# 第九章 网络安全

## 课前思考


- 计算机网络面临哪些安全威胁？
- 公开密钥密钥体制的基本原理是什么？
- 公开密钥算法主要有哪几种？
- 为什么说身份认证是网络安全的第一道屏障？
- 防火墙与入侵检测系统有什么区别？

# 本章内容

9.1 计算机网络面临的威胁

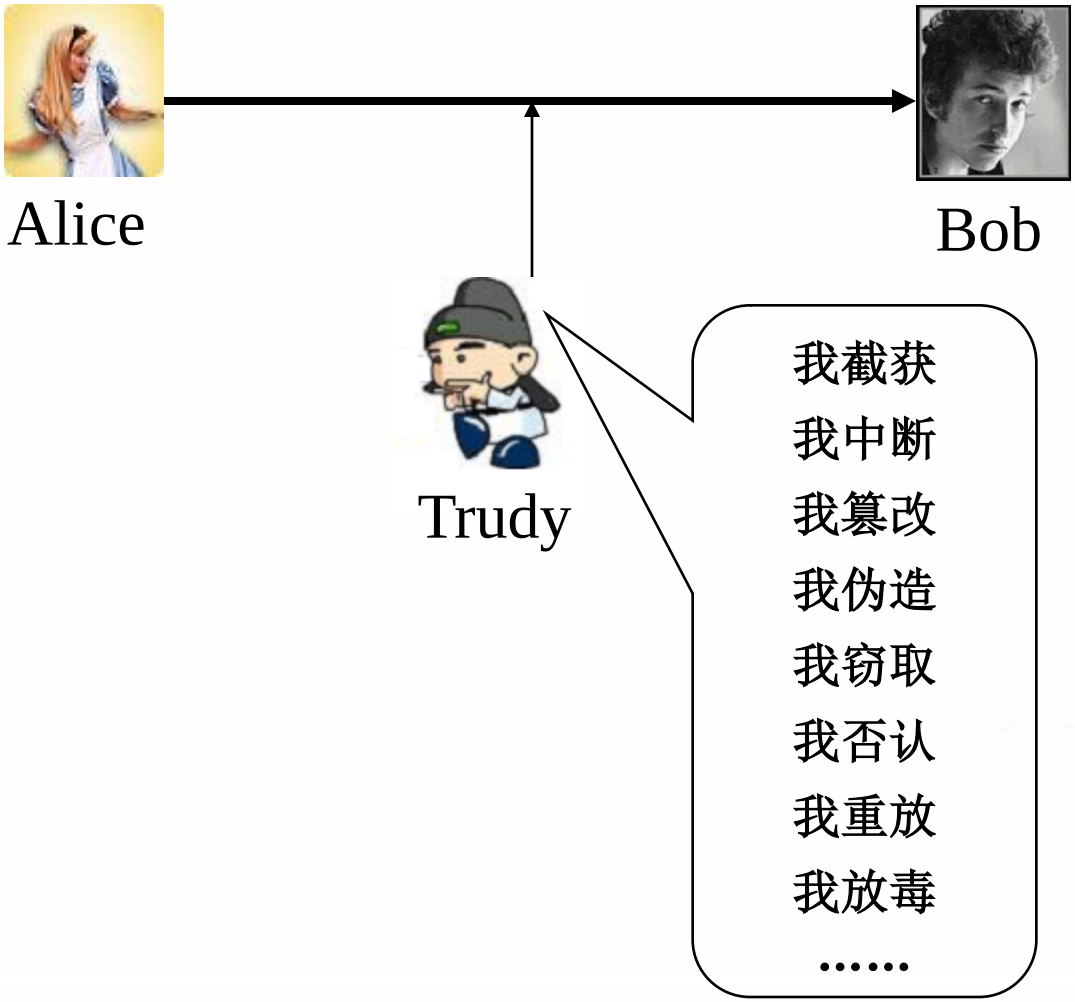
9.2 数据加密

9.3 数字签名

9.4 身份认证

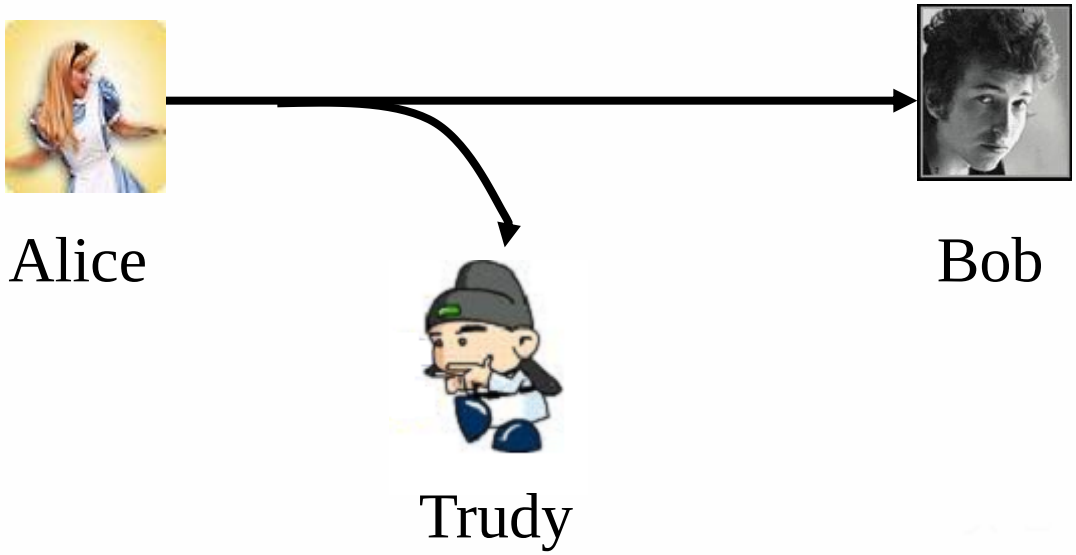
9.5 网络安全技术

# 9.1 计算机网络面临的威胁



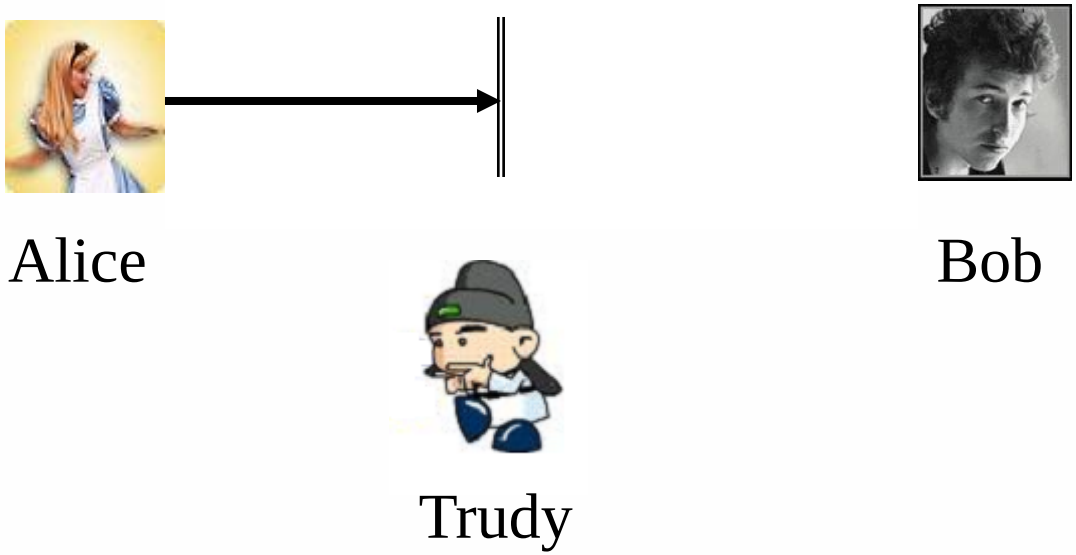
# 9.1 计算机网络面临的威胁

- 截获



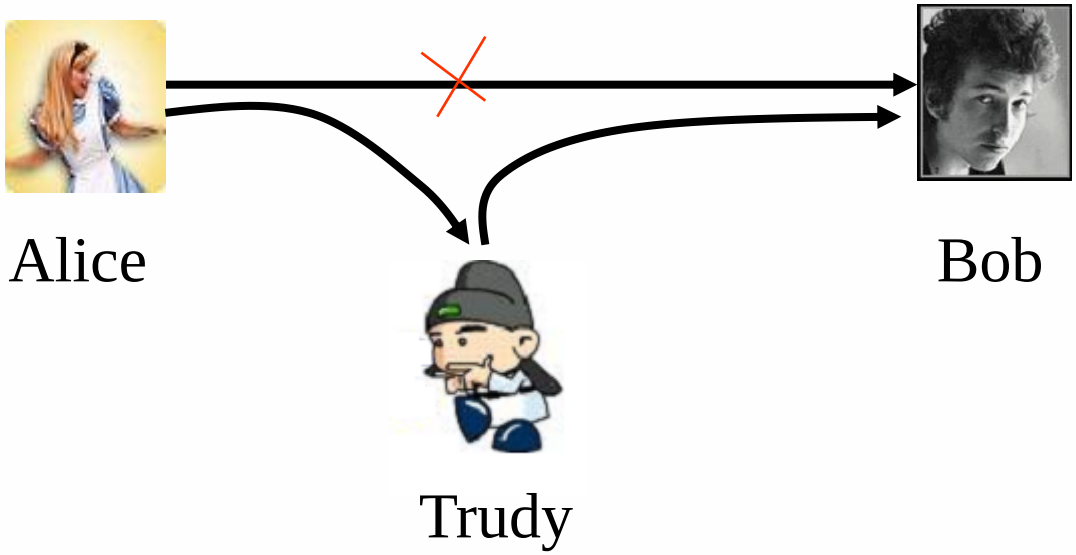
# 9.1 计算机网络面临的威胁

- 中断



# 9.1 计算机网络面临的威胁

- 篡改



# 9.1 计算机网络面临的威胁

- 伪造

