第七讲
公钥密码与报文鉴别

郑燕飞

认证与认证系统

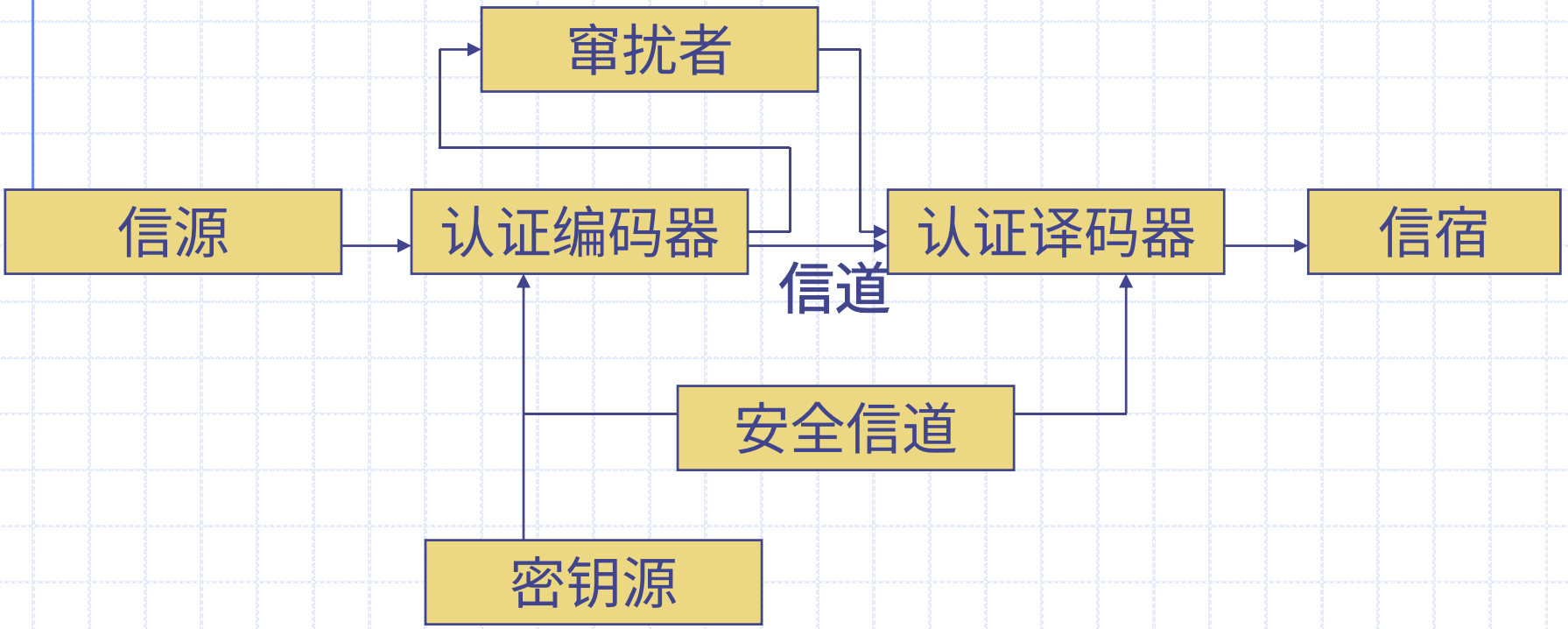
- 认证(Authentication)是防止主动攻击的重要技术,对开发系统安全性有重要作用.
- 认证的主要目的
  - 实体认证(发送者非冒充)
  - 消息认证(验证信息的完整性)

认证与认证系统(Cont.)

