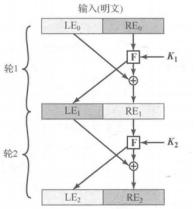
第一章知识：计算机安全、网络安全、因特网安全。***OSI 安全架构***：框架，系统的定义了安全需求以及以实现这些需求的方法为特征。安全攻击安全服务安全机制。***信息安全***：信息+系统安全（保护硬件、软件、网络、数据）***X.800 安全服务***：数据机密性【加密】、完整性【哈希】、实体认证、消息认证【MAC】、不可抵赖性【公私钥】、访问控制、可用性 ***安全攻击***：被动攻击/预防（监听和侦测，信息内容的泄露和流量分析目标是获取信息）、主动攻击/检测恢复难以预防（对数据流进行修改和伪造数据流，伪装、重放、消息修改和拒绝服务）***安全服务***：X.800 在开放系统中，为系统或数据传输提供足够安全的协议层服务。RFC4949 安全服务是一直有系统提供的对系统资源进行特殊保护的处理或通信服务 ***安全机制***：特定的协议层实现（加密、签名、数据完整性、认证、流量填充）、普遍的安全机制（可信功能、安全标签、事件检测、安全审计跟踪、安全恢复）。***设计安全服务***：设计一个攻击者不能攻破的安全相关变换的算法。产生双方所使用的秘密信息。设计分配和共享秘密信息的方法。指明通信协议。

Table 1.4 Relationship Between Security Services and Mechanisms

SERVICE \ MECHANISM	Encipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

第三章知识传统加密技术：*对称密码模型*：明文、加密算法、密钥、密文、解密算法。 ***密码算法这两个基本函数***：代替和置换 ***传统密码的安全使用要求***：加密算法必须足够强。密钥安全分发。***密码编码学三个独立的特征***：转换明文为密文的运算类型（代替、置换、乘积），密钥数（对称加密，非对称加密），处理明文方法（分组，流加密）***密码分析学和穷举攻击***：恢复使用的密钥而不是仅仅恢复出单个密文对应的明文。【暴力 or 数学分析】***密码分析学攻击***：唯密文攻击、已知明文攻击、选择明文攻击、选择密文攻击、选择文本攻击。***无条件安全***：无论又多少可使用的密文，都不足以唯一的确定密文锁对应的明文。除了一次一密外都不是无条件安全。***计算安全***：破译密码的代价超出密文信息的价值；破译密码的时间超出密文信息的有效生命期。***代替技术***：***Caesar 密码***，对字母表中的每个字母，用它之后的第 n 个字母来代替,密钥空间 25，不安全容易被穷举攻击。***单表代替密码***，密钥空间 26！可以抵挡穷举攻击，但还是较容易被攻破，因为它带有原始字母使用频率的一些统计学特征。***多表代替加密***，在明文消息中采用不同的单表代替，维吉尼亚密码，每一个代替表是对明文字母表移位 0~25 次后得到的代替单表，字母出现的频率信息被屏蔽了，不过并非所有的明文结构信息都隐蔽了（猜测密钥词的长度，一旦猜测出来就可以转为单表进行密码分析）。***置换技术***：***栅栏技术***，按照对角线的顺序写出明文，按行的顺序读出作为密文。更复杂的方案是把消息一行一行地写出矩形块，然后按列读出，但是把列次序打乱。列的次序就是算法的密钥。单纯的置换密码有着与原始明文相同的字母频率特征而易被识别。置换密码：改变明文中字母的顺序，从没有密钥发展为有密钥。***转轮机***：转轮机包括一组相互独立的旋转圆筒；快速转子，中速转子，慢速转子，每个圆筒有 26 个输入引脚和 26 个输出引脚。内部连线使每一个输入仅同唯一一个输出连接。***一次一密（One time pad）***：使用与消息一样长且无重复的随机密钥来加密信息且密钥只对一个消息进行加解密，之后丢弃不用。两个难点：产生大规模随机密钥有困难，密钥的分配和保护挑战。***隐写术的缺点***：需要许多额外的付出来隐藏 i 相对较少的信息。一旦被破解，整个方案就毫无价值。

