网络安全——

应用安全—PGP

北京邮电大学

郑康锋

zkfbupt@163.com

目录

PGP——

PGP概述

安全电子邮件系统
PGP (Pretty Good Privacy)

- 由个人发展起来——
  - Phil Zimmermann(齐默尔曼)
- PGP为电子邮件和文件存储应用提供了认证和保密性服务
  - 选择理想的密码算法
  - 把算法很好地集成到通用应用中，独立于操作系统和微处理器
  - 自由发放，包括文档、源代码等
  - 与商业公司(Network Associates)合作，提供一个全面兼容的、低价位的商业版本PGP
- 历史
  - 1991年推出1.0版，1994年推出2.6版，现在9.6版等
  - 算法的专利之争。困扰了3年多
  - 与美国出口管理限制之争，长达5年的调查

PGP(Pretty Good Privacy)

- Philip R. Zimmerman的主要工作
  - 选择了最好的加密算法作为基础构件
  - 集成加密算法，形成通用的应用程序
  - 制作软件包和文档，包括源码，免费提供
  - 提供完全兼容的低价格的商用版本
- PGP快速发展和流行的原因
  - 免费获得，运行不同平台的多个版本
  - 建立在普遍认为非常安全的算法的基础上，算法的安全性已经得到了充分的论证，如公钥加密包括RSA、DSS、Diffie-Hellman，单钥加密包括CAST-128、IDEA、3DES、AES，以及SHA-1散列算法
  - 应用范围广泛，适用性强
  - 不受任何组织和政府控制

你如何设计？

对于电子邮件安全，大家讨论下应该如何进行设计？

应用背景	安全需求	已有基础	特殊性
存储转发	机密性	DES\AES\..	离线
实时性低	完整性	MD5\SHA\..	未知可能
邮件大小	可用性	IKE\..	检索
通信双方	可审性	DH\..	协商
...	...	...	...

相对于SSL、IPSec等，有新的问题：

- 身份认证怎么解决?
- 如何进行密钥协商？

PGP功能列表

服　务	采用算法	说　明
数字签名	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——

PGP操作

PGP所使用的符号

Ks：常规加密中的会话密钥
KRa：公开密钥系统中用户A的私有密钥
KUa：公开密钥系统中用户A的公开密钥
EP：公开密钥加密
DP：公开密钥解密
EC：常规加密
DC：常规解密
H:　散列函数
||：　串接操作(并置)
Z：　使用ZIP算法进行压缩
R64: 基数为64的ASCII格式转换

PGP操作描述

Function	Algorithms Used	Description
Digital signature	DSS/SHA or RSA/SHA	A hash code of a message is created using SHA-1. This message digest is encrypted using DSS or RSA with the sender's private key and included with the message.
Message encryption	CAST or IDEA or Three-key Triple DES with Diffie-Hellman or RSA	A message is encrypted using CAST-128 or IDEA or 3DES with a one-time session key generated by the sender. The session key is encrypted using Diffie-Hellman or RSA with the recipient's public key and included with the message.
Compression	ZIP	A message may be compressed, for storage or transmission, using ZIP.
Email compatibility	Radix 64 conversion	To provide transparency for email applications, an encrypted message may be converted to an ASCII string using radix 64 conversion.
Segmentation	—	To accommodate maximum message size limitations, PGP performs segmentation and reassembly.

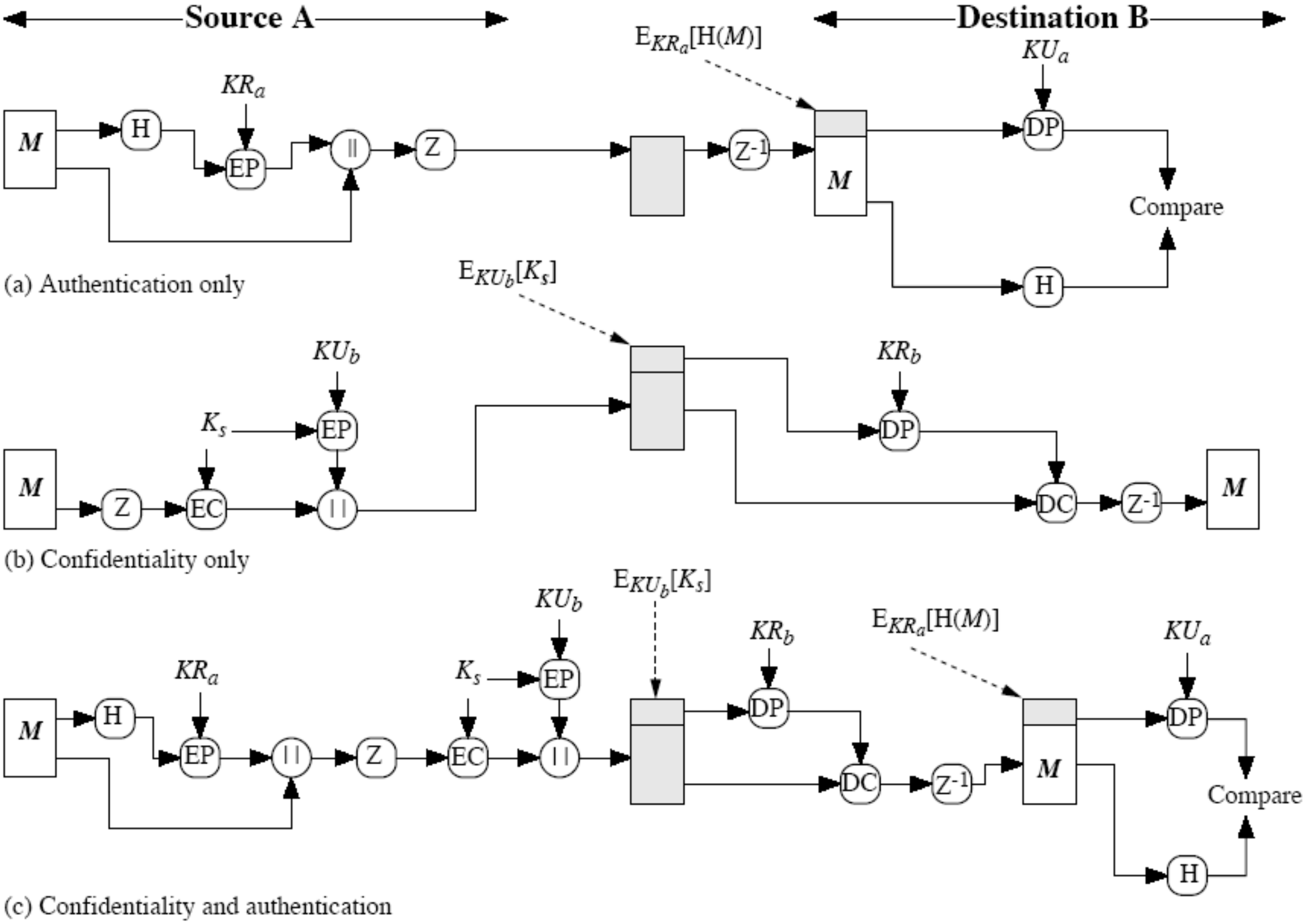
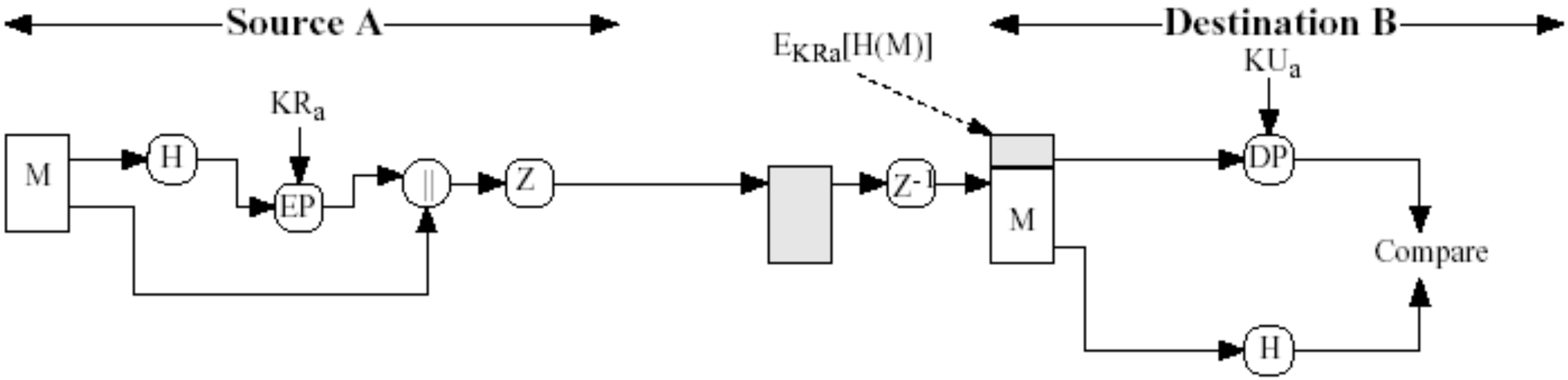