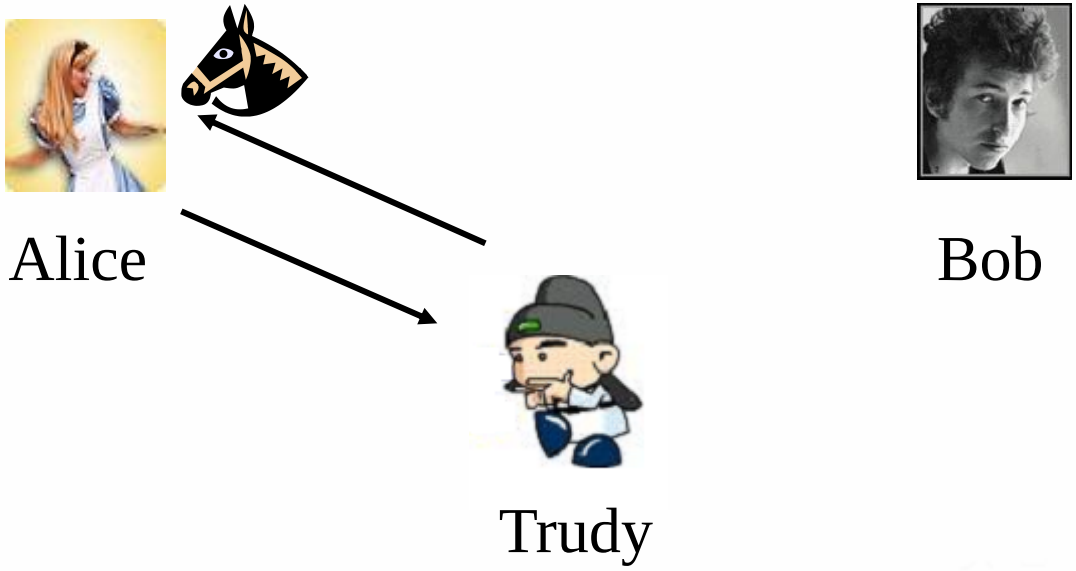
Alice

Trudy

Bob

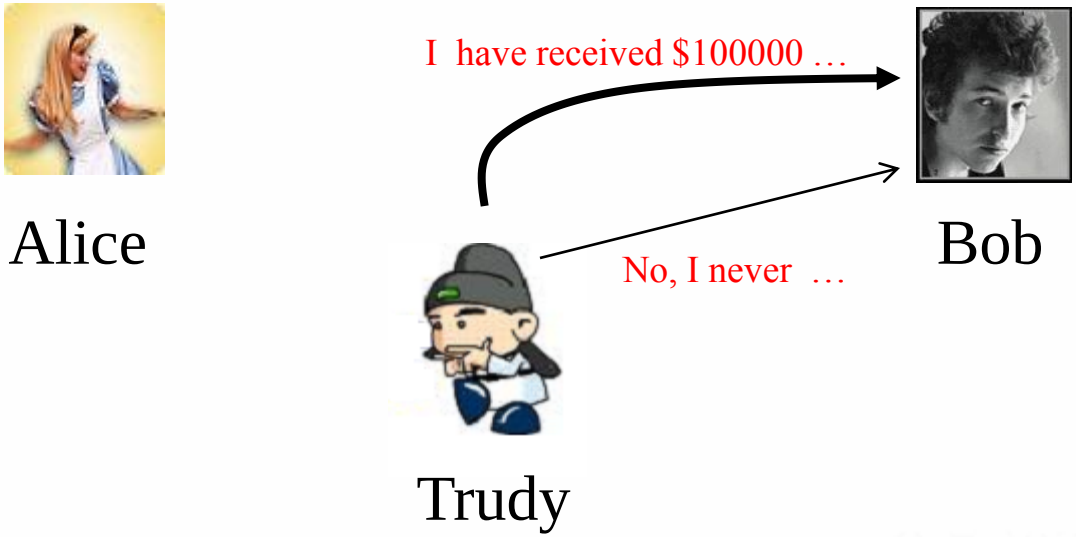
# 9.1 计算机网络面临的威胁

- 窃取



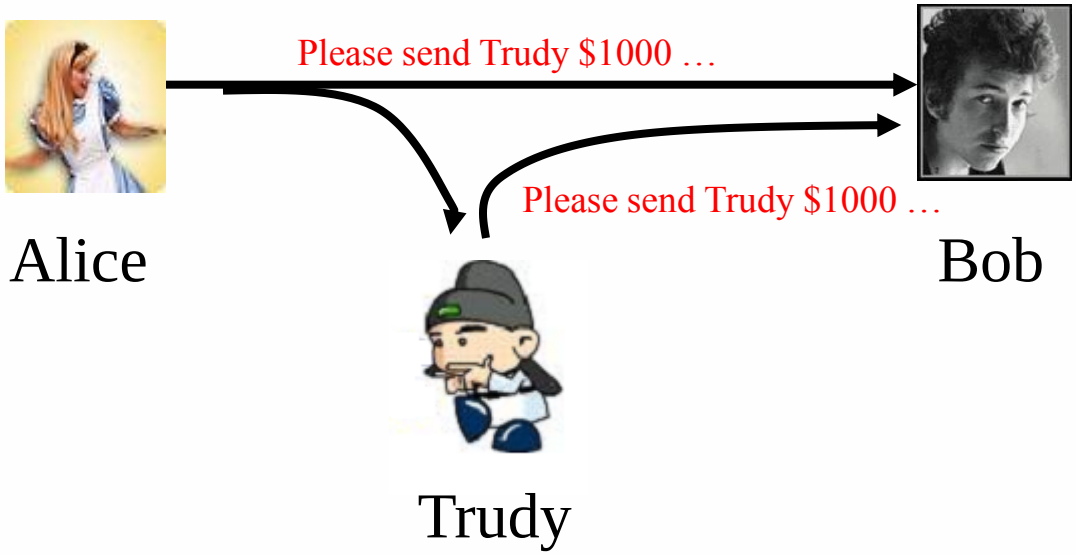
# 9.1 计算机网络面临的威胁

- 否认



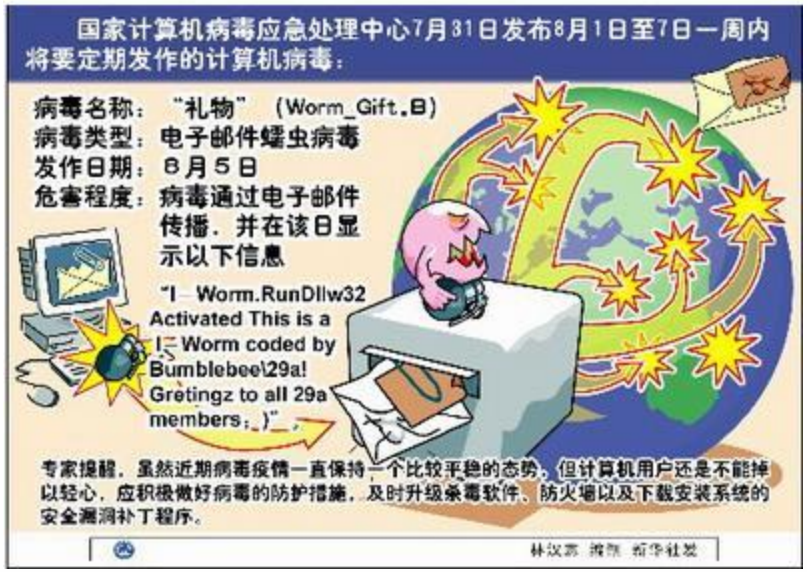
# 9.1 计算机网络面临的威胁

- 重放

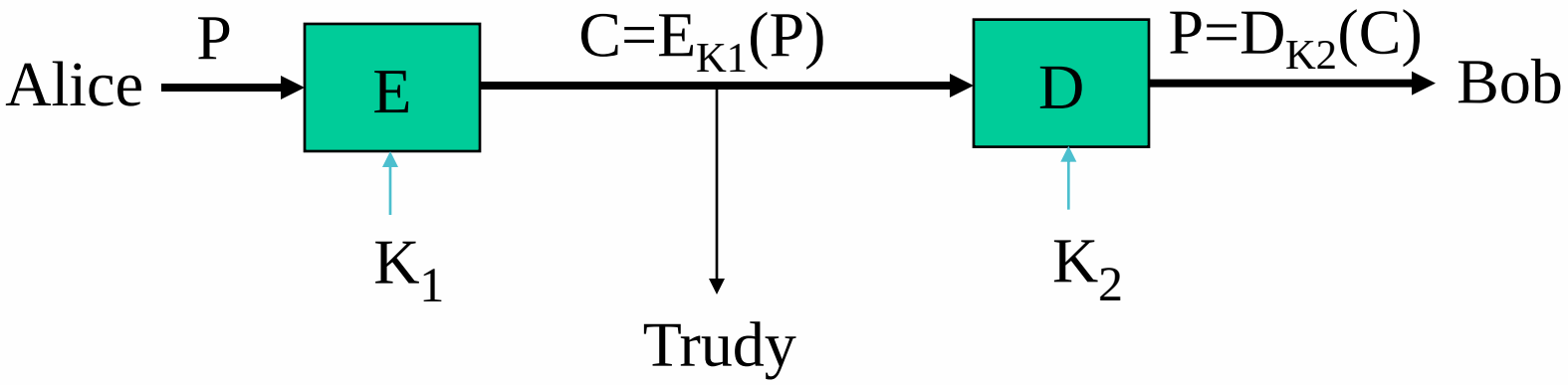


# 9.1 计算机网络面临的威胁

- 网络病毒
  - 木马
  - 蠕虫



## 9.2.1 数据加密模型




P：明文；　　C：密文；

E：加密算法；　　D：解密算法；

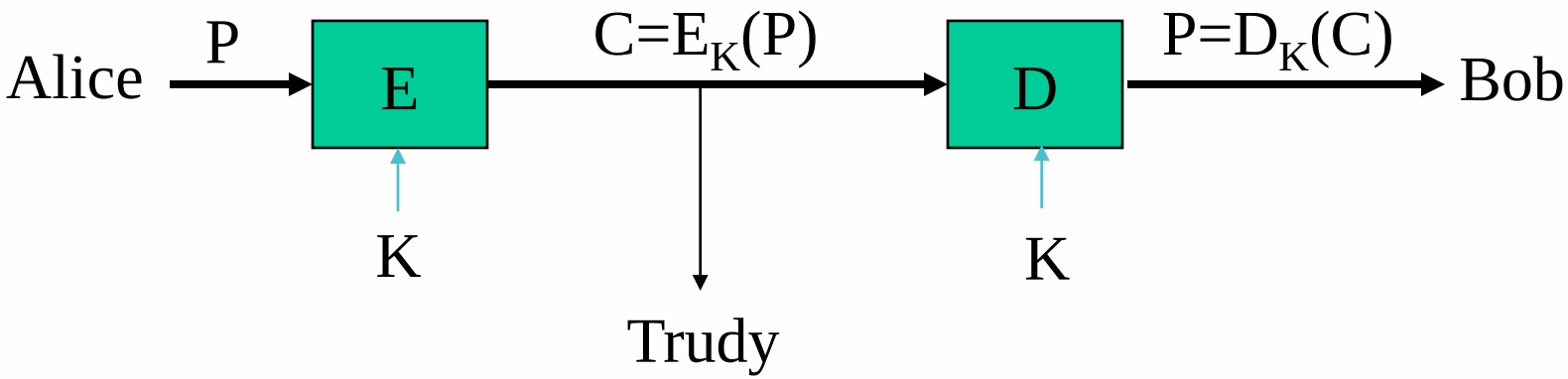
K1：加密密钥；　K2：解密密钥。

通常，加密算法和解密算法是公开的，数据安全性取决与密钥的安全性。

