浙江大学电气工程学院
College of Electrical Engineering Zhejiang University

网络安全导论

加密、认证

1. 概述、基础知识
2. **加密与认证技术**
3. 软件与通讯安全
4. 电力工控系统安全
5. 物联网终端安全
6. 智能无人系统安全

一个通讯游戏

假定两人赌博决定胜负，最常用的办法是抛硬币.

通常规则是：一人选定一面，另一人抛硬币. 不妨假定乙选定一面，甲抛硬币. 如果乙选定的一面出现，则乙胜出，否则甲胜出.

请注意：上述游戏必须两人面对面进行.

规 定：两人以上进行的游戏规则，通常我们称为协议. 一人可以执行的规则，只能称为程序.

来源：www.icourse163.org，厦门大学慕课《信息安全》

一个通讯游戏

我们的问题是：如果两人不是面对面，通过电话或者其它通讯手段，如何执行上述协议？

因为上述协议能够进行的前提是：两人面对面进行．如果甲在电话上说:你选一面，我来抛并告诉你是否赢了．乙会同意吗？

为了在通讯中(电话中）完成这个游戏， 需要修改上述协议．密码学家想出一个办法，在协议中增加密码技术．这个密码技术依赖下述奇妙的数学函数：

来源：www.icourse163.org，厦门大学慕课《信息安全》

一个通讯游戏

定义 1.1

一个函数 $f(x)$称为单向函数，如果满足以下两条性质：

1. 对任意整数 x，由 x 计算 $f(x)$ 是容易的. 而给出 $f(x)$，要找出对应的原像 x是不可能的，不管 x 是奇数还是偶数.
2. 不可能找出一对整数：

$$x \neq y, f(x) = f(y)$$

注意：这里的词“容易”和“不可能”需要严格的数学表述，即给出某种量化的表达方式. 以后我们会说明这一点，因为它们反映了安全性. 这种函数的存在性问题也需要进一步讨论.

来源：www.icourse163.org，厦门大学慕课《信息安全》

一个通讯游戏

现在假定这样一个单向的函数 $f(x)$ 已经找到，双方同意以偶数代表正面，奇数代表反面．我们可以制定一个电话抛币的协议：

协议 1.2

电话掷币．假定：双方同意

1. 具有定义*1.1* 的单向函数 $f(x)$；
2. 偶数 x 代表正面，奇数 x代表反面；

然后执行

1. 甲选择一个大随机数 x,计算 $f(x)$，然后通过电话告诉乙 $f(x)$的值；
2. 乙告诉甲，对 x 的奇偶性的猜测；
3. 甲告诉乙 x 的值；
4. 乙验证 $f(x)$，从而看出他所作出的猜测是正确或错误的．

主观题 1分

设置

请同学们分析下上述协议的合理性，即协议的安全性。

作答

一个通讯游戏

- 首先，有函数f(x)的性质，甲找不到两个数（一奇一偶）使其函数值相等，也就是一旦电话告诉了乙f(x)的值，就选定了x的值且无法改变；**（第一步掷硬币）**
- 第二，乙获得f(x)，无法判断甲使用的x奇偶性，不得不做出真实猜测；**（第二步）**
- 第三，甲告诉乙真实的x，乙再计算f(x)，确认自己的猜测是否正确；**（第三、四步）**

来源：www.icourse163.org，厦门大学慕课《信息安全》

一个通讯游戏

上述游戏能够进行，关键有两点：

- 对甲而言：无法（从计算上看非常困难）找到两个奇偶性不同的数：

$$x \neq y, f(x) = f(y)$$

因此乙愿意执行这个协议;

- 对乙而言：依据 $f(x)$ 的值，他没有可以利用的资源猜测或非常难于计算 x的值，或他猜测奇数或偶数的概 率都是 $\frac{1}{2}$，所以甲愿意执行这个协议。

因此我们说，依据上述协议，游戏对双方是公平的.

来源：www.icourse163.org，厦门大学慕课《信息安全》

一个通讯游戏

- 计算的困难性保证了双方在游戏中的安全；数学上的**计算困难性**是安全得到保障的基础；
- 一个数学问题不能在合理时间解决，就称为困难问题；
- 增加密码技术的协议，为安全密码协议；协议1.2的存在性依赖**单向函数**的存在性；
- 保证通信安全**不能仅靠数学特性**，例如，电话掷币时，还要有电话录音、身份鉴别、第三方公证等。有的依赖数学方法，有的依赖物理设备。

来源：www.icourse163.org，厦门大学慕课《信息安全》

主观题 1分

设置

请列举具有单向函数性质的函数。

作答

网络安全体系结构

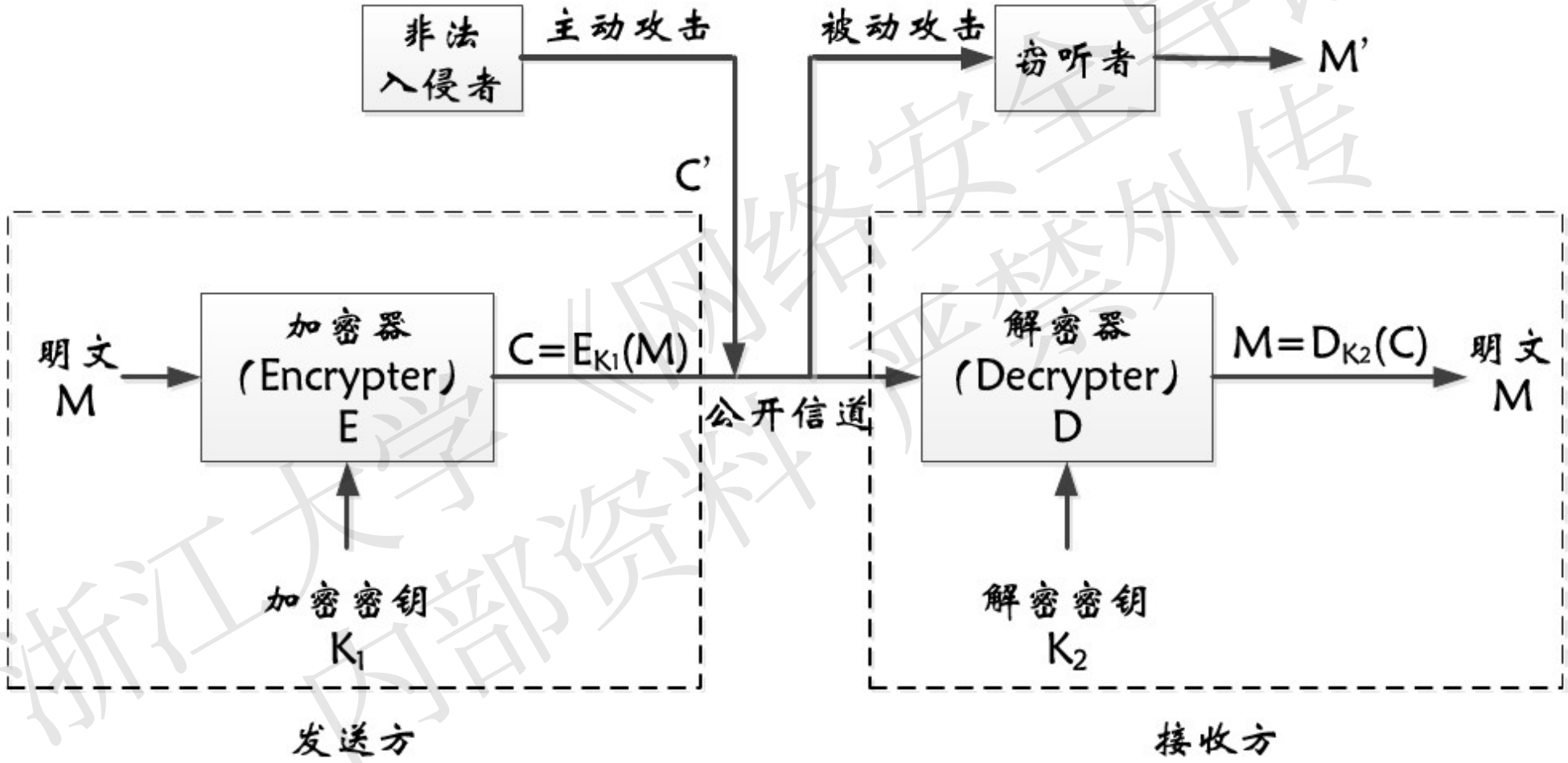
❖ISO/OSI安全结构：安全服务与安全机制的关系

安全服务	安全机制							
	加密	数字签名	访问控制	数据完整性	身份鉴别	业务流填充	路由控制	公证
认证服务	Y	Y	-	-	Y	-	-	-
访问控制服务	-	-	Y	-	-	-	-	-
机密性服务	Y	-	-	-	-	Y	Y	-
完整性服务	Y	Y	-	Y	-	-	-	-
抗否认服务	-	Y	-	Y	-	-	-	Y

2.1

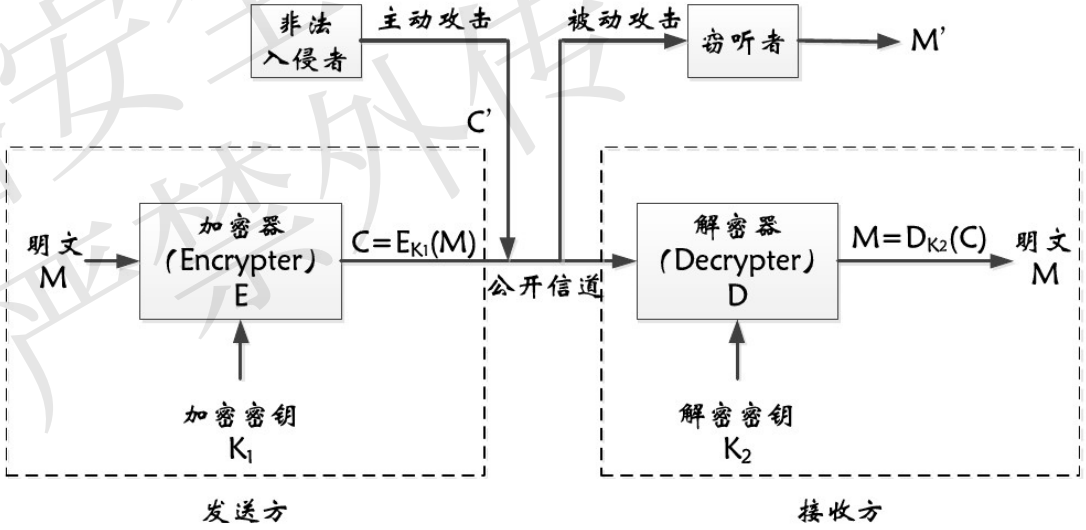
对称密码与非对称密码

密码通讯模型



密码学基本概念

- 明文m：需要秘密传送的信息
- 密文c：明文经过密码变换后的消息
- 加密 E_k1(m)：由明文到密文的变换
- 解密 D_k2(c)：从密文恢复出明文的过程
- 破译：非法接收者试图从密文分析出明文的过程
- 密钥：加密和解密时使用的一组秘密信息, k1和k2
- 加密/解密算法：对明/密文进行加/解密时的规则