Figure 15.1 PGP Cryptographic Functions

PGP操作描述

- 数字签名与认证
  - 发送者创建报文
  - 使用SHA-1生成报文的160位散列码
  - 使用发送者的私有密钥，用RSA算法对散列码加密(签名)，并置在报文前面
  - 接收者使用发送者的公开密钥，用RSA解密和恢复散列码
  - 接收者计算报文的散列码，与解密得到的进行比较，如果两者匹配，则报文通过鉴别
- 签名也可以使用DSS/SHA-1来生成
- PGP也支持分离的数字签名

功能：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。

身份认证说明

- 说明

  1. RSA的强度保证了发送方的身份

  2. SHA-1的强度保证了签名的有效性

  3. DSS/SHA-1可选替代方案。

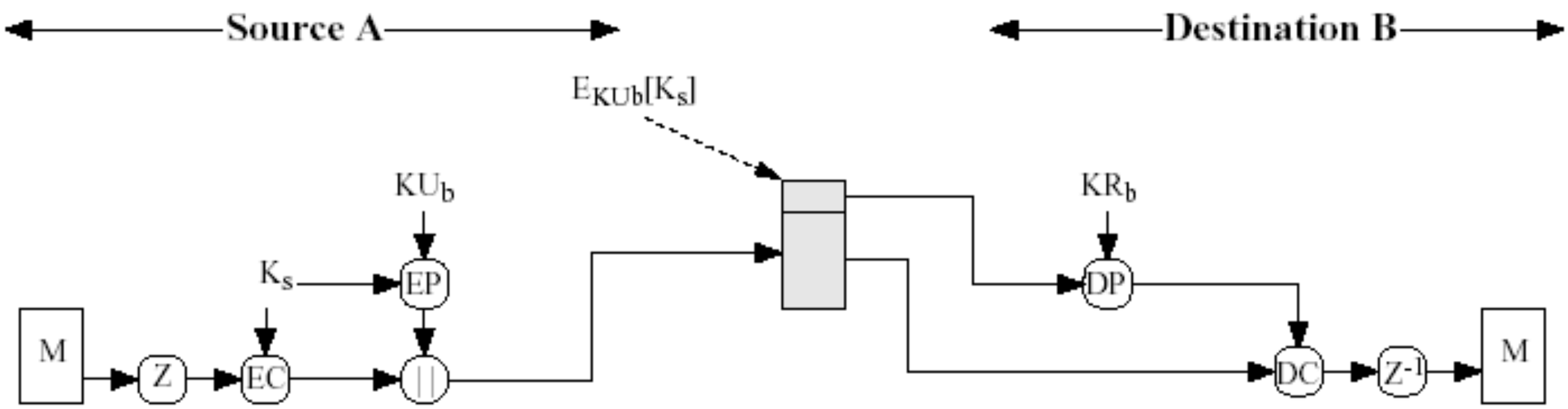
- 签名与消息可以分离

  - 对消息进行单独的日志记录
  - 可执行程序的签名记录，检查病毒
  - 文档多方签名，可以避免嵌套签名

PGP操作描述

- 保密性
  - 发送者生成报文和128位会话密钥随机数
  - 采用CAST-128(或IDEA或3DES)对报文加密
  - 采用RSA，使用接收者的公开密钥加密会话密钥，并置到报文前面
  - 接收者采用RSA，解密和恢复会话密钥
  - 接收者使用会话密钥解密报文
  - 可以使用Diffie-Hellman算法生成会话密钥
- 保密性与认证
  - 同时实现保密和认证

保密性



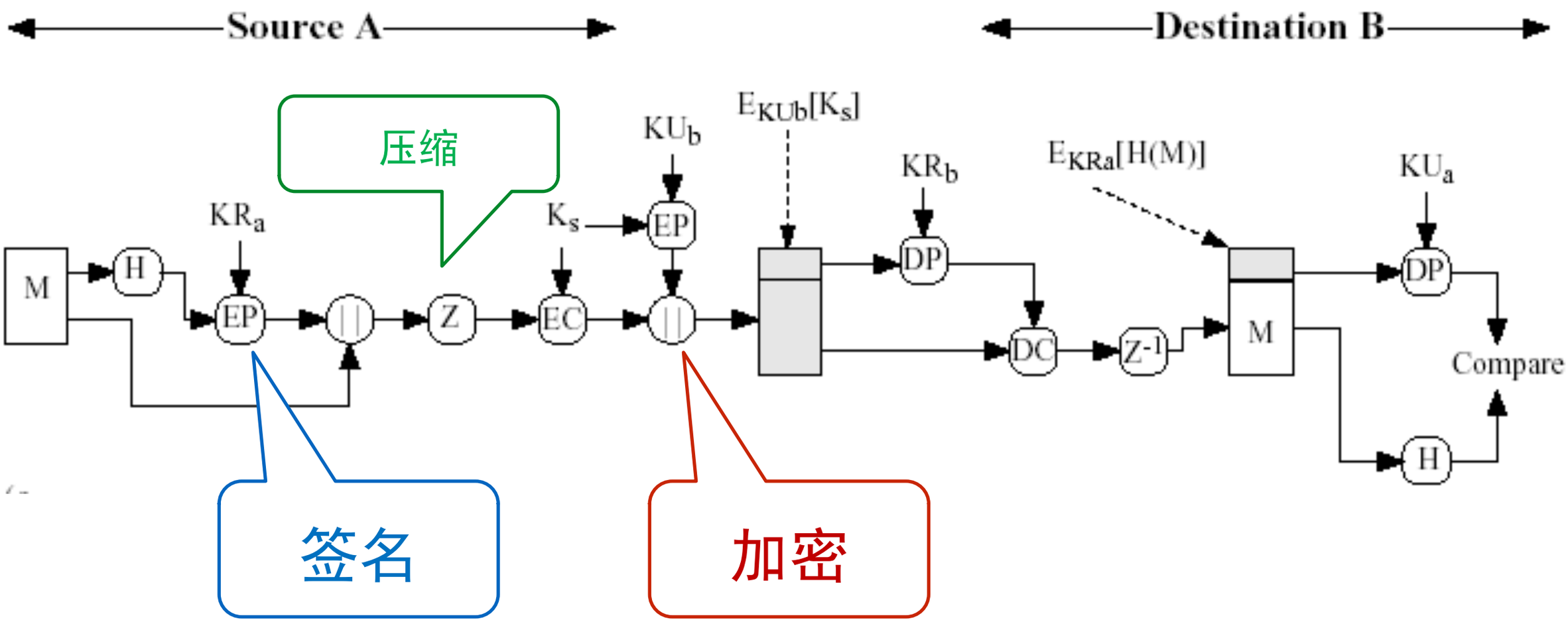
- 发送方
  - 生成消息M并为该消息生成一个随机数作为会话密钥。
  - 用会话密钥加密M
  - 用接收者的公钥加密会话密钥并与消息M结合

