绪论

**古典密码**

* + 单表代替密码：Caesar密码
  + 多表代替密码：Vigenere密码、Hill密码
  + 转轮密码：Enigma密码

**密码学发展三个阶段（古典密码、近代密码、现代密码）**

**现代密码学的要求**

（1）必须提供高度的安全性；

（2）具有相当高的复杂性，使得破译的开销超过可能获得的利益，同时又便于理解和掌握；

（3）安全性应不依赖于算法的保密，其加密的安全性仅以加密密钥的保密为基础；

（4）必须适用于不同的用户和不同的场合；

（5）实现算法的电子器件必须很经济、运行有效；

（6）必须能够验证。

**安全机制**

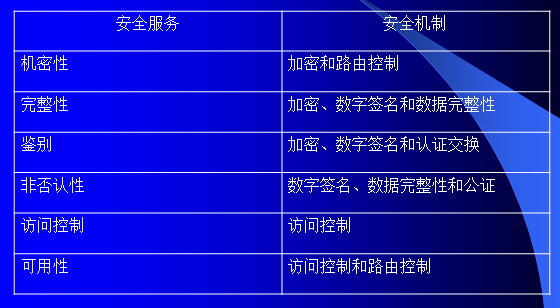
* + **概念：**用来保护系统免受侦听、阻止安全攻击及恢复系统的机制
  + **特定的安全机制：**加密、数字签名、访问控制、数据完整性、认证交换、 流量填充…
  + **通用的安全机制:**可信功能、安全标签、事件检测、安全审计跟踪、安全恢复

**安全服务**

**概念：**加强数据处理系统和信息传输的安全性的一类服务

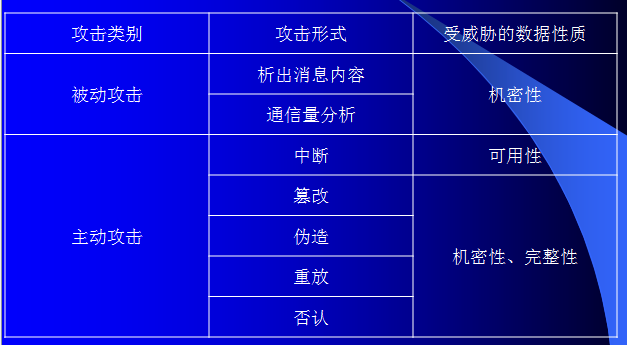
**目的：**利用一种或多种安全机制阻止安全攻击

**安全服务的特点：机密性、完整性、鉴别、非否认性、访问控制、可用性**



**安全攻击的主要形式：**

**截取、中断、篡改、伪造、重放、否认**



**被动攻击**

* + **攻击者只是观察通过一个连接的协议数据单元PDU，以便了解与交换相关的信息，并不修改数据或危害系统；这种消息的泄露可能会危害消息的发送方与接收方，但对系统本身不会造成任何影响，系统能够正常工作**
  + **难以检测**
  + **重点是防止，提供机密性**

**主动攻击**

* + **指攻击者对连接中通过的PDU进行各种处理，这些攻击涉及某些数据流的篡改或一个虚假流的产生**
  + **难以防止**
  + **重点是检测，发现并恢复**

**密码学基础**

**密码分析分类**

* **唯密文攻击（Ciphertext only）**
  + **破译者已知：加密算法、待破译的密文**
* **已知明文攻击（Known plaintext）**
  + **破译者已知：加密算法、一定数量的密文和对应的明文**
* **选择明文攻击（Chosen plaintext）** 
  + **破译者已知：加密算法、选定的明文和对应的密文**
* **选择密文攻击（Chosen ciphertext）** 
  + **破译者已知：加密算法、选定的密文和对应的明文**
* **选择文本攻击（Chosen text）**
  + **破译者已知：加密算法、选定的明文和对应的密文、选定的密文和对应的明文**

