密 码 学

（第十四讲）

认证

张焕国

武汉大学计算机学院

目　录

1、密码学的基本概念
2、古典密码
3、数据加密标准（DES）
4、高级数据加密标准（AES）
5、中国商用密码（SMS4）
6、分组密码的应用技术
7、序列密码
8、习题课：复习对称密码
9、公开密钥密码（1）

目　录

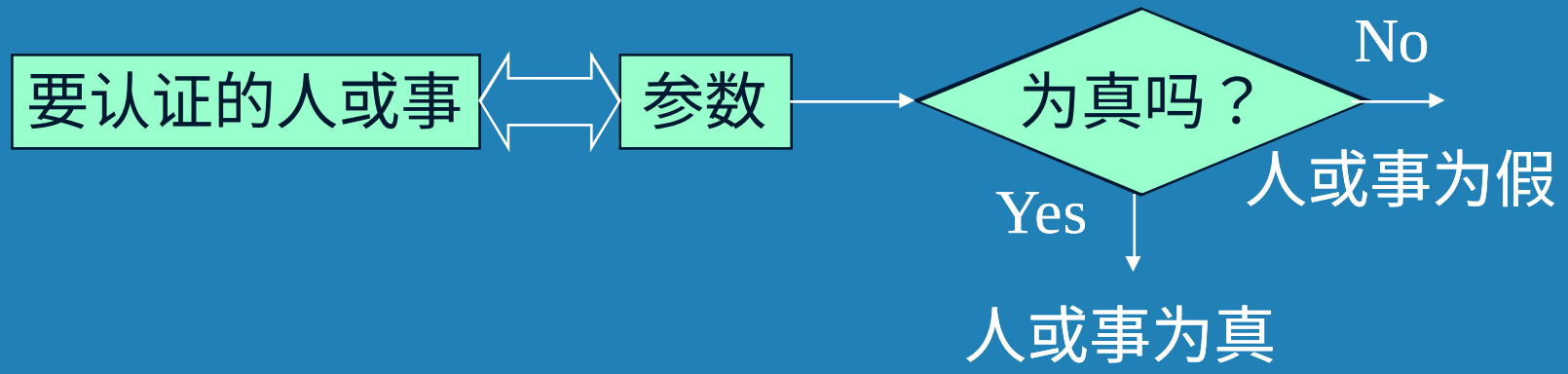
10、公开密钥密码（2）
11、数字签名（1）
12、数字签名（2）
13、HASH函数
14、*认证*
15、密钥管理
16、PKI技术
17、习题课：复习公钥密码
18、总复习/检查：*综合实验*

一、认证的概念

- *认证（Authentication）又称鉴别，确认，它是证实某人某事是否名符其实或是否有效的一个过程。*
- *认证往往是许多应用系统中安全保护的第一道设防，因而极为重要。*

一、认证的概念

- *认证模型*



一、认证的概念

- *认证参数有口令、标识符、密钥、信物、智能卡、指纹、视网纹等。*
- *一般说来，利用人的生理特征参数进行认证的安全性高，但技术要求也高，至今尚未普及。*
- *目前广泛应用的还是基于密码的认证技术。*
- *目前主要有：身份认证，站点认证，报文认证*

一、认证的概念

- *认证和加密的区别：*
- *加密用以确保数据的保密性，而认证用以确保报文发送者和接收者的真实性以及报文的完整性。*

一、认证的概念

- *认证和数字签名的区别：*

①*认证总是基于某种收发双方共享的保密数据来认证被鉴别对象的真实性，而数字签名中用于验证签名的数据是公开的。*

②*认证允许收发双方互相验证其真实性，不准许第三者验证，而数字签名允许收发双方和第三者都能验证。*

③*数字签名具有发送方不能抵赖、接收方不能伪造和能够公开验证解决纠纷，而认证则不一定具备。*

二、站点认证

- 为了确保通信安全，在正式传送报文之前，应首先认证通信是否在意定的站点之间进行，这一过程称为站点认证。
- 站点认证是通过验证加密的数据能否正确地在两个站点间进行传送来实现的。

二、站点认证

- 设A、B是意定的两个站点，A是发送方，B是接收方。利用传统密码体制，则A和B相互认证的过程如下(假定A、B共享保密的会话密钥K_S):