- 网络环境中的攻击(认证的需求)
  - 1.泄漏
  - 2.通信量分析
  - 3.伪装(假报文)
  - 4.内容篡改(插入,删除,调换和修改)
  - 5.序号篡改(报文序号的修改)
  - 6.计时篡改(报文延迟或回放)
  - 7.抵赖(否认收或发某报文)

1,2加密, 3~6报文认证, 7数字签名(3~6)

保密和认证同时是信息系统安全的两个方面，但它们是两个不同属性的问题，认证不能自动提供保密性，而保密性也不能自然提供认证功能。一个纯认证系统的模型如下图所示：



认证与认证系统

- 三类产生认证符的函数
  - 报文加密

以整个报文的密文为认证码;

  - 报文认证码(MAC)

以报文和密钥为输入的公共函数产生的定长值作为认证符;

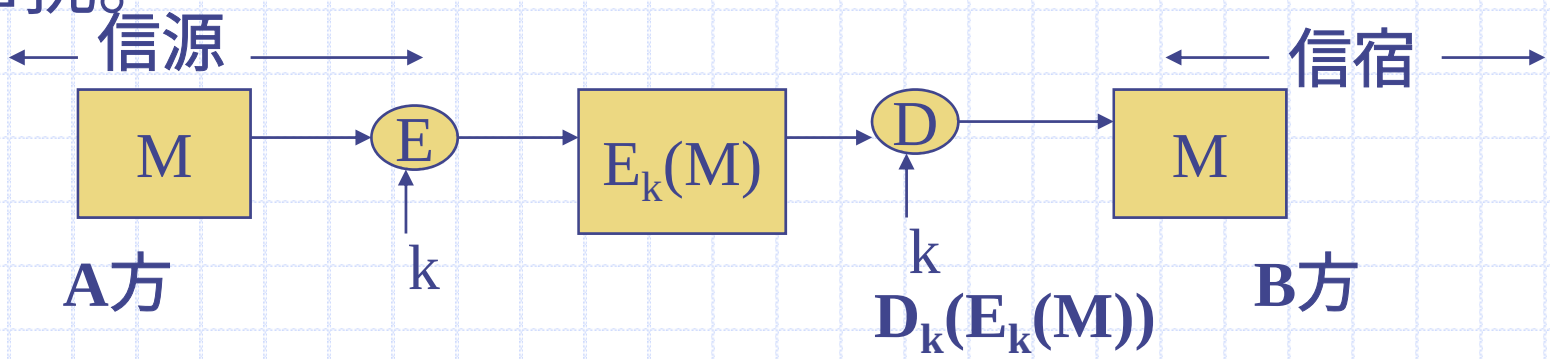
  - 散列函数

一个将任意长度的报文映射为定长的散列值的公共函数,以散列值作为认证符;

