志存高远 责任为先

电子邮件安全

地址：赣州市红旗大道86号 信息工程学院
网址：www.jxust.edu.cn
邮编：341000

目录/Contents

01
Part

电子邮件协议概述

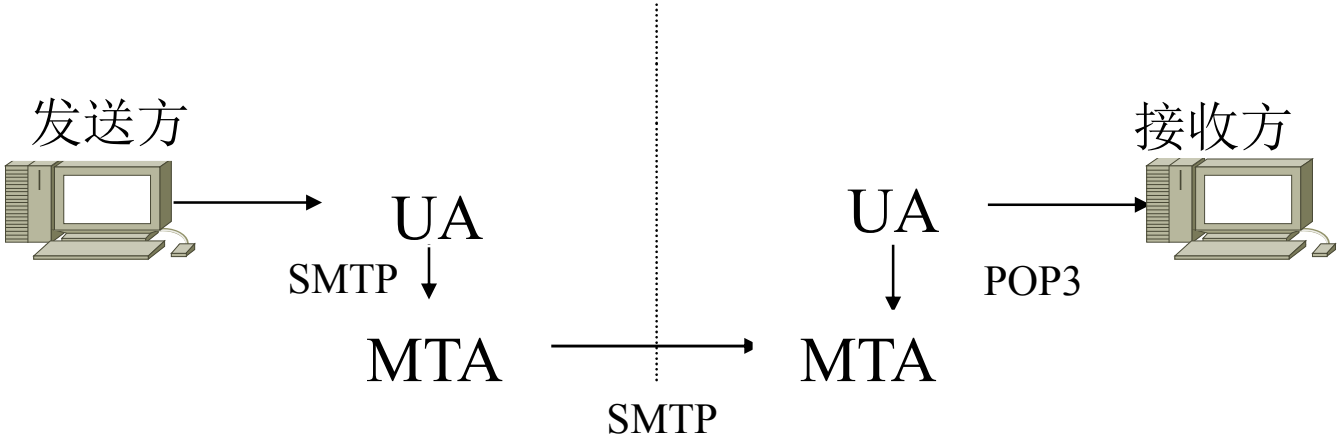
电子邮件概述

- **电子邮件（E-mail）是Internet上应用最广、最基本的服务之一**
- **电子邮件将邮件发送到收信人的邮箱中，收信人可随时进行读取**
- **不仅使用方便，而且还具有传递迅速和费用低廉的优点**
- **不仅可传送文字信息，而且还可附上声音和图像等多媒体信息文件**

电子邮件系统

- **E-mail服务是一种客户机/服务器模式的应用**
  - **客户机负责的是邮件的编写、阅读、管理等处理工作**
  - **服务器是负责的是邮件的传送工作**
- **一个完整的电子邮件系统具有三个主要的组成部分**
  - **客户端软件用户代理UA(User Agent)**
    - **用户接口，负责邮件生成与邮件处置；一般放在个人计算机内**
  - **邮件服务器软件MTA(Message Transfer Agent)**
    - **电子邮局，扮演网关的角色，主要负责邮件传输；一个MTA可以带若干UA**
  - **电子邮件使用的协议**

TCP/IP电子邮件系统原理



SMTP协议

- 简单邮件传输协议（Simple Mail Transfer Protocol, SMTP ）
  - 一组用于由源地址到目的地址传送邮件的规则，用来控制信件的中转方式
  - 属于TCP / IP协议族的应用层协议，帮助每台计算机在发送或中转信件时找到下一个目的地
  - 通过SMTP协议所指定的服务器，我们就可以把E - mail寄到收信人的服务器上
- SMTP服务器
  - 遵循SMTP协议的发送邮件服务器，用来发送或中转电子邮件

SMTP常用命令和应答

- 命令（以\r\n结束）
  - HELO、MAIL FROM、RCPT TO、DATA、QUIT
- 应答
  - xyz
- BASE64加密（等于没加密）

SMTP协议工作过程

- 1.TCP三次握手建立连接
- 2.认证阶段
  - EHLO、AUTH　LOGIN
- 3.操作阶段
  - MAIL FROM、RCPT TO、DATA
- 4.退出阶段
  - QUIT

SMTP流程实例

192.168.1.104	121.248.60.52	TCP	66 37143 > smtp [SYN] Seq=2313396911 Win=8192 Len=0 MSS=1460 WS=256
121.248.60.52	192.168.1.104	TCP	66 smtp > 37143 [SYN, ACK] Seq=3188786718 Ack=2313396912 Win=5840 L
192.168.1.104	121.248.60.52	TCP	54 37143 > smtp [ACK] Seq=2313396912 Ack=3188786719 Win=65792 Len=0
121.248.60.52	192.168.1.104	SMTP	119 S: 220 seu.edu.cn Anti-spam GT for Coremail System (seu[2016123(
192.168.1.104	121.248.60.52	SMTP	76 C: EHLO TXGTYPRI5FW5ABA
121.248.60.52	192.168.1.104	TCP	54 smtp > 37143 [ACK] Seq=3188786784 Ack=2313396934 Win=5888 Len=0
121.248.60.52	192.168.1.104	SMTP	254 S: 250 mail | 250 PIPELINING | 250 AUTH LOGIN PLAIN | 250 AUTH=
192.168.1.104	121.248.60.52	SMTP	66 C: AUTH LOGIN
121.248.60.52	192.168.1.104	SMTP	72 S: 334 dXNlcm5hbWU6
192.168.1.104	121.248.60.52	SMTP	68 C: User:[redacted]
121.248.60.52	192.168.1.104	SMTP	72 S: 334 UGFzc3dvcmQ6
192.168.1.104	121.248.60.52	SMTP	76 C: Pass: [redacted]
121.248.60.52	192.168.1.104	SMTP	85 S: 235 Authentication successful
192.168.1.104	121.248.60.52	SMTP	86 C: MAIL FROM: <[redacted]seu.edu.cn>
121.248.60.52	192.168.1.104	SMTP	67 S: 250 Mail OK
192.168.1.104	121.248.60.52	SMTP	83 C: RCPT TO: <[redacted]@qq.com>
121.248.60.52	192.168.1.104	SMTP	67 S: 250 Mail OK
192.168.1.104	121.248.60.52	SMTP	60 C: Data
121.248.60.52	192.168.1.104	SMTP	91 S: 354 End data with <CR><LF>.<CR><LF>
192.168.1.104	121.248.60.52	SMTP	377 C: DATA fragment, 323 bytes
121.248.60.52	192.168.1.104	TCP	54 smtp > 37143 [ACK] Seq=3188787114 Ack=2313397372 Win=6912 Len=0
192.168.1.104	121.248.60.52	IMF	1175 from: [redacted]@seu.edu.cn>, subject: hellotest,
121.248.60.52	192.168.1.104	TCP	54 smtp > 37143 [ACK] Seq=3188787114 Ack=2313398493 Win=9216 Len=0
121.248.60.52	192.168.1.104	SMTP	110 S: 250 Mail OK queued as rD34eQBXuB2GFgtcQYZnAA--.63417S2
192.168.1.104	121.248.60.52	SMTP	60 C: QUIT
121.248.60.52	192.168.1.104	SMTP	63 S: 221 Bye
192.168.1.104	121.248.60.52	TCP	54 37143 > smtp [RST, ACK] Seq=2313398499 Ack=3188787179 Win=0 Len=
121.248.60.52	192.168.1.104	TCP	54 smtp > 37143 [FIN, ACK] Seq=3188787179 Ack=2313398499 Win=9216 L

发送邮件代码

```
void SendMail(char *cSMTPServer, char *cFrom, char *cTo)
{
    WSADATA wsaData;
    SOCKET s;
    sockaddr_in serverAddr;
    int nRet;
    char buf[1024];
    char cCmd[256];

    WSAStartup(MAKEWORD(2,2), &wsaData);

    s = socket(AF_INET, SOCK_STREAM, 0);
    memset(&serverAddr, 0, sizeof(serverAddr));
    serverAddr.sin_family = AF_INET;
    serverAddr.sin_port = htons(25);
    serverAddr.sin_addr.s_addr = inet_addr(cSMTPServer); //inet_addr();
    nRet = connect(s, (struct sockaddr *)&serverAddr, sizeof(serverAddr));
    nRet = recv(s, buf, 1024, 0);

    sprintf(cCmd, "EHLO %s\r\n", cSMTPServer);
    nRet = send(s, cCmd, strlen(cCmd), 0);
    nRet = recv(s, buf, 1024, 0);

    nRet = send(s, "AUTH LOGIN\r\n", strlen("AUTH LOGIN\r\n"), 0);
    nRet = recv(s, buf, 1024, 0);

    Base64Encode(cCmd, cFrom);
    strcat(cCmd, "\r\n");
```

POP3协议

- 协议是邮局协议（Post Office Protocol, POP ）
  - 一种允许用户从邮件服务器收发邮件的协议
- POP3（Post Office Protocol 3）
  - 邮局协议的第3个版本
  - 规定怎样将个人计算机连接到Internet的邮件服务器和下载电子邮件的电子协议，是因特网电子邮件的第一个离线协议标准
  - 允许用户从服务器上把邮件存储到本地，同时删除保存在邮件服务器上的邮件
  - 与SMTP协议相结合，POP3是目前最常用的电子邮件服务协议
- POP3服务器
  - 遵循POP3协议的接收邮件服务器，用来接收电子邮件的

POP3常用命令和应答

- 命令（以\r\n结束）
  - USER、PASS、QUIT、STAT、RETR、DELE
- 应答
  - +OK 或 +ERR

POP3协议工作过程

- 1.TCP三次握手建立连接
- 2.认证阶段
  - USER、PASS、STAT
- 3.操作阶段
  - RETR
- 4.更新阶段
  - DELE
- 5.退出阶段
  - QUIT

POP3流程实例

192.168.1.104	121.248.60.52	TCP	66 36980 > pop3 [SYN] Seq=4159500324 Win=8192 Len=0 MSS=1460 WS=256
121.248.60.52	192.168.1.104	TCP	66 pop3 > 36980 [SYN, ACK] Seq=1686754901 Ack=4159500325 Win=5840 L
192.168.1.104	121.248.60.52	TCP	54 36980 > pop3 [ACK] Seq=4159500325 Ack=1686754902 Win=65792 Len=0
121.248.60.52	192.168.1.104	POP	138 S: +OK Welcome to coremail Mail Pop3 Server (seus[fb65022c23356
192.168.1.104	121.248.60.52	POP	70 C: USER [redacted]
121.248.60.52	192.168.1.104	TCP	54 pop3 > 36980 [ACK] Seq=1686754986 Ack=4159500341 Win=5888 Len=0
121.248.60.52	192.168.1.104	POP	69 S: +OK core mail
192.168.1.104	121.248.60.52	POP	74 C: PASS [redacted]
121.248.60.52	192.168.1.104	TCP	54 pop3 > 36980 [ACK] Seq=1686755001 Ack=4159500361 Win=5888 Len=0
121.248.60.52	192.168.1.104	POP	91 S: +OK 90 message(s) [2559819 byte(s)]
192.168.1.104	121.248.60.52	POP	60 C: STAT
121.248.60.52	192.168.1.104	TCP	54 pop3 > 36980 [ACK] Seq=1686755038 Ack=4159500367 Win=5888 Len=0
121.248.60.52	192.168.1.104	POP	70 S: +OK 90 2559819
192.168.1.104	121.248.60.52	POP	60 C: UIDL
121.248.60.52	192.168.1.104	POP	1454 S: +OK 90 2559819
121.248.60.52	192.168.1.104	IMF	1094 mCtgwAcsh , 53 1tbiAgARA1LLpn0ZcwAhsZ , 54 1tbiAgARA1LLpoShnwA
192.168.1.104	121.248.60.52	TCP	54 36980 > pop3 [ACK] Seq=4159500373 Ack=1686757494 Win=65792 Len=0
192.168.1.104	121.248.60.52	POP	60 C: LIST
121.248.60.52	192.168.1.104	POP	922 S: +OK 90 2559819
192.168.1.104	121.248.60.52	POP	60 C: QUIT
121.248.60.52	192.168.1.104	POP	69 S: +OK core mail
192.168.1.104	121.248.60.52	TCP	54 36980 > pop3 [RST, ACK] Seq=4159500385 Ack=1686758377 Win=0 Len=
121.248.60.52	192.168.1.104	TCP	54 pop3 > 36980 [FIN, ACK] Seq=1686758377 Ack=4159500385 Win=5888 L
192.168.1.104	121.248.60.52	TCP	54 36980 > pop3 [RST] Seq=4159500385 Win=0 Len=0

