第一讲

1.密码学的五个安全属性（目标）

**保密性：信息不泄露给非授权实体**

**完整性：未经授权不能篡改信息**

**实体认证性：实体本身被正确标识**

**不可否认性：用户不能在事后否认信息的生成行为**

**可用性：保障资源随时可提供服务**

2.对称密码体制和非对称密码体制的区别是什么

**对称(分组密码\流密码;消息鉴别码)** ,**非对称(公钥加密;数字签名)**

**对称密码：key1=key2，也称为私钥密码**

**非对称密码：key1≠key2，也称为公钥密码**

第二讲

1.举例说明古典密码体制体现下列技术的分别是哪个密码？

代换、置换、扩散、分组/填充

**（1）代换密码：代换是古典密码中 用到的最基本的处理技巧之一。所谓代换，就是将明文中的一个字母由其它字母、数字或符号替代的一种方法。又分为：凯撒密码、仿射密码、单表代换、多表代换（维吉尼亚）**

**（2）置换密码：是古典密码中用到的另一个最基本的处理技巧。将明文字符按照某种规律重新排列而形成密文的过程。比如：希尔密码**

**（3）扩散原理​：通过多表代换，使得单个明文字符对应多个密文字符（取决于密钥字母）。示例：希尔密码**

**（4）分组/填充。分组​：将明文分成双字母组，对每组独立加密。填充​：若明文长度为奇数，需添加填充字符（如‘X’）完成分组。密码示例：希尔密码**

2.维吉尼亚密码的惟密文分析都有哪些方法？

**统计攻击（频率攻击）、重合指数法、拟重合指数法**

3.惟密文分析的前提条件是什么？

**密文足够多、密码算法已经知道或可以推测、明文语言特征可识别、密码算法存在弱点、没有破坏明文的频率统计规律**

第三讲

1.完善保密的定义是什么？

**一个密码体制满足完善保密，当且仅当密文不泄露明文的任何信息。**

**密码系统（P,C,K,E,D）是完善保密（无条 件保密）的充分必要条件是H (P | C)=H (P) = 或 I (P, C) =0 。攻击者即使截获密文，也无法获得比已知明文分布更多的信息。**

2.计算安全的含义是什么？

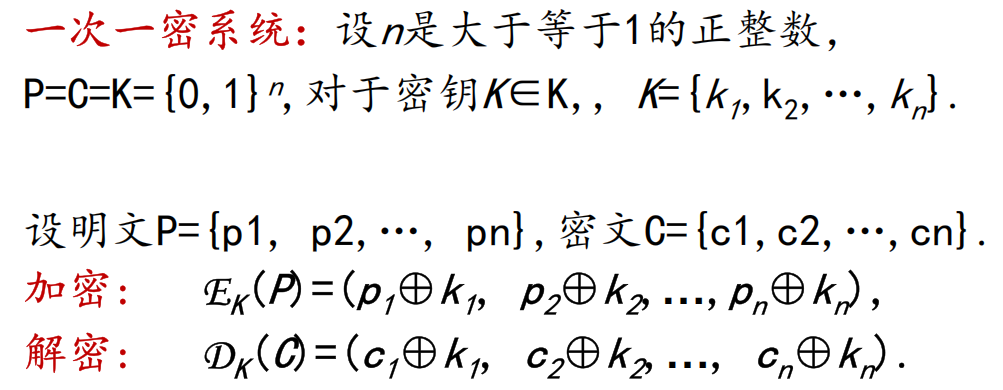
**当问题输入长度足够大，分析密码体制的算法的复杂度较大，可能的计算能力下，在保密的期间内可以保证算法不被攻破，这就是密码体制的计算安全性思想。**