传统加密方法

❖移位加密

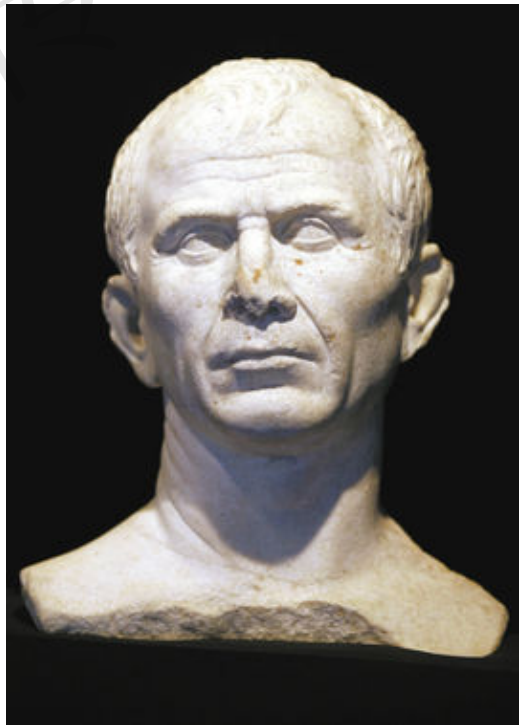
1.由于英文字符有26个字母，可以建立英文字母和模26的剩余之间的对应关系：

A = 0　B = 1　C = 2　…　Y = 24 Z = 25

2.加密过程：　$y = x + k \pmod{26}$

3.解密过程：　$x = y - k \pmod{26}$

4.例如可以用k=3、k=5进行加密，k=3同时是加密钥和解密钥



凯撒大帝是如何指挥军队的?

传统加密方法

❖移位加密

明文字母	ABCDEFGHIJKLMNOPQRSTUVWXYZ
密文字母	DEFGHIJKLMNOPQRSTUVWXYZABC

- 设明文为：LOVE
- 则密文为：ORYH

❖置换加密

- 一个有限集合上的一一置换；
- 移位就是一种置换，有规律的置换；

例如设

$$f=\begin{pmatrix} a & b & c & \cdots & y & z \\ z & y & x & \cdots & b & a \end{pmatrix}=(az)(by)\cdots(mn)$$

大家对明文 we will meet 加密，得到什么密文？

密文为：dvdroonvvg. 如何解密，即 $f^{-1}=?$

传统加密方法

❖仿射加密

- 加密：给定密钥k=(α,β)　　$y = \alpha x + \beta \pmod{26}$
- 解密：　　$x = \frac{1}{\alpha}(y - \beta) \pmod{26}$

1/a不是a的倒数，而是**逆元**

- 逆元的简单定义：a的逆元是满足ab=1(mod26)的b的值

例如，a=7,n=26 则我们寻找a的逆元：

7*1 = 7 mod 26　　7*4 = 28 = 2 mod 26

7*2 = 14 mod 26　　7*5 = 9 mod 26

7*3 = 21 mod 26　　7*6 = 16 mod 26　…

得出7*15=1mod26

Example 3

取 $k = (7, 3) \in \mathbb{Z}_{26}^* \times \mathbb{Z}_{26}$. 加密运算为: $e_k(x) = 7x + 3$. 解密运算为: $d_k(y) = 15(y - 3)$.

传统加密方法

❖仿射加密

- 根据数论中的知识，如果α的逆元存在，则α的模数与26必互质，因此α的取值范围为

{1，3，5，7，9，11，15，17，19，21，23，25}

只有12个值，所以对于仿射加密，所有可能的加密方式只有12*26=312种

仿射加密安全吗?

例.Pu yfo of oin hvy ufa hrpkpyb, jlar ph hopkk py oin hvy oinan, svo jnjpkk klvbi rfan zfyupgnyo zlkr; pu ovayng of ufvyg iph fjy hilgfj, lmmafmaplon nhzlmn, oin hvy jpkk sn oiafvbi oin inlao,jlar nlzi mklzn snipyg oin zfayna; pu ly fvohoanozing mlkr zlyyfo ulkk svoonaukx, oiny zknyzing jlcpyb larh, bpcny mfjna; pu P zly'o ilcn sapbio hrpkn, po jpkk ulzn of oin hvyhipyn, lyg hvyhipyn hrpkn ofbnoina, py uvkk skffr.

传统加密方法

❖仿射加密

- 仿射加密是**线性映射**，所以明文和对应密文出现的**频率是一致**的。

1.统计密文中字母的频率

{'a': 18, 'c': 3, 'b': 7, 'g': 8, 'f': 19, 'i': 23, 'h': 17,
'k': 22, 'j': 10, 'm': 7, 'l': 21, 'o': 30, 'n': 37, 'p': 26,
's': 6, 'r': 10, 'u': 11, 'v': 13, 'y': 27, 'x': 1, 'z': 12}

2.与标准字母频率比较，找到两个明文密文映射

分类	使用频率分类字母集	每个字母约占百分数
I	极高使用频率字母集:e	12%
II	次高使用频率字母集:t,a,o,i,n,s,h,r	6%~9%
III	中使用频率字母集:d,l	4%
IV	低使用频率字母集:c, u,m,w,f,g,y,p,b	1.5%~2.3%
V	次低使用频率字母集:v,k,j,x,q,z	1%

3.确定映射关系

e→n; t→o

传统加密方法

❖佛吉尼亚(Vigenere)密码

- **加密方式**：
  - 列出明文并重复明文
  - 用密钥逐个字母进行移位加密
  - 加密公式：

    C=(P+K)mod26

    C：密文

    P：明文

    K：第几套加密方式
  - 例如

	H	e	r	e	i	s	h	o	w	i	t
Shift	21	4	2	19	14	17	21	4	2	19	14
	C	I	T	X	W	J	C	S	Y	B	H

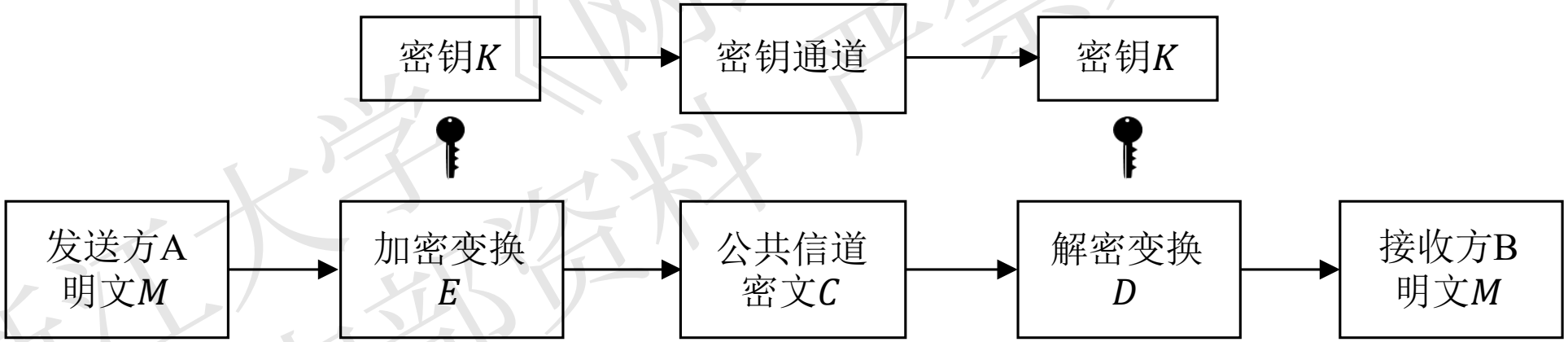
- **特点**：
  - 维吉尼亚密码实际上移位密码的一种扩展
  - 能够消除字母的频率特征?

想一想为什么?