接收邮件代码

```
void GetMail(char *cPOP3Server, char *cUserName, char *cPassword)
{
    WSADATA wsaData;
    SOCKET s;
    sockaddr_in serverAddr;
    int nRet;
    char buf[1024];
    char cCmd[256];

    WSAStartup(MAKEWORD(2,2), &wsaData);

    s = socket(AF_INET, SOCK_STREAM, 0);
    memset(&serverAddr, 0, sizeof(serverAddr));
    serverAddr.sin_family = AF_INET;
    serverAddr.sin_port = htons(110);
    serverAddr.sin_addr.s_addr = inet_addr(cPOP3Server);
    nRet = connect(s, (struct sockaddr *)&serverAddr, sizeof(serverAddr));
    nRet = recv(s, buf, 1024, 0);

    sprintf(cCmd, "USER %s\r\n", cUserName);
    nRet = send(s, cCmd, strlen(cCmd), 0);
    nRet = recv(s, buf, 1024, 0);

    sprintf(cCmd, "PASS %s\r\n", cPassword);
    nRet = send(s, cCmd, strlen(cCmd), 0);
    nRet = recv(s, buf, 1024, 0);

    nRet = send(s, "STAT\r\n", strlen("STAT\r\n"), 0);
```

电子邮件系统安全问题 - 1

- **匿名转发**
  - **邮件没有发件人信息**
  - **发件人刻意隐瞒自己的电子邮箱地址和其他信息，或者通过某些方法给你一些错误的发件人信息**
  - **发送者首先将邮件发送给匿名转发系统，匿名转发邮件系统再把邮件转发给真正的收件者，并将自己的地址作为发信人地址显示在邮件的信息表头中**
- **电子邮件欺骗**
  - **在电子邮件中改变名字，使之看起来是从某地或某人发来的行为**
  - **三种基本方法**
    - **相似的电子邮件地址**
    - **修改邮件客户**
    - **远程联系，登录到端口25，装作是一台邮件服务器**

电子邮件系统安全问题 - 2

- **E-mail炸弹**
  - **发送大量的垃圾邮件，从而充满邮箱，大量的占用了系统的可用空间和资源，使机器暂时无法正常工作**
  - **过多的邮件垃圾会占用大量的CPU时间和网络带宽，加剧网络的负载力和消耗大量的空间资源**
- **安全方案**
  - **PEM**
  - **S/MIME**
  - **PGP**

02
Part

Privacy Enhanced Mail

PEM

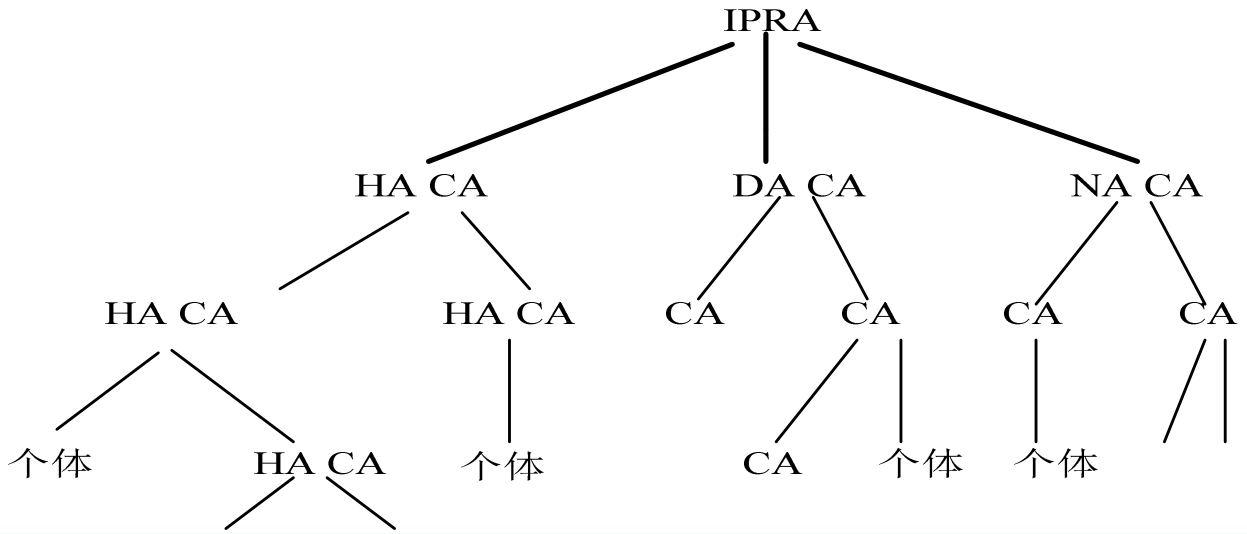
- 保密增强邮件(Privacy Enhanced Mail, PEM)是基于X.509v1 而提出的一个专用于安全E-mail通信的正式因特网标准。
- PEM目的是为了增强个人的隐私功能, 它在电子邮件的标准格式上增加了加密、鉴别和密钥管理的功能, 允许使用公开密钥和专用密钥的加密方式, 并能够支持多种加密工具。
- 在制定PEM的时候，由于MIME标准在当时还并不完善, 所以使用了在RFC934中定义的较老的基于文本的邮件格式。因此，PEM是一个只能够保密文本信息的非常简单的系统, 不适合处理当前多种形式的邮件内容实体

PEM密钥

- PEM 使用两级密钥：数据加密密钥(DEK)和交换密钥（IK）。
- DEK 用来加密消息正文和计算消息集成校验(MIC），同时用来加密 MIC 的签名表示；一般对每个消息都要生成一个随机数作为DEK，从而达到一次性密钥的效果。
- IK是长期密钥，用来加密DEK，以便在每次会话的初始阶段对DEK进行加密交换。

PEM证书分层结构

- **一个简单而又严格的全球认证分级的严格信任模型，需要所有参与认证的个人必须相互认识并予以对方信任，这样的标准对于那些大规模的企业或组织来说难以接受**



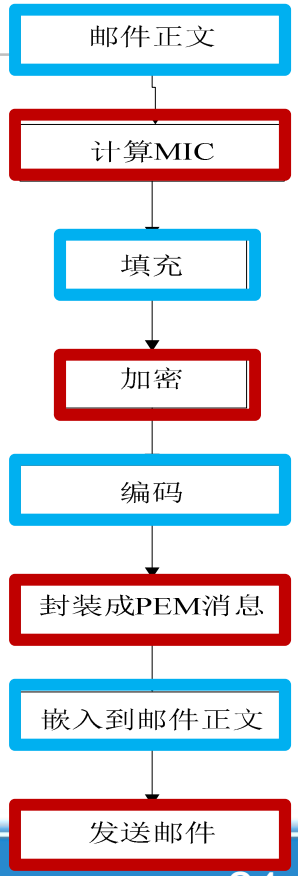
PEM消息

- PEM消息通常只是普通文本邮件消息的一部分。
- 一个邮件消息可以包含由PEM以不同方式处理的多个部分。比如，消息的一部分经过加密，而另一部分经过完整性保护处理。
- PEM在不同的部分开始和结束的地方做上标记，以便接收方对消息的处理。
  - 比如，对加密的数据块，PEM会在数据开始出插入文本串

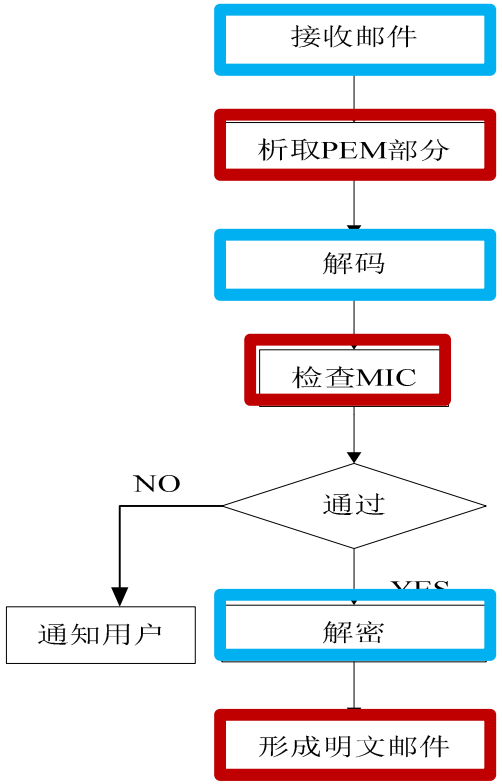
  -----BEGIN PRIVACY-ENHANCED MESSAGE-----
  - 并在数据块结束处插入

