字签名

- 数字签名必须保证以下三点：

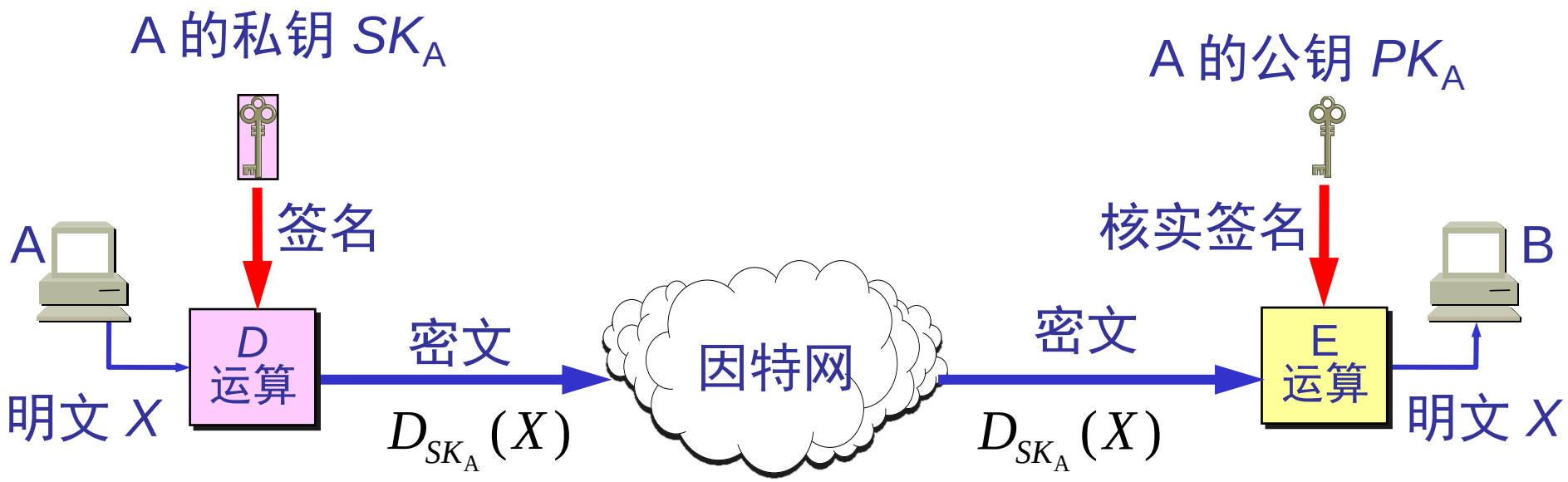
(1) 报文鉴别——接收者能够核实发送者对报文的签名；

(2) 报文的完整性——发送者事后不能抵赖对报文的签名；

(3) 不可否认——接收者不能伪造对报文的签名。

- 现在已有多种实现各种数字签名的方法。但采用公钥算法更容易实现。

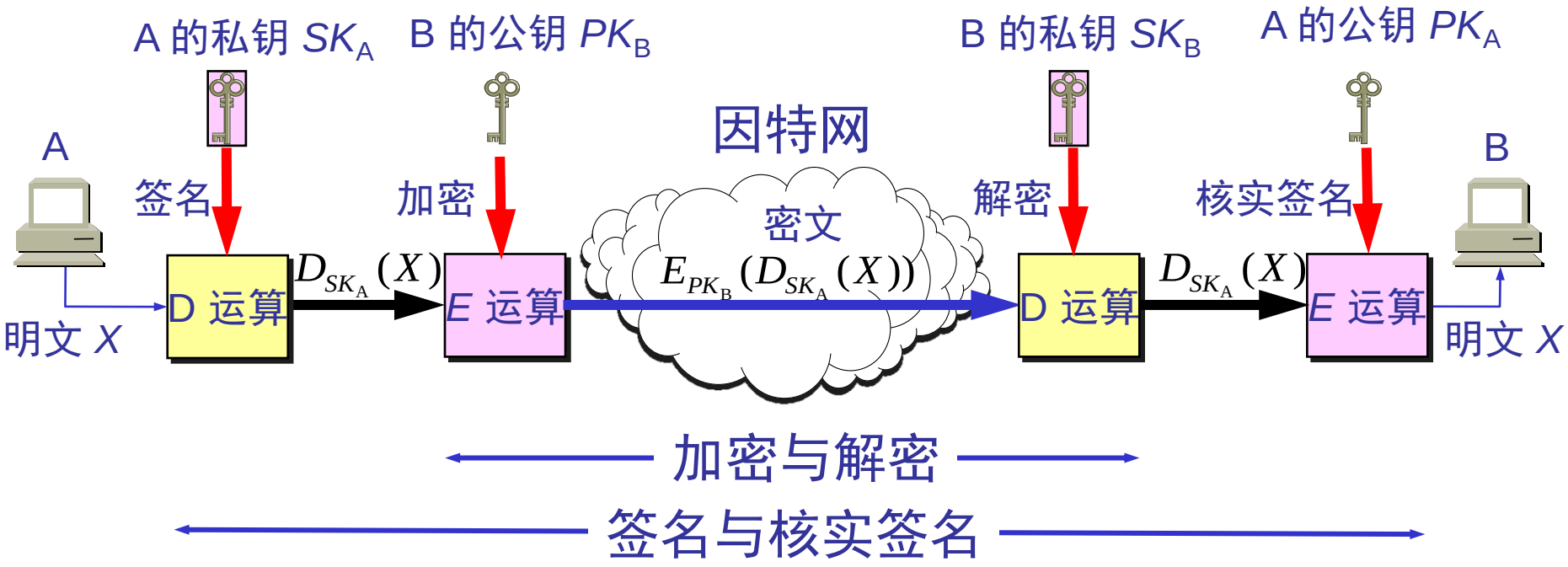
数字签名的实现


A 的私钥 SK_A
A 的公钥 PK_A
签名
核实签名
A
B
D
运算
E
运算
密文
密文
因特网
明文 X
明文 X
$D_{SK_A}(X)$
$D_{SK_A}(X)$

数字签名的实现

- 因为除 A 外没有别人能具有 A 的私钥，所以除 A 外没有别人能产生这个密文。因此 B 相信报文 *X* 是 A 签名发送的。
- 若 A 要抵赖曾发送报文给 B，B 可将明文和对应的密文出示给第三者。第三者很容易用 A 的公钥去证实 A 确实发送 *X* 给 B。
- 反之，若 B 将 *X* 伪造成 *X*‘，则 B 不能在第三者前出示对应的密文。这样就证明了 B 伪造了报文。

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
D 运算
$D_{SK_A}(X)$
E 运算
密文
$E_{PK_B}(D_{SK_A}(X))$
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

7.4 鉴别

- 在信息的安全领域中，对付被动攻击的重要措施是加密，而对付主动攻击中的篡改和伪造则要用鉴别(authentication) 。
- 报文鉴别使得通信的接收方能够验证所收到的报文（发送者和报文内容、发送时间、序列等）的真伪。
- 使用加密就可达到报文鉴别的目的。但在网络的应用中，许多报文并不需要加密。应当使接收者能用很简单的方法鉴别报文的真伪。

鉴别与授权不同

- 鉴别与授权(authorization)是不同的概念。
- 授权涉及到的问题是：所进行的过程是否被允许（如是否可以对某文件进行读或写）。

7.4.1 报文鉴别

- 许多报文并不需要加密但却需要数字签名，以便让报文的接收者能够鉴别报文的真伪。
- 然而对很长的报文进行数字签名会使计算机增加很大的负担（需要进行很长时间的运算。
- 当我们传送不需要加密的报文时，应当使接收者能用很简单的方法鉴别报文的真伪。

