6. 各个层次的安全性

6.1 安全电子邮件

Alice:
产生随机的对称密钥，KS
使用KS对报文加密(为了效率)
对 KS使用 Bob的公钥进行加密.
发送KS(m) 和KB(KS) 给 Bob.
Bob:
使用自己的私钥解密 KS
使用 KS解密 KS(m) 得到报文

Alice:
需要提供源端的可认证性和报文完整性
数字签署文件
发送报文（明文）和 数字签名
需要提供机密性，源端可认证性和报文的完整性
使用了3个keys: 自己的私钥，Bob的公钥，新产生出的对称式密钥

Pretty good privacy PGP
Internet e-mail加密方案，事实上的标准.
使用前面讲述的：对称密钥加密，公开密钥加密，散列函数和数字签名.
能够提供机密性，源端的可认证性和报文完整性.
发明者，Phil Zimmerman，是 3 年的犯罪调查的目标

6.2 安全socket

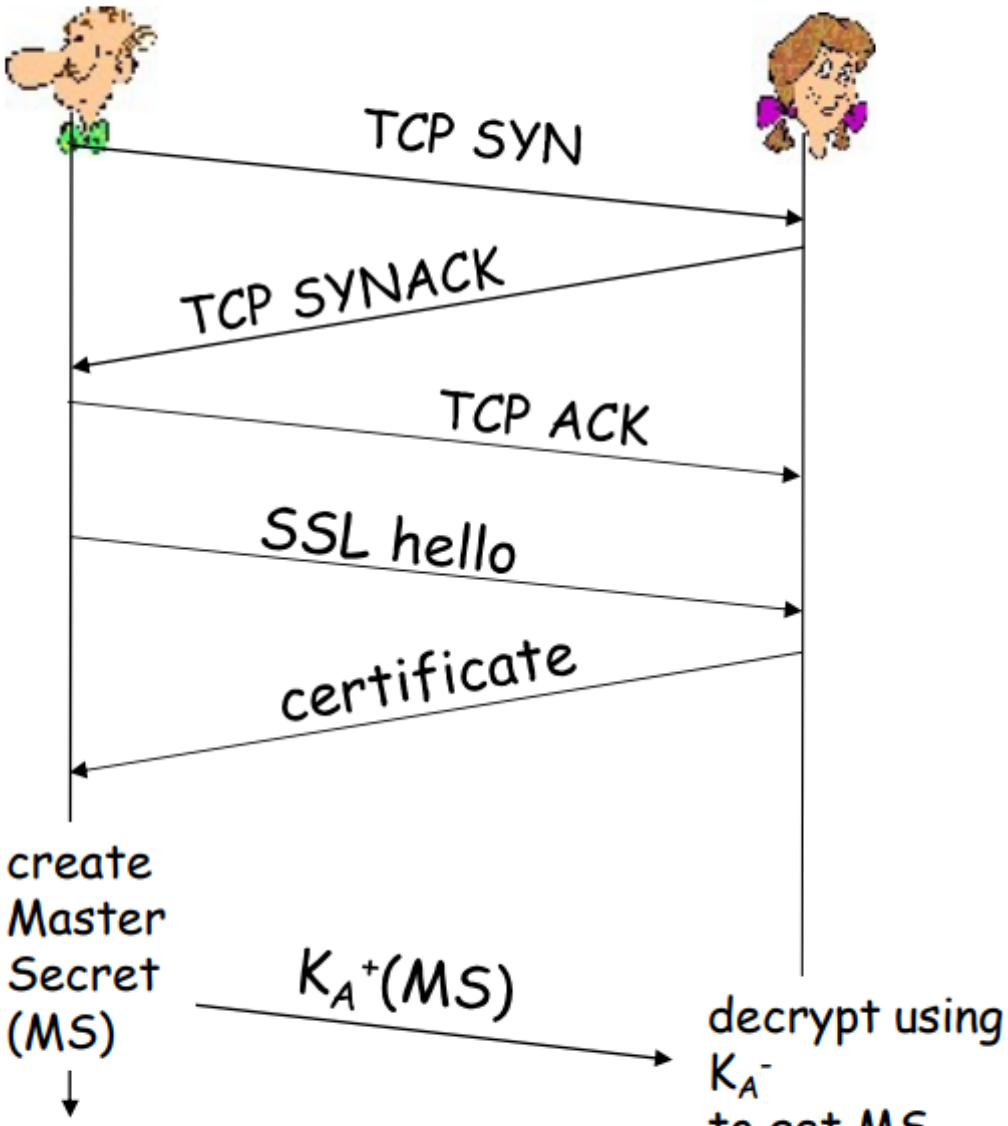
Secure sockets layer (SSL) 安全套接字层
为使用SSL服务的、基于TCP的应用提供传输层次的安全性
e.g., 在WEB的浏览器和服务器之间进行电子商务的交易 (shttp)
所提供的安全服务:
服务器的可认证性，数据加密，客户端的可认证性 (可选)