第四章分组密码和数据加密标准：*流密码与分组密码*：流密码每次加密数据流的一位或一个字节，两个用户需要共享生成密钥，则各自可以生产密钥流。分组密码是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。两个用户共享一个对称加密密钥。***Feistel 密码结构***：使用乘积密码的概念来逼近理想分组密码。交替地使用代替和置换。代替，每个明文元素或元素组被唯一地替换为相应的密文元素或元素组。置换，明文元素的序列被替换为该序列的一个置换。***扩散***：尽可能地使明文和密文间的统计关系变得复杂。***混淆***：尽可能使密文和加密密钥间的统计关系更加复杂，可以使用复杂的代替算法实现。***Feistel 结构参数和特征***：分组长度、密钥长度、迭代轮数、子密钥产生算法、轮函数。***Feistel 解密算法***：本质上与加密过程一致，密文作为算法的输入但是逆序使用子密钥，因此不需要分别实现加密和解密两个算法。轮函数不需要是可逆的，通过相同数据异或抵消掉轮函数产生的影响。***数据加密标准（DES）***：采用 64 位分组长度和 56 位密钥长度（64 位，8 位奇偶校验码）。将 64 位的输入经过一系列变换得到 64 位的输出。解密使用了相同步骤和序相反的子密钥。***DES 加密***：首先 64 位明文经过初始置换 IP。然后进行 16 轮的置换和代替。最后一轮迭代输出有 64 位。然后 32 位互换产生预输出，最后预输出再被与初始置换 IP 互逆的置换作用产生 64 位密文。每轮结构：轮函数 F 接从受 32 位的 R 和 48 位的 K，使用 E 盒扩展 R 为 48 位，与 K 进行 XOR，然后用 S 盒产生 32 位数据（非线性），再将这 32 位数据经过 P 盒进行置换。***雪崩效应***：明文的某一位发生变化会导致密文的很多位发生变化。***DES 的强度***：56 位密钥共有 2^56 种可能，穷举攻击不切实际。***双重 DES***：加密 C=E(K2,E(K1,P))，解密 P=(K1,D(K2,C))。2DES 多对应的映射不能为单 DES 所定义。***中间相遇攻击***：对于 2DES，其付出的是 2^56 数量级，比攻击单 DES 所需的 2^55 数量级多不了多少。***使用两个密钥的 3DES***：C=E(K1,D(K2,E(K1,P)))，P=D(K1,E(K2,D(K1,C)))。***使用三个密钥的 3DES***：C=E(K3,D(K2,E(K1,P)))，P=D(K1,E(K2,D(K3,C)))，当 K3=K2 或 K1=K2 就兼容单 DES，使用 EDE 的结构就是为了代码的兼容性。



第 6 章 AES：有限域满足随机映射的特点。***AES 总体结构***：明文分组长度为 128 位 16 字节组成一个 4×4 的状态数组，密钥长度可以为 16 字节，24 字节或者 32 字节。AES 结构不是一个 Feistel 结构。在每一轮都使用代替和混淆将整个数据分组作为一个单一的矩阵处理。除最后一轮外，每轮由字节代替、行移位、列混淆和轮密钥加四个阶段组成。轮密钥加实质上是一种 Vermam 密码形式，另外三个阶段一起提供了混淆、扩散以及非线性功能。同大多数分组密码一样，解密算法按逆序方式利用了扩展密钥。然而，AES 的解密算法和加密算法并不一样。加密和解密过程的最后一轮均包含三个阶段。Rijndael 使用的密钥和区块长度均可以是 128，192 或 256 比特。AES 不等于“Rijndael”，AES 是 Rigndael 的子集。***字节代替变换***：正向字节代替是一个简单的查表操作。构建 S 盒，对每个{xy}计算在有限域 GF(2^n)中的逆，然后对 S 盒的每个字节的每个位做一个不知道为什么的变换。S 和必须是可逆的，即逆 S[S(a)]=a，然而 s[a]!=逆 S[a]，在这个意义上 S 盒不是自逆的。***行移位变换***：正向行移位变换。状态的第一行保持不变。状态的第二行循环左移一个字节，状态的第三行循环左移两个字节以此类推。逆向行移位变换将状态中的后三行执行相反方向的移位操作。***列混淆变换***：一个矩阵乘数据矩阵，矩阵的系数是基于码字间有最大距离的线性编码，这使得在每列的所有字节中有良好的混淆性。***轮密钥加变换***：128 位状态按位与 128 位的轮密钥异或。***AES 密钥扩展***：AES 密钥扩展算法的输入值是 4 个字，输出是一个 44 字组成的一维线性数组。***AES 安全性分析***：雪崩效应比 DES 效果好