对称密码

❖对称加密

- 也称为单钥密码算法，加密和解密都使用同一把密钥，是20世纪70年代公钥密码诞生之前唯一的加密类型，也是目前应用最广泛的加密类型。
- 通信流程



加密：$C = E(K, M)$

解密：$M = D(K, C)$

对称密码

❖对称加密

- **序列（流）密码：**
  - 通常每次加密数据流的一位或一个字节，如：RC4算法。

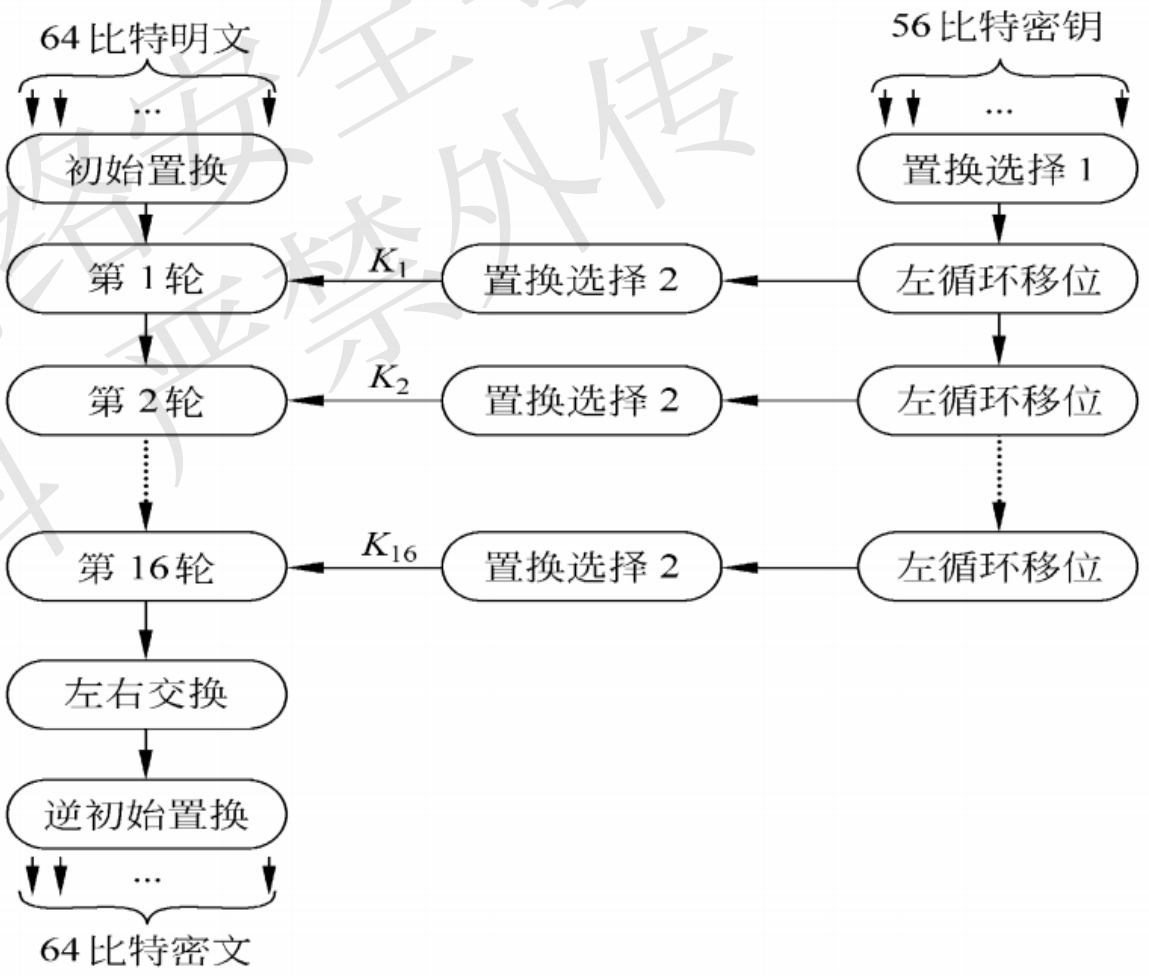
- **分组密码：**
  - 将一个明文分组作为整体加密，并且通常得到的是与明文等长的密文分组。如：DES、AES、SM4等。

SM4是一种国产商用对称密码算法

对称密码

❖DES：Data Encryption Standard

- 分组长度为64bits(8bytes)
- 密文分组长度64bits
- 密钥长度64bits，8bits奇偶校验，有效密钥长度56bits
- 算法主要包括：初始置换IP、16轮迭代的乘积变换、逆初始置换IP^{-1}以及16个子密钥产生器

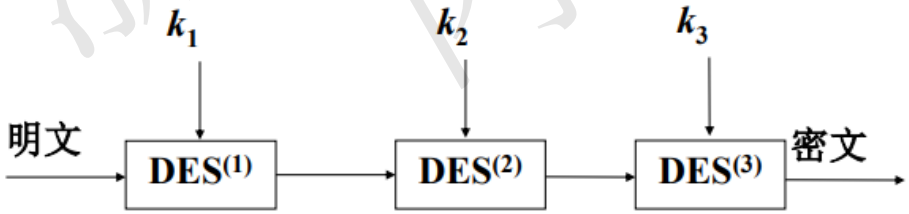


对称密码

❖DES的安全性

- **密钥长度**
  - 密钥长度56bits，密钥数量$2^{56}=7.2*10^{16}$
- **密钥搜索与超级计算**
  - DES的56位短密钥面临的严峻现实：国际互联网Internet的超级计算能力
  - 1997年1月28日，美国RSA数据安全公司在互联网上开展了“**密钥挑战**”的竞赛，一位名叫Rocke Verser的程序员设计了一个通过互联网分段运行的密钥穷举搜索程序，成千上万的志愿者加入其中，在1997年6月17日成功找到了密钥。

❖3DES：三重DES，三个密码组件

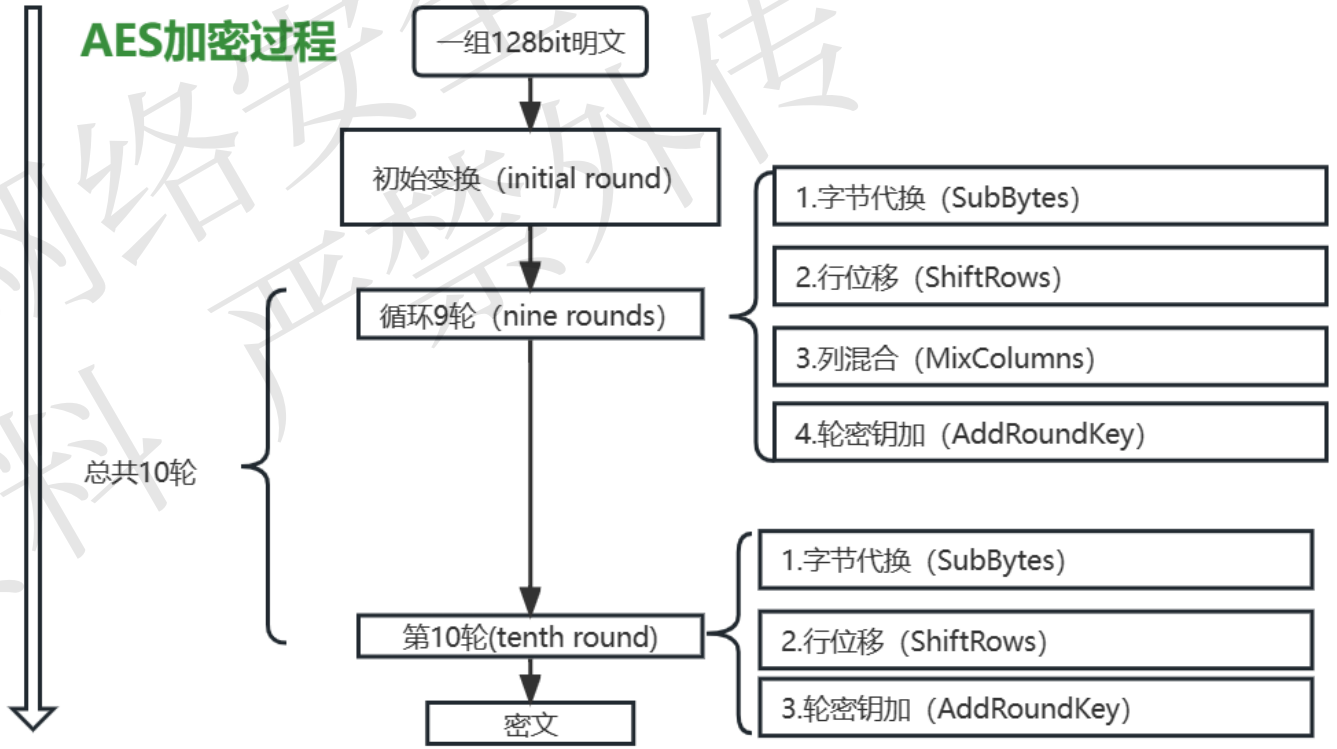


- 若k_1、k_2、k_3互不相等，密钥长度56*3=168暴力破解需要$5.8*10^{29}$年；
- 3DES目前仍有足够的安全性；

对称密码

❖AES：Advanced Encryption Standard

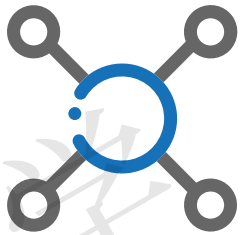
- **AES算法设计思想**
  - 设计简单
  - 在多个平台上速度快，编码紧凑
  - 抵抗所有已知的攻击
  - 轮函数由3个不同的可逆**均匀变换**构成，称为3个层
  - **均匀变换**是指状态的每个bit都用类似的方法处理



非对称密码

❖对称加密的“限制”

- 考虑一个具有N个用户的团体，如果用户两两之间都需要进行安全通信：采用对称密码体制来保护用户之间的通信：每个用户需要与其余的N-1个用户共享私钥，**整个系统需要管理N(N -1)/2个密钥。**



密钥分发难度大

不支持“开放系统”

密钥管理成本高

❖非对称加密

- 也称双钥密码算法、**公钥密码算法**，每个用户至少有一对密钥；
- 其中一个可以公开，称为**公钥**；另一个仅限用户拥有和使用，称为**私钥**；
- 公钥和私钥是难以互相计算的，但它们可以**互相分别作为加密密明和解密密钥。**