3.实际安全的含义是什么？

**破解该密码系统的成本超过被加密信息本身的价值；**

**破译该密码系统的时间超过被加密信息的有效生命周期**

4.满足完善保密的密码体制是哪些算法？



第四讲

1.对称密码的五要素是什么？

**明文、密文、加密算法、解密算法、密钥**

2.分组密码的设计技术主要是什么？

**迭代结构：软、硬件实现节省了代码（硬件）资源，多次迭代有可能提高密码体制的安全性**

**混淆：明文/密钥和密文之间的关系复杂**

**扩散：明文/密钥的每一个比特都影响密文的每一个比特**

3.DES和AES的迭代结构分别是什么？

**DES：Feistel结构；AES：SPN结构**

4.2DES为什么不安全？

**中间相遇攻击，且2DES的密钥空间并未如预期扩大，反而能被高效破解。**

**攻击者已知​若干 (*P*,*C*) 明文-密文对。**

**正向计算​：对所有可能的 *K*1​，计算 *X*=*EK*1​​(*P*)，并存储 (*X*,*K*1​) 在表 *T* 中。**

**逆向计算​：对所有可能的 *K*2​，计算 *X*=*DK*2​​(*C*)，并检查 *X* 是否在表 *T* 中。**

**匹配成功​：若 *X* 匹配，则 (*K*1​,*K*2​) 即为正确密钥对。**

**​DES单次加密​：256次尝试（暴力破解）。**

**2DES预期​：256×256=2112（看似安全）。**

**中间相遇攻击​：仅需 256+256=257 次计算（比预期低得多）。**

5.为什么DES迭代的轮数比AES迭代的轮数多？

**（1）结构差异**​：

**DES（Feistel）每轮仅处理半块，需16轮交叉混淆。**

**AES（SPN）每轮全块并行处理，10轮即可达到强安全性。**

**（2）操作复杂度​：AES的列混合、行移位等操作提供更快扩散，减少所需轮数。**

**（3）密钥长度​：DES的56位密钥依赖多轮弥补弱点，AES的长密钥本身更安全。**

6.AES算法中承担扩散作用和混淆作用的函数分别是哪些？

**扩散：列混合、行移位**

**混淆：字节代换（非线性）、轮密钥加**

7.为什么ECB模式不能加密长消息？

**ECB（电子密码本）模式不能安全加密长消息，是因为它将消息分成独立加密的块，导致相同的明文块始终生成相同的密文块。这会暴露明文中的重复模式（如图像轮廓、文本结构），使攻击者能推断部分信息，且无法抵抗块重放或篡改攻击。因此，ECB仅适用于加密单个数据块，长消息应使用CBC、CTR等更安全的模式。**