  ----- END PRIVACY-ENHANCED MESSAGE-----

PEM邮件处理



(a)PEM邮件加密和签名



(b)PEM邮件接收和验证

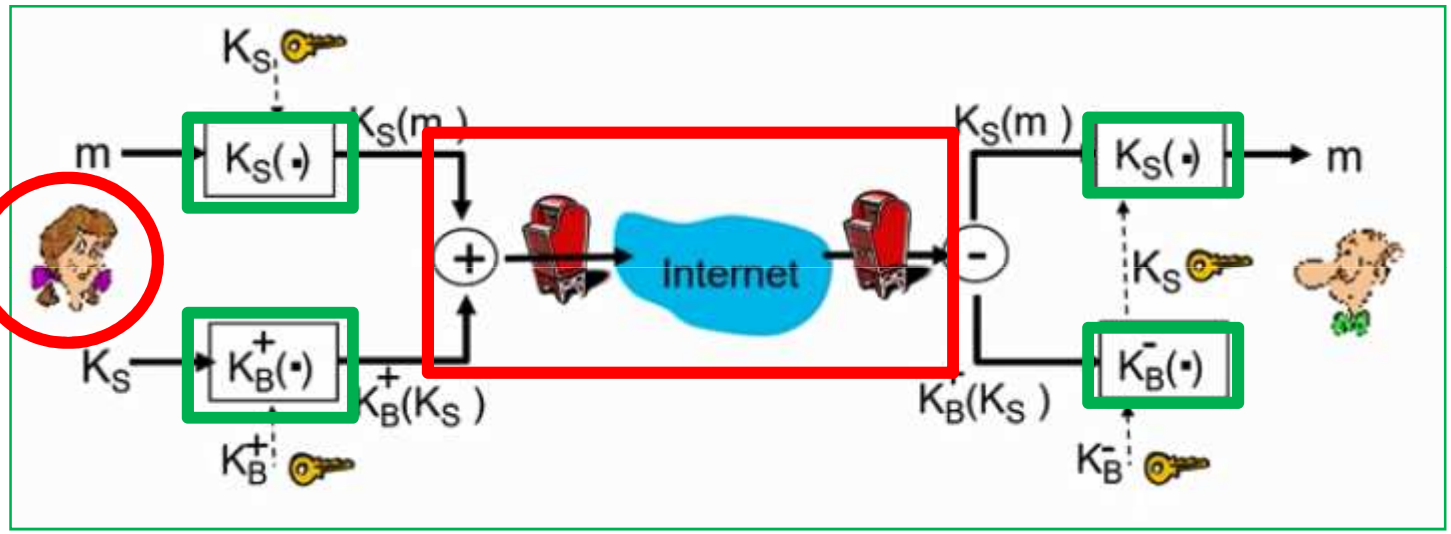
03
Part

PGP

背景

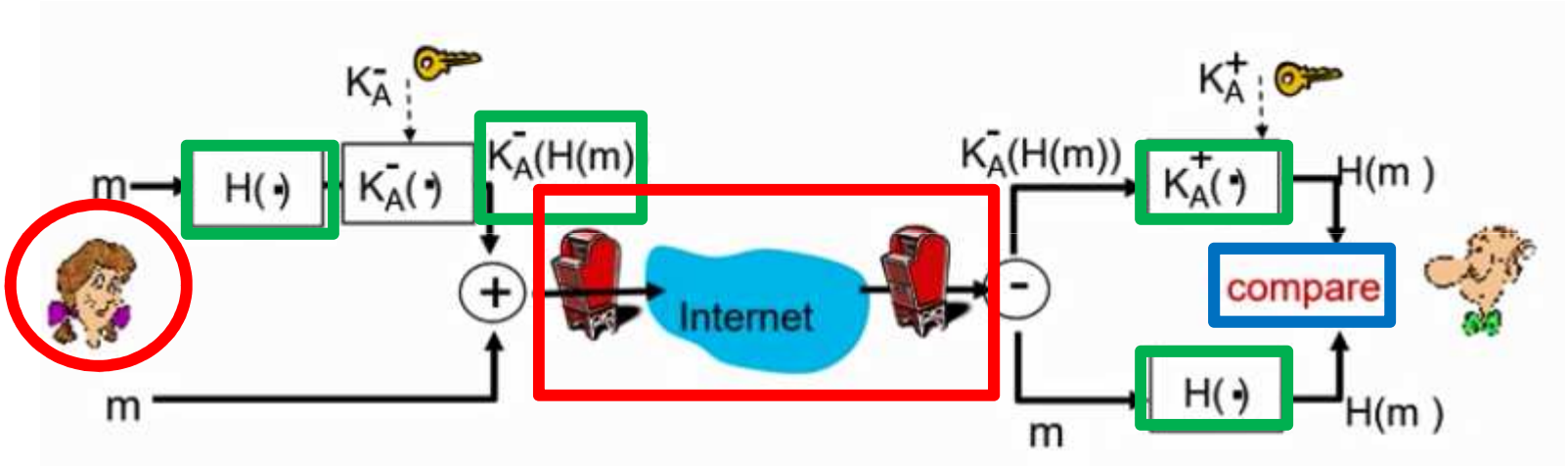
- Alice想要给Bob发一封封保密信息m
  - 保证机密性
- Alice:
  - 随机生成共享密钥Ks
  - 用Ks给信息m加密
  - 同时用Bob的公钥加密共享密钥Ks
  - 把Ks(m)和K_B^+(Ks)同时发给Bob

保密电子邮件

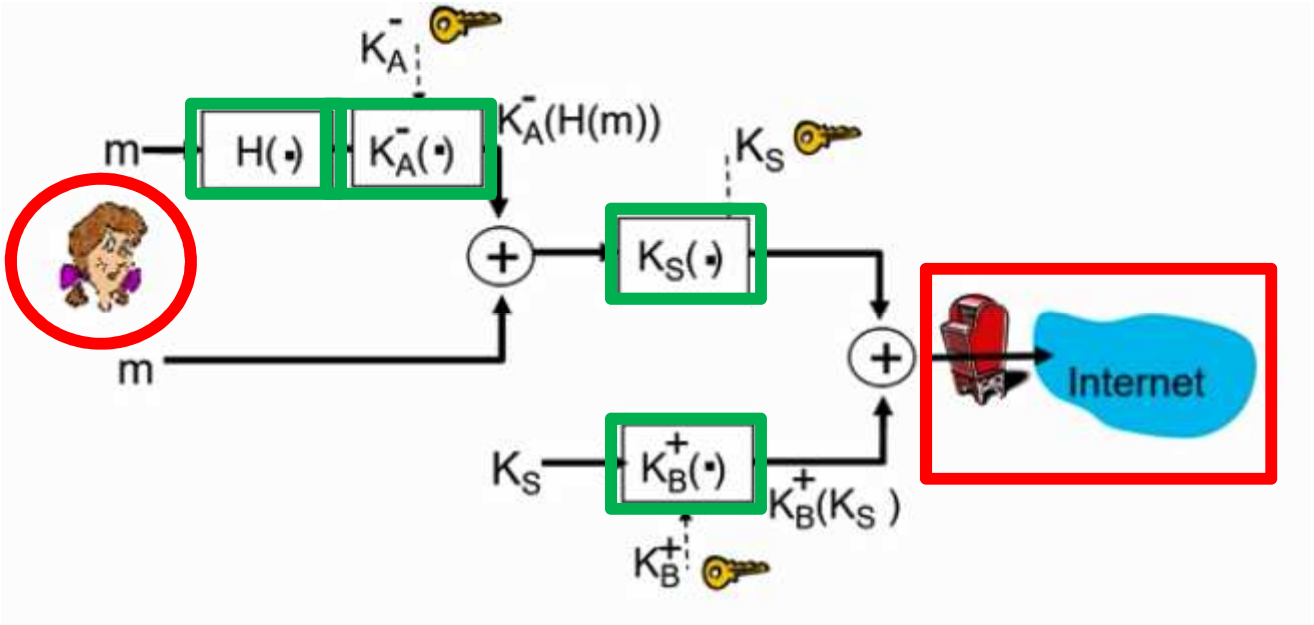

K_S
$K_S(m)$
m
$K_S(\cdot)$
K_S
$K_B^+(\cdot)$
$K_B^+(K_S)$
K_B^+
internet
$K_S(m)$
$K_S(\cdot)$
m
K_S
$K_B^-(\cdot)$
$K_B(K_S)$
K_B^-

认证电子邮件

- **Alice希望证明自己是真正的发出方，以及确保信息的完整性**



电子邮件安全PGP



8.1 PGP(Pretty Good Privacy)

- 提供可用于电子邮件和文件存储应用程序的
- 由Phil Zimmermann开发

  选择最佳可用加密算法作为构建数据块。

  将这些算法集成到一个独立于操作系统和处理器的
  只依赖于一小组易用的命令集。

  将其封装成源代码的包及其文档，可通过Internet
  上免费使用。

  与一家公司签订协议，提供完全兼容，低成本的PG

PGP的成长

- 它在全球范围内免费提供，可在各种平台上运行
- 商业版本的用户可以得到销售商的技术支持
- 它基于经过广泛的公众审查而被认为非常安全的算法
- 它具有广泛的适用性
- 它不是由任何政府或标准组织开发的，也不是由它控制的
- 现在已经成为互联网标准文档

8.1.1 符号约定

- Ks -- 用于对称加密体制中的会话密钥
- PR_a- -用户A的私钥，用于私钥加密体制
- PU_a- -用户A的公钥，用于公钥加密体制
- E_P - -公钥加密
- D_P - -公钥解密
- E_C - - 对称加密
- D_C - - 对称解密
- H - - - 散列函数
- || - - - 串接
- Z - - - 用ZIP算法压缩
- R64 - -转换为基-64的ASCII格式

8.1.2 操作描述

- 与密钥管理相对应，PGP的实际操作包括四种服务：
  - 1. 认证
  - 2. 保密
  - 3. 压缩
  - 4. 电子邮件兼容性

PGP服务概述

	采用算法	说明
数字签名（包含鉴别）	DSS/SHA或RSA/SHA	用SHA-1创建散列码，用发送者的私钥和DSS或RSA加密消息摘要
消息加密	CAST或IDEA或3DES、AES及RSA或D-F	消息用一次性会话密钥加密，会话密钥用接收方的公钥加密
压缩	ZIP	消息用ZIP算法压缩
邮件兼容性	Radix 64	邮件应用完全透明，加密后的消息用Radix 64转换
数据分段		为了适应邮件的大小限制，PGP支持分段和重组

PGP的功能

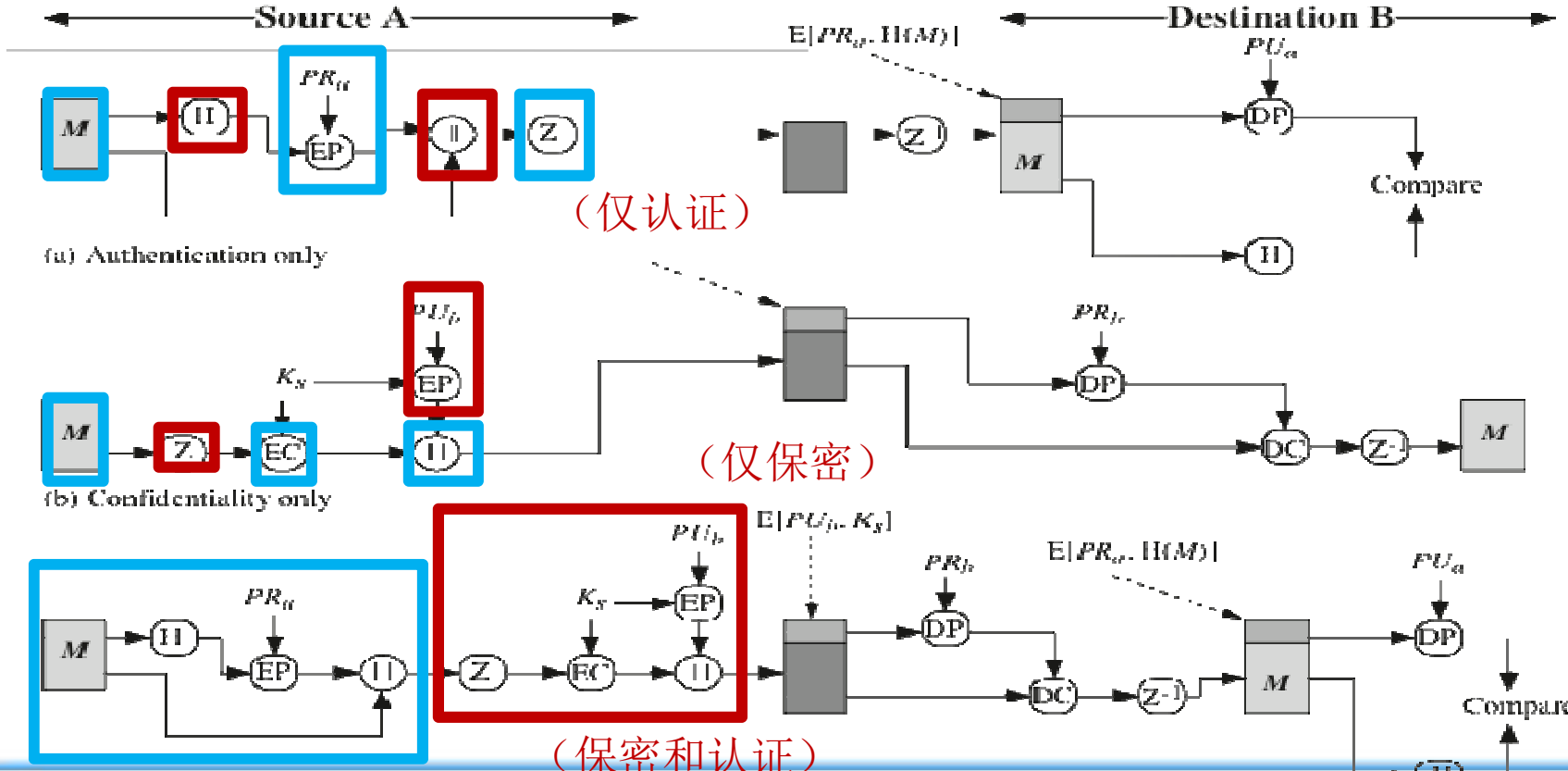
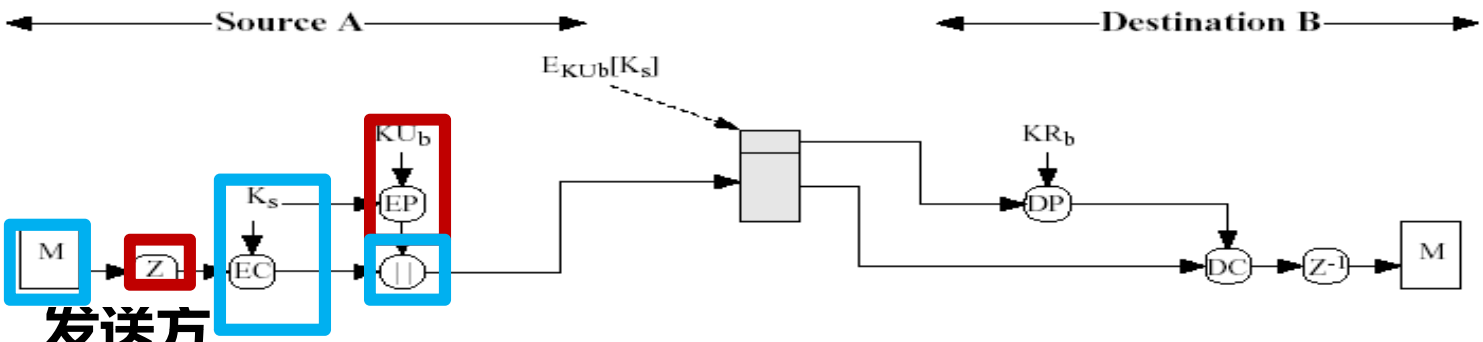


