密码编码学与网络安全

> 几乎所有的内容都是对大学课本《密码编码学与网络安全-原理与实践》的回忆与总结。

密码算法和协议可以分成四个主要领域：

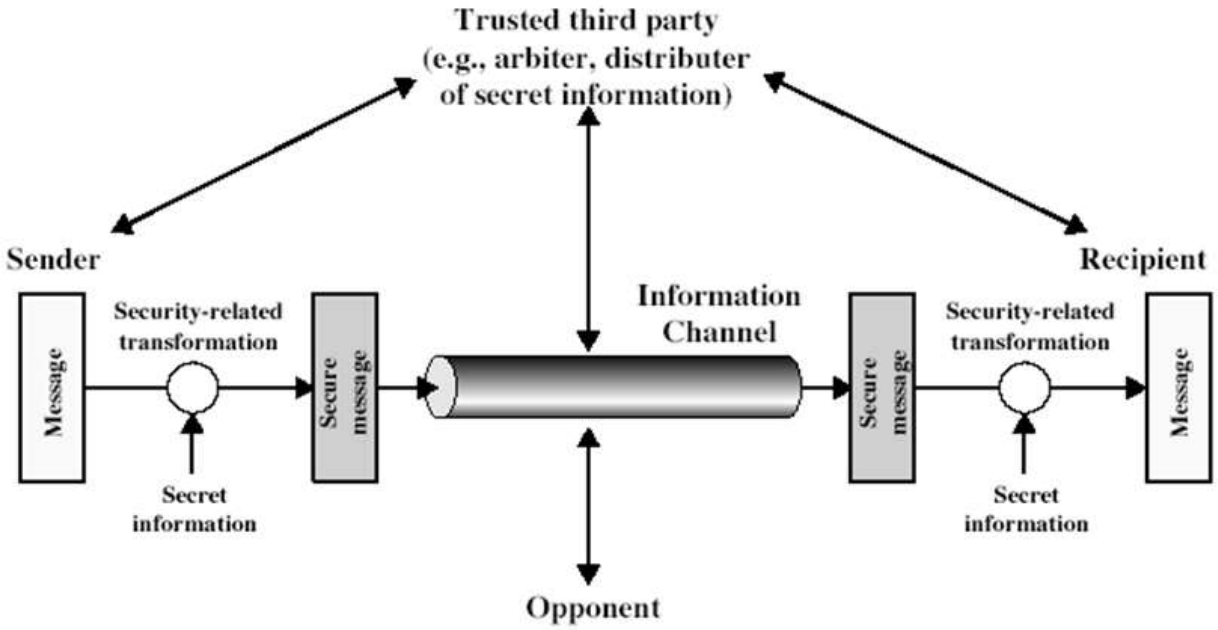
- 对称加密
- 非对称加密
- 数据完整性算法
- 认证协议

计算机安全核心地位的三个关键目标（CIA三元组）：

- 保密性（Confidentiality）
- 完整性（Integrity）
- 可用性（Availability）

ITU-T（国际电信联盟电信标准化组）推荐方案*X.800*，即***OSI安全框架***，提供了一个定义和提供安全需求的系统化方法，主要关注：

- 安全攻击（Security Attack）——问题
  - 被动攻击：对传输进行窃听和检测
  - 主动攻击：对数据流进行修改或伪造数据流
- 安全机制（Security Service）——方法
  - 认证：保证通信的实体使它所声称的实体
  - 访问控制：阻止对资源的非授权使用
  - 数据保密性：保护数据免于非授权使用
  - 数据完整性：保证收到的数据的确是授权实体所发出的数据
  - 不可否认性：防止整个或部分通信过程中，任一通信实体进行否认的行为
- 安全服务（Security Mechanism）——效果
  - 特定安全机制：可以并入适当协议层以提供一些OSI安全服务
  - 普遍安全机制：不局限于任何特定的OSI安全服务或协议层的控制



【图：网络安全模型】

在网络安全模型下，设计安全服务应包含四个方面的内容：

1. 涉及执行安全相关传输的算法
2. 产生算法所使用的秘密信息
3. 涉及分配和共享秘密信息的方法
4. 指明通信双方使用的协议，该协议利用安全算法和秘密信息实现安全服务