报文加密提供认证

- 常规加密

下图的通信双方，用户A为发信方，用户B为接收方。用户B接收到信息后，通过解密来判决信息是否来自A，信息是否是完整的，有无窜扰。

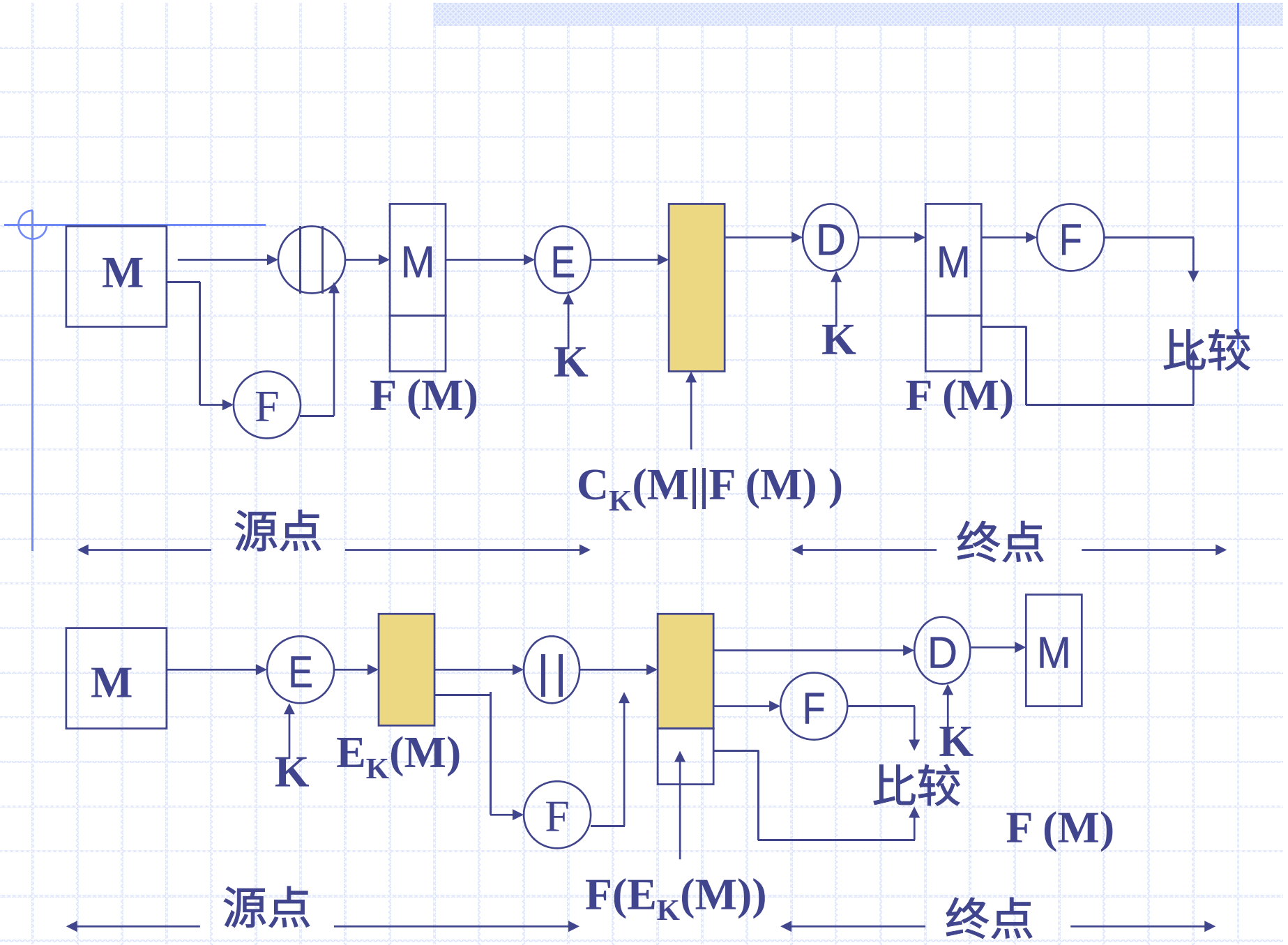


常规加密：具有机密性，可认证

- 常规加密

问题:如果报文是任意比特的组合,接收方没有自动的方法确定报文的合法性.

解决方案:强调明文的某种结构,这种结构是易于识别但不能复制且无需加密的.


M
F
M
F (M)
E
K
D
K
M
F (M)
F
比较
$C_K(M||F(M))$
源点
终点
M
E
K
$E_K(M)$
F
F
D
K
比较
M
F (M)
$F(E_K(M))$
源点
终点

常规(对称)加密与认证的关系

A->B: E(K, M)