非对称密码

❖非对称加密

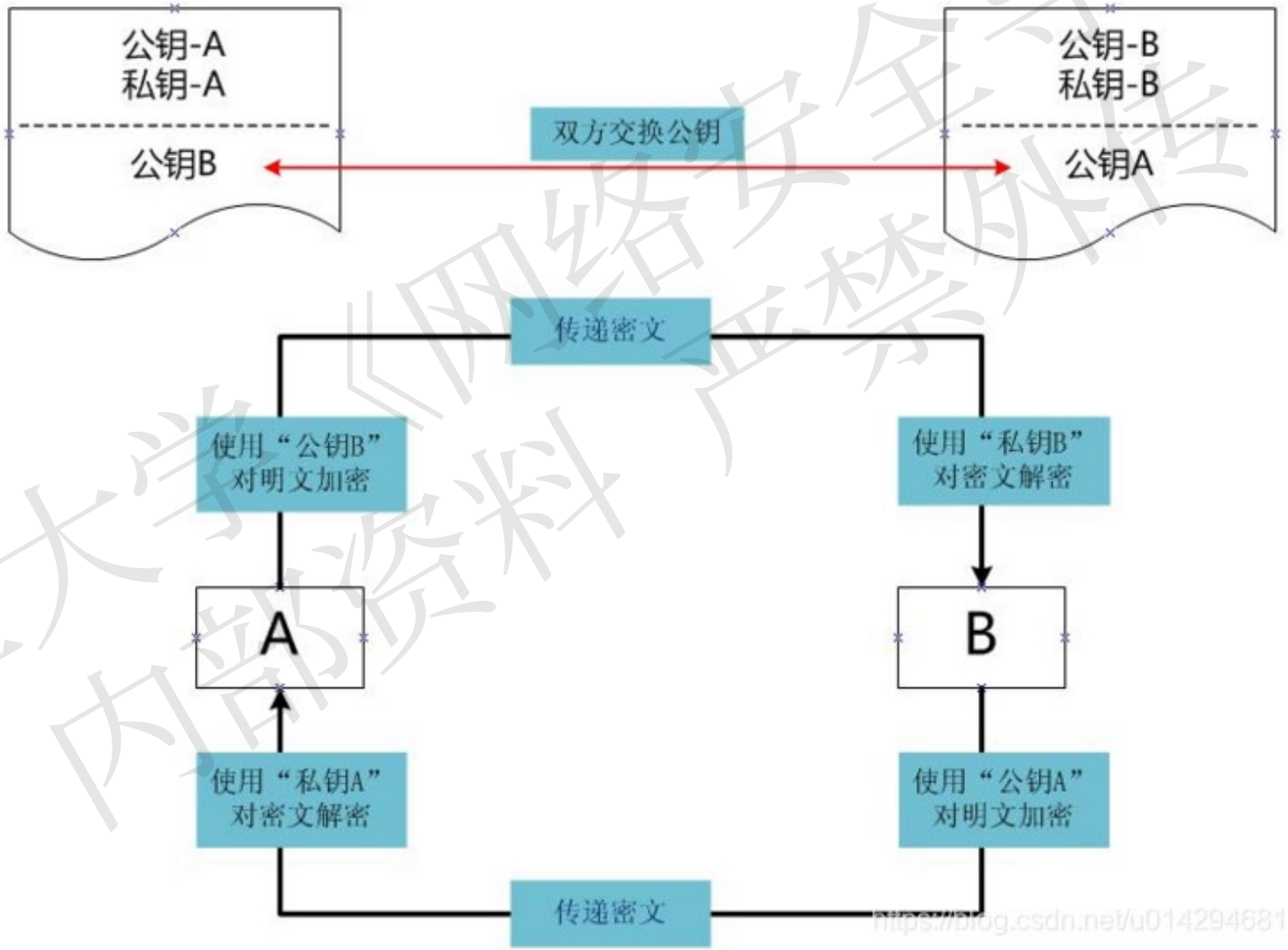
- 例如RSA、ECC、D-H、SM2等。

SM2是一种国产商用公钥密码算法

- **密钥生成：**通过相对容易的计算过程生成一对公钥PK与私钥SK。
  - 如果仅获得公钥PK，得到私钥SK的操作在计算上是不可行的。
- **加密**: 给定明文M与公钥PK，很容易计算得到密文$C=E_{PK}(M)$
- **解密**: 给定密文$C=E_{PK}(M)$ 和私钥SK，很容易计算得到明文M
  - 如果缺少私钥SK，从密文C**不可以**计算得到明文M。
  - **Trapdoor function**: Decrypt(SK,Encrypt(PK,M))=M

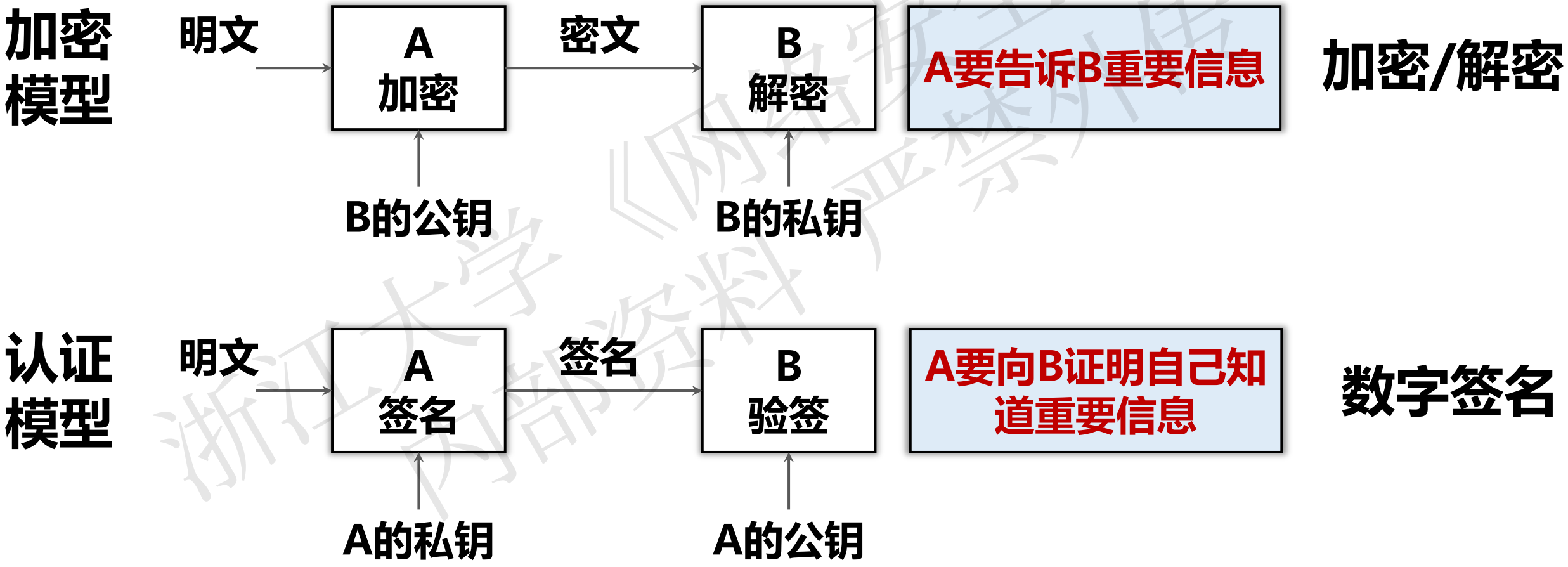
非对称密码

❖非对称加密



非对称密码

❖非对称密码应用



非对称密码

❖非对称加密

密钥分发

公钥能够采用公开(认证的)信道进行传输

开放系统

没有预先建立关系的用户也能通过对方的公钥建立安全通信

密钥管理

N人系统中，整个系统仅仅需要维护N个公钥

- **非对称加密应用**
  - **HTTPs**：Hyper Text Transfer Protocol over Secure Socket Layer，在HTTP协议下加入SSL，提升安全性，可用于敏感信息的通讯。
  - **PGP**：Pretty Good Privacy：secure E-mail
  - 军工、政府

非对称密码

❖RSA算法

密钥生成：

1. 选择两个大素数p, q（例如：每个数字1024位)
2. 选择$n = pq, z = (p-1)(q-1)$
3. 随机选取 e（其中$e < n$），e与z没有公因数。（e, z“互为质数”）
4. 选取d使得$ed-1$能够被z完全整除。（即：$ed \bmod z = 1$）
5. 公钥是$\underbrace{(n, e)}_{K_B^+}$。私钥是$\underbrace{(n, d)}_{K_B^-}$。

❖RSA算法

加密/解密算法：

如上所述给出(n, e)和(n, d)

加密：由$c = m^e \ mod \ n$将明文m转变为密文c（即：当m^e除以n所得的余数）。

注意：$m < n$（如果需要，则分块）

解密：$m = c^d \ mod \ n$ （即：c^d除以n所得的余数）。

核心思想： $m = (\underbrace{m^e \bmod n}_{c})^d \bmod n$

❖RSA算法

Bob选择$p=5, q=7$，则$n=35, z=24$。$e=5$（所以e, z互为质数）

$d=29$（所以$ed-1$能完全被z整除）

字母：L，字母顺序No.12

加密 $letter$ → m → m^e → $c = m^e \bmod n$

1 → 12 → 1524832 → 17

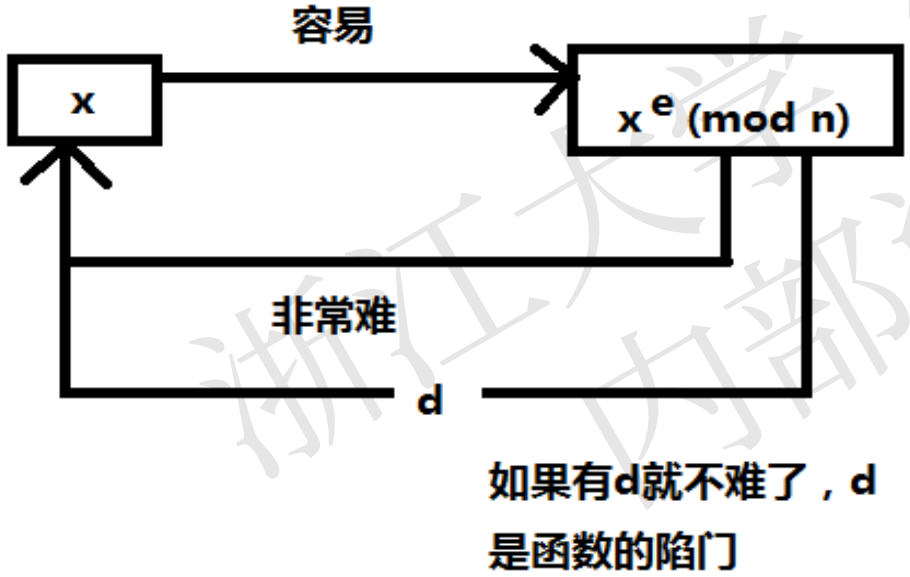
解密 c → c^d → $m = c^d \bmod n$ → $letter$

17 → 481968572106750915091411825223071697 → 12 → 1

非对称密码

❖RSA算法

- **核心思想与安全性**
  - **对于大素数 p 和 q，计算 n = pxq 非常简单，但是在已知 n 的情况下分解因子得到 p 和 q 则相当困难。**