8.说明分组模式和流模式的主要区别

**（1）​加密单位​：**

**分组模式​（如AES-CBC、AES-GCM）按固定长度（如128位）分组处理数据，需填充不足部分。**

**流模式​（如RC4、ChaCha20）逐比特或字节加密，无需填充，适合实时数据流。**

**（2）工作方式​：**

**分组模式依赖初始向量（IV）和反馈机制（如CBC的链式加密），增强安全性但可能引入延迟。**

**流模式通过密钥流（伪随机序列）与明文直接异或，速度快但需确保密钥流不重复。**

第五讲

1.为什么一次一密不在现实中使用？

**一次一密（OTP）​​在理论上具有无条件安全性​（只要密钥完全随机且仅使用一次），但在实际中极少使用，主要原因包括：**

**（1）密钥分发难题​：密钥长度必须与明文等长，且需安全传输给接收方（如物理交付），难以大规模应用（如互联网通信）。**

**（2）密钥管理复杂​：每次通信需生成并存储新密钥，长期使用会导致密钥量爆炸式增长（如1GB文件需1GB密钥）。**

**（3）密钥不可复用​：若密钥重复使用或泄露，OTP安全性完全崩溃（可通过密文异或破解明文）。**

**（4）无错误容忍性​：密钥或密文的单比特错误会导致解密结果完全错误，缺乏纠错机制。**

**（5）效率低下​：相比现代加密算法（如AES），OTP的密钥生成、存储和传输成本过高，不适合实时应用。**

2.流密码分为同步和自同步流密码，常用的是哪一种？

**常用的流密码是同步流密码**

**​效率与性能​：同步流密码通过独立密钥流加密（如计数器模式），无需依赖密文反馈，加解密速度快，适合高速通信（如TLS、视频流）。**

**无错误传播​：传输中若个别密文比特出错，仅影响对应明文比特，不会扩散到后续数据（自同步流密码会因反馈机制导致错误蔓延）。**

**安全性控制​：密钥流完全由密钥和初始向量（IV/nonce）生成，需确保IV不重复，但设计更简单（如ChaCha20的抗IV重用特性）。**

**​自同步流密码​（如CFB模式）因错误传播和性能限制，仅用于特殊场景（如信道稳定性差的传统系统）。**

3.硬件实现的流密码的主要技术是什么？

**（1）线性反馈移位寄存器（LFSR）​​：高效生成伪随机密钥流，通过反馈多项式实现长周期序列。**

**（2）非线性组合函数​：增强LFSR输出的安全性，防止线性攻击。在硬件中引入非线性逻辑门（如AND、OR）或S盒（如AES中的查表）。**

**​（3）并行处理架构​：通过流水线（Pipeline）​或多路复用（Multiplexing）​同时处理多个数据块，提升吞吐量（如CTR模式的并行加密）。**

4.m序列是什么？如何设计一个生成m序列的LFSR？

**（1）m序列是由线性反馈移位寄存器（LFSR）​生成的一种伪随机二进制序列**

**（2）设计步骤：**

**​①确定LFSR的阶数（n）​​：选择n位寄存器​（如4位LFSR可生成周期15的m序列）。**

**​②选择本原多项式：本原多项式决定了LFSR的反馈结构，确保序列周期最大化。**

**​示例​（4位LFSR）：**

**本原多项式：*x*4+*x*3+1（对应反馈位：第4位和第3位异或）。**

**反馈逻辑：*b*4​=*b*3​⊕*b*0​（寄存器右移，最高位由反馈计算）。**

**​③硬件实现​**

**​④验证周期​：初始化LFSR为非全零状态​（全零会导致序列停滞）。运行2*n*−1次后，检查是否回到初始状态。**

5.LFSR为什么不能直接用来生成密钥序列？

**（1）线性可预测性​：LFSR的输出由线性反馈多项式决定，攻击者只需截获2n位连续输出​（n为寄存器位数），即可通过Berlekamp-Massey算法逆向推导出反馈结构，完全破解密钥流。**

**（2）统计缺陷​：生成的m序列虽然具有伪随机性，但高阶统计特征​（如连续比特模式）仍存在规律，易受相关性攻击（如快速相关攻击）。**

**（3）周期限制​：即使采用最大周期（2n−1），在加密长消息时密钥流可能重复，导致密钥重用漏洞​（如两次异或相同密钥流会泄露明文差异）。**

**（4）缺乏非线性混淆​：纯线性运算（异或、移位）无法隐藏密钥与密文的关系，无法抵抗已知明文攻击。**

**（5）无扩散性​：单个密钥比特错误或泄露不影响其他部分，攻击者可局部破解，不符合雪崩效应的安全要求。**

6.如何基于LFSR设计安全的流密码？

**（1）​多LFSR非线性组合​：并行运行多个LFSR，通过非线性函数​（如多数表决、AND/OR门）混合输出，破坏线性关系。**

**（2）引入非线性滤波函数​：将单个LFSR的输出通过非线性布尔函数​（如S盒、多项式函数）过滤，提高复杂度。**

**（3）​钟控机制：动态控制LFSR的移位节奏（如停走生成器、收缩生成器），使输出序列非线性化。**

**（4）增加记忆单元与反馈复杂性​：在LFSR中引入非线性反馈​（如使用乘积项）或外部记忆状态**

7.为什么流密码的随机数要不可预测且足够长？

