密 码 学

第十四讲　认证

张焕国

武汉大学计算机学院

空天信息安全与可信计算教育部重点实验室

内容简介

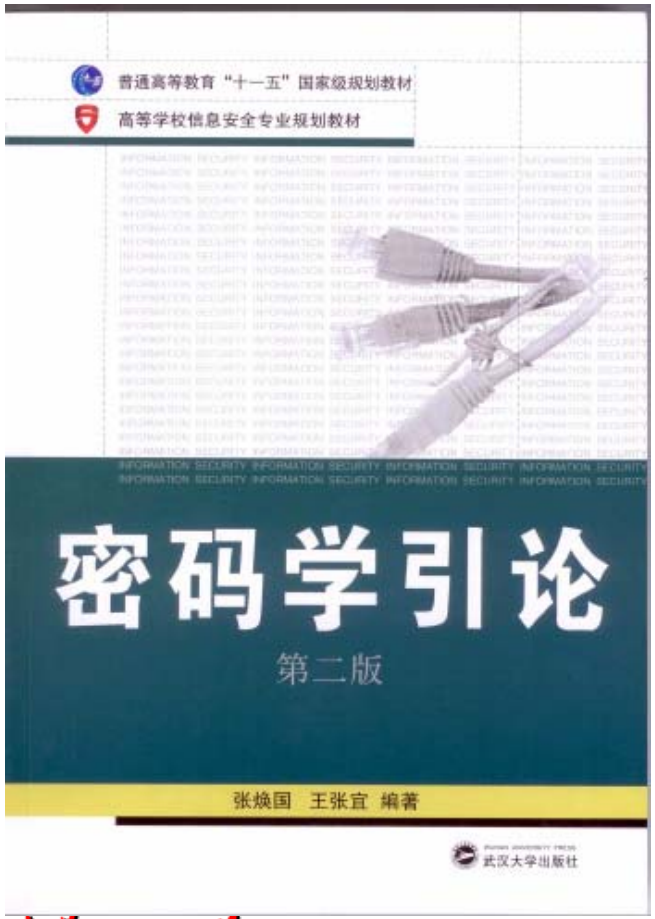
第一讲 信息安全概论
第二讲 密码学的基本概念
第三讲 数据加密标准（DES）
第四讲 高级数据加密标准（AES）
第五讲 中国商用密码（SMS4）
第六讲 分组密码的应用技术
第七讲 序列密码
第八讲 复习
第九讲 公钥密码（1）

内容简介

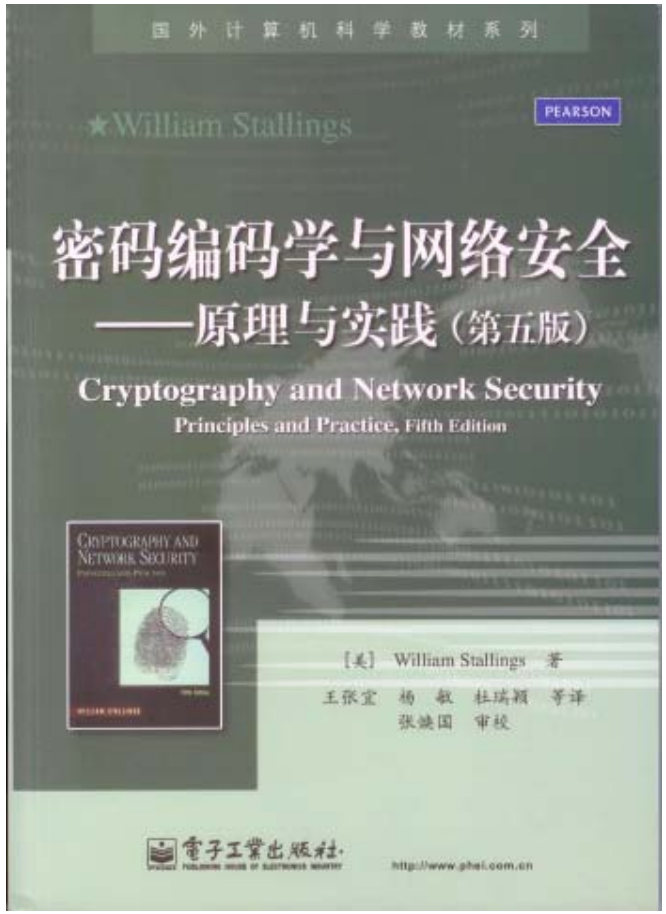
第十讲 公钥密码（2）
第十一讲 数字签名（1）
第十二讲 数字签名（2）
第十三讲 HASH函数
第十四讲 认证
第十五讲 密码协议
第十六讲 密钥管理（1）
第十七讲 密钥管理（2）
第十八讲 复习

