计算机与网络技术

第15讲 网络安全（2）

课程回顾

- 计算机网络概述
- 物理层
- 数据链路层
- 网络层
- 运输层
- 应用层
- 网络安全

计算机网络安全概述

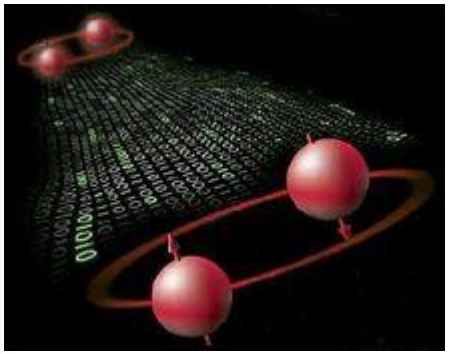
- **计算机网络安全的技术定义：**
  - 计算机系统的**硬件、软件、数据**受到保护，不因偶然或恶意的原因遭到**破坏、更改、显露**，系统能连续**正常运行，提供相应的服务**

- **公安部计算机管理监察司的定义：**
  - 指计算机资产安全，即计算机信息系统资源和信息资源不受自然和人为有害因素的威胁和危害

- **公安部网络安全保卫局**

网络信息安全技术措施

- 在物理层——通信线路上加密技术
- 在数据链路层——点对点链路加密来保障数据传输的安全性
- 在网络层——防火墙技术，IPV6认证加密
- 在传输层——TCP/UDP的安全机制-安全套接层协议(SSL、TLS)
- 在传输层以上的各层，采用更加复杂的安全手段，例如加密用户级的身份认证、数字签名技术等

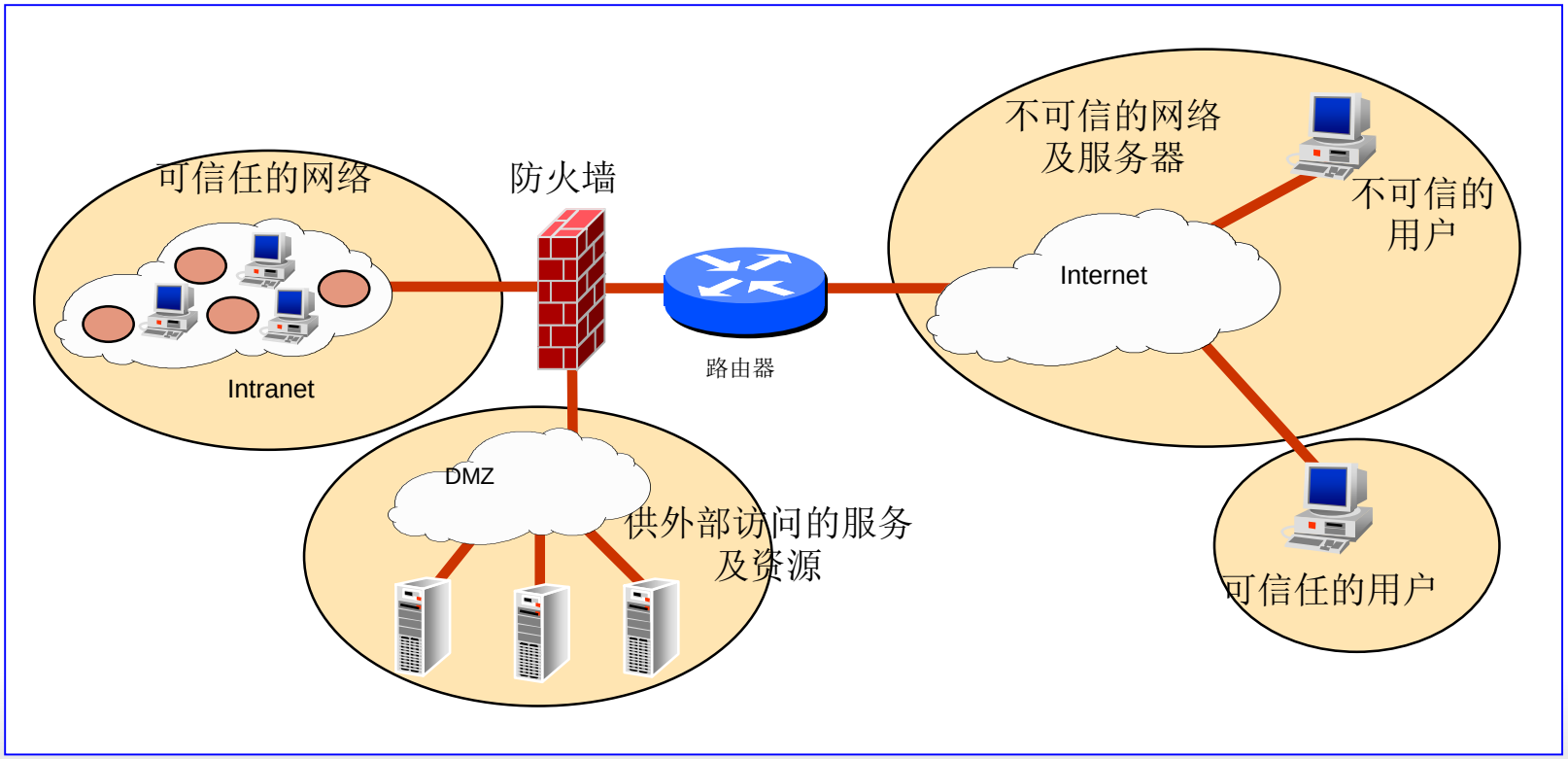


量子通讯
量子纠缠
绝对安全
超距通讯

防火墙的分类

防火墙体系

- 包过滤防火墙
- 代理防火墙（应用层网关防火墙）



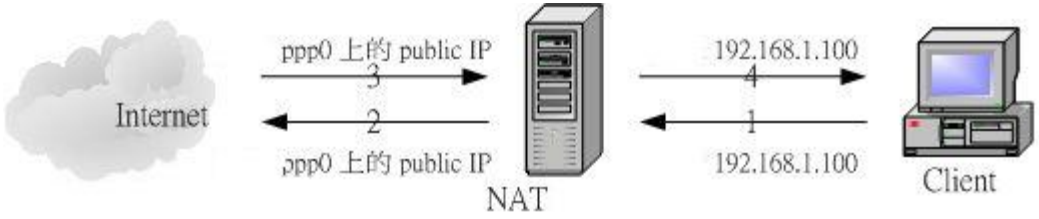
代理型防火墙：自适应代理防火墙

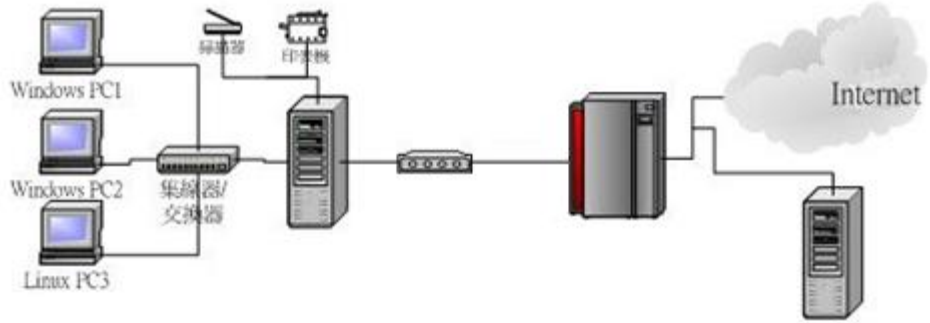
- 自适应代理技术（Adaptive proxy）结合包过滤和代理的特点，性能提高
- 组成这种类型防火墙的基本要素有两个：自适应代理服务器（Adaptive Proxy Server）与动态包过滤器（Dynamic Packet filter）。
- 在自适应代理与动态包过滤器之间存在一个控制开关。
- 自适应代理可以根据用户的配置信息，决定是使用代理服务从应用层代理请求还是从网络层转发包。

