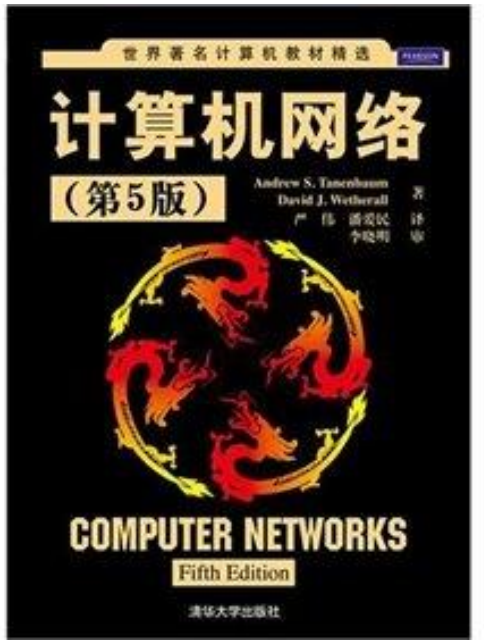
计算机网络

Andrew S. Tanenbaum（5 Edition）



计算机网络

第1章 引言

第2章 物理层

第3章 数据链路层

第4章 介质访问控制子层

第5章 网络层

第6章 传输层

第7章 应用层

第8章 网络安全

第8章 网络安全

8.1 网络安全问题概述

计算机网络面临的安全性威胁

大多数安全问题都是由于某些恶意的人企图获得某种利益、引起别人注意、或者伤害他人而有意制造的。

攻击者	目的
学生	乐于窥探他人电子邮件
黑客	测试某人的安全系统；盗取数据
推销员	声称能代表整个欧洲，而不只是安道尔
公司	发现竞争者的策略性市场计划
离职员工	因被解雇而实施报复
会计	挪用公司公款
股票经纪人	拒绝通过E-mail向顾客做过的承诺
身份盗取	出售窃取信用卡号码
政府	了解敌人的军事或工业机密
恐怖分子	窃取生物战秘密

图 8-1　最常见的攻击者及目的

8.1 网络安全问题概述

计算机网络面临的安全性威胁

大多数安全问题都是由于某些恶意的人企图获得某种利益、引起别人注意、或者伤害他人而有意制造的。

计算机网络上的通信面临以下四种威胁：

① 截获——从网络上窃听他人的通信内容

② 中断——有意中断他人在网络上的通信

③ 篡改——故意篡改网络上传送的报文

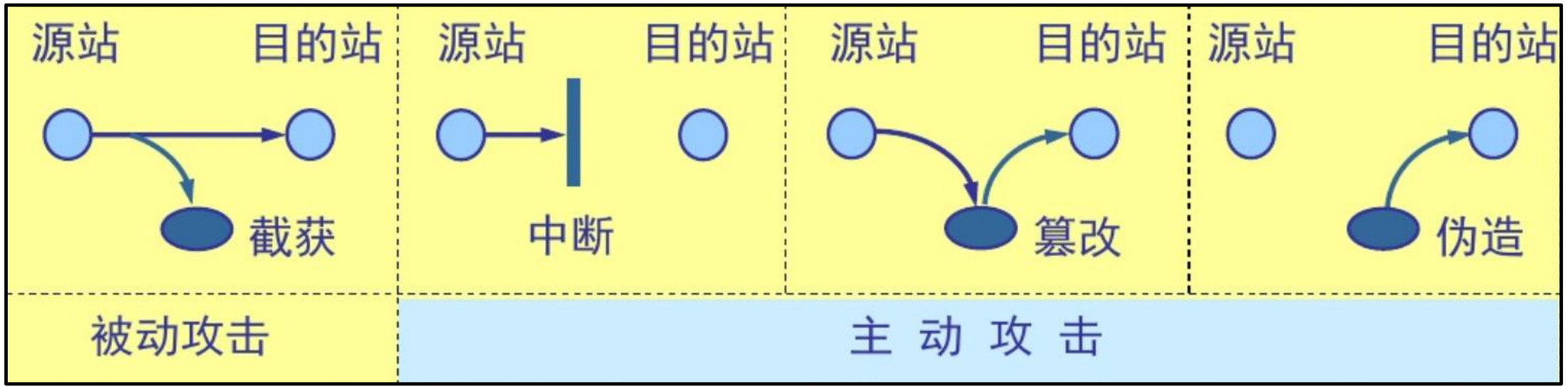
④ 伪造——伪造信息在网络上传送

截获信息的攻击称为被动攻击，而更改信息和拒绝用户使用资源的攻击称为主动攻击

8.1 网络安全问题概述

计算机网络面临的安全性威胁

对网络的被动攻击和主动攻击



8.1 网络安全问题概述

计算机网络面临的安全性威胁

恶意程序

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某种特殊功能的程序

8.1 网络安全问题概述

计算机网络面临的安全性威胁

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

计算机网络安全的内容

① 保密性

② 安全协议的设计

③ 访问控制

8.1 网络安全问题概述

计算机网络面临的安全性威胁

- 计算机网络安全问题可以分成4个相互交织的领域：

① 保密：防止被窃听

② 认证：确定通信用户的身份

③ 不可否认：不可抵赖的电子签名

④ 完整性控制：防止信息被篡改

8.1 网络安全问题概述

密码学基础

密码编码学是密码体制的设计学，而密码分析学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。两者合起来统称为密码学

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市安全的。

8.1 网络安全问题概述

密码学基础

密码编码学是密码体制的设计学，而密码分析学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。两者合起来统称为密码学