教材与主要参考书

教材

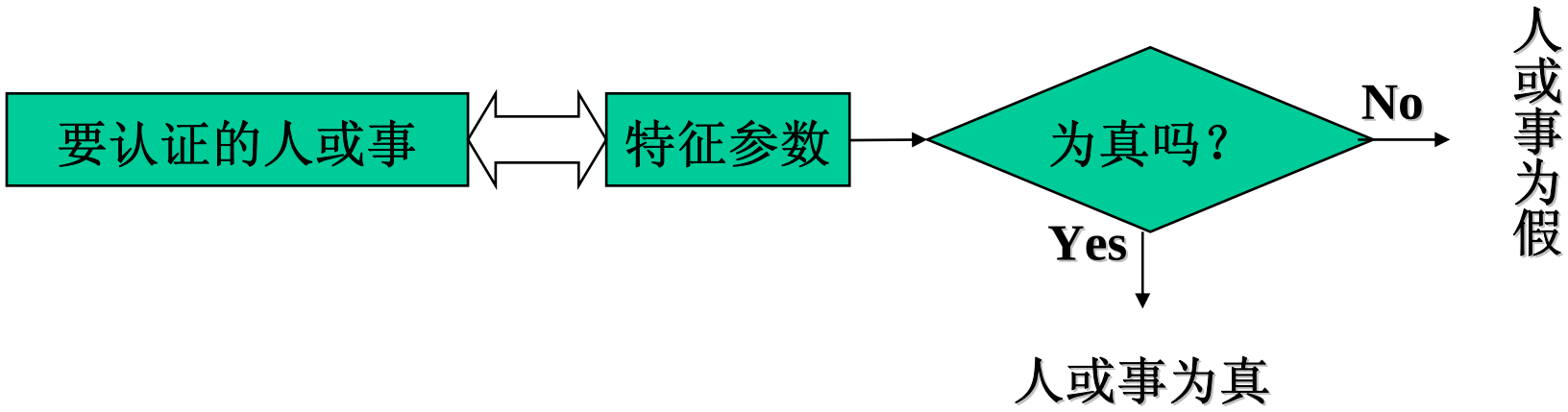


参考书



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。
- 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、USB-Key 、指纹、视网膜纹（巩膜和虹膜）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。指纹识别和人脸识别应用逐渐推广。
- 目前广泛应用的还是基于密码的认证技术。