$d = e^{-1}\ mod\ (\varphi(n))$
即已知e，$\varphi(n)$未知，求d

若可知$\varphi(n)$，求d十分容易
即已知n，求$\varphi(n)$

若利用$n = pq, \varphi(n) = (p-1)(q-1)$，则求解十分容易

问题本质：已知n，求$n = pq$即数的**素分解问题**。
这一问题的时间复杂度是exp（sqrt（ln n lnln n））

一般情况下，破解RSA密钥成为计算上的不可解问题。

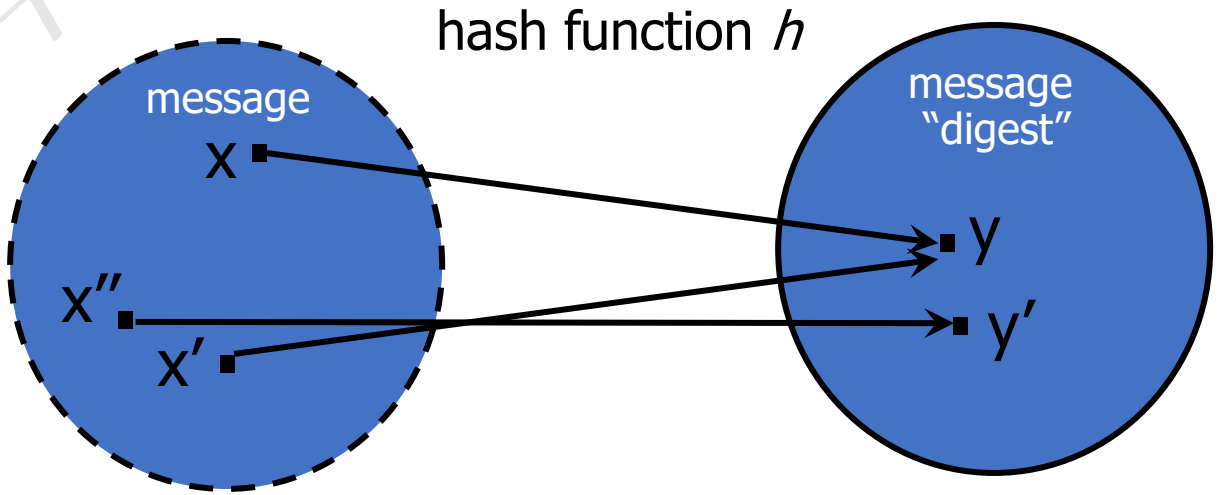
两种密码对比

	对称密码算法	非对称密码算法
加解密密钥关系	相同或容易推导	不同且推导困难
安全强度	较强	较强
算法效率	简便、高效	复杂、效率较低
密钥保护	需要安全分发、存储等	公钥可公开，私钥需要加密保护
应用场景	数据加密（大量数据）、消息认证	少量数据加密、密钥交换和数字签名

哈希（Hash）函数

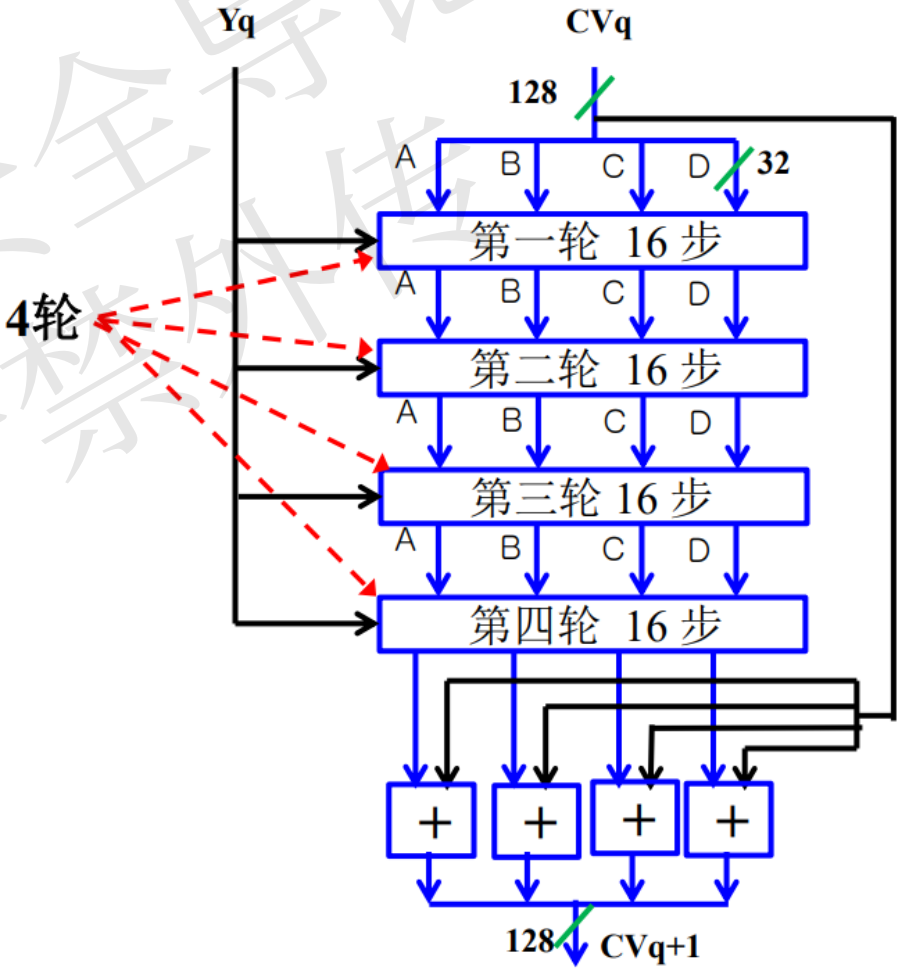
- **特点：**
  - H 可以作用于**任意长度的数据块**；H能够生成**大小固定的输出**。
  - 任意给定消息M，**容易计算出H(M)**；任意给定X，很难找到M来满足 H(M)=X，计算上具有不可行性，即**单向性**；计算复杂度低
  - 任意给定数据 M，找到不等于 M 的 M′，使得 H(M)=H(M′) 在计算上是不可行的，即抗碰撞性；
  - 例子：**MD5、SHA系列、SM3**
  - 应用：**消息认证、身份认证、密钥分发**

SM3是国产商用Hash算法



哈希（Hash）函数

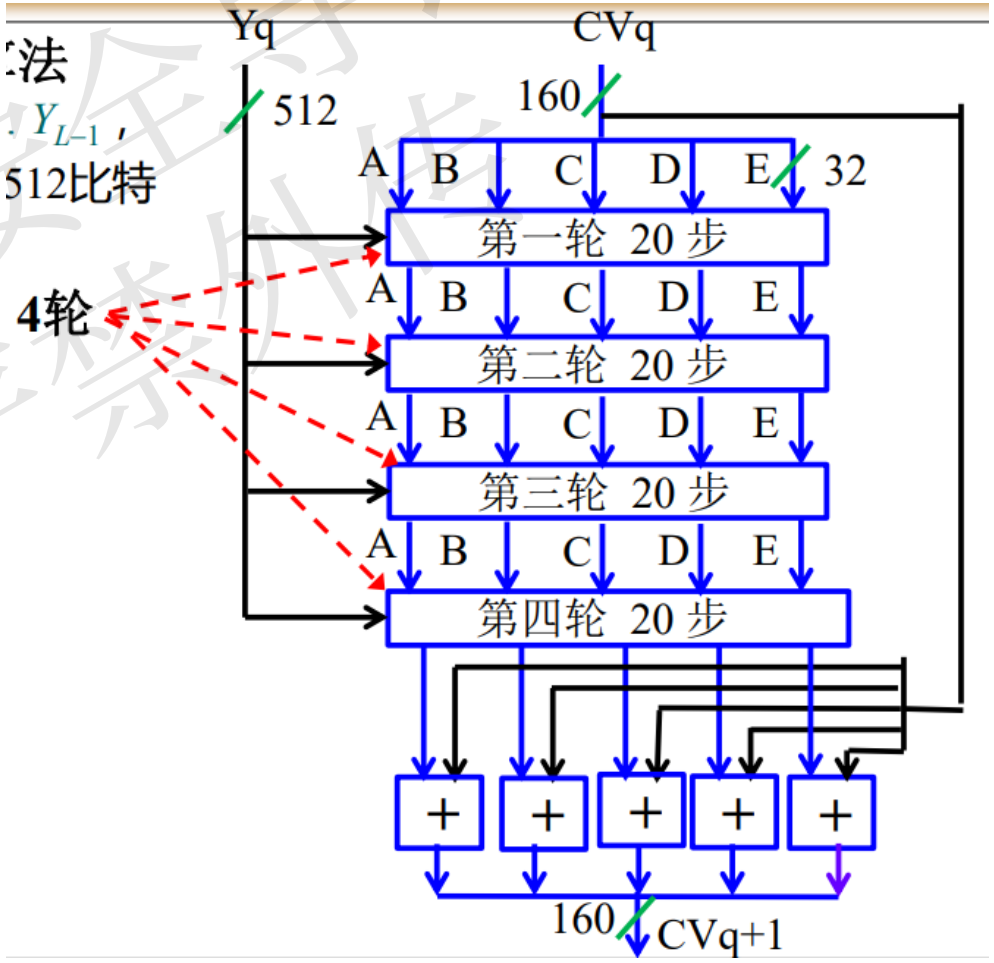
- **MD5 (Message Digest, 消息摘要)算法**
  - 输入消息可以是**任意长度**
  - 每次迭代处理512bits的消息分组
  - 最终输出散列值为128bits
  - 智能手机中每过数秒就可以找到一个**MD5碰撞案例**，不被推荐作为应用中的算法方案
  - 取代的是SHA (secure hash algorithm)家族算法



哈希（Hash）函数

- **SHA (Secure Hash Algorithm)算法**
  - **最大消息长度<2^64**
  - 每次迭代处理512bits的消息分组
  - 输出散列值为160bits

	SHA-1	MD5
最大消息长度	$<2^{64}$	不限
消息分组长度	512	
结构	Merkle迭代	
链接变量长度	160	128
散列值长度	160	128



主观题 1分

设置

设计加密方案：100MB数据，A只允许B获得数据，A有B的RSA公钥，规定算法RSA、SM4，选择哪种密码算法?

算法的选择，涉及安全强度、计算效率、实现代价等多种因数。

作答

2.2

密钥管理与密钥分发

密钥管理

❖为什么要管理密钥?