1. A产生随机数R_A
2. A→B：$E(R_A, K_S)$ ——→ 2. B接受$E(R_A, K_S)$
3. A接受$E(R_A||R_B, K_S)$ ←—— 3. B→A：$E(R_A||R_B, K_S)$

   并解密判断 $R_A = R_A$?
4. A→B：$E(R_B, K_S)$ ——→ 4. B接受$E(R_B, K_S)$

   5. B判断 $R_B = R_B$?

1. B产生随机数R_B

二、站点认证

- 利用公钥密码，则A和B相互认证的过程如下:

1. A产生随机数R_A
2. A→B：R_A

1. B产生随机数R_B
2. B接受R_A
3. B→A：$D(R_A||R_B, K_{dB})$

3. A接受$D(R_A||R_B, K_{dB})$ 并验证B的签名
4. A→B：$D(R_B, K_{dA})$

4. B接受$D(R_B, K_{dA})$ 并验证A的签名

- *注意：基于公钥密码的站点认证本质上是利用数字签名来确保A，B的真实性。*

三、报文认证

- 报文认证必须使通信方能够验证每份报文的发送方、接收方、内容和时间性的真实性和完整性。能够确定：

(1) *报文是由意定的发送方发出的；*

(2) *报文传送给意定的接收方；*

(3) *报文内容有无篡改或发生错误；*

(4) *报文按确定的次序接收。*

三、报文认证

1、报文源的认证

- *采用传统密码*
- *设A为发送方，B为接收方。A和B共享保密的密钥K_S。A的标识为ID_A，报文为M，在报文中增加标识ID_A,那么B认证A的过程如下：*

$$A \rightarrow B：E(ID_A \| M，K_S)$$

- ***B收到报文后用K_S解密，若解密所得的发送方标识与ID_A相同，则B认为报文是A发来的。***

三、报文认证

1、报文源的认证

- *采用公开密钥密码*

报文源的认证十分简单。只要发送方对每一报文进行数字签名，接收方验证签名即可：

$A \rightarrow B: <M, SIG(ID_A \| M, K_{dA})>$

$B: VER(SIG(ID_A \| M, K_{dA}), K_{eA})$

若收方验证签名正确，则认为发方为真。

三、报文认证

2、报文宿的认证

只要将报文源的认证方法稍加修改便可实现报文宿的认证。

- *采用传统密码*

在每份报文中加入接收方标识符ID_B：

$$A \rightarrow B：E(ID_B \| M，K_S)$$

- *若采用公开密钥密码*
- *对每份报文用B的公开加密钥进行加密即可。*

$$A \rightarrow B：E(ID_B \| M，K_{eB})$$

三、报文认证

3、报文内容的认证

- *报文内容认证使接收方能够确认报文内容的真实性，这可通过验证认证码 的正确性来实现。*
- *消息认证码MAC（Message Authentication Code）是消息内容和密钥的公开函数，其输出是固定长度的短数据块：*