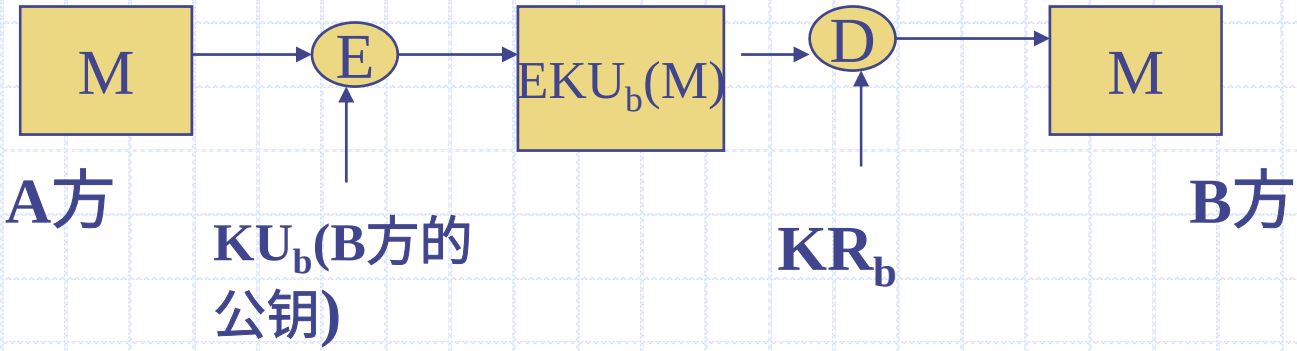
- 提供保密(仅A和B共享密钥K)
- 提供一定程度的认证
  - 仅来自A
  - 传输中不会被更改
  - 需要某种结构或冗余
- 不提供签名
  - 接收者可以伪造报文
  - 发送者可以否认报文

报文加密提供认证(Cont.)

- 公开密钥加密
  - 发送方用自己的私钥加密报文,接收方用发送方的公钥解密(与对称密钥加密原理相同,需要某种特定报文结构).该方案不提供加密.
  - 发送方先用自己的密钥加密以提供认证,然后使用接收方公钥加密提供保密性.缺点是效率不高.