- 根据Kerckhoffs原则，密码体制的保密性取决于密码系统所使用的密钥的安全性。
- 因此，**密钥管理是保证密码系统安全性的关键。**

Kerckhoffs Principle （柯克霍夫原则）：即使密码系统的任何细节已为人悉知，只要密钥未泄漏，它也应该是安全的。

密钥管理

❖密钥管理概述

- 密钥也是数据，是用来加密其他数据的数据，设计密码系统时，对于密钥必须考虑**以下问题**：
  - 哪些地方需要用到密钥，如何设置和安装在那个地方
  - 密钥预计使用期限是多长（**=限制破译时间**）
  - 隔多久更换一次密钥，不同应用场景密钥生存周期不同（会话密钥、主密钥）
  - 如何对密钥进行严格的保护（**密码保护方法，下一页ppt)**
- **密钥保护基本原则**：
  - 密钥永远不可以以明文的形式出现在密码装置之外，密码装置可以是硬件或软件

密钥管理

❖密钥保护

- **采用密码技术**：
  - 加密保护密钥， E(K_e, K)
  - 完整性验证、数字签名
  - 时间戳限定密钥有效期、抵抗重放攻击
- **采用物理手段**：
  - 脱机存储密钥
  - 从独立的安全密钥存储设备中加载密钥

密钥管理

❖密钥管理服务

- **密钥生成**：
  - 为特定密码算法以**安全的方式生成密钥**的服务
  - 过程不能被篡改，生成方式不可预测，分布符合指定要求
  - 密钥生成常与随机数生成器相关：**随机性、不可预测性、不可重现性**
- **密钥存储**：
  - 密钥存储服务为当前或近期使用的密钥或是备份密钥提供安全存储
  - **常用方法**：物理安全防护、密钥加密存储、口令或PIN码保护

密钥分发

❖密钥分发

- 为已授权实体安全地提供（分发和传送）密钥的过程，其关键在于**如何保证此过程的安全性。**

- **对称密钥分发：**

- **1）点对点**
  - 利用A与B之间的预共享密钥加密保护
  - 利用B的公钥加密保护
  - 每对用户间至少共享一个密钥

主观题 1分

设置

点对点的对称密钥分发中，每对用户间至少共享一个密钥。假设有N个用户，则每个用户管理多少个密钥？系统需要管理多少个密钥？

作答

密钥分发

❖密钥分发

- **对称密钥分发：**
- **2）基于中心**
  - **密钥管理中心（KMC）**，密钥分发中心，密钥传递中心
  - 如有N个用户需要两两通信，设置KMC，系统管理预共享密钥N个，用户管理预共享密钥1个。
  - **存在问题**：中心是瓶颈
  - **解决方式**：分域，为每一个域建立一个KMC，域间如何分发密钥？

    分层KMC，不同区域通过全局KMC负责

密钥分发

❖密钥分发

- **公钥分发：**
- **安全需求**
  - 公钥分发不需要保护其保密性，但需要**保护其真实性**，防止被攻击者替换或假冒
- **常用方法**
  - 公钥证书：公钥基础设施PKI的基础。公钥证书主要功能是实现了用户身份与用户公钥的绑定，而这种绑定的真实性则是通过证书认证机构CA的签名来保证的。

2.3

身份认证与消息认证

信息认证

❖信息认证

- **身份认证**
  - 验证用户、设备是合法的，而不是冒充的，即实体认证；
  - 传统网络安全主要指通信方合法，包括信源、信宿的认证和识别。
- **消息认证**
  - 验证通信消息的完整性，验证数据在传输和存储过程中是否被篡改、重放或延迟。

身份认证

❖（1）基本原理

■ 定义

- 身份认证是指证实主体的真实身份与其所声称的身份是否相符的过程。
- 这一过程通常通过**特定的协议**和**算法**来实现的。

■ 认证协议

- 认证协议：通信参与者为完成相互的身份认证或识别而采用的规程、约定、约束和交换信息的总和。
- **单向认证协议**
- **双向认证协议**

身份认证

❖（2）实现途径

- 所知 (something the user knows)：密码、口令
- 所有 (something the user possesses)：密钥卡、护照/身份证、钥匙
- 特征 (something the user is or how she/he behaves)：指纹、声纹等以及用户的行为，如签名
- 可单因素或组合实现

身份认证

❖（3）技术分类

❖口令认证

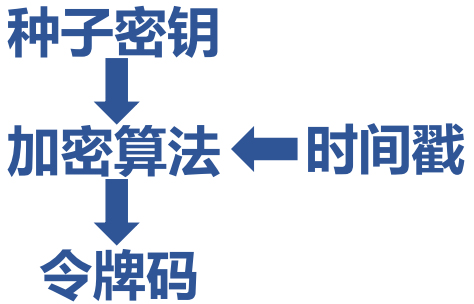
- **简单口令认证**
  - 选用静态密码做为认证的主要因素；
  - **面临的安全威胁**：口令易破解、易受重放攻击（重放用户先前发送的登录信息）、非技术原因窃取。
  - **防护措施**：口令强度、增加随机字符串、限制登录次数、采用强哈希算法等

身份认证

❖（3）技术分类

❖口令认证

- **一次性口令认证（动态）**
  - 用户每次登录系统时认证的口令都不同，以提高系统的安全性；
  - 如何实现：用户记忆口令（固定不变） + 变化因子
  - **时间同步变化因子**：以时间做不确定因子。时间同步令牌，内置时钟、种子密钥和加密算法，定时生成一个动态口令。例如：PIN + 令牌码



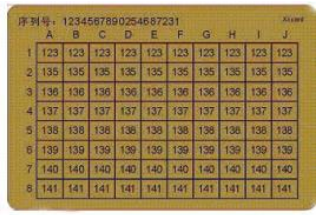
身份认证

❖（3）技术分类

❖口令认证

- **一次性口令认证（动态）**
  - **挑战/应答变化因子**：验证者首先发给示证者一个挑战，并要求后续从示证者收到的应答中包含这个挑战值或这个挑战值进行某种事先约定的计算后的正确结果 。
  - 口令卡，图像网格等

电子银行口令卡正面



电子银行口令卡背面

身份认证

❖（3）技术分类

❖口令认证

- **一次性口令认证（动态）**
  - **事件同步变化因子**：事件同步机制是以事件（次数N）作为变量。
  - S/KEY是首次基于一次性口令思想开发的身份认证系统，现已作为标准协议(RFC 1760）。Opt进行1次Hash计算，与前一次存储口令比较。
  - **S/KEY特点**：用户的秘密口令不在网上传输
    不存储在服务器端及客户端
  - **S/KEY不足**：用户登录一定次数后，必须重新初始化口令序列；单向认证

身份认证

❖（3）技术分类

❖基于共享密钥认证

- 基于共享密钥的认证依靠一定协议下的数据加密处理。通信双方**共享一个密钥**，该密钥在认证协议中处理或加密信息交换。
- **无可信第三方参与的认证（事先认识）**
  - 如何安全地向验证者证明自己有共享密钥?
  - 如何确保消息地时效性（新鲜性）？
  - 时间戳、挑战/应答、ISO对称密钥三次传输双向认证
- **有可信第三方参与的认证（Needham/Schroeder、Kerberos等认证协议）**

身份认证

❖（3）技术分类

❖公钥认证

- 声称者要通过证明他知道私钥来证实身份。
- **公钥认证特点**
  - 验证过程不泄露自己的私钥
  - 密钥分配简化
- **方法一：**验证者发明文挑战值，示证者以自己的私钥签名；验证者以其公钥验证。
- **方法二：**验证者以示证者公钥加密挑战值，示证者以其私钥解密挑战值回送验证者。

身份认证

❖设备认证

- IP 地址
- Web Cookies
- 设备 ID

设备指纹（特征）

示例：浏览器Cookies

身份认证

❖设备认证

- **设备指纹定义**：一种唯一标识出该设备特征的设备标识。
- **设备指纹构成**：通常由**单种**或**多种**设备特征信息构成，其包含的特征信息越多，安全性越高。
- **设备指纹认证技术**：使用设备指纹作为设备标识，对物联网终端设备进行识别和认证的技术。

身份认证

❖设备认证

- **设备指纹来源**：软件、硬件
- **软件设备指纹**
  - 来源于终端设备软件层面，例如浏览器信息、设备网络行为及设备软件环境等。
  - 特殊软件设备指纹：设备ID，如MAC地址等。

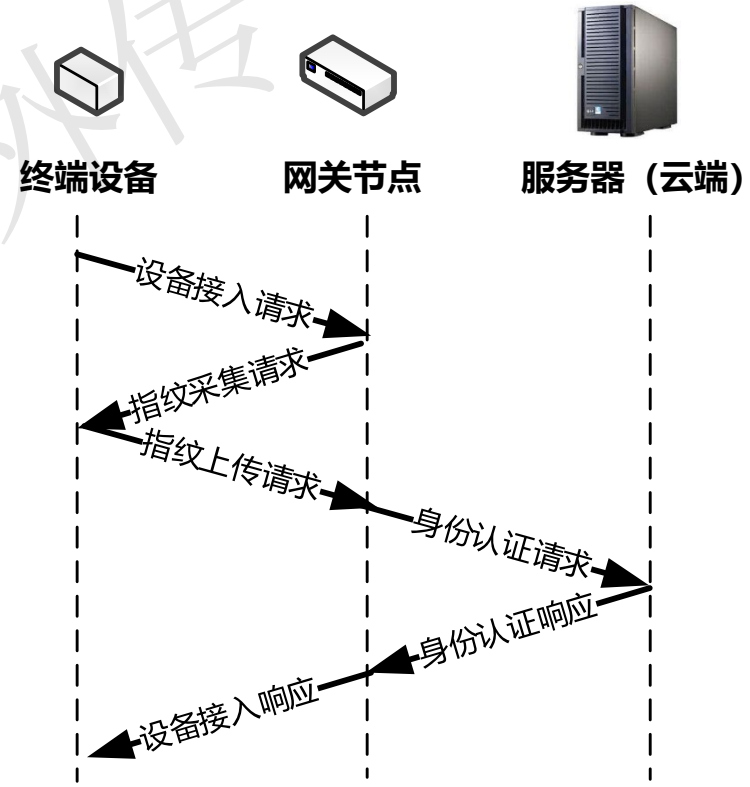
示例：路由器标签上的MAC地址

- **硬件设备指纹**
  - 来源于终端设备的硬件层面，例如终端设备的感知、计算和传输单元等。
  - 终端设备硬件部件在制造过程中存在细微差异，可通过相应部件的输出信号进行观测