第 7 章分组加密的工作模式：***电码本模式（ECB）***：一次处理一组明文块，每次使用相同的密钥加密。应用于单个数据的安全传输。使用加密和解密算法。***密文分组连接（CBC）***：加密算法的输入是上一个密文组和下一个明文组的异或。面向分组的通用传输。使用加密和解密算法。***密文反馈（CFB）***：一次处理 s 位，上一块密文作为加密算法啊的输入，产生的伪随机数输出与明文异或作为下一单元的密文。面向数据流的通用传输。使用加密算法。***输出反馈（OFB）***：与 CFB 类似，加密算法的输入是上一次加密的输出，且使用整个分组。用于噪声信道上的数据流传输。使用加密算法。***计数器模式（CTR）***：每个明文分组与一个经过加密的计数器相异或。对每个后续分组计数器递增。用于面向分组的通用传输。使用加密算法。

第 8 章伪随机数的产生和流密码：*随机数序列要求*：随机性（分布均匀性，独立性）、不可预测性（不能够从先前的随机数推导出后面的随机数）***TRNG***：把一个随机的源作为输入，产生随机的二元输出。可能会产生不平衡的二元序列。***PRNG***：取一个固定值作为种子输入，用一个确定性的算法产生位输出序列。要求，随机性、不可预测性。种子必须不可预测且必须是随机数或伪随机数。算法设计：特意构造的算法（RC4），基于现有密码算法的算法（对称分组密码，非对称密码，Hash 函数和消息认证码）***PRF***：伪随机函数，产生固定长度的伪随机位串，与 PRNG 的区别是产生位数量不同。***伪随机数发生器***：线性同余发生器，BBS 发生器，使用分组密码工作模式的 PRNG（两种模式 CTR 和 OFB），ANSI X9.17 伪随机数发生器，NIST CTR_DRBG。***流密码***：按位进行加密，由 PRNG 生成流密钥，不要重用流密钥。***RC4***：可变密钥长度、面向字节操作的流密码。该算法以随机置换作为基础。***随机数应用：***认证时变值、会话密钥、RSA 算法中的随机数、流密码。

第 9 章公钥密码学与 RSA：公钥算法是基于数学函数即为单向陷门函数，公钥密码是非对称的，它使用两个独立的密钥。公钥密码体制成分：明文、加解密算法、公私钥。***公钥和私钥的区别***：私钥是私有的只有自己知道。公钥所有人都知道。私钥签名公钥验证。公钥加密私钥解密。***公钥密码体制的应用***：加密/解密、

签名、密钥交换，同时满足的只有 rsa 和 ecc。dss 满足签名，DH 满足交换。***公钥密码的要求***：产生一对密钥计算上是容易的。加密是容易的。解密是容易的。公钥不能推出私钥。公钥和密文不能推出明文。加密和解密顺序可交换。***公钥密码安全分析***：易受穷举攻击，使用长密钥。为了实现加解密，密钥又必须足够短。在实际提出的密钥长度确实可以抗穷举攻击，但是它也使得加/解密速度变慢，所以公钥密码目前仅限于密钥管理和签名中。还一种公钥体制中特有的攻击是穷举消息攻击。例如用公钥对 56 位 DES 密钥加密，可以对 56 位密钥进行穷举攻击。抗这种攻击的方法是在要发送的消息后附加上一个随机数。***RSA 安全性***：穷举攻击：试图穷举所有可能的私钥；数学攻击：试图分解两个素数的乘积；计时攻击：依赖于解密算法的运行时间，记录计算机解密信息所用的时间来确定私钥。解决办法： 不变的幂运算时间，随机延时，隐蔽，在执行幂运算之前将密文乘上一个随机数；选择密文攻击：利用了 RSA 算法的性质。攻击者选择一些密文并获得相应的明文，利用目标对象的私钥解密获得的。攻击者选择一个明文，运用目标对象的公钥加密，然后在用目标对象的私钥解密而取回明文。在别人的密文上乘上自己精心设计的加密后的数据给对方解密，在把解密后的数据发回来能得到有用的信息。

