高级网络安全研究与应用——

安全需求与安全应用

北京邮电大学

郑康锋 zkfbupt@163.com

伍淳华 wuchunhua@bupt.edu.cn

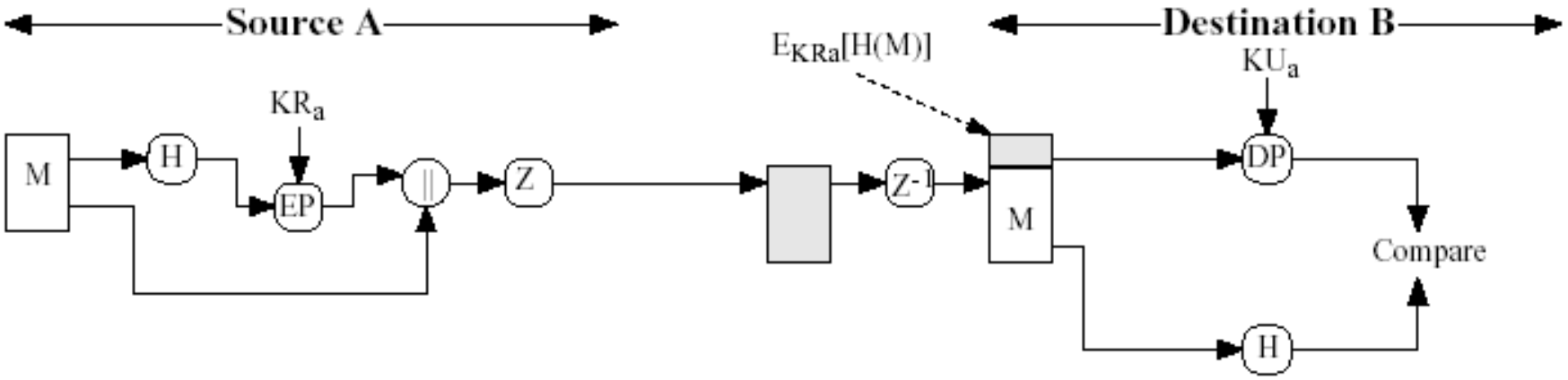
PGP

- 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

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

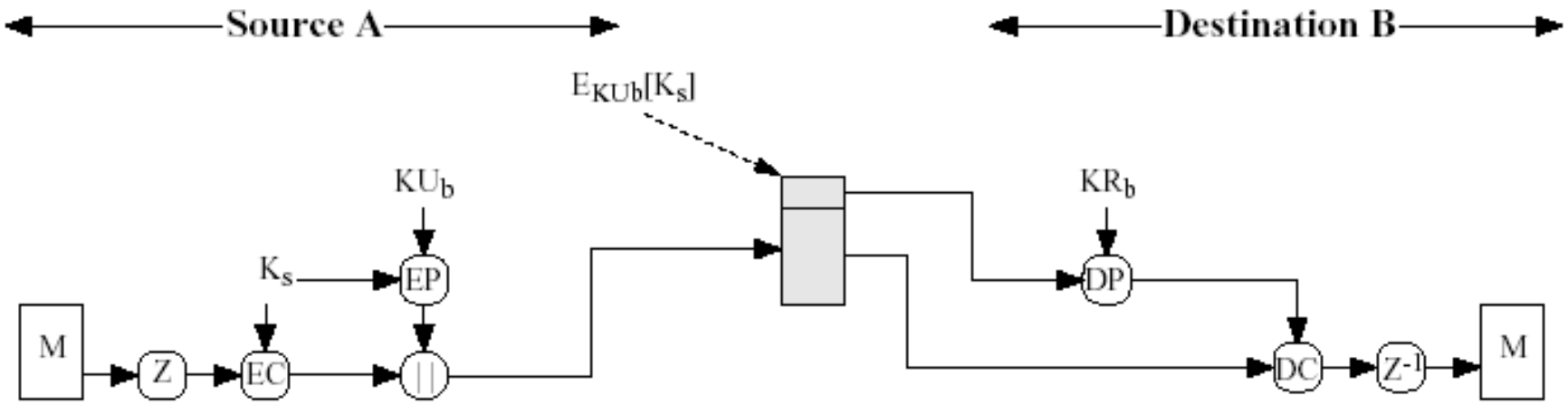
- 接收方
  - 用发送者的公钥解密并恢复散列码H
  - 对消息M生成一个新的散列码，与H比较。如果一致，则消息M被认证。