身份认证

❖设备认证方法

- **面向网络**
  - 终端设备请求接入网络或进行数据交换时，向网关节点发出一个接入或数据交换请求。
  - 当网关节点收到该请求时，通过设备的 API接口或外置测量设备收集指纹相关信息，并生成设备指纹**X**。
  - 网关节点将此设备指纹上传到指纹库（通常存在于云端），发送身份认证请求。
  - 指纹库收到身份认证请求时，通过匹配算法将X与设备指纹库中预先记录的指纹信息进行比对。
  - 指纹库根据认证结果向网关节点发送身份认证响应，网关节点根据该响应向终端设备发送接入或数据交换响应。

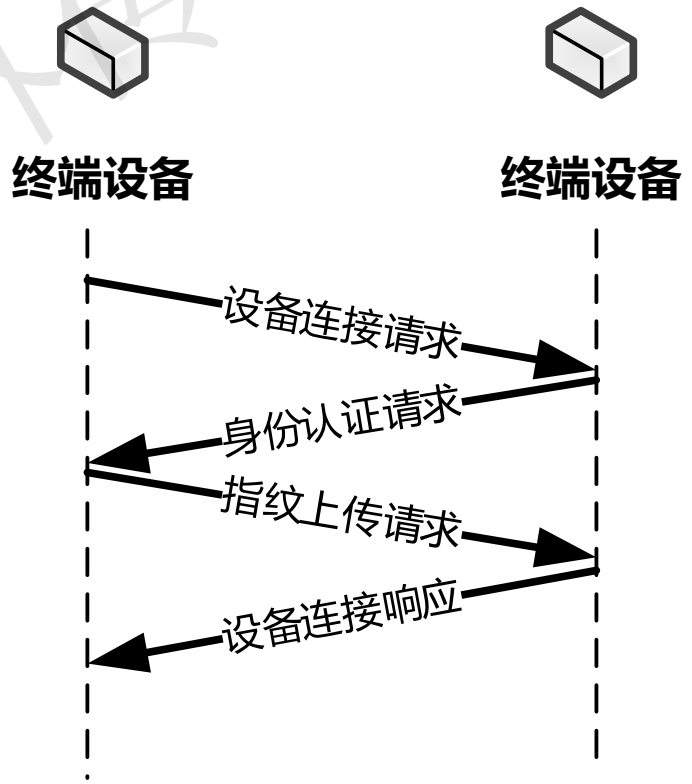


身份认证

❖设备认证方法

■ 面向设备

- 终端设备**A**请求与另一终端设备**B**建立连接或进行数据传输时，向终端设备**B**发出一个建立连接或数据交换请求。
- 当终端设备**B**收到该请求时，向终端设备**A**返回身份认证请求。
- 终端设备**A**收到身份认证请求后，通过设备的API接口或外置测量设备收集指纹相关信息生成设备指纹**X**，并发送到终端设备**B**进行身份认证。
- 终端设备**B**收到后，通过匹配算法将**X**与本地设备指纹库中预先记录的指纹信息进行比对，并根据认证结果向终端设备**A**发送接入或数据交换响应。



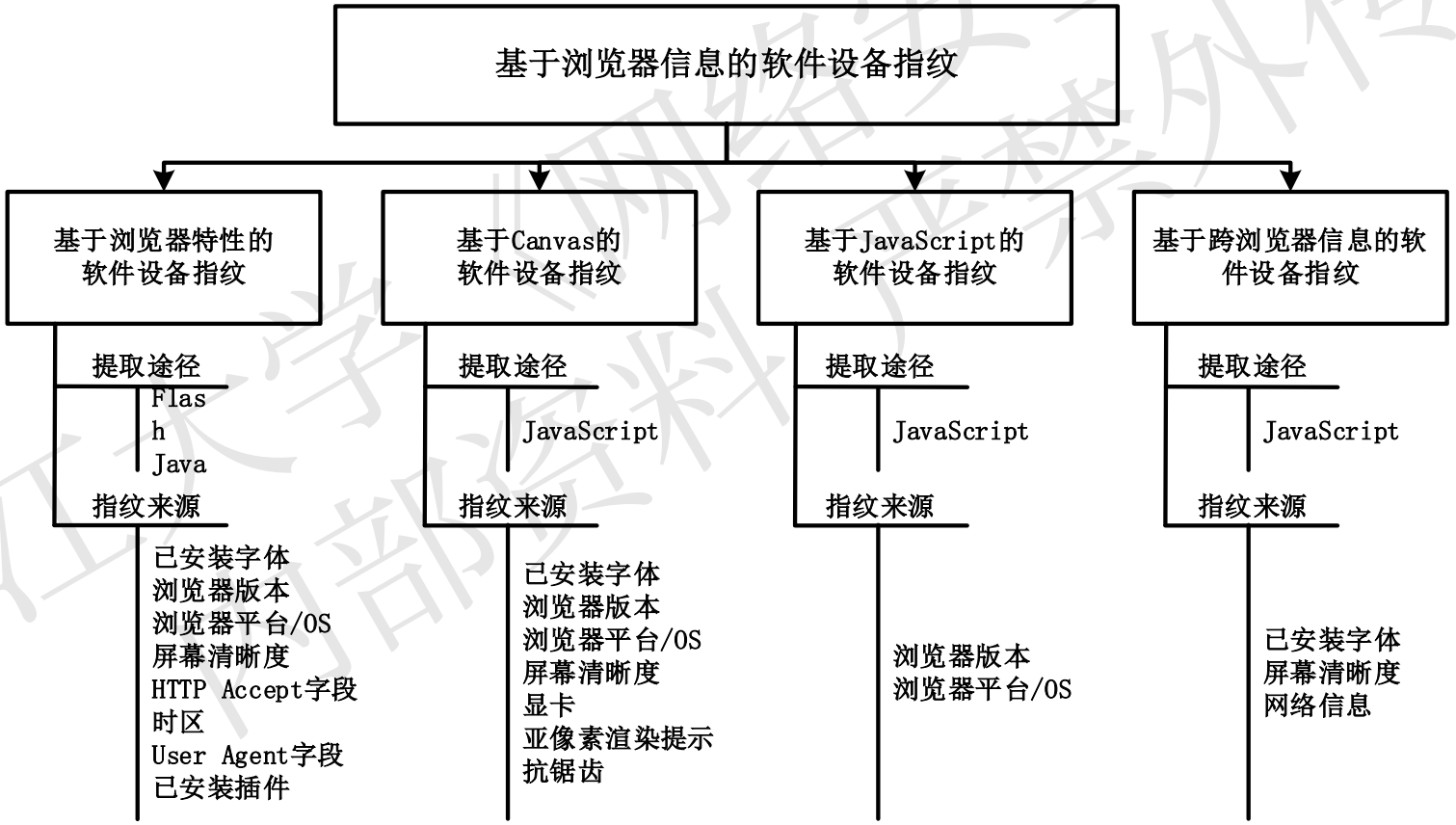
❖软件设备指纹

- **基于设备ID的软件设备指纹**

- **MAC地址：**16进制数字，0~23位数字为组织唯一标志符，24~47位由厂家自行分配，第48位是组播地址标志位，具有全球唯一性。（可用特殊工具擦写）
- **IMEI/MEID码：**国际移动设备识别码（IMEI），用于在移动电话网络中识别每一部独立的手机等移动通信设备，即通常所说的手机序列号。（可用特殊工具擦写）
- **UDID码：**设备唯一标识符（UDID）是iOS设备身份标识码，具有全球唯一性。

❖软件设备指纹

■ 基于浏览器信息的软件设备指纹



身份认证

❖硬件设备指纹

■ 基于感知单元的硬件设备指纹

■ MEMS传感器：

- 智能设备常见MEMS传感器主要包括加速度计（Accelerometers），陀螺仪（Gyroscope）和磁力计（Magnetometer）。

- MEMS传感器的测量值可以近似为其真值的线性函数，即$v_m = v_t S + O$，其中v_m和v_t分别为传感器的测量值和真值，S和O为传感器的灵敏度和偏移量，也称为传感器的校正参数。理想情况下，S和O的参数值应为

智能手环中的MEMS加速度计

身份认证

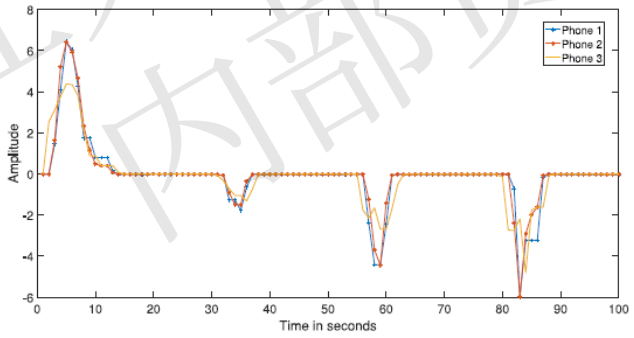
❖硬件设备指纹

■ 基于感知单元的硬件设备指纹

■ MEMS传感器：

- 由于MEMS传感器在制造过程中受到工艺精度的限制，即便是同一型号的不同传感器个体，其硬件电路也存在细微差异，从而导致校正参数S和O的不同的不同。该种差异可以在特定的刺激（如震动）下，体现在传感器读数上，从而成为设备硬件指纹的来源。

- 基于MEMS传感器的硬件设备指纹可以基于单个MEMS传感器或者多个MEMS传感器组合进行构造，其优点在于MEMS传感器应用范围十分广泛，且调用MEMS传感器无需特殊权限，可在用户无感知的情况下实现设备认证。