- 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

保密性说明

- 对称加密算法和公钥加密算法的结合可以缩短加密时间
- 用公钥算法解决了会话密钥的单向分发问题
  - 不需要专门的会话密钥交换协议
  - 由于邮件系统的存储-转发的特性，用握手方式交换密钥不太可能
- 每个消息都有自己的一次性密钥，进一步增强了保密强度。所以，每个密钥只加密很小部分的明文内容

保密与认证的结合



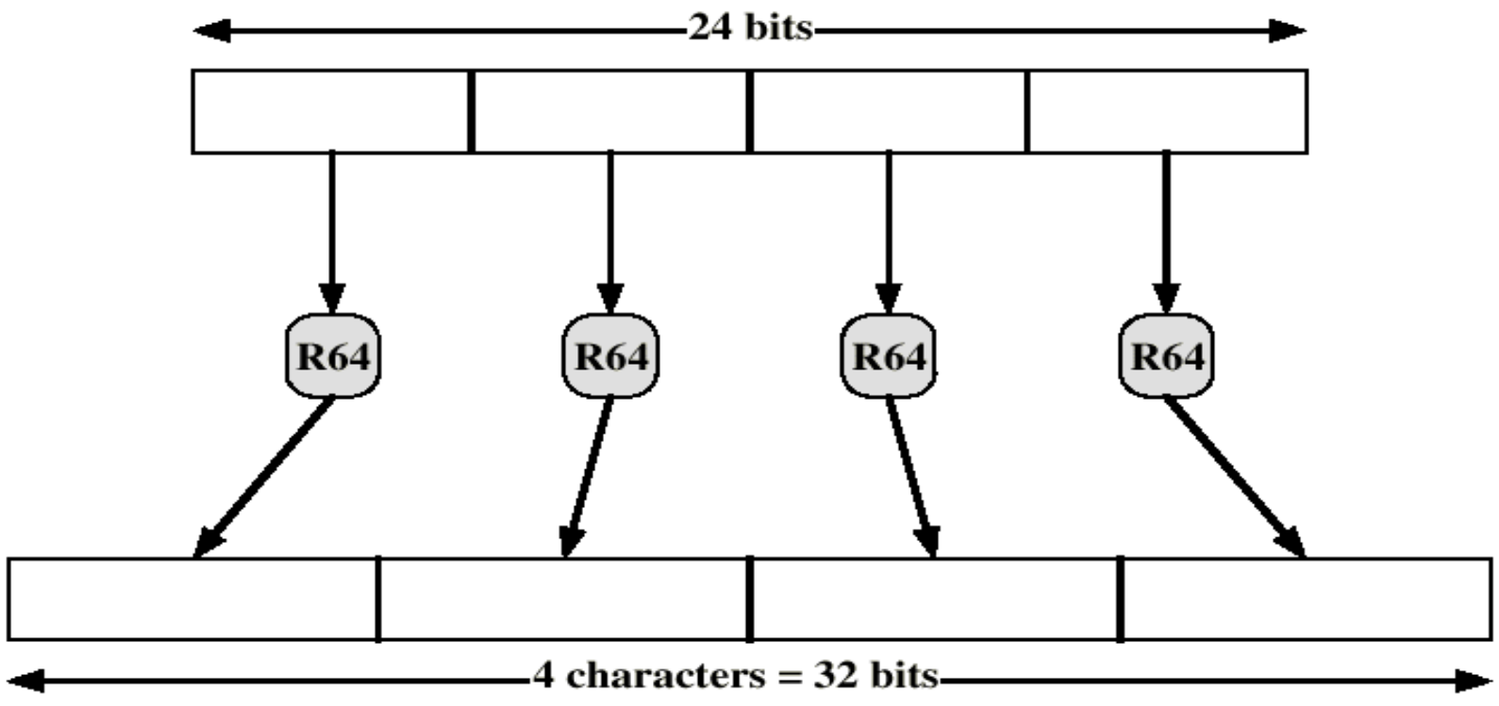
- 两种服务都需要时，发送者先用自己的私钥签名，然后用会话密钥加密消息，再用接收者的公钥加密会话密钥。

PGP操作描述

- 压缩
  - 压缩有利于在电子邮件传输和存储时节省空间
  - 压缩在签名之后进行
    - 对没有压缩过的报文进行签名，验证时只需要存储没有压缩过的报文和签名
    - 便于采用不同的压缩算法
  - 加密压缩过的报文可以加强加密的强度，因为冗余减少，密码分析更加困难
  - PGP采用ZIP算法进行压缩