- 认证和加密的区别：
  - 加密用以确保数据的保密性
  - 认证用以确保当事人身份的真实性以及数据的完整性

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的能力，而认证则不一定具备。

二、身份认证

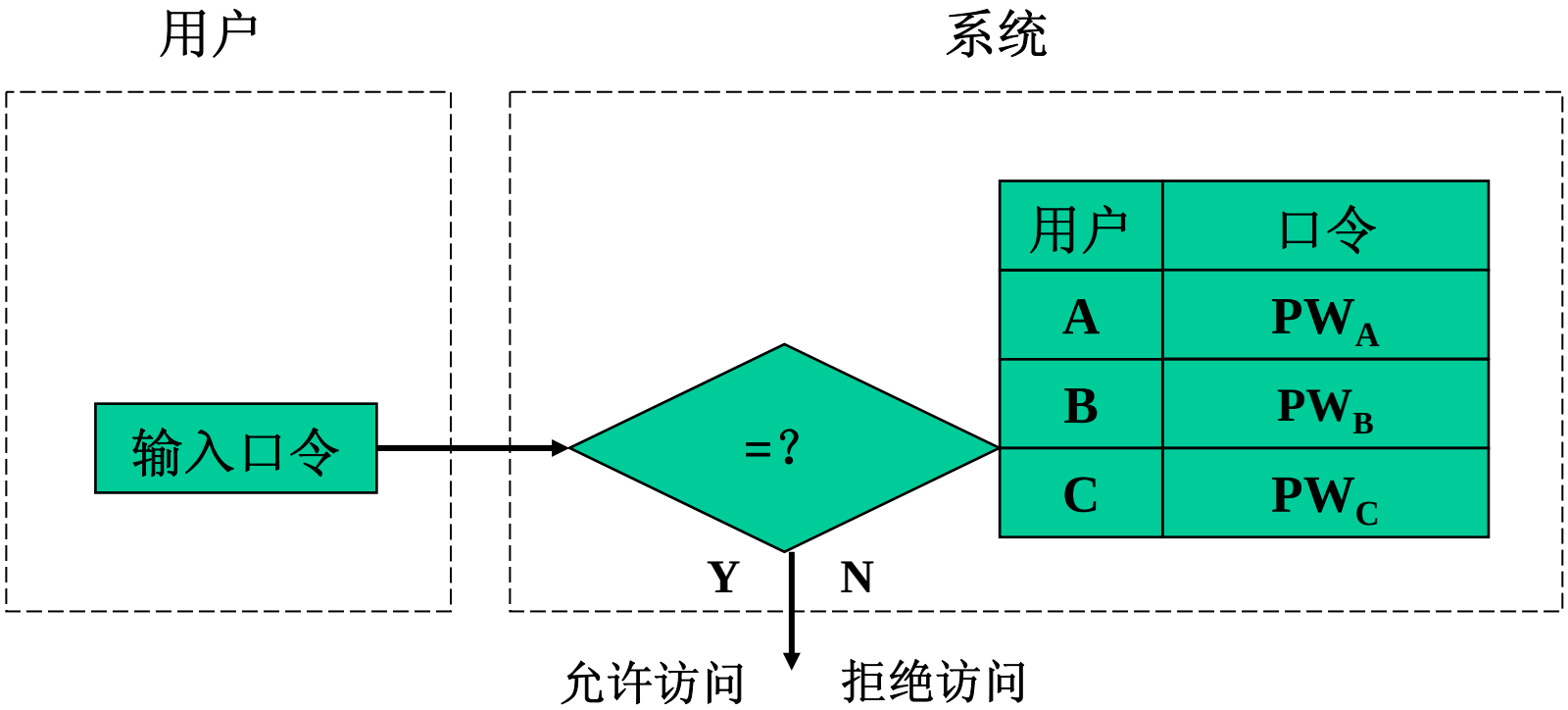
- 用户的身份认证是许多应用系统的第一道防线，其目的在于识别用户的合法性，从而阻止非法用户访问系统。
- 可见，身份认证对确保系统的信息安全是极其重要的。
- 一般，可以通过以下验证，来认证用户的身份：
  - 用户知道什么
  - 用户拥有什么
  - 用户的生理特征

二、身份认证

1. 口令

- 口令是双方预先约定的秘密数据，口令认证属于验证用户知道什么。
- 口令验证的安全性虽然不如其他几种方法，但是口令验证简单易行，因此口令验证仍是目前应用最为广泛的身份认证方法。
- 在一些简单的系统中，用户的口令以口令表的形式存储。当用户要访问系统时，系统要求用户提供口令，系统将用户提供的口令与口令表中存储的口令进行比较，若相等则确认用户身份有效，否则确认用户身份无效，拒绝访问。