Figure 8.1 PGP Cryptographic Functions

PGP机密性

- 通过对要发送的消息或要在本地存储的文件进行加密来实现保密服务
  - 在两种情况下，可以使用对称加密算法CAST-128
  - 也可以使用IDEA或3DES
  - 使用64位密码反馈（CFB）模式
- 在PGP中，每个对称密钥仅使用一次
  - 虽然称为会话密钥，但它实际上是一次性密钥
  - 会话密钥绑定到消息并与其一起传输
  - 为了保护密钥，它使用接收者的公钥加密
- 作为使用RSA进行密钥加密的替代方案，PGP使用ElGamal，它是Diffie-Hellman的一种变体，提供加密/解密

PGP 机密性



- **发送方**
  - **生成消息M并为该消息生成一个随机数作为会话密钥**
  - **用会话密钥加密M**
  - **用接收者的公钥加密会话密钥并与消息M结合**
- **接收方**
  - **用自己的私钥解密恢复会话密钥**
  - **用会话密钥解密恢复消息M**

PGP认证

- **SHA-1和RSA的组合提供了有效的数字签名方案**

  由于RSA的强度，接收者可以确保只有匹配私钥的拥有者才能生成签名

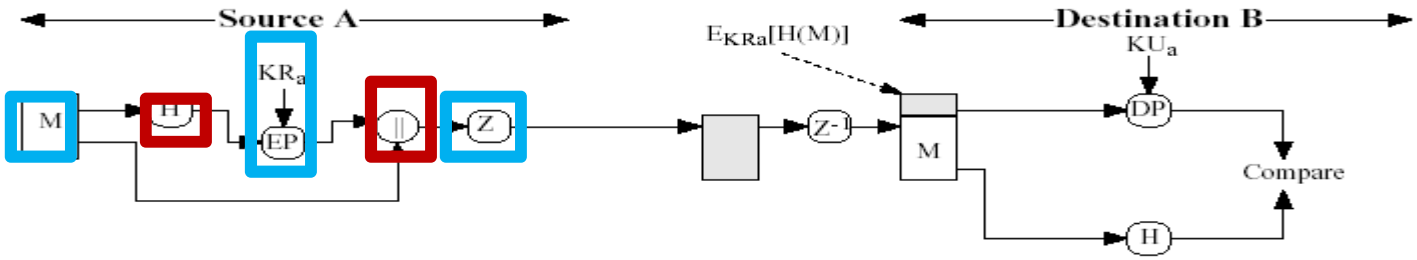
  由于SHA-1的强大，接收者可以确保没有其他人可以生成与哈希码匹配的新消息

  作为替代方案，可以使用DSS / SHA-1生成签名

  支持分离的签名

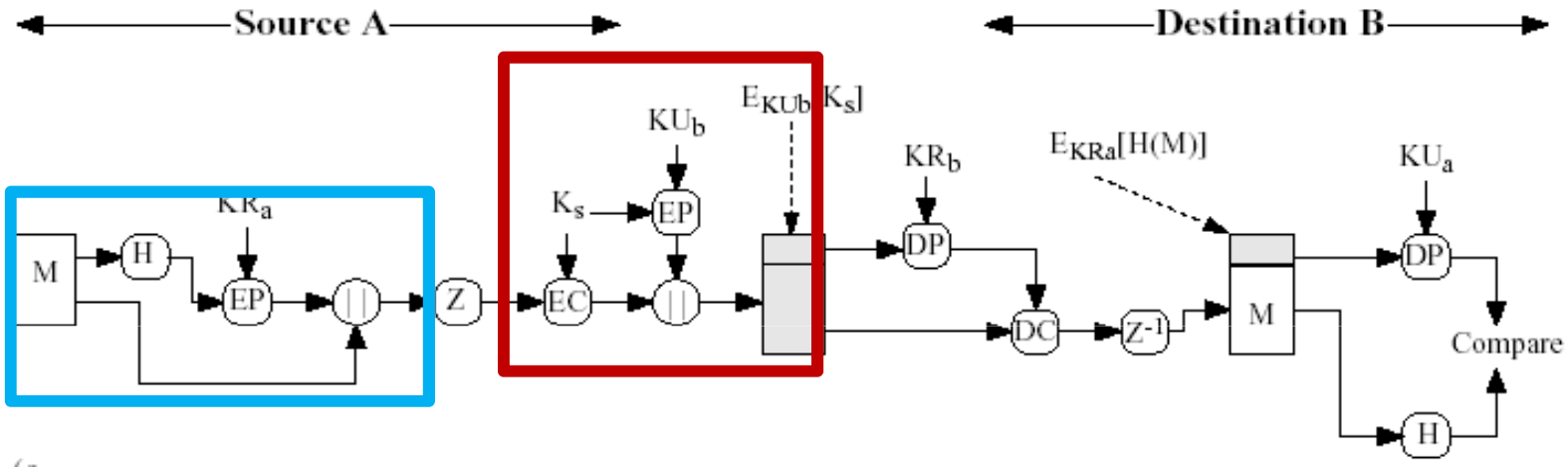
  每个人的签名都是独立的，因此签名仅适用于该文档

PGP身份认证



- **发送方**
  - **产生消息M**
  - **用SHA-1对M生成一个160位的散列码H**
  - **用发送者的私钥对H加密，并与M连接**
- **接收方**
  - **用发送者的公钥解密并恢复散列码H**
  - **对消息M生成一个新的散列码，与H比较。如果一致，则消息M被认证**

PGP保密与认证



- **两种服务都需要时，发送者先用自己的私钥签名，然后用会话密钥加密消息，再用接收者的公钥加密会话密钥**

PGP压缩

- **PGP在应用签名之后、加密之前要对消息进行压缩**
  - **使用的压缩算法是ZIP**
  - **压缩对邮件传输或存储都有节省空间的好处**
- **签名后压缩**
  - **不需要为检验签名而保留压缩版本的消息**
  - **为了检验而再做压缩不能保证一致性，压缩算法的不同实现版本可能会产生不同的结果**
- **压缩后加密**
  - **压缩后的消息其冗余小，增加密码分析的难度**
  - **若先加密，则压缩难以见效**

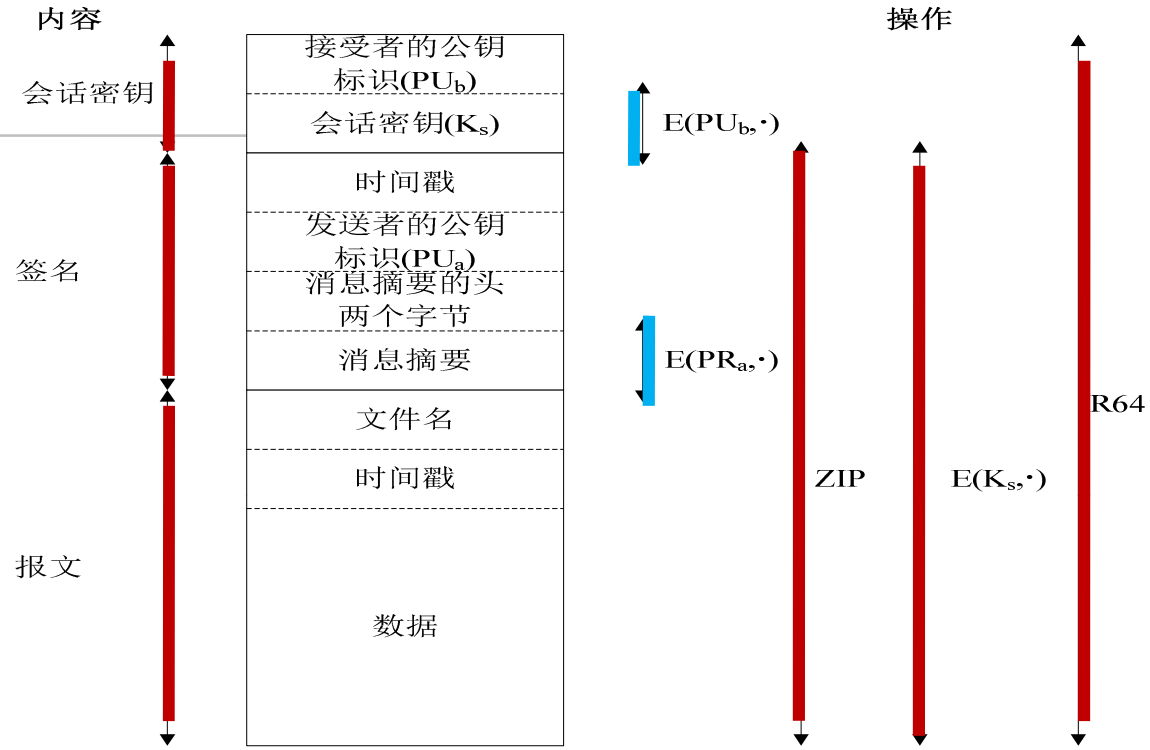
PGP密钥

- PGP使用四种类型的密钥
  - 一次性会话传统密钥
  - 公钥
  - 私钥
  - 基于口令短语的传统密钥
- PGP对密钥的需求
  - 会话密钥
    - 需要一种生成不可预知的会话密钥的方法，PGP使用了一种复杂的随机密钥生成算法(一定的真随机性)
  - 公钥和私钥
    - 需要某种手段来标识具体的密钥
    - 一个用户拥有多个公钥/私钥对
    - 密钥更新管理
  - 每一个用户都要维护通信必须的密钥对
    - 用一个文件来维护自身的公钥/私钥对
    - 用另一个文件维护其他用户的公钥信息

密钥标识符

- **一个用户有多个公钥/私钥对**
  - **接收者如何知道发送者是用哪个公钥来加密会话密钥的？**
  - **解决方法**
    - **将公钥与消息一起传送：开销太大**
    - **为每个公钥分配一个标识符，传输时将标识符与消息一块传送**
- **密钥标识符**
  - **对每个用户，每个公钥与唯一的KeyID相关联**
  - **发送方必须容易了解一个公钥在其所有者上分配的KeyID**
  - **PGP采用公钥的低64位作为KeyID**
  - **数字签名也需要使用KeyID**
    - **接收方需要确定使用发送方的那一个公钥验证签名**