**（1）​不可预测性**

**防止密钥流破解​：若攻击者能通过已知的密钥流片段推测后续输出（如LFSR的线性缺陷），则可解密全部密文。**

**抵抗已知明文攻击​：若密钥流可预测，攻击者可通过明文-密文对异或恢复密钥流，进而解密其他消息。**

**（2）足够长的周期**

**​避免密钥流重复​：短周期会导致密钥流循环使用，若同一密钥流加密不同明文（如*C*1​=*M*1​⊕*K*，*C*2​=*M*2​⊕*K*），则异或两密文会泄露*M*1​⊕*M*2​。**

**适应长消息加密​：流密码需支持大文件或持续通信（如视频流），密钥流周期必须远大于明文长度。**

8.保密体制的攻击者按照目的分为哪些？

**​8. 保密体制的攻击者按照目的分为哪些？​​**

**（1）​被动攻击：仅窃听或截获密文，不干扰通信过程（如网络嗅探），唯密文攻击。**

**（2）主动攻击：篡改、伪造或重放数据，破坏完整性或真实性，如中间人攻击）。**

**（3）选择明文攻击：诱使加密系统加密特定明文，分析密文以推断密钥。**

**（4）选择密文攻击：通过解密特定密文获取密钥或明文信息。**

**（5）已知明文攻击​​：攻击者已知部分明文-密文对（如破解历史加密数据）。**

9.满足什么条件的保密体制是安全的？

**​9. 满足什么条件的保密体制是安全的？​​**

**（1）机密性​：即使攻击者截获密文，也无法推断明文或密钥的任何有效信息。加密算法需抵抗唯密文攻击和已知明文攻击​（如AES满足此条件）。**

**（2）完整性：任何对密文的篡改均可被检测（如通过MAC或哈希验证）。**

**（3）​不可预测性：密钥流或密文必须呈现统计随机性，无法通过历史数据预测未来输出。**

**（4）​抗密钥泄露：即使长期密钥泄露，历史会话仍保持安全（如Diffie-Hellman密钥交换）。**

**（5）算法公开性（Kerckhoffs原则）​​：安全性仅依赖密钥保密，而非算法保密（如RSA、AES的设计公开）。**

**（6）计算安全性：在有限时间和资源下，破解成本远高于收益（如暴力破解AES-256需22562^{256}2256次操作）。**

​

第六讲

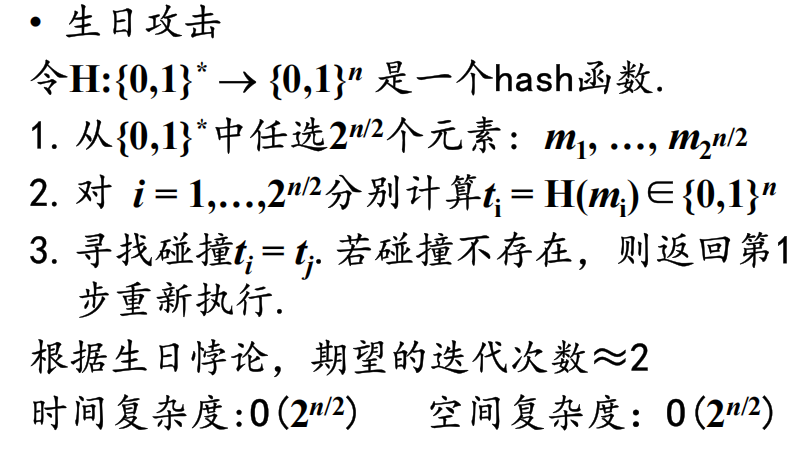
1.Hash函数的三个安全要求是什么？

**（1）单向性（抗原像）：对干任意给定的消息，计算其哈希值 容易. 但是，对于给定的哈希值h，要找到M使得H(M)＝h 在计算上是不可行的.**

**（2）弱抗碰撞（抗二次原像）：对于给定的消息M1，要发现另一个消息M2，满足H(M1)＝H(M2)在计算上是不可行的.**

**（3）强抗碰撞：找任意一对不同的消息M1，M2，使H(M1)＝H(M2)在计算上是不可行的**

2.生日攻击用于求碰撞的复杂度是多少？



3.目前推荐使用的SHA-2（或SM3）使用的是什么迭代结构？压缩函数又是什么结构？

**​​（1）迭代结构​：SHA-2（如SHA-256）和SM3均采用MD迭代结构**

**具体流程：**

**​①消息填充：将输入消息填充至长度满足 length≡448mod 512，并附加64位消息长度。**

**②分块处理：将填充后的消息分割为固定大小的块（SHA-256为512位，SM3为512位）。**

**③迭代压缩​：初始化哈希值（IV），逐块通过压缩函数处理，前一块的输出作为下一块的输入（链式反馈）。**

**④最终输出​：最后一轮压缩后的状态即为哈希值（SHA-256输出256位，SM3输出256位）。**

**​​（2）压缩函数结构​：SHA-256的压缩函数基于D-M结构，核心步骤如下：**

**①消息扩展：将512位输入块扩展为64个32位字（Wt），通过移位和异或增强扩散。**

**②状态更新​：8个32位工作变量（a,b,c,d,e,f,g,h）经过64轮非线性运算（含加法、移位、逻辑函数）。每轮结合常量Kt和扩展消息Wt​。**

**③反馈叠加​：最终将压缩输出与初始状态（上一块哈希值）相加（模232）。**

**​SM3的压缩函数类似但更复杂：使用64轮迭代，每轮结合消息扩展字 Wj和 Wj和Wj′​（双重扩散）。非线性逻辑函数（FF/GG）和置换运算（P0/P1​）增强混淆**

4.消息鉴别码用于保护消息的什么属性？

**（1）完整性​：确保消息在传输或存储过程中未被篡改。MAC通过哈希或加密生成固定长度的标签，接收方通过重新计算并比对标签验证数据是否一致。**

**（2）真实性：验证消息确实来自声称的发送方（即未被第三方伪造）。MAC的生成依赖共享密钥​（对称密钥），只有合法通信双方能生成/验证有效标签。**

5.完整性保护角度来说，hash函数和消息鉴别码的区别是什么？

| **​特性​** | **​Hash函数（如SHA-256）​​** | **​消息鉴别码（如HMAC）​​** |
| --- | --- | --- |
| ​**保护目标**​ | 数据完整性（防篡改） | 数据完整性 + 真实性（防篡改且验证发送方） |
| ​**密钥依赖**​ | 无密钥，公开计算 | 依赖共享密钥（对称密钥） |
| ​**抗伪造能力**​ | 仅防偶然修改，无法抵抗恶意篡改（无身份绑定） | 抵抗恶意篡改（需密钥才能生成合法MAC） |
| ​**安全性场景**​ | 适用于非对抗环境（如文件校验、密码存储） | 适用于对抗环境（如网络通信、金融交易） |
| ​**攻击风险**​ | 若攻击者修改数据并重新计算Hash，无法检测 | 无密钥则无法生成有效MAC，篡改可被发现 |