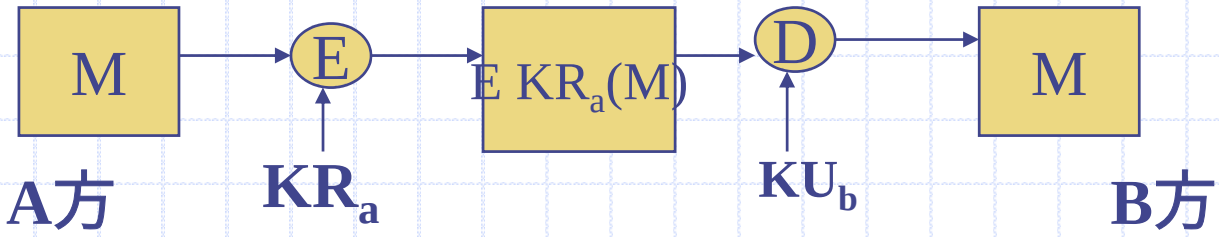
公开密钥加密与认证的关系

- A->B: E(KU_b,M)
  - 提供保密(仅B能解密)
  - 不提供认证



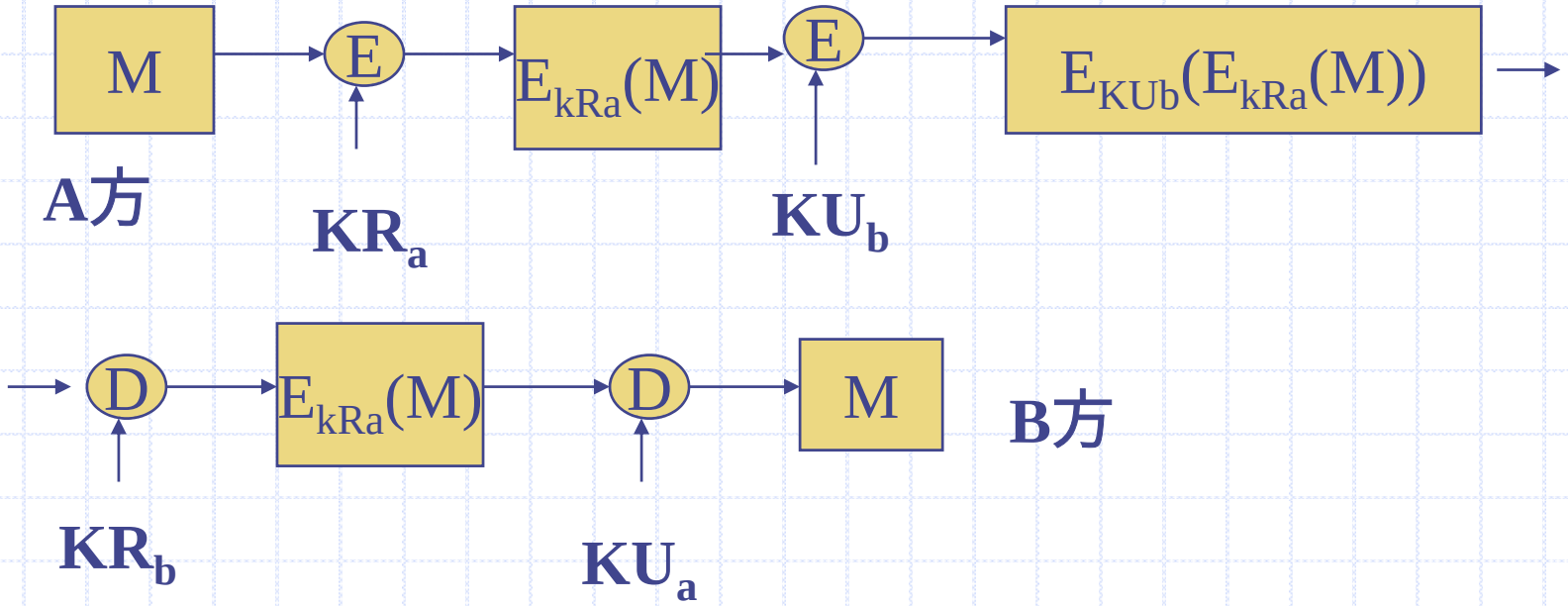
(1) 公钥加密：具有机密性

- A->B: E(KR_a,M)
  - 提供认证和签名(仅有A可加密,需要某种结构和冗余,任何一方均能验证签名)



(2) 公钥加密：认证和签名

- A->B: $E(KU_b, E(KR_a, M))$
  - 可提供保密
  - 可提供认证和签名



(3) 公钥加密：机密性，可认证和签名

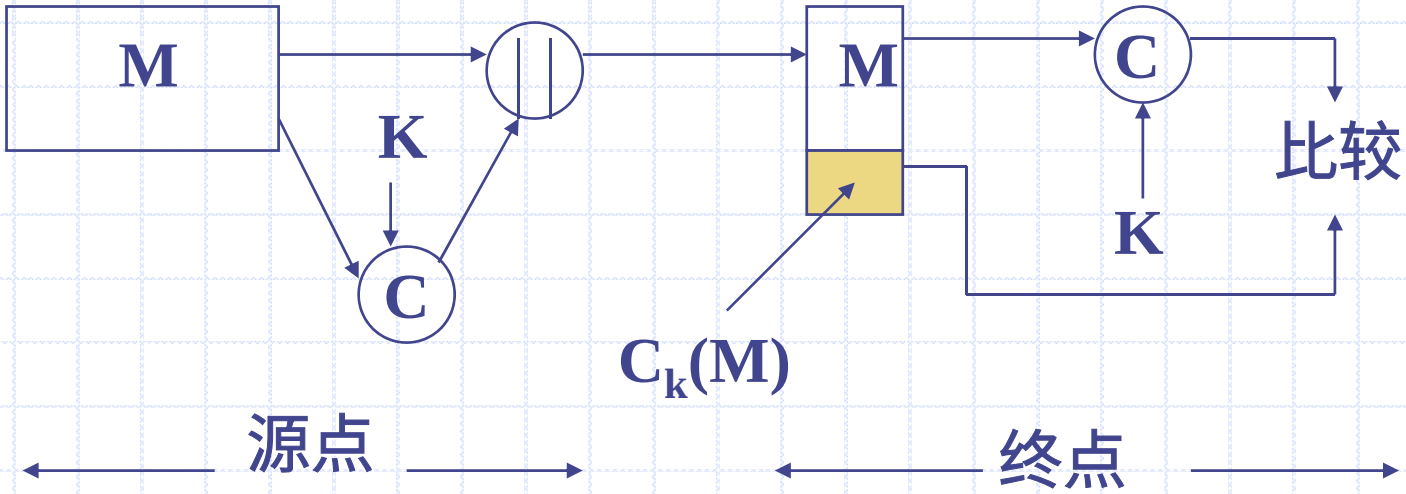
报文认证码(MAC)