二、身份认证



二、身份认证

1. 口令

- 这样的简单口令系统存在以下问题：

① 因为用户的口令以明文形式存储在系统中，系统管理员可以获得所有口令，攻击者也可利用系统的漏洞来获得他人的口令。

② 因为用户的口令在用户终端到系统的线路上以明文形式传输，所以攻击者可在传输线路上截获用户口令。

③ 只有系统验证用户的身份，用户不能验证系统的身份。

二、身份认证

1. 口令

- 用单向函数加密口令：

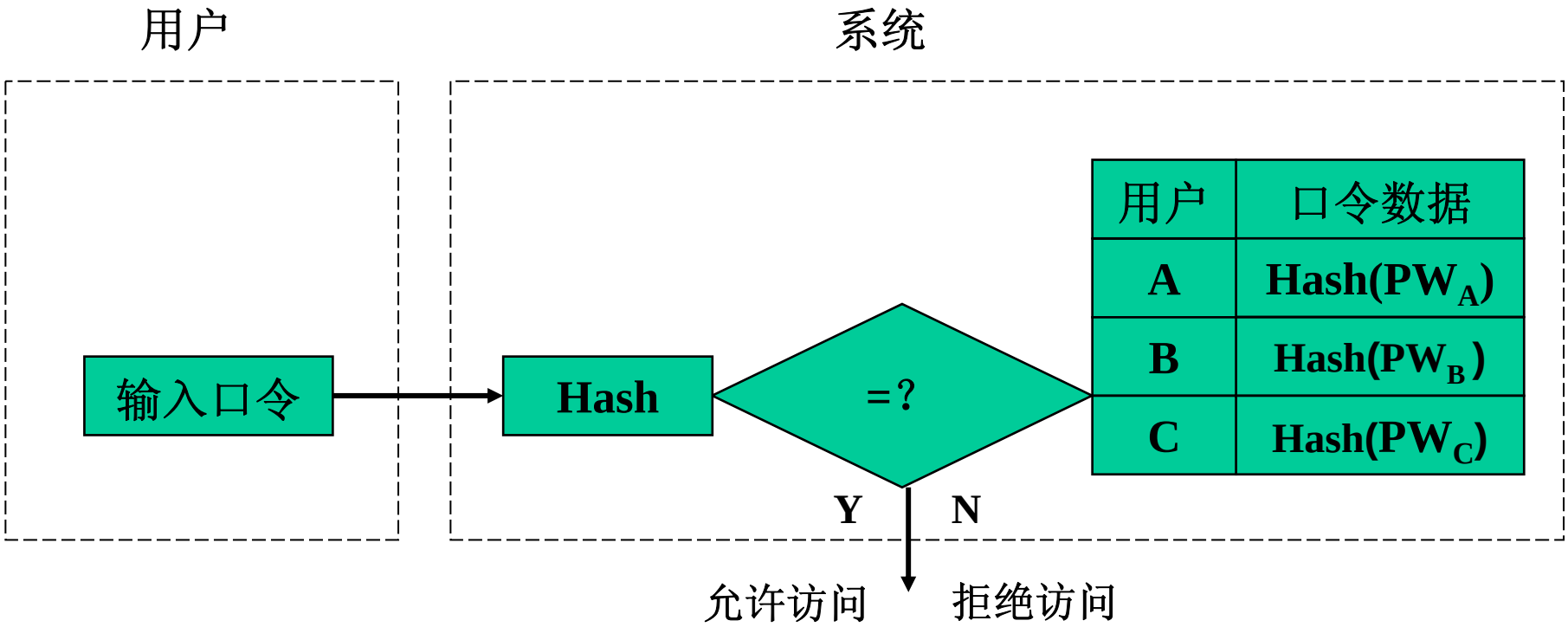
① 用户的口令在系统中以密文的形式存储。

② 口令一旦加密，将不可解密。

③ 用户访问系统时提供其口令，系统对该口令用单向函数加密，并与存储的密文相比较。若相等，则确认用户身份有效，否则确认用户身份无效。

④ 可选用强的**HASH**函数作为单向函数。

二、身份认证


用户
系统
输入口令
Hash
=?
用户
口令数据
A
Hash(PW_A)
B
Hash(PW_B)
C
Hash(PW_C)
Y
N
允许访问
拒绝访问

二、身份认证

1. 口令

- 利用数字签名方法验证口令：

① 用户*i*将其公钥提交给系统，作为验证口令的数据，系统为每个用户建立一个已访问次数标志T_i

② 用户访问系统时将其签名信息提供给系统，

$$ID_i \| D((ID_i, N_i), K_{di}),$$

其中N_i表示本次访问是第N_i次访问。

③ 系统根据明文形式的标识符ID_i查出K_{ei}，并计算

$$E(D((ID_i, N_i), K_{di}), K_{ei}) = < ID_i^*, N_i^* >$$

二、身份认证

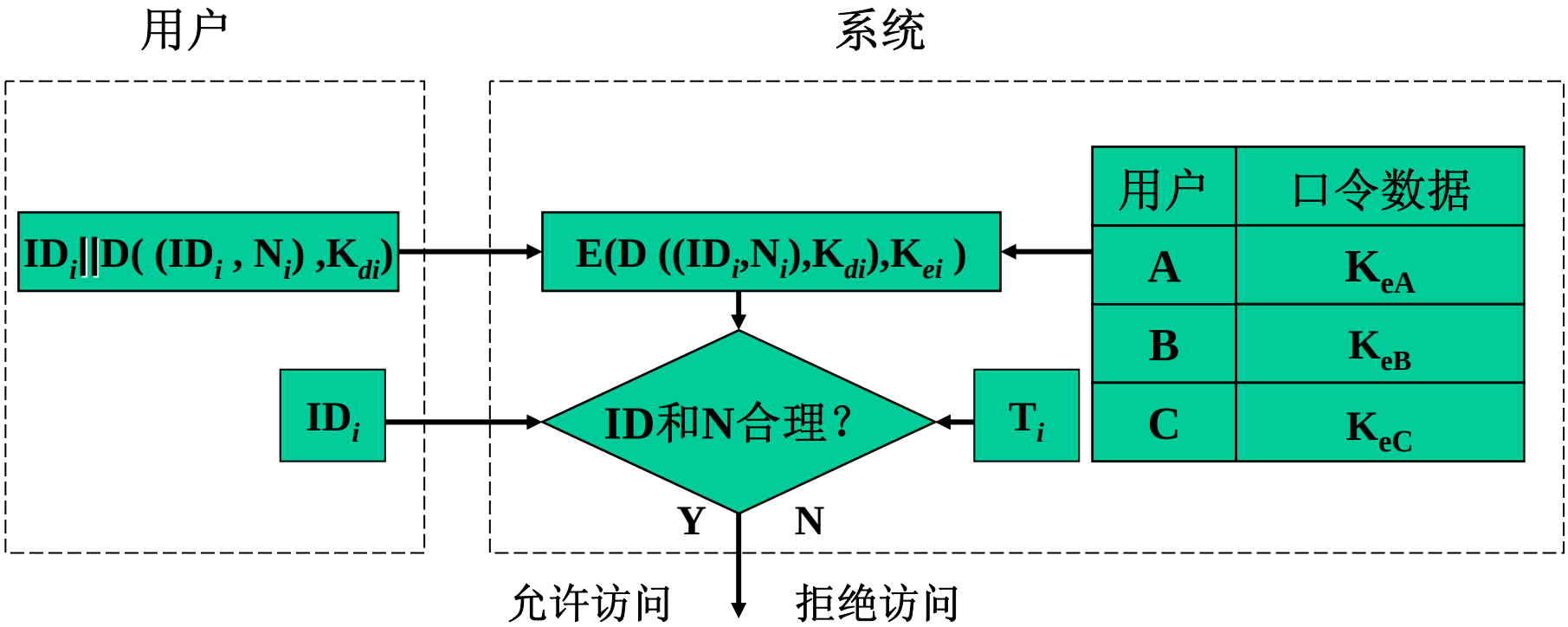
1. 口令

- 利用数字签名方法验证口令：

④ 当且仅当$ID_i = ID_i^*, N_i^* = T_i + 1$时系统才确认用户身份有效。