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市安全的。

8.1 网络安全问题概述

密码学基础

密码学=密码编码学+密码分析学

一般的数据加密模型（对称密钥密码）

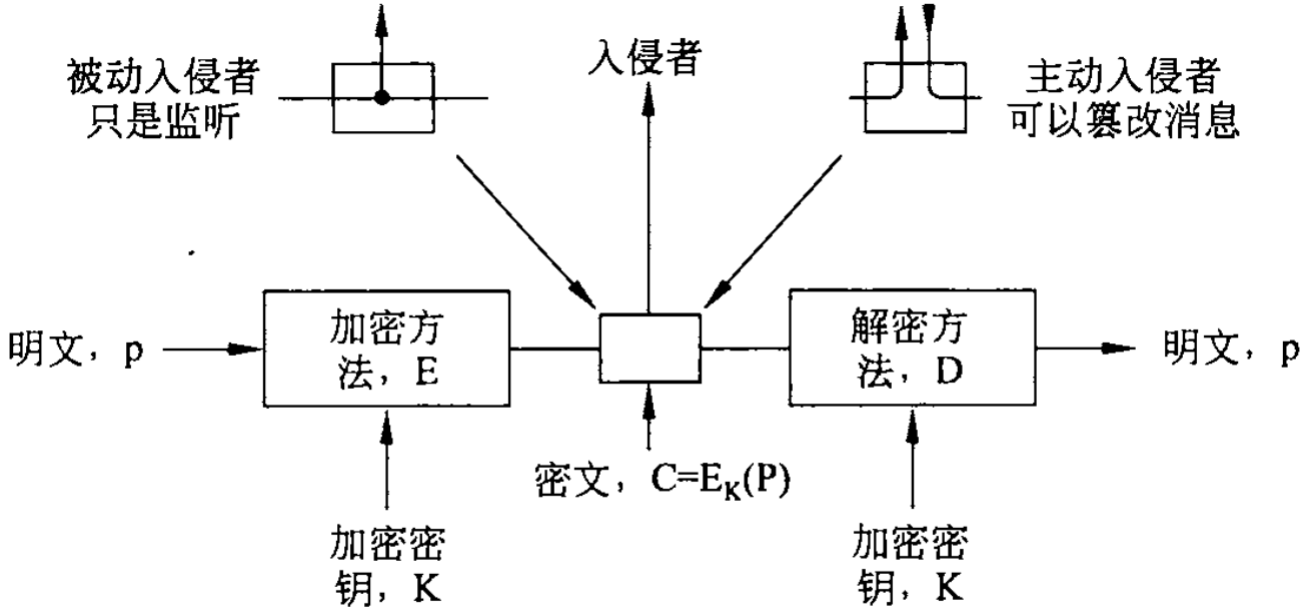


图 8-2　加密模型（对称密钥密码）

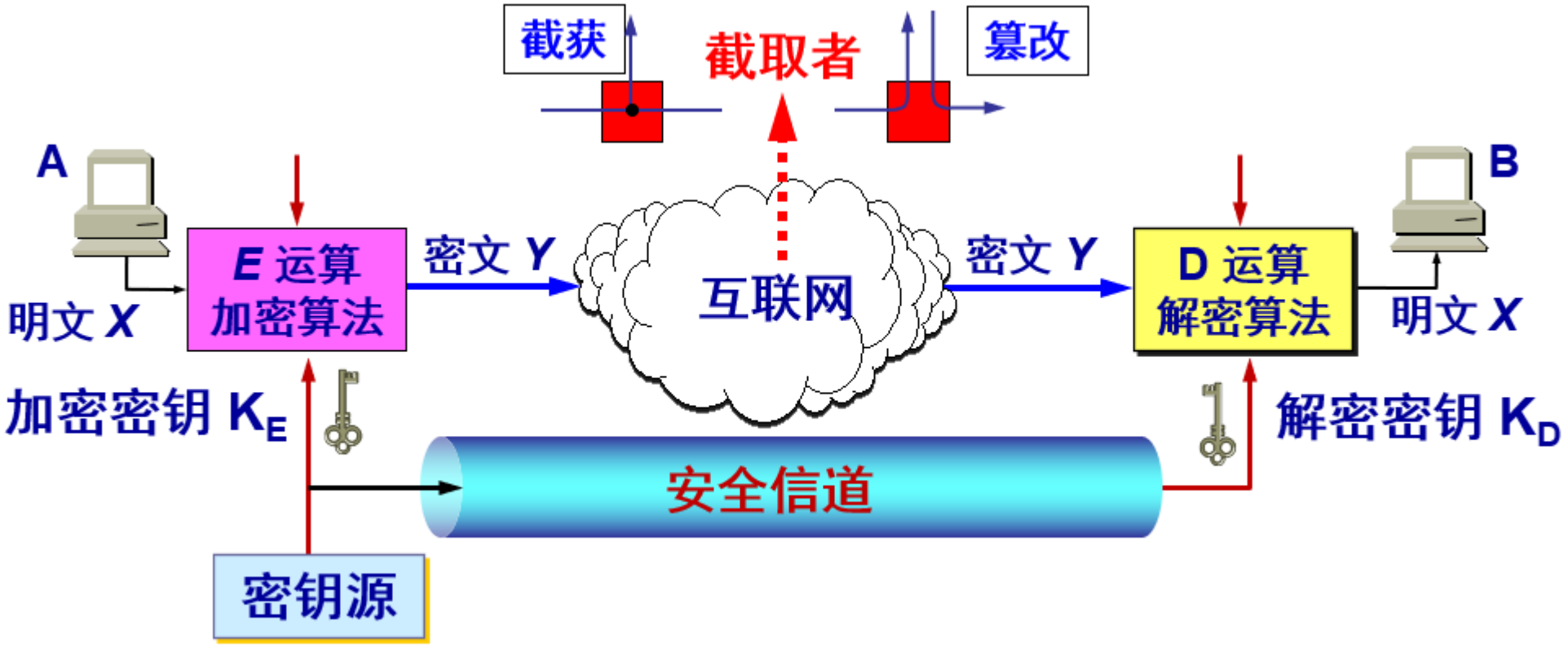
8.1 网络安全问题概述

密码学基础

- **密码：**逐个字符或者逐个位的进行变化，它不涉及信息的语言结构
- **编码：**用一个词或符号来代替另一个词，编码学是密码体制的设计学
- **明文：**待加密的消息称为明文。明文经过一个以密钥为参数的函数变换，这个过程的结果就是所谓的**密文。密钥**是一种参数，它是在明文转换为密文或将密文转换为明文的算法中输入的参数
- 入侵者不仅可以监听通信性的，还可以将记录下来，在以后回放或插入他自己的消息，或者篡改消息内容发送给接收方。

8.1 网络安全问题概述

密码学基础



- Kerckhoff原则：加密算法市公开的，但是密钥是保密的

8.1 网络安全问题概述

密码学基础

- **密码学的基本规则：假定密码分析者一定知道加密和解密所使用的方法**
- 让密码分析者知道加解密算法，并且把所有的秘密信息全部放在密钥中。
- 佛兰德军事密码学家August Kerckhoff在1883年第1次提出Kerckhoff原则：**所有的算法必须是公开的，而密钥是保密的，**
- **密码分析者的角度来看，密码分析问题有三个主要的变种：**

1、**唯密文问题**：有一定量的密文，但是没有明文--报纸上猜谜栏目中的密码难题就是属于这类问题

2、**已知明文问题**：有一些相匹配的密文和明文

3、**选择明文问题**：能够加密某一些他自己选择的明文

8.1 网络安全问题概述

密码学基础

历史上，加密方法被分成：置换密码和替代密码

- 1、**置换密码**：每个字母或者每一组字母被另一个字母或另一组字母替代，从而将原来字母掩盖起来，最古老的密码之一是凯撒密码.