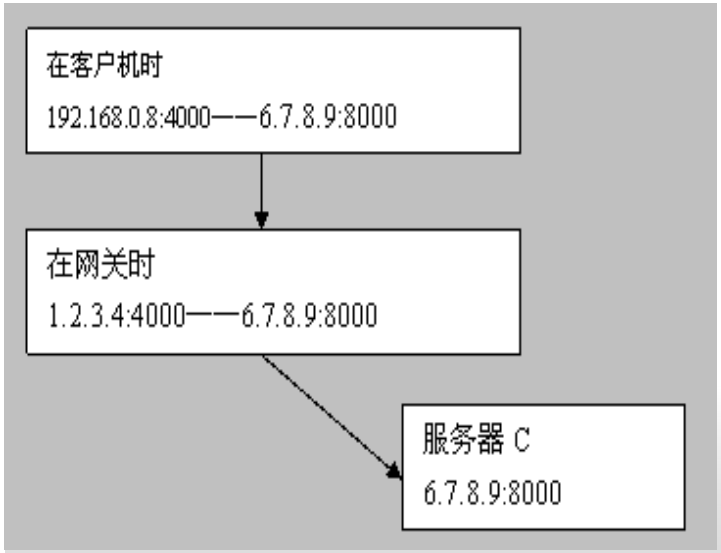
防火墙：NAT

- NAT（Network Address Translation，网络地址转换）
  - 静态地址转换
  - 动态地址转换
  - 端口多路复用

Class	范围	子网掩码
Class A	10.0.0.0 ~ 10.255.255.255	255.0.0.0
Class B	172.16.0.0 ~ 172.31.255.255	255.255.0.0
Class C	192.168.0.0 ~ 192.168.255.255	255.255.255.0







传输层安全协议

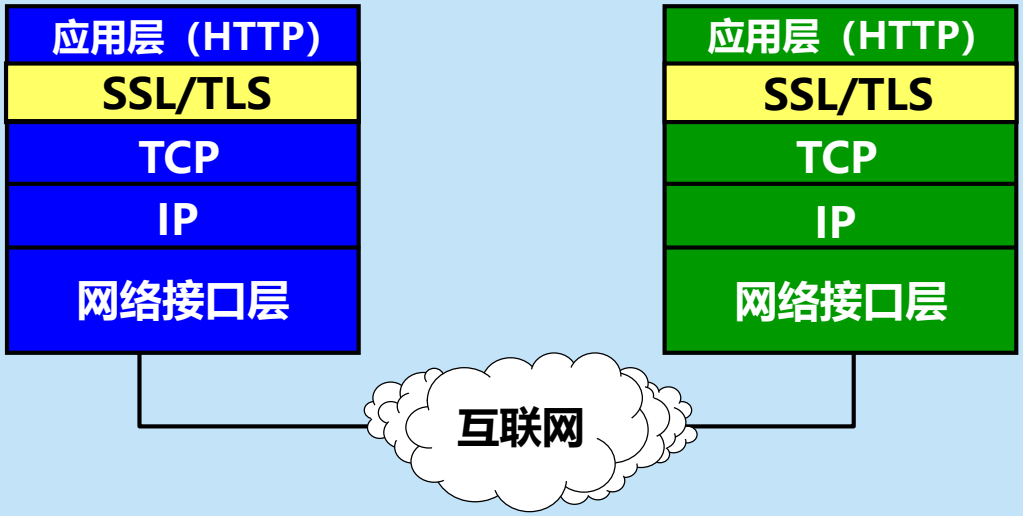
传输层安全协议

SSL 和 TLS

- 安全套接层 SSL 由 Netscape 于 1994 年开发，广泛应用于基于万维网的各种网络应用（但不限于万维网应用）。
- SSL 作用在应用层和运输层之间，在 TCP 之上建立起一个安全通道，为通过 TCP 传输的应用层数据提供安全保障。
- 1996 年发布 SSL 3.0，成为 Web 安全的事实标准。
- 1999 年，IETF 在 SSL 3.0 基础上推出了传输层安全标准 TLS，为所有基于 TCP 的网络应用提供安全数据传输服务。

传输层安全协议

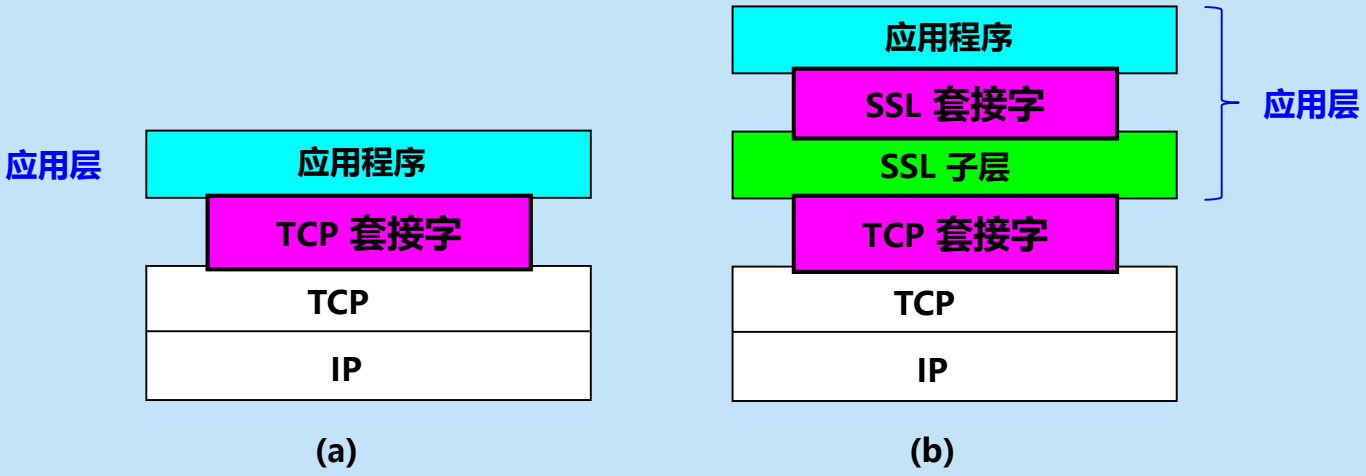
SSL / TLS 的位置



在发送方，SSL 接收应用层的数据，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。

传输层安全协议

传输层不使用安全协议和使用安全协议的对比



- SSL / TLS 建立在可靠的 TCP 之上，与应用层协议独立无关。
- SSL / TLS 已被所有常用的浏览器和万维网服务器所支持。
- SSL / TLS 基本目标：实现两个应用实体之间的安全可靠通信。

