计算机网络及应用

Computer Networks and Applications

第八章　网络安全

密码学的原则、报文完整性和认证、安全电子邮件、传输层安全性TCP与TLS、网络层安全性IPsec

主讲：清华大学　贾庆山

教材：J.F. Kurose, K.W. Ross，Computer Networking: A Top-Down Approach, Addison Wiley, 7th Edition, 2017（机械工业出版社中文版，2018）

Special thanks to Prof. Kurose and Prof. Ross for presentation material

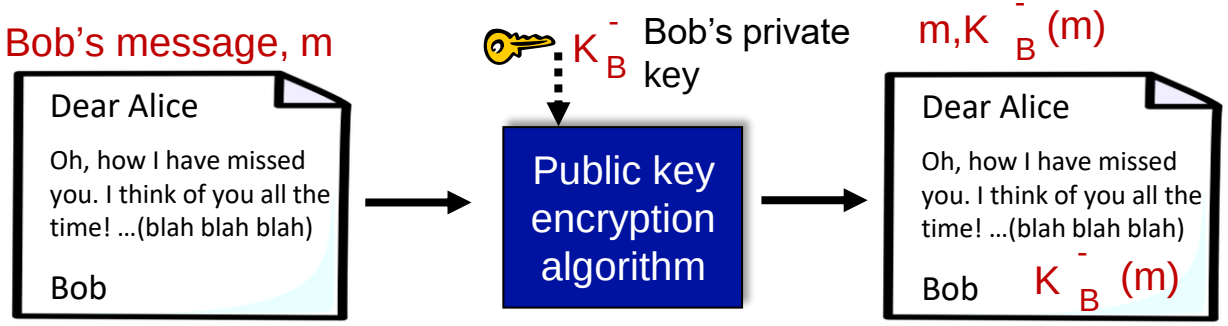
提纲

- 什么是网络安全？
- 密码学的原则
- **身份验证，报文完整性**
- 安全电子邮件
- 传输层安全性：TCP与TLS
- 网络层安全性：IPsec
- 无线网络和移动网络安全
- 运行安全性：防火墙和入侵检测系统IDS

数字签名

类似于手写签名的密码技术:

- 发送方(Bob)对文档进行数字签名:他是文档所有者/创建者
- *可验证，不可伪造：*接收方（Alice）可以证明，只有Bob能够对文件进行签名，而不是其他人，包括Alice在内。
- 对于信息m的简单数字签名:
  - Bob通过他的私钥K_B^-对消息m进行加密，创建 “已经签名的”报文，$K_B^-(m)$



数字签名

- 假设Alice收到消息m，签名为:m, $K_B^-(m)$
- Alice对Bob已经签名的m进行验证，方法是通过使用Bob's 的公钥 K_B^+ 检查 $K_B^-(m)$ ，判断$K_B^+(K_B^-(m))$ 是否等于 m.
- 如果 $K_B^+(K_B^-(m)) = m$, 那么对m进行签名的人 一定用了Bob的私钥。

Alice 从而验证:

- Bob对m进行了签名
- 其他人没有对m进行签名
- Bob对m而不是m'进行了签名

不可否认性:

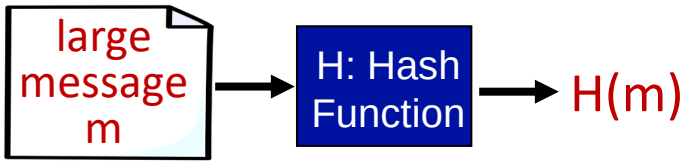
✓ Alice 可以将m和签名后的 $K_B^-(m)$ 去法院 证明Bob对m进行了签名

数字签名

用公共密钥加密长消息的计算成本很高

目标: 生成固定长度、便于计算的数字 “指纹”

- 将哈希函数H应用于*m*, 获取固定大小的信息摘要, *H(m)*



哈希函数的特性:

- 多对一(many-to-1)
- 生成固定长度的信息摘要(指纹)
- 给定信息摘要*x*, 无法通过计算得到*m* 使得*x = H(m)*

互联网校验和: 糟糕的哈希加密函数

互联网校验和具有哈希函数的一些属性:

- 生成消息的固定长度摘要(16位校验)
- 多对一(many-to-one)

但是对于具有给定哈希值的消息，很容易找到具有相同哈希值的另一条消息:

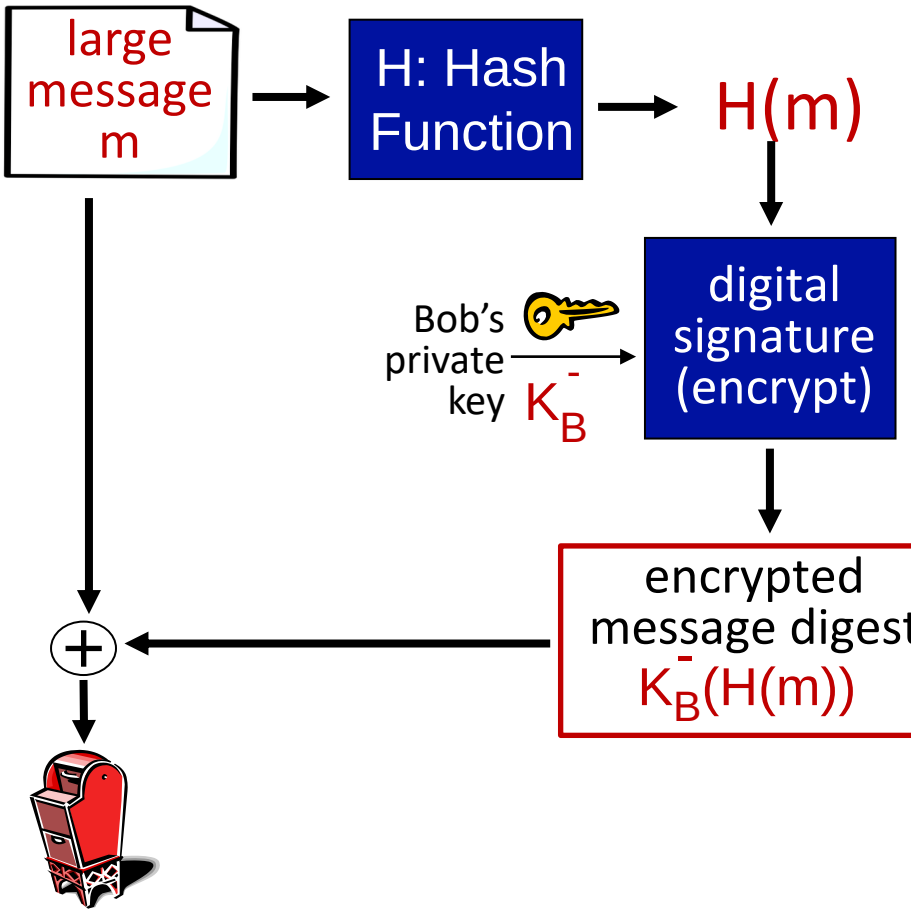
message	ASCII format
I O U 1	49 4F 55 31
0 0 . 9	30 30 2E 39
9 B O B	39 42 D2 42
	B2 C1 D2 AC