PGP消息



注：

$E(PU_b,\cdot)$ ——用用户b的公钥加密

$E(PR_a,\cdot)$ ——用用户a的公钥加密

$E(K_s,\cdot)$ ——用会话密钥加密

ZIP ——Zip压缩函数

R64 ——基数64的转换函数

密钥环

- KeyID对于PGP非常关键
  - PGP消息中包括两个keyID，分别提供保密与认证功能。
  - 需要一种系统化的方法存储和组织这些密钥以保证有效使用这些密钥
- 在每一个用户节点上设置数据结构，管理用户密钥，称为密钥环
  - 私钥环：存储本节点拥有的公钥/私钥对
  - 公钥环：存储本节点所知道的其他用户的公钥
- 密钥环实际上是一个保存密钥的列表
  - 密钥数据库
  - 每一表项保存一个用户密钥

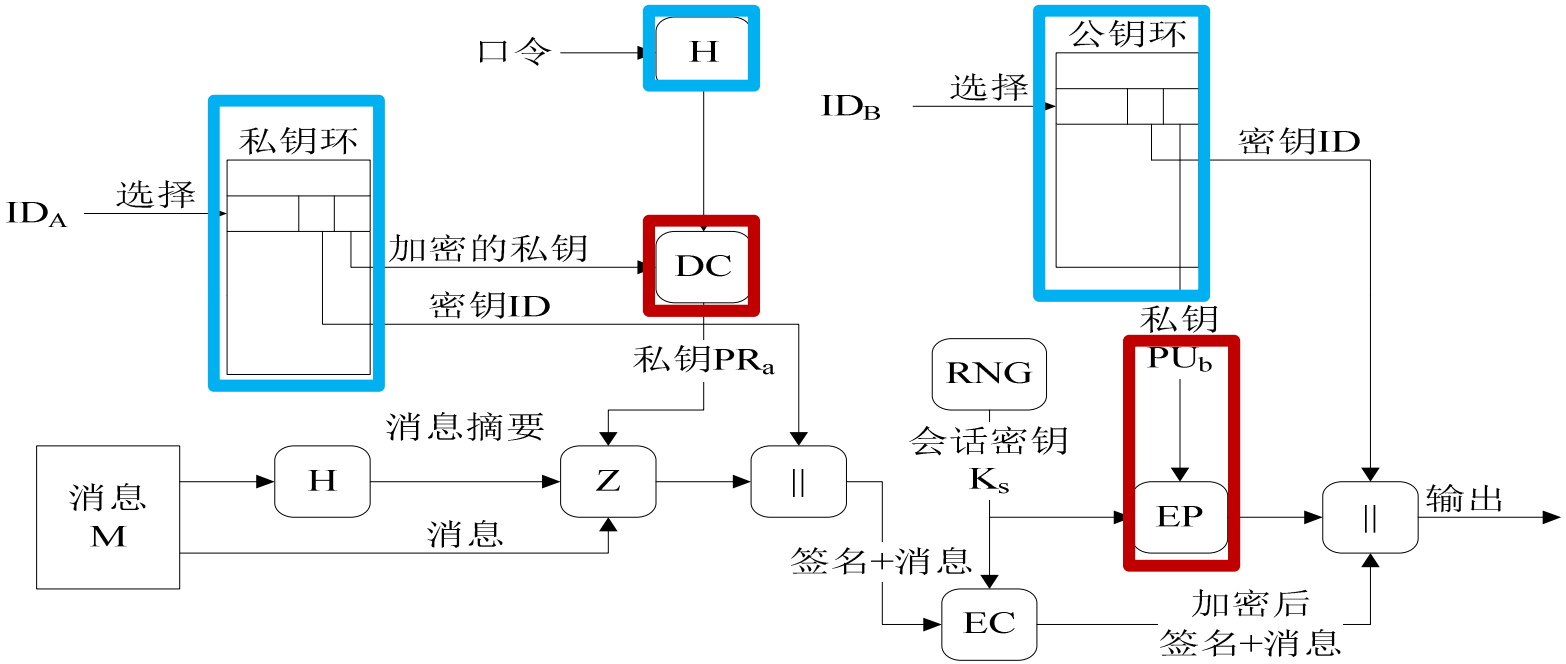
PGP私钥环

- 信息
  - 时间戳、KeyID、公钥、私钥、UserID
- UserID
  - 通常是用户的邮件地址
  - 也可以是一个名字，可以重名
- 私钥如何保存
  - 用户选择一个口令短语用于加密私钥
  - 当系统用RSA生成一个新的公钥/私钥对时，要求用户输入口令短语。对该短语使用SHA-1生成一个160位的散列码后，销毁该短语
  - 系统用其中128位作为密钥用CAST-128加密私钥，然后销毁这个散列码，并将加密后的私钥存储到私钥环中
  - 当用户要访问私钥环中的私钥时，必须提供口令短语。PGP将取出加密后的私钥，生成散列码，解密私钥

PGP公钥环

- **信息**
  - **时间戳、KeyID、公钥、对所有者信任度、用户ID、密钥合法度、签名、对签名者信任度**
- **UserID**
  - **公钥的拥有者**
  - **多个UserID可以对应一个公钥**
- **公钥环可以用UserID或KeyID索引**

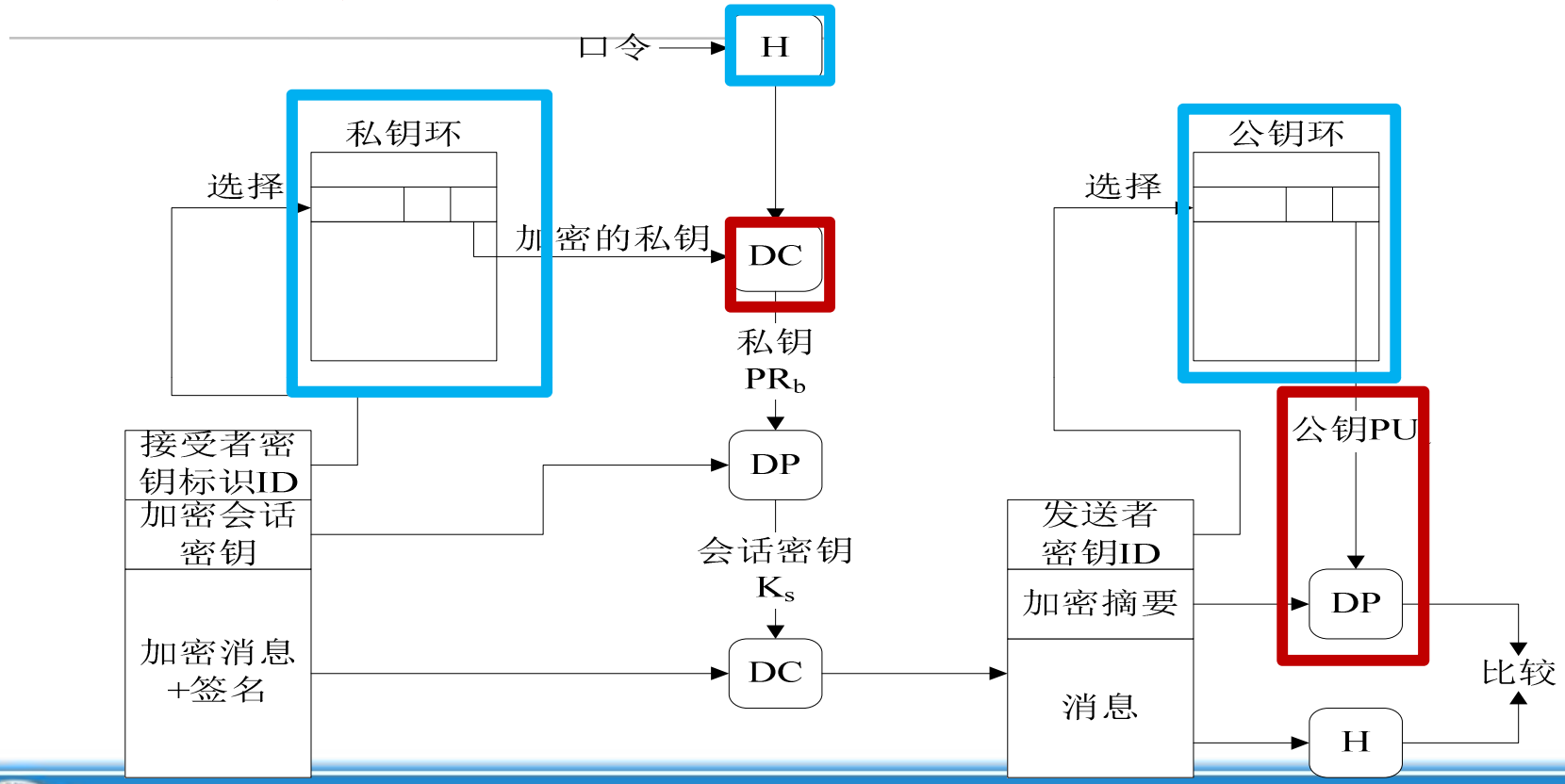
PGP消息生成


口令
H
公钥环
ID_B
选择
密钥ID
私钥环
ID_A
选择
加密的私钥
DC
密钥ID
私钥
PU_b
私钥PR_a
RNG
消息摘要
会话密钥
K_s
消息
M
H
Z
||
EP
||
输出
消息
签名+消息
EC
加密后
签名+消息

发送方处理消息的过程

- **签名**
  - **从私钥环中得到私钥，利用userid作为索引**
  - **PGP提示输入口令短语，恢复私钥**
  - **构造签名部分**
- **加密**
  - **PGP产生一个会话密钥，并加密消息**
  - **PGP用接收者userid从公钥环中获取其公钥**
  - **构造消息的会话密钥部分**

PGP消息接收


口令
H
私钥环
选择
加密的私钥
DC
私钥
PR_b
接受者密钥标识ID
加密会话密钥
DP
会话密钥
K_s
加密消息+签名
DC
公钥环
选择
公钥PU
发送者密钥ID
加密摘要
DP
比较
消息
H

接收方处理消息的过程

- **解密消息**
  - **PGP用消息的会话密钥部分中的KeyID作为索引，从私钥环中获取私钥**
  - **PGP提示输入口令短语，恢复私钥**
  - **PGP恢复会话密钥，并解密消息**
- **验证消息**
  - **PGP用消息的签名部分中的KeyID作为索引，从公钥环中获取发送者的公钥**
  - **PGP恢复被传输过来的消息摘要**
  - **PGP对于接收到的消息作摘要，并与上一步的结果作比较**

PGP公钥管理

- PGP没有建立严格的公钥管理模式
  - 重在广泛地在正式或非正式环境下的应用
- 有关的问题
  - 私钥泄漏
    - 别人可以伪造你的签名
    - 其他人发送给你的保密信件可被别人读取
  - 防止公钥环上包含错误的公钥
- 保证公钥环上公钥的正确性
  - 物理方式得到其他用户的公钥：可靠，但有一定局限性
  - 通过电话验证公钥
  - 从双方都信任的个体D处获得其他用户的公钥
  - 从一个信任的CA中心得到其他用户的公钥

PGP公钥信任模型

- PGP利用信任关系管理公钥
  - 每一个公钥都与一个信任度相关联
  - A的公钥环中某公钥K_{UB}信任度越高，则A就可以越相信K_{UB}是B的公钥
- 信任度
  - 密钥合法性（Key legitimacy）
    - 由PGP计算
    - 表明PGP对“此用户公钥是合法的”的信任程度；信任级别越高，公钥的可信度就越高
  - 签名信任度（Signature Trust）
    - 用于计算密钥合法性
    - 公钥环中的每一个公钥项都有若干个介绍人的签名，每一个签名与一个签名信任度关联，表明这个PGP用户对签名的信任程度
  - 拥有者信任度（Owner Trust）
    - 由用户给出
    - 表明用户A对公钥K_{Ui}的拥有者i的信任程度
    - 当i用K_{Ui}生成其它公钥证书的签名时，A对该签名的信任程度等于KUi拥有者信任度