计算机安全主要涉及：

- 病毒
- 访问控制
- 防火墙
- 入侵检测

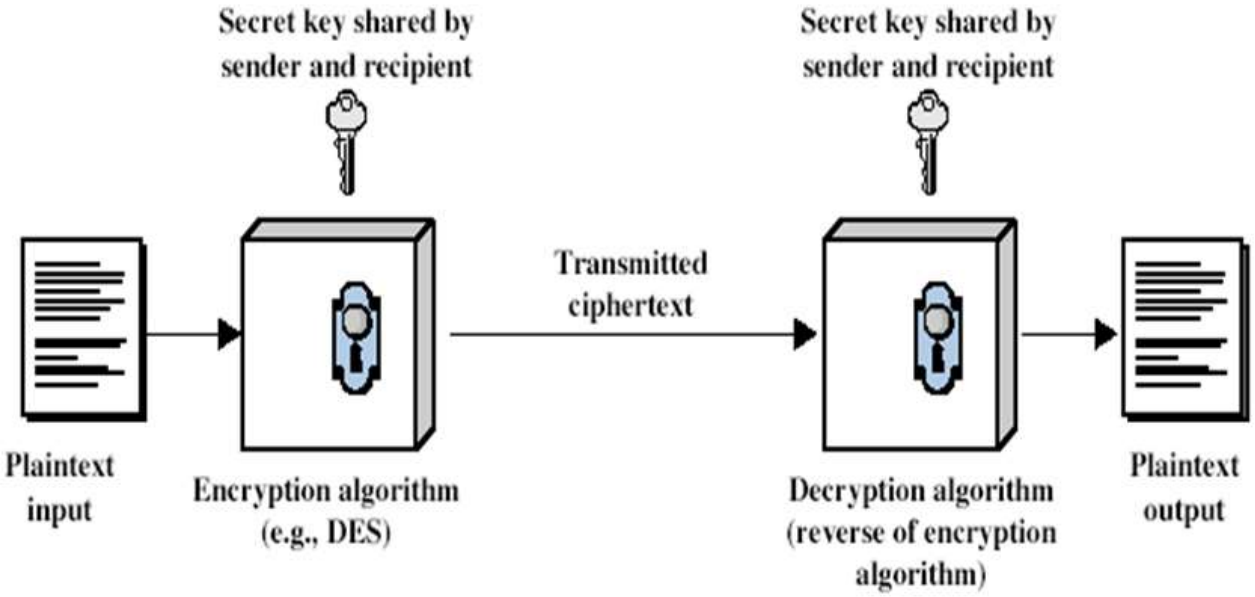
传统的对称密码（计算机出现前）对数据安全保证依赖于算法的保密，计算机出现后，数据的安全基于密钥而不是算法的保密。1949年香农的《保密系统的信息理论》证明了密码编码学是如何置于坚实的数学基础之上。算法是基于密钥的，那么通信双方必须在某种安全形式下获得密钥并必须保证密钥的安全1976年，Diffie和Hellman的《密码学新方向》突破传统密码体制使用秘密密钥所带来的密钥管理难题，使密码的发展进入公钥密码学阶段。19世纪，Kerckhoff（柯克霍夫）提出的原则：系统的保密性不依赖于对加密体制或算法的保密，而依赖于对密钥的保密。

领域

对称加密（传统密码）

- 特征

    - 加密解密使用相同的密钥
    - 运算类型：代替，置换
    - 种类：分组密码，流密码
- 攻击方法
    - 密码分析学（Cryptoanalytic Attack）
        - 唯密文攻击（Ciphertext Only）
        - 已知明文攻击（Known Plaintext）
        - 选择明文攻击（Chosen Plaintext）
        - 选择密文攻击（Chosen Ciphertext）
        - 选择文本攻击（Chosen Text）
    - 穷举攻击（Brute-force Attack）
- 分组密码的工作模式
    - 五种标准的工作模式
        - 电码本模式（Electronic Code Book，ECB）
        - 密文分组链接模式（Cipher Block Chaining，CBC）
        - 密文反馈模式（Cipher Feedback，CFB）
        - 输出反馈模式（Output　Feedback，CFB）
        - 计数器模式（Counter，CTR）
    - 面向分组的存储设备的XTS-AES模式