保密性

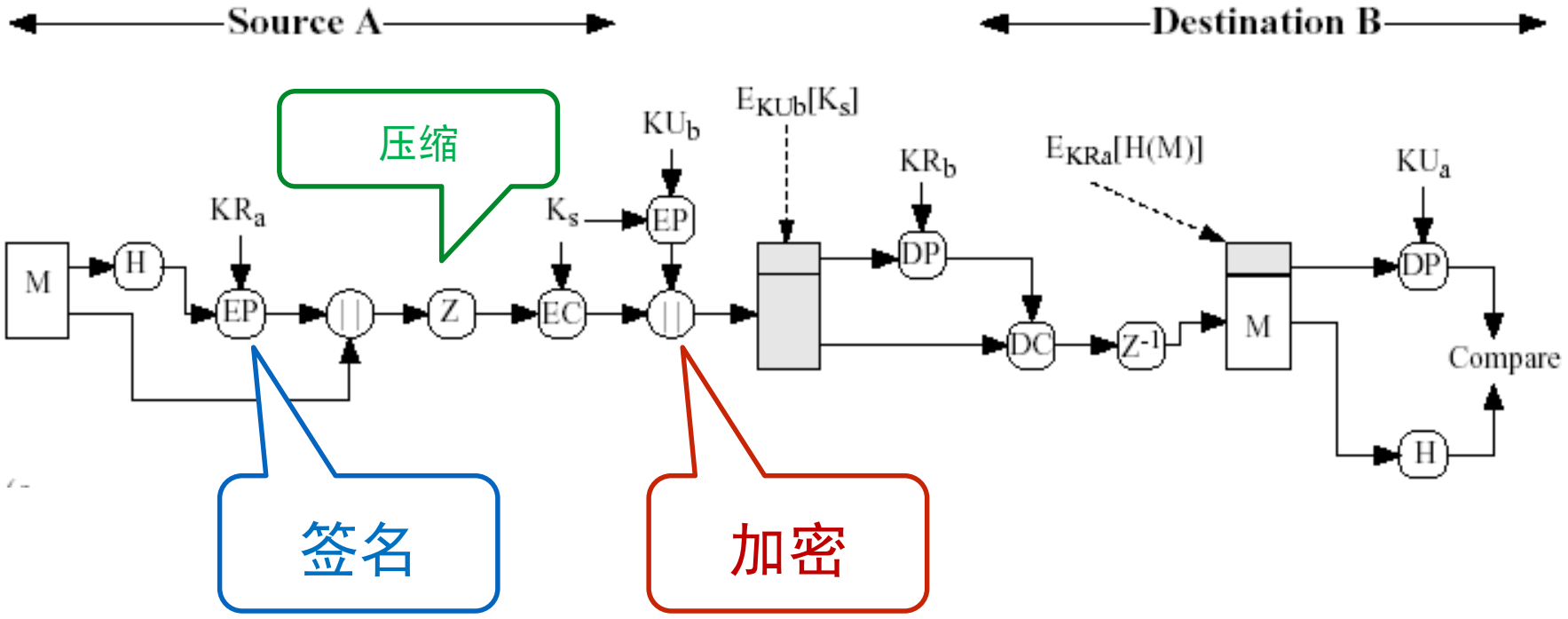
- 发送方
  - 生成消息M并为该消息生成一个随机数作为会话密钥。
  - 用会话密钥加密M
  - 用接收者的公钥加密会话密钥并与消息M结合