## 9.2.2 数据加密体制分类

数据加密体制有两类：对称密钥体制和非对称密钥体制。

- 对称密钥体制




- 加密密钥和解密密钥相同，所以称为对称密钥体制。
- 对称密钥体制已有两千多年历史，又称为传统密钥体制。

# 9.2 数据加密

- 对称密钥算法
  - 替换算法

这是一种最古老，最简单的加密算法，即将明文中的每个字符替换成另一个字符。

密钥：

| |
|---|
| 明文：a b c….j k l …s t u…x y z |
| 密文：q w e….p a s …l z x…b n m |

明文： attack → 密文:qzzqea

从理论上说，要破译该密码系统需要尝试26！次，这是一个天文数字。然而，根据英文中各字母出现的频度，破译这样的密码是很容易的事。

# 9.2 数据加密

- 置换算法

置换算法是按照某一种规则重新排列明文的字符出现位置。

明文： **Please transfer the file now**

密钥： **M E G A B U C K**

顺序： **7 4 5 1 2 8 3 6**

明文重排： **p l e a s e t r**
**a n s f e r t h**
**e f i l e n o w**

密文：**aflseettolnfesirhwpaeern**

# 9.2 数据加密

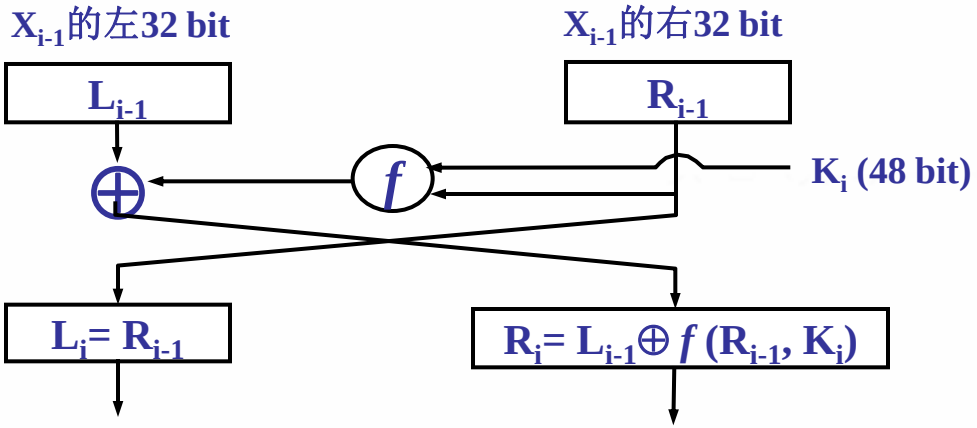
- 数据加密标准（DES）

1977年1月，IBM提出的加密算法lucifer被美国政府定为数据加密标准DES（Data Encryption Standard）。

DES的基本思想：

将明文64位分为一组，进行初始置换，即左32位与右32位交换。然后对56位密钥进行处理，生成16个不同的48位密钥($K_1, K_2, \ldots K_{16}$)，再进行16轮迭代加密，每次输出64 位结果, 并对最后64位结果进行置换（左32位与右32位交换），产生最终64位密文。

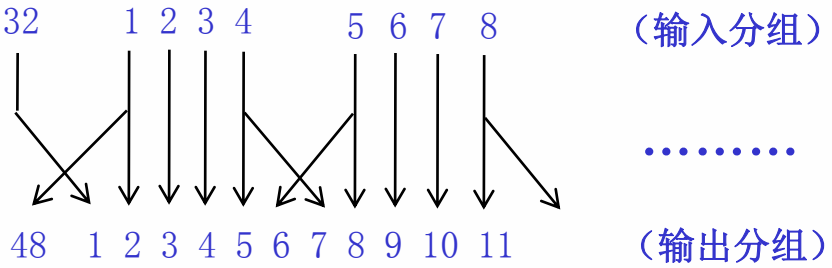
迭代加密过程：



# 9.2 数据加密

$f(R_{i-1}, K_i)$函数包括3步运算：