  明文：a b c d e f g …

  密文：D E F G H I J…

一般化方案：允许明文按字母顺序被移动k个字母，k变成一个密钥。

8.1 网络安全问题概述

密码学基础

历史上，加密方法被分成：置换密码和替代密码

- **1、置换密码**：每个字母或者每一组字母被另一个字母或另一组字母替代，从而将原来字母掩盖起来，最古老的密码之一是凯撒密码.
- **改进：**让明文中的每一个符号映射到其他某个字母上---**单字母置换密码**

明文：	a b c d e f g h i j k l m n o p q r s t u v w x y z
密文：	Q W E R T Y U I O P A S D F G H J K L Z X C V B N M

- **破解方法：**利用自然语言的统计特性，通过猜测常见的字母、两字母连字和三字母连字，并且利用元音和辅音的各种可能组合，逐个字母地构造出试探性的明文。

8.1 网络安全问题概述

密码学基础

历史上，加密方法被分成：置换密码和替代密码

- 2、**替代密码**：重新对字母进行排序，但是并不伪装明文

常见的替代密码：列换位--该方案用一个不包含任何重复字母的单词或者短语作为密钥.

M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
p	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d

明文：
pleasetransferonemilliondollarsto
myswissbankaccountsixtwotwo

密文：
AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRCXB

图 8-3　替代密码

8.1 网络安全问题概述

密码学基础

- **一次性密钥**：选择一个随机串作为密钥，逐位异或后产生的加密序列具有不可攻破的特性。
- 原因：任何给定长度的明文都有相同的可能性，所以消息中根本不存在任何可疑用来解密的信息。

消息 1：	1001001 0100000 1101100 1101111 1110110 1100101 0100000 1111001 1101111 1110101 0101110
一次性密钥 1：	1010010 1001011 1110010 1010101 1010010 1100011 0001011 0101010 1010111 1100110 0101011
密文：	0011011 1101011 0011110 0111010 0100100 0000110 0101011 1010011 0111000 0010011 0000101
一次性密钥 2：	1011110 0000111 1101000 1010011 1010111 0100110 1000111 0111010 1001110 1110110 1110110
明文：	1000101 1101100 1110110 1101001 1110011 0100000 1101100 1101001 1110110 1100101 1110011

图 8-4　利用一次性密钥进行加密，通过其他一次性密钥可从密文获得任何可能明文

8.1 网络安全问题概述

密码学基础

- **一次性密钥可以抵挡现在和将来的攻击**。理由源于信息理论：因为任何指定长度的明文都有相同的可能性，所以信息中根本不存在任何可以用来解密的信息
- **缺点**：1、无法记忆　2、传送的数据总量收到可用密钥数量的限制　3、对于丢失字符和插入字符非常敏感。---同步问题
- 量子密码

8.1 网络安全问题概述

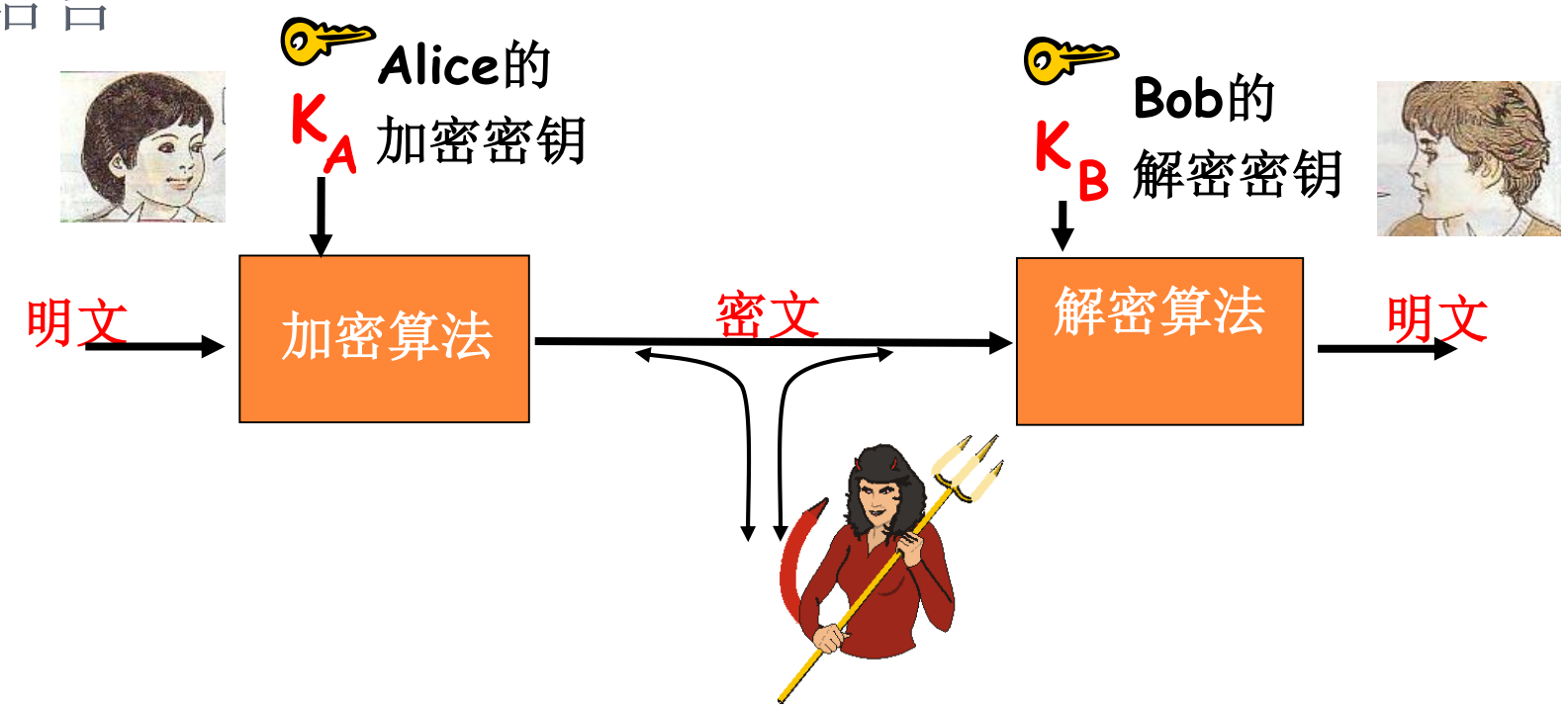
密码学基础

- 两个基本的密码学原则：
  - 1、消息必须包含一定的冗余度。---冗余度
  - 2、需要采取某种方法来对抗**重放攻击**。---新鲜度
- **重放攻击**：使用截获数据包的身份信息伪造数据包