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

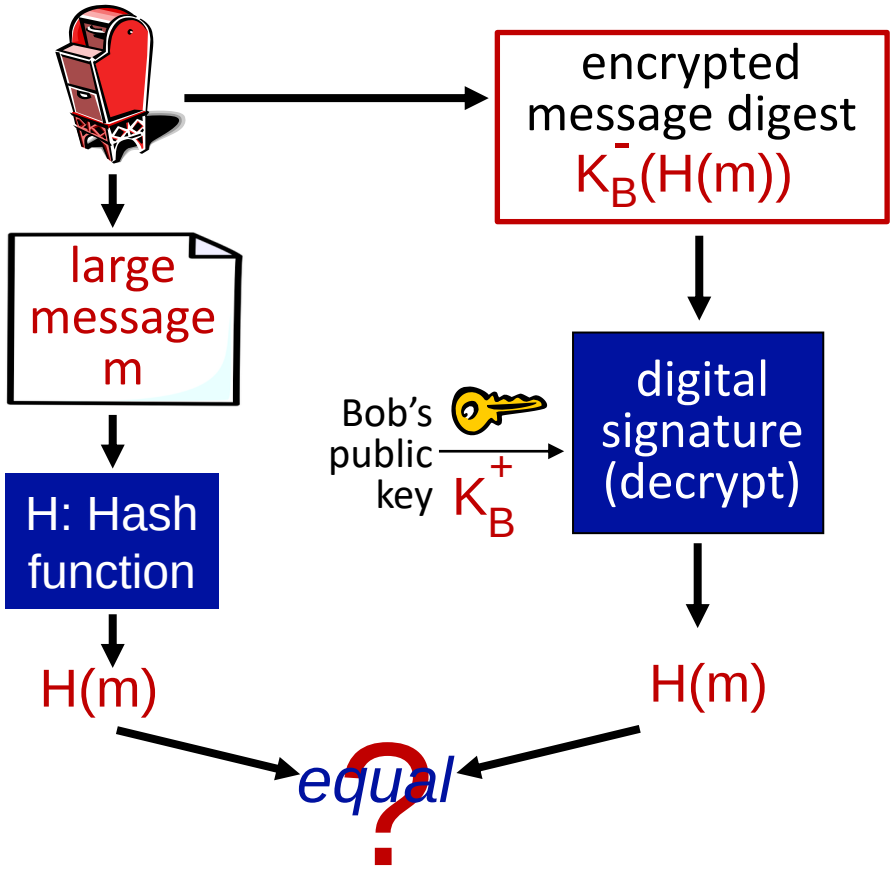
不同的信息
但是校验和相同!

数字签名=经过签名的消息摘要

Bob发送进行了数字签名的消息:



Alice验证签名，确定数字签名信息的完整性:

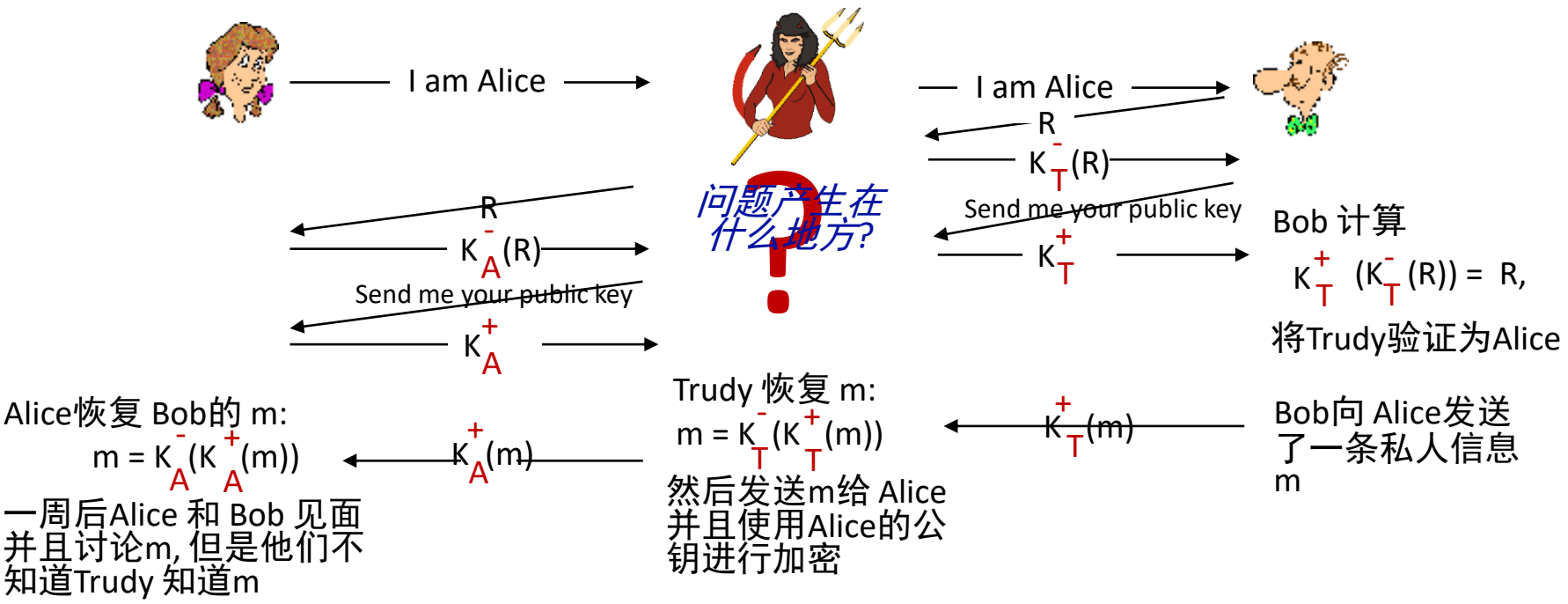


哈希函数算法

- 广泛使用的MD5 哈希函数(RFC 1321)
  - 经过4个步骤，计算得到128比特的信息摘要
  - 通过128比特的字符串x, 很难构造出一个字符串m，使得m的MD5的哈希值等于x
- 另外一种算法SHA-1
  - 美国标准[NIST, FIPS PUB 180-1]
  - 160比特的信息摘要

身份验证: 让我们完善验证协议5.0

问题回顾: Trudy 向Bob 假装自己是Alice， 向Alice假装自己是Bob

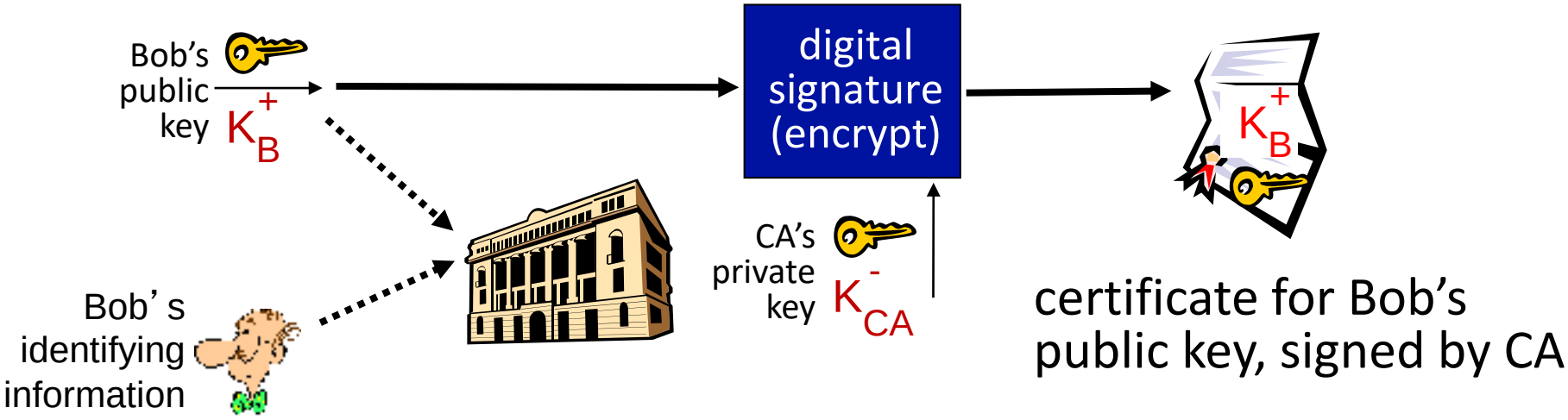


需要被认证的公钥

- 动机: Trudy对Bob玩了披萨恶作剧
  - Trudy创造了一封e-mail订单:
    亲爱的披萨店, 请给我送四个意大利香肠披萨. 谢谢, Bob
    - Trudy用她的私钥签署了订单
    - Trudy把订单发送给披萨店
    - Trudy把她的公钥发送给披萨店, 声称这是Bob的公钥
    - 披萨店验证了签名; 然后给Bob送去了四个意大利香肠披萨
    - Bob 一点儿都不喜欢意大利香肠