报文摘要 MD (Message Digest)

- A 将报文 *X* 经过报文摘要算法运算后得出很短的报文摘要 *H*。然后然后用自己的私钥对 *H* 进行 *D* 运算，即进行数字签名。得出已签名的报文摘要 *D*(*H*)后，并将其追加在报文 *X* 后面发送给 B。
- B 收到报文后首先把已签名的 *D*(*H*) 和报文 *X* 分离。然后再做两件事。
  - 用A的公钥对 *D*(*H*) 进行*E*运算，得出报文摘要 *H* 。
  - 对报文 *X* 进行报文摘要运算，看是否能够得出同样的报文摘要 *H*。如一样，就能以极高的概率断定收到的报文是 A 产生的。否则就不是。

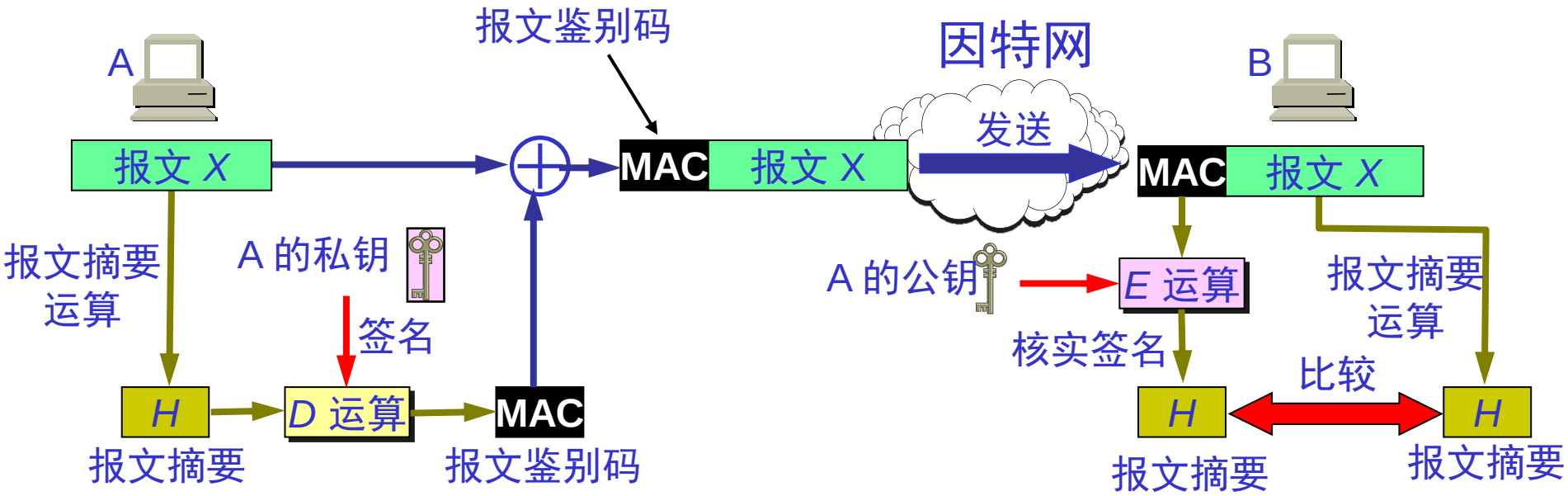
报文摘要的优点

- 仅对短得多的定长报文摘要 *H* 进行数字签名要比对整个长报文进行数字签名要简单得多，所耗费的计算资源也小得多。
- 但对鉴别报文 *X* 来说，效果是一样的。也就是说，报文 *X* 和已签名的报文摘要 *D*(*H*) 合在一起是不可伪造的，是可检验的和不可否认的。

报文摘要算法

- 报文摘要算法就是一种散列函数。这种散列函数也叫做密码编码的检验和。报文摘要算法是防止报文被人恶意篡改。
- 报文摘要算法是精心选择的一种单向函数。
- 可以很容易地计算出一个长报文 *X* 的报文摘要 *H*，但要想从报文摘要 *H* 反过来找到原始的报文 *X*，则实际上是不可能的。
- 若想找到任意两个报文，使得它们具有相同的报文摘要，那么实际上也是不可能的。

报文摘要的实现

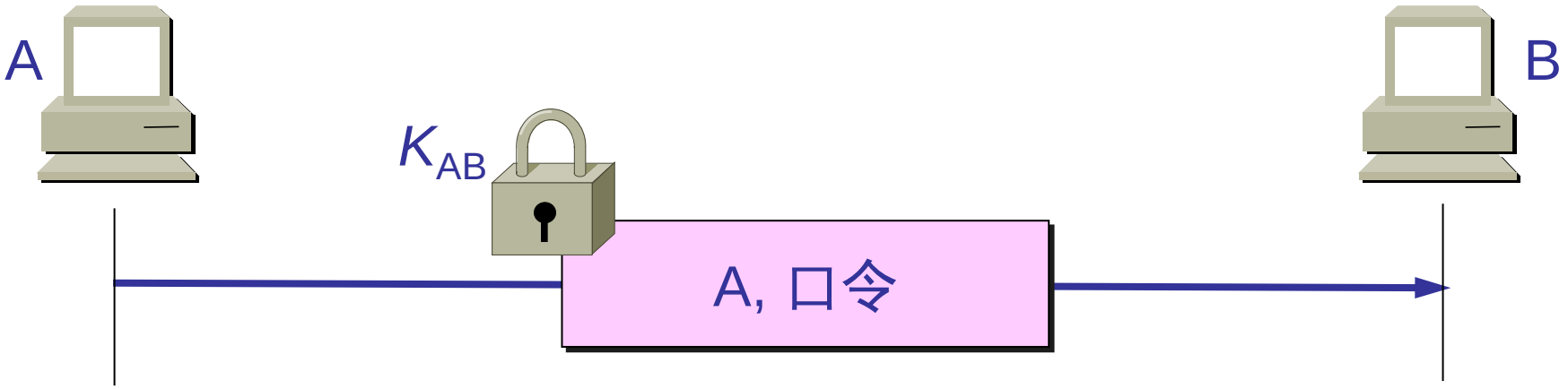

A
报文鉴别码
因特网
B
报文 X
发送
MAC
报文 X
MAC
报文 X
报文摘要
运算
A 的私钥
签名
A 的公钥
E 运算
报文摘要
运算
核实签名
比较
H
D 运算
MAC
H
H
报文摘要
报文鉴别码
报文摘要
报文摘要

7.4.2 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 的报文的被加密，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。