- 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。



独特之处

- 无需通信双方实时在线——非常适用于Email
- 无需实时认证——使用发送方私钥加密
- 无需协商加密密钥——使用接收方公钥加密

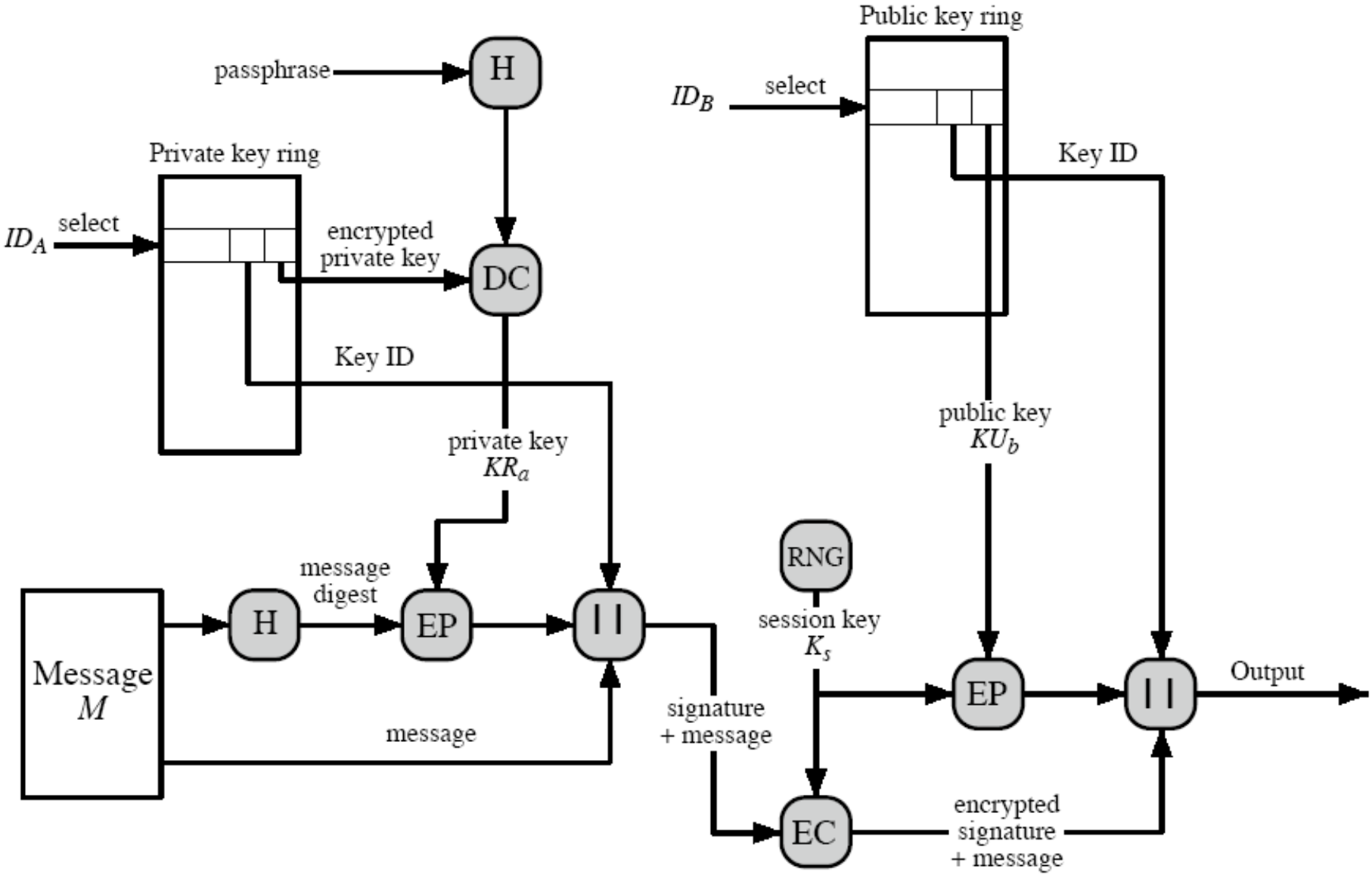


Figure 15.5 PGP Message Generation (from User A to User B; no compression or radix 64 conversion)