【图：对称密码模型】

对称密码的发展致力于：1.减少明文与密文之间的关系；2.增大密钥空间。因此出现了理论上绝对安全的一次一密（事实上，一次一密的安全性完全取决于密钥的随机性），基于多层加密原理的转轮机密码系统。前者出现了流密码，后者为DES指明了方向。

> Note:
> - 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。

> - 替换：明文元素的序列被替换为该序列的一个置换。也就是说，序列中没有元素被添加、删除或替换，但序列中元素出现的顺序改变了。

Shannon引进**扩散**和**混淆**挫败基于统计方法的密码分析。

> 扩散是指明文的统计特征消散在密文中。
> 这可以通过让每个明文数字尽可能地影响多个密文数字获得，等价于说每个密文数字被许多明文数字影响。在二进制分组密码中，对明文进行置换后再用某个函数作用，重复多次就可以获得较好的扩散效果；这来自于原始明文中不同位置的多个位对密文的某个位产生的影响。
> 混淆是指尽可能地使密文和加密密钥间的统计关系更复杂，以阻止攻击者发现密钥。
> 可以使用复杂的代替算法来实现，简单的线性替代函数几乎增加不了混淆。

许多分组密码采用Feistel结构，这样的结构由许多相同的轮函数组成。每一轮中，对输入数据的一半进行代替，接着用一个置换来交换数据的两个等分部分，拓展初始密钥使得每一轮中使用不同的子密钥。数据加密标准（Data Encryption Standard，DES）体现了经典的Feistel结构。
高级加密标准（Advanced Encryption Standard，AES）未采用Feistel结构，每轮由四个单独的运算组成：字节代替、置换、有限域GF(2^8)的算术运算、密钥的异或运算。

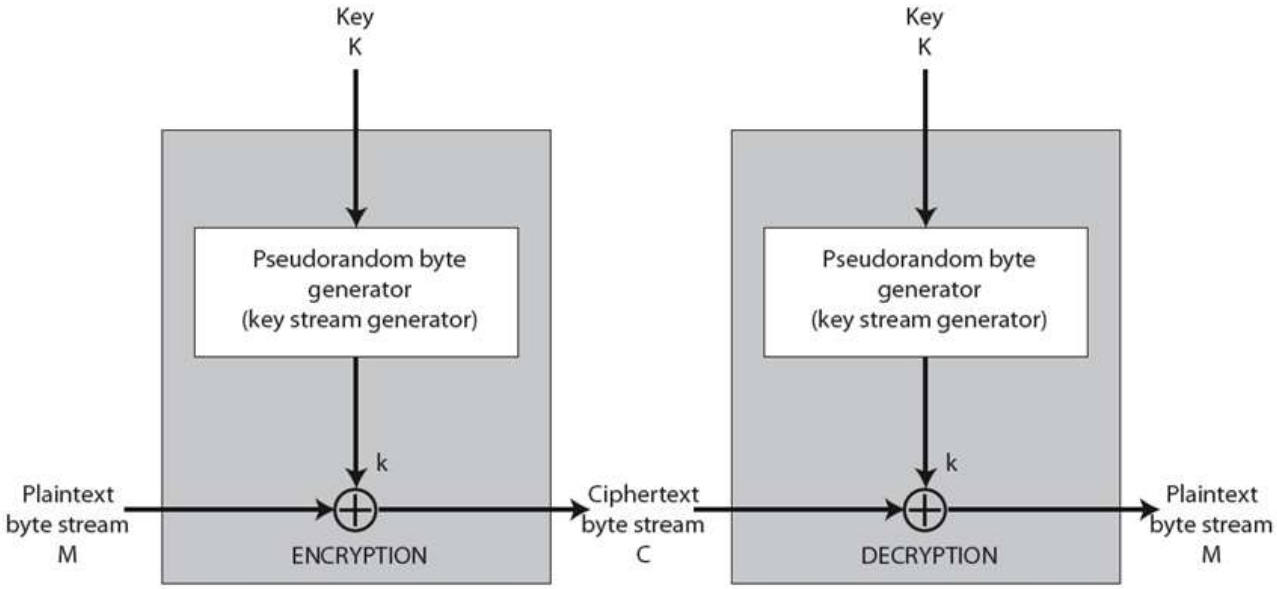
明文或密钥的某一位发生变化会导致密文的很多位发生变化，这被称为**雪崩效应**。DES、AES有很好的雪崩效应。