6.消息鉴别码的攻击者的攻击目标分为哪些？

**（1）攻击者资源**

**被动攻击：已知消息攻击。攻击者通过窃听等手段，获取一些消息和用同一个密钥认证这些消息所得的认证码**

**主动攻击：选择消息攻击。攻击者通过选取一些消息，发送给oracle（MAC设备）得到相应的认证码**

**（2）攻击目的**

**密钥恢复攻击：攻击者找到合法用户的密钥*k*.**

**伪造攻击：攻击者在未知密钥*k*的情况下，伪造一个未经过认证的(*m*,*t*)对.**

**选择性伪造：如果攻击者能够对由他选择的消息*m\** 进行伪造(*m\**,*t\**) ，那么这种伪造攻击称为选择性伪造攻击**

**存在性伪造：如果攻击者只能够对一个不由他控制 的消息进行伪造，那么这种伪造攻击称为存在性伪造攻击**

7.满足什么条件的消息鉴别码是安全的？

**（1）不可伪造性：条件​：即使攻击者已知大量（消息, MAC）对，也无法伪造新消息的有效MAC。需抵抗选择明文攻击（CMA）​，即攻击者即使能获取任意消息的MAC，仍无法伪造未查询过的消息的MAC。**

**（2）计算安全性：在多项式时间内，伪造MAC的成功概率可忽略**

**（3）密钥保密性：MAC密钥不可泄露，否则攻击者可任意生成合法MAC​**

**（4）抗重放攻击：需结合序列号或时间戳，否则MAC本身无法防止旧消息重放**

**（5）算法鲁棒性​：即使部分消息或MAC被篡改，验证失败概率应为1**

8.CBC-MAC的输出处理和截断有什么作用？

**（1）输出处理的作用​：​防止长度扩展攻击​（对最后一个密文块进行密钥二次加密​（如AES加密）或使用固定长度输出）、增强不可预测性​（通过截断输出隐藏部分内部状态）、标准化输出长度​（某些应用要求固定长度的MAC）**

**​​（2）截断的具体实现​：截断位置​通常保留CBC链的最高有效位（MSB）​或最低有效位（LSB）​​**

**​安全性影响​：若截断过短（如32位），可能降低安全性（暴力破解风险）。需确保剩余位数满足安全需求（如64位抗264攻击）。**

9.HMAC的设计中，如何防止消息延展攻击的？

​**（1）密钥预处理​：若密钥KKK短于哈希函数块长度（如SHA-256的512位），填充至块长度（补零）；若密钥过长，则先哈希压缩KKK再填充。**

**​（2）双重哈希结构：攻击者即使知道InnerHash，也无法反向推导或扩展消息，因外层哈希的密钥K⊕opad未知。**

**​（3）哈希函数的单向性​：哈希函数HHH的抗碰撞性和单向性，确保无法从 HMAC逆推出KKK或中间状态。**

**​（4）对比原始哈希的长度扩展漏洞​：双重哈希结构彻底阻断了此类扩展，因攻击者无法构造合法的InnerHash输入。**

10.如何保障保密体制达到选择密文攻击下的安全性？

**​（1）加密与认证结合：使用同时提供机密性和完整性的算法，确保密文被篡改时解密会失败**

**​（2）不可延展性：采用CCA安全的加密方案，攻击者无法通过修改密文生成另一有效密文**

**​（3）随机化加密：每次加密引入随机数​，使得相同明文加密后生成不同密文，防止攻击者通过重复提交密文推断密钥。**

**​（4）密钥分离原则：加密与认证使用独立密钥​​，避免密钥重用导致CCA漏洞**

**​（5）安全填充方案：采用抗CCA的填充，避免填充Oracle攻击**

**​（6）拒绝无效密文​​：解密时严格校验密文格式、MAC标签或填充有效性，立即丢弃非法输入，阻断攻击者通过错误响应获取信息的渠道。**

第七讲

1.非对称密码作为对称密码的补充，可以解决什么问题？

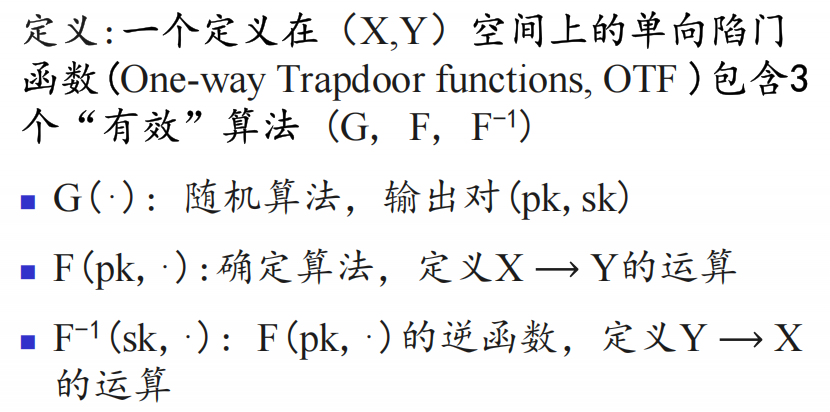
**（1）密钥分发难题。公钥可公开分发（如通过证书），私钥严格保密，无需预先共享密钥（如RSA密钥交换）。**

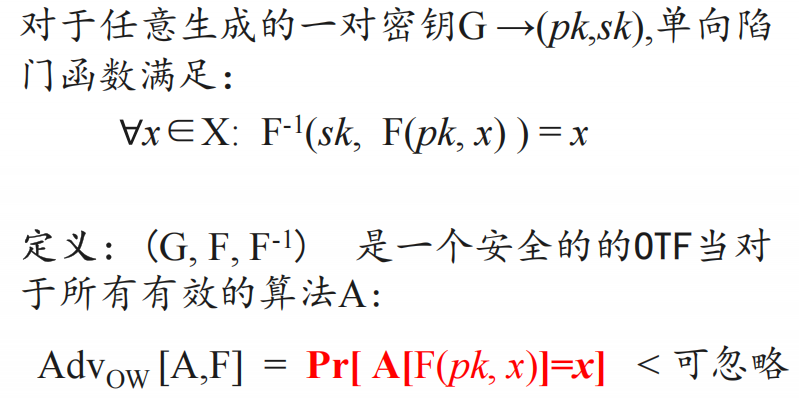
**​（2）数字签名与身份认证：对称密码无法实现不可否认性（如AES无法证明消息来源）。非对称用私钥签名、公钥验证（如ECDSA），确保消息真实性和发送方身份（如SSL证书签名）。**