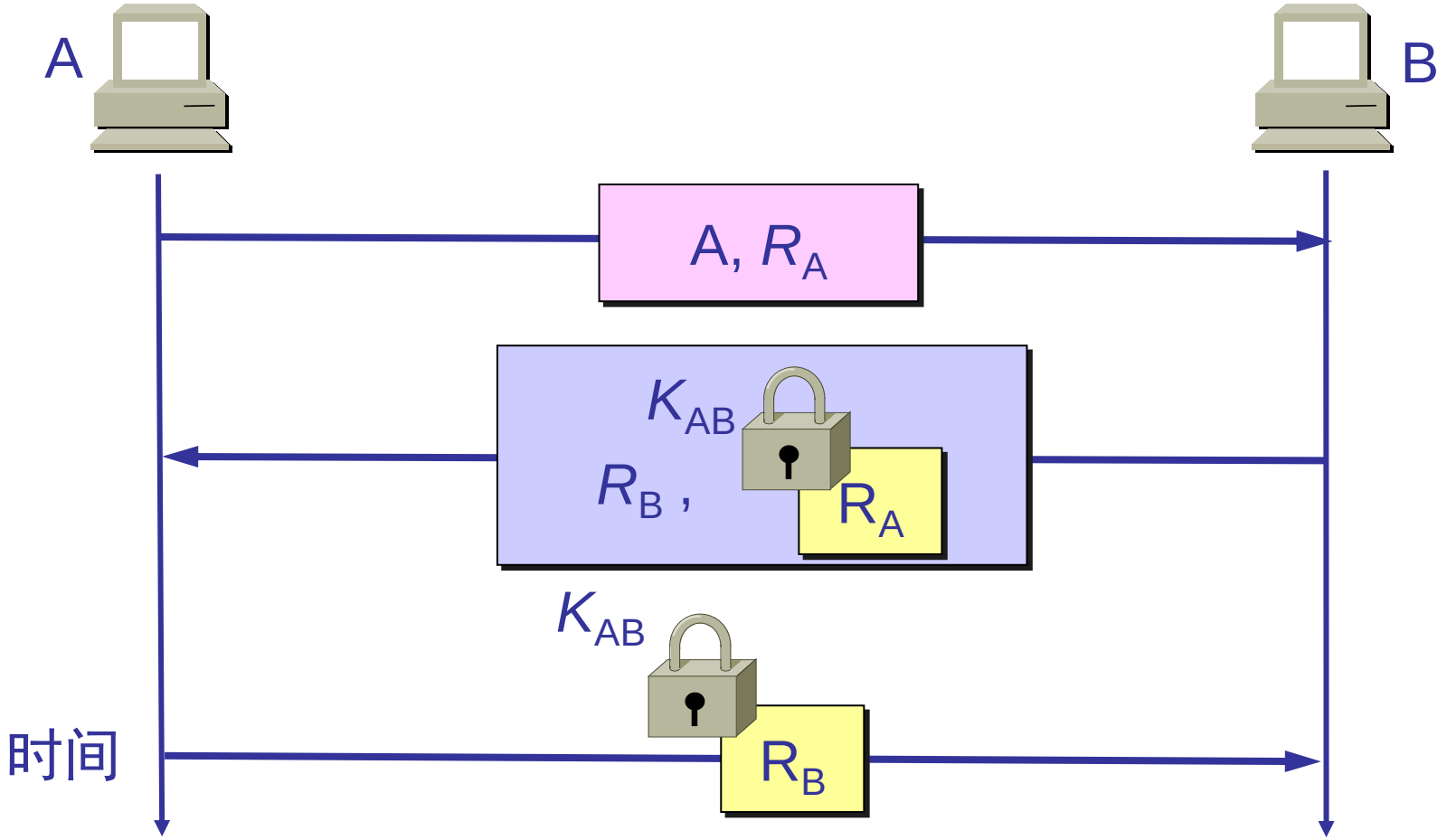
明显的漏洞

- 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（因为这可能很花很多时间）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。

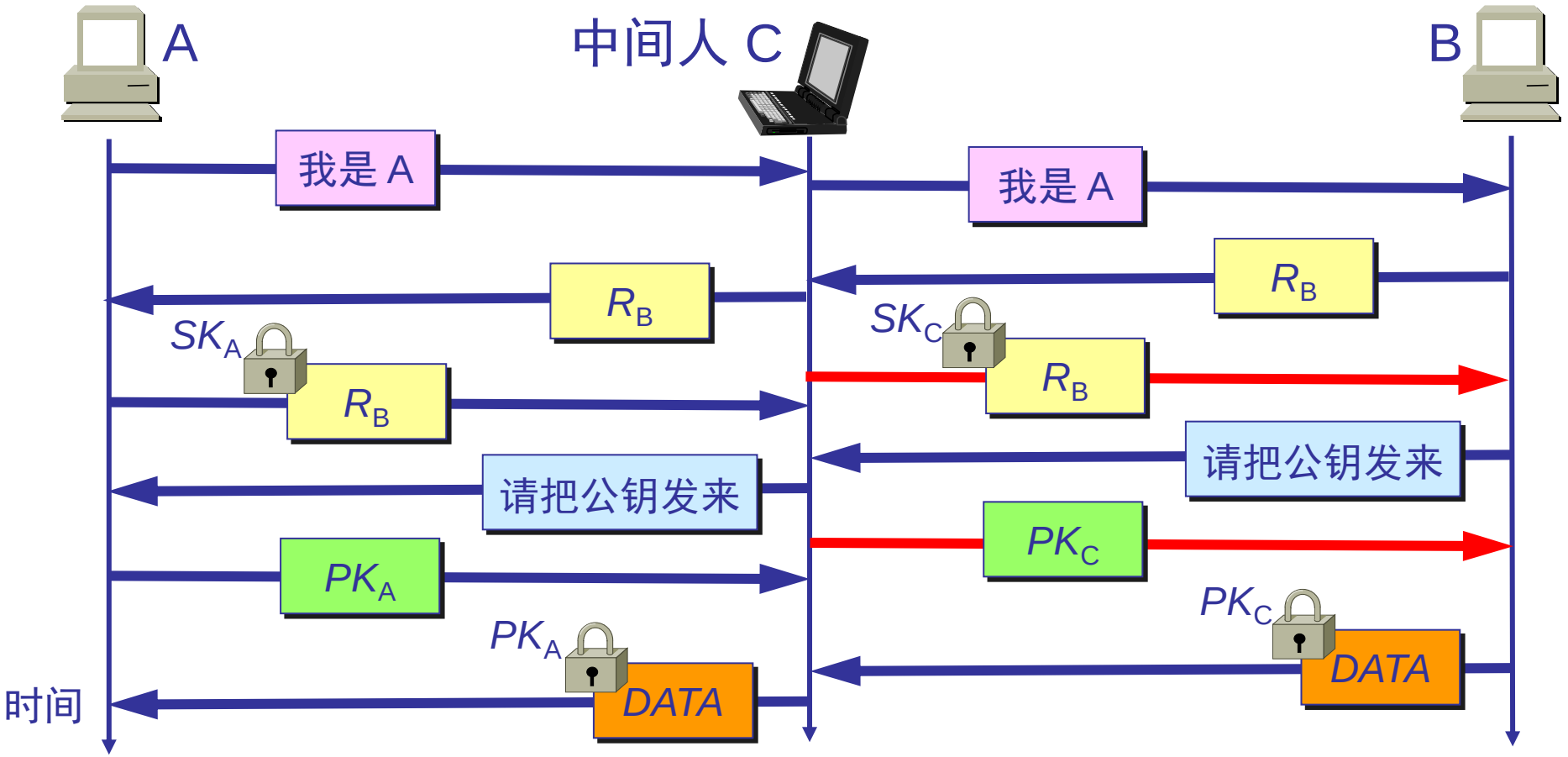
使用不重数

- 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



课件制作人：谢希仁

中间人攻击说明

- A 向 B 发送“我是 A”的报文，并给出了自己的身份。此报文被“中间人” C 截获，C 把此报文原封不动地转发给 B。B 选择一个不重数 R_B 发送给 A，但同样被 C 截获后也照样转发给 A。
- 中间人 C 用自己的私钥 SK_C 对 R_B 加密后发回给 B，使 B 误以为是 A 发来的。A 收到 R_B 后也用自己的私钥 SK_A 对 R_B 加密后发回给 B，中途被 C 截获并丢弃。B 向 A 索取其公钥，此报文被 C截获后转发给 A。
- C 把自己的公钥 PK_C 冒充是 A 的发送给 B，而 C 也截获到 A 发送给 B 的公钥 PK_A。
- B 用收到的公钥 PK_C（以为是 A 的）对数据加密发送给 A。C 截获后用自己的私钥 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。

