哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY
立足航天，服务国防，面向国民经济主战场

计算机网络之危机四伏

主讲人：李全龙

本讲主题

安全电子邮件标准

PEM标准

- PEM（Privacy Enhanced Mail）标准
  - IETF与IRTF研究增强E-Mail的保密以及PEM的标准化
  - 1993年初，提出四份RFC(1421~1424)作为建议标准
  - PEM的运行依赖PKI(公钥基础设施)，如CA
    - 没有被广泛配置
  - PEM提供4种安全服务：
    - 邮件加密
    - 报文完整性
    - 发送方的认证
    - 防发送方否认

PGP标准

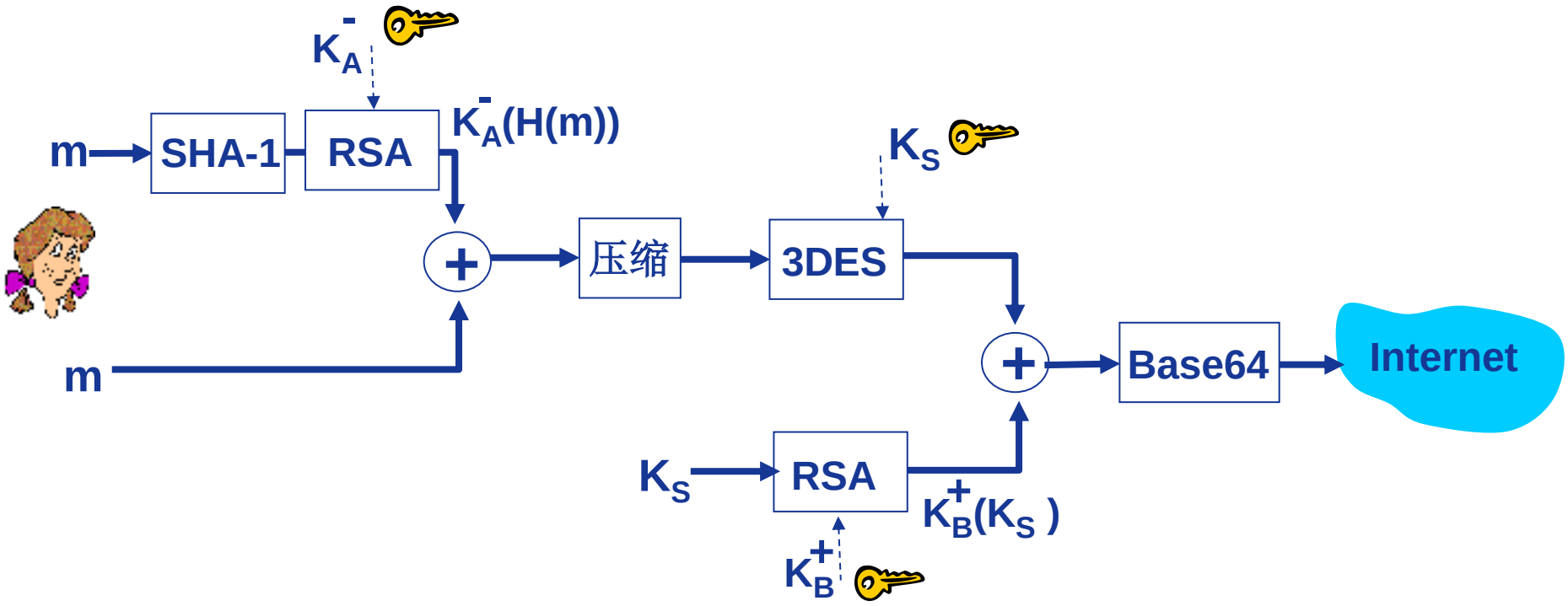
- PGP（Pretty Good Privacy）标准
  - Philip Zimmermann于1991年发布PGP 1.0
    - 事实上标准
  - 可在各种平台（Windows、UNIX等）免费运行
  - 还可用于普通文件加密及军事目的
  - 所用算法被证实为非常安全：
    - 公钥加密算法：RSA、DSS或Diffie-Hellman
    - 对称加密算法：CAST、3DES或IDEA
    - 散列算法：MD5或SHA-1