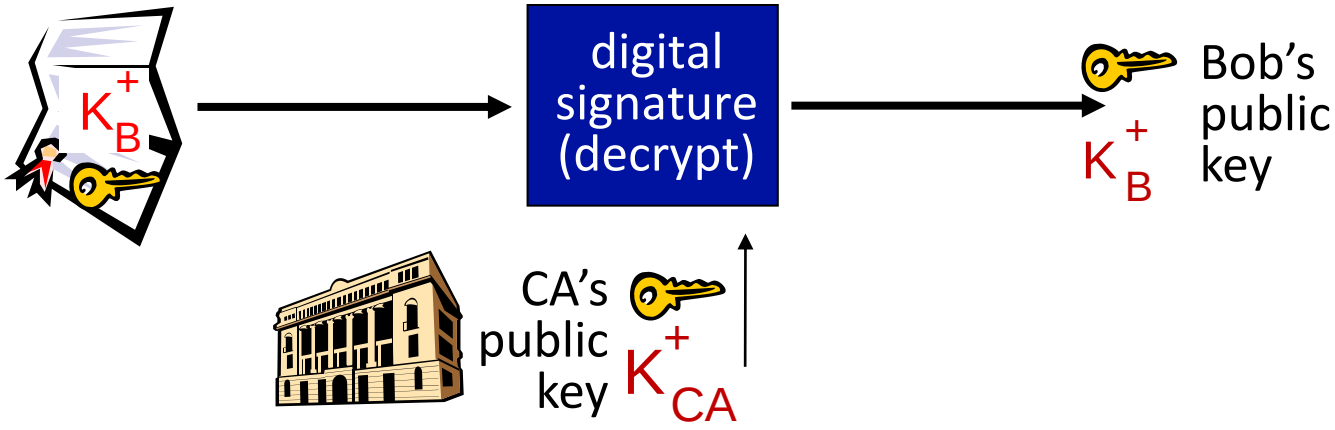
公钥认证机构(CA)

- 认证机构(CA): 将公钥绑定到特定实体E
- 实体(个人、网站、路由器)向CA注册其公钥，并向CA提供"身份证明"
  - CA创建证书，将E与E的公钥绑定
  - 证书包含由CA进行了数字签名的E的公钥:CA证明"这是E的公钥"



公钥认证机构(CA)

- 当Alice想要Bob的公钥时:
  - 获得Bob的证书(从Bob处或其他地方)
  - 对Bob的证书使用CA的公钥，获得Bob的公钥

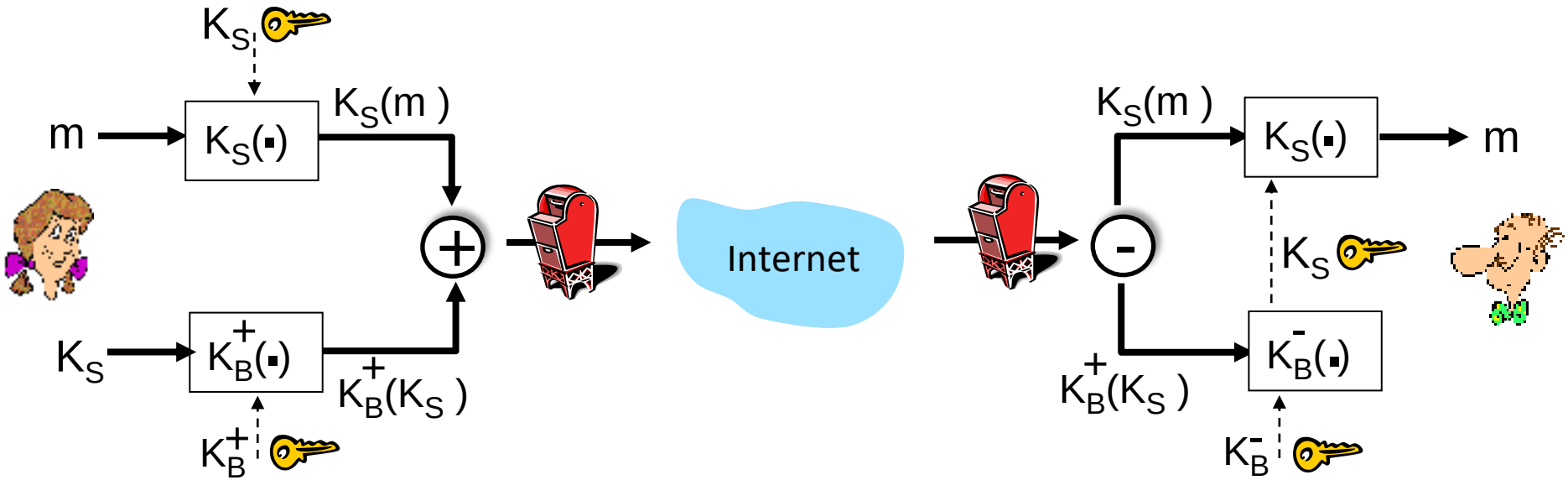


提纲

- 什么是网络安全？
- 密码学的原则
- 身份验证，报文完整性
- **安全电子邮件**
- 传输层安全性：TCP与TLS
- 网络层安全性：IPsec
- 无线网络和移动网络安全
- 运行安全性：防火墙和入侵检测系统IDS

安全电子邮件:保密

Alice希望给Bob发送一封*秘密*e-mail m

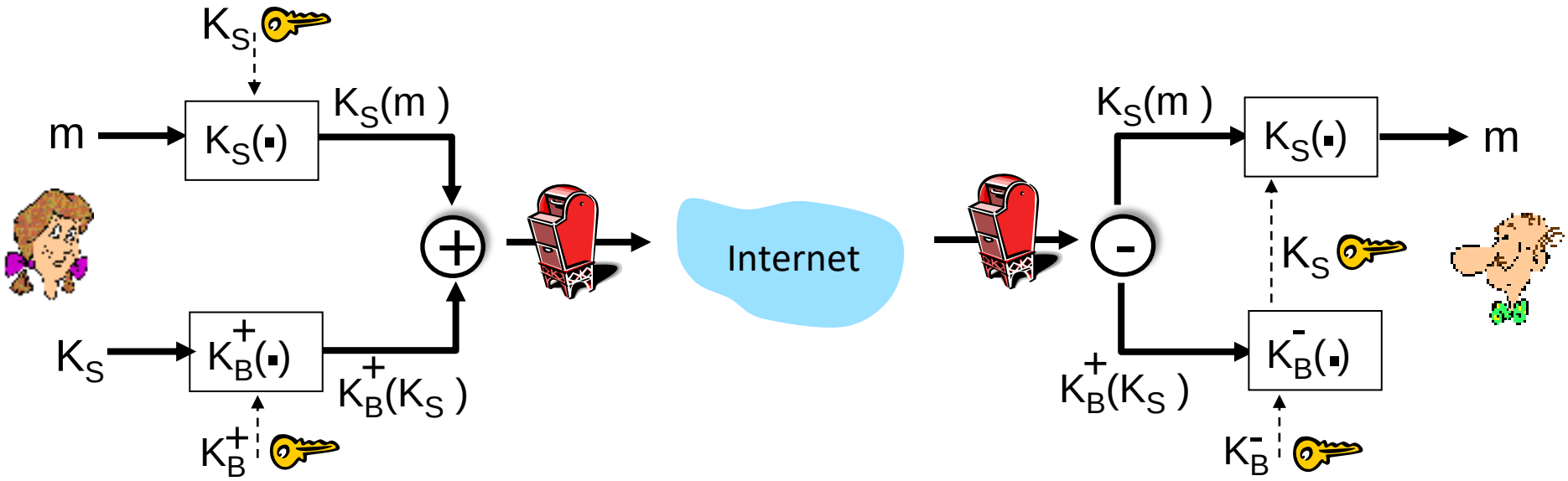


Alice:

- 生成随机的*对称私钥* K_S
- 使用K_S 对信息进行加密(为了效率)
- 同时使用Bob的公钥对K_S 进行加密
- 发送$K_S(m)$ 和$K^+_B(K_S)$ 给Bob

安全电子邮件:保密（续上文）

Alice希望给Bob发送一封*秘密*e-mail m

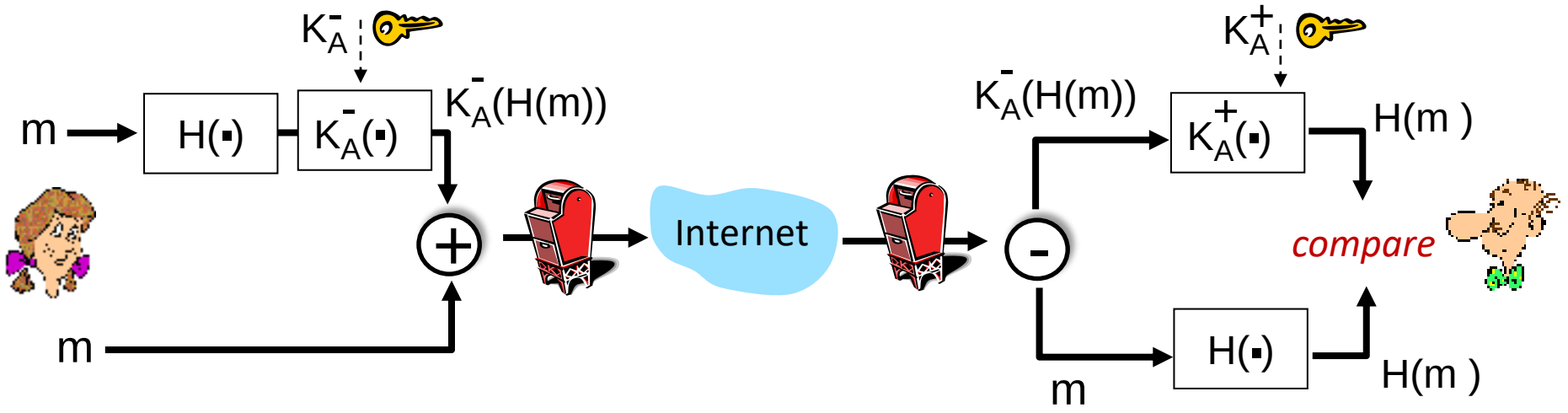


Bob:

- 使用他的私钥解密并恢复K_S
- 使用 K_S 对$K_S(m)$ 进行解密，恢复m

安全电子邮件:完整性、身份验证

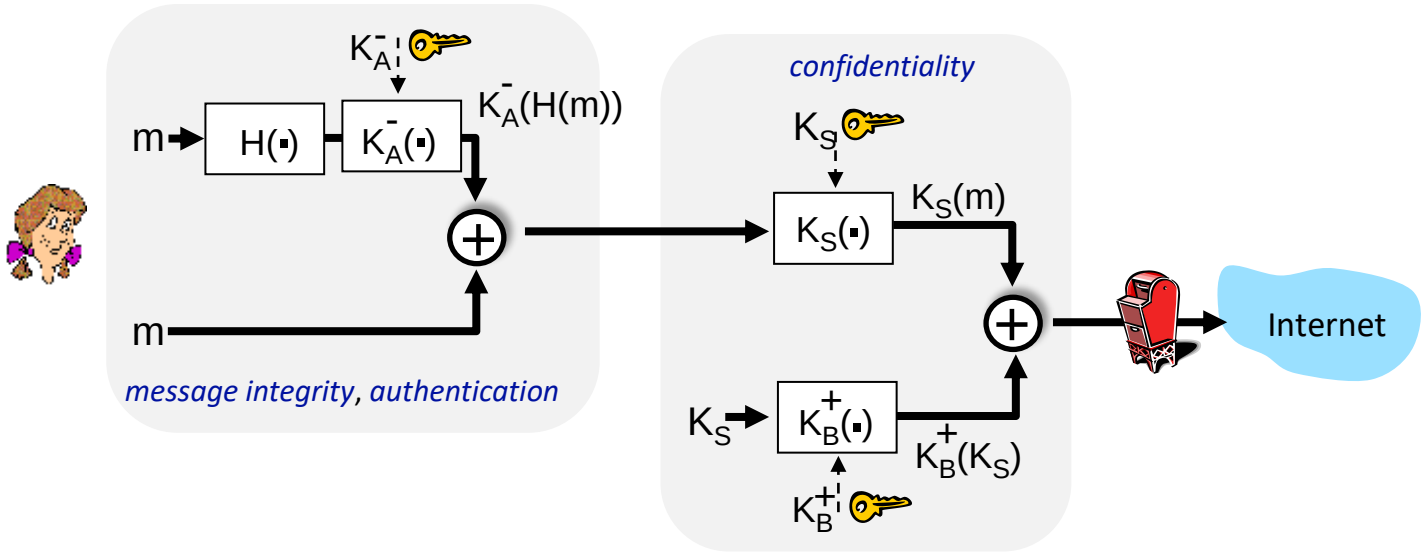
Alice希望给Bob发送一封e-mail m，附带*完整性与身份验证*



- Alice用她的私钥对她的消息进行数字签名，从而提供完整性和身份验证
- 发送消息(明文)和数字签名

安全电子邮件:完整性、身份验证

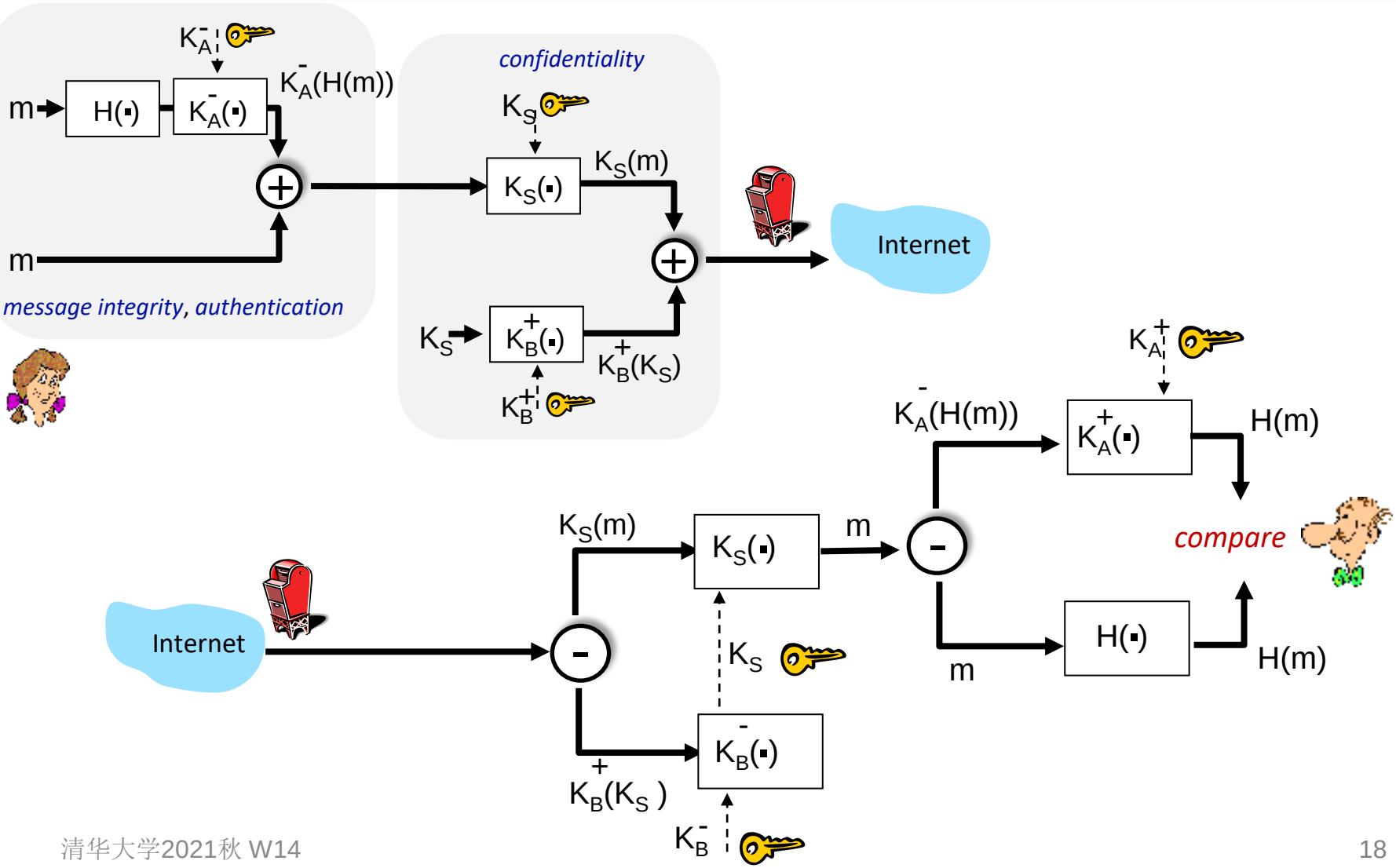
Alice希望给Bob发送一封e-mail m，附带*完整性与身份验证*



Alice使用了三种密钥: 她的私钥, Bob的公钥, 新的对称密钥

Bob的对应操作是什么?