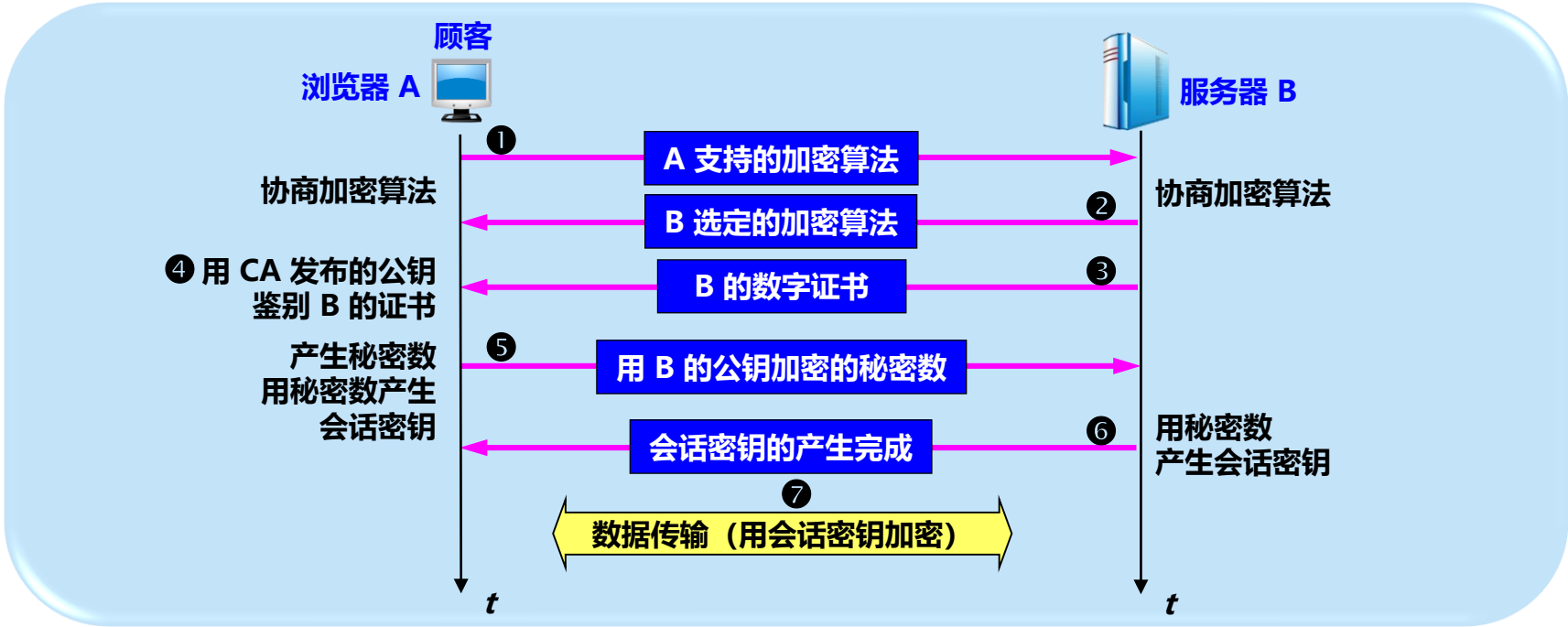
传输层安全协议

SSL 和 TLS

- 应用层使用 SSL 最多的就是 HTTP，但 SSL 并非仅用于 HTTP，而是可用于任何应用层的协议。
- 应用程序 HTTP 调用 SSL 对整个网页进行加密时，网页上会提示用户，在网址栏原来显示 http 的地方，现在变成了 https。在 http 后面加上的 s 代表 security，表明现在使用的是提供安全服务的 HTTP 协议（TCP 的 HTTPS 端口号是 443，而不是平时使用的端口号 80）。

传输层安全协议

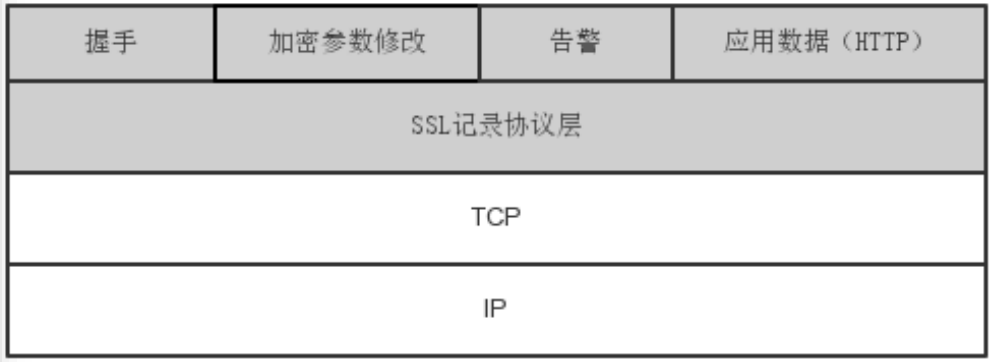
SSL 安全会话建立过程



加密技术

网络信息安全技术措施

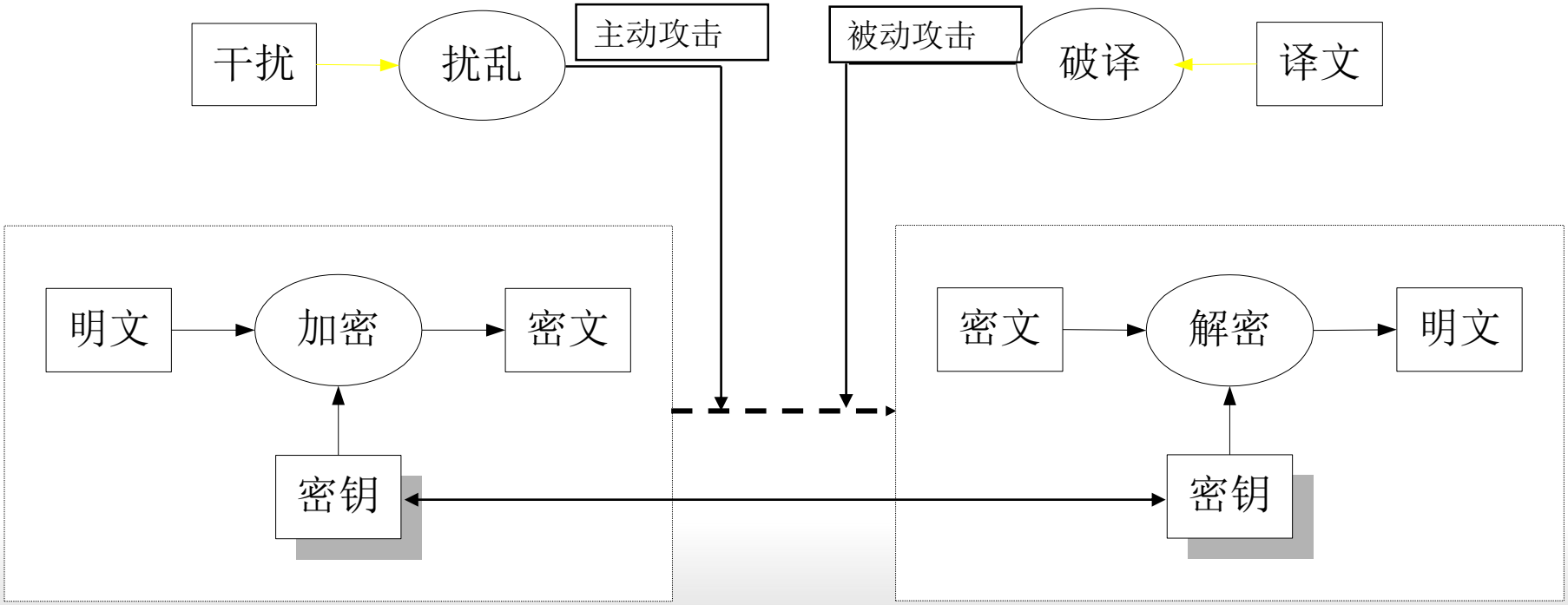
- 在物理层——通信线路上加密技术
- 在数据链路层——点对点链路加密来保障数据传输的安全性
- 在网络层——防火墙技术，IPV6认证加密
- 在传输层——TCP/UDP的安全机制-安全套接层协议(SSL)
- 在传输层以上的各层，采用更加复杂的安全手段，例如加密用户级的身份认证、数字签名技术等