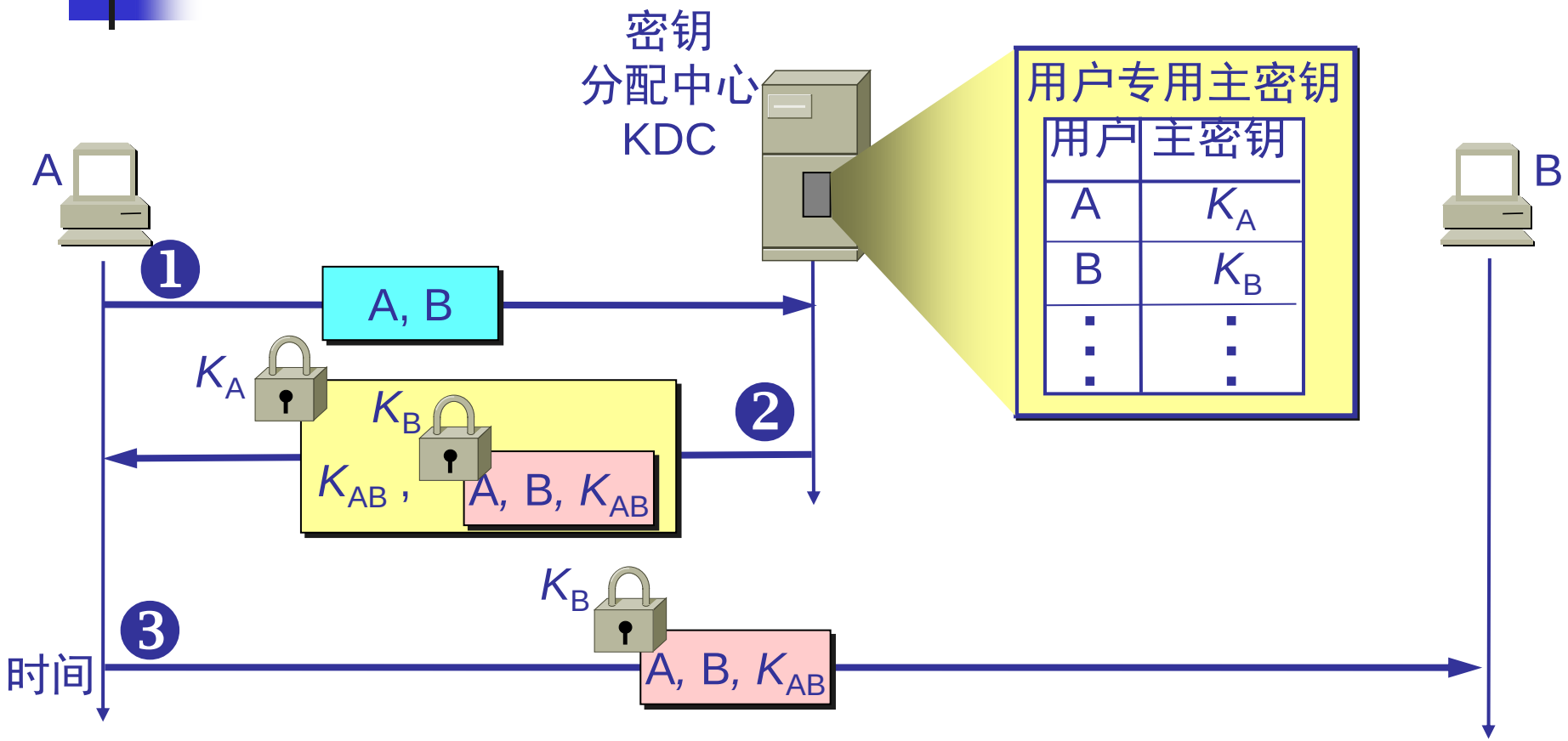
7.5 密钥分配

- 密钥管理包括：密钥的产生、分配、注入、验证和使用。本节只讨论密钥的分配。
- 密钥分配是密钥管理中最大的问题。密钥必须通过最安全的通路进行分配。
- 目前常用的密钥分配方式是设立密钥分配中心 KDC (Key Distribution)，通过 KDC 来分配密钥。