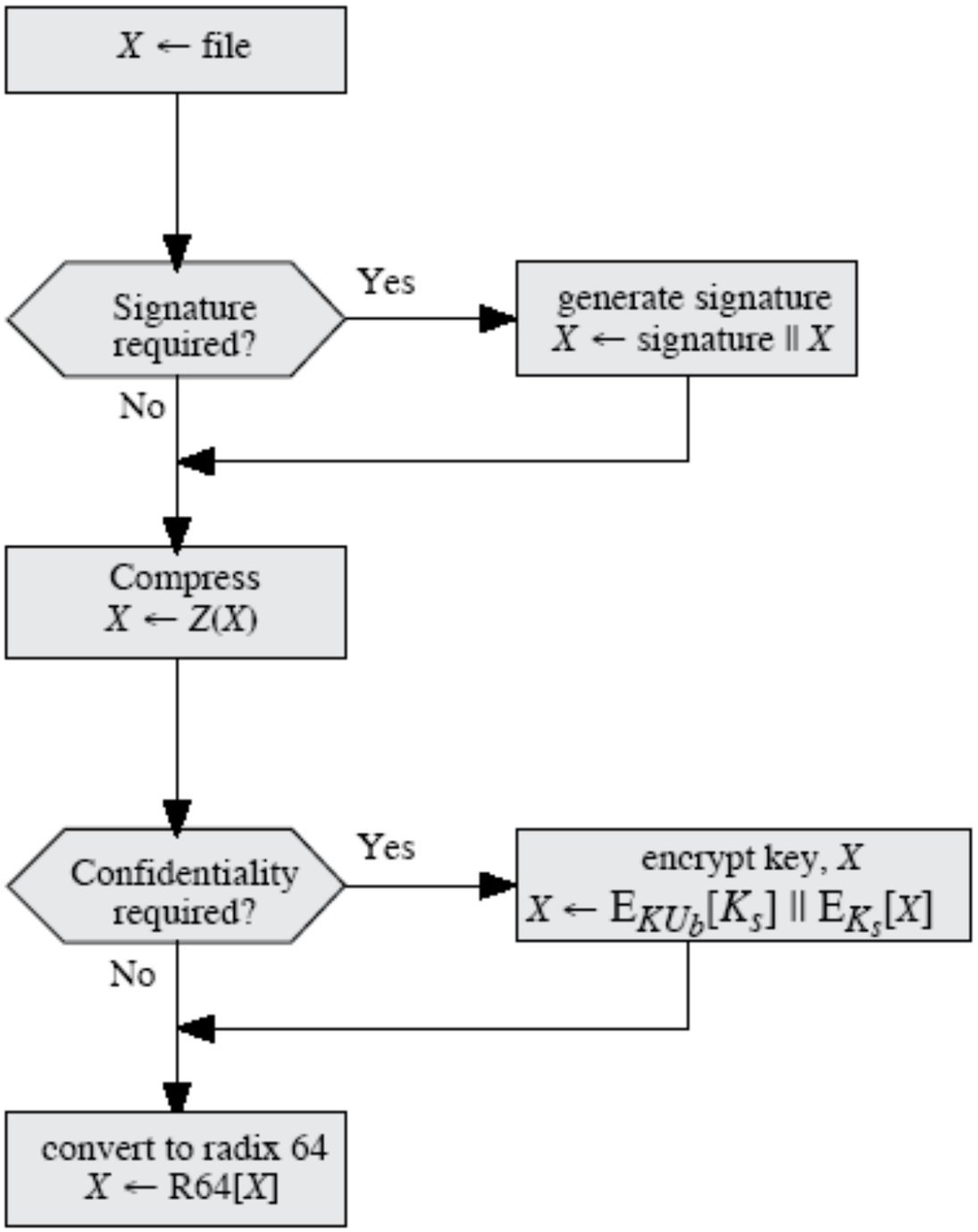
PGP操作描述

- 电子邮件的兼容性
  - PGP提供把原始8位二进制流转换成可打印ASCII字符的服务
  - 采用Radix-64转换，每三个字节的二进制数据为一组映射成四个ASCII字符，附加CRC校验
  - 使用Radix-64，报文长度增加了33%

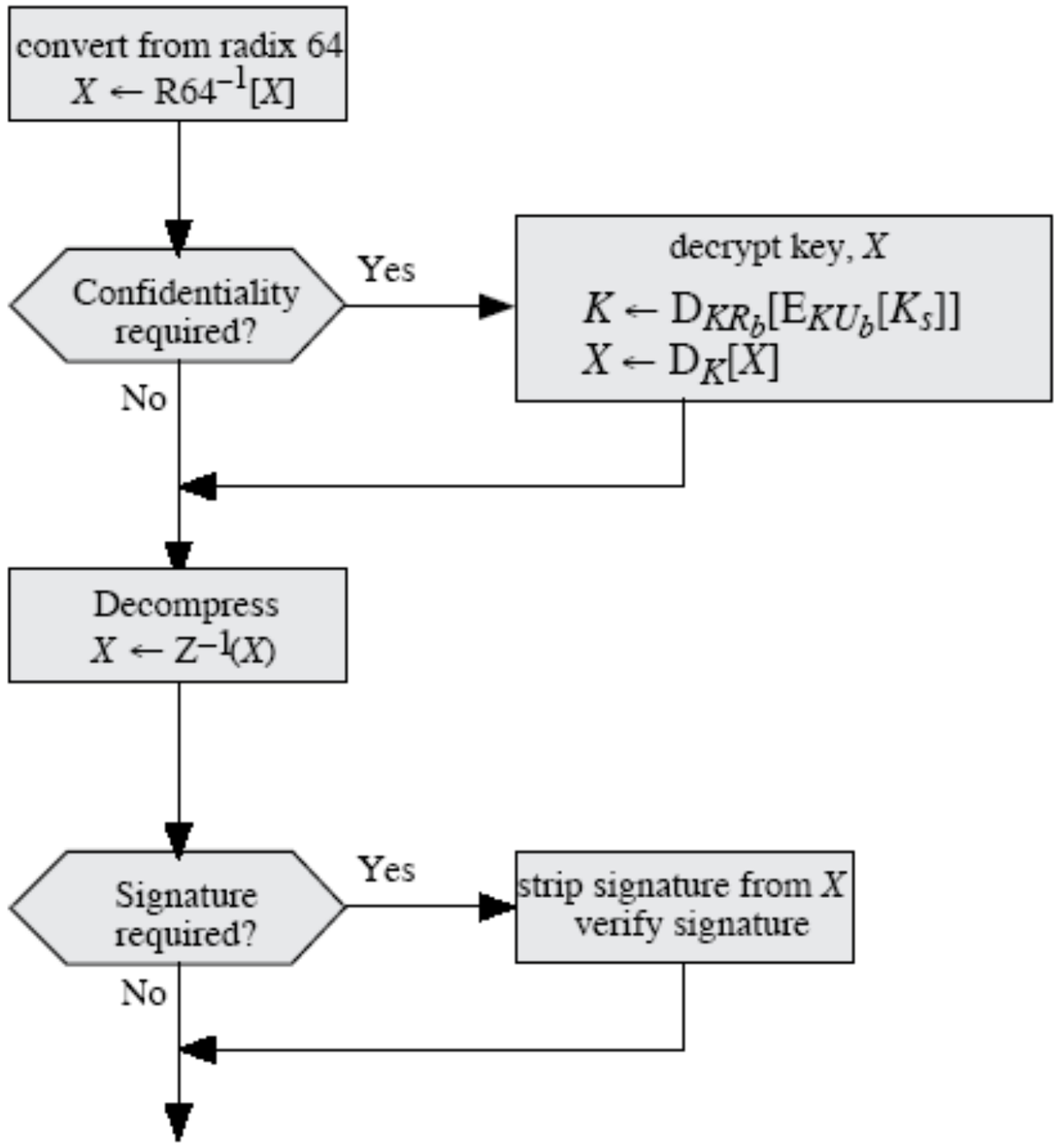


PGP操作描述

- 分段与重组
  - 电子邮件工具通常限制消息的最大长度，一般在50,000字节
  - 任何大于该长度的消息必须分成若干小段，单独发送
  - PGP自动将长消息分段使之可以通过电子邮件发送，分段在所有操作之后进行，包括基数64转换
  - 接收方剥去所有电子邮件头，按步骤重新组装



