第六章 密码学与对称加密算法

6.1 密码学历史上的里程碑

6.1.1 凯撒密码

简单的将字母表中的每个字母替换成其后的三个字母，是单一字母的替代置换密码

6.1.2 美国内战

美国内战使用词汇替代和置换的复杂组合，从而试图破坏敌人的破译企图

6.1.3 Ultra与Enigma

6.2 密码学基础

6.2.1 密码学的目标

密码系统基本目标： 机密性、完整性、身份认证和不可否认性

- 机密性
  - 机密性：确保存储中或在传输中保持秘密状态
  - 对称秘钥密码：密码系统中所有用户都使用一个共享的秘钥
  - 公钥密码系统: 每个用户都能够使用公钥和私钥的组合密码
- 完整性
  - 完整性：确保数据在传输过程中不背修改
  - 完整性通过传输消息时创建的数字签名摘要来强制实施，公钥和私钥密码都能实施完整性
- 身份认证
  - 身份认证： 声明的系统用户身份进行验证，是密码系统的主要功能
- 不可否认性
  - 不可否认性为接受者提供了担保，保证消息确实来自发送者而不是来自伪装成发送者的人
  - 秘密秘钥（对称秘钥）密码系统不提供不可否认性
  - 公钥(非对称秘钥)密码系统提供不可否认性

6.2.2密码学概念

- 消息发送者使用密码学算法将明文消息加密为密文消息，使用字母C表示

- 创建和实现秘密编码和密码的技术被称为密码术
- 密码术和密码分析学被成为密码学
- 编码或解码在硬件或软件商的具体操作被成为密码系统

6.2.3 密码学的数学原理

- 二进制数学：
- 逻辑运算: OR、AND、NOT、XOR、模函数、单向函数、随机数、零知识证明、分割知识、工作函数
- 分割知识：单个解决方案中包含职责分离和两人控制被称为分割知识
- 零知识证明：零知识证明就是既能充分证明自己是某种权益的合法拥有者，又不把有关的信息泄露出去——即给外界的“知识”为“零”。证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。
- 工作函数：从成本和/或时间方面来度量所有努力，就可以度量密码学系统的强度

6.2.5 密码

- 编码与密码：
  - 编码：密码学系统中标识词汇或短语的符号
  - 密码：隐藏消息的真实含义
- 换位密码：使用某种加密算法重新排列明文消息中的字母，从而形成密文消息
- 替代密码：使用加密算法将明文消息中的每一个字符或比特都替换为不同的字符、如凯撒密码
- 一次性填充密码：对明文消息的每个字母都使用一个不同的字母表，极为强大的替代密码，一个不可破解的加密方案必须满足如下要求：
  i. 加密秘钥必须随机生成
  ii. 一次性填充必须进行物理保护
  iii. 每个一次性填充必须只使用一次
  iv. 秘钥必须至少与被加密的消息一样长
  v. 一次性填充缺点：只可用于短消息、分发和保护需要冗长的秘钥
- 分组密码：按消息的"组块"或分组进行操作，并且对整个消息分组同时应用加密算法
- 流密码：对消息中的每一个字符或每一位操作，每次只处理一个/以为，如凯撒密码
- 混淆与扩散：
  - 混淆：攻击者不能通过继续修改明文和分析产生的密文来确定秘钥
  - 扩展：明文改变导致多种变化时，这个变化扩散到整个密文中

6.3 现代密码学

6.3.1 密钥

- 现代密码系统并不依赖其算法的安全性
- 现代密码系统不依赖于保密的算法
- 现代密码学系统依赖具体的用户或用户组专用的一个或多个秘钥

6.3.2 对称秘钥算法

- 对称秘钥依赖一个共享的加密秘钥，该秘钥会分发给所有参与通信的成员
- 对称秘钥也被成为秘密秘钥密码学或私有秘钥密码学
- 对称秘钥的弱点
    i. 秘钥分发是一个问题： 对称秘钥建立通信之前，通信参与必须具备一个安全的交换秘钥的方法
    ii. 对称秘钥密码学并未实现不可否认性
    iii. 这种算法不可扩充
    iv. 秘钥必须经常更新
- 对称秘钥密码可扩展性问题：n个通信方之间完全连接需要的秘钥总数为：n*（n-1）/2

6.3.2 非对称秘钥算法

- 非对称秘钥算法也被成为公钥算法，每个用户都有公钥和私钥
- 非对称秘钥的优点：
    i. 新增用户只需要生成一对公钥-私钥对
    ii. 从非对称系统中更容易删除用户
    iii. 只有在用户的私钥被破坏时，才需要进行秘钥重建
    iv. 非对称秘钥加密提供了完整性、身份认证和不可否认性
    v. 秘钥分发是一个简单的过程
    vi. 不需要预先存在通信链接
- 对称和非对称密码学系统比较：