- 认证码(MAC,也称密码检验和)
  - 对选定报文,使用一个密钥,产生一个短小的定长数据分组,称认证码,并将它附加在报文中,提供认证功能. (MAC = $C_k(M)$,其中M是可变长的报文, K是共享密钥,$C_k(M)$是定长的认证码.)
- 应用认证码,如果只有收发方知道密钥,同时收到的MAC与计算得出的MAC匹配:
  - 确认报文未被更改;
  - 确信报文来自所谓的发送者;
  - 如果报文包含序号,可确信该序号的正确性;

报文认证码(MAC)

- 报文认证码的基本用法1
  - A->B: M || Ck(M)

    提供认证, 因仅A和B共享K;

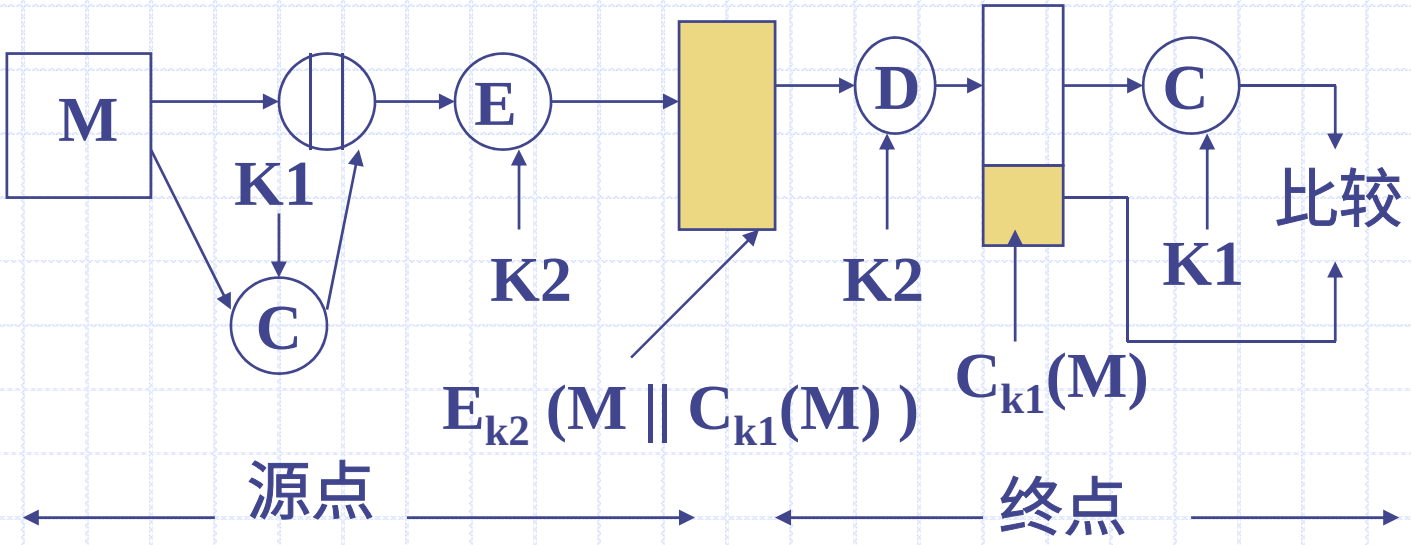


报文认证码(MAC)

- 报文认证码的基本用法2
  - A->B: E_{k2} (M || C_{k1}(M))