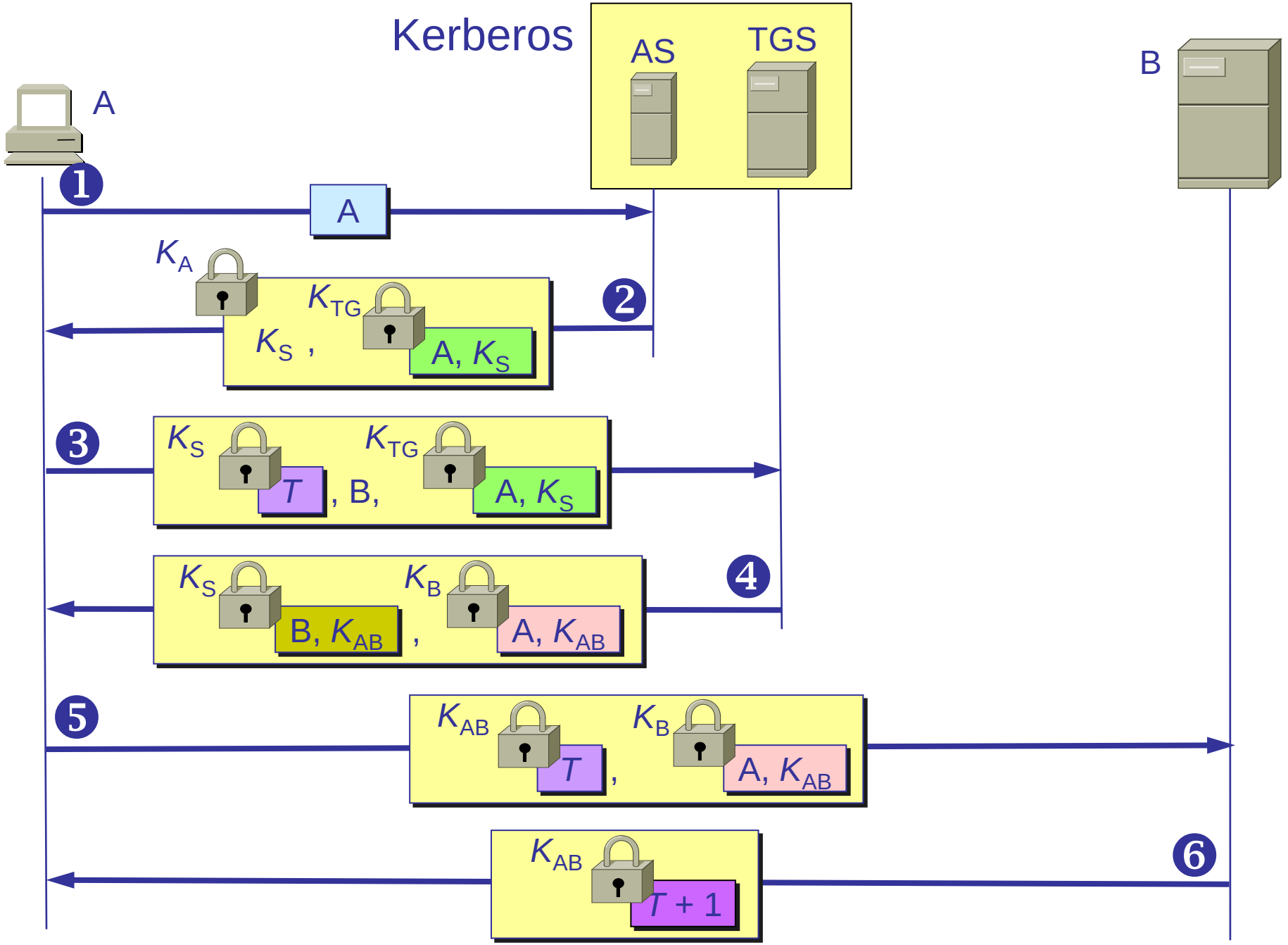
7.5.1 对称密钥的分配

- 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



课件制作人：谢希仁


Kerberos
AS
TGS
A
B
1
A
K_A
K_{TG}
K_S ,
A, K_S
2
3
K_S
K_{TG}
T
, B,
A, K_S
4
K_S
K_B
B, K_{AB}
,
A, K_{AB}
5
K_{AB}
K_B
T
,
A, K_{AB}
6
K_{AB}
$T + 1$

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。

7.6 因特网使用的安全协议

7.6.1 网络层安全协议

1. IPsec 协议

网络层保密是指所有在 IP 数据报中的数据都是加密的。

IPsec 中最主要的两个部分

- 鉴别首部 AH (Authentication Header)：AH鉴别源点和检查数据完整性，但不能保密。
- 封装安全有效载荷 ESP (Encapsulation Security Payload)：ESP 比 AH 复杂得多，它鉴别源点、检查数据完整性和提供保密。

安全关联 SA (Security Association)

- 在使用 AH 或 ESP 之前，先要从源主机到目的主机建立一条网络层的逻辑连接。此逻辑连接叫做安全关联 SA。
- IPsec 就把传统的因特网无连接的网络层转换为具有逻辑连接的层。

安全关联的特点

- 安全关联是一个单向连接。它由一个三元组唯一地确定，包括：

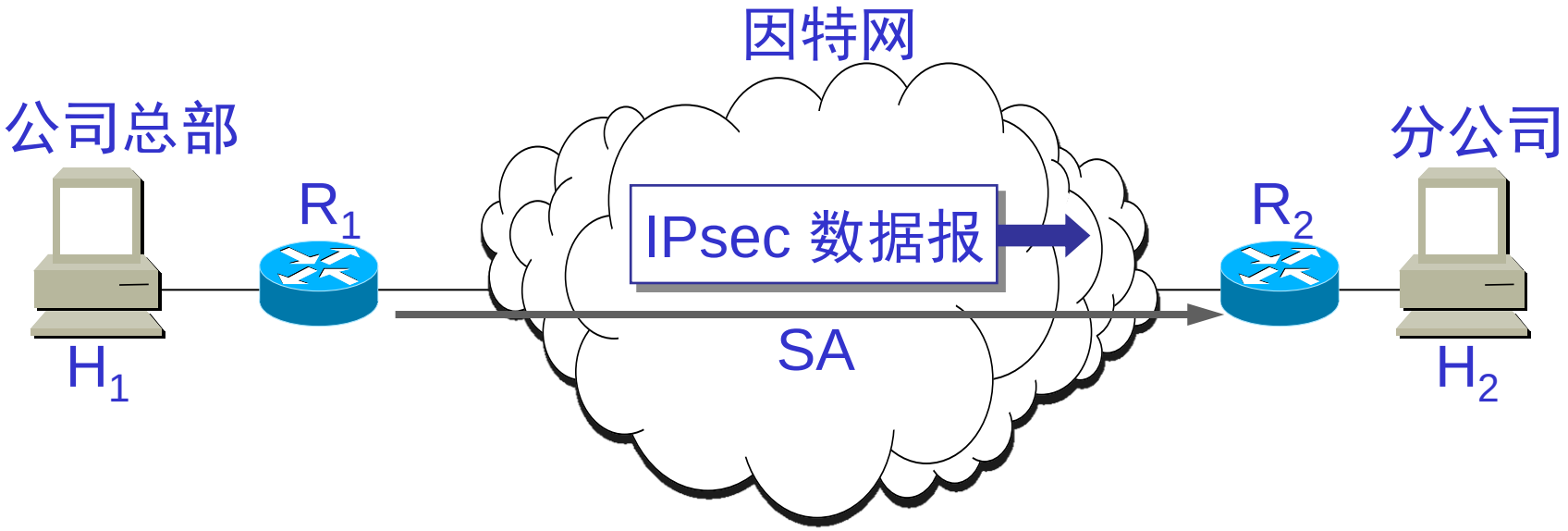
(1) 安全协议（使用 AH 或 ESP）的标识符

(2) 此单向连接的源 IP 地址

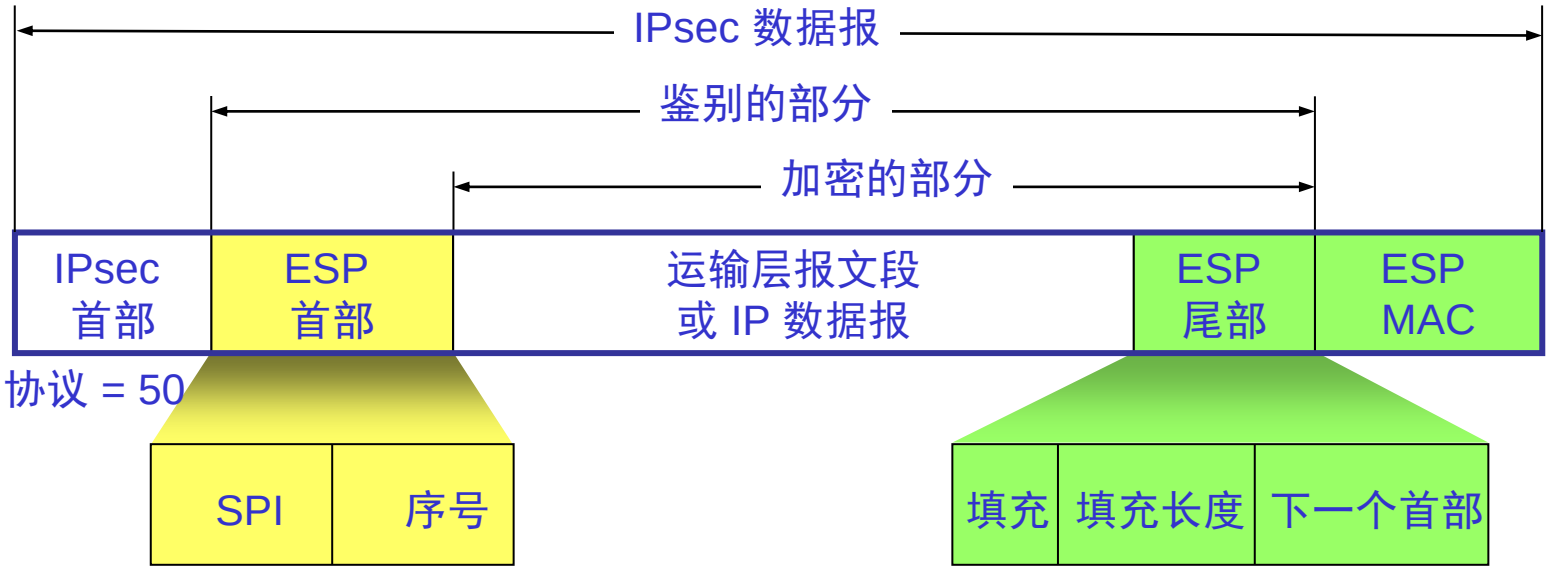
(3) 一个 32 位的连接标识符，称为安全参数索引 SPI (Security Parameter Index)