（1）通过一个扩展置换将$X_{i-1}$的右32 bit扩展成48位；扩展置换过程：每4位输入作为一个分组，第1位和第4位表示输出分组的两位。



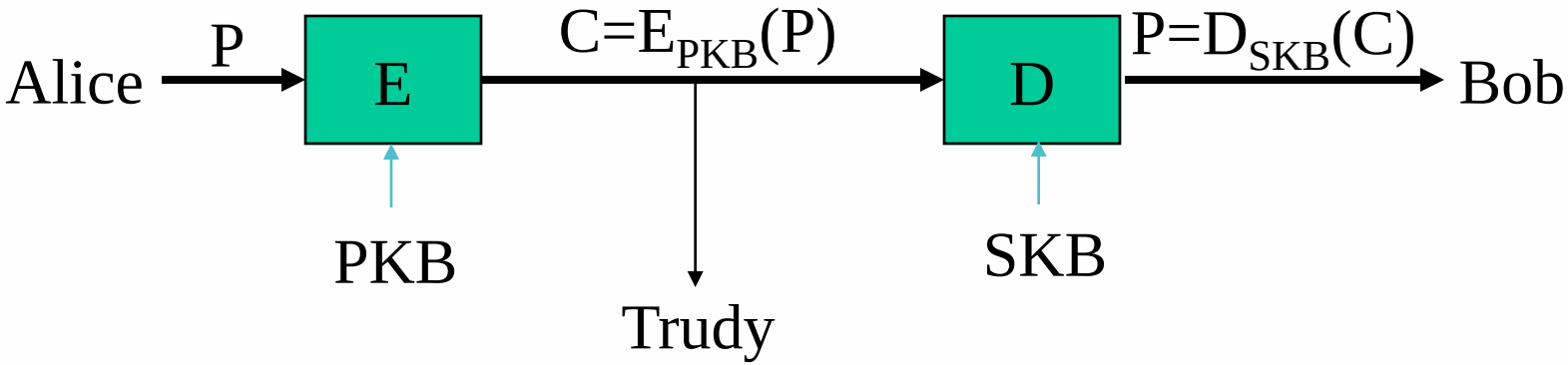

（2）将扩展后的48位与48位密钥进行异或操作。

（3）通过8个不同的S盒将这48位替代为32位数据；每个S盒都有6位输入，4位输出； S盒是一个4行、16列的表，每一个表项都是4位， S盒的6位输入确定其对应的输出在哪一行、哪一列。

# 9.2 数据加密

- 非对称密钥体制

1976年，斯坦福大学的Diffie和Hellman提出非对称密钥体制，又称为公开密钥体制。




- 非对称密钥体制的特征
  - 每个用户都有一个加密密钥PK和一个解密密钥SK，PK公开，SK保密。
  - $D_{SK}(E_{PK}(P)) = P$

    $D_{PK}(E_{PK}(P)) \neq P$
  - 已知SK很容易导出PK，已知PK很难导出SK。
  - 加密和解密运算可以对调，即$E_{PK}(D_{Sk}(P)) = P$，这一特征用于数字签名。