第8章 网络安全

8.2 两类密码算法

- 加密语言



对称密钥密码学：发送方和接收方的密钥相同

公开密钥密码学：发送方使用接收方的公钥进行加密，接收方使用自己的私钥进行解密

8.2 两类密码算法

➢ 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

① 数据加密标准DES属于常规密钥密码体制，是种分组密码。

② 在加密前，先对整个明文进行分组。每一组长为64位。

③ 然后对每一个64位二进制数据进行加密处理，产生一组64为密文数据。

④ 最后将各组密文串接起来，即得出整个的密文。

⑤ 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）。

8.2 两类密码算法

➢ 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。

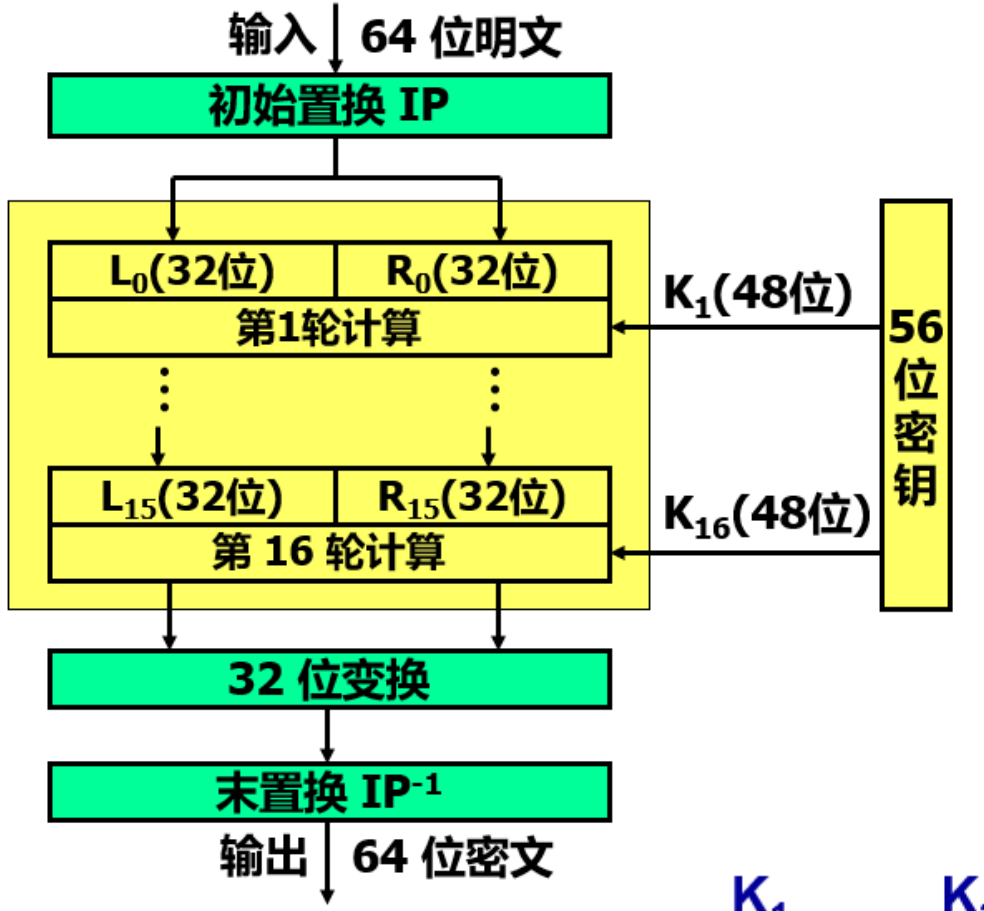
数据加密标准DES

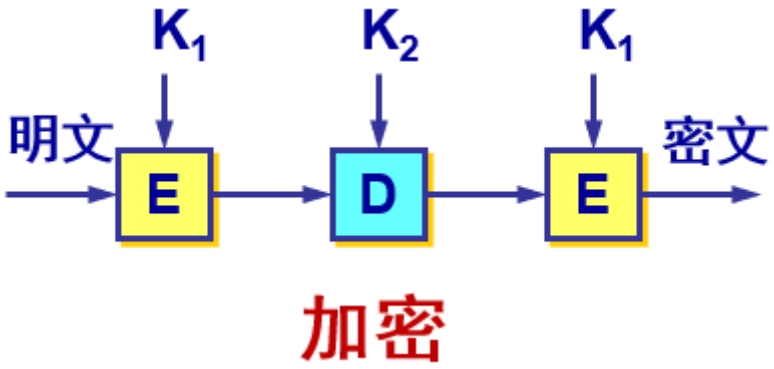
- 对称密钥的保密性仅取决于对密钥的保密，而算法是公开的。尽管人们在破译DES方面取得了许多进展，但是至今仍未能找到比穷尽搜索密钥更有效的方法。
- DES是世界上第一个公认的实用密码算法标准，它曾对密码学的发展做出了重大的贡献。
- 目前较为严重的问题是DES的密钥的长度。
- 现在已经设计出来搜索DES密钥的专用芯片。