PGP标准

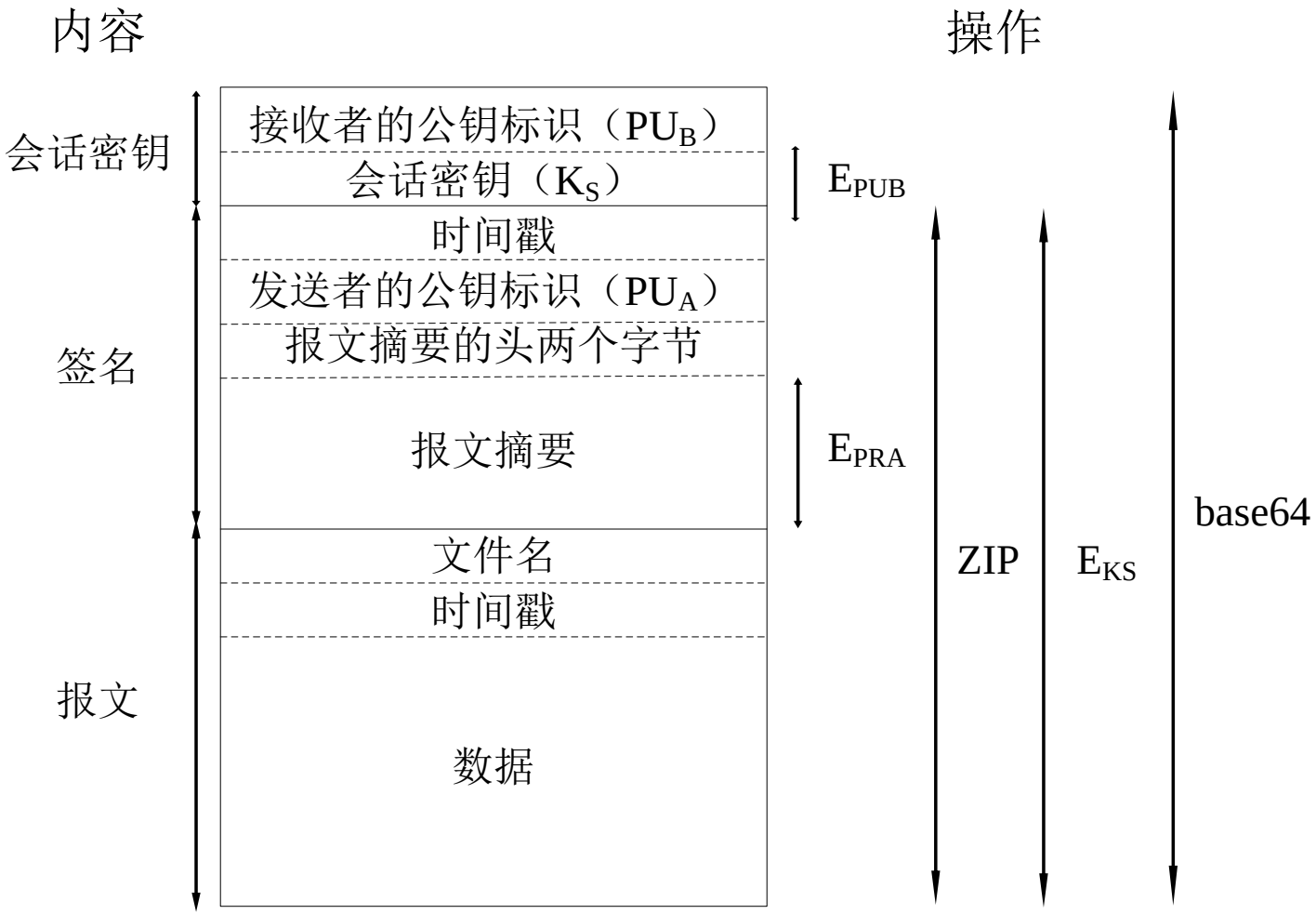
- PGP特点：
  - 对邮件内容进行数字签名，保证信件内容不被篡改
  - 使用公钥和对称加密保证邮件内容机密且不可否认
  - 公钥的权威性由收发双方或所信任的第三方签名认证
  - 事先不需要任何保密信道来传递对称的会话密钥

PGP功能框架

- Alice期望PGP提供保密、发送者认证与报文完整性



PGP报文的格式


内容
操作
会话密钥
签名
报文
接收者的公钥标识（PU_B）
会话密钥（K_S）
时间戳
发送者的公钥标识（PU_A）
报文摘要的头两个字节
报文摘要
文件名
时间戳
数据
E_{PUB}
E_{PRA}
ZIP
E_{KS}
base64

PGP密钥

- 安装PGP时，软件为用户生成一个公开密钥对
  - 公钥放置用户网站或某公钥服务器上
  - 私钥则使用用户口令进行保护
    - 用户为随机生成的RSA私钥指定一个口令，只有给出口令才能将私钥释放出来使用
- PGP公钥认证机制与传统CA差异较大：
  - PGP公钥可以通过可信的Web认证
  - 用户可以自己认证任何其信任的“公钥/用户名”对
  - 用户还可以为其他公钥认证提供“担保”
- 防止篡改公钥的方法（Alice）：
  - 直接从Bob手中得到其公钥
  - 通过电话认证密钥
  - 从双方信任的David那里获得Bob的公钥
  - 通过CA

S/MIME标准

- S/MIME（Secure/Multipurpose Internet Mail Extensions）标准
  - 提供数据保密、完整性和认证等安全服务
  - 不仅限于邮件使用，可用于任何支持MIME数据的传输机制，如HTTP
  - 增加了新的MIME数据类型：
    - “应用 /pkcs7-MIME”（application/pkcs7-MIME）
    - “复合/已签名”（multipart/signed）
    - “应用 /pkcs7-签名”（application/pkcs7-signature）等
  - 只保护邮件的邮件主体，对头部信息则不进行加密
  - 认证机制依赖于层次结构的CA(Tree of Trust)
  - 证书格式采用X.509规范

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

立足航天，服务国防，面向国民经济主战场

谢 谢！