SSL在应用层

SSL：3阶段
1. 握手:
Bob 和Alice 建立TCP连接
通过CA签署的证书认证 Alice的身份
创建，加密 (采用Alice的公钥)，传输主密钥给Alice
不重数交换没有显示

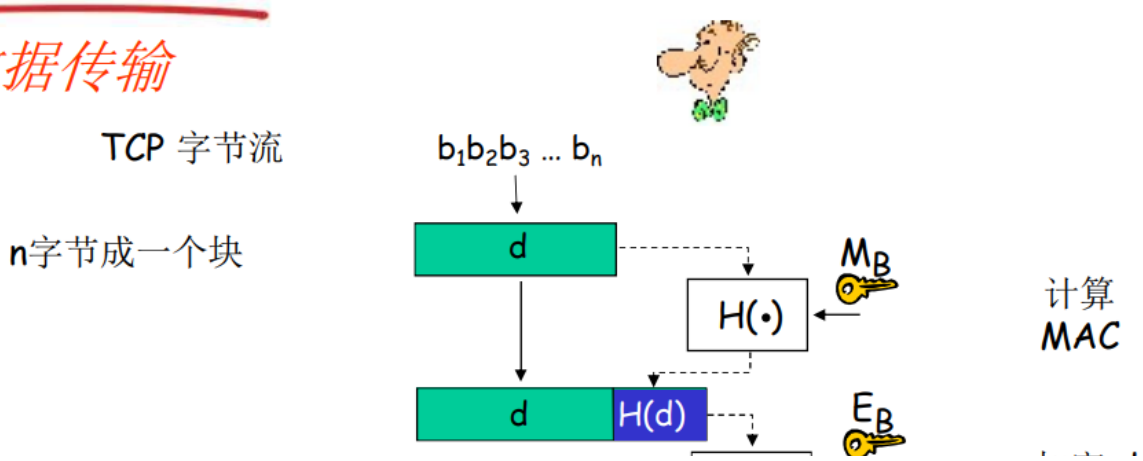
2.密钥导出：
Alice，Bob采用共享的MS产生4个keys:
EB: Bob->Alice 数据加密key
EA: Alice->Bob数据加密key
MB: Bob->Alice MAC（报文鉴别编码）key
MA: Alice->Bob MAC key
加密和MAC算法在Bob，Alice之间协商
为什么要4个keys?
更安全