**分析**

**唯密文攻击是最困难的**

**上述攻击的强度是递增的**

**一个密码体制是安全的，通常是指在前三种攻击下的安全性**

**密码系统**

**概念：用于加密与解密的系统**

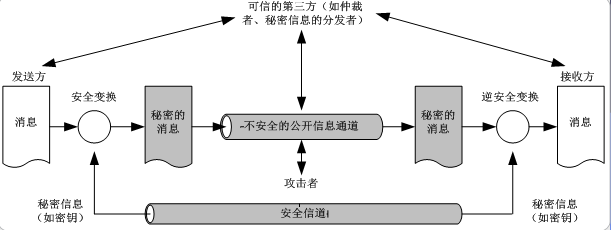
**衡量攻击方法的复杂性**

* **数据复杂性（data complexity）**
* **处理复杂性（processing complexity）**
* **存储需求（storage requirement）**

**安全模型**

**网络传输中的信息安全**

* + **动态数据的安全**
  + **网络安全模型**



**计算机系统中的信息安全**

* + **静态数据的安全**
  + **网络访问安全模型**

****

**密码体制**

* **对称密码体制**
* **非对称密码体制（公钥密码体制）**

**对称密码算法的优、缺点**

* **优点：加/解密处理速度快、保密度高等。**
* **缺点：**

1. **如何把密钥安全地送到收信方，是对称密码算法的突出问题。对称密码算法的密钥分发过程十分复杂，所花代价高**
2. **多人通信时密钥组合的数量会出现爆炸性膨胀，使密钥分发更加复杂化**
3. **通信双方必须统一密钥，如果发信者与收信人素不相识，这就无法向对方发送秘密信息了**
4. **存在数字签名困难问题**