多重加密是一个加密算法多次使用的技术，建立在多重加密所对应的映射不能为单次加密所定义的前提下。DES在穷举攻击下相对比较脆弱，因此出现三重DES（3DES），共用到两组或者三组密钥。

为了将分组密码应用于各种各样的实际应用，NIST（SP800-38A）定义了物种工作模式。本质上，工作模式是一项增强密码算法或者使算法适应具体应用的技术。XTS-AES标准描述了一种对基于扇区的设备上的数据进行加密的方法，此时的威胁模型包括敌手对存储数据的访问。

分组密码的工作模式见Wikipedia：https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

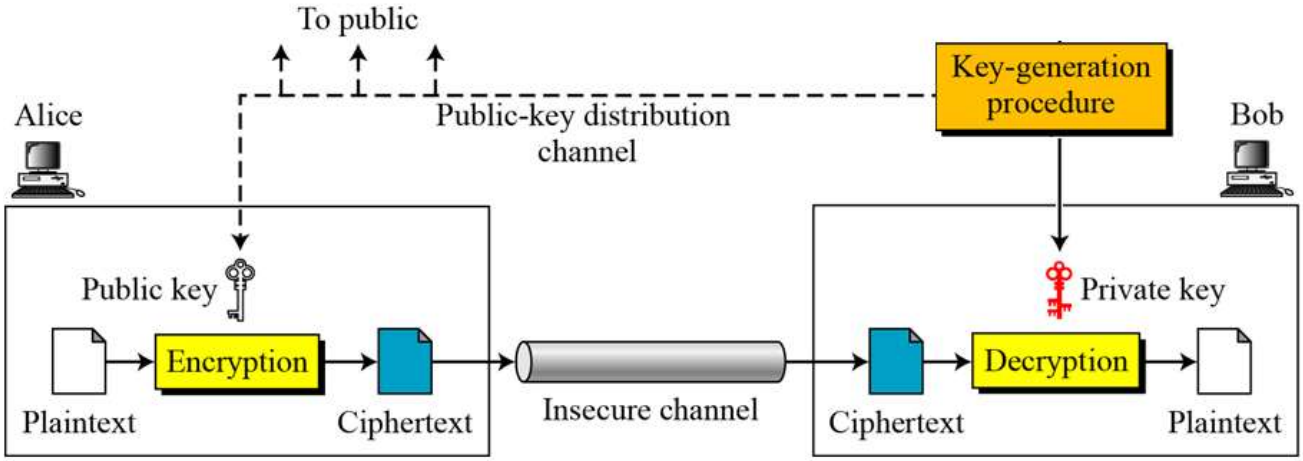
大量密码函数需要随机或伪随机数的产生。随机序列应有良好的统计特征，满足：分布均匀性（序列中的位分布应是均匀的，即 0 和 1 出现的频率大约相等）、独立性（序列中任何子序列不能由其他子序列推导）、不可预测性。通过设计合适的伪随机数发生器（PRNG），当密钥长度相当时，流密码可以提供和分组密码一样的安全性。



【图：流密码结构】

公钥密码

- 特征
  - 加密算法和解密算法使用不同的密钥
  - 基于数学函数
    - 原理：每个函数值都存在唯一的逆，并且计算函数值是容易的，但求逆却是不可行。
- 攻击方法：
  - 穷举攻击
  - 从给定公钥计算私钥
  - 穷举消息攻击
- 应用：加密/解密、数字签名、密钥交换



【图：公钥密码体制】

公钥密码学的出现为了解决传统密码学中最困难的两个问题：密钥分配问题、数字签名问题。

> 对称密钥体制的缺陷：
> - 密钥分配问题：通信双方要进行加密通信，需要通过秘密的安全信道协商加密密钥，而这种安全信道可能很难实现。
> - 密钥管理问题：在有多个用户的网络中，任何两个用户之间都需要有共享的密钥，当网络中的用户n很大时，需要管理的密钥数n(n-1)/2是巨大的。
> - 数字签名问题：当主体A收到主体B的电子文档（电子数据）时，无法向第三方证明此电子文档确实来源于B。