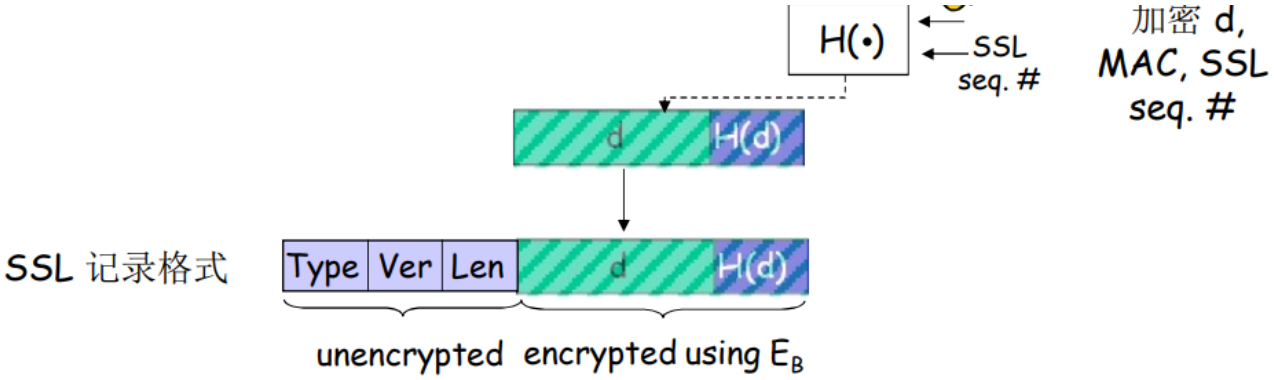
3.数据传输



SSL: 3阶段

3. 数据传输



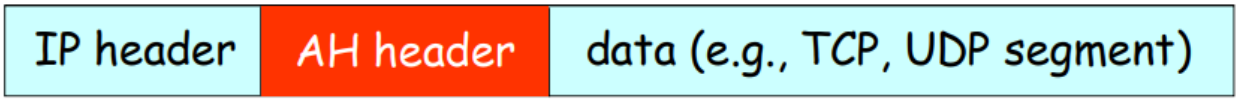


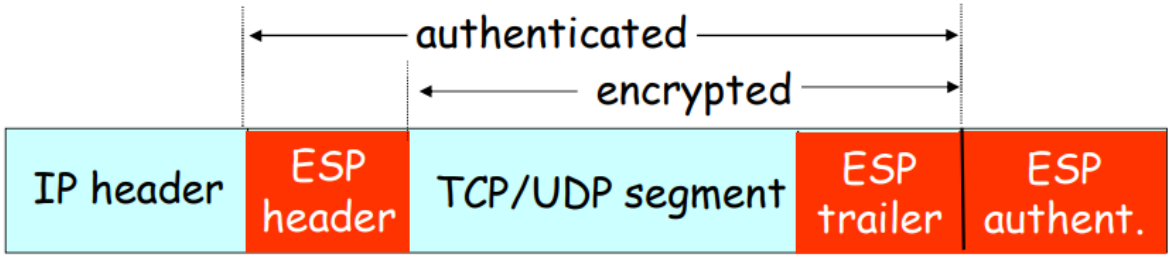
6.3 IPsec　网络层次的安全性

在IP协议之上

网络层次的机密性：
　　发送端主机对IP数据报中的数据进行加密
　　数据：TCP或者UDP的段，ICMP和SNMP的报文
网络层次的可认证性：
　　目标主机可以认证源主机的IP地址
2个主要协议：
　　认证头部（AH）协议
　　封装安全载荷
　　　　encapsulation security payload (ESP) 协议
不管AH还是ESP，源和目标在通信之前要握手：
　　创建一个网络层次的逻辑通道：安全关联security association(SA)
每一个SA都是单向
由以下元组唯一确定：
　　安全协议（AH or ESP）
　　源IP地址
　　32-bit连接ID

Authentication Header (AH) 协议
　　提供源端的可认证性，数据完整性，但是不提供机密性
　　在IP头部和数据字段之间插入AH的头部
　　协议字段：51
　　中间的路由器按照常规处理这个数据报
　　AH 头部包括：
　　　　连接ID
　　　　认证数据：对原始数据计算报文摘要，使用源端的私钥进行数字签名.
　　　　下一个字段：定义了数据的类型 (e.g., TCP, UDP,ICMP)
ESP 协议
　　提供机密性，主机的可认证性，数据的完整性.
　　数据和ESP尾部部分被加密
　　next header字段在ESP尾部
　　ESP 认证的头部与AH类似
　　协议号 = 50.





6.4 802.11中的安全性

每一个IP分组都通过异或加密