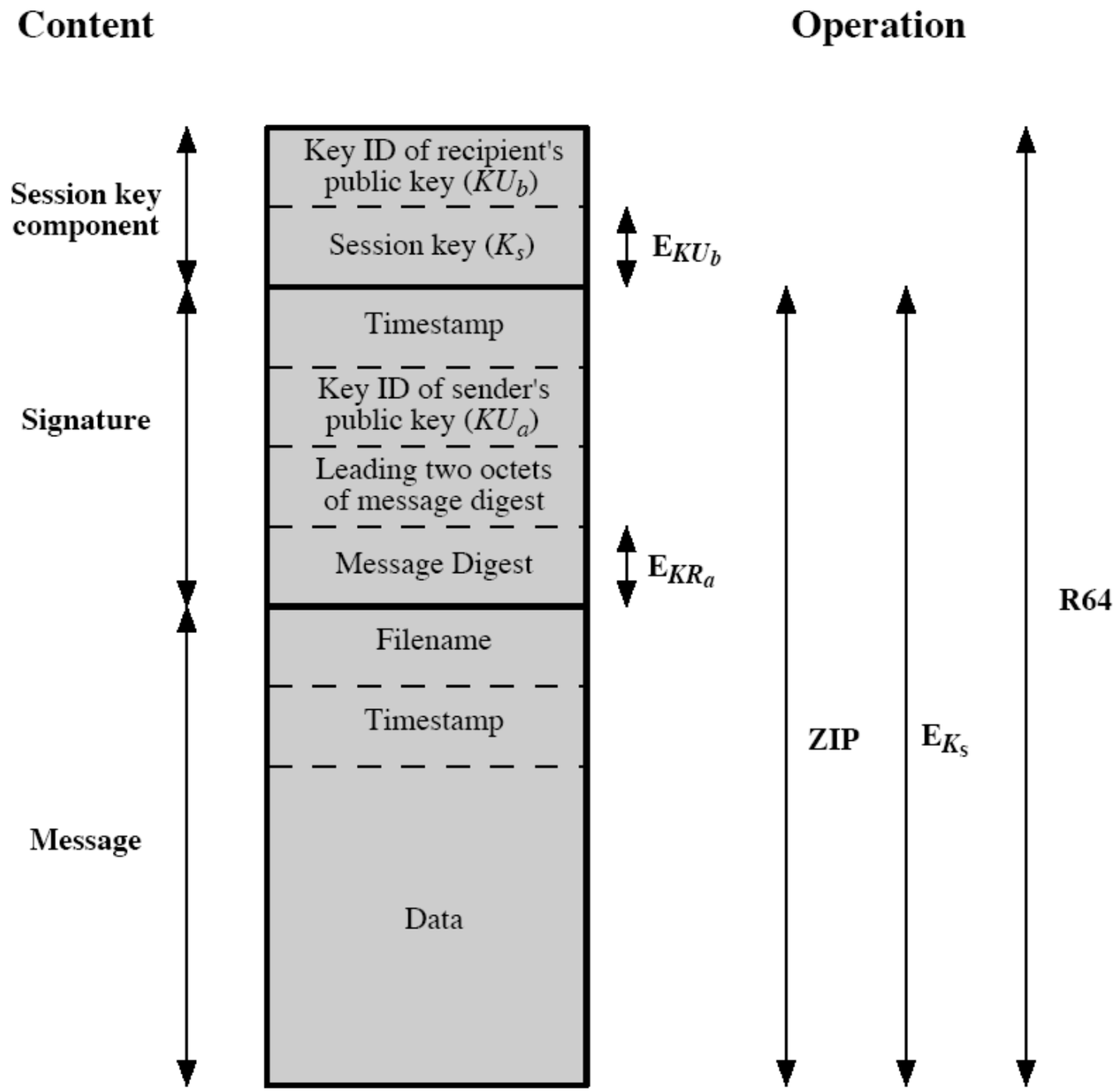
(a) Generic Transmission Diagram (from A)



(b) Generic Reception Diagram (to B)

Figure 15.2 Transmission and Reception of PGP Messages

Format of PGP Message



Notation:

E_{KU_b} = encryption with user b's public key
E_{KR_a} = encryption with user a's private key
E_{K_s} = encryption with session key
ZIP = Zip compression function
R64 = Radix-64 conversion function

Figure 15.3 General Format of PGP Message (from A to B)

PGP——

PGP密钥管理

加密密钥和密钥环

- 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
  - 私钥如何保存

密钥标识符和钥匙环

- **一个用户有多个公钥/私钥对时，接收者如何知道发送者是用哪个公钥来加密会话密钥的？**
  - 将公钥与消息一起传送。
  - 将一个标识符与一个公钥关联，对一个用户来说唯一。即用户ID和密钥ID标识一个密钥
- **定义KeyID 包括64个有效位(PGP采用公钥的低64位作为KeyID)**
- **对于PGP数字签名，KeyID也很必需。用哪个公钥来验证签名？**
- **钥匙环**
  - 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
- **PGP密钥管理方案**
  - 用户机器(节点)上有一对数据结构：
    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

PGP私钥环

- 信息
  - 时间戳、KeyID、公钥、私钥、UserID
- User ID
  - 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。

Private Key Ring

Timestamp	Key ID*	Public Key	Encrypted Private Key	User ID*
• • •	• • •	• • •	• • •	• • •
T_i	KU_i mod 2^{64}	KU_i	$E_{H(Pi)}[KR_i]$	User i
• • •	• • •	• • •	• • •	• • •

Public Key Ring

Timestamp	Key ID*	Public Key	Owner Trust	User ID*	Key Legitimacy	Signature(s)	Signature Trust(s)
• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •
T_i	KU_i mod 2^{64}	Ku_i	$trust\_flag_i$	User i	$trust\_flag_i$		
• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •

* = field used to index table

Figure 15.4 General Structure of Private and Public Key Rings

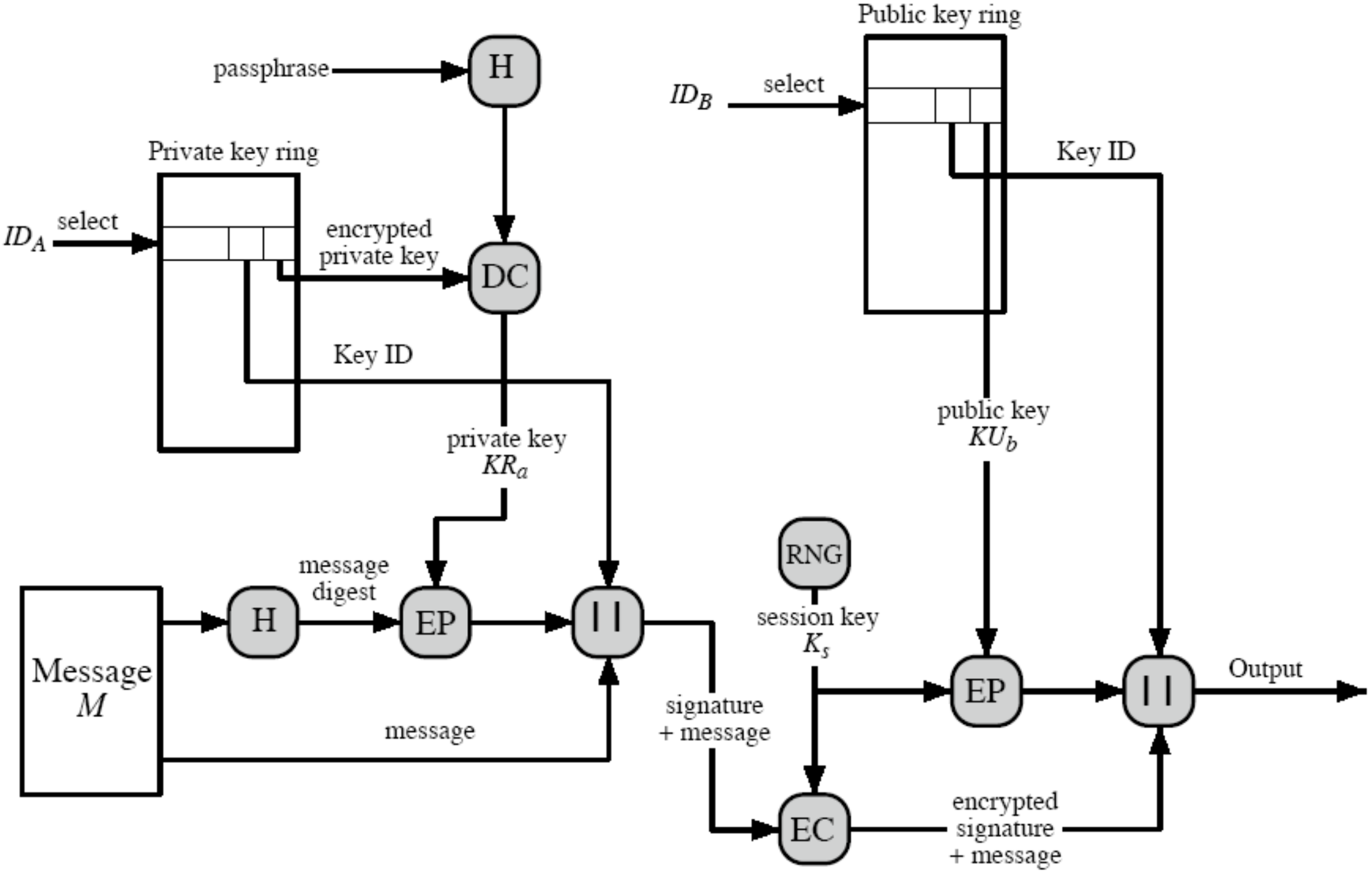


Figure 15.5 PGP Message Generation (from User A to User B; no compression or radix 64 conversion)

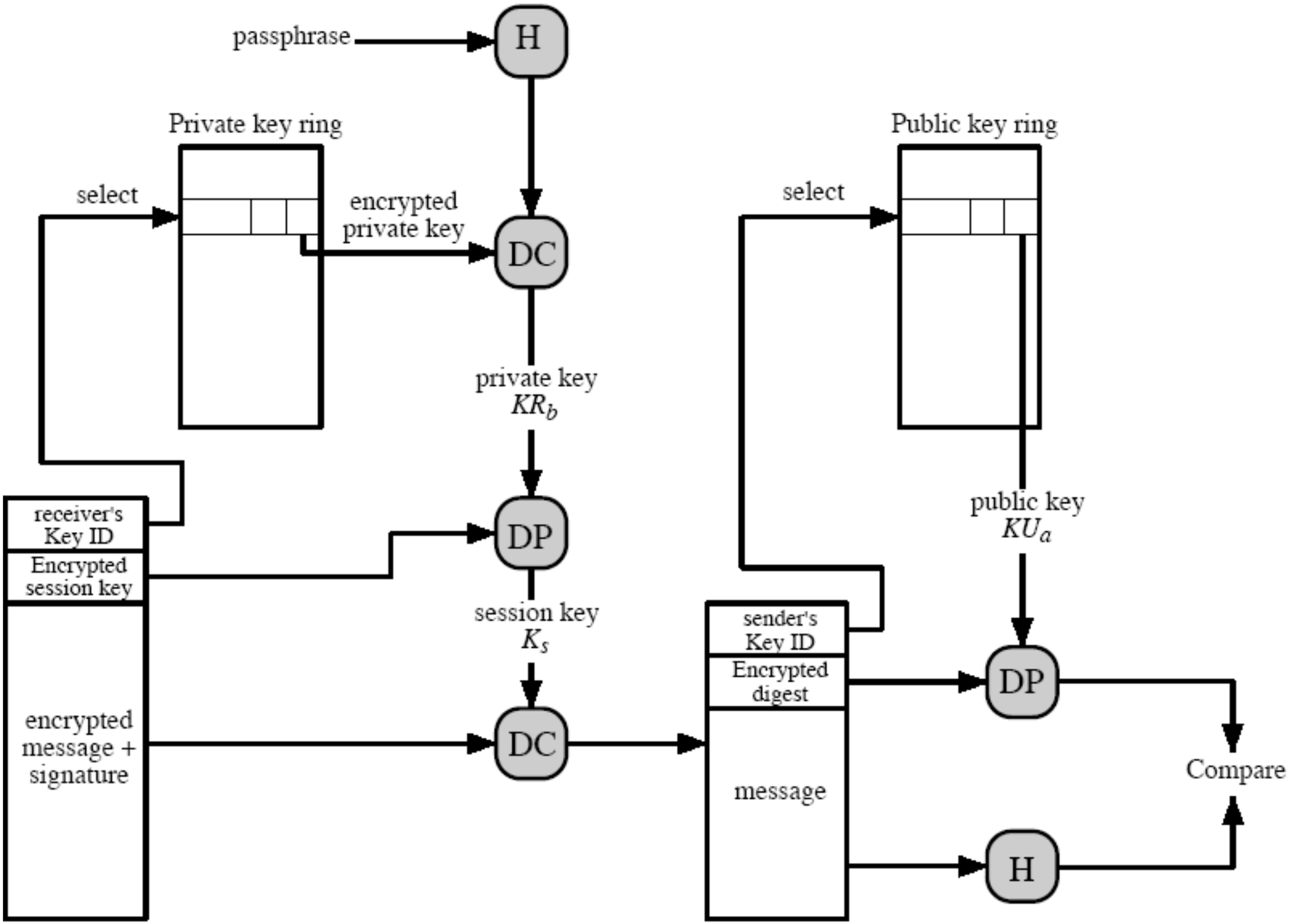


Figure 15.6 PGP Message Reception (from User A to User B; no compression or radix 64 conversion)

邮件数据处理

- 顺序：签名 —— 压缩 —— 加密
- 压缩对邮件传输或存储都有节省空间的好处
- 签名后压缩的原因
  - 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
- 压缩之后再做加密的原因
  - 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
- E-mail兼容性
  - PGP处理后的消息，部分或者全部是加密后的消息流，为任意的8位字节。某些邮件系统只允许ASC字符，所以PGP提供了转换到ASC格式的功能。采用了Radix-64转换方案

PGP 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

- 由于PGP重在广泛地在正式或非正式环境下的应用，所以它没有建立严格的公钥管理模式。
- 有关的问题
  - 一旦用户私钥泄漏，存在两种危险：
    - 别人可以伪造用户的签名
    - 其他人发送给用户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
  - 物理上得到B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B的公钥
  - 从一个信任的CA中心得到B的公钥

PGP公钥信任模型

- 尽管PGP没有包含任何建立认证权威机构或建立信任体系的规范，但它提供了一个利用信任关系的方法，将信任关系与公钥联系起来。每个公钥有三个相关的属性：

  - Key legitimacy field：合法性或者有效性，表明PGP对“此用户公钥是合法的”的信任程度；信任级别越高，这个userID与该公钥的绑定越强。这个字段是由PGP计算的。