- 对于一个给定的安全关联 SA，每一个 IPsec 数据报都有一个存放 SPI 的字段。通过此 SA 的所有数据报都使用同样的 SPI 值。

路由器 R_1 到 R_2 的安全关联 SA



2. IPsec数据报的格式



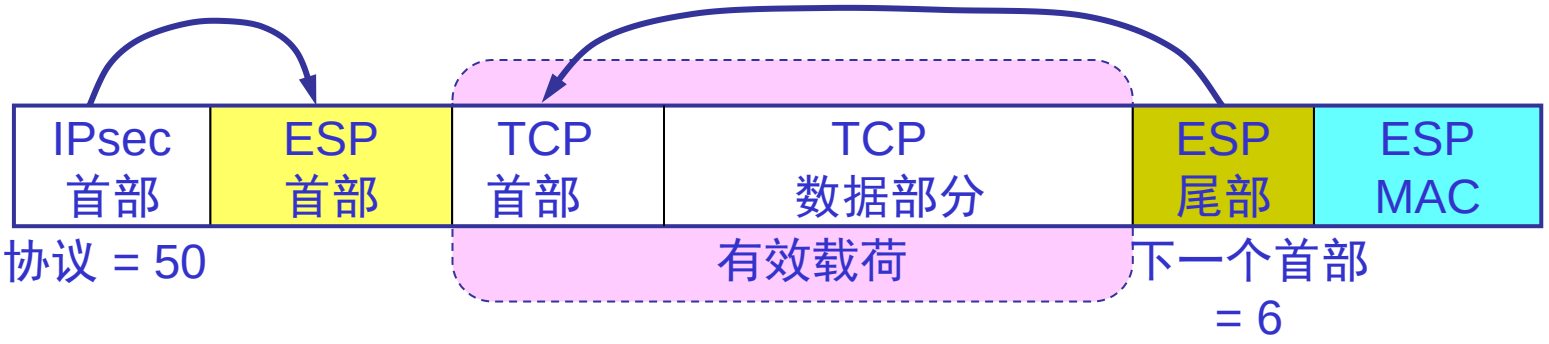
IPsec数据报有以下两种不同的工作方式

一、运输方式(transport mode)：在整个运输层报文段的后面和前面分别添加一些控制字段，构成 IPsec 数据报，把整个运输层报文段都保护起来，很适合于主机到主机之间的安全传送，但这需要使用 IPsec 的主机都运行 IPsec协议。

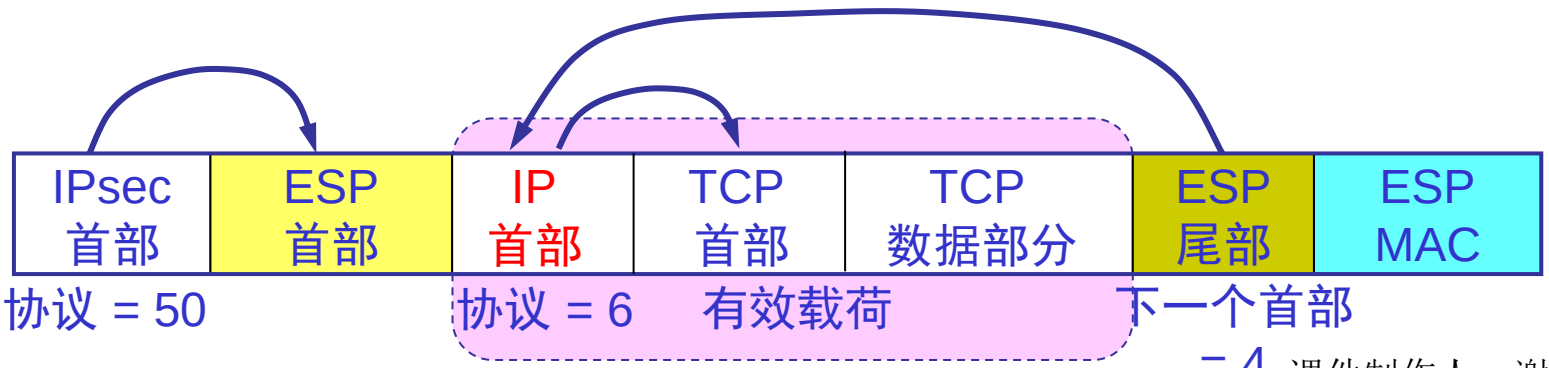
二、隧道方式(tunnel mode)：在 IP 数据报的后面和前面分别添加一些控制字段，构成 IPsec 数据报。 这需要在 IPsec 数据报所经过的所有路由器都运行 IPsec 协议。隧道方式常用来实现虚拟专用网 VPN。

下一个首部的作用

(a) 运输方式



(b) 隧道方式



3. IPsec 的其他构件

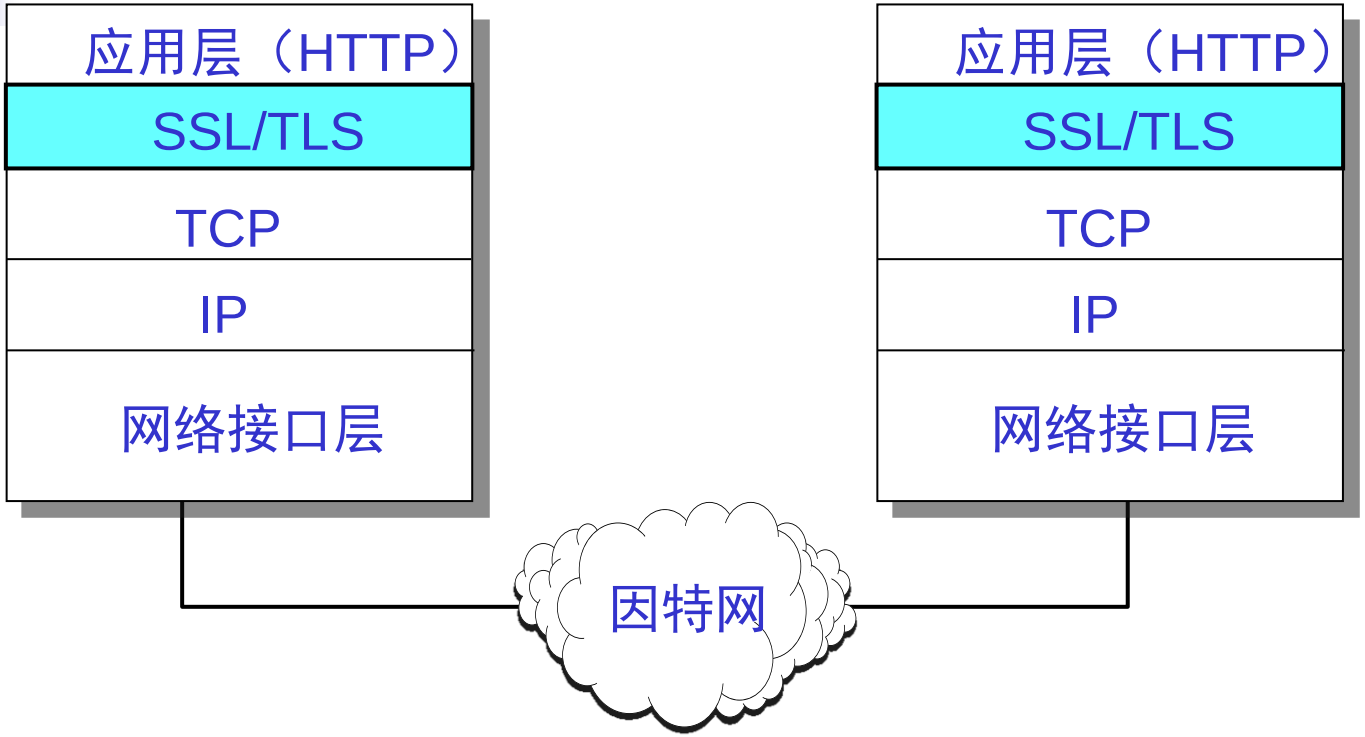
- 安全关联数据库 SAD (Security Association Database) 。
- 安全策略数据库 SPD (Security Policy Database) 。
- 因特网密钥交换 IKE (Internet Key Exchange)协议
  - Oakley——密钥生成协议
  - 安全密钥交换机制 SKEME (Secure Key Exchange Mechanism) ——用于密钥交换的协议
  - 因特网安全关联和密钥管理协议 ISAKMP (Internet Secure Association and Key Management Mechanism) ——用于实现 IKE 中定义的密钥交换