**（非对称密码体制）公开密钥密码体制的优、缺点**

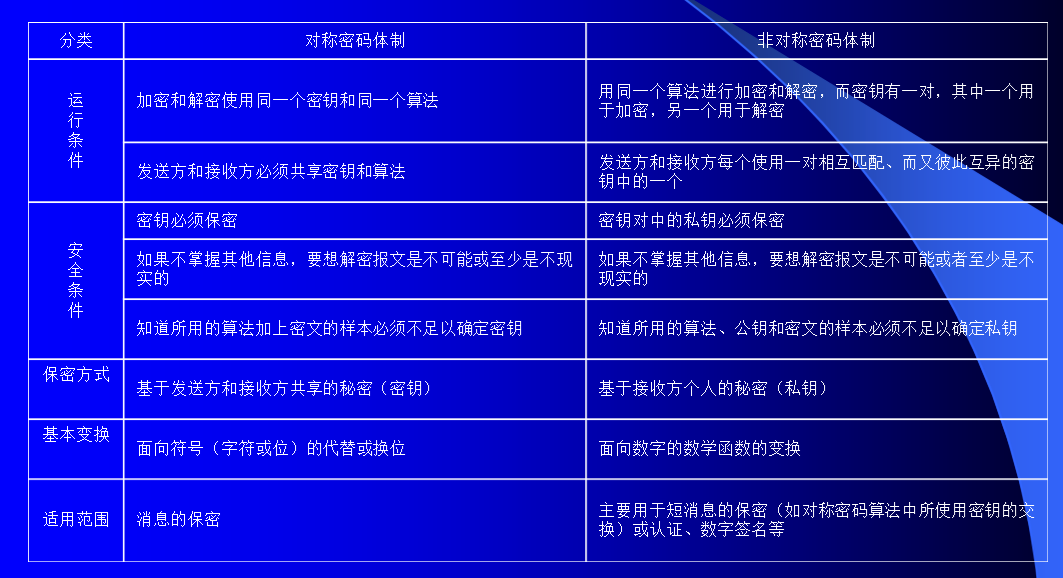
* **优点：**

1. **网络中的每一个用户只需要保存自己的私有密钥。密钥少，便于管理**

**2、密钥分配简单，不需要秘密的通道和复杂的协议来传送密钥**

**3 可实现数字签名**

* **缺点：加密、解密处理速度相对较慢，同等安全强度下所要求的密钥位数多一些**



**古典密码**

**隐写术**

**代替**

**换位**

**代替密码的实现方法分类**

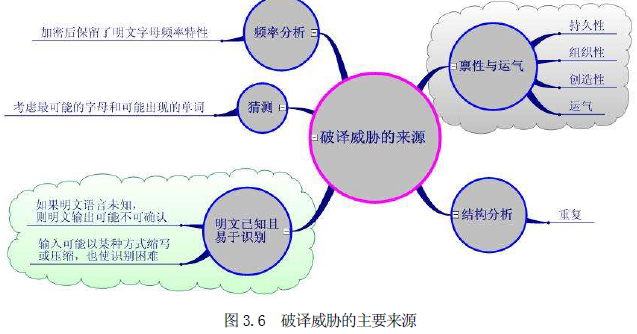
* 单表代替密码
  + 使用密钥的单表代替加密
  + 仿射加密

**特点**：

密钥量很小，不能抵抗穷尽搜索攻击

没有将明文字母出现的概率掩藏起来，很容易受到频率分析的攻击

* 多表代替密码
  + Playfair密码
  + Hill密码
  + Vigenere密码

****

**密码学的数学引论**

**现代密码技术：**

**分组密码： DES、AES**

**非对称密码： Diffie-Hellman算法、RSA、椭圆曲线密码体制**

**序列密码： RC4**

**杂凑算法： SHA-1**

**其它密码技术： 量子密码技术**

**例子.通过同余式演算证明：**

**（1）560－1是56的倍数**

**（2）223－1是47的倍数。**

**解： 注意53=125≡13(mod56)**

**于是有56≡169≡1(mod56)**

**对同余式的两边同时升到10次幂， 即有56∣560-1。**

**同理, 注意到26=64≡17(mod47), 于是**

**223=(26)3·25=(26 · 26)26 · 25**

**≡289\*(17)\*(32) mod47**

**≡7\*17\*32 (mod47)**

**≡ 25\*32(mod47)**

**≡1(mod47)**

**于是有 47∣223-1**

**扩展欧几里得算法（例子）**

* **Extended EUCLID(d,f)：**
* **1）(X1,X2,X3) ←(1,0,f)；(Y1,Y2,Y3)←(0,1,d)**
* **2）如果Y3=0返回X3=gcd(d,f)；无逆元**
* **3）如果Y3=1返回Y3=gcd(d,f)；Y2=d-1modf**
* **4）Q=max\_int(X3/Y3)**
* **5）(T1,T2,T3) ←(X1-Q·Y1,X2-Q·Y2,X3-Q·Y3)**
* **6）(X1,X2,X3) ←(Y1,Y2,Y3)**
* **7）(Y1,Y2,Y3) ←(T1,T2,T3)**
* **8）回到 2）**

**例：求gcd(20,117)和20-1mod117**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Q** | **X1** | **X2** | **X3** | **Y1（T1）** | **Y2（T2）** | **Y3(T3)** |
| **-** | **1** | **0** | **117** | **0** | **1** | **20** |
| **5** | **0** | **1** | **20** | **1** | **-5** | **17** |
| **1** | **1** | **-5** | **17** | **-1** | **6** | **3** |
| **5** | **-1** | **6** | **3** | **6** | **-35** | **2** |
| **1** | **6** | **-35** | **2** | **-7** | **41** | **1=gcd** |