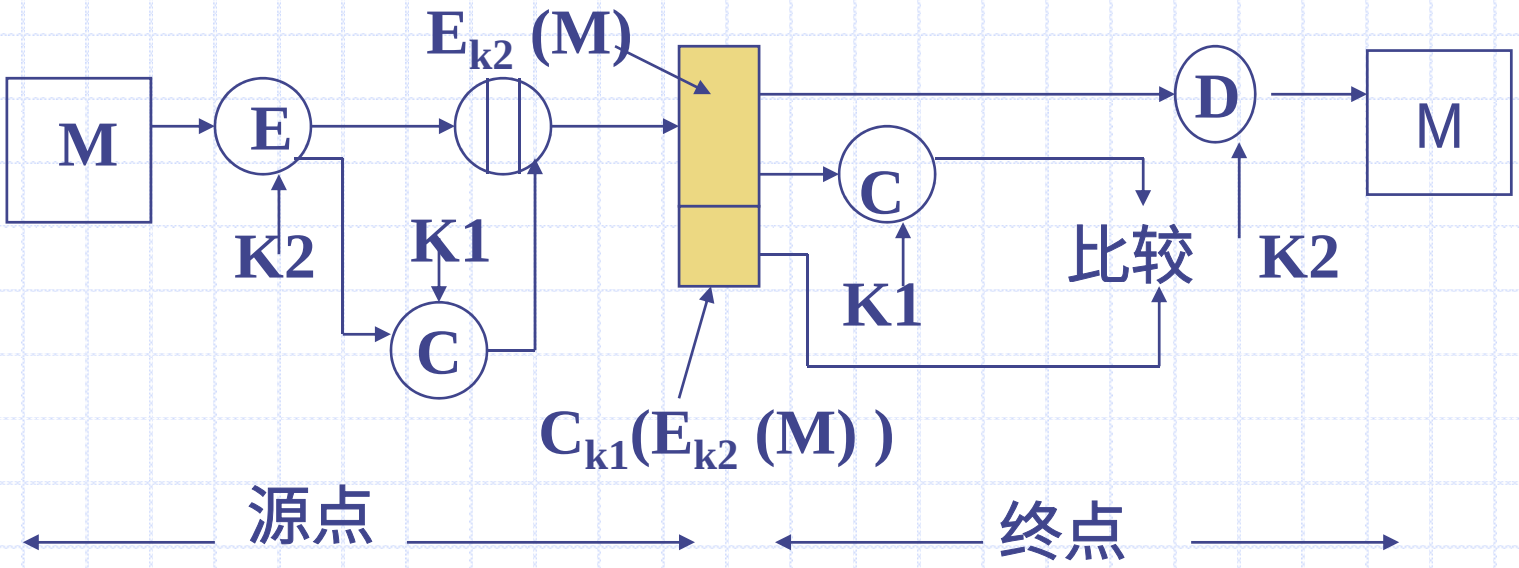
    提供认证, 因仅A和B共享K1;

    提供保密,因仅A和B共享K2;



报文认证码(MAC)

- 报文认证码的基本用法3
  - A->B: E_{k2} (M) || $C_{k1}(E_{k2}$ (M))
    提供认证, 因仅A和B共享K1;
    提供保密,因仅A和B共享K2;



报文认证码(MAC)

- 为什么使用报文认证(而不是用常规加密)
  - 适用于报文广播(并不需要每个点都有密钥);
  - 报文加密解密的工作量比较大;
  - 某些应用不关心报文的保密而只关心报文的真实性;
  - 认证函数与保密函数的分离能提供结构上的灵活性(认证与保密可在网络协议的不同层次进行).
  - 认证码可延长报文的保护期限,同时能处理报文内容(使用加密,当报文解密后,保护就失效了).

报文认证码(MAC)

- 注意
  - 认证函数类似加密函数,但它是不可逆的,这个性质使其比加密函数更难破解;
  - 认证函数并不提供数字签名;
- 认证码的信息论
  - G.J. Simmons发展的认证系统的信息理论,类似保密系统的信息理论,也是将信息论用于研究认证系统的理论安全性和实际安全性问题,指出认证系统的性能极限以及设计认证码必须遵循的原则,是研究认证问题的理论基础.