安全电子邮件:完整性、身份验证



计算机网络及应用

Computer Networks and Applications

课程重点回顾和总结

主讲：清华大学　贾庆山

期末考试

- 时间
  - 2022年01月09日上午09:00-11:00
- 地点
  - 一教201、205
- 考题形式
  - 简答
  - 分析计算
- 考前答疑
  - 2022年01月07日下午13:30-15:30，FIT楼3-620

第一章重点内容（概述）

- 计算机网络的基本术语及其功能定位
  - 主机/端系统，通信链路，交换设备(路由器/交换机)
- 分组交换/电路交换的特点
- 网络性能指标
  - 带宽，时延，带宽时延积，丢包概率
- 时延的基本组成和计算
  - 传播时延+传输时延+排队时延+处理时延
  - 存储转发网络中的时延计算
- 分层模型：因特网5层模型/OSI 7层模型

单选题 1分

设置

智能手机位于_____，电子邮件服务器位于_____

A 网络边缘，网络边缘

B 网络边缘，网络核心

C 网络核心，网络边缘

D 网络核心，网络核心

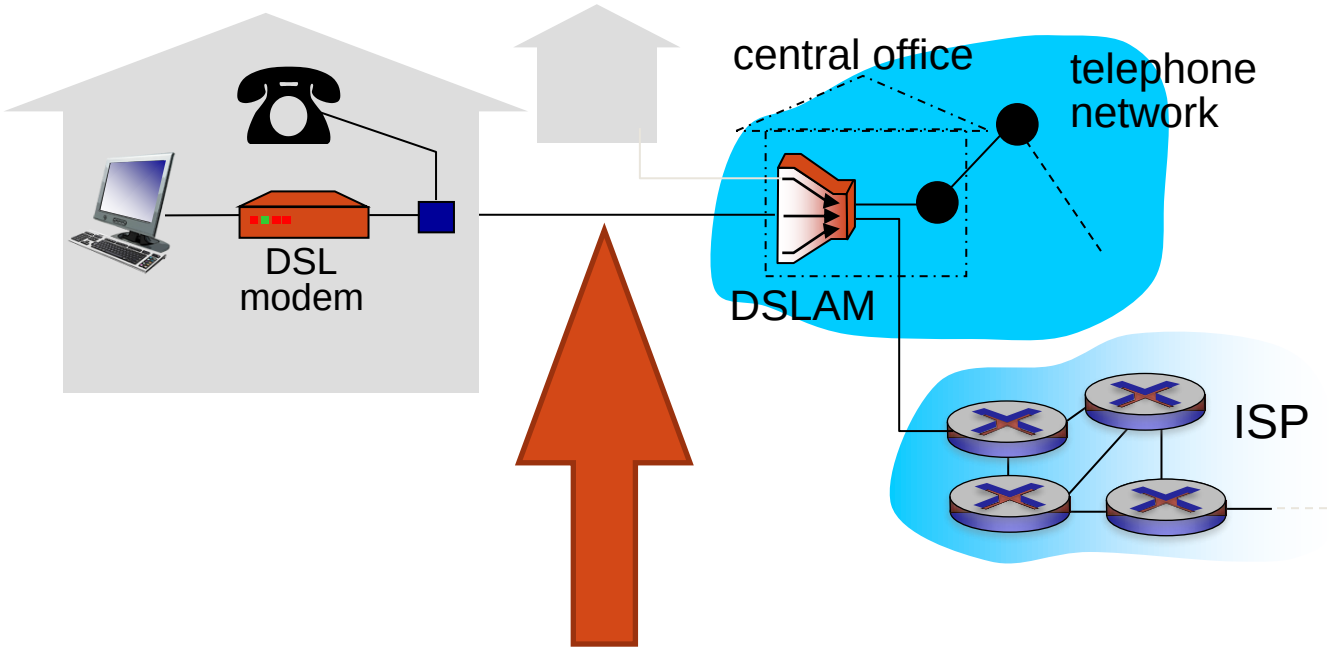
提交

设置

DSL住宅接入在电话线（双绞铜线）上传递的是_____信号

A 数字

B 模拟

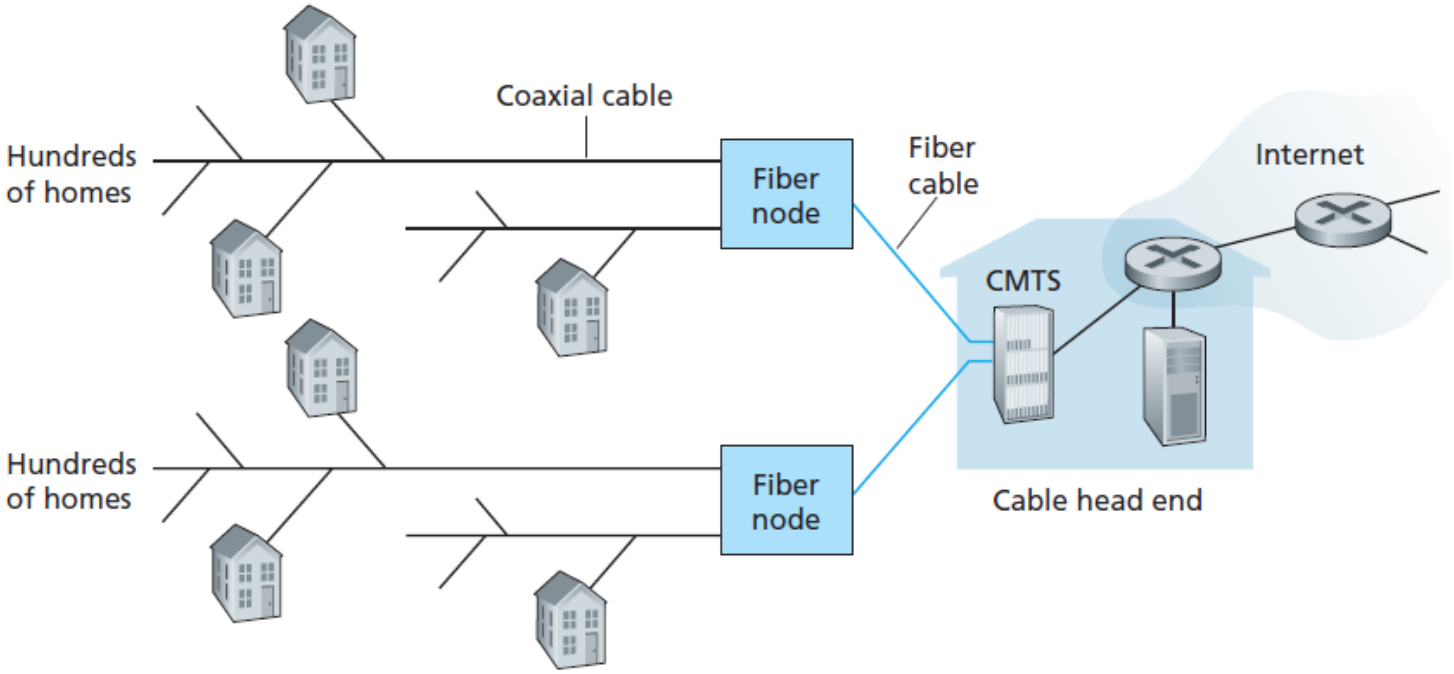


提交

主观题 10分

设置

在下行HFC信道中，有可能发生冲突吗？



正常使用主观题需2.0以上版本雨课堂

作答

2021年秋

因特网三要素

设备　协议　服务

多选题 1分

设置

Google已经与第一层ISP相连，为什么还要与较低层的ISP对等?

A 绕过较高层ISP，减少了向顶层ISP支付的费用

B 有一些接入ISP不与顶层ISP相连

C 能更好地控制其服务最终如何交付给端用户

提交

单选题 1分

设置

La/R=1表明数据到达的速率刚好等于数据的传输速率，为什么在这种情况下排队时延会趋向于无穷大?