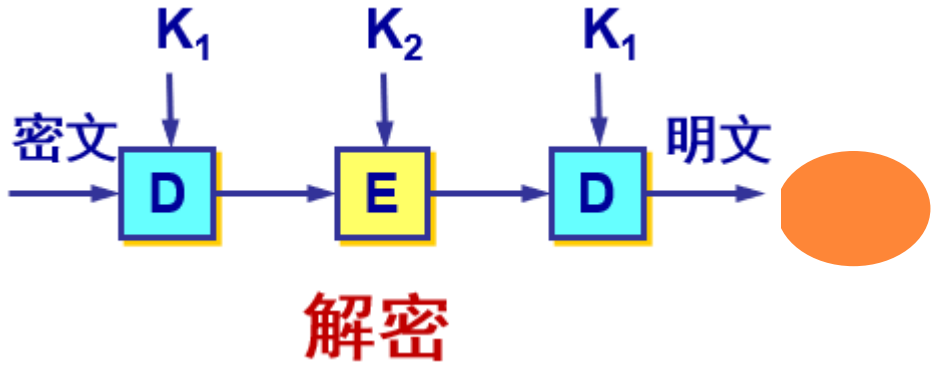
8.2 两类密码算法

- 对称密钥密码体制

  数据加密标准DES







8.2 两类密码算法

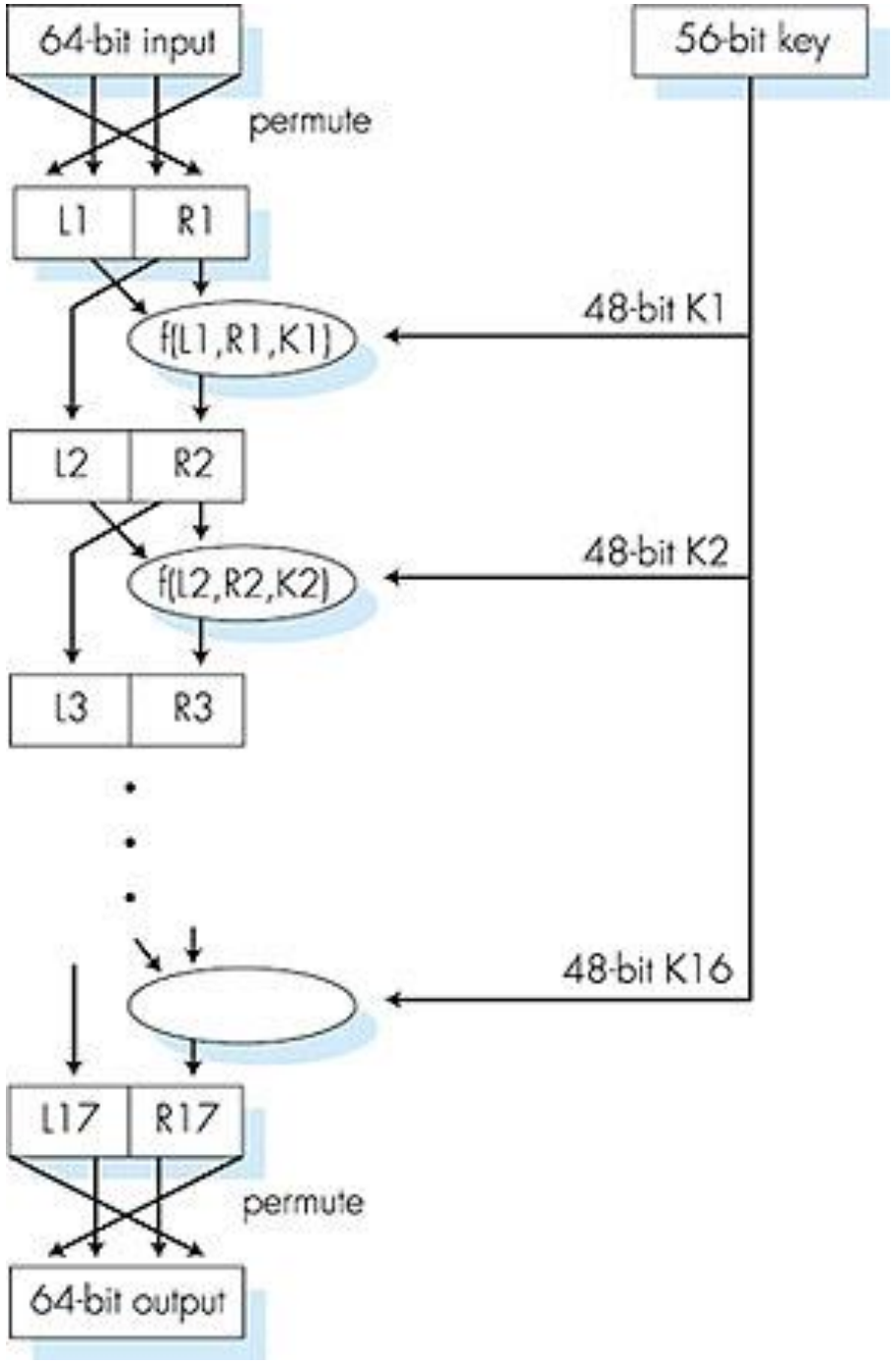
对称密钥加密学：DES

DES operation

初始替换

16 轮一样的函数应用，每一轮使用不同的48bit密钥

最终替换



8.2两类密码算法-〉对称加密

- 对称密钥系统

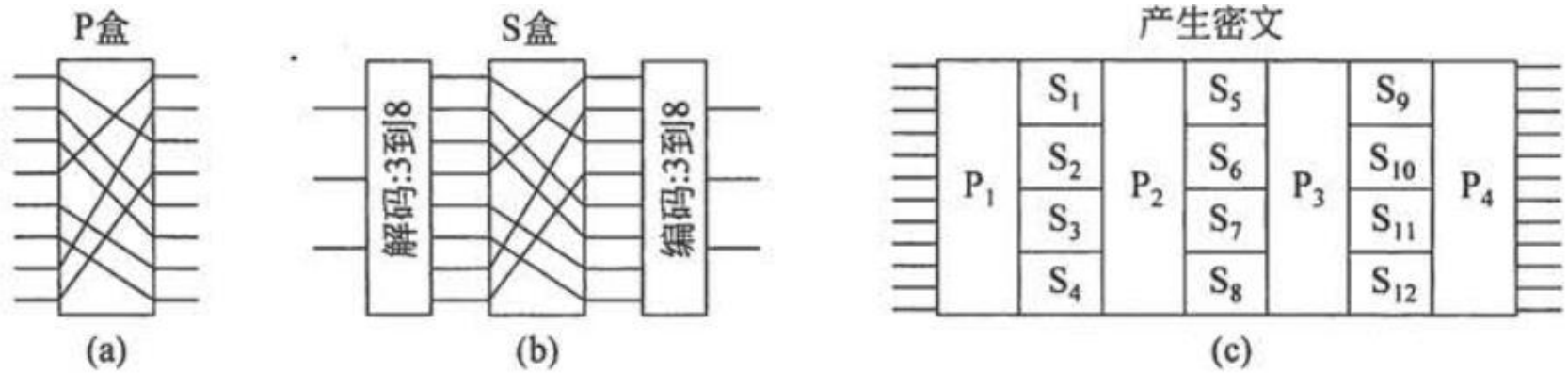
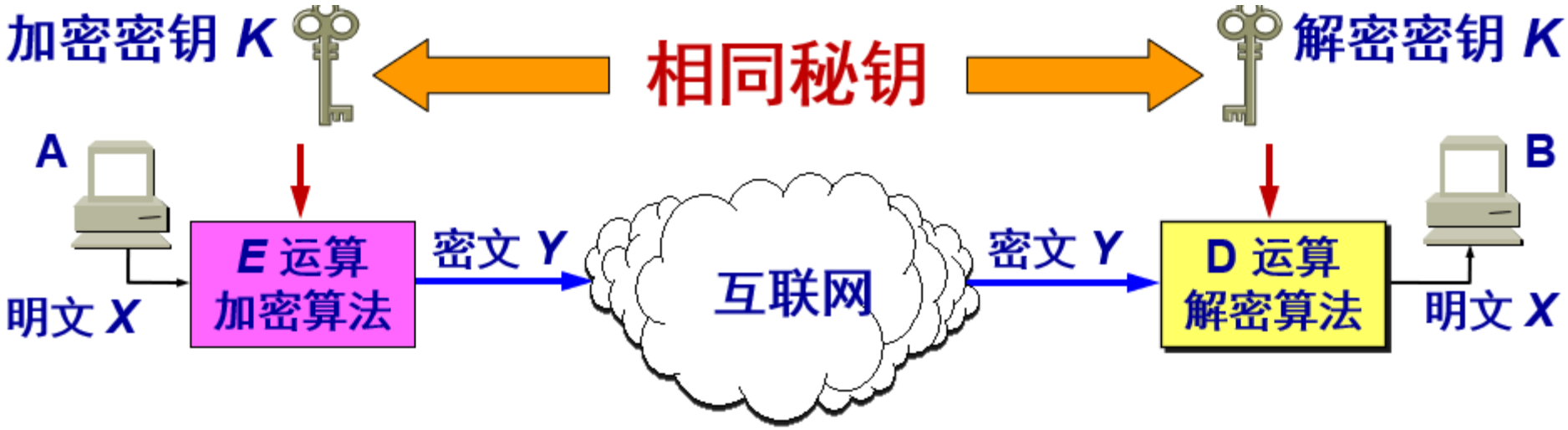