**威尔逊定理：**

**当且仅当p为质数时，(p－1)!＋1能被p整除。（逆定理成立）**

**Fermat定理：**

**如果p是素数并且a是不能被p整除的正整数,那么，ap-1≡1(mod p)**

**例子：**

**a=7,p=19,求ap-1modp**

**解：72=49≡11mod19**

**74≡121mod19≡7mod19**

**78≡49mod19≡11mod19**

**716≡121mod19≡7mod19**

**ap-1=718=716×72≡7×11mod19≡1mod19**

**欧拉定理（Euler）（文字表述）：**

**若整数a与整数n互素，则a φ(n)≡1(mod n)**

**注：**

**1\*. n＝p时，有ap-1≡1(mod p)为Format定理！**

**2\*.易见a φ(n)+1≡a(mod n)**

**中国剩余定理(CRT)**

**群论**

* **群的概念**
  + **是由一个非空集合G组成，在集合G中定义了一个二元运算符“· ”，并满足以下性质的代数系统，记为｛G, · ｝**

****

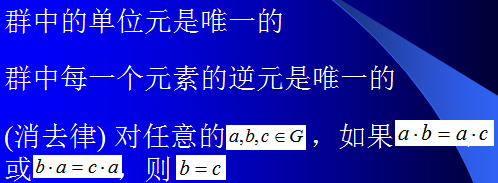
****

****

****

**群的分类：交换群、有限群、无限群、有限群的阶**

**群的性质：**



**环：环R，记为{R,+, x}**

* + 是一个有两个二元运算的集合，分别称为加法和乘法，且对于R中的任意元素a,b,c，满足如下公理：

M1：乘法的封闭性：如果a,b∈R，则axb ∈R (即ab ∈R)

M2：乘法的结合律：对于任意a,b,c∈R，有a(bc)=(ab)c

M3：分配率：对于任意a,b,c∈R，下面两个式子总成立：

a(b+c)=ab+ac

(a+b)c=ac+bc

如果环还满足交换率，则成为交换环。

**域的概念**

**域是由一个非空集合F组成，在集合F中定义了两个二元运算符：“+”和“· ”，并满足：**

****

****

****

****

**域记为｛F,+,·}**

**对称密码体制（第五章）**

1. **分组密码**

**分组密码要求：**

* **分组长度足够大**
* **密钥量足够大**
* **密码变换足够复杂**

**原理：扩散**

就是将每一位明文的影响尽可能迅速地作用到较多的输出密文位中去，以便隐藏明文的统计特性。

**混乱**

**是指**密文和明文之间的统计特性关系尽可能地复杂化。

**乘积密码**

指依次使用两个或两个以上的基本密码，所得结果的密码强度将强于所有单个密码的强度

（s盒与p盒，s盒混淆，p盒扩散）

**雪崩效应：**

**雪崩效应：输入（明文或密钥）即使只有很小的变化，也会导致输出发生巨大变化的现象**

**输入位有很少的变化，经过多轮变换以后导致多位发生变化。即明文的一个比特的变化应该引起密文许多比特的改**

**第九章 密钥管理**

**1.密钥的重要性**

* **密钥的作用：作为密码变换的参数，实现消息的机密性保护**
* **密钥的好处：**
  + **不用担心算法的安全性，保护好密钥比保护好算法要容易得多**
  + **可以使用不同的密钥保护不同的秘密，灵活性、安全性更强**

**2.密钥管理**

**(负责密钥的生成、存储、分配、使用、备份/恢复、更新、撤销和销毁等)**

**密钥管理要求管理与技术并重**

**3.密钥的种类与层次结构:**

**会话密钥**

**在一次通信或数据交换中，直接用于向用户数据提供密码操作的密钥**

* + **短期会话密钥**
  + **长期会话密钥**

**一般密钥加密密钥**

* + **用于会话密钥或其下层密钥的加密，从而可实现这些密钥的在线分发**

**主密钥**

* + **位于整个密钥层次体系的最高层**
  + **可在较长时间内由用户所专用的秘密密钥**
  + **主要用于对密钥加密密钥或会话密钥的保护**
  + **主密钥的分发基于物理渠道或其他可靠的方法**

**4.层次式密钥管理的优势**

* **安全性强**
* **可实现密钥管理的自动化**

**5.密钥的安全存储**

* **基于口令的软保护**
* **基于硬件的物理保护**

**6.密钥的协商与分发**

* **密钥的协商**
  + **是保密通信双方(或多方)通过公开信道的通信来共同形成秘密密钥的过程**
* **密钥的分发**
  + **是保密通信中的一方生成并选择秘密密钥，然后把该密钥发送给通信参与的其他一方或多方的机制**
  + **密钥分发协议**
  + **分类：网外分发、网内分发、密钥的分发、公开密钥的分发**