  - 每一个公钥项都有一个或者多个签名，这是公钥环主人收集到的、能够认证该公钥项的签名。每一个签名与一个signature trust field关联，表明这个PGP用户对“签名人对公钥签名”的信任程度。Key legitimacy field 是由多个signeture trust field 导出的。

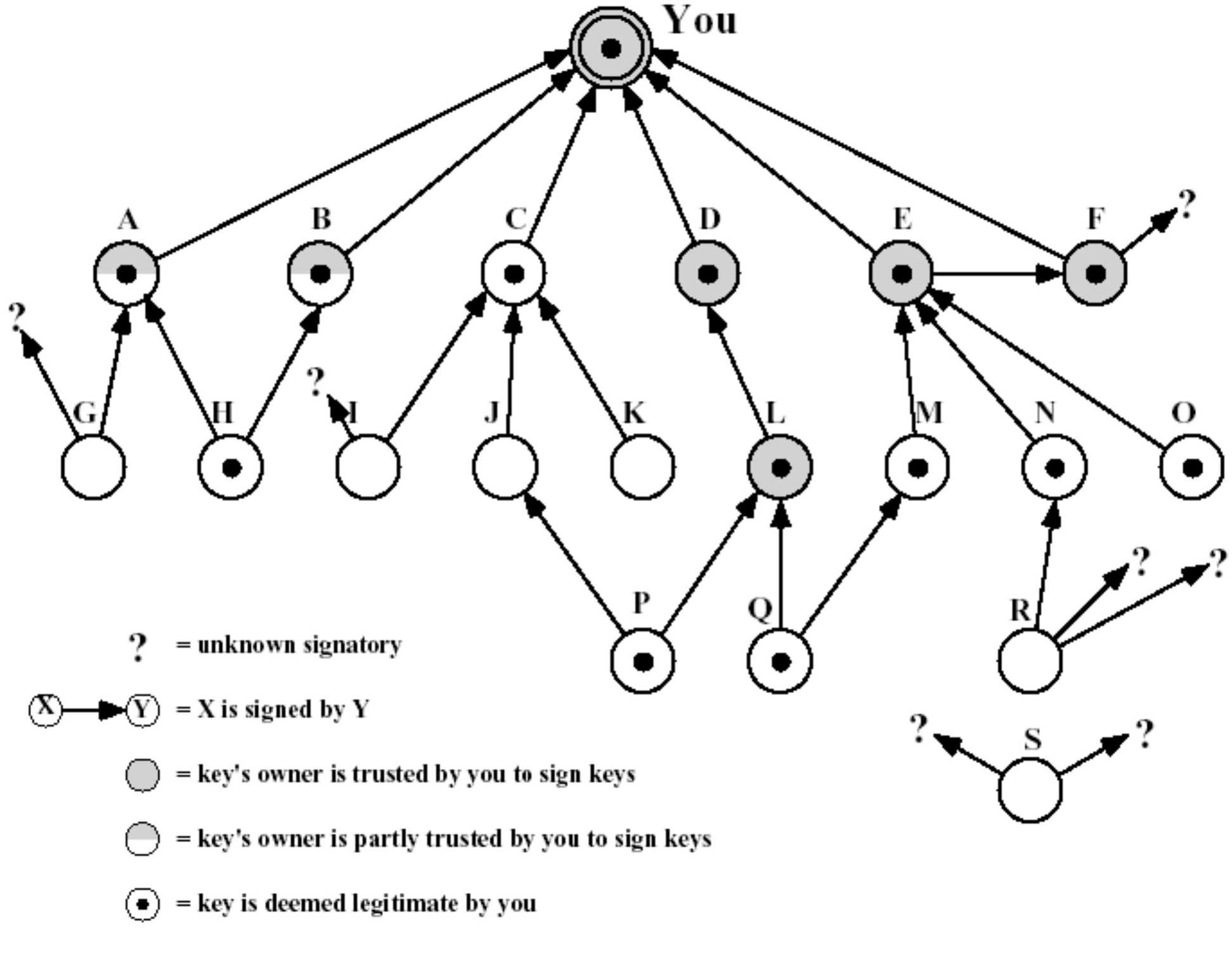
  - Owner trust field：表明该公钥被用于签名其它公钥证书时的信任程度。这个信任程度是由用户给出的

信任标志字节的内容

Table 15.2 Contents of Trust Flag Byte

(a) Trust Assigned to Public-Key Owner (appears after key packet; user defined)	(b) Trust Assigned to Public Key/User ID Pair (appears after User ID packet; computed by PGP)	(c) Trust Assigned to Signature (appears after signature packet; cached copy of OWNERTRUST for this signator)
OWNERTRUST Field —undefined trust —unknown user —usually not trusted to sign other keys —usually trusted to sign other keys —always trusted to sign other keys —this key is present in secret key ring (ultimate trust) BUCKSTOP bit —set if this key appears in secret key ring	KEYLEGIT Field —unknown or undefined trust —key ownership not trusted —marginal trust in key ownership —complete trust in key ownership WARNONLY bit —set if user wants only to be warned when key that is not fully validated is used for encryption	SIGTRUST Field —undefined trust —unknown user —usually not trusted to sign other keys —usually trusted to sign other keys —always trusted to sign other keys —this key is present in secret key ring (ultimate trust) CONTIG bit —set if signature leads up a contiguous trusted certification path back to the ultimately trusted key ring owner

PGP信任模型示例


You
A
B
C
D
E
F
?
G
H
?
I
J
K
L
M
N
O
P
Q
R
?
?
?
S
?
= unknown signatory
X
Y
= X is signed by Y
= key's owner is trusted by you to sign keys
= key's owner is partly trusted by you to sign keys
= key is deemed legitimate by you

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
- 注意：对手也可以发出这个证书，然而，这将导致他自己也被否决。因此，这样比起恶意使用偷来的私钥来看，似乎会减少漏洞。