同一型号不同设备的陀螺仪对特定刺激的响应

身份认证

❖硬件设备指纹

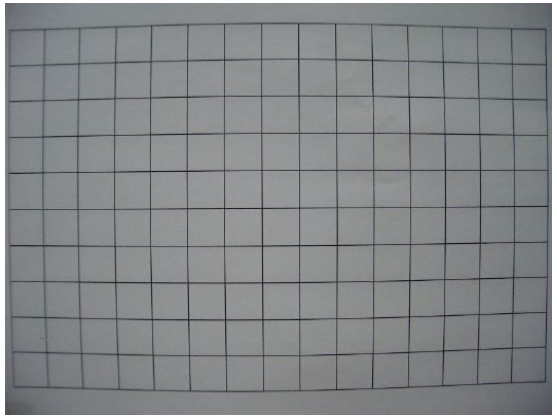
- **基于感知单元的硬件设备指纹**

- **摄像头：**
  - 互补金属氧化物半导体（CMOS）传感器和（或）后续图像处理（如去马赛克，JPEG压缩等）引起的**图像伪像。**

- **作用：**
  - **硬件指纹**和**图像溯源。**

- **指纹来源：**
  - 镜头（Lens）
  - 色彩过滤阵列（Color Filter Array）
  - 传感器（Sensor）
  - 压缩算法（Compression Algorithm）
  - 综合差异

智能手机摄像头结构

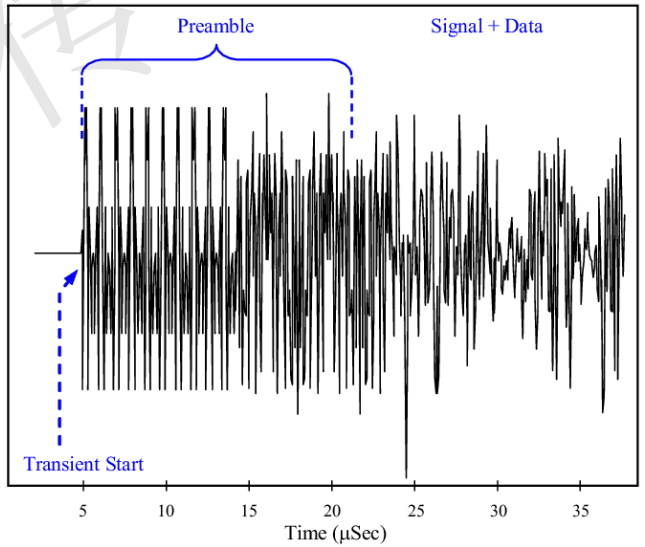


图像畸变

身份认证

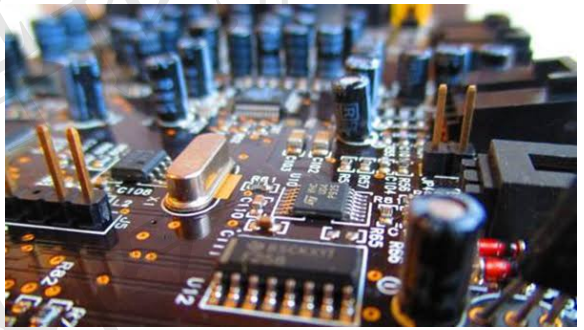
❖硬件设备指纹

- **基于传输单元的硬件设备指纹**
- **射频指纹：**
  - **射频指纹 (Radio Frequency Fingerprinting，RFF)** 即硬件的差异，这种硬件上的差异会反映在通信信号中，每个无线设备有不同的射频指纹。
- **指纹存在位置：**
  - **物理层**
- **发展历史**
  - 在1995 年Toonstra等人明确提出利用无线发射机的**瞬态信号**产生独特的“指纹”进行设备识别。
  - 在2003 年加拿大的Hall 等人：通过提取蓝牙通信信号中的射频指纹进行蓝牙通信设备的识别
  - 在2008 年Kennedy等人：首次提出了基于**稳态信号**的射频指纹研究

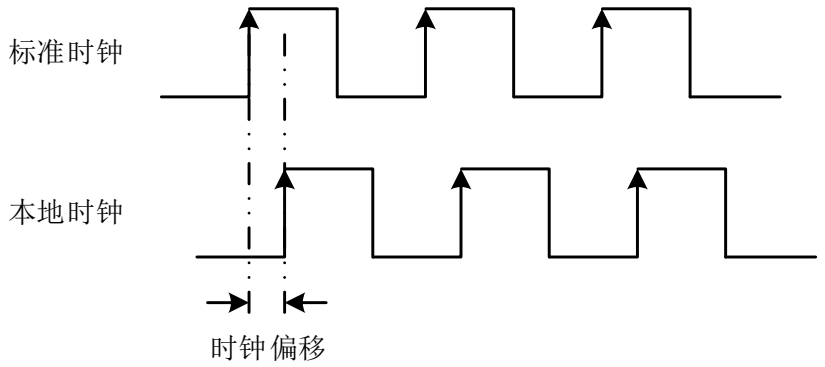


身份认证

❖硬件设备指纹



- **基于计算单元的硬件设备指纹**
- **时钟晶振：**
  - 受到当下制造工艺限制，智能设备硬件之间存在微小差异，该差异导致智能设备的本地时钟相对于标准时钟存在细微的**时钟偏移（Clock Skew）**
  - 经过长时间的积累，智能设备本地时钟相对于标准时钟的偏移变得可观测和可测量，而两者相对变化的速率则称为设备的**时钟偏移率（Clock Skewness）**

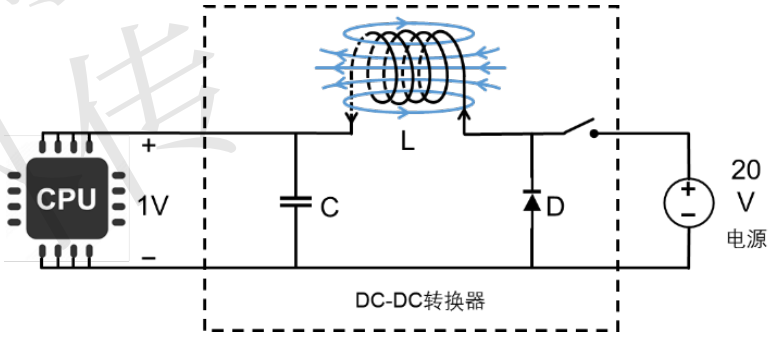


- **特性：**
  - 可测性：不会被时间同步消除
  - 唯一性和区分性
  - 稳定性
  - 由设备硬件系统决定的**常量**，与设备的位置、IP 地址、网络拓扑和测量时刻均无关，可用于硬件设备指纹

身份认证

❖硬件设备指纹

- **基于计算单元的硬件设备指纹**
- **中央处理器（CPU）：**
  - 不同型号的CPU，其**硬件结构**和**参数规格**存在差异。
  - 即使相同型号的CPU，由于制造过程中工艺限制引入的**缺陷**，其硬件电路也存在**细微差异**。该种差异可以体现在CPU辐射的电磁信号上。
- **原理：**
  - CPU电流除流经CPU单元，还将流经CPU附属的DC-DC电压转换模块。该模块中存在的**电感器件**将产生与CPU电流对应的**电磁辐射**。由于CPU硬件电路的不同常导致其工作电压、电流存在细微差异，且CPU及其附属DC-DC电压转换模块辐射的电磁信号可以放大且体现差异。
- **优点：**
  - 更具有**通用性**，且其指纹数据来源可在设备外部测量得到，可以免受设备内部安全问题干扰



CPU模块电磁辐射机理

身份认证

❖生物认证

- **身份认证类型：**
  - 基于“**用户有什么**（what you have）”：令牌（token）
  - 基于“**用户知道什么**（what you know）”：密码，PIN码等
  - 基于“**用户是什么**（what you are）”：生物识别技术等
- **生物认证技术作用：**
  - 可以支持信息安全中**识别**，**身份验证**和**不可抵赖性**等多方面的需求
  - 不需要用户拥有或者记忆特定的身份信息，且可以在个体和身份之间建立牢不可破的**一对一**对应关系。

❖生物认证

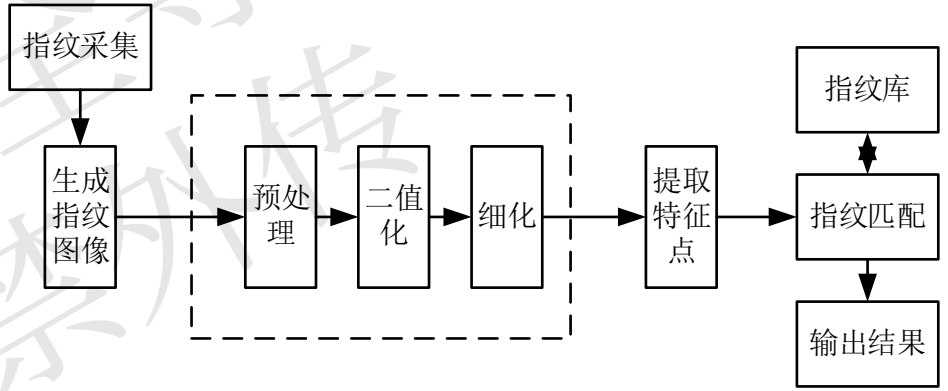
- **选取：**
  - 每种生物识别技术均拥有其优点和缺点，没有一种可以有效地满足所有应用的要求。换句话说，没有生物特征是“最佳的”。因此，生物识别技术的选用通常取决于**应用的实际需求**
- **分类：在现代生物认证技术中，使用的生物特征可分为两大类别**
  - **生理性特征。**该类生物特征与用户身体生理形状有关，如指纹，面部特征，手部几何特征及虹膜等。
  - **行为性特征。**该类生物特征与用户行为习惯有关，如签名、说话方式、打字习惯等。

身份认证

❖生物认证

■ 指纹识别

- 其形成在胎儿发育的前七个月期间确定
- 指纹形态特征包括中心（上、下）和三角点（左、右）等，指纹的细节特征点主要包括纹线的起点、终点、结合点和分叉点。



■ 人脸识别

- 最常见、最自然的生物识别技术之一。
- 利用可见光获取人脸图像信息，无需用户参与，因此更易被用户接受。
- 基于人脸特征点的识别算法、基于模板匹配的识别算法、基于人工神经网络的识别算法
- 制约因素：光照、姿态、遮挡、年龄变化、图像质量

■声纹、虹膜、手型、视网膜、DNA、掌纹、静脉几何形状

小节

- 对称/非对称密码算法：加解密、数字签名
- Hash函数：消息认证、身份认证
- 密钥管理、密钥分发
- 身份认证（用户、通信）
- 设备认证，设备指纹
- 用户生物认证