A 传输速率存在波动

B 平均分组到达率存在波动，导致形成队列

C 分组传输需要占用一定的时间

提交

多选题 1分

设置

以下能识别IP地址的有

A 路由器

B 链路层交换机

C 主机

D 智能手机

提交

第二章重点内容（应用层）

- 应用程序结构模式
  - 客户端-服务器模式：服务器一直开机，不同程序，扩展性需采用服务器集群
  - P2P模式：同时有客户端/服务器功能，相同程序版本，扩展性强但难于管理
- 套接字(socket)/进程通信，客户端进程/服务器进程
  - 套接字：工作在运输层与应用层间，应用层协议由套接字具体定义，API函数库，选择传输协议/缓存、最大报文段长度等参数，IP地址+端口号来实现进程寻址

第二章重点内容（应用层）

- 应用层协议
  - Web和HTTP协议
    - 对象，URL地址，C/S模式，80端口，TCP协议，无状态
    - 非持久HTTP与持久HTTP，及其响应时间计算
      - 单个对象：2RTT+传输时间
      - 带流水线/不带流水线的持久HTTP：1RTT v.s. nRTT
      - 并行和非并行的非持久HTTP
    - HTTP请求报文/响应报文，基本格式和方法(post,get)
    - Cookie和Web缓存(代理服务器)及其对时延计算的影响
- Email协议：SMTP协议，25#，POP3/IMAP协议，基于Web的电子邮件
- DNS协议：分层/分布式
  - 根域名/顶级域名/权威域名/本地名字服务器，迭代/递归查询，DNS协议和报文
- P2P协议：集中式目录/洪泛查询，文件分发时间计算
- HTTP流和DASH，根据网络条件动态调整压缩率
- 内容分发网CDN：确定合适的服务器集群，客户请求重定向

主观题 10分

设置

在沿链路传播的过程中，先出发的报文应当领先于后出发的报文，那么使用UDP协议进行传输为什么可能导致报文乱序呢?

到达顺序不同

正常使用主观题需2.0以上版本雨课堂

作答

条件GET方法存在于下列哪个位置:

A 用户代理和缓存器之间

B 缓存器和初始服务器之间

C 用户代理和初始服务器之间

单选题 1分

设置

HTTP是带内传输还是带外传输?

A 带内传输

B 带外传输

提交

单选题 1分

设置

Alice给Bob发邮件的过程中，下面哪个过程使用的协议不会是SMTP

A Alice的用户代理发送报文到Alice的邮件服务器

B Alice的邮件服务器发送报文到Bob的邮件服务器

C Bob的用户代理收取Bob邮件服务器上的报文

提交

单选题 1分

设置

下列哪种DNS服务器不属于DNS层次结构

A 根DNS服务器

B 顶级域DNS服务器

C 权威DNS服务器

D 本地DNS服务器

提交

单选题 1分

设置

下列哪种DNS服务器不属于DNS层次结构

A 根DNS服务器

B 顶级域DNS服务器

C 权威DNS服务器

D 本地DNS服务器

提交

多选题 1分

设置

相对于单一的大规模数据中心，CDN的优点有哪些?

A 减少停滞时延

B 节约网络带宽

C 便于内容管理

D 规避单点故障

提交

第三章重点内容（运输层）

- 运输层的基本服务
  - 复用/分解，可靠数据传输，流量控制，拥塞控制
  - TCP/UDP，有连接/无连接
  - 复用/分解：运输层和套接字之间，根据TCP四元组/UDP二元组进行复用和分解
  - 典型若干应用层协议所采取的TCP/UDP协议情况
- UDP：服务的优缺点，报头格式
- 可靠数据传输原理
  - 使用有限状态自动机FSM表达接收方和发送方的行为
  - rdt1.0 : 完全可靠信道；
  - rdt2.0: 具有比特差错信道，错误检测+ACK/NAK+重传

第三章重点内容（运输层）

- 可靠数据传输原理
  - rdt2.1: ACK/NAK有损时，重传+序号(处理冗余分组)
  - rdt2.2: 只用ACK，ACK分组也使用序号
  - rdt3.0: 有位差和数据丢失时，定时器+超时重传
  - GBN (滑动窗口)协议：滑动窗口N+累积确认，基序号，丢弃失序分组（简化流程单浪费资源）
  - SR协议(选择性重传)：无累积确认，每个分组分别确认、分别设立一个定时器，仅重传未收到ACK的包，乱序+缓存，充分利用带宽
- TCP协议
  - TCP报文头格式，20字节，几个重要字段域，端口号/序号/确认号/接收窗口大小/校验和/报头长度/…

第三章重点内容（运输层）

- TCP协议
  - 超时时间间隔 = estimated_RTT+4dev_RTT > RTT
  - 累积确认，单定时器，超时重传+快速重传(3次冗余确认)，SR和GBN的组合
  - TCP流量控制: 避免缓存溢出，RcvWindow域通知发送方空闲缓存大小，发送方保证未确认数据量小于该值
  - TCP三次握手，SYN；关闭连接，FIN
  - TCP拥塞控制: 合理设置窗口Congwin和阈值Threshold，慢启动/拥塞避免阶段，指数倍增/加性增乘性减，超时/三次冗余确认，Taheo/Reno(快速恢复)
  - TCP的公平性，折线图

多选题 1分

设置

下列哪些会被用于UDP的套接字识别?

A 源IP地址

B 源端口号

C 目的IP地址

D 目的端口号

提交

单选题 1分

设置

rdt2.0（有位差信道上的可靠数据传输）能否处理ACK/NAK损坏的问题

A 可以

B 不可以

提交

单选题 1分

设置

TCP是GBN还是SR?

A GBN

B SR

C GBN和SR的组合

提交

单选题 1分

设置

选择性重传的窗口大小与序号范围有什么关系?

A 2*窗口大小 ≤ 序号范围

B 2*序号范围 ≤ 窗口大小

C 各自可以独立选择，彼此无关

提交

单选题 1分

设置

主机A向主机B发送一个（SYN=1,seq=11220）的TCP段，期望与主机B建立连接，若主机B接受该连接请求，则主机B 向主机A发送的TCP报文段可能是()

A (SYN=0,seq=11221,ACK=11221)

B (SYN=1,seq=11220,ACK=11220)

C (SYN=1,seq=11221,ACK=11221)

D (SYN=0,seq=11220,ACK=11220)

提交

单选题 1分

设置

有两条TCP连接C1和C2，共享一段拥塞链路。假设C1和C2均处于拥塞避免阶段，这两条连接有相同的MSS，但RTT1>RTT2。经长时间运行后，哪条连接将取得更多带宽？ ()

A C1

B C2

C C1和C2取得相同带宽

D 无法确定

提交

第四章重点内容（网络层:数据平面）

- 路由器：
  - 存储转发，路由表，基本物理结构
  - 最大前缀匹配
  - 排队和调度：先进先出、优先权排队、加权公平排队
- IP协议：数据报格式，分片与重组
  - IP编址：32bit，网络部分+主机部分，子网掩码或前缀长度, 网络地址, 特殊地址, CIDR编码与子网划分
  - DHCP和层次化编址
  - NAT：本地网络只使用一个IP地址和外部世界相连接
  - IPv6原理：128bit，报头格式，与IPv4的区别，从IPv4到IPv6的过渡技术

第四章重点内容（网络层:数据平面）

- 网络层概述
  - 控制平面：路由算法，数据平面：转发
  - 传统控制平面，SDN控制平面
- 通用转发和SDN
  - 流表：首部字段值集合、计数器集合、动作集合
  - 匹配：分组匹配字段
  - 动作：转发、丢弃修改
  - 匹配加动作的OpenFlow例子：简单转发、负载均衡、充当防火墙

单选题 1分

设置

考虑向具有700字节MTU的一条链路发送一个2400字节的数据报。将会分成多少个分片？最后一个数据报的长度（含IP头）为？（）

A 3，360

B 4，300

C 4，340

D 4，360

提交

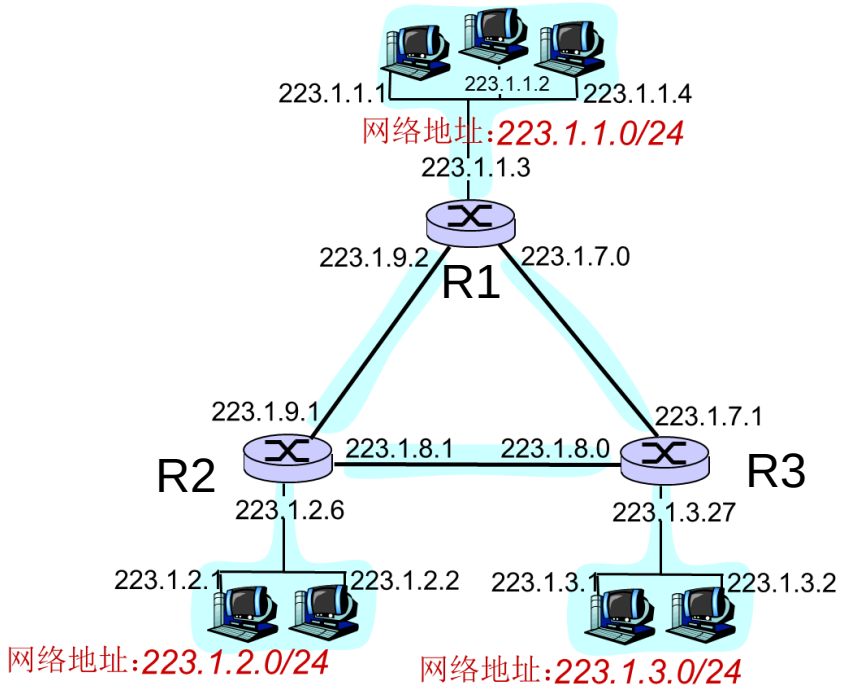
请问右图中其余三个子网是（）

A 223.1.9.0/24

B 223.1.6.0/24

C 223.1.8.0/24

D 223.1.7.0/24



提交

单选题 1分

设置

假设清华大学分配的地址为194.24.0.0/21；北京大学分配的地址为194.24.16.0/20；人民大学分配的地址为194.24.8.0/22.一个目的地址194.24.17.4的包到达路由器，请问这个包被发送到哪个大学（）

