第三章 密码技术

密码学是研究信息安全保密的学科，是保护信息在信道的传输过程不被窃取、解读和利用的方法。基于密码学的密码技术是计算机通信信息系统安全的核心技术，几乎渗透到信息系统安全的各个领域以及大部分安全机制之中。

3.1 基本概念

密码学是与信息的机密性、数据完整性、身份认证和数据起源认证等信息安全问题相关的一门数学技术学科。

3.1.1 加密与解密

3.1.2 加密算法

3.1.3 密码体制分类

3.1.4 密码体制与安全服务

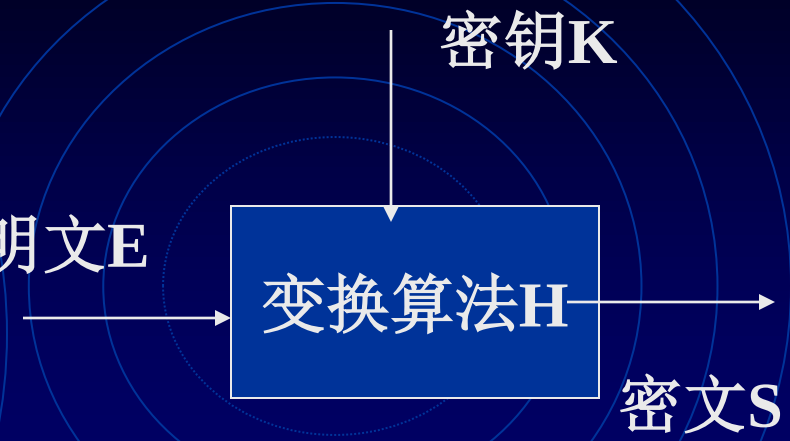
3.1.5 密钥

3.1.6 计算机通信安全与保密

3.1.1 加密与解密

1、加密

- 密码体制：数据变换
- 作用：保证数据的机密性
- 明文：原始数据
- 密文：变换后的数据
- 加密变换：明文->密文



有两种主要的加密（编码）方法，分别是：

换位：将组成信息块的数字位进行交换，很像那种把组成一个单词的字母组成顺序打乱的游戏。

置换：将每一个字符或数位替换为其他内容。对文件中的字符或符号进行替换，就能创建一个置换密码。

3.1.1 加密与解密

2、解密

加密的逆过程称为解密。

解密变换：密文->明文

要对一段加密的信息进行解密，需要具备两个条件，一个条件是需要知道解密规则或者算法，另一个条件是需要知道解密的密钥。

密钥：数据变换所用的独立输入项

加密密钥

解密密钥

3.1.1 加密与解密

3、密码破译

未经授权的解密称为破译。破译者不具有解密密钥，因此，他首先要试图得到解密密钥。

为了防止密码破译，可采取以下机制：

（1）强壮的加密算法；

（2）动态会话密钥；

（3）保护关键密钥；

（4）基于密码技术的访问控制是防止数据传输泄密的主要防护手段,访问控制的类型可分为两类：初始保护和持续保护。

3.1.1 加密与解密

4、加密分类

信息加密可分为两种：

- 通信加密：在传输过程中的数据加密
- 文件加密：将存储数据进行加密

以加密实现的通信层次来区分，可分三个不同层次：

- 节点加密
- 链路加密
- 端到端加密。

5、安全管理

安全管理主要涉及密钥以及机密信息的产生、分发、使用、销毁等问题。

3.1.2 加密算法

1、加密算法

信息加密是通过密钥使用加密算法实现的。加密算法是实施具体加密的基础，它决定了加密的强度、运算量以及它的实用性。

密码算法可分为保密的和公开的两种。

密码算法可以看作是一个复杂的函数变换，s=F（m，k），s代表密文，即加密后得到的字符序列，m代表明文，即待加密的字符序列，k表示密钥，是秘密选定的一个字符序列。

3.1.2 加密算法

- 例：

明文E：1234567890

加密算法H：间隔K个数取值排列，将剩下的数值按顺序排在后面。

如果加密钥K:1

则密文S=1357924680

如果加密钥K:2

则密文S=1470235689

3.1.2 加密算法

2、加密算法的实现

加密算法的实现可划分为两大类，一类是软件加密，另一类是硬件加密。

- **软件加密**：通过算法的计算机程序实现。

  特点：实现简单，成本低；速度比较慢；相对来说，机密性差。

- **硬件加密**：通过具体的电子线路实现加密算法。

  特点：实现复杂，成本高；加密速度比较快；相对软件加密算法实现，其机密性更好。

3.1.3 密码体制分类

密码体制类型：

1. 对称密码体制（私钥）：加密密钥和解密密钥相同，且都需要保密。
2. 非对称密码体制（公钥）：加密密钥和解密密钥不相同，一个公开，一个保密。

3.1.4 密码体制与安全服务

密码学主要为存储和传输中的数字信息提供以下4个方面的安全保护。

1、机密性

机密性服务是指只允许特定用户访问和阅读信息，任何非授权用户对信息都不可理解的服务。

2、数据完整性

数据完整性用于确保数据在存储和传输过程中不被未授权修改的服务。

3、认证

认证服务是一种与数据和身份识别有关的服务。

4、不可否认性

不可否认性服务是一种用于阻止合法用户否认先前的言论或行为的服务。

3.1.5 密钥

密钥是密码算法中的可变参数。密码体制的安全性完全建立在对密钥的安全性上。

密钥管理涉及密钥的各个方面，包括密钥的产生、密钥的分发、密钥输入和输出、密钥的更换、密钥的存储、密钥的保存和备份、密钥的生命周期以及密钥的销毁等。

3.1.6 计算机通信安全与保密

1、信息安全与保密

信息系统安全保密研究的对象是系统而不仅是系统中的某个或某些元素，系统内所有元素或成分都是研究的内容。

从系统内看，研究内容包括通信安全、计算机安全、操作安全、信息安全、人事安全、工业安全、资源保护和实体安全。

从系统外看（因为系统不是孤立的），研究内容还包括管理和法律两个方面，它们的综合构成了一个合理的研究结构和层次。

3.1.6 计算机通信安全与保密

2、计算机安全与保密

计算机安全保密涉及计算机硬件、软件以及所处理数据的安全和保密。

计算机安全保密研究数据的以下方面的内容：

- 机密性：解决数据的非授权存取（泄露）问题；
- 完整性：保护数据不被篡改或破坏；
- 可用性：研究如何避免系统性能降低和系统崩溃等威胁。

在计算机安全保密研究中，主体（Subject）和客体（Obicct）是两个重要概念，保护客体的安全、限制主体的权限构成了访问控制的主题。

3.1.6 计算机通信安全与保密

3、通信安全与保密

通信安全保密研究围绕寻找更强、更好的密码体制而展开。

4、安全保密研究

信息系统的安全保密研究有以下三个阶段：

- 计算机诞生前的密码学（通信安全保密）研究；
- 计算机安全保密研究；
- 信息系统的安全保密研究。

3.1.6 计算机通信安全与保密

通信安全保密作为实施安全保密策略的基本工具（基础层次）；计算机安全保密利用基础密码学来研究计算机的安全保密问题，表现了研究对象的个体性，而不管计算机系统之外的事情（中间层次）；信息系统安全保密综合利用通信和计算机安全保密的研究成果，并将研究定位在系统这个层次，系统内的一切成分都是研究的对象（最高层次）。