⑤ 安全性分析：口令是用户的保密的解密密钥K_{di}，它不存储于系统中，所以任何人都不可能得到；虽然K_{ei}存储于系统中，但是由K_{ei}不能推出K_{di}；由于从终端到系统的通道上传输的是签名数据而不是K_{di}本身，所以攻击者也不能通过截取获得K_{di}；由于系统为每用户设置了已访问次数标志T_i，且仅当$N_i^* = T_i + 1$是才接收访问，所以可以抗重播攻击。但必须对T_i实施保护。

二、身份认证


用户
系统
$ID_i \| D((ID_i, N_i), K_{di})$
$E(D((ID_i, N_i), K_{di}), K_{ei})$
用户
口令数据
A
K_{eA}
B
K_{eB}
C
K_{eC}
ID_i
ID和N合理？
T_i
Y
N
允许访问
拒绝访问

二、身份认证

1. 口令

- 口令的双向验证：
  - 仅有系统验证用户的身份，而用户不能验证系统的身份，是不全面的，也是不平等的。
  - 设A的口令为P_A，B的令为P_B。当A要求与B通信时，B必须验证A的身份，因此A应当首先向B出示表示自己身份的数据。但此时A尚未对B的身份进行验证，所以A不能直接将自己的口令发给B。如果B要求与A通信也存在同样的问题。

二、身份认证

1. 口令

- 口令的双向验证：
  - 设f是单向函数，R_A是A的随机数，R_B是B的随机数。P_A是A的口令，P_B是B的口令，A和B共享口令。

① A→B：R_A

② B→A：$f(P_B \| R_A) \| R_B$

  - A利用单向函数f对自己的R_A和共享的P_B进行加密，并与接收到的$f(P_B \| R_A)$进行比较。若两者相等，则A确认B的身份是真实的。

③ A→B：$f(P_A \| R_B)$

  - B利用单向函数f对自己的R_B和共享的P_A进行加密，并与接收到的$f(P_A \| R_B)$进行比较。若两者相等，则B确认A的身份是真实的。
  - 由于f是单向函数，即使知道$f(P_A \| R_A)$和R_A也不能计算出P_A，即使知道$f(P_B \| R_B)$和R_B也不能计算出P_B，所以在上述口令验证中，即使有一方是假冒者，他也不能骗得对方的口令。为了阻止重播攻击，可在$f(P_B \| R_A)$和$f(P_A \| R_B)$中加入时间性参量。