图 8-6　乘积密码的基本元素

(a) P 盒；(b) S 盒；(c) 乘积

8.2两类密码算法-〉对称加密

- 对称密钥系统

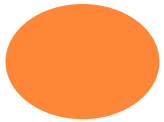


8.2 加密原理-〉对称加密DES

- 对称密钥加密学：DES

DES：Data 加密算法 Standard

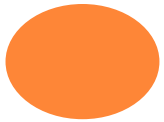
- US 加密标准[NIST 1993]
- 56-bit 对称密钥，64-bit明文输入
- DES有多安全?
  - DES挑战：56-bit密钥加密的短语（“Strong cryptography makes the world a safer place”）被解密，使用了4个月的时间
  - 可能有后门
- 使DES更安全：
  - 使用3个key， 3重DES运算
  - 密文分组成串技术



8.2两类密码算法-〉对称加密AES

➢ AES：Advanced 加密算法 Standard

- 新的对称密钥NIST标准(Nov. 2001）用于替换 DES
- 数据128bit成组加密
- 128, 192, or 256 bit keys
- 穷尽法解密如果使用1秒钟破解DES, 需要花149万亿年破解AES



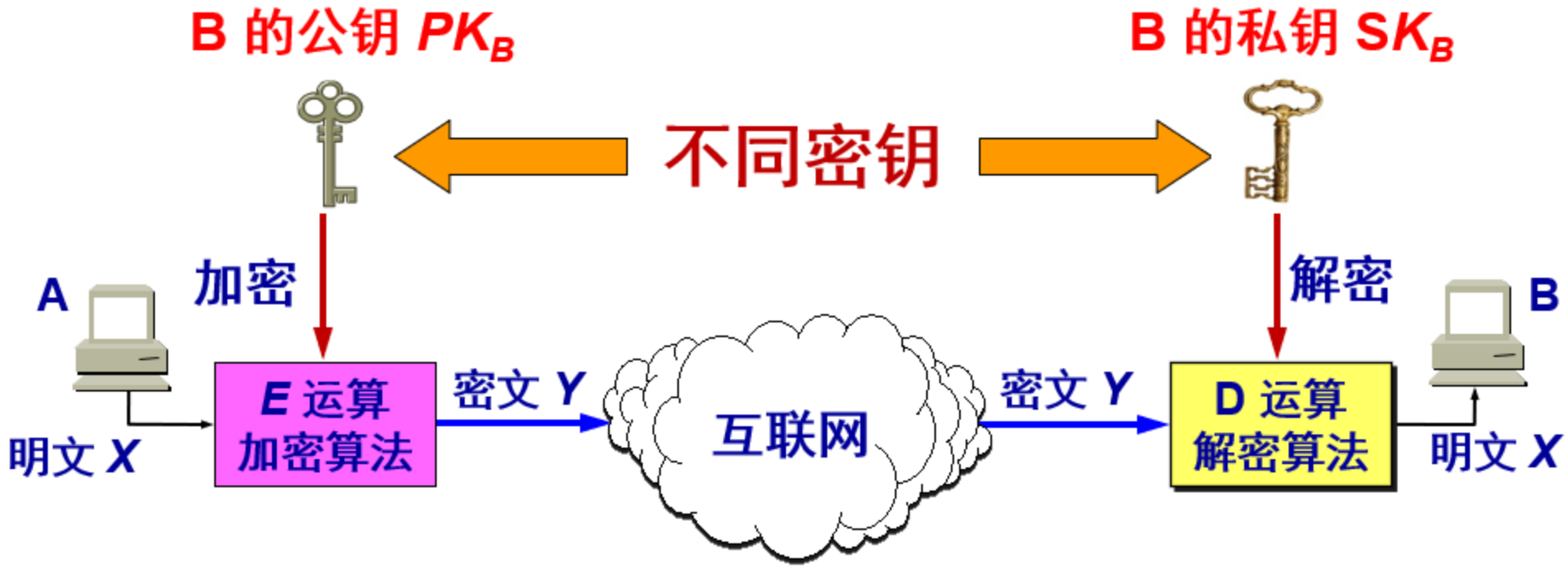
8.2 两类密码算法-〉公开密钥加密体系

➢ 公开密钥密码体制

- 公钥密码体制**使用不同的加密密钥与解密密钥**，是种“由已知的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有两个方面的原因:1、常规密钥密码体制的密钥分配问题2、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, Adelman于1976年提出并在1978年正式发表。

8.2 两类密码算法-〉公开密钥加密体系

- 公开密钥密码学



1、发送者A用B的公钥PK_B对明文X加密（E运算）后，接收者B用自己的私钥SK_B解密（D运算），即可恢复出明文X $D_{SK_B}(Y)=D_{SK_B}(E_{PK_B}(X))=X$

2、解密密钥是接收者专用的秘钥，对其他人都保密。

3、加密密钥是公开的，但不能用它来解密，即 $D_{PK_B}(E_{PK_B}(X))\neq X$

8.2 两类密码算法-〉公开密钥加密体系

➢ 公开密码体制

- 加密密钥和解密密钥：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
- 公钥算法的特点：

1. 加密和解密的运算可以对调，即

   $E_{P_B}(D_{SK_B}(X)) = D_{SK_B}(E_{PK_B}(X))=X$---（*数字签名的原理*）

2. ***在计算机上可容易地产生成对的PK 和SK—公钥密码体制中最核心***
3. 虽然私钥SK是有PK决定的，但是却不能根据PK计算出SK，即从已知的*PK实际上不可能推导出SK，即从PK到SK*是“计算上不可能的”。
4. 加密算法E和解密算法D也都是公开的

8.2 两类密码算法-〉公开密钥加密体系

- RSA：选择密钥

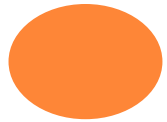
1. 选择2个很大的素数 *p*, *q* (e.g., 1024位)

2. 计算 *n* = *pq*, *z* = (*p*-1)(*q*-1)

3. 选择一个*d* (要求 *d*<*n*) 和z 没有一个公共因子，互素

4. 找到 *e*，使其满足*ed*-1 正好能够被*z整除*.
   (也就是： *ed* mod *z* = 1).

5. 公钥(*e*, *n*). 私钥 (*d*, *n*).