**​（3）多用户安全通信：对称密码*N*个用户需 *O*(*N*2)个密钥，管理复杂度高。非对称每个用户仅需一对公私钥，公钥目录即可支持任意双方通信。**

**​（4）前向安全性：​对称密码长期密钥泄露会导致历史通信被解密。非对称通过临时密钥交换实现前向安全，即使长期私钥泄露，会话密钥仍安全。**

2.给出单向陷门函数的定义？

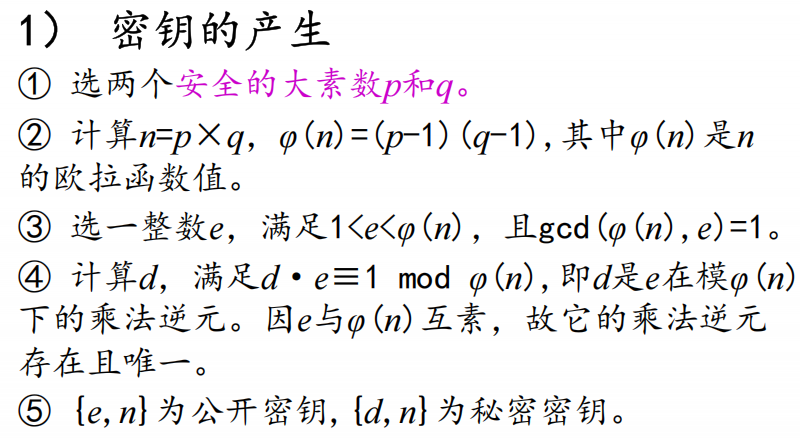


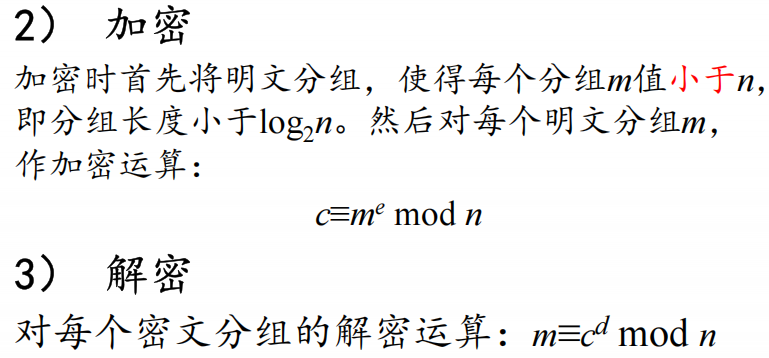


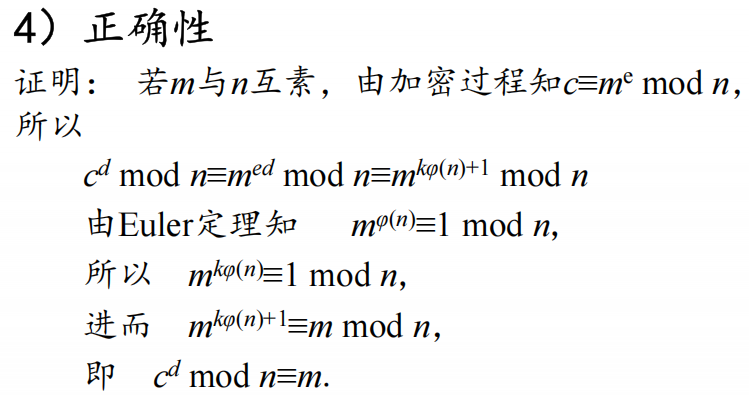
3.后量子密码提出的意义是什么？

**抵抗量子计算攻击、保障长期数据安全、维护密码生态系统稳定、推动新型数学理论应用​、国家战略与产业安全**

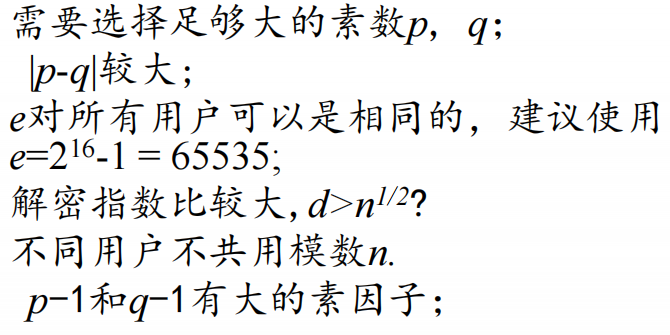
4.给出RSA单向陷门函数的基本流程。



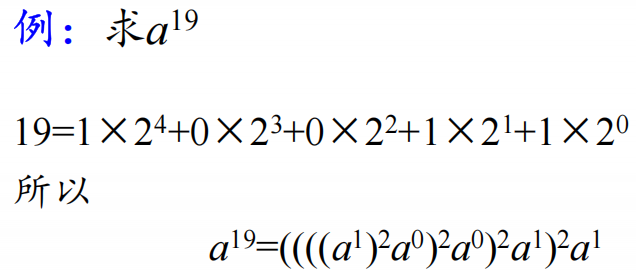




5.RSA的参数选取有哪些安全性要求？



6.给出用平方-乘方法求a^13的表达式。



7.为什么RSA单向陷门函数不能直接应用于加密数据？

**（1）确定性加密导致安全性缺陷​​：RSA加密是确定性的​，易受重放攻击或字典攻击。**

**（2）​缺乏语义安全性：攻击者可通过密文推断明文部分信息，违背现代加密的不可区分性要求。**

**​（3）明文空间限制与填充需求​：RSA仅能加密小于模数 *N* 的整数，且需填充以扩展明文空间并随机化输入。若直接加密短明文，暴露数学结构。**

**​（4）性能瓶颈​：RSA计算复杂度高，直接加密大数据效率极低。**

8.ElGamal和SM2基于的困难问题分别是什么？

**（1）ElGamal加密方案的安全性基于离散对数问题（DLP）​，即在有限域中计算*gx* mod *p*的逆运算困难。**

**（2）SM2作为中国商用密码标准，其安全性基于椭圆曲线离散对数问题，即在椭圆曲线群上求解*xG*=*P*中的标量*x*困难。相较于传统DLP，ECDLP在相同密钥长度下提供更高安全性。**

9.椭圆曲线密码体制相比RSA和ElGamal的优点是什么？

**（1）更高的安全性​：在相同安全强度下，ECC的密钥长度远小于RSA，破解ECC所需的计算量更大。**

**（2）更快的运算速度​：ECC的加密、解密和签名生成速度更快。**

**（3）更低的存储和带宽需求​：短密钥节省存储空间，减少传输数据量。**

**（4）​更强的抗量子计算潜力​：其密钥长度扩展空间优于RSA。**

10.解释DL/ECIES(IEEE 1363a-2004) 标准加密的基本思想？

**（1）密钥封装：发送方使用接收方的公钥​（DL公钥 *gx*或EC公钥 *xG*）生成临时共享秘密​（如 *K*=(*gx*)*k* 或 *K*=*k*⋅(*xG*)），并派生对称密钥​。**

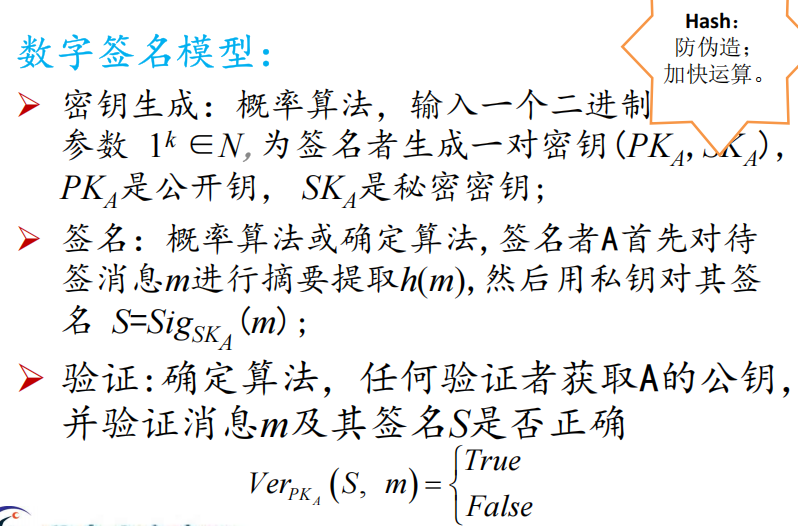
**（2）数据封装：用派生的对称密钥加密明文，生成密文 *C*。**

**（3）认证与完整性​：可选地附加MAC标签​（如HMAC）或通过认证加密模式确保密文完整性。**

**（4）传输内容​：发送方将临时公钥参数（如 *gk*或 *kG*）与密文 *C*（及MAC）一并传输。**

第八讲

1.简述数字签名算法模型