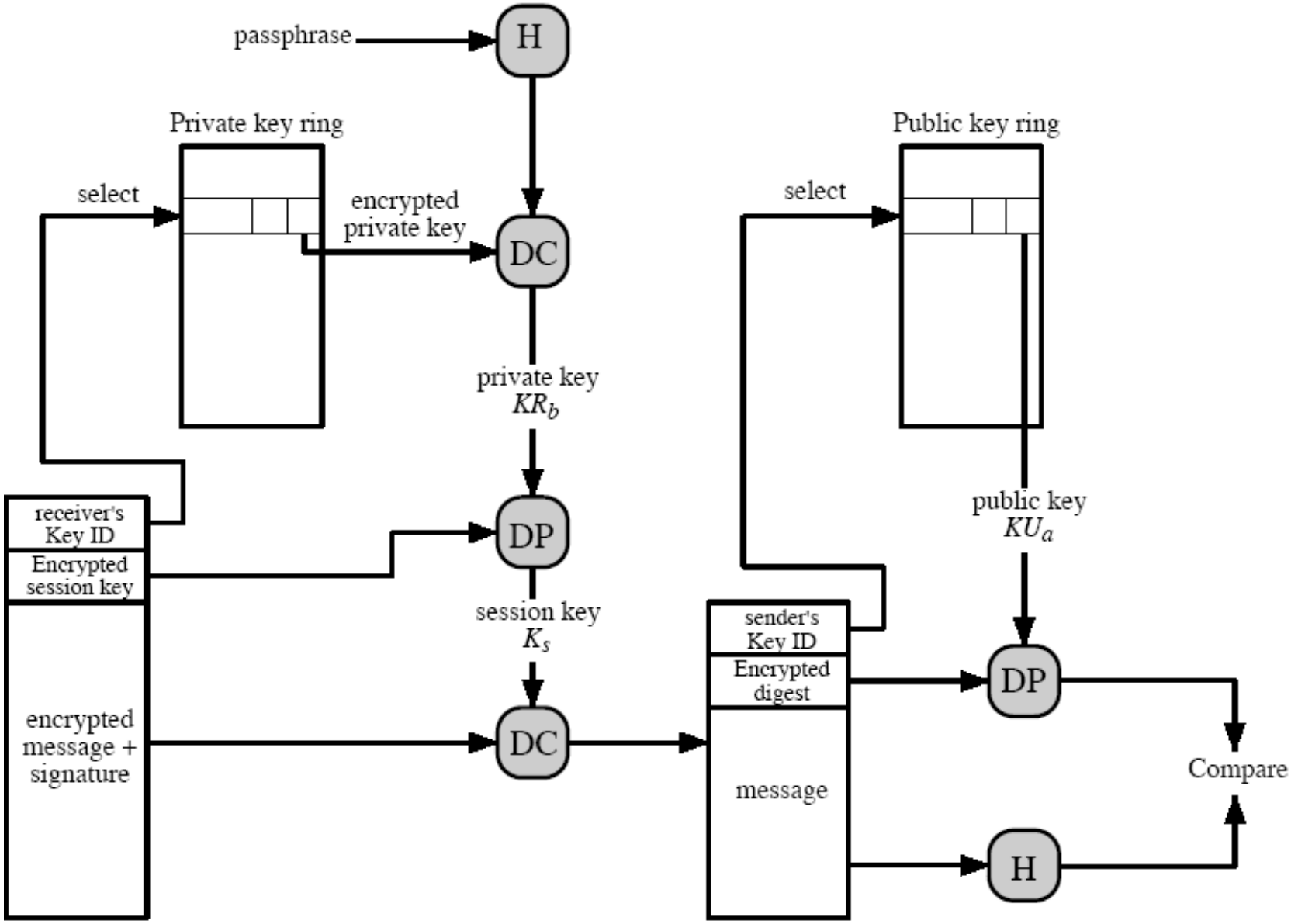


Figure 15.6 PGP Message Reception (from User A to User B; no compression or radix 64 conversion)

巧妙之处

- 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