二、身份认证

1. 口令

- 一次性口令：
  - 为了安全，口令应当经常更换，最好是一个口令只使用一次，即一次性口令。利用单向函数可实现一次性口令。
  - 设A和B要进行通信，A选择随机数x，并计算$y_0=f^n(x)$
  - A将y_0发送给B作为验证口令的数据。因为f是单向函数，所以对y_0不需保密。
  - A以

$$y_i=f^{n-i}(x) \quad (1 \leqslant i \leqslant n-1)$$

作为其第i次通信的口令发送给B。

  - B计算并验证：$f(y_i)=y_{i-1}$吗？若相等，则确认A的身份是真实的，否则可知A的身份是不真实的，

二、身份认证

2. 磁卡、智能卡和USB-Key

- 磁卡：
  - 磁卡是目前已广泛应用的一种个人身份持证物，在银行界得到广泛地应用。磁卡使用方便、成本低。但磁卡仅有有限的数据存储能力，无数据处理能力，安全性低。

二、身份认证

2. 磁卡、智能卡和USB-Key

- 智能卡：
  - 智能卡是一种镶嵌有单片机芯片的集成电路卡。卡上有CPU、RAM、EEPROM或FLASH、ROM和I/O接口。因此智能卡被誉为最小的个人计算机。芯片操作系统COS（Chip Operating System）管理资源。安全性高。

二、身份认证

2. 磁卡、智能卡和USB-Key

- **USB-Key：**
  - **USB-Key是一种具有USB 接口，具有加解密、数字签名等多种安全保密功能的便携式安全设备。从技术上看，USB-Key就是一个具有USB接口智能卡。**

二、身份认证

2. 磁卡、智能卡和USB-Key

- 如果仅仅只靠磁卡、智能卡和USB-key这种物理持物来作为用户的身份凭证进行身份认证，尚有不足。因为它们会丢失，则捡到的人就可假冒真正的用户。为此，还需要一种磁卡、智能卡和USB-key上不具有的身份信息。这种身份信息通常采用个人识别号PIN(Personal Identification Number)。

二、身份认证

3. 生理特征识别

- 人的指纹、掌纹、面孔、发音、视网膜、DNA等都具有唯一性和稳定性的特征，即每个人的这些特征都与别人不同且终生不变，因此可以据此进行身份识别。基于这些特征，人们发展了指纹识别、视网膜识别、语音识别、人脸识别等多种生物识别技术，其中指纹识别和人脸识别技术比较成熟，得到广泛应用。

三、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。

三、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接收$E(R_A, K_S)$
3. A接收$E(R_A \| R_B, K_S)$ ⟵ 3. B→A：$E(R_A \| R_B, K_S)$

   并解密判断 $R_A = R_A$?

   若相等则A认为B是合法站点。

4. A→B：$E(R_B, K_S)$

1. B产生随机数R_B
4. B接收$E(R_B, K_S)$
5. B判断 $R_B = R_B$?

   若相等则B认为A是合法站点。

- 安全性：上述协议成功，则表明A拥有K_S且B也拥有K_S，K_S是保密的，因此A、B是合法的

三、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 ⟶ 2. B接收R_A

3. B→A：$D(R_A \| R_B，K_{dB})$

3. A接收$D(R_A \| R_B，K_{dB})$
并验证B的签名，如正确则A认为B是合法站点。

4. A→B：$D(R_B，K_{dA})$ ⟶ 4. B接收$D(R_B，K_{dA})$
并验证A的签名，如正确则B认为A是合法站点。

- 安全性：上述认证本质上是验证数字签名，数字签名具有确保真实性的能力。

四、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。

四、报文认证

1、报文源的认证

① 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：

$$A \rightarrow B: < ID_A , E(ID_A||M , K_S) >$$

- 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。

四、报文认证

1、报文源的认证

② 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→B：$< ID_A, D(ID_A||M，K_{dA}) >$
  - B：E（ $D(ID_A||M ,K_{dA})$，K_{eA} ），并验证加密所得ID_A是否等于ID_A？若收方验证签名正确，则认为发方为真。
  - 注意：此方案不能保密，因为K_{eA}是公开的，任何人都可以得到，并加密得到M。