PGP公钥的注销

- **公钥注销功能的必要性：密钥暴露或定时更新**
- **通常的注销途径是由私钥主人签发一个密钥注销证书**
  - **私钥主人应尽可能越广越快散布这个证书，以使得潜在的有关人员更新他们的公钥环**
  - **对应的私钥必须用来签名该密钥报废证书，否则其他人无法验证其真伪**

PGP证书管理软件

- **PGP证书管理软件 —— 服务器软件**
- **集中管理PGP公钥证书**
- **提供LDAP、HTTP服务**
- **本地密钥环可以实时地连接到服务器，适合于企业使用**
  - **更新老的证书**
  - **查找新的证书**
  - **查询CRL**

PGP E-mail兼容性

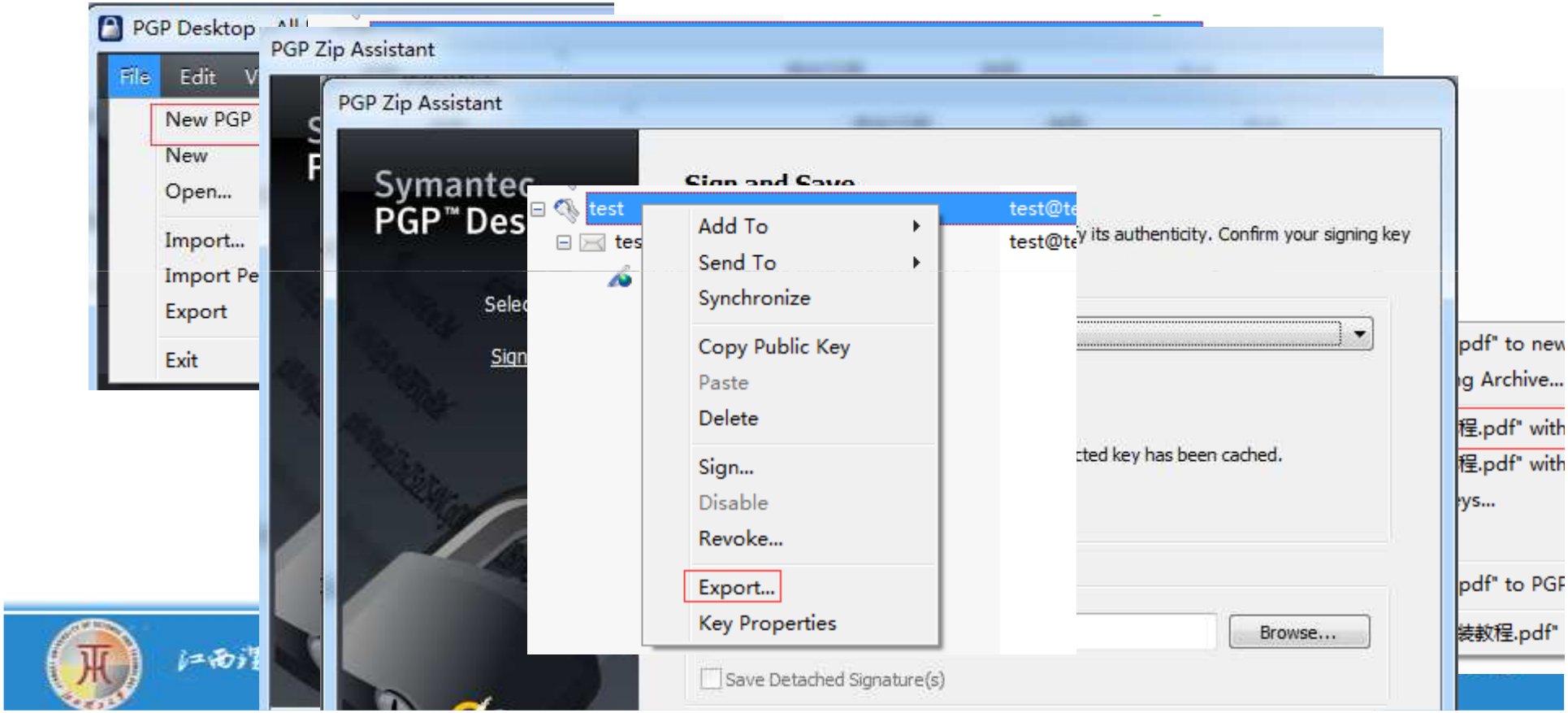
- **许多电子邮件系统仅允许使用由ASCII文本组成的块**

  为了适应这种限制，PGP提供了将原始8位二进制流转换为可打印ASCII字符流的服务

  用于此目的的方案是Radix-64转换

  - **每组三个八位字节的二进制数据被映射为四个ASCII字符**
  - **该格式还附加CRC以检测传输错误**

实例


PGP Desktop
File
Edit
New PGP
New
Open...
Import...
Import Pe
Export
Exit
PGP Zip Assistant
PGP Zip Assistant
Symantec
PGP™ Des
Sign and Save
test
test@te
Add To
Send To
Synchronize
Copy Public Key
Paste
Delete
Sign...
Disable
Revoke...
Export...
Key Properties
its authenticity. Confirm your signing key
cted key has been cached.
Browse...
Save Detached Signature(s)
pdf" to new
g Archive...
程.pdf" with
程.pdf" with
ys...
pdf" to PGP
装教程.pdf"

04
Part

S / MIME

8.2 S / MIME （安全/多用途网际邮件扩展）

- S / MIME是基于RSA 数据安全性，对互联网电子邮件格式标准MIME的安全性增强
- 定义于

  RFCs 3370, 3850, 3851, 3852

8.2.1 RFC 5322

- 定义使用电子邮件发送的文本消息的格式
- 消息包含信封和内容两部分

  信封包含完成传输和传递所需的任何信息

  内容是指要发送给收件人的对象

  RFC 5322标准仅适用于内容
- 内容标准包括一组标题字段，邮件系统可以使用这些标题字段来创建信封

8.2.2 多用途网际邮件扩展(MIME)

- **多用途网际邮件扩展(MIME) 是对RFC 5322框架的扩展，旨在解决使用简单邮件传输协议（SMTP）的一些问题和限制**

  旨在以与现有RFC 5322实现兼容的方式解决这些问题

  该规范在RFC 2045至2049中提供

  MIME规范包括以下元素：

定义了五个新的报头域，它们可以包含在**RFC 5322**头中; 这些字段提供有关邮件正文的信息

定义了许多内容格式，从而标准化了支持多媒体电子邮件的表示

定义了转移编码，使得能够将任何内容格式转换为受邮件系统保护以免被更改的形式

MIME中定义的五个报头域

MIME-版本

- 必须具有参数值1.0
- 该字段指示该消息符合RFC 2045和2046

内容类型

- 描述主体中包含的数据，其中包含足够的详细信息，使得用户代理可以选择适当的代理或机制来向用户表示数据或以适当的方式处理数据

内容传输编码

- 将消息正文转换为可传输类型的转换方式

内容ID

- 用于在多个上下文中唯一标识MIME实体

内容描述

- 正文对象的文字描述; 当正文对象不可读时（如音频数据）时使用

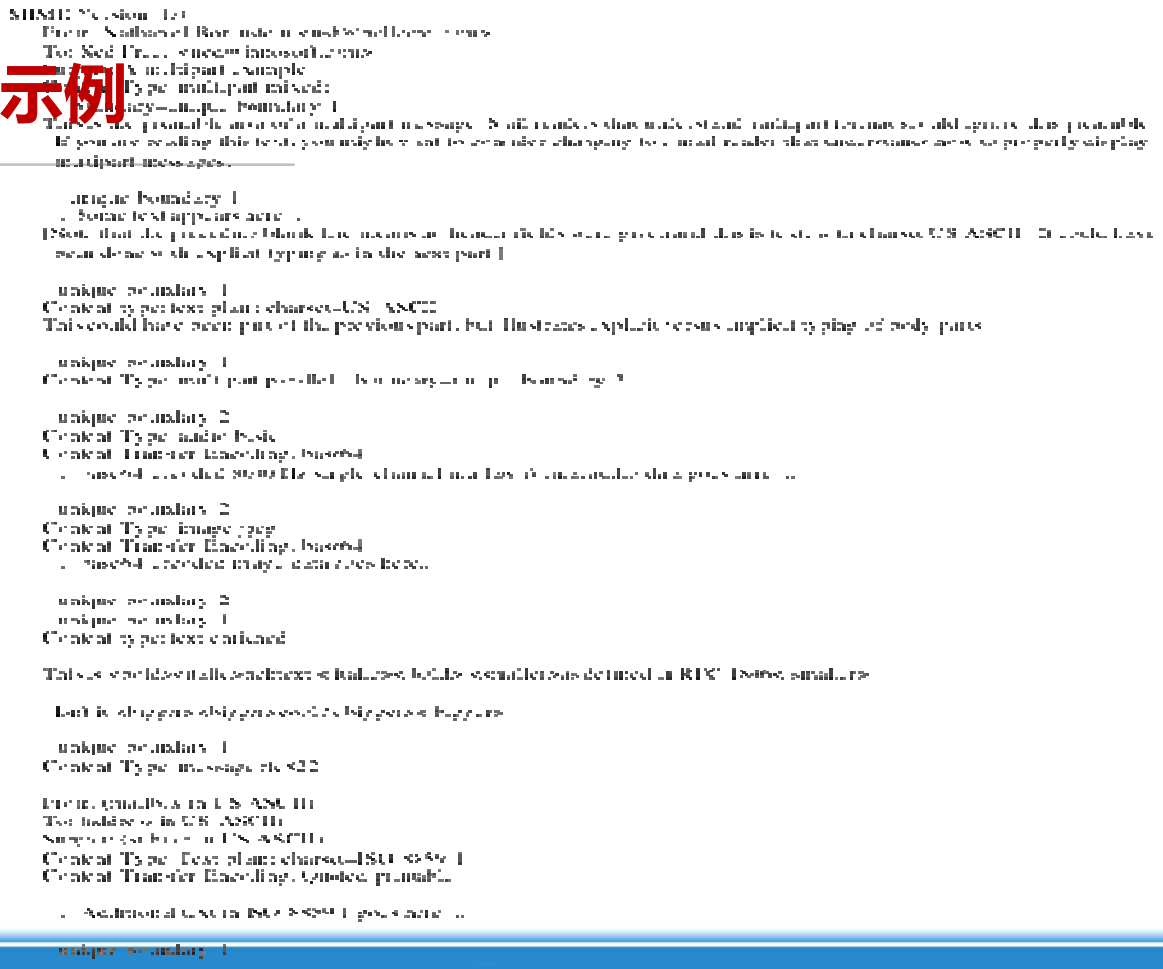
MIME内容类型

Type	Subtype	Description
Text	Plain	Unformatted text; may be ASCII or ISO 8859.
	Enriched	Provides greater format flexibility.
Multipart	Mixed	The different parts are independent but are to be transmitted together. They should be presented to the receiver in the order that they appear in the mail message.
	Parallel	Differs from Mixed only in that no order is defined for delivering the parts to the receiver.
	Alternative	The different parts are alternative versions of the same information. They are ordered in increasing faithfulness to the original, and the recipient's mail system should display the "best" version to the user.
	Digest	Similar to Mixed, but the default type/subtype of each part is message/rfc822.
Message	rfc822	The body is itself an encapsulated message that conforms to RFC 822.
	Partial	Used to allow fragmentation of large mail items, in a way that is transparent to the recipient.
	External-body	Contains a pointer to an object that exists elsewhere.
Image	jpeg	The image is in JPEG format, JFIF encoding.
	gif	The image is in GIF format.
Video	mpeg	MPEG format.
Audio	Basic	Single-channel 8-bit ISDN mu-law encoding at a sample rate

表 8.3 MIME传输编码

7bit	The data are all represented by short lines of ASCII characters.
8bit	The lines are short, but there may be non-ASCII characters (octets with the high-order bit set).
binary	Not only may non-ASCII characters be present but the lines are not necessarily short enough for SMTP transport.
quoted-printable	Encodes the data in such a way that if the data being encoded are mostly ASCII text, the encoded form of the data remains largely recognizable by humans.
base64	Encodes data by mapping 6-bit blocks of input to 8-bit blocks of output, all of which are printable ASCII characters.
x-token	A named nonstandard encoding.