TCP/IP协议栈中的安全机制

保密系统模型

- 机密性：数据传输过程中，不能被非授权者偷看
- 完整性：数据传输过程中，不能被非法篡改
- 有效性：数据不能被否认



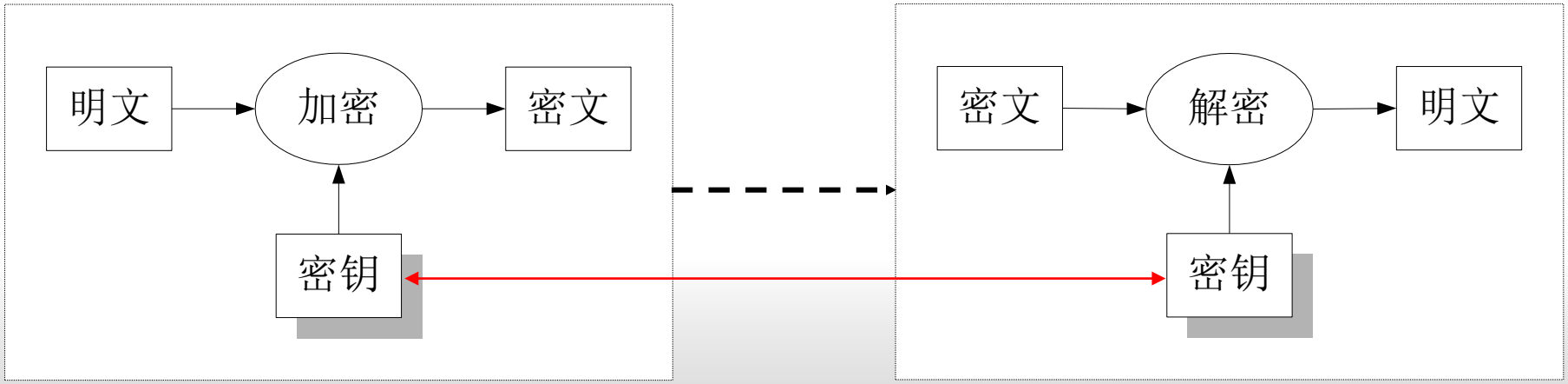
网络信息加密方法（传统）

- **密码算法**
  - **传统密码算法**
    - **对称密码算法(Symmetric Cryptographic Algorithms)**
      - **E=encrypt (K , M)**
      - **M =decrypt(K, E)**
        =decrypt (encrypt (K , M))
- **密钥(key)的概念**
  - **密钥是一个数值,它和加密算法一起生成特别的密文**
  - **密钥的尺寸用位(bit)来衡量，在公开密钥加密方法中,密钥的尺寸越大,密文就越安全**

E=M+1　　M=E-1

网络信息加密方法（传统）

- **传统的加密方法**
  - 密钥管理和加密方法
  - 优势
    - 速度快
    - 加密强度大
  - 不足
    - 安全地发布密钥非常困难

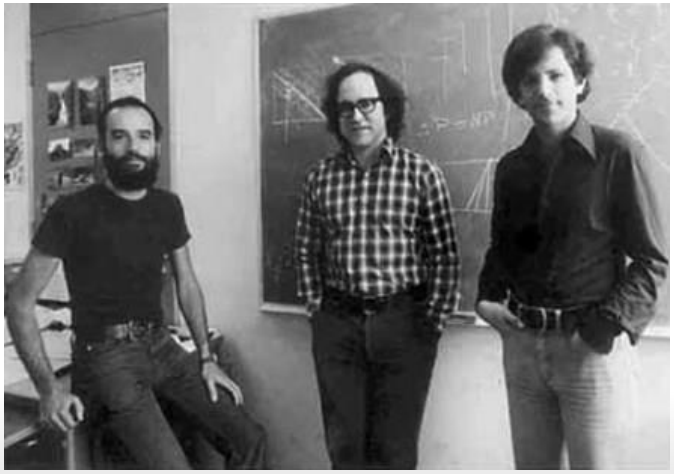


网络信息加密方法（现代）

- **密码算法**
  - **现代密码算法**
    - **非对称密码算法或公钥密码算法**
    - **Public-Key Cryptographic Algorithms**

      –M=decrypt (prv-ul, encrypt (pub-ul, M))

    - **只需公开其加密密钥(称公钥）即可，实体之间可以进行秘密通信**
    - **RSA、Elgamal、背包算法、Rabin、D-H、ECC（椭圆曲线加密算法）**