A 清华大学

B 北京大学

C 人民大学

D 都不是

提交

多选题 1分

设置

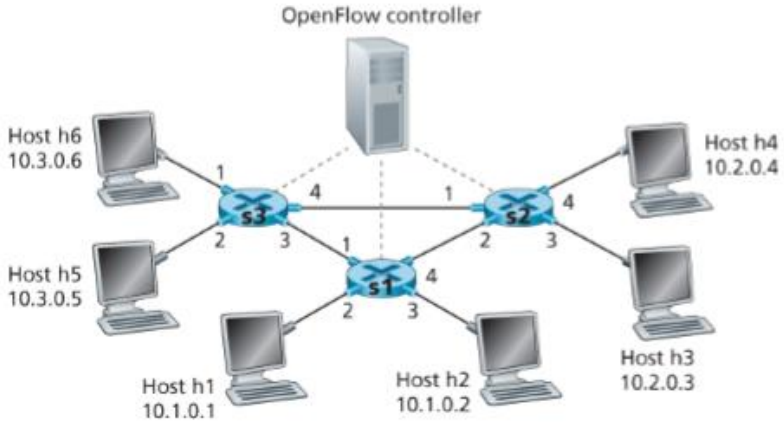
如图所示的SDN OpenFlow网络，为使得具有h3或h4源地址的任何到达数据报被路由到在IP数据报的目的地址字段中定义的目的主机，s1的流表中需要包括哪些项才完整（）

A IP Src=10.2.*.*,IP Dst=10.1.0.1 Forward(2)

B IP Src=10.2.*.*,IP Dst=10.3.0.5 Forward(1)

C IP Src=10.2.*.*,IP Dst=10.1.0.2 Forward(3)

D IP Src=10.2.*.*,IP Dst=10.3.*.* Forward(1)



提交

第五章重点内容（网络层:控制平面）

- 路由选择算法：
  - 链路状态选路算法：Dijkstra算法，振荡现象
  - 距离向量选路算法：Bellman-Ford方程，毒性逆转
  - LS与DV算法比较：报文复杂性，收敛速度，健壮性
- OSPF
  - 自治系统内路由选择协议，支持层次结构
  - 区域边界路由器、主干路由器、边界路由器
- BGP
  - eBGP、iBGP；属性：AS-PATH，NEXT-HOP
  - BGP报文：TCP交换报文，OPEN，UPDATE等
  - 路由选择：本地偏好，最短AS-PATH，热土豆，标识符

第五章重点内容（网络层:控制平面）

- SDN控制平面：
  - 特征：基于流转发，数控分离，控制功能在交换机外，可编程网络
  - 体系结构：数据平面交换机，控制器，应用程序
  - 控制器组件：通信层，管理层，应用程序的接口
  - OpenFlow协议：控制器到交换机，交换机到控制器
- ICMP：因特网控制报文协议
  - 主机与路由器沟通网络层信息，Traceroute程序
- 网络管理与SNMP
  - 网络管理框架：管理服务器，被管设备，网络管理协议
  - SNMP：被管设备与管理服务器请求相应，陷阱报文

单选题 1分

设置

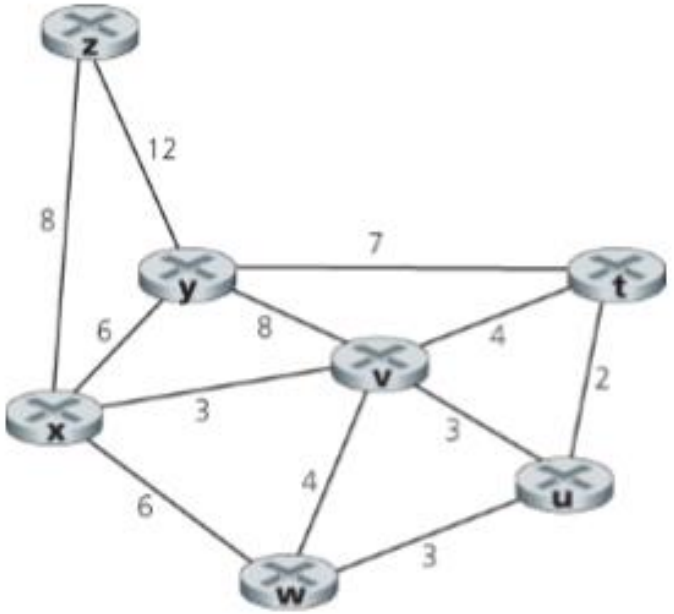
在使用Dijkstra算法计算从w到所有网络节点的最短路径时，z是第几个被确定的节点（计数不包含w自身）（）

A 3

B 4

C 5

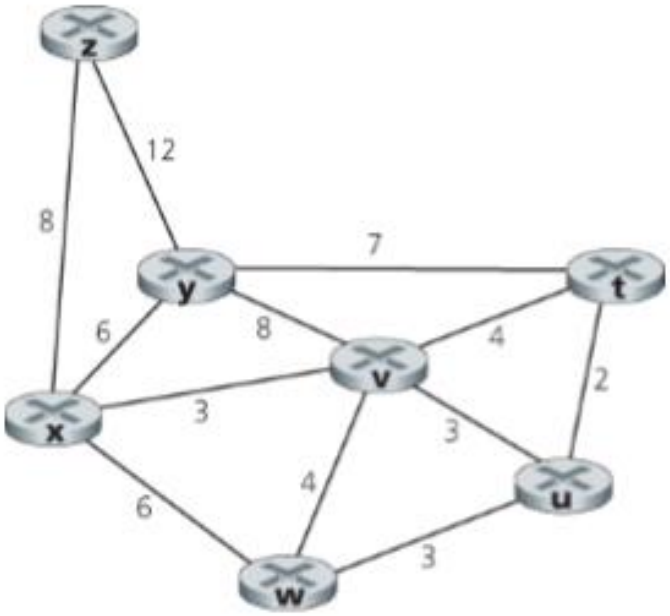
D 6



提交

答案解析

具体计算过程如下表所示，可见z最后一个被确定，是第6个点。



Step	N'	D(x), p(x)	D(u),p(u)	D(v),p(v)	D(t),p(t)	D(y),p(y)	D(z),p(z)
	w	6,w	3,w	4,w	∞	∞	∞
1	wu	6,w	3,w	4,w	5,u	∞	∞
2	wuv	6,w	3,w	4,w	5,u	12,v	∞
3	wuvt	6,w	3,w	4,w	5,u	12,v	∞
4	wuvtx	6,w	3,w	4,w	5,u	12,v	14,x
5	wuvtxy	6,w	3,w	4,w	5,u	12,v	14,x
6	wuvtxyz	6,w	3,w	4,w	5,u	12,v	14,x