相关密钥的密码算法需要寻找一个单向陷门函数，它满足：每个函数值都存在唯一的逆，并且计算函数值是容易的，但求逆却是不可行的。当前存在的单向陷门函数：大合数的素因子分解、离散对数。

> 单向陷门函数：一个函数，若计算函数值很容易，并且在缺少一些附加信息时计算函数的逆是不可行的，但是已知这些附加信息时，可在多项式时间内计算出函数的逆。

公钥加密标准（Public Key Cryptography Standards, PKCS）定义了若干公钥密码学标准。

RSA基于寻找大合数的素因子的困难性，易受选择密文攻击（CCA），但可通过在加密之前对明文进行随机填充防止，建议使用最优非对称加密填充（OAEP）的程序对明文进行修改。
Diffie-Hellman密钥交换协议使得通信的双方利用基于离散对数问题的公钥算法建立密钥。它可以通过公共信道交换一个信息，就可以创建一个可以用于在公共信道上安全通信的共享秘密（shared secret）。但它易受中间人攻击，仅当通信双方的真实性能够得到保证的前提下是安全的。
ElGamal密码体系也基于离散对数问题，应用于诸如数字签名标准中。

椭圆曲线密码学（Elliptic Curve Cryptography，ECC）基于椭圆曲线离散对数问题。它的加法运算与RSA中的模乘运算相对应，乘法运算与RSA中的模幂运算对应，可以用较小的密钥长度达到较高的计算难度。

密码学数据完整性算法

- Hash函数
  - 作用：浓缩任意长的消息到一个固定长度的取值
  - 种类：专为Hash函数设计的函数，对称分组密码
  - 用途：用于检测消息的改变
- 应用
  - 消息认证
    - 认证加密
  - 数字签名
  - 使用Hash函数和MAC产生伪随机数
  - 密钥推导函数（HKBF，key derivation function based on a hash-based message authentication）

    - ...
- 安全性需求
    - 输入长度可变
    - 输出长度固定
    - 效率
    - 抗原像攻击（单向性）
    - 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
- 攻击方法
    - 穷举攻击
        - 原像攻击和第二原像攻击
        - 碰撞攻击
        - 理论：生日悖论
    - 密码分析攻击

Hash函数要求如下两种情况在计算上不可行（即没有攻击方法比穷举攻击更有效）：1.对预先指定的Hash值找到对应的数据块（单向性）；2.找到两个不同的数据块对应相同的Hash值（抗碰撞性）。

消息认证是用来验证消息完整性的一种机制或服务，保收到的数据确实和发送时的一样（即没有修改、插入、删除或重放），且发送方声称的身份是真实有效的。
消息认证是通过使用消息认证码（Message Authentication Code，MAC）来实现的，即带密钥的Hash函数，通过密钥验证方也知道发送方是谁。它可以是基于Hash函数的MAC（HMAC），或基于分组密码的MAC（数据认证算法DAA，基于密码的消息认证码CMAC）。
认证加密（Authenticated Encryption，AE）是指在通信中同时提供保密性和认证（完整性）的加密系统。通用方案有：1.先Hash再加密；2.先MAC再加密；3.先加密再MAC；4.加密并且MAC。存在CCM（Counter with CBC-MAC）工作模式、GCM（Galois/Counter Mode）工作模式等。

数字签名是一种认证机制，使得消息的产生者可以添加一个起签名作用的码字。通过计算消息的Hash值并用产生者的私钥加密Hash值来生成签名。签名保证了消息的来源和完整性。

> 消息认证可以保护消息交换双方不受第三方的攻击，但是它不能处理通信双方自身发生的攻击。比如：
> 1）Marry伪造一条消息并称该消息发自John。Marry只需产生一条消息，用John和Marry共享的密钥产生认证码，并将认证码附于消息之后。
> 2）John可以否认曾发送过这条消息。因为Mary可以伪造消息，所以无法证明John确实发送过该消息。