8.2 两类密码算法-〉公开密钥加密体系

明文(P)			密文(C)		解密后	
符号	数值	P^3	$P^3 \pmod{33}$	C^7	$C^7 \pmod{33}$	符号
S	19	6859	28	13 492 928 512	19	S
U	21	9261	21	1 801 088 541	21	U
Z	26	17 576	20	1 280 000 000	26	Z
A	01	1	1	1	01	A
N	14	2744	5	78 125	14	N
N	14	2744	5	78 125	14	N
E	05	125	26	8 031 810 176	05	E

发送方计算　　接收方计算

图 8-17　RSA 算法的一个例子

8.2 两类密码算法-〉公开密钥加密体系

- RSA：加密，解密

0. 给定按照上述算法得到的 (n,e) and (n,d)

1. 加密一个bit模式，m，如此计算：

$c = m^e \mod n$ (i.e.，m^e除以n的余数)

2. 对接收到的密文c解密，如此计算

$m = c^d \mod n$ (i.e.，c^e除以n的余数) d

Magic happens!

$$m = \underbrace{(m^e \mod n)}_{c}{}^d \mod n$$

8.2 两类密码算法-〉公开密钥加密体系

- RSA 例子：

Bob 选择 *p=5, q=7*. 因此 *n=35, z=24*.

e=5 (so *e, z* 互素).

d=29 (so *ed-1* 能够被 *z*整除).

加密：

letter	m	m^e	$c = m^e \bmod n$
l	12	1524832	17

解密：

c	c^d	$m = c^d \bmod n$	letter
17	481968572106750915091411825223071697	12	l

8.2 两类密码算法-〉公开密钥加密体系

- RSA：为什么 $m = (m^e \bmod n)^d \bmod n$

一个有用的数论定理：如果 p,q 都是素数，$n = pq$，

那么：

$$x^y \bmod n = x^{y \bmod (p-1)(q-1)} \bmod n$$

$$(m^e \bmod n)^d \bmod n = m^{ed} \bmod n$$

$$= m^{ed \bmod (p-1)(q-1)} \bmod n$$

(使用上述定理)

$$= m^1 \bmod n$$

(因为我们选择ed 使得正好被z 除余1)

$$= m$$

第8章 网络安全

8.3 数字签名

➢ 数字签名基础

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对签名；

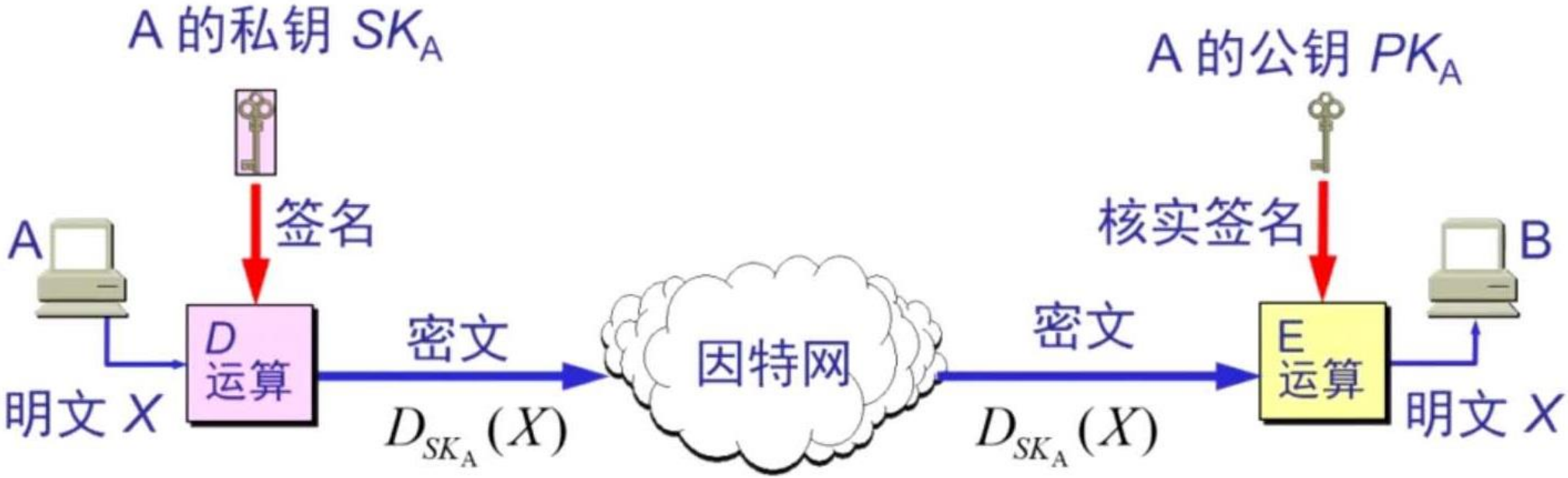
② 报文的完整性——发送者事后不能抵赖对报文的签名；

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。

8.3 数字签名

采用公钥算法的数字签名



发送方使用发送方的私钥签名，这里是D运算

接收方使用发送方的公钥加密核实签名，采用E运算，获得明文。

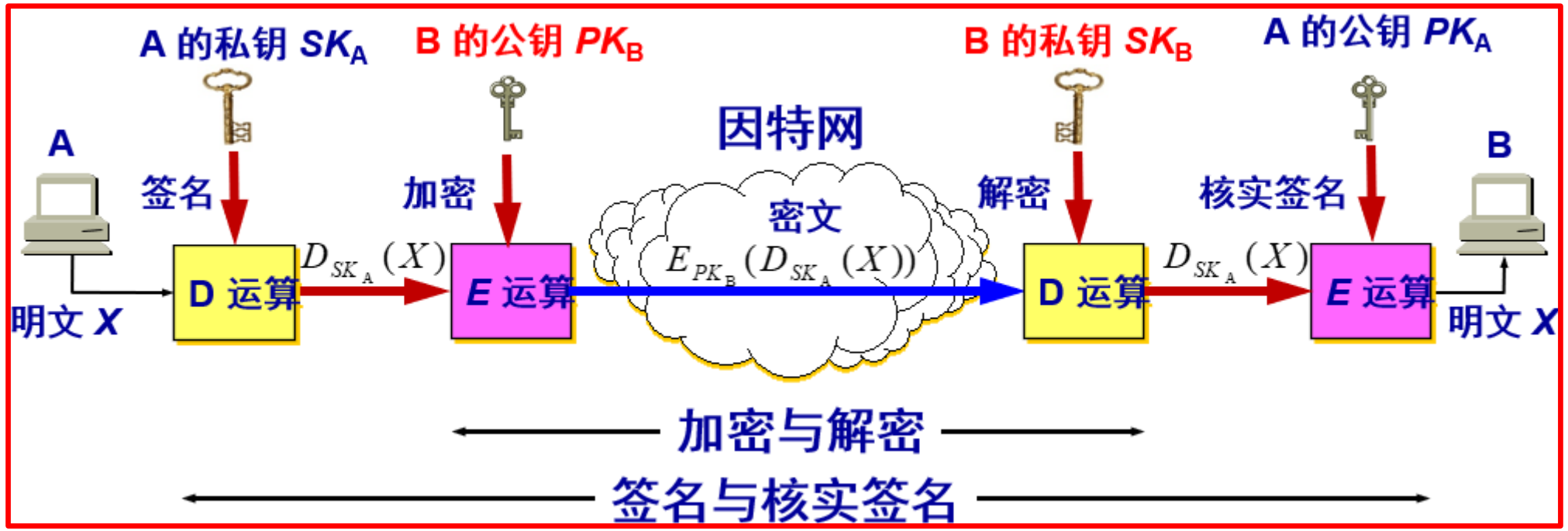
8.3 数字签名

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。---确认是A发送的
- ✓ 若A要抵赖曾发送报文给B，B可讲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。---不可抵赖
- ✓ 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B伪造了报文。---不可伪造