**第十章 序列密码**

**1.序列密码**

**概念：，流密码，按位或字节处理。**

**特点：实现简单、**

**便于硬件实现、**

**加解密处理速度快、**

**没有或只有有限的错误传播**

**分类：**

**同步流密码**

**自同步流密码**

**2.同步流密码**

**特点：**

* + **同步要求**
  + **无错误传播**
  + **如果密钥流为无限随机序列，则成为一次一密**

**2.自同步流密码**

**特点：**

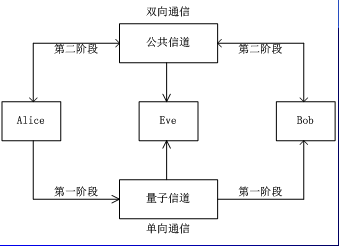
* + **自同步**
  + **有限的错误传播**

**3.流密码和分组密码**

* **流密码的优点**
  + **转换速度快**
  + **低错误传播**
* **流密码的缺点**
  + **低扩散**
  + **有意插入及修改的不敏感性**
* **分组密码的优点**
  + **扩散性**
  + **插入的敏感性**
* **分组密码的缺点**
  + **加密速度慢**
  + **错误传播**

**第11章量子密码学（BB84、B92、E91）**

**BB84量子密码协议**

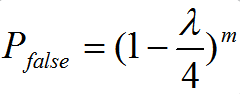


**阶段一：基于量子信道的通信**

* **Alice每次传输单个位，对应光子的一个极化状态，被要求等概率地使用×基极化或＋基极化方式**
* **接收方测量仪的极化方式设置得与发送方一致，就能保证正确地接收，否则正确接收的概率是50%**
* **由于×基极化和＋基极化的测量仪不兼容，根据Heisenberg测不准原理，没有人能够以高于75%的准确率收到Alice传输的光子**

**第二阶段：基于公共信道的两过程通信**

* **过程一：原密钥的确定**
  + **Bob通过公共信道告诉Alice他对每一个收到位的测量设置，Alice通过与自己的设置进行比较，向Bob返回正确的设置位。双方删除不正确的设置位以产生更短的位序列，即原密钥**
* **过程二：通过出错检查来发现入侵行为**
  + **在没有噪声的环境中，双方原密钥间的任何不一致都是有入侵的证据**
  + **比较从原密钥中随机选择的一个位，如果发现至少一个不一致，说明窃听行为的存在**
  + **Eve逃脱发现的概率：**



* **阶段一：基于量子信道的通信**
* **阶段二：基于公开信道的四个通信过程**
  + **过程一：确定原密钥**
    - **与无噪声情况一致**
  + **过程二：原密钥错误估计**
    - **随机取样原密钥，比较并删除这些位以获得错误率的估计值，如果超过了一定的阈值，回到阶段一重新开始**
  + **过程三：确定协调密钥**
    - **步骤一：将原密钥按一定长度分组，公开地比较每个分组的偶校验，如果出现不一致，就启动一个双叉错误搜索。步骤一将重复**
    - **步骤二：公开地随机选取剩余原密钥的子集，比较偶校验结果，每次处理所选定的密钥取样中的一位，重复N次，如果未发现错误，将余下的原密钥定义为协调密钥**
  + **过程四：确定最终密钥**

**量子密码学的分析**

**优势**

1. **密钥生成、分发和存储期间密钥的安全性得到保证**
2. **不存在单向函数的问题**
3. **能通过一个明确的方法来发现威胁的发生**

**缺点**

1. **BB84量子密钥协议的安全性取决于生成和处理单个光子的能力**
2. **必须随机地设置所发出的光子的极化状态。但计算机是有限状态机**
3. **存在长距离通信实现困难性**
4. **传输效率相对较低**