# 9.2 数据加密

- 非对称密钥算法 (公钥算法)
  - 背包公钥算法
  - RSA公钥算法
  - 离散对数公钥算法
  - 椭圆曲线公钥算法
- RSA公钥算法
  - 用户秘密地选择两个大素数p和q，计算 $n = p \times q$ 和 $z = (p-1) \times (q-1)$。
  - 秘密地选择一个与z互素的数d作为解密密钥（私钥）。
  - 解同余方程：$(e \times d) \bmod z \equiv 1$，得到加密密钥e（公钥）。
  - (e,n)公开，(d,z)保密。
  - 将明文**P**视为二进制整数，则明文**P**应满足： **P** <n。如果明文太长，则分块处理。
  - 加密：$\mathbf{C} = \mathbf{P}^e \bmod n$
  - 解密：$\mathbf{P} = \mathbf{C}^d \bmod n$

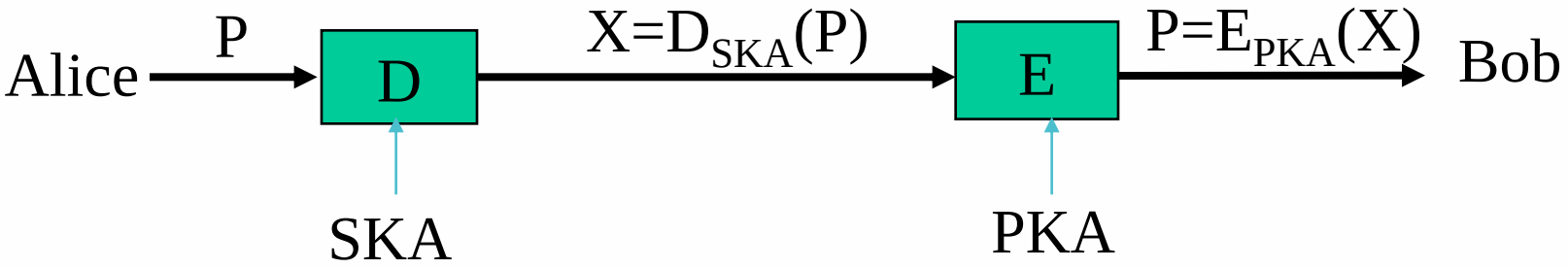
RSA安全性基于大数分解的困难性，即当$n = p \times q$足够大时，已知n，很难求出p和q。

# 9.2 数据加密

- RSA公钥算法示例
  - 选择p = 3，q = 11。
  - n = p×q = 33　z = (p-1) ×(q-1) = 20 。
  - 再选择d = 7（7与20互素） 。
  - 求解同余方程：7×e mod 20≡1 得 e=3 。
  - 设明文 **P** = $(10011)_2$ = 19 < 33。
  - 加密：**C** = $\mathbf{P}^3$ mod n
    = 6859 mod 33
    = 28
    = $(11100)_2$
  - 解密：**P** = $\mathbf{C}^7$ mod n
    =13492928512 mod 33
    =19
    = $(10011)_2$

# 9.3 数字签名

- 数字签名是对电子文档签名，须满足如下三个条件：
  - 接收者能够核实发送者对报文的签名。
  - 发送者不能抵赖对报文的签名。
  - 接收者不能篡改已签名的报文。
- 基于公开密钥体制实现数字签名的基本原理




  - Bob用PKA解开报文**P**，则确信**P**是Alice发来的。
  - 若Alice否认已发送过报文**P**，则Bob向第三方出示**P**和$D_{SKA}(\mathbf{P})$，第三方用PKA解开$D_{SKA}(\mathbf{P})$中的**P**，证实Alice确实发送过**P**。
  - 若Bob将**P**改成**P'**，则无法出示$D_{SKA}(\mathbf{P'})$。

# 9.3 数字签名

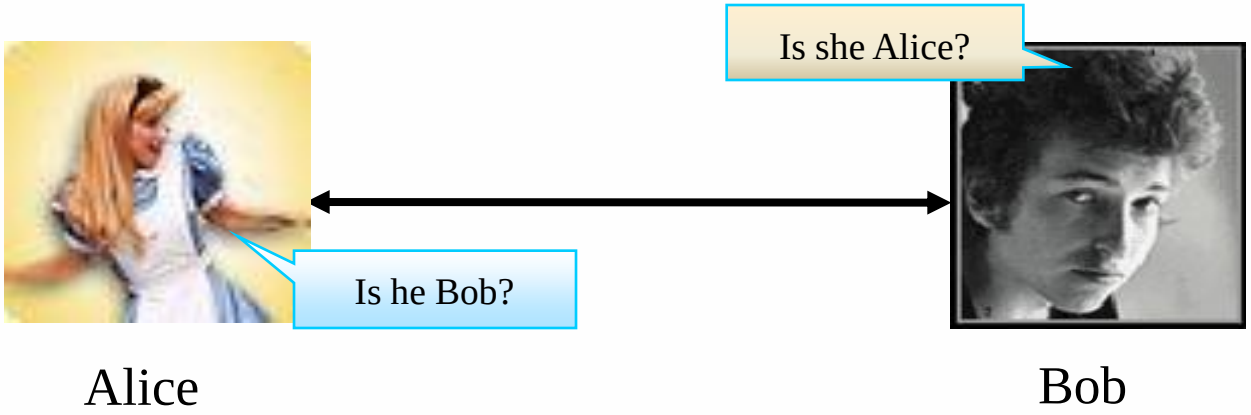
- 基于RSA的数字签名算法
  - 设m为待签报文，H为一Hash函数。
  - 生成密钥对（公钥和私钥）
    - 签名者秘密地选择两个大素数p和q，计算 $n = p \times q$ 和 $z = (p-1) \times (q-1)$。
    - 秘密地选择一个与z互素的数d作为解密密钥（私钥）。
    - 解同余方程：$(e \times d) \bmod z \equiv 1$，得到加密密钥e （公钥）。
    - (e,n)公开，(d,z)保密。
  - 产生签名
    - 签名者计算： $M = H(m)$

      $S = M^d \bmod n$
    - 将(m, S)发送给验证者 。
  - 验证签名
    - 验证者计算： $M' = S^e \bmod n$
    - 若 $M' = H(m)$ ， 则签名有效。