8.3 MIME消息结构示例



本地格式和规范格式

Native Form	The body to be transmitted is created in the system's native format. The native character set is used and, where appropriate, local end-of-line conventions are used as well. The body may be a UNIX-style text file, or a Sun raster image, or a VMS indexed file, or audio data in a system-dependent format stored only in memory, or anything else that corresponds to the local model for the representation of some form of information. Fundamentally, the data is created in the "native" form that corresponds to the type specified by the media type.
Canonical Form	The entire body, including "out-of-band" information such as record lengths and possibly file attribute information, is converted to a universal canonical form. The specific media type of the body as well as its associated attributes dictate the nature of the canonical form that is used. Conversion to the proper canonical form may involve character set conversion, transformation of audio data, compression, or various other operations specific to the various media types. If character set conversion is involved, however, care must be taken to understand the semantics of the media type, which may have strong implications for any character set conversion (e.g. with regard to syntactically meaningful characters in a text subtype other than "plain").

8.2.3 S/MIME的功能

S/MIME

封装数据

- 由各种类型的加密内容和接收者用于加密内容的一个或多个密钥组成

签名数据

- 通过获取要签名内容的消息摘要，并用签名者的私钥加密得到数字签名。然后使用**base64**编码对内容加签名进行编码签名数据邮件只能由收件人查看**S/MIME capability**

透明签名数据

- 只使用**base64**编码数字签名
- 因此，没有**S / MIME**功能的收件人可以查看邮件内容，尽管他们无法验证签名

签名并封装数据

- 只有签名和加密的实体可以嵌套，这样以便对加密的数据进行签名，对签名的数据或透明签名的数据进行加密

S/MIME中使用的加密算法

Function	Requirement
Create a message digest to be used in forming a digital signature.	MUST support SHA-1. Receiver SHOULD support MD5 for backward compatibility.
Encrypt message digest to form a digital signature.	Sending and receiving agents MUST support DSS. Sending agents SHOULD support RSA encryption. Receiving agents SHOULD support verification of RSA signatures with key sizes 512 bits to 1024 bits.
Encrypt session key for transmission with a message.	Sending and receiving agents SHOULD support Diffie-Hellman. Sending and receiving agents MUST support RSA encryption with key sizes 512 bits to 1024 bits.
Encrypt message for transmission with a one-time session key.	Sending and receiving agents MUST support encryption with tripleDES Sending agents SHOULD support encryption with AES. Sending agents SHOULD support encryption with RC2/40.
Create a message authentication code	Receiving agents MUST support HMAC with SHA-1. Sending agents SHOULD support HMAC with SHA-1.

8.2.4 S/MIME消息

- **表 8.6 S/MIME内容类型**

Type	Subtype	smime Parameter	Description
Multipart	Signed		A clear-signed message in two parts: one is the message and the other is the signature.
Application	pkcs7-mime	signedData	A signed S/MIME entity.
	pkcs7-mime	envelopedData	An encrypted S/MIME entity.
	pkcs7-mime	degenerate signedData	An entity containing only public-key certificates.
	pkcs7-mime	CompressedData	A compressed S/MIME entity.
	pkcs7-signature	signedData	The content type of the signature subpart of a multipart/signed message.

1. 保护MIME实体

- S / MIME使用签名，加密或两者来保护MIME实体
- MIME实体将按照MIME消息准备常规规则进行准备工作。

  将MIME实体和一些与安全相关的数据（如算法标识符和证书)一起用S/MIME处理，以生成所谓的PKCS对象

  然后将PKCS对象视为消息内容封装到MIME中
- 在所有情况下，要发送的消息都将转换为规范形式

2. 封装数据

- **准备封装数据 MIME实体的步骤如下：**

为特定的对称加密算法生成伪随机会话密钥

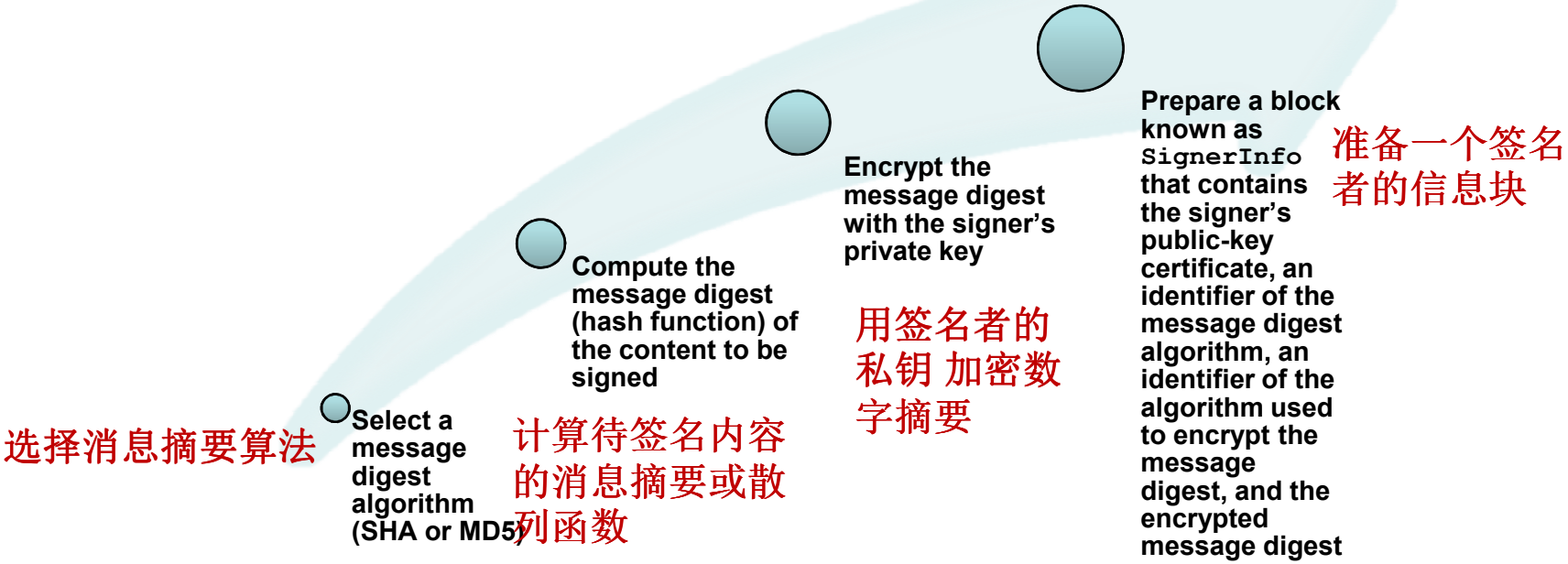
对于每个收件人，使用收件人的**RSA**公钥加密会话密钥

为每个收件方准备一个接收方信息块，其中包含收件人的公钥证书的标识符，用于加密会话密钥的算法的标识以及加密的会话密钥

使用会话密钥加密邮件内容

3. 签名数据

- **MIME实体准备签名数据的步骤如下：**



4. 透明签名

- 透明签名在对多部分内容类型的子类型签名时使用
- 此签名过程不涉及对签名的消息的转换
- 具有MIME能力而不具有S/MIME能力的收件人也能够读取传来的消息

8.2.5 S/MIME证书处理过程

- **S / MIME使用符合X.509第3版的公钥证书**
- **S / MIME使用的密钥管理方案在某种程度上是严格的X.509认证层次结构和PGP的基于Web信任方式的一种混合方式**
- **S / MIME管理者和/或用户必须为每个客户端配置可信任密钥列表和证书撤销列表**

  验证收到的签名和对输出消息的签名工作都是通过在本地维护证书实现的。
- **证书由认证机构颁发**

用户代理职责

- **一个S/MIME用户需要执行若干密钥管理职能**

密钥生成

与一些管理机构相关的用户必须能够生成单独的**Diffie-Hellman**和**DSS**密钥对，并且应该能够生成**RSA**密钥对

用户代理应生成长度在**768**到**1024**位范围内的**RSA**密钥对，并且不得生成小于**512**位的长度

注册

为获得**X.509**公钥证书，用户的公钥必须到认证机构注册

证书存储和检索

为验证接收到的签名和加密输出消息，用户需要访问本地证书列表

VeriSign证书

- VeriSign提供与S/MIME应用兼容的一种认证授权服务
- 颁发名为VeriSign Digital ID的X.509证书
- 每个数字身份证(Digital ID)至少包含：

  所有者的公钥

  所有者的名字或别名

  Digital ID的有效期

  Digital ID的序列号

  颁发Digital ID的认证中心名

  颁发Digital ID的认证中心的数字签名

表 8.7 VeriSign公钥证书类型

	Class 1	Class 2	Class 3
Summary of Confirmation of Identity	Automated unambiguous name and e-mail address search.	Same as Class 1, plus automated enrollment information check and automated address check.	Same as Class 1, plus personal presence and ID documents plus Class 2 automated ID check for individuals; business records (or filings) for organizations.
IA Private Key Protection	PCA: trustworthy hardware; CA: trustworthy software or trustworthy hardware.	PCA and CA: trustworthy hardware.	PCA and CA: trustworthy hardware.
Certificate Applicant and Subscriber Private Key Protection	Encryption software (PIN protected) recommended but not required.	Encryption software (PIN protected) required.	Encryption software (PIN protected) required; hardware token recommended but not required.
Applications Implemented or Contemplated by Users	Web-browsing and certain e-mail usage.	Individual and intra- and inter-company e-mail, online subscriptions, password replacement, and software validation.	E-banking, corp. database access, personal banking, membership-based online services, content integrity services, e-commerce server, software validation; authentication of LRAAs; and strong encryption for certain servers.