$$MAC = C(M, K)。$$

三、报文认证

3、报文内容的认证

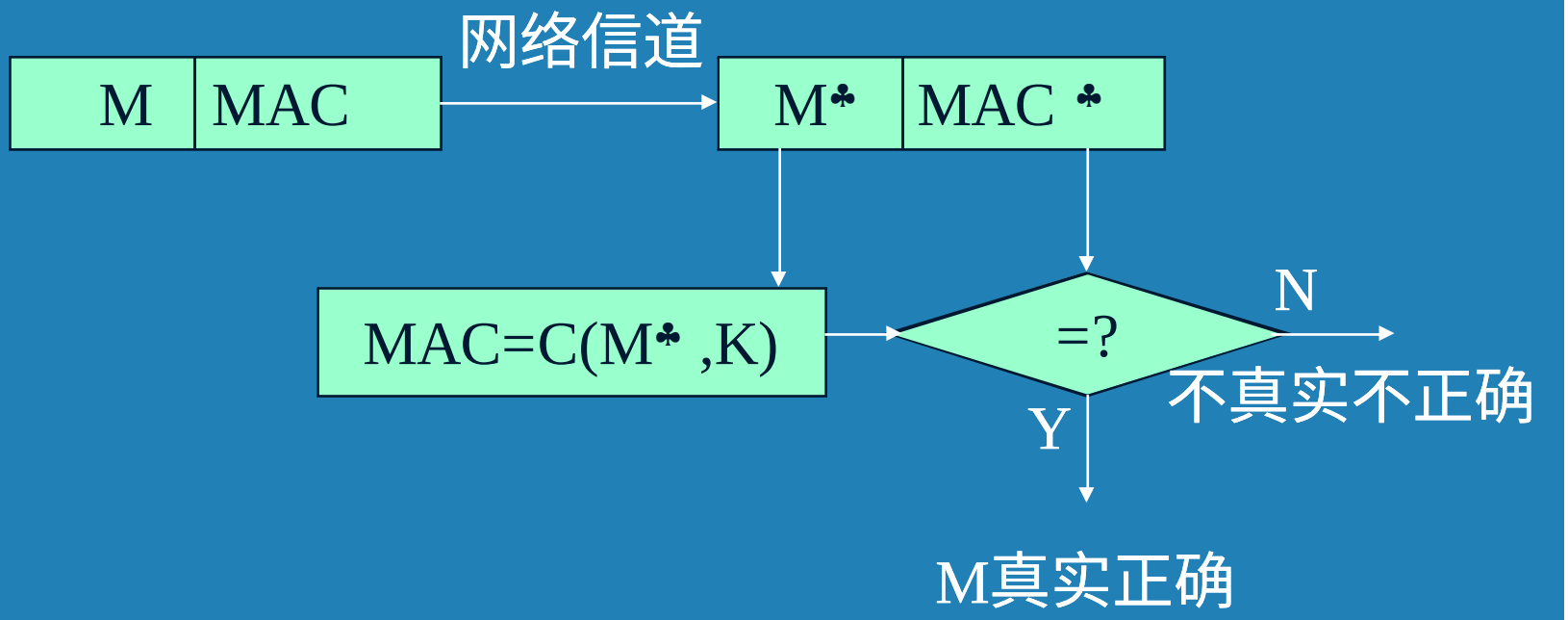
- *通信双方共享秘密钥K。A计算MAC并将报文M和MAC发送给接收方：*

$$A \rightarrow B：M \| MAC$$

- *接收方收到报文M后用相同的秘密钥K重新计算得出新的MAC，并将其与接收到的MAC进行比较，若二者相等，则认为报文正确真实。*

三、报文认证

3、报文内容的认证



三、报文认证

3、报文内容的认证

- *在上述方法中，报文是以明文形式传送的,所以该方法可以提供认证，但不能提供保密性。若要获得保密可在MAC算法之后对报文加密：*

$$A \rightarrow B：E\ (M||MAC，K_2)$$

$$其中MAC=C(M，K_1)$$

因为只有A和B共享K_1，所以可提供认证；

因为只有A和B共享K_2，所以可提供保密。

三、报文认证

3、报文内容的认证

- *注意：*

  MAC算法不要求可逆性而加密算法必须是可逆的；

  与加密相比，认证函数更不易被攻破；

  由于收发双方共享密钥，因此MAC不能提供数字签名功能。

三、报文认证

3、报文内容的认证

- *注意：理论上，对不同的M，应不同产生MAC。因为若$M_1 \neq M_2$，而$MAC_1 = MAC_2$，则攻击者可将M_1篡改为M_2，而接收方不能发现。*
- *但是要使函数C具备上述性质，将要求报文认证码MAC至少和报文M一样长，这是不方便的。*