RSA公钥加密算法
1977年
罗纳德·李维斯特（Ron Rivest）
阿迪·萨莫尔（Adi Shamir）
伦纳德·阿德曼（Leonard Adleman）

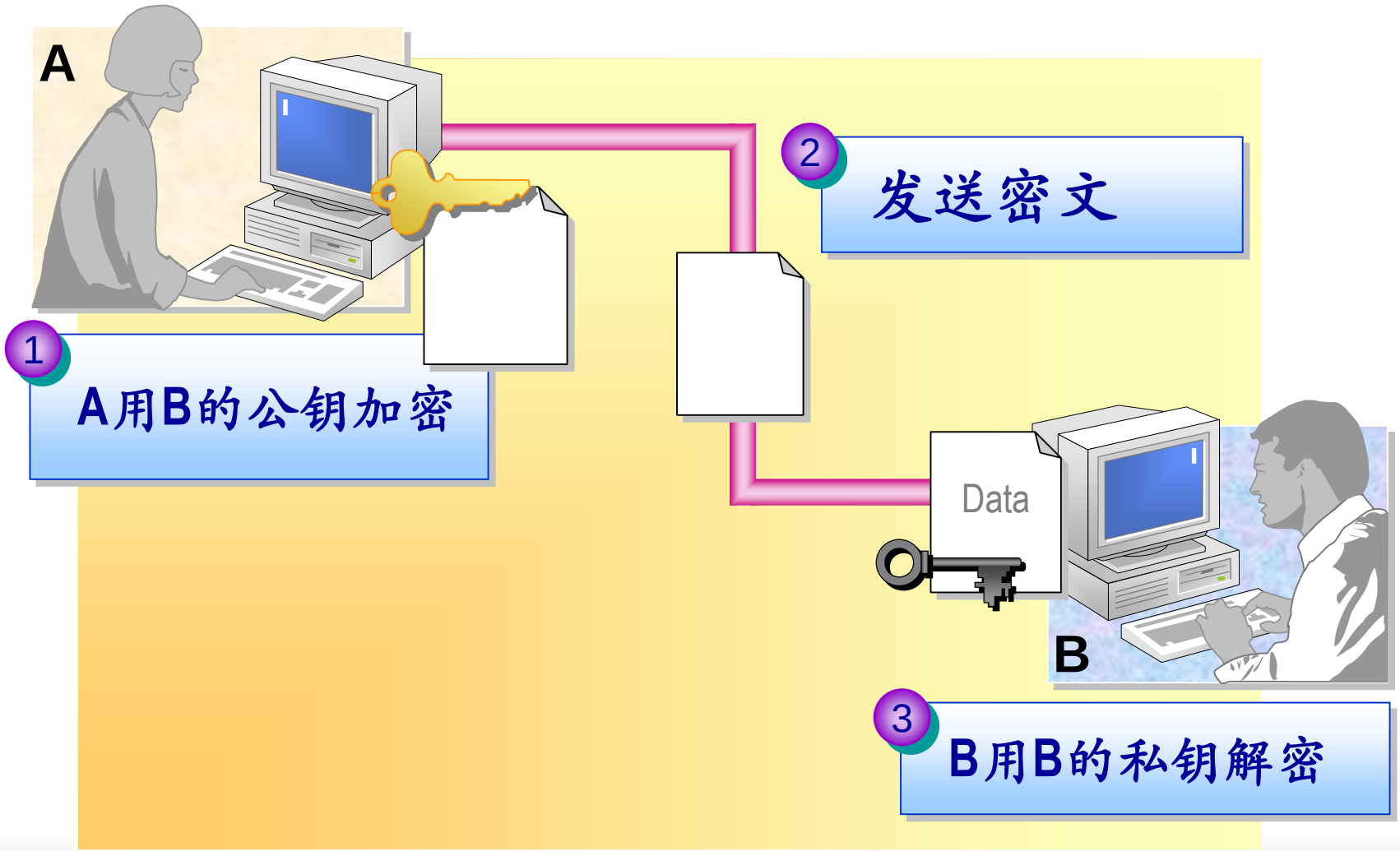
网络信息加密方法（现代）

- **RSA-1977**
  - **n、e1、e2**
    - **n是两个大质数p、q的积，n的二进制表示时所占用的位数，就是所谓的密钥长度**
    - **e1与(p-1）*(q-1）互质**
    - **（e2*e1）mod((p-1）*(q-1））=1**
  - **（n，e1）,(n，e2）就是密钥对**
    - **(n，e1）为公钥**
    - **(n，e2）为私钥**
  - **RSA加解密的算法完全相同，设A为明文，B为密文**
    - **B=A^e1 mod n**
    - **A=B^e2 mod n**
  - **e1和e2可以互换使用**
    - **B=A^e2 mod n**
    - **A=B^e1 mod n**

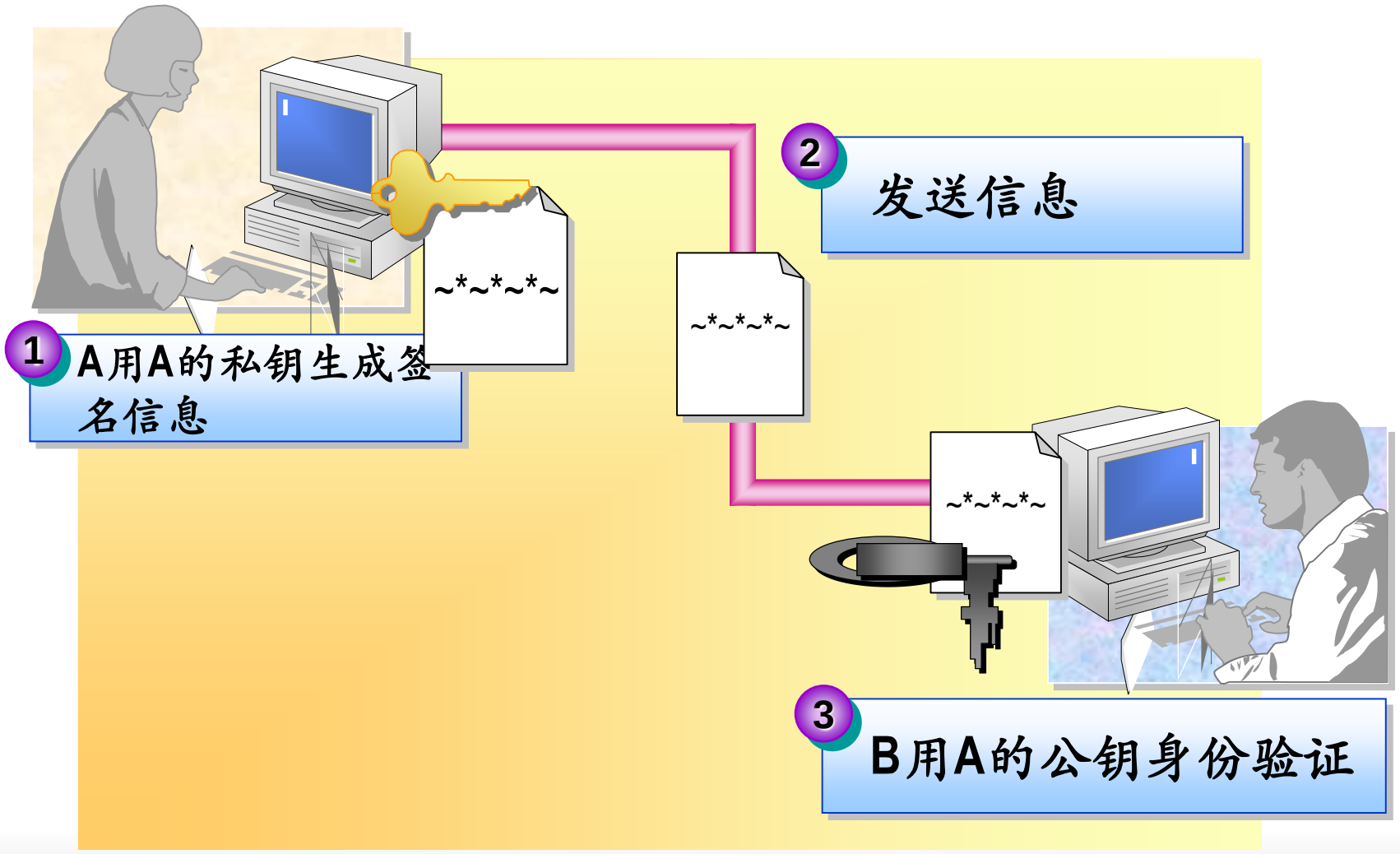
网络信息加密方法（现代）

- **公开密钥加密法**
  - 公开密钥加密法可以解决密钥发布的问题
  - 可以让事先没有安全通道的人安全地交换信息
  - 用加密算法生成两个密钥，分别作为公钥和私钥
  - 公钥密钥算法
    - 公钥密钥:利用数学算法生成的一对数据
    - 经过任一密钥加密后，相互之间可以解密
    - 相互之间不可以互推得到对方
- **现代加密技术主要应用**
  - **公钥加密，私钥解密：可以进行加密通信**
  - **私钥加密，公钥解密：可以进行身份验证（来源）和无可抵赖性验证**
  - **Hash验证：断定未被篡改（一般还要加上密钥加密技术）**