IA 发证机构
CA 认证机构
PCA VeriSign公用的基本认证机构
PIN 个人识别码
LRAA 本地注册授权管理员

8.2.6 增强的安全服务

- **互联网草案中提出了三项增强的安全服务：**

签收

- 返回一条签收消息，告知消息的发送方已经收到消息，并通知发送方第三方收件人已收到邮件。

安全标签

- 安全标签是描述被S/MIME封装信息的敏感度的安全信息集合。

安全邮件列表

- S / MIME邮件列表代理（MLA）可以接收单个传入邮件，为各接收方进行相应的加密处理，并自动发送邮件

05
Part

DKIM（域名密钥识别邮件）

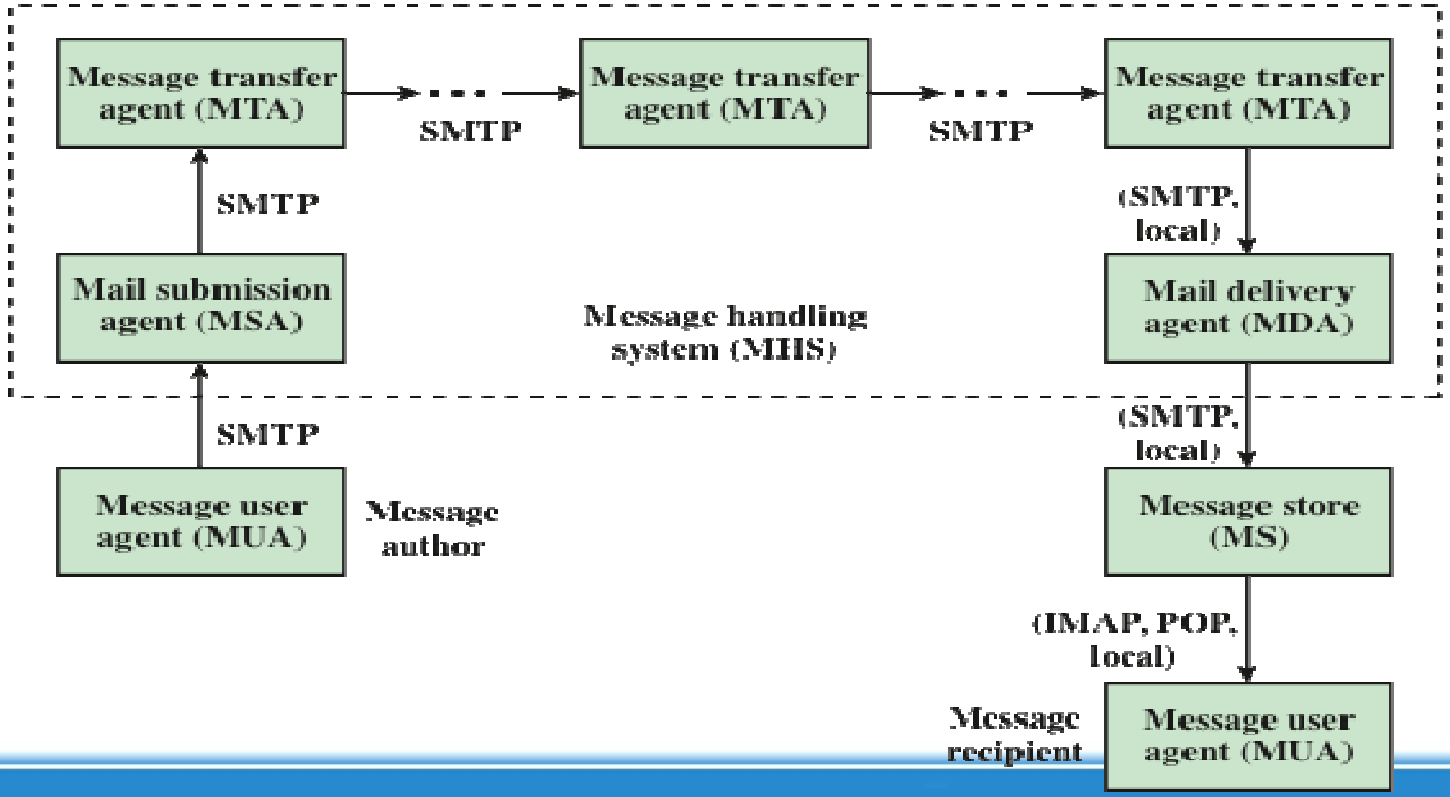
8.3 DKIM（域名密钥识别邮件）

- DKIM是一个电子邮件信息密码签名规范，允许签名域声明对邮件流中的某个邮件负责
- 邮件收件人可以通过直接查询签名者的域，获得适当的公钥并确定信息是由掌握密钥 的一方发出的，从而验证签名
- 建议的Internet标准RFC 4871
- 已被一系列电子邮件提供商和互联网服务提供商（ISP）广泛采用

8.3.1 互联网邮件体系结构

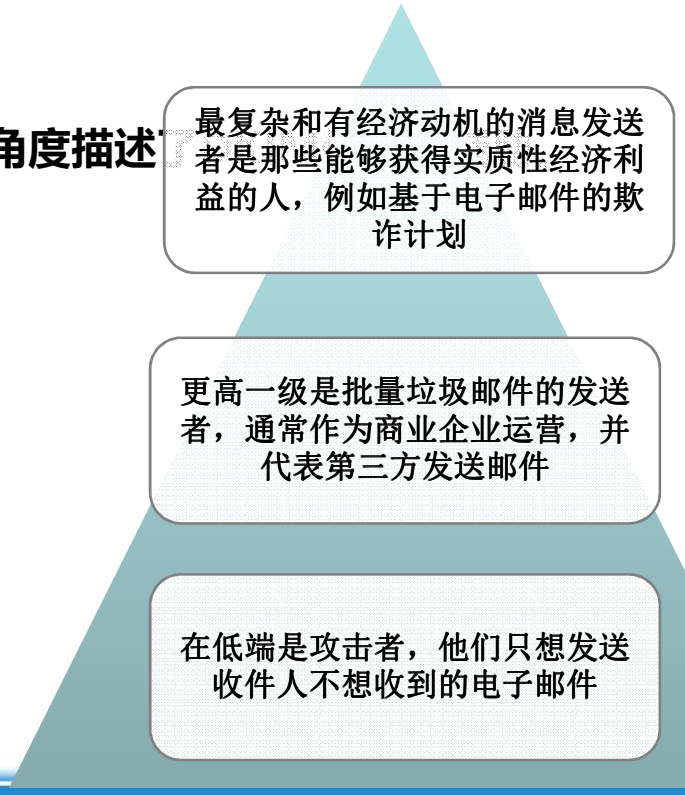
- 互联网邮件体系结构是由用户和传输组成
- 用户表现为信息用户代理（MUA）
- 传输表现为信息处理服务（MHS），由信息传输代理 （MTA)组成

功能模块和互联网标准化协议



E-mail威胁

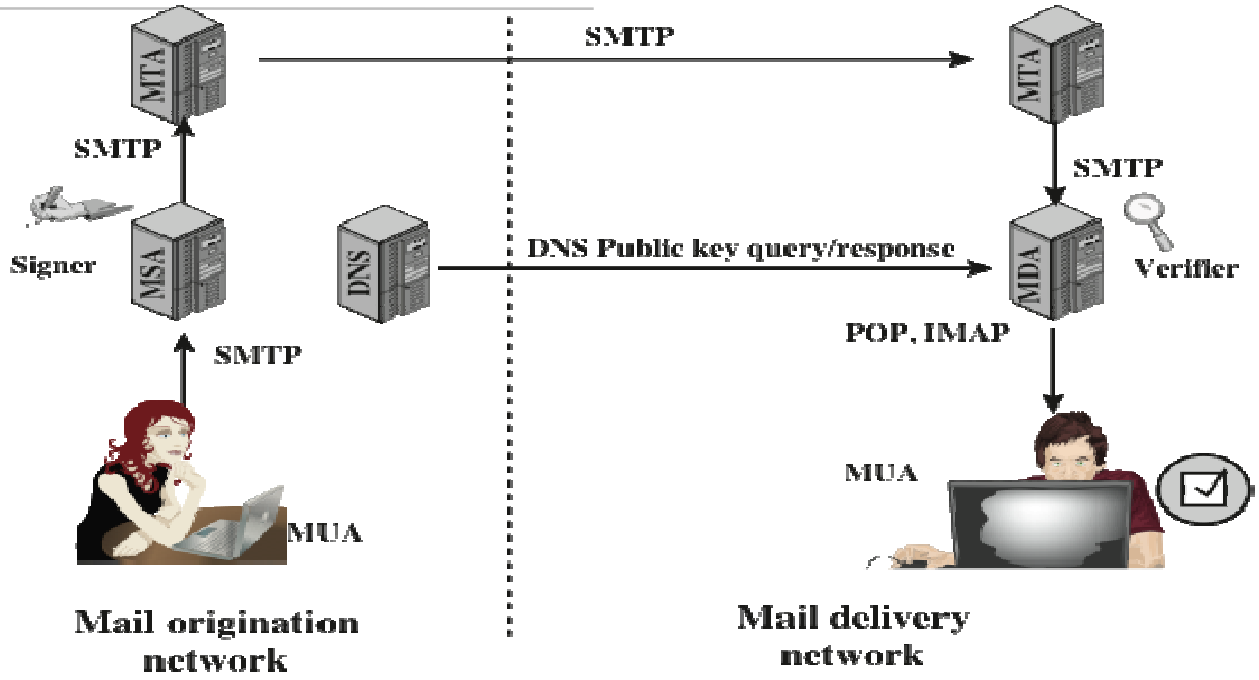
- **RFC 4684（威胁分析）**
  - **从潜在攻击者的特征，功能和位置三个角度描述**
- **以三级威胁为特征**



8.3.3 DKIM策略

- DKIM被用来提供一种对终端用户透明的E-Mail认证技术。
- 一个用户的E-Mail信息被管理域中的私钥签名。签名包括了信息的所有内容以及一些RFC 5322信息头。
- 在接收端，MDA可以通过DNS获得对应的公钥并且验证签名，从而确定信息来自特定的管理域。

DKIM应用举例



DNS = domain name system
MDA = mail delivery agent
MSA = mail submission agent
MTA = message transfer agent
MUA = message user agent

8.3.4 DKIM的功能流程

- 图8.6 对DKIM工作中的元素提供了更加详细的说明
- 基本的信息处理被分为签名行政处理域（ADMD)和一个验证用的ADMD

DKIM功能流程

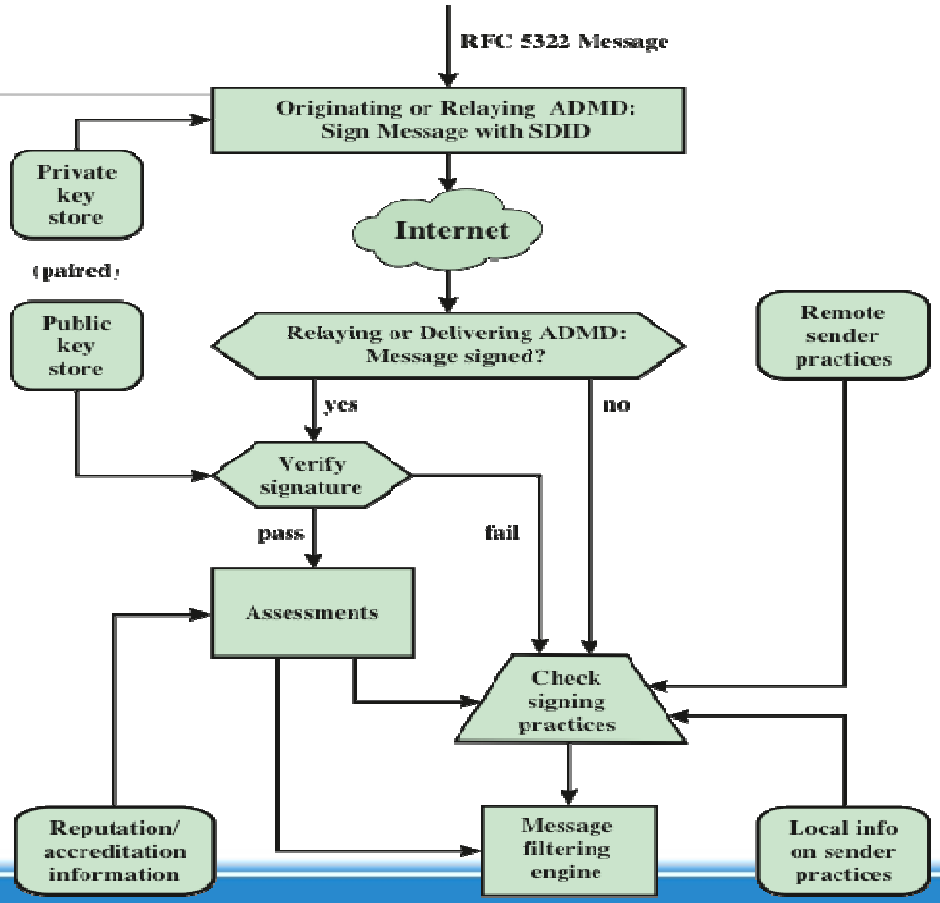


Figure 8.6 DKIM Functional Flow

小结

- **相当不错的隐私**
  - **符号**
  - **操作说明**
- **DomainKeys识别邮件**
  - **Internet邮件架构**
  - **E-mail威胁**
  - **DKIM 策略**
  - **DKIM功能流程**
- **S/MIME**
  - **RFC 5322**
  - 多用途Internet邮件扩展
  - **S/MIME功能**
  - **S/MIME 消息**
  - **S/MIME认证处理**
  - 增强的安全服务

志存高远 责任为先

感谢聆听

网址：www.jxust. edu.cn
邮编：341000