提示：采用Hash函数的目的是为了减少待签报文的长度，提高效率。

# 9.4 身份认证

- 身份认证的含义
  - 证实通信双方的真实身份。



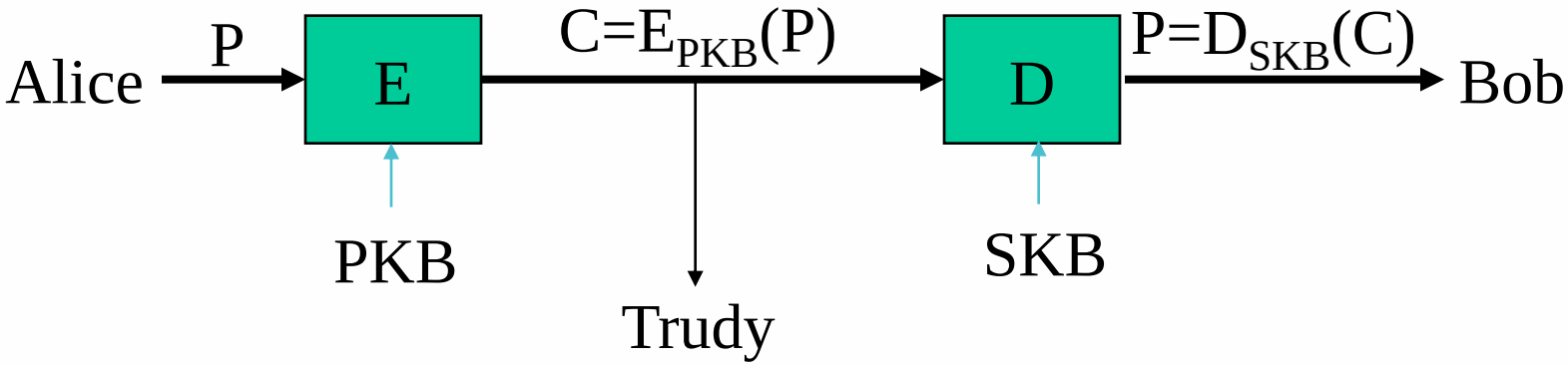

- 身份认证是保障网络安全的第一道屏障
- 身份认证技术
  - 基于主体知道的秘密，如口令、密钥。
  - 基于主体拥有的物品，如IC卡、USB Key。
  - 基于主体具有的特征，如指纹、声音、视网膜。

# 9.4 身份认证

- 基于密钥的身份认证
  - 基本原理：通信前，Alice对消息进行加密，只有Bob能够解密，因为只有Bob知道密钥；换句话说，能够解密的一定是Bob。
  - 在对称密钥体制中，通信双方必须约定一个共享密钥。如Alice和Bob事先约定一个共享密钥“666888”， Alice与Bob之间传输的消息用“666888”加密，从而使Alice确信对方一定是Bob， Bob确信对方一定是Alice （如果Trudy假冒，则无法解密）。但在实际应用中如何约定共享密钥是一件麻烦事。
  - 在非对称密钥体制中，基于密钥的认证可转化为对公钥的认证 。

# 9.4 身份认证

- 公钥认证问题

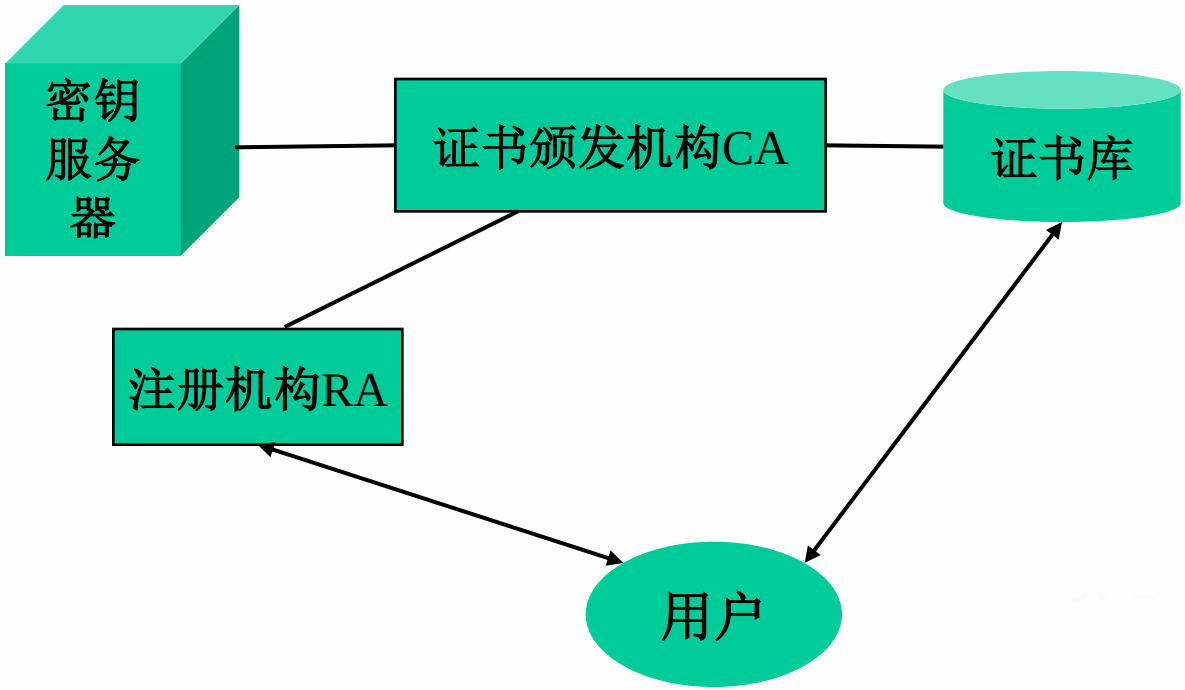



- Alice进行加密之前必须确信只有Bob才能解密，即使用Bob的公钥PKB进行加密（设真实的PKB 为3721）。
- Trudy可能假冒Bob，宣称：“我是Bob，我的公钥PKB是4728”。如果Alice用4728进行加密，其结果是Bob不能解密，而Trudy却能够解密。
- Alice如何确信PKB确实是3721而不是4728？即如何对Bob的公钥PKB进行认证？