四、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。

① 采用传统密码

- 在每份报文中加入接收方标识符ID_B，并加密：

$$A \rightarrow B: < ID_B, E(ID_B \| M, K_S) >$$

② 若采用公开密钥密码

- 对每份报文加入接收方标识符ID_B，并用B的公开加密钥进行加密：

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

- 注意：此方案不能保真，因为K_{eB}是公开的，任何人都可以冒充A，发送$E(ID_B \| M, K_{eB})$。

四、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和完整性，这可以通过验证消息认证码 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：

$$MAC=C(M，K)$$

四、报文认证

3、报文内容的认证

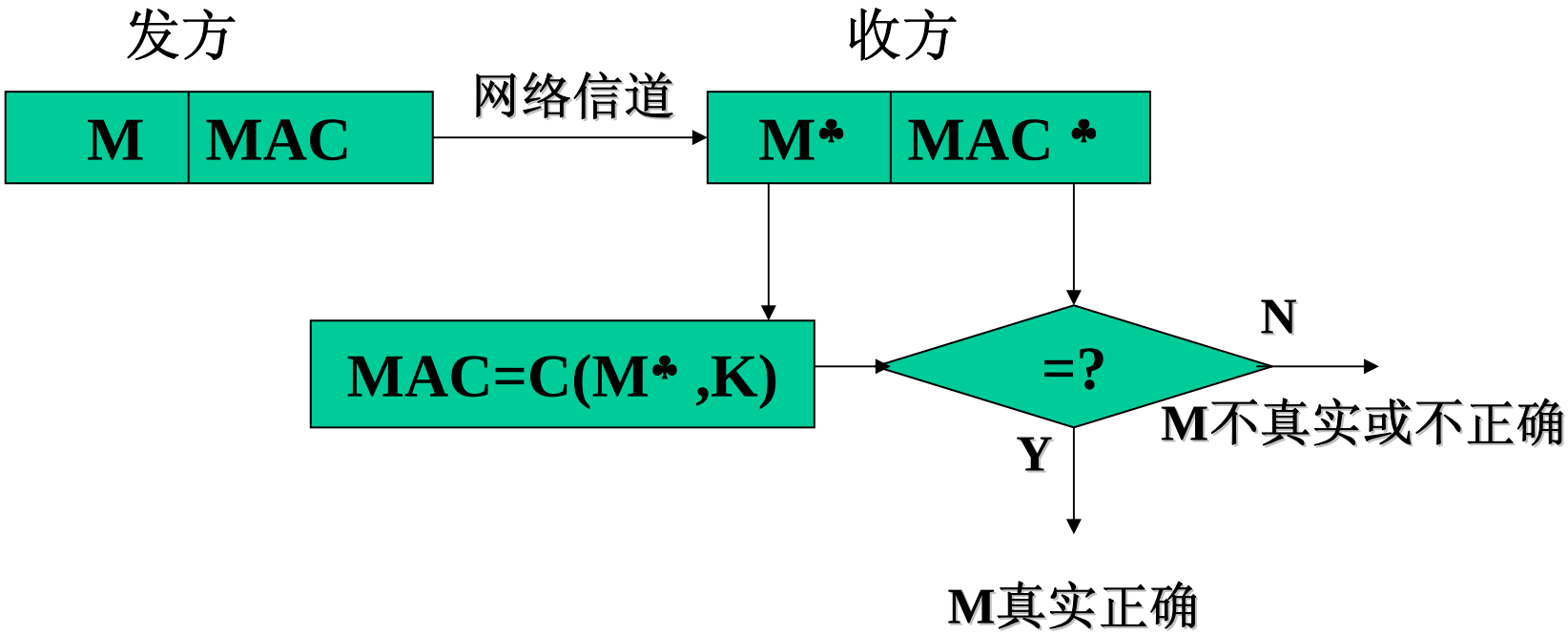
- 通信双方共享秘密钥K，A计算MAC并将报文M和MAC发送给接收方：

$$A \rightarrow B: < M \| MAC >$$

- 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，则认为报文是真实的完整的。

四、报文认证

3、报文内容的认证



四、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：

$$A \rightarrow B: E(M||MAC, K_2)$$

$$其中\ MAC=C(M, K_1)$$

- 安全性分析
  - 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。

四、报文认证

3、报文内容的认证

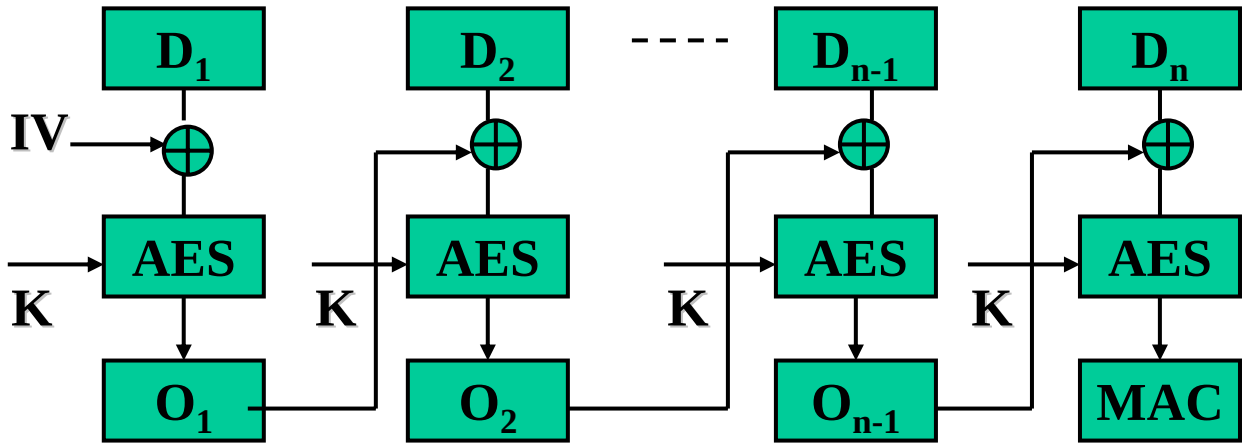
- 注意：
  - MAC算法不要求可逆，而加密算法必须可逆；
  - 由于采用传统密码，收发双方共享密钥，因此MAC不能提供数字签名功能。
  - 理论上，对不同的M，应产生不同的MAC。否则，若$M_1 \neq M_2$，而$MAC_1 = MAC_2$，则攻击者可将M_1篡改为M_2，而接收方不能发现。
  - 但是要使函数C具备上述性质，将要求报文认证码MAC至少和报文M一样长，这是不方便的。

四、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}。