第 10 章密钥管理和其他公钥密码体制：***DH 密钥交换算法：*** 容易遭受中间人攻击。匿名 DH 方案、固定 DH 方案、瞬时 DH 方案【多一个认证，但是双方都要有一个一个公私钥用于认证，三次握手】***ElGamal 密码体制***：ElGamal 的也是选择一个素数 q，a 是 q 的原根。用户 A：随机生成整数 XA，使得 1<XA<q-1，计算 YA=a^XAmodq。A 的私钥为 XA，公开密钥为{q，a，YA}。其他用户 B 通过 A 的公开密钥加密信息：将信息表示为一个整数 M，其中 1<=M<=q-1，以分组密码序列的方式来发送消息。选择一个整数 k，1<=k<=q-1。计算一次密钥 K=(YA)^kmodq。将 M 加密成密文对（C1，C2），C1=a^kmodq C2=KMmodq。用户 A 恢复明文：计算 K=C1^XAmodq。计算 M=（C2K^-1）modq。如果 k 用于多个分块。可以计算出 M1/M2，如果 M1 泄露，则可以容易计算出 M2。ElGamal 的安全性是基于计算离散对数的困难性之上。***椭圆曲线***：y^2=x^3+ax+b，用 E(a,b)描述椭圆曲线，还要包含一个 O 的隐点，也称为无穷远点。这个值在椭圆权限算法中用作恒等式，当 4a^3+27b^2!=0 是 E(a,b)+O 是一个群，隐点 O 就是单位元。***椭圆曲线密码 ECC***：比 RSA 密钥长度短，但是安全程度和较长密钥长度的 RSA 同等。***ECC 安全性***：ECC 的安全性是建立在由 kP 和 P 确定 k 的困难程度上的。

第 11 章密码学 Hash 函数：*应用*：消息认证、数字签名、文件指纹。产生单项口令文件。***sha2 压缩函数：*** 构建块，使用到了 AND，or，not，xor 循环移位，80 轮迭代后加法求 2^32/64 摸。***Hash 安全性需求***：输入长度可变。输出长度固定。效率。抗原像攻击（单项性）。抗第二原像攻击（抗弱碰撞性）。抗碰撞攻击（抗强碰撞性）。伪随机性。 ***sha3***：海绵结构，分组 r，吸水阶段对每个分组扩充为 b=r+c。r 位速率，c 容量提供安全复杂度。最后结果为 b 位，看要求进入挤压阶段。

第 12 章消息认证码：***解决的攻击***：伪装、内容修改、顺序修改、计时修改（对消息的延时和重播）***消息认证函数***：任何消息认证或数字签名机制在功能上有上下两层。下层为生成认证符函数，上层是验证消息的真实性。生成认证符函数，Hash 函数、消息加密、消息认证码。***消息认证码***：利用密钥生成一个固定长度的短数据块，可以提供认证，但不能提供保密性。MAC 函数与加密类似，区别之一是 MAC 算法不要求可逆性而加密算法必须是可逆的，由于认证函数的数学性质，与加密相比，认证函数更不易被攻破。***MAC 的安全性***：重放，暴力破解、生日攻击，攻击密钥 2^k，攻击 MAC 值 2^n。所以 MAC 算法的穷举攻击所需的代价为 min(2^k,2^n)。***MAC 函数的需求***：攻击者知道 M 和 MAC(K,M)，则他构造 MAC(K,M)=MAC(K,M ')的消息 M'在计算上是不可行的。MAC(K,M)应该是均匀分布的，即对任何随机选择的消息 M 和 M '碰撞的概率为 2^-n【抵抗基于选择明文攻击的穷举攻击】。认证算法对消息的某部分或位不应比其他部分或位更弱。***HMAC***：HMAC(K,M)=H[(k' xor opad)|| H[(K' xor ipad)||M]] ***HMAC 的安全性***：依赖于 Hash 函数的强度。对密钥的穷举攻击或者生日攻击。***基于分组密码的 MAC-DAA 和 CMAC***：DAA（数据认证算法）采用 DES 运算的密文块链接（CBC）模式。此方案不安全，如攻击者知道一个消息分组的 CBC MAC 如 T=MAC(K,X)，则攻击者马上就知道两个消息分组 X||(X xor T)的 MAC 就是为 T。