7.6.2 运输层安全协议

现在广泛使用的有以下两个协议：

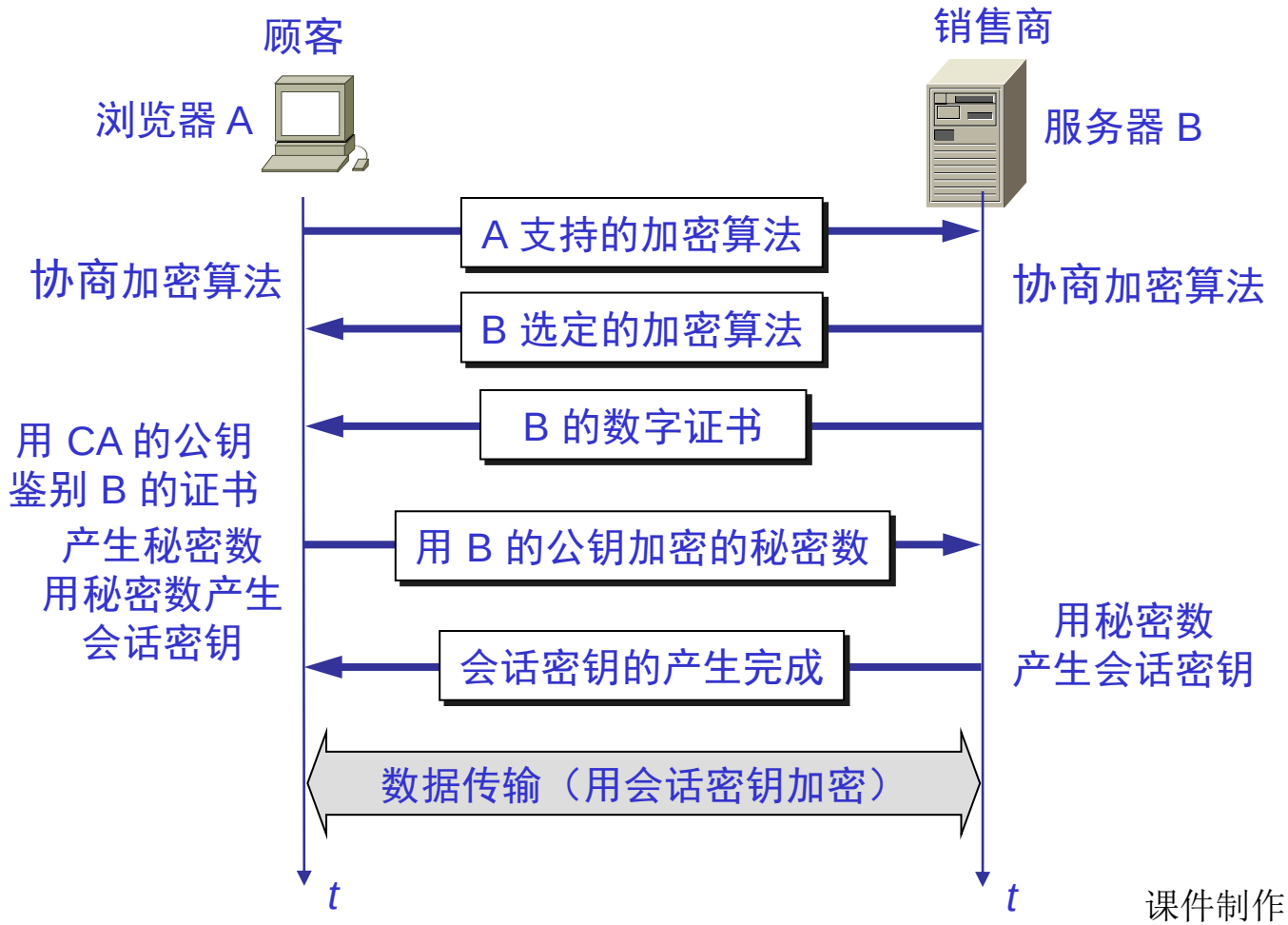
- 安全套接字层 SSL (Secure Socket Layer)
- 运输层安全 TLS (Transport Layer Security)。

SSL/TLS 的位置



在发送方，SSL 接收应用层的数据（如 HTTP 或 IMAP 报文），对数据进行加密，然后把加了密的数据送往 TCP 套接字。
在接收方，SSL 从 TCP 套接字读取数据，解密后把数据交给应用层。

SSL安全会话建立过程如下



课件制作人：谢希仁

7.6.3 应用层的安全协议 PGP (Pretty Good Privacy)

- PGP 是一个完整的电子邮件安全软件包，包括加密、鉴别、电子签名和压缩等技术。
- PGP 并没有使用什么新的概念，它只是将现有的一些算法如 MD5，RSA，以及 IDEA 等综合在一起而已。
- 虽然 PGP 已被广泛使用，但 PGP 并不是因特网的正式标准。