公钥加密



公钥认证



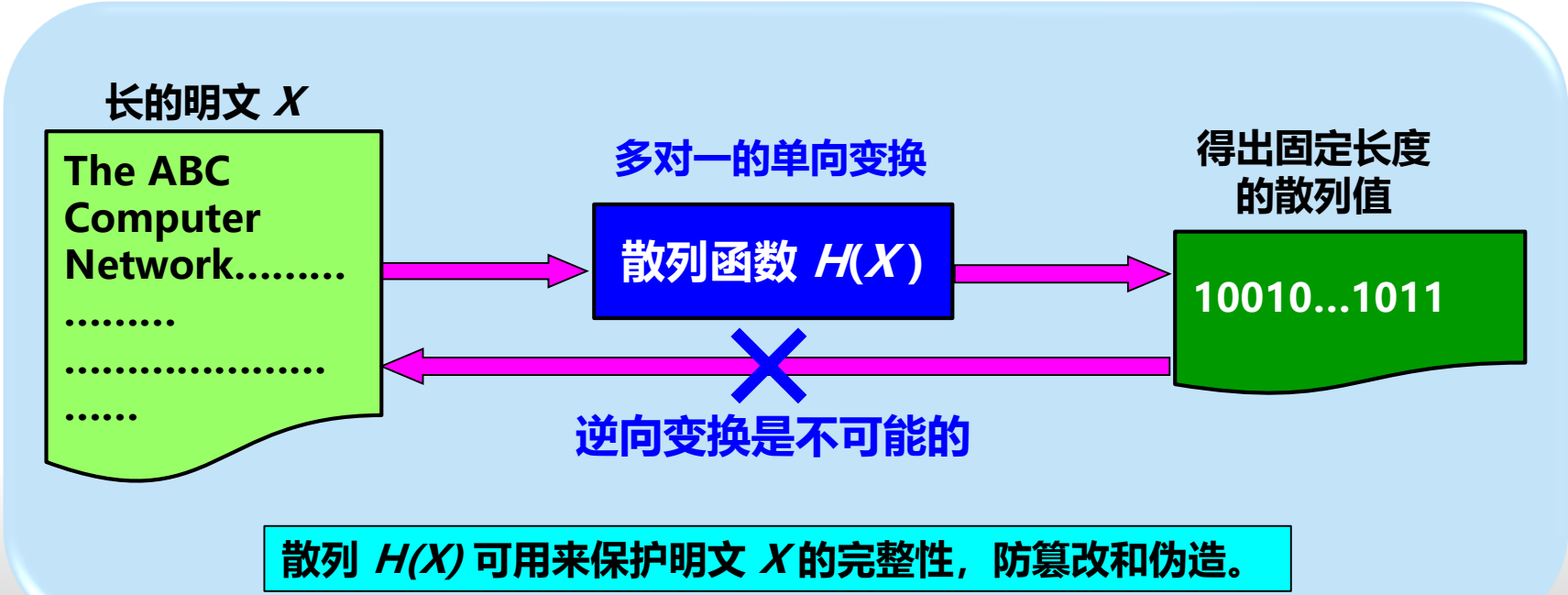
网络信息加密方法：加密强度

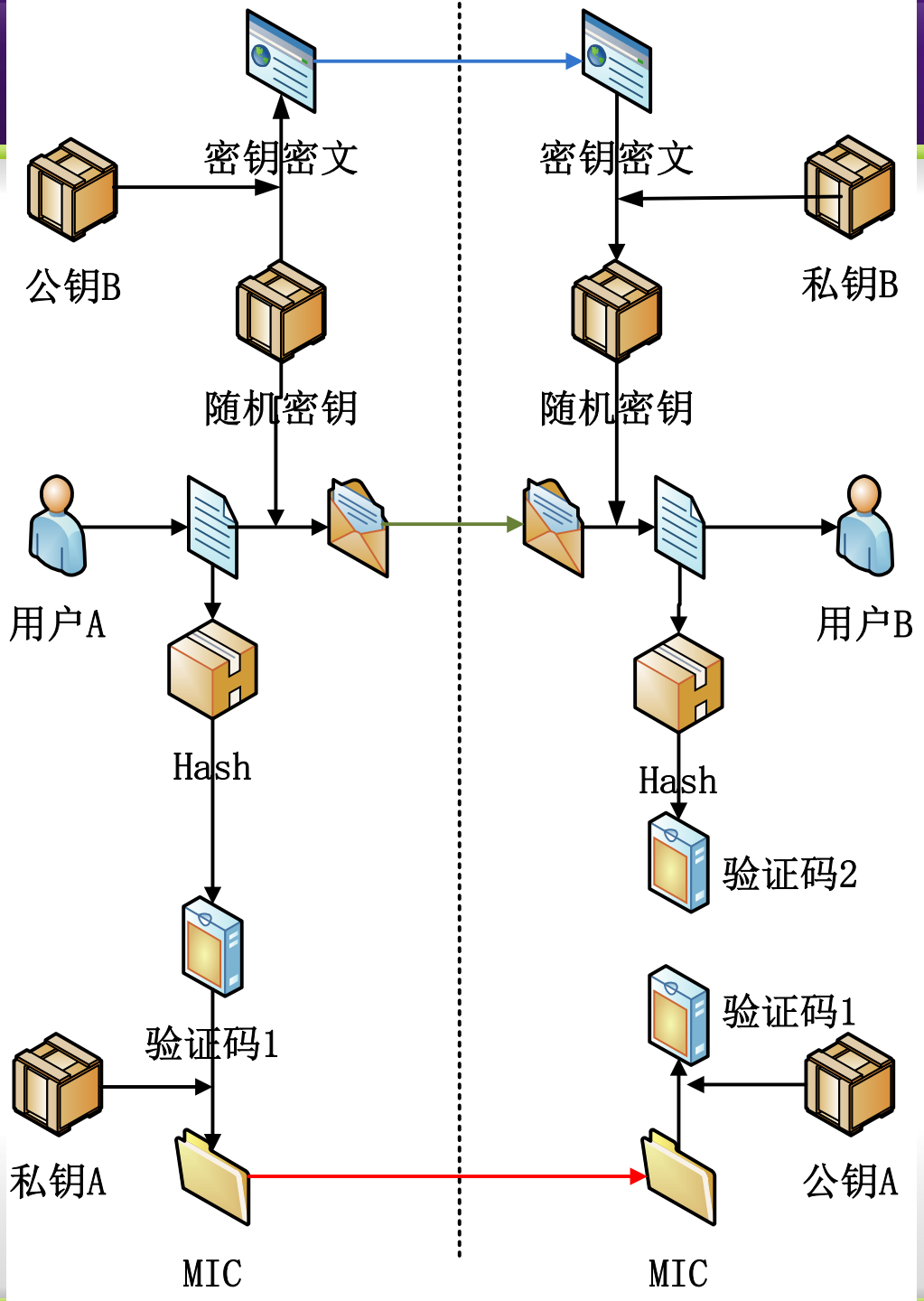
- **传统和现代密钥加密强度**
  - **公钥的尺寸和传统加密方法中密钥的尺寸是不相关的**
  - **传统80位密钥的强度等同于1024位的公钥**
  - **传统128位密钥的强度等同于3000位的公钥**

保密级别	对称密钥长度（bit）	RSA密钥长度（bit）
80	80	1024
112	112	2048
128	128	3072
192	192	7680
256	256	15360

网络信息加密方法：数据完整性

- 安全散列算法（Secure Hash Algorithm）SHA
  - 一种规范，将报文生成验证值，消息摘要：
    - 单向函数，不可逆运算；
      - 难以对指定的验证值生成一个报文,由该报文可以得出指定的验证值;
      - 难以生成两个不同的报文具有相同的验证值。
    - Hash函数可以接受可变长度的输入
      - 输入可以是任意长的消息,其产生固定长度的输出
    - Hash函数保证：敏感性好，可以很好标识出信息变化
    - MD5 (tanajiya.tar.gz) = 38b8c2c1093dd0fec383a9d9ac940515



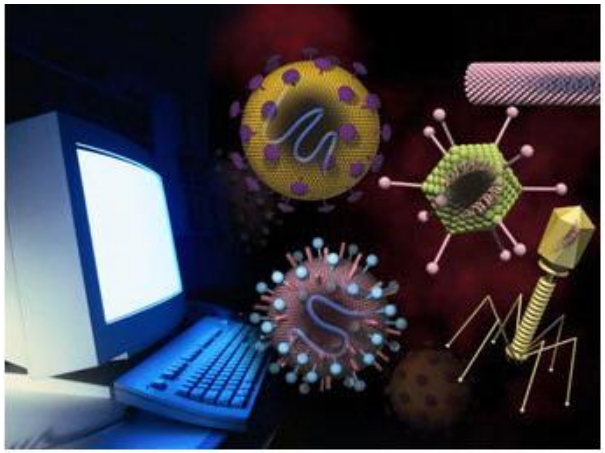

密钥密文
密钥密文
公钥B
私钥B
随机密钥
随机密钥
用户A
用户B
Hash
Hash
验证码2
验证码1
验证码1
私钥A
公钥A
MIC
MIC

计算机病毒及防护

计算机病毒

病毒

- 是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码-《中华人民共和国计算机信息系统安全保护条例》
- 1983 佛瑞德·科恩(Fred Cohen)，提出了“计算机病毒”(Computer Virus)的概念