2.简述数字签名的攻击（安全）模型

**（1）攻击者资源：**

**①惟密钥攻击：攻击者只有用户的公开密钥**

**②已知消息攻击：攻击者拥有一些消息的合法签名，但是消息不由他选择**

**③选择消息攻击：攻击者可以自由选择消息并获取 消息相应的签名**

**（2）攻击结果：**

**①完全破译：攻击者恢复出用户的私有密钥**

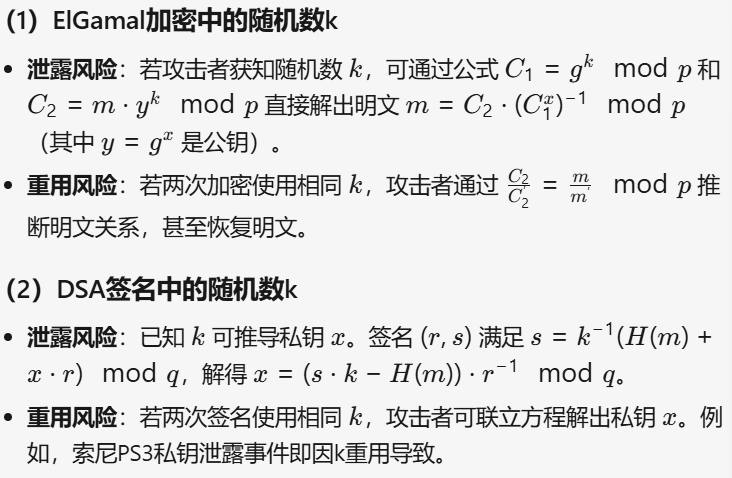
**②选择性伪造：攻击者可以对一个自己选取的消息伪造签名**

**③存在性伪造：攻击者可以生成一些消息的签名，但在伪造前对该消息一无所知**

3.Hash在数字签名算法中的作用是什么？

**防伪造，加快运算**

4.ElGamal加密和DSA签名中的随机数k不能泄露和重用的原因分别是什么？



第九讲

1.简述Kerckhoffs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，它也应是安全的**

2.密钥管理的环节都有哪些？

**密钥生成、密钥建立、密钥存储、密钥使用、密钥备份、密钥恢复/更新、密钥撤销、密钥更新、密钥存档、密钥销毁**

3.举例说明如何分层管理密钥？为什么密钥要分层分类管理？

**（1）举例：**

**会话密钥：在一次通信或数据交换中，用户之间所使用的密钥，是由通信用户之间进行协商得到的。它一般是动态地、仅在需要进行会话数据加密时产生，并在使用完毕后立即进行清除掉的，也称为数据加密密钥。**

**密钥加密密钥：一般是用来对传输的会话密钥进行加密时采用的密钥，又称为二级密钥。密钥加密密钥所保护的对象是实际用来保护通信或文件数据的会话密钥。**

**主密钥：对应于层次化密钥结构中的最高层次，它是对密钥加密密钥进行加密的密钥，主密钥应受到严格的保护。**

**（2）①最小化泄露影响​：若DEK泄露，仅需更换该密钥，无需重置整个系统。**

**​②提升安全性​：主密钥离线存储，减少暴露风险；临时密钥频繁更换，限制攻击窗口。**

**​③适应不同生命周期​：主密钥长期不变，会话密钥即时销毁，符合业务需求。**

**​④满足合规要求​**

4.密钥分配和密钥协商的区别是什么？

**​4. 密钥分配与密钥协商的区别​**

| **​特性​** | **​密钥分配​** | **​密钥协商​** |
| --- | --- | --- |
| ​**生成方式**​ | 单方/第三方生成 | 双方共同计算生成 |
| ​**交互性**​ | 单向传输（无需双方交互） | 需双向交互（如交换公钥参数） |
| ​**依赖方**​ | 可能需要可信第三方（KDC） | 完全去中心化 |
| ​**前向安全**​ | 通常不具备（除非动态分配） | 天然支持（如DH临时密钥） |

5.利用对称密码体制分配密钥的前提条件是什么？

**（1）预共享密钥：通信双方必须预先安全共享一个主密钥。**

**（2）​安全信道保障​：密钥分配过程需通过防窃听、防篡改的信道**

**（3）​密钥唯一性与时效性​：分配的密钥必须一次性使用或短期有效，避免长期重用导致泄露风险。**

**（4）可信第三方**

6.举例说明如何实施重放攻击？

**（1）网络认证场景​攻击过程​：用户A登录系统时发送认证请求（如密码哈希或令牌）。攻击者截获该请求，​不破解内容，直接重复发送至服务器。服务器误认为合法请求，允许攻击者冒充用户A。比如​Wi-Fi认证​**

**（2）金融交易场景​攻击过程​：用户B发起转账请求。攻击者截获该请求并多次重放，导致用户B账户被重复扣款。比如比特币交易​**

7.举例说明如何使密钥分配协议达到新鲜性和一致性。