**第13章**

**五种安全机制**

* **І.网络接入安全**
* **П.网络域安全**
* **Ш.用户域安全**
* **Ⅳ.应用域安全**
* **V.安全的可视性和可配置性**

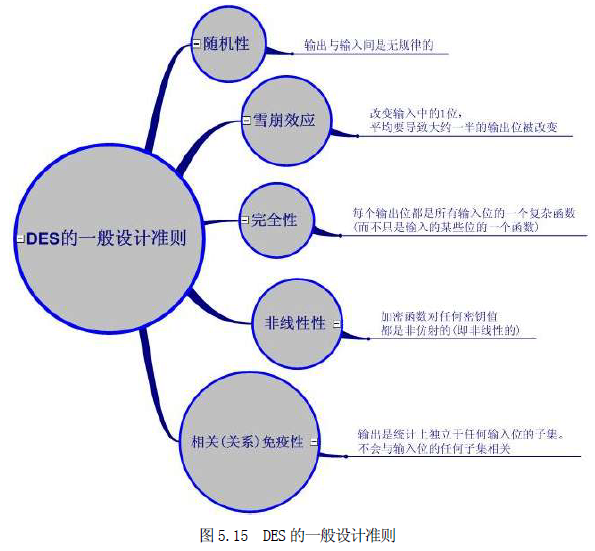
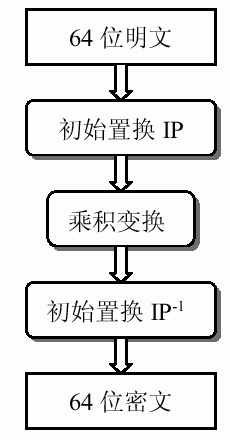
**安全攻击**

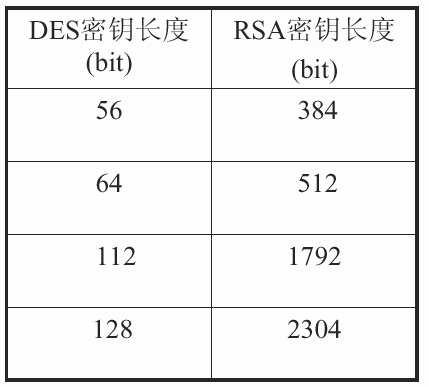
**窃听、略读、克隆和物理攻击、重放、屏蔽、失效**

**安全服务**

**访问控制、标签认证、消息加密**

DES加密：





**例子.通过同余式演算证明：**

**（1）560－1是56的倍数**

**（2）223－1是47的倍数。**

**解：**

**注意53=125≡13(mod56)**

**于是有56≡169≡1(mod56)**

**对同余式的两边同时升到10次幂，**

**即有56∣560-1。**

**同理, 注意到26=64≡17(mod47), 于是**

**223=(26)3·25=(26 · 26)26 · 25**

**≡289\*(17)\*(32) mod47**

**≡7\*17\*32 (mod47)**

**≡ 25\*32(mod47)**

**≡1(mod47)**

**于是有 47∣223-1**

**RSA的数字签名应用**

**数字签名方案：一个签名方案是由签署算法与验证算法两部分构成。可由五元关系组（M,A,K,S,V）来描述：**

**(1)M是由一切可能消息所构成的有限集合；**

**(2)A是一切可能的签名的有限集合；**

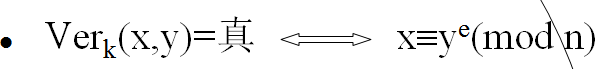
**(3)K为有限密钥空间，是一些可能密钥的有限集合；**

**(4)任意k ∈K，有签署算法Sigk ∈ S且有对应的验证算法Verk∈V,对每一个Sigk和Verk满足条件：任意一个**



**RSA的数字签名方案**

* **选取整数n=pq,　M=A=Zn**
* **定义密钥集合K={(n,e,p,q,d)}|n=pq,d\*e≡1(mod ϕ(n))}**
* **n和e为公钥；p,q,d为保密的（私钥）**
* **对x∈M, Bob要对x签名，取k∈K：**
* **Sigk(x)≡ xd(mod n)≡y(mod n)**



**签名消息的加密传递问题**

* **假设Alice想把签了名的消息加密送给Bob：对明文x，Alice计算对x的签名y=SigAlice(x)，然后用Bob的公钥加密函数eBob,算出z=eBob(x,y) ,Alice 将z传给Bob**
* **Bob收到z后，先解密：dBob(z)=dBobeBob(x,y)=(x,y)**
* **后检验：**
* **VerAlice(x,y)= 真？**
* **问题：若Alice首先对消息x进行加密,z=eBob(x),然后再签名， y=SigAlice(eBob(x)),结果如何呢？**
* **Alice 将（z,y)传给Bob，Bob先将z解密，获取x;然后用VerAlice检验关于x的加密签名y**
* **一个潜在问题：如果Oscar获得了这对（z,y)，他能用自己的签名来替代Alice的签名**
* **y′=SigOscar(eBob(x))**