计算机病毒特点-被创造的

- 非授权性
- 破坏性
- 隐蔽性
- 潜伏性
- 可触发性
- 传染性
- 不可预见性-进化

计算机病毒

- 计算机病毒的分类
  - 根据系统区分
    - DOS、UNIX、Windows
  - 寄生方式
    - 引导区、文件型、网络型、混合型
  - 破坏能力
    - 无害、无危险、危险、非常危险
- 传播途径
  - 软盘
  - 光盘
  - U盘
  - 网络

计算机病毒

计算机病毒的命名方式

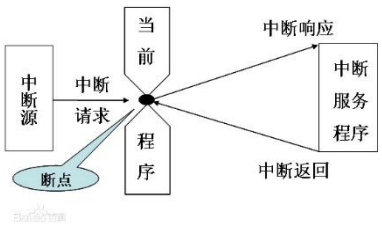
- <病毒前缀>.<病毒名>.<病毒后缀>
- 病毒前缀——类型
  - 危害系统——Win32、PE、Win95、W32、W95
  - 蠕虫病毒——Worm
  - 木马病毒、黑客病毒——Trojan、Hack
  - 宏病毒——宏病毒的前缀是：Macro，第二前缀是：Word、Word97、Excel、Excel97
  - 脚本病毒——Script、VBS、JS
  - 密码病毒——PSW
  - 后门病毒——Backdoor
  - 病毒种植程序病毒——Dropper
  - 破坏性程序病毒——Harm
  - 玩笑病毒——Joke
- 后缀——变种

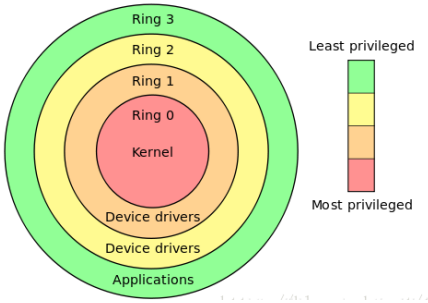
Win95.CIH.V1.2
Trojan.LMir.PSW.60
新冠病毒奥密克戎BQ.1.1

计算机病毒

□ 最有影响力的病毒

- Creeper
  - 第一个计算机病毒
  - 在1971年由Bob Thomas使用Tenex操作系统制作





Win95.CIH.V1.2

+ CIH
  - × 1998年6月爆发于中国台湾，是一位名叫陈盈豪的台湾大学生所编写，是公认的有史以来危险程度最高、破坏强度最大的病毒之一
  - × 4月26日爆发，切尔诺贝利病毒
  - × 破坏硬盘数据、覆盖BIOS
  - × 1003字节

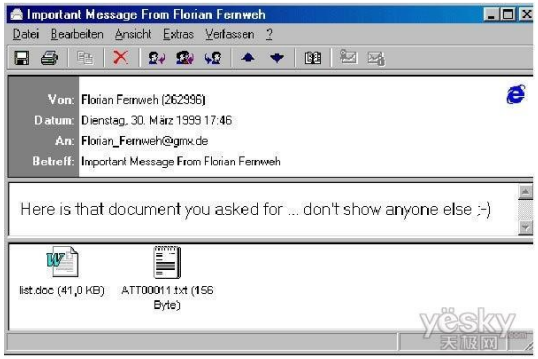
计算机病毒

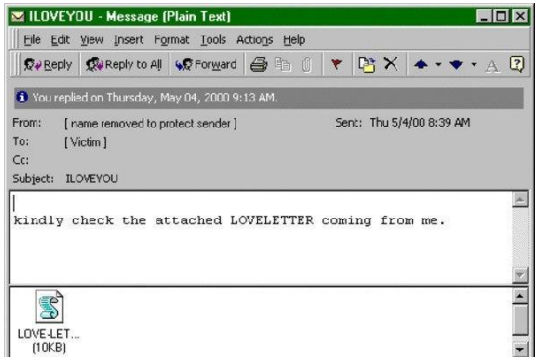
- 最有影响力的病毒
  - 熊猫烧香
    - 2006年底
    - 感染型的蠕虫病毒
    - 感染系统中exe，com，pif，src，html，asp等文件
    - 中止大量的反病毒软件进程并且会删除扩展名为gho的文件
    - 作者-李俊-成为中国第一批因制造电脑病毒获刑的人
  - 勒索病毒WannaCry
    - 2017年5月12日爆发
    - 150个国家、30万名用户中招，造成损失达80亿美元
    - 445端口
    - 加密技术、区块链
    - 大中华圈、NSA

Worm.WhBoy.cw

计算机病毒

- **最有影响力的病毒**
  - 我爱你(ILOVEYOU)
    - 损失估计：全球约100亿~150亿美元
    - 2000年5月3日，“我爱你”蠕虫病毒首次在香港被发现
    - Visual Basic脚本，邮件传播
  - 梅利莎(Melissa)
    - 1999年3月26日爆发
    - Word宏脚本病毒
  - 尼姆达（Nimda）
    - 历史上传播速度最快的病毒之一，在上线之后的22分钟之后就成为传播最广的病毒
    - 攻击服务器
  - 红色代码(Code Red)
    - 计算机蠕虫病毒，能够通过网络服务器和互联网进行传播
    - 2001年7月13日，红色代码从网络服务器上传播开来，窃取数据
  - SQL Slammer
    - 2003年1月25日首次出现
    - 蠕虫病毒，给互联网的流量造成了显而易见的负面影响，Dos，针对SQL Server
  - MyDoom
    - 2004年1月26日爆发
    - 高峰期全球互联网的速度性能下降了10%，网页的下载时间增加了50%。





计算机反病毒软件

软件结构

- 病毒库-抗药性、变种
- 扫描器
- 虚拟机

病毒检测方法

- 特征代码法
  - 检测已知病毒的最简单、开销最小的方法
  - 在病毒样本中，抽取特征代码
  - **WHboy、5E CC 56 8B F0,CIH**
- 校验和法
  - 定期地或每次使用文件前，检查文件现在内容算出的校验和与原来保存的校验和是否一致，因而可以发现文件是否感染，这种方法叫校验和法，它既可发现已知病毒又可发现未知病毒

计算机反病毒软件

病毒检测方法

- 行为监测法
  - 利用病毒的特有行为特征性来监测病毒的方法
- 软件模拟法
  - 先使用特征代码法发现病毒，启动软件模拟模块，待病毒密码破译后，用特征码法识别并杀毒

常用杀毒软件

- 江民
  - KV系列
- Norton，Symantec
  - 嵌入系统很深
- Kaspersky
  - 卡巴和瑞星在监控时的资源占用问题比较突出
- Kingsoft金山

计算机与网络技术

课程期末安排

期末考试初步安排

- 考试时间：2025-06-10(周二) 9:00~11:00
- 考试地点：五教-5104、5105
- 考试方式：开卷考试
  - 可携带《计算机组成原理》、《计算机网络》两本教材
  - 可携带 1 张A4纸的复习笔记

期末考试初步安排

- 考试范围：课堂讲义，两本教材中讲授过的内容，实验环节内容
- 考试题型：简答、综合分析等
- 答疑时间：2025-06-08 (周日)下午14:00~17:00，地点待网络学堂/雨课堂通知

期末考试范围

课次	主题	主要知识点	教材章节
1	计算机系统概述	摩尔定律 计算机发展简史 计算机分类特点 计算机基本定义、组成 计算机相关名词概念	《~原理》 1.1、1.2、1.3、 1.5、1.6
2	计算机工作流程、 指令系统	程序创建执行过程 CPU微观工作流程 计算机宏观工作流程 指令系统定义、指令格式 MIPS指令设计与实现	《~原理》 6.1~6.7、 7.1、7.2、7.4、 7.5、7.7
3	指令系统（续）、 逻辑电路模块	寻址方式 运算器（ALU） 多路开关、译码器 寄存器、指令指针与取指单元	《~原理》 7.3、4.5、4.6、 4.7、4.8、5.2、 5.4.1