PGP证书管理软件

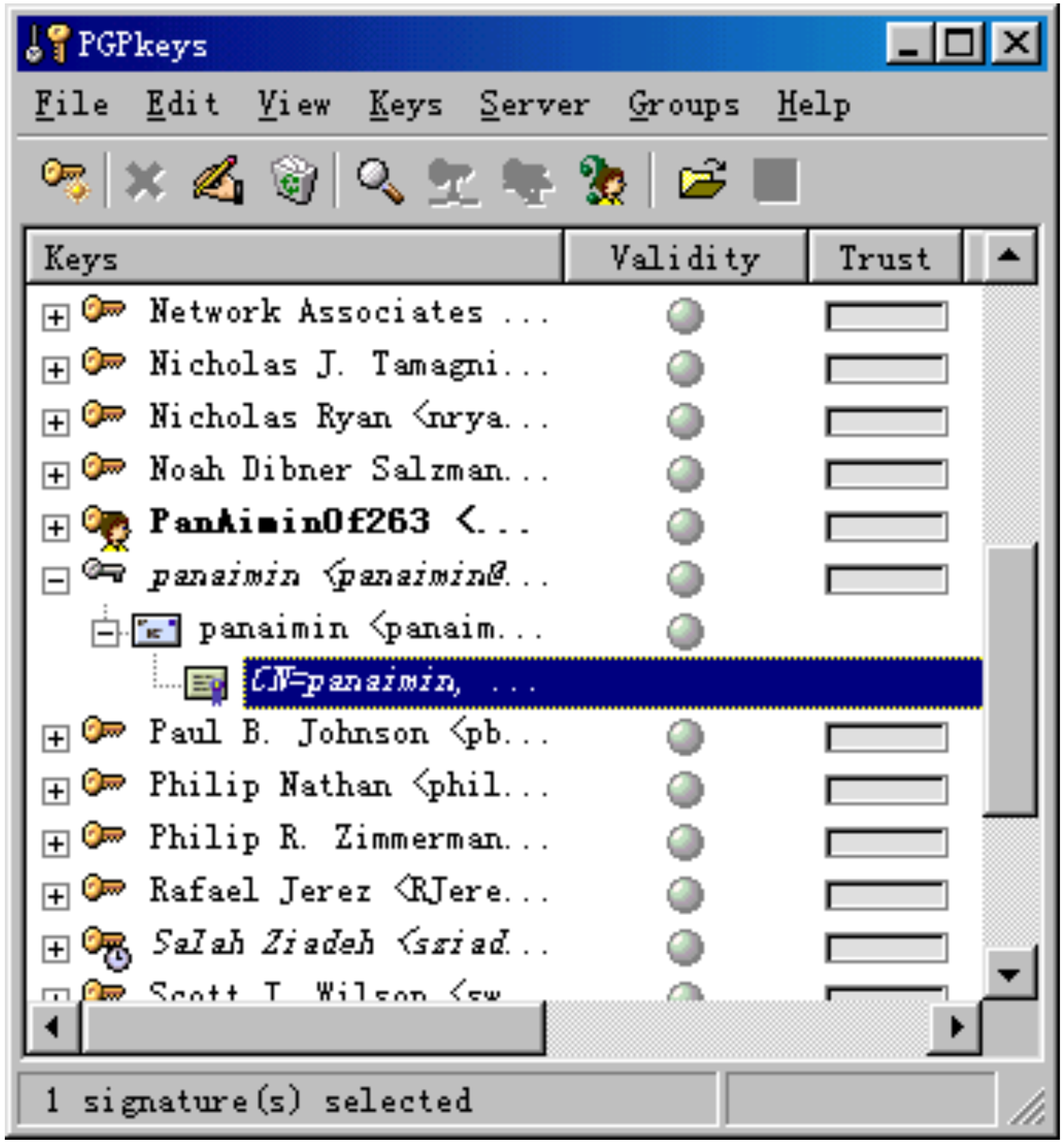
- PGP证书管理软件 —— 服务器软件
- 集中管理PGP公钥证书
- 提供LDAP、HTTP服务
- 本地Keyring可以实时地连接到服务器，适合于企业使用
  - 更新老的证书
  - 查找新的证书
  - 查询CRL

PGP——

PGP用法

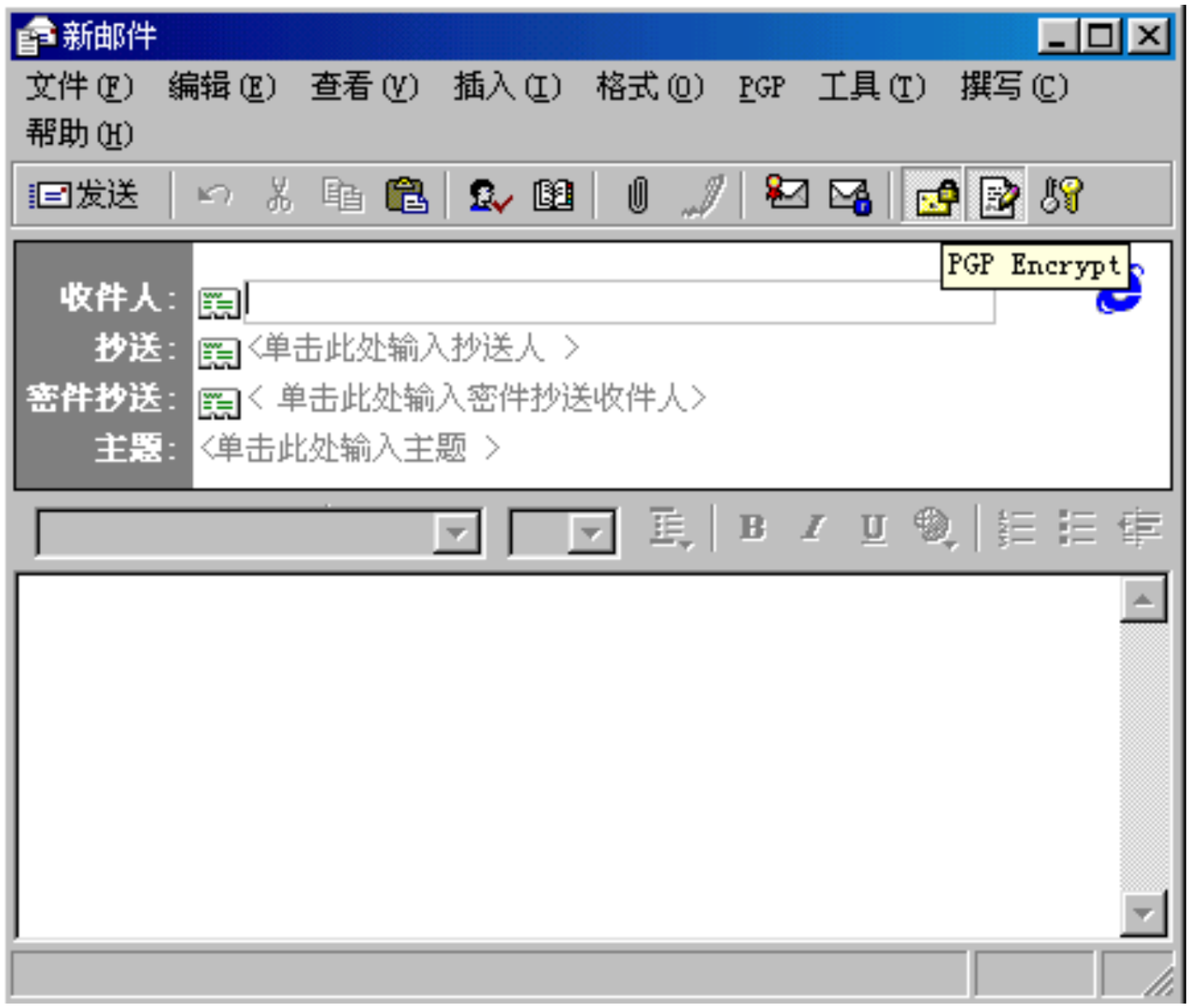
PGP用法(1)

- 密钥管理
  - 生成新的密钥对
  - 导出、导入
  - 指定信任关系
  - 保存和备份
  - 改变私钥的访问口令



PGP用法(2)

- 撰写邮件时，发送之前指定加密和签名
  - 通过属性配置，可以指定默认状态



PGP用法(3)

- 其他辅助功能
  - 有关网络的功能
    - 个人防火墙
    - VPN
    - 网络传输
  - 文件加解密、签名认证
  - 当前窗口内容加解密、签名认证
  - 剪贴板内容加解密、签名认证

问题和讨论