单选题 1分

设置

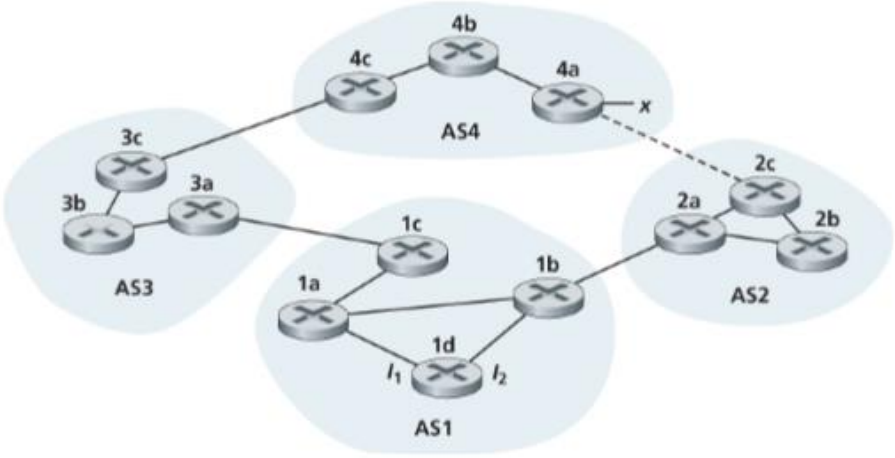
如图所示的网络，假定所有AS运行OSPF作为其AS内部路由选择协议，假定AS间路由选择协议使用的是eBGP和iBGP，假定在AS2和AS4之间不存在物理链路。请问路由器3c、3a从下列哪个协议学习到了前缀x:OSPF、eBGP或iBGP（）？

A iBGP、eBGP

B eBGP、iBGP

C OSPF、eBGP

D OSPF、iBGP



提交

多选题 1分

设置

下列哪些报文流跨越SDN控制器的北向API？()

A 链接状态路由选择应用与流表管理器交互，流表管理器决定更新的流表

B 控制器从交换机查询统计数据和计数器值

C Dijkstra路由算法访问网络图信息、控制器中的链路状态信息，从而计算新的路由

D 交换机向控制器通知端口状态的变化

提交

第六章重点内容（链路层）

- 链路层提供的服务
  - 成帧，链路访问，可靠数据传输，流量控制，差错检测，差错纠正，半双工/全双工
- 差错检测和纠错技术
  - 奇偶校验，检验和，循环冗余检测(CRC校验)
- 多路访问协议
  - 信道划分协议（TDMA/FDMA/CDMA）
  - 随机访问协议（Aloha/CSMA）
  - 轮流协议（Token Ring）

第六章重点内容（链路层）

- 多路访问协议
  - 时隙Aloha协议的基本原理和效率计算
  - 纯Aloha协议的基本原理和效率计算
  - CSMA协议的基本原理
- 链路层寻址
  - MAC地址与ARP协议的基本原理
  - 子网内/子网外的ARP工作流程
- 以太网技术
  - 802.3帧格式
  - CSMA/CD的具体工作流程
  - 载波侦听，碰撞检测，二进制指数避让（随机访问）

第六章重点内容（链路层）

- 交换机的工作原理
  - 存储转发
  - 交换机表：自学习
  - 交换机与Hub：隔离碰撞域
- 虚拟局域网
  - VLAN的基本原理与作用
  - 跨VLAN通信，Trunking，802.1Q帧格式
- 链路虚拟化MPLS
  - MPLS的动机与原理
  - MPLS与IP路由的差异
- 数据中心网络
  - 等级架构拓扑，对等拓扑

单选题 1分

设置

假设某分组的信息内容是比特模式1110 0110 1001 1101,并且使用了偶校验方案。在采用二维奇偶校验方案的情况下,包含该检验比特的字段的值是什么?你的回答应该使用最小长度检验和字段。 ( )

A

1 1 1 0 1
0 1 1 0 0
1 0 0 1 0
1 1 0 1 1
1 1 0 0 0

B

1 1 1 0 0
0 1 1 0 1
1 0 0 1 1
1 1 0 1 0
0 0 1 1 1

C

1 1 1 0 0 1 1 0 0
1 0 0 1 1 1 0 1 0
1 0 0 0 0 1 0 0 1

D

1 1 1 0 0 1 1 0 1
1 0 0 1 1 1 0 1 1
0 1 1 1 1 0 1 1 0

提交

单选题 1分

设置

假定在不考虑转发的情况下，100m长的CSMA/CD网络的数据率为1Gb/s,设信号在网络上的传播速率为2 * 10^5 km/s，求使得CDMA/CD发挥作用的最短帧长？

A 50 bytes

B 125 bytes

C 500 bytes

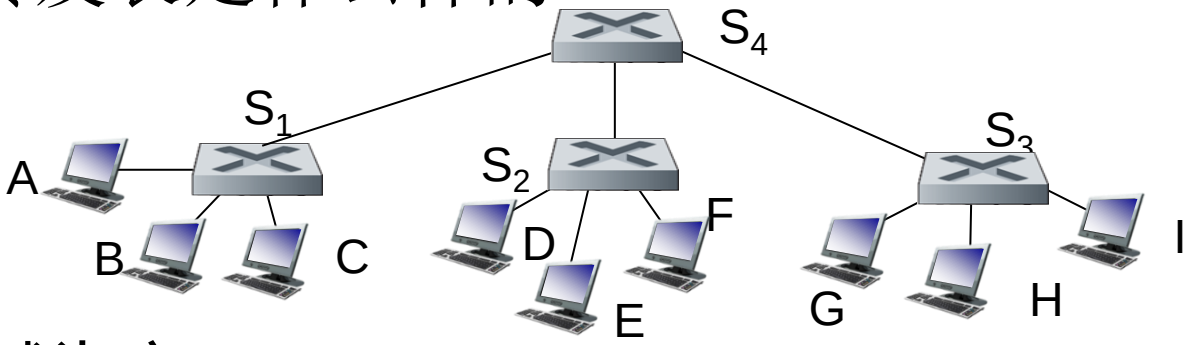
D 625 bytes

提交

单选题 1分

设置

假设初始转发表都为空，主机C发送数据帧到主机I，主机I再发送响应给主机C，此时交换机S2的转发表是什么样的？



A 仍然为空

B 具有主机C 的表项

C 具有主机I 的表项

D 同时具有主机C和I的表项

提交

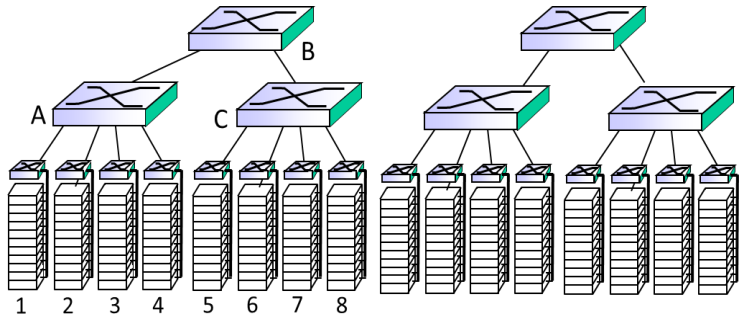
- **问题：主机到主机的容量受限**
  - 假设每个机架有10台主机，主机TOR交换机总是1Gbps链路，要想满足机架1-8之间的任意主机间全部满速相互通信，至少需要交换机A, B, C分别提供多大的下行速率？

A 1 Gbps, 10 Gbps, 1 Gbps

B 10 Gbps, 10 Gbps, 10 Gbps

C 10 Gbps, 40 Gbps, 10 Gbps

D 40 Gbps, 40 Gbps, 40 Gbps



提交

第七章重点内容（无线移动网络）

- 两大特点: 无线/移动，两大模式: 基础设施/自组织
- 无线链路特点：
  - 信号衰减/多径效应，SNR与BER
  - 隐藏终端问题
  - CDMA原理
- 802.11协议
  - CSMA/CA的基本原理
  - 载波侦听、碰撞避免（与碰撞检测的区别）、指数回退算法（与CSMA/CD在应用上区别）
  - 链路层确认与重传（与传输层确认的异同），使用ARQ机制
  - RTS/CTS机制处理隐藏终端问题 (集中式)
  - 802.11的帧格式
  - 速率自适应与电源管理

第七章重点内容（无线移动网络）

- 蜂窝网络接入
  - 了解2G/3G/4G的基本结构与异同即可
- 移动管理原理
  - 永久地址/转交地址，归属网络/访问网络，归属代理/外部代理，注册，封装/拆封
  - 直接选路与间接选路
- 移动性案例
  - 移动IP：代理发现与代理通告
  - 处理蜂窝网络中的移动性：在不同的MSC之间切换

单选题 1分

设置

判断题：在移动IP网络中的某终端A对一固定服务器B发起TCP连接，其中：

- TCP连接建立阶段，B向A发送的数据是否经过归属地代理？
- 数据传输阶段，B向A发送的数据是否经过归属地代理？

A 经过，经过

B 经过，不经过

C 不经过，经过

D 不经过，不经过

提交