报文认证码(MAC)

- MAC函数应有如下性质(攻击者没有K):
  - 有M和$C_k(M)$,试图生成M', 使得$C_k(M')=C_k(M)$, 这在计算上不可行;
  - $C_k(M)$应能均匀分布;对于随机选取的报文M和M', $C_k(M)= C_k(M')$的概率为2^{-n}其中n 为MAC的比特长度;(抗选择明文攻击)
  - 报文M'为M的某种已知代换,即M'=f(M),则$C_k(M)= C_k(M')$的概率为2^{-n}.

报文认证码(MAC)

- 基于DES的报文鉴别码

描述如下:

被鉴别报文分成连续的64bit分组:$D_1,D_2,\ldots$ D_n(必要时用0填充).使用DES算法E,密钥K,数据鉴别码计算如下(16<= M <=64):

$$C_1 = E_k(D_1)$$
$$C_2 = E_k(D_2 \oplus C_1)$$
$$\cdots$$
$$C_n = E_k(D_n \oplus C_{n-1})$$

散列函数

- 散列函数
  - 散列函数是将任意长度的报文映射成一个较短的定长输出报文的函数.
  - 如下形式: h = H(M), M是变长的报文,h是定长的散列值.
  - 散列函数的目的是为文件、报文或其它的分组数据产生“数字指纹”.

散列函数

- 使用散列码提供报文鉴别的方式
  - (a) A->B: E_k(M || H(M))
    - 提供保密**(仅A和B共享K)**
    - 提供鉴别**(加密保护 H(M))**
  - (b) A->B: M || E_k(H(M))
    - 提供鉴别**(加密保护 H(M))**
  - (c) A-> B: M || E_{KRa}(H(M))
    - 提供鉴别和数字签名**(加密保护 H(M) ,且仅A能生成E_{KRa}(H(M))**

散列函数

- 使用散列码提供报文鉴别的方式(续.)
  - (d) A->B: $E_k(M \,||\, E_{KRa}(H(M)))$
    - 提供鉴别和数字签名
    - 提供保密(仅A和B共享K)
  - (e)A->B: $M \,||\, H(M \,||\, S)$
    - 提供鉴别(S是通信双方共享的一个秘密值, 仅A和B共享S)
  - (f)A->B: $E_k(M \,||\, H(M \,||\, S))$
    - 提供鉴别 (仅A和B共享S)
    - 提供保密(仅A和B共享K)

散列函数

- 杂凑函数的需求
  - H能用于任何大小的数据分组;
  - H产生定长输出;
  - 对任意给定的x, H(x)要相对易于计算,使得软硬件实现都实际可行;
  - 对任意给定的码h, 寻求x使得H(x)=h在计算上是不可行的(单向性);
  - 任意给定分组x, 寻求不等于x的y, 使得H(y)= H(x)在计算上不可行(弱抗冲突性);
  - 寻求对任何的(x,y)对使得H(x)=H(y)在计算上不可行(强抗冲突性);

散列函数

- 简单的杂凑函数

  每个分组按比特异或:

  $C_i = b_{i1} \oplus b_{i2} \oplus \ldots\ldots \oplus b_{im}$

  其中, C_i是第I个比特的散列码,$1 \le i \le n$;

  m是输入的n比特分组数;

  b_{ij}是第j分组的第I比特;

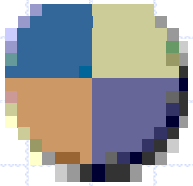
  (简单的奇偶校验)

  针对应用中的可预测数据格式,提出如下改进方案:

散列函数

- 简单的散列函数的改进方案
  - 先将n比特的散列值设置为0;
  - 按如下方式依次处理数据分组:
    - 将当前的散列值循环左移一位.
    - 将数据分组与散列值异或形成新的散列值.

这将起到输入数据完全随机化的效果,并且将输入中的数据格式掩盖掉.



END