> 因此，数字签名是解决这类问题的最好方法。

相互信任

- 密钥管理和分发
  - 对称加密的对称密钥分发
  - 非对称加密的对称密钥分发
  - 混合方式的密钥分配
  - 公钥分发
    - X.509认证服务
    - 公钥基础设施（Public Key Infrastructure，PKI）
- 用户认证
  - 远程用户认证原理
    - 双向认证
    - 单向认证
  - 基于对称加密的远程用户认证
    - Kerberos机制
  - 基于非对称加密的远程用户认证
  - 攻击方法
    - 重放攻击
    - 压制重放攻击
    - 中间人攻击

密钥分发的功能是给想要交换安全加密数据的双方分发密钥，并提供密钥安全分发所需要的一些方法或协议，分发的包括双方之间的频繁使用且长期存在的主密钥以及临时使用的会话密钥。任何密码系统的强度取决于密钥分发技术，即在想要交换数据的两者之间传递密钥且不被其他人知道的方法。

对称密钥分发的一种典型方案是每个用户和密钥分发中心（KDC）共享唯一密钥，对于大型网络来说可以建立KDC的层次体系使得主密钥分发的开销最小化。会话密钥更换得越频繁越安全。对于面向对象的协议，在会话的整个生命周期中使用同一个会话密钥，为每一次新的会话使用新的会话密钥。对于无连接的协议最安全的方法是每次都是用新的会话密钥，但否定了无连接协议的优点，因此一个比较好的策略是为特定时期或特定数量的事务分配不同的会话密钥。
公钥加密系统的效率比较低，经常用于小数据块的加密，最重要的应用之一是用于密钥的加密分发。只有在公钥的可靠性可以保证时，公钥加密方案才是安全的。提出以下的公钥分配方法：1.公开发布，2.公开可访问的目录，3.公钥授权，4.公钥证书。

公钥的可以公开，人热可以公开发布，但缺点明显：任何人都可以伪造这种公钥并公开发布，也就是说，某个用户可以假冒用户A并将一个公钥发送给通信的另一方或广播该公钥。维护一个动态的可访问的公钥目录可以获得更大的安全性，由某可信的实体或组织负责这个公开目录的维护或分配，可一旦攻击者获得或计算出目录管理员的私钥，或通过修改目录管理员保存的记录，则他可以假冒任何通信方，以窃取发送给该通信方的信息。通过更加严格地控制目录中的公钥分配，假定中心管理员负责维护通信各方公钥的动态目录，除此之外，每一通信方可靠地知道该目录管理员的公钥，并且只有管理员知道相应的私钥，可使公钥分配更加安全，但公钥管理员容易成为系统的瓶颈，因为用户与其他用户通信时必须向目录管理员申请对方的公钥。因此引入公钥证书，这种方法满足以下要求：

1. 任何通信方可以读取并确定证书拥有者的姓名和公钥。
2. 任何通信方可以验证该证书出自管理员而不是伪造的。
3. 只有证书管理员可以产生并更新证书。
4. 4.任何通信方可以产生并更新证书。

X.509标准是一个广为接受的方案，用来规范公钥证书的格式。IETF（Internet Engineering Task Force）的PKIX（Public Key Infrastructure X.509）工作组在X.509的基础上，建立了一个可以用来构建网络认证体系的基本模型。

RFC 282定义了用户认证中的两个阶段：鉴定阶段（给安全系统提供身份标志）、核实阶段（提供或者产生可以证实实体和标志之间对应关系的认证信息）。已认证的密钥交换主要关注两个问题：保密性和时效性。时效性用于防止消息重放的威胁。防止重放攻击的方法：

1. 序列号：对每一个用于认证交互的消息附上一个序列号，新的消息只有其序列号满足适当的顺序时才会被接收。
2. 时间戳：只有当消息中包含一个时间戳时，A才接收该消息。该时间戳由A来判断，要接近于A所知的当前时间。该方法要求不同参与者之间的时钟是同步的。
3. 挑战/应答：A想要一个来自B的新消息，首先发给B一个临时交互号（询问），并要求后面从B收到的消息（回复）中包含正确的临时交互号。

---

by river(river@vvl.me)

2019.03.14: initialization