用 PGP 进行加密

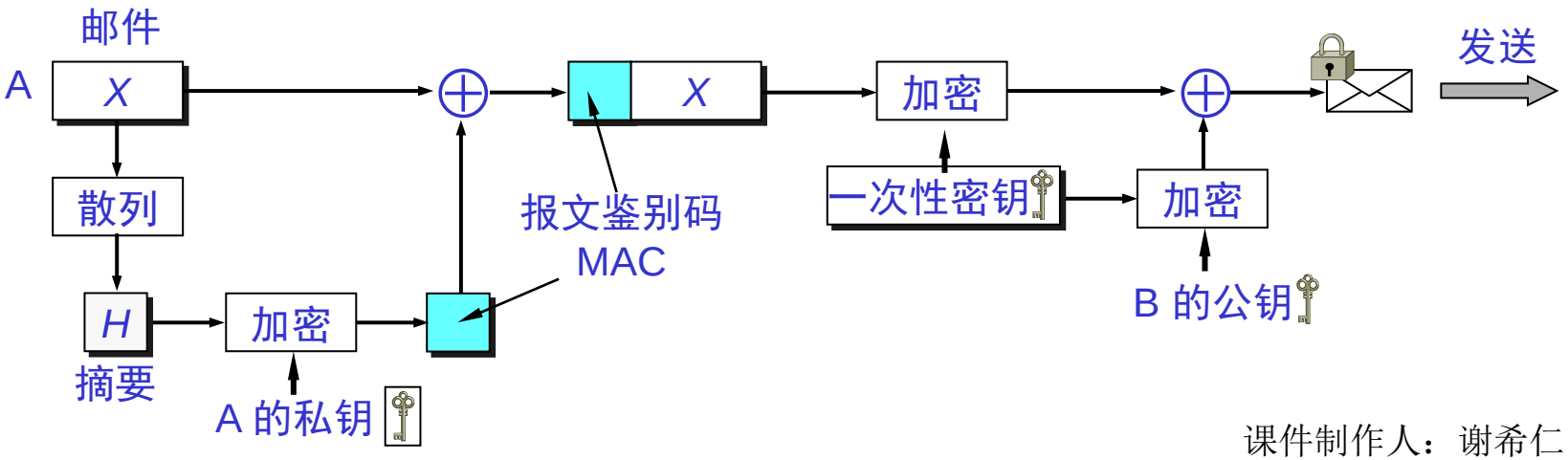
A有三个密钥：

自己的私钥、B的公钥

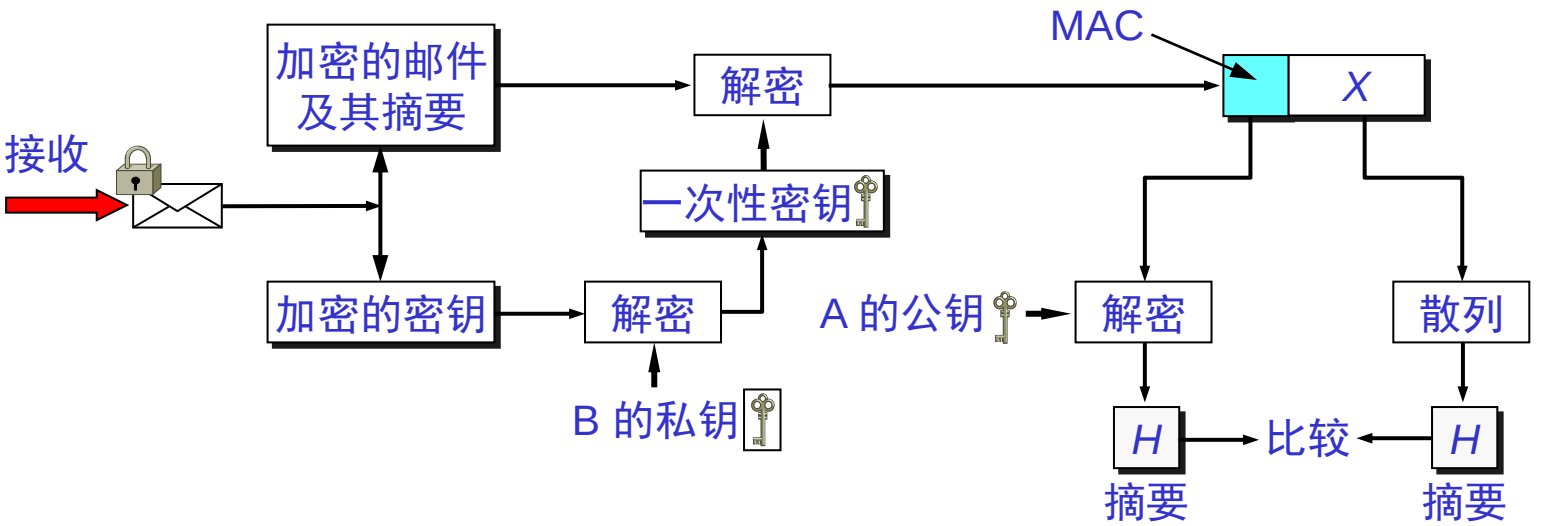
和自己生成的一次性密钥。

B有两个密钥：

自己的私钥和A的公钥。



用 PGP 进行解密

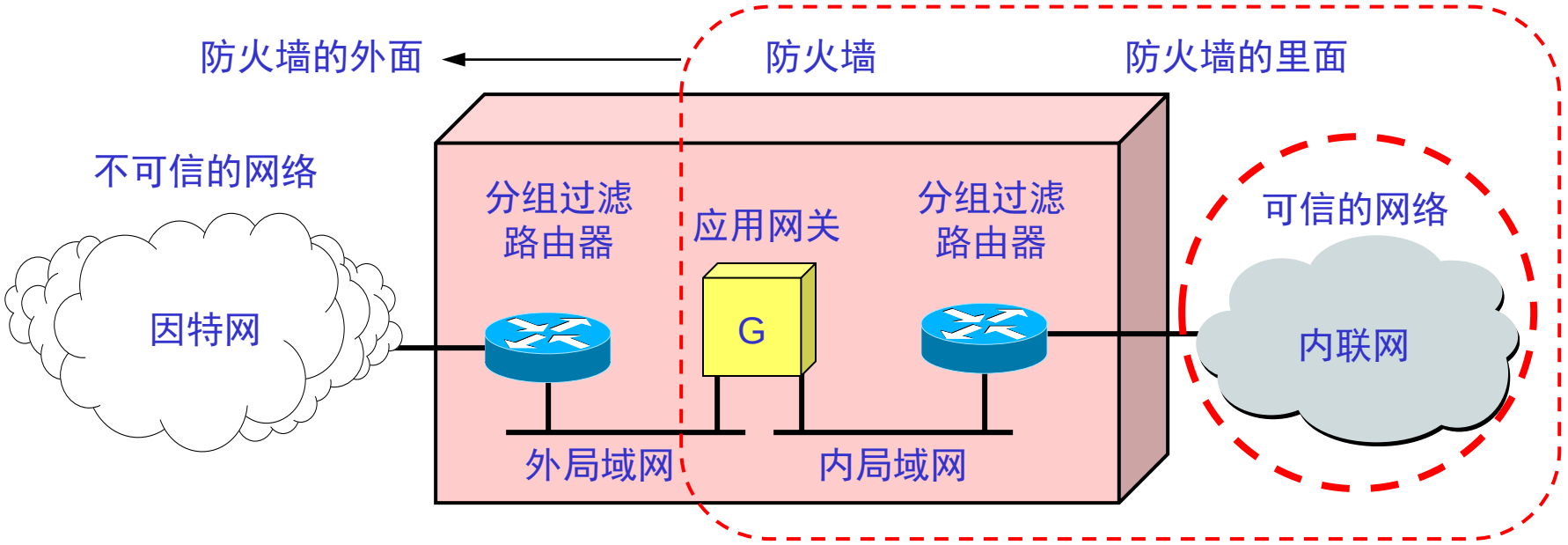


7.7 系统安全：防火墙与入侵检测

7.7.1 防火墙

- 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“可信的网络”(trusted network)，而将外部的因特网称为“不可信的网络”(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



课件制作人：谢希仁

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。

7.7.2 入侵检测系统

- 入侵检测系统 IDS (Intrusion Detection System)能够在入侵已经开始，但还没有造成危害或在造成更大危害前，及时检测到入侵，以便尽快阻止入侵，把危害降低到最小。
- 基于特征的 IDS 维护一个所有已知攻击标志性特征的数据库。
- 基于特征的IDS只能检测已知攻击，对于未知攻击则束手无策。