期末考试范围

课次	主题	主要知识点	教材章节
4	简易CPU设计	系统指令数据通路设计 系统指令控制逻辑设计 系统指令数据通路与控制逻辑集成	《~原理》 8.1~8.4、8.6
5	简易CPU设计(续）、CPU性能	CPU时序分析、CPU指令周期、流水线、并行计算 计算机性能评价与提升（CPU参数、缓存、运算器）、指令系统分类（CISC、RISC）	《~原理》 1.4、8.7~8.8、10.1~10.5、7.6
6	存储系统	存储系统层次设计、常用内存单元类型、内存单元总线连接、外部辅助存储单元、计算机的虚拟内存	《~原理》 11.1~11.7

期末考试范围

课次	主题	主要知识点	教材章节
7	总线、I/O、中断	总线定义及作用 总线分类与演进 总线的工作原理 I/O接口概述 I/O接口实现 数据传送方式 中断概述、关键问题 中断程序结构	《~原理》 12.1~12.3、 12.4.1~12.4.4、 13.1~13.6
8	计算机网络概述	计算机网络基本概念 互联网基本概念 互联网组成及工作模式 计算机网络体系结构（分层传输） 计算机网络协议概念 计算机网络性能指标	《~网络》 1.1~1.7

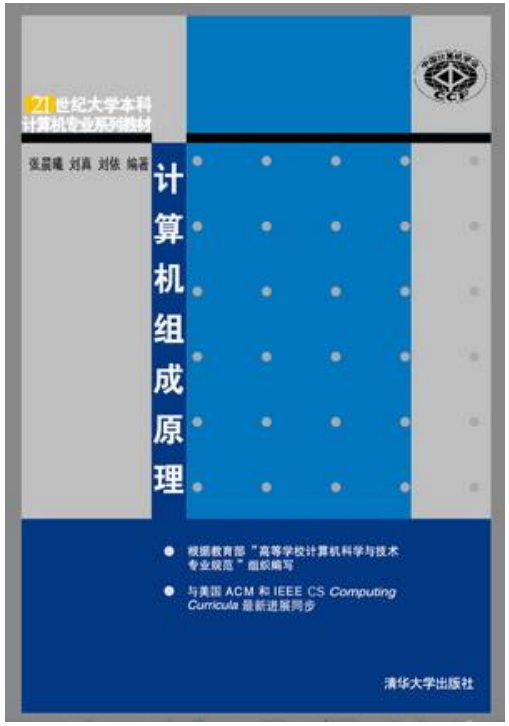
期末考试范围

课次	主题	主要知识点	教材章节
9	物理层、数据链路层	物理层基本概念、传输媒体 数据链路层基本概念 网络适配器及其MAC地址 数据链路层信道 集线器、交换机	《~网络》 2.1、2.2、2.3、2.4、2.5、3.1、3.3、3.4、3.5
10	网络层	IP协议及地址、ARP协议 路由器、IP数据报 子网掩码、IPv6 网络地址转换NAT ICMP报文及应用	《~网络》 4.1、4.2、4.3.1、4.4、4.5.1-3、4.8.2
11	运输层	运输层协议概述 运输层端口 用户数据报协议UDP 传输控制协议TCP	《~网络》 5.1~5.9

期末考试范围

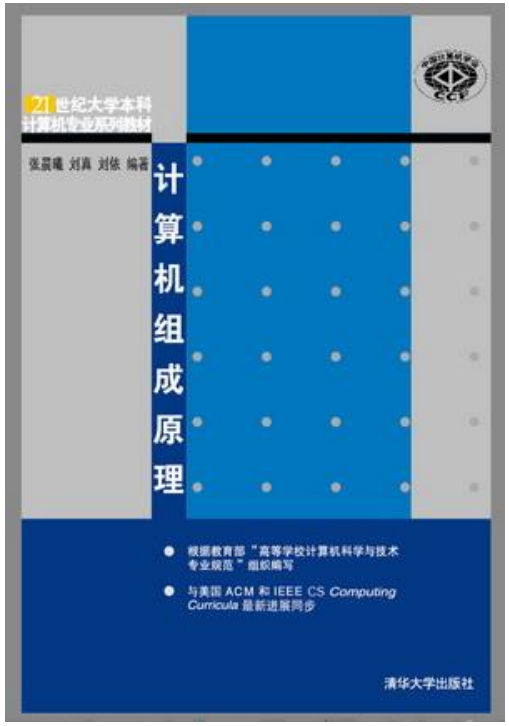
课次	主题	主要知识点	教材章节
12	应用层及 网络服务	域名系统DNS 文件传输协议FTP 万维网WWW 电子邮件	《~网络》 6.1-6.6
13~ 14	网络安全 移动网络	云平台概要 网络安全问题概述 网络安全防护方法 互联网安全协议 移动网络	《~网络》 7.1~7.6、9.3

期末考试范围



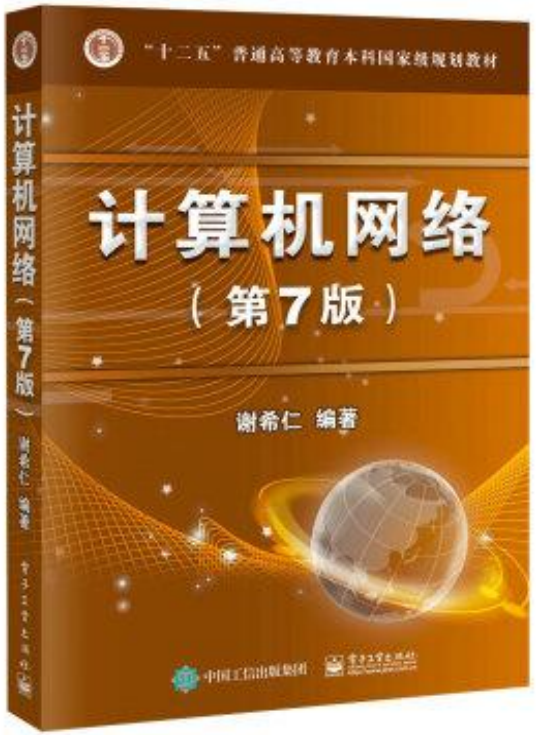
- 第1章：全部
- 第4章：4.5、4.6、4.7、4.8
- 第5章：5.2、5.4.1
- 第6章：全部
- 第7章：全部
- 第8章：全部
- 第10章：全部
- 第11章：全部
- 第12章：12.1~12.3、12.4.1~12.4.4、12.4.7、12.4.9
- 第13章：全部

期末考试范围



- 第1章：全部
- 第4章：4.5、4.6、4.7、4.8
- 第5章：5.2、5.4.1
- 第6章：全部
- 第7章：全部
- 第8章：全部
- 第10章：全部
- 第11章：全部
- 第12章：12.1~12.3、12.4.1~12.4.4、12.4.7、12.4.9
- 第13章：全部

期末考试范围



- 第1章：全部
- 第2章：2.1、2.3、2.4、2.5
- 第3章：3.1、3.3、3.4、3.5
- 第4章：4.1、4.2、4.3.1、~~4.4~~、4.5.1~4.5.3、4.8.2
- 第5章： 5.1~5.9
- 第6章： 6.1~6.6、6.9
- 第7章： 7.1~7.6
- 第9章： 9. 3

谢 谢

请不要将课件上传到公共网络平台上~~