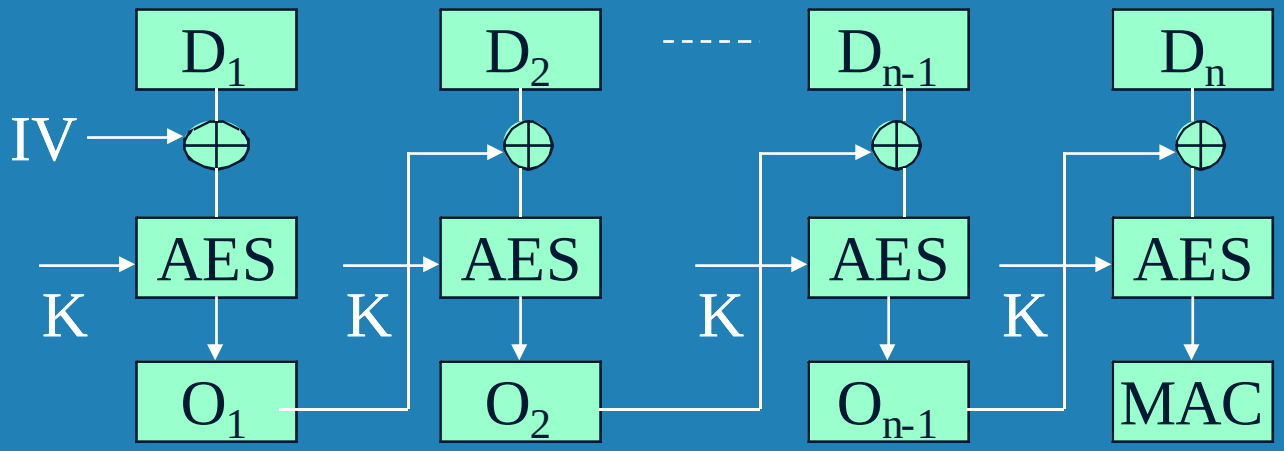
三、报文认证

实际应用时要求函数C具有以下性质：

- *对已知M_1和MAC_1构造满足$MAC_2=MAC_1$的M_2在计算上是不可行的；*
- *MAC函数应是均匀分布的，即对任何随机的报文M_1和M_2，$MAC_1=MAC_2$ 的概率是2^{-n}，其中n是MAC的位数；*
- *设M_2是M_1的某个已知的变换，即$M_2=f(M_1)$，如f改变M_1的一位或多位，那么$MAC_1=MAC_2$的概率2^{-n}。*

四、利用分组密码产生MAC

- *利用强的分组密码可以产生MAC：*
  - *需认证的数据被分成128位的分组 $D_1||D_2||\cdots||D_N$，若最后分组不足128位，则在其后填0直至成为128位的分组。*
  - *用AES按CBC方式加密，产生MAC。*



四、利用分组密码产生MAC

- 其中，$O_1 = AES(D_1 \oplus IV , K)$

  $O_i = AES(D_i \oplus O_{i-1} , K)$　　$(2 \le i \le N)$

  $MAC=O_n$

  IV为初始向量，此处取0；K为密钥。

- *很容易用其它强的分组密码来计算产生MAC。*

五、利用HASH函数产生MAC

1、*HASH函数的应用*

- *Hash函数将任意长的报文M变换为定长的码，记为：h=HASH(M)或 h=H(M)。*
- *Hash码也称报文摘要。*
- *它具有错误检测能力。*
- *用Hash码作MAC，可认证报文；*
- *用Hash码辅助数字签名；*
- *Hash函数可用于保密。*

五、利用HASH函数产生MAC

2、*安全Hash函数的应用：*

- 报文认证

  A→B：< M || E（Hash（M），K）>

- *发方生成报文M的Hash码Hash(M)并使用传统密码对其加密，将加密后的结果附于消M之后发送给接收方。*
- *B由M重新计算Hash（M），并与接受到的比较。由于Hash(M)受密码保护，所以B通过比较Hash(M)可认证报文的真实性和完整性。*

五、利用HASH函数产生MAC

2、*安全Hash函数的应用：*

- 保密与认证

A→B：< E （M || Hash （M） ,K） >

- *由于只有A和B共享秘密钥，所以B通过比较Hash(M)可认证报文源和报文的真实性。由于该方法是对整个报文M和Hash码加密，所以也提供了保密性。*

五、利用HASH函数产生MAC

2、*安全Hash函数的应用：*

- 数字签名与认证

  $A \rightarrow B: < M \| D(H(M), K_{dA}) >$

- *发方使用公钥密码用其私钥K_{dA}对消息M的hash码签名，并将其附于报文M之后发送给收方。B可以验证Hash值来认证报文的真实性，因此该方法可提供认证；由于只有发方可以进行签名，所以该方法也提供了数字签名。*

习题

① 设计一个综合报文认证方案，包括报文源、报文宿、报文顺序、报文内容的认证。

② 论述安全HASH函数在认证中的作用。


谢 谢！