对称密码学系统	非对称密码学系统
单个共享的密钥	密钥对
带外交换	带内交换
不可扩展	可扩展
快速	慢速
批量加密	小块数据分组、数字签名、数字封装、数字证书
机密性	完整性、机密性、身份认证、不可否认性

6.3.4 散列算法

- 常用的散列算法：
    - 消息摘要2（MD2）

- 消息摘要5（MD5）
- 安全散列算法(SHA-0,SHA-1,SHA-2)
- 基于散列的消息身份认证代码(HMAC)

6.4 对称密码

- 常见对称密码系统：DES（数据加密标准）、3DES（三重数据加密标准）、IDEA（国际数据加密算法）、Blowfish、Skipjack、AES（高级加密标准）

6.4.1 数据加密标准(DES) 来源于Lucifer算法，DEA是实现DES标准的算法

- DES是一个64位的分组密码，具有五种操作模式
  i. 电子代码本模式（ECB）：安全性最差，每次处理一个64位分组，简单的使用秘钥对这个分组进行加密
  ii. 密码分组链接模式（CBC）：未加密文本的每个分组使用DES算法加密前，都与前一密文分组进行异或操作。
    - 缺点：错误传播，一个分组在传输中被破坏，这个分组将无法解密。
  iii. 密码回馈模式（CFB）：流密码形式的CBC、针对实时生成的数据进行操作
  iv. 输出回馈模式（OFB）：与CFB模式几乎相同。
    - 优点是不存在链接功能，传输错误不会通过传播影响之后分组的解密。
  v. 计数模式（CTR）：流密码，每次操作后都增加的计数，与OFB模式一样，不传播错误。

6.4.2 三重数据加密算法(3DES)

- 3DES有四个版本：
  i. DES EEE3：使用三个不同的秘钥对明文加密三次
  ii. DES EDE3：使用三个秘钥，但是将第二个加密操作替换成解密操作
  iii. DES EEE2：只使用两个秘钥
  iv. DES EDE2：使用两个秘钥、中间使用解密操作

6.4.3 国际数据加密算法（IDEA）

- 针对DES算法的秘钥长度不够开发的，采用128位的秘钥进行操作，

6.4.4 Blowfish（SSH使用）

- Blowfish扩展了IDEA的秘钥长度，可使用变长秘钥，BlowFish比IDEA和DES更快的算法

6.4.5 Skipjack

- 对64位的文本分组操作，使用80位的秘钥
- 没有被密码学团队普通接受，因为托管程序由美国政府控制

6.4.6 高级加密协议(AES)（ Rijndael、Twofish算法加密 ）

- 使用128、192、和256位加密，支持128分组处理对称加密算法记忆表
- Twofish算法 利用了两种技术：预白噪声化、后白噪声化

表 6.3　对称加密算法记忆表

算法名	分组大小(单位为位)	密钥大小(单位为位)
数据加密标准(DES)	64	56
三重 DES(3DES)	64	112 或 168
高级加密标准(AES)	128	128、192、256
Rijndael	可变	128、192、256
Twofish	128	1-256
Blowfish(通常在 SSH 中使用)	64	32-448
IDEA(在 PGP 中使用)	64	128
基于 RSA 的 Rivest 密码 5(RC5)	32、64、128	0-2040
基于 RSA 的 Rivest 密码 4(RC4)	流式	128
基于 RSA 的 Rivest 密码 2(RC2)	64	128
Skipjack	64	80

6.4.7 对称秘钥管理

1. 创建和分发对称密码
    - 离线分发：一方向另一方提供包括秘钥的一张纸或一份存储介质
    - 公钥加密：使用公钥加密建立初始的通信链接，在链接中交换秘钥
    - Diffie-Hellman算法：在不安全的链路中交换秘钥
2. 存储和销毁对称秘钥
    - 永远不要将加密秘钥存储在存放加密数据一起
    - 敏感秘钥考虑两个人分别持有秘钥的一般
3. 秘钥托管
    - 公平密码系统：私钥分成多分，交给独立的第三方
    - 托管加密标准：向政府提供解密密文的技术手段

6.4.8 密码生命周期

- 确定组织可以接受和使用的加密算法
- 基于传输信息的敏感性确认算法可接受的秘钥长度
- 列出可以使用的安全传输协议（SSL和TLS）