第 14 章密钥管理和分发：*密钥层次结构*：会话密钥，主密钥。***会话密钥生命周期***：效率和安全的平衡。***分布式密钥控制***：配置 n 个终端的分布式密钥分发需要大概 n(n-1)/2 个主密钥。A 发送会话密钥请求给 B，包括一个临时交互号 N1。B 用共享主密钥加密信息并回复给 A，该信息中包含 B 选择的会话密钥、B 的标识符、值 f(N1)、临时交互号 N2。使用新的会话密钥，A 返回信息 f(N2)给 B。***基于对称加密的对称密钥分发***：集中式：KDC，不存在中间人攻击，认证阶段通过临时交互号**第 13 章数字签名**：***消息认证争议***：1、一方伪造对方发送的消息。2、对方对自己发送的消息否认。***数字签名的需求***：1 签名必须是与消息相关的二进制位串 2 签名必须使用发送方独有的信息 3 产生数字签名比较容易 4 识别和验证签名比较容易 5 伪造数字签名在计算上是不可行的 6 保存数字签名的副本是可行的。***直接数字签名***：只涉及通信双方。先进行签名然后执行外层的加密。有一个弱点就是私钥的安全性。可以说私钥丢了来进行否认。X 的私钥可能在时刻 T 被盗用，但攻击者可用 X 的签名发一条消息在 T 或 T 之前的时间戳。***ElGamal 数字签名方案、Schnorr 数字签名方案：大概的了解。数字签名标准 DSS（DSA）***：只提供数字签名的算法不能用于加密或密钥换。流程 hash+随机数用私钥和全局公钥进行签名生成 s 和 r 签名对。流程类似于 ***Schnorr 签名算法。***防止重放攻击。分布式：主体之间已经存在一对共享的密钥。***基于非对称加密的对称密钥分发***：A 产生一个公私钥对，然后发送公钥和 A 的身份给 B，B 产生会话密钥并用公钥加密返回给 A，A 解密后得到会话密钥。最后双方丢弃公私钥。此协议存在中间人攻击。***确保保密性和身份验证的密钥分发***：A 用 B 的公钥加密 IDA 和临时交互号 N1，B 用 A 的公钥加密 N1 和 B 产生的临时交互号 N2。A 使用 B 的公钥返回 N2。A 选择密钥 Ks 用 A 的私钥加密然后在用 B 的公钥加密发送给 B。***混合方案***：仍然延续使用 KDC，KDC 和每个用户共享一个主密钥，用主密钥加密要分发的会话密钥，公钥方案被用于分发主密钥。***公钥分发***：***公开发布***：任一通信方可以将他的公钥发送给另一个通信方或广播给通信各方。但是缺点是任何人都可以伪造这种公钥并公开发布。***公开可访问的目录***：维护一个动态可访问的公钥目录。某可信的实体或组织负责整个公开目录的维护和分配。为了安全传输公钥，管理员到通信方有安全的认证通信。缺点是目录管理员的私钥一旦泄露就全泄露了。***公钥授权***：还是有缺陷。公钥管理员会成为系统的瓶颈。管理员所维护的含有姓名和公钥的目录容易被篡改。***公钥证书***；通信双方使用证书来交换密钥而不是公钥管理员。证书包含公钥、主体标识、时间、算法、版本号、证书序列号等，整个数据块由可信第三方进行签名。***证书链***：由不同的 CA 创建的一系列的证书组成。前向证书，由其它 CA 发给 X 的证书。后向证书，X 发给其它 CA 的证书。***证书撤销链表***：每个个 CA 保留一张表包含被 CA 撤销且还未到期的证书。

第 15 章用户认证：*实体认证 VS 消息认证*：实体认证需要实时认证发送方的身份且消息一般固定的，无意义，消息认证则不需要及时性且消息变化的有意义。***认证协议的需求***：A 能向 B 证明自己（单向认证）。B 不能重用 A 向 B 的认证，时间戳或挑战应答。不能伪造一个认证。***认证的依据***：知道的东西，拥有的物理东西，生物特征。***强认证***：挑战响应，零知识；不会将秘密透露给验证方 。弱认证：密码。***PINs***：用户身份认证码。pins+拥有的物理东西，pins 一般很短所以需要限制尝试次数。***挑战响应***：时变值：随机数、序列值、时戳。eg：needham，公钥密码密钥分发等。重放攻击、交织攻击。***零知识证明***：非对称技术，不会用到数字签名和公钥加密。使用随机数作为挑战。A 需要把秘密封装，不让 B 知道。A 选择一个随机数生成一个证据来干扰让 B 认证秘密时不会知道秘密。B 发一个挑战给 A，A 收到挑战后回答一个响应，B 收到响应后判断响应是否正确，在验证正确的过程中不能获得 A 的秘密信息。一般会执行 t 轮，t 越大，被冒充的概率越低。证明起到干扰的作用，避免 si 的泄露。

- **A→B：$x = r^2 \bmod n$**
- **A←B：e∈{0,1}**
- **A→B：$y = r \times s^e \bmod n$**

群环域：加法封闭性、结合律、单位元、逆元】、交换律】，乘法封闭性、集合率、分配律】、乘法交换律】，乘法单位元、非零因子】，乘法逆元

AES 中的数学：GF(2^3)域中的字节代替中的 S 盒生成、列混淆变换也可转为多项式的乘法。

RSA 中的数学：模算数的求幂运算，快 R 速幂算法并对之间结果取模。攻击方利用 CRT 进行攻击，当使用相同的公钥对同一个数据加密，但是模数不一样，能够求出 M^e 进而得到明文。防范的手段是加一个伪随机位串。对于使用者通过 CRT 和费马定理加快运算速度