五、利用分组密码产生MAC

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



五、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，可以取为0；K为密钥。

● 很容易用其它强的分组密码（如SMS4）来计算产生MAC。

六、利用HASH函数产生MAC

- 将HASH码用作MAC
  - 简单Hash MAC
  - 带密钥的HMAC
- 基于简单Hash MAC的报文认证

  设A，B共享密钥K：

  $$A \rightarrow B: < M \| E(Hash(M), K) >$$

- 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由收到的M重新计算Hash（M），再加密，并与接受到的比较，若相同则认为报文是真的。
- Hash(M)受密码保护，没有密钥的人篡改M将被发现。
- 注意：此方案没有保密功能。

武漢大學

六、利用HASH函数产生MAC

② 保密认证

设A，B共享密钥K：

$A \rightarrow B: < ID_A , E(ID_A \| M \| Hash(M), K) >$

- 由于只有A和B共享秘密钥，所以B可以解密，如果B验证ID_A正确，便认证了报文源。
- B根据M计算新的Hash(M)，并与接收到的Hash(M)比较，如果相等，则可认证报文M的真实性和完整性。
- 由于该方法是对整个报文M和Hash(M)加密，所以也提供了保密性。

六、利用HASH函数产生MAC

③ 数字签名与认证

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

- B根据ID_A用A的公钥K_{eA}验证签名，得到Hash(M)。对收到的M重新计算HASH(M)码，并与接收到的比较。如果两者相等，则可断定M是真实的完整的。
- 由于发方A进行了签名，所以该方法也提供了数字签名。A不能抵赖，其他人不能伪造，还可以解决纠纷。
- 注意：此方案没有保密功能，因为M没有加密。

武漢大学

六、利用HASH函数产生MAC

③ 数字签名与认证

- 改进方案

$$A \rightarrow B: < E(ID_A||M||D(Hash(M),K_{dA}), K_{eB})>$$

- 由于有A的签名，所以可以确保M的真实性和完整性。
- 由于有B的加密，所以确保了M的秘密性。

作 业 题

1、p236第9题。

- 所谓完整方案，是指具有报文源、报文宿、报文内容和报文时间的认证。

谢　谢！