8.3 数字签名

具有保密性的数字签名



8.3 数字签名

➢ 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。
- ✓ 使用加密就可以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。
- ✓ 鉴别和授权（**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）

8.3 数字签名

➢ 鉴别之报文鉴别

- ✓ 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。

8.3 数字签名

➢ 鉴别之报文摘要MD

- ✓ A将报文X经过摘要算法运算后得出很短的报文摘要H。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：

1. 用A的公钥对**D(H)**进行E运算得出报文摘要H
2. 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，

   如果一样，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

8.3 数字签名

➢ 鉴别之报文摘要算法

- ✓ 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校验和。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。
- ✓ 可以很容易的计算出一个长报文X的报文摘要H，但要想从H找到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。

8.3 数字签名

- INTERNET校验和： 弱的散列函数

Internet 校验和拥有一些散列函数的特性:

- ✓ 产生报文m的固定长度的摘要 (16-bit sum)
- ✓ 多对1的

但是给定一个散列值，很容易计算出另外一个报文具有同样的散列值:

message	ASCII format
I O U 1	49 4F 55 31
0 0 . 9	30 30 2E 39
9 B O B	39 42 D2 42
	B2 C1 D2 AC

message	ASCII format
I O U 9	49 4F 55 39
0 0 . 1	30 30 2E 31
9 B O B	39 42 D2 42
	B2 C1 D2 AC

different messages but identical checksums!

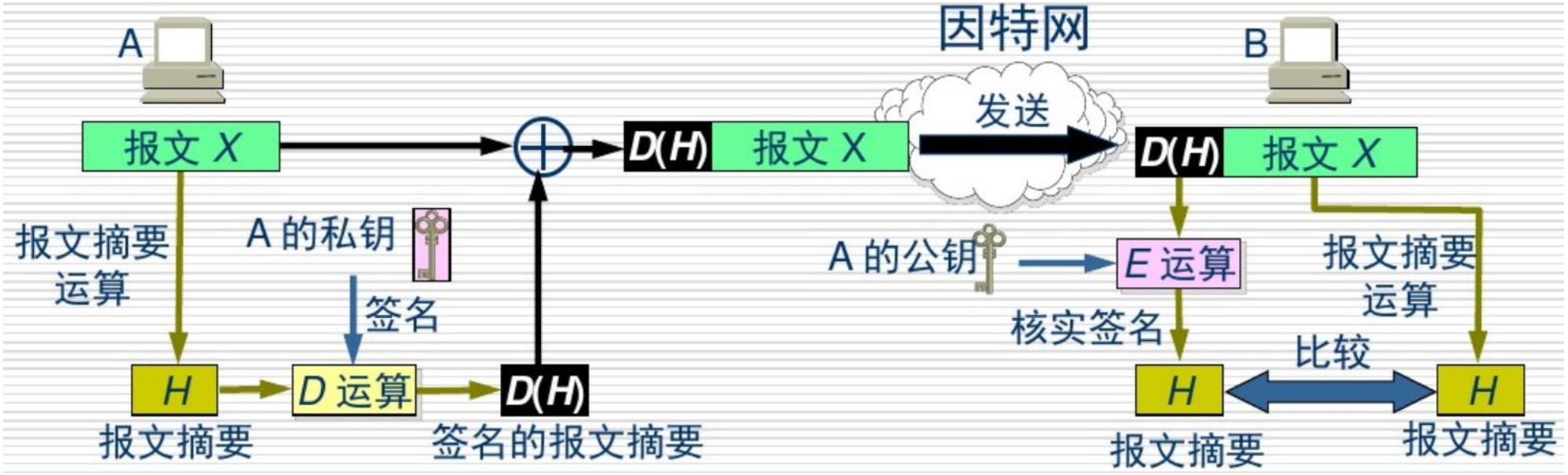
8.3 数字签名

➢ 散列函数算法

- MD5散列函数被广泛地应用 (RFC 1321)
  - 4个步骤计算出128-bit的报文摘要
  - 给定一个任意的128-bit串x, 很难构造出一个报文m 具有相同的摘要x.
- SHA-1也被使用.
  - US标准 [NIST, FIPS PUB 180-1]
  - 160-bit报文摘要

8.3 数字签名

- 鉴别之报文摘要的实现

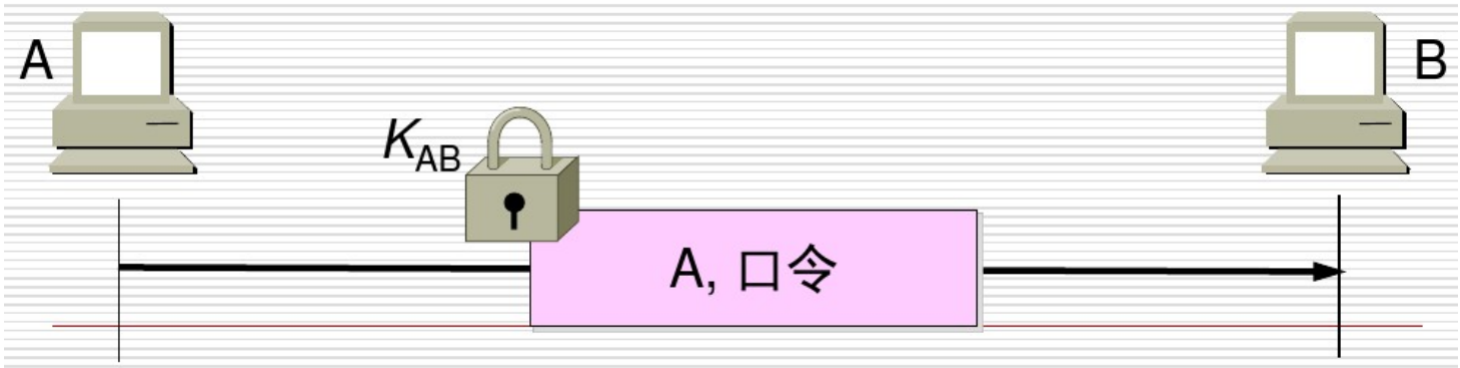


8.3 数字签名

➢ 鉴别之实体鉴别

- ✓ 实体鉴别和报文件别不同。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：

1. A发送给B的报文被加密，使用的是对称密钥K_{AB}
2. 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。



8.3 数字签名

➢ 鉴别之实体鉴别

- ✓ 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”。