# 9.4 身份认证

- 公钥基础设施PKI（Public Key Infrastructure）

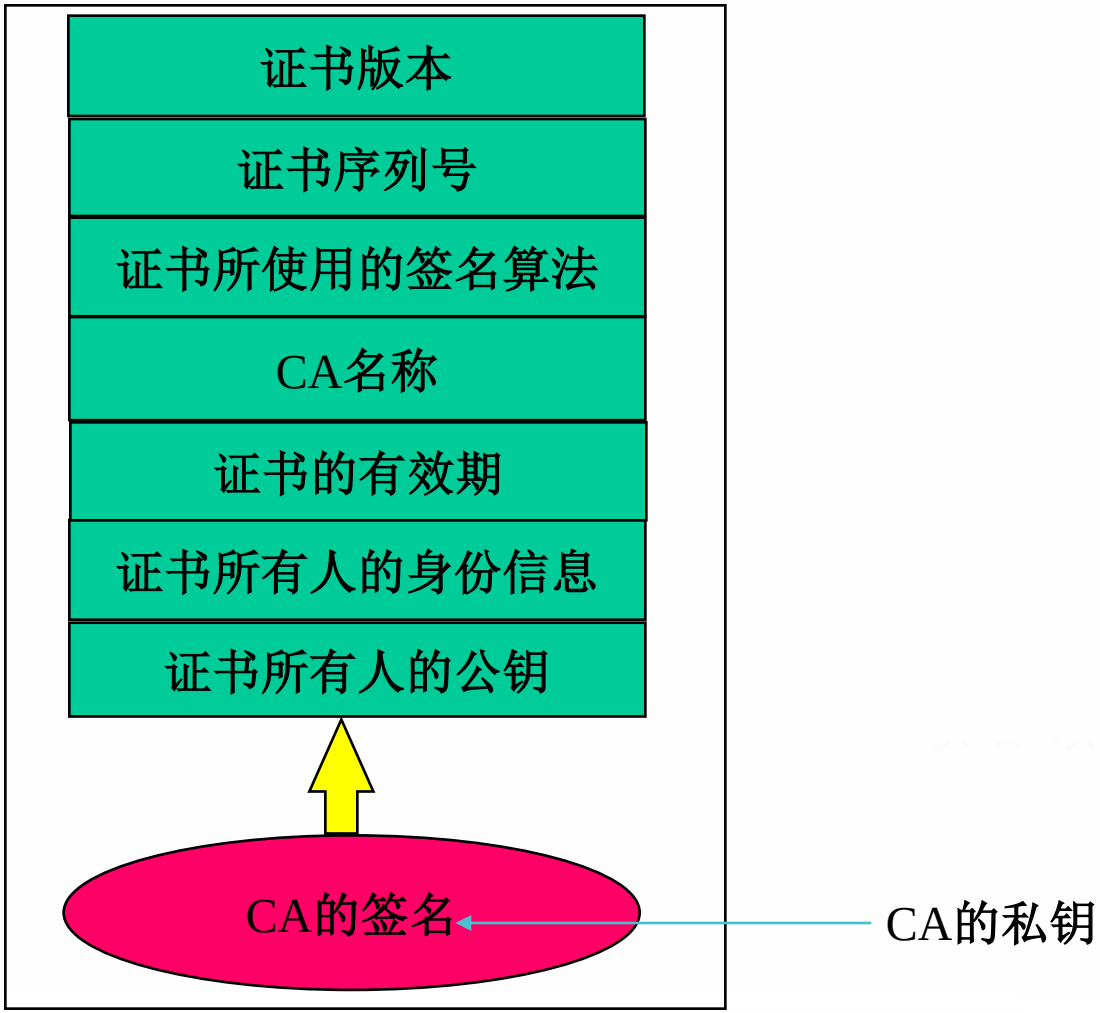
PKI是一种标准的密钥管理平台，它以离线方式为数据加密和数字签名等提供公钥认证，进而实现身份认证。 PKI的组成如下：




- 证书颁发机构（CA）是可信的第三方，负责颁发、管理和撤消公钥证书（数字证书）。

# 9.4 身份认证

- 公钥证书用来宣布主体公钥的真实性，其格式（X.509标准）如下：



# 9.4 身份认证

- 注册机构（RA）可视为PKI 的一个扩展，充当PKI与用户之间的桥梁，分担CA的部分功能，包括：
  - 验证用户注册信息。
  - 代表用户生成密钥对。
  - 接收证书授权和吊销请求。
  - ……
- 证书库是公开的信息库，用于存放公钥证书，以便用户查询。
- PKI工作流程
  - Alice向RA提交注册信息，包括用户标识，用户其他基本信息等。
  - RA为Alice生成密钥对，并将密钥对通过安全信道发送给Alice 。
  - RA将Alice的用户标识、公钥等信息提交给CA，请求颁发公钥证书。
  - CA产生公钥证书，并用自己的私钥对其签名。
  - CA将Alice的公钥证书存放到证书库中，供其他用户查询。
  - Bob从证书库中查到Alice的公钥证书，并用CA的公钥进行验证。

# 9.5 网络安全技术

- 防火墙技术
- 入侵检测系统
- 网络准入技术
- 网络访问行为审计
- ……

# 本章小结

- 主要内容：

  主要介绍网络安全概述、数据加密技术（包括对称密钥体制和非对称密钥体制）、数字签名和身份认证等。

- 重点：

  非对称密钥体制和数字签名。