**（1）新鲜性：确保密钥是最新生成且未被重放，常用时间戳（通信双方验证消息时间在有效窗口内）、​随机数（每次会话生成唯一随机数）、​序列号​（每次密钥分配递增序列号，拒绝重复或乱序请求）**

**​​（2）一致性：确保通信双方最终持有相同的密钥，常用密钥确认（通过MAC或哈希验证密钥一致性）、双向认证​（双方交换签名或加密的挑战值）**

8.DH密钥协商协议的中间人攻击成功的原因是什么？怎样防止该攻击？

**​​（1）中间人攻击成功的原因​：DH协议本身不验证通信方身份，导致攻击者可拦截并篡改交换的公钥参数：**

**拦截公钥​：攻击者截获Alice发送的 g amod p，替换为 gm mod p（m为攻击者私钥），再转发给Bob。**

**伪造共享密钥​：Alice与攻击者协商出 K1​=gam mod p；Bob与攻击者协商出 K2​=gbm mod p。**

**双向解密​：攻击者用 K1​ 解密Alice的消息，用 K2​ 解密Bob的消息。**

**​根本原因​：DH协议缺乏身份认证机制，无法确认公钥来源的真实性。**

**​​（2）防御措施​：**

**数字签名认证​：双方对DH公钥参数签名，接收方验证签名真实性。**

**​公钥基础设施（PKI）​​：依赖CA签发的证书绑定公钥与身份。**

**​预共享密钥（PSK）​​：预先共享密钥用于认证DH交换。**

**在线可信第三方（STS协议）​​：引入在线签名服务实时认证公钥。**

**口令认证（PAKE）​​：结合弱口令与DH（如SRP协议），防止离线破解。**

9.PKI管理公钥的优点是什么？如何实现密钥和持有者身份绑定？

**公钥基础设施（PKI）以公钥技术为基础，将个人、组织、设备的标识信息与各自的公钥捆绑在一起，为用户建立起一个安全、可信的网络运行环境，使陌生用户可以在多种应用环境下方便地使用加密和数字签名技术，在互联网上验证用户的身份，从而保证了互联网上所传输信息的真实性、完整性、机密性和不可否认性。**

10.简要说明RA和CA的主要职责？

**（1）RA：主体注册证书的个人认证、确定主体所提供信息的有效性、对被请求证书属性确定主体的权利、认证机构代表主体开始注册过程、为识别身份的目的分配名字、在注册初始化和证书获得阶段产生共享秘密、产生公私钥对、在需要撤销时报告密钥泄露或终止事件、开始密钥恢复处理。**

**（2）CA：确定是否接受最终用户数字证书的申请、验证最终用户的公钥是否合法、向申请者颁发、拒绝颁发数字证书、接受、处理最终用户的数字证书更新请求、接受最终用户数字证书的查询、撤销、产生和发布证书注销列表（CRL）、数字证书的归档、密钥归档、历史数据归档。**

11.从个人角度，如何保障口令安全？

**​​（1）创建强口令​：长度与复杂度​、避免规律性​**

**​​（2）口令管理策略​：唯一性​（每个账户使用独立口令）、定期更新、​禁用自动保存**

**​​（3）使用密码管理器​：加密存储​（通过主密码保护）、双重验证​（主密码+生物识别（指纹/面部）解锁管理器）**

**​​（4）防范社会工程学​：不透露口令​、警惕钓鱼网站**

**​​（5）启用多因素认证（MFA）​​：二次验证​、​生物识别​**

**​​（6）应急措施​：密保问题​、​备用邮箱/手机​**