ISSN 1009-3044
Computer Knowledge and Technology 电脑知识与技术
Vol.7, No.2, January 2011,pp.295-296,309
E-mail: info@cccc.net.cn
http://www.dnzs.net.cn
Tel:+86-551-5690963 5690964

基于 DES 的加密算法

曹晓丽

(河南职业技术学院,河南 郑州 450046)

摘要:密码技术是信息安全的核心技术,该文主要通过阐述 DES 的算法原理与步骤,特点及安全性,以实现密码技术,增强信息安全。

关键词:算法;DES 算法;加密;解密;密钥

中图分类号:TP312 **文献标识码**:A **文章编号**:1009-3044(2011)02-0295-02

Based on DES Encryption Algorithm

CAO Xiao-li

(Henan Polytechnic, Zhengzhou 450046, China)

Abstract: Password technology is the core technology of information security This paper expounds principles and steps of DES algorithm, characteristics and safety, to realize the password techniques and strengthen information security.

Key words: algorithm; DES algorithm; encryption; decryption; key

密码学的发展大致经历了两个阶段:传统密码和现代密码学。这两个阶段的分界标志是 1949 年香农发表了他的经典论文——《保密系统的通信理论》,在此之前称为传统密码阶段,这个阶段持续的时间长,大约有几千年的历史,此时的密码体制主要是依靠手工或机械操作方式来实现的,采用代换和换位技术,通信手段是以人工或电报为主,是一种艺术(富有创造性的方式、方法)。在香农发表了他的经典论文之后至今称为现代密码学阶段,此阶段的密码体制主要是依靠计算机来实现,有坚实的数学理论基础,通信手段是无线通信、有线通信、计算机网络等,形成一门科学,是密码学发展的高级阶段。

1 算法和 DES 算法描述

用来描述问题解决办法的过程称为算法,算法是多种数学知识的综合应用,所以密码学是一门交叉学科,同时它也是计算机科学的重要基础。

根据加密密钥和解密密钥是否相同,现代密码算法被分为两大类:对称密码算法和非对称密码算法。对称加密算法的特点是:加密密钥和解密密钥户有关联,加密密钥可以从解密密钥中推导出来,解密密钥也可以从加密密钥中推导出来。在大多数的对称算法中,加密密钥和解密密钥是相同的。通常情况下,对称密钥加密算法的加密与解密速度非常快,因此,这类算法适用于大批量数据加密的应用场合。

原始的信息,也就是需要被密码保护的信息,被称为明文。采用数学方法对明文进行再组织,加密后的信息称为密文。密文在网络上公开传输,其内容对于非法接收者来说起到了一定的保护功能。解密是将密文通过解密过程得到明文。密钥是用于加、解密的一些特殊信息,它是控制明文与密文之间变换的关键,密钥可以是数字、词汇、或语句。密钥分为加密密钥和解密密钥。明文、密文、加密、解密、加密密钥和解密密钥之间的关系如图 1 所示。

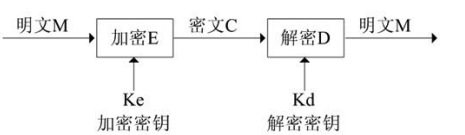

图 1 加密解密过程

数据加密标准(DES,Data Encryption Standard)的出现是现代密码发展史上的一个非常重要的事件, 它是密码学历史上第一个广泛应用于商业数据保密的密码算法,并开创了公开密码算法的先例,极大的促进了密码学的发展。由于 DES 算法保密性强,到目前为止,除了穷举法外,还没有找到更好的方法破解,因此 DES 得到了广泛的应用,并成为其他加密方法的典范。

DES 算法主要研究的是加密与解密算法。解密是加密的逆过程,从加密过的信息中得到明文。密钥是一串适当长度的字符或数字串,它可以控制加密和解密过程。

2 DES 算法原理描述

DES 是一个对称密码体制,加密和解密使用同一密钥,有效密钥的长度为 56 位。同时,一个分组密码,分组长度为 64 位,明文和密文的长度相同,及 64 位的明文从算法的一端输入,从另一端输出 64 位密文。

2.1 DES 加密算法的基本结构

DES 密钥初始长度是 64 位,第 8、16、24、32 等 8 的倍数位的数字用于奇偶检验,所以 DES 密钥有效密约长度是 56 位。密钥可以为任意的 56 位的数,且根据使用情况可以随时更换,同时,所有的安全性都依赖于密钥的保密。

DES 对 64 位的明文分组进行操作,经过一个初始转换(IP),然后将明文转换成左半部分与右半部分(L_0,R_0),各 32 位,再进行

收稿日期:2010-11-15

作者简介:曹晓丽(1979-),女,河南职业技术学院讲师,研究方向为多媒体技术、信息安全。

16 轮完全相同函数的迭代运算，这些运算用函数 F 表示，在每一轮迭代运算过程中，R_i 与密钥 K_i 在轮迭代的作用下，其结果与 L_i 做异或运算，其结果作为下一轮的 R_{i+1}，而下一轮的 L_{i+1} 则由本轮的 R_i 担任，在第 16 轮输出结果出现后，左右半部分在一起经过一个逆初始转换(IP–1)，最终产生一个 64 位的密文，算法完成。如图 2 所示。

现在常用的 DES 算法是 16 轮迭代算法，在每一轮中，DES 的一轮迭代运算步骤为：

1)把 64 位输入码分成左右两组，分别用 L_{i-1} 和 R_{i-1} 来表示，每组 32 位比特。其中 i 代表第 i 轮 F 函数，i=1,2,…,16。

2)把该轮 F 函数输入分组的右组 32 位比特输出作为下一轮 F 函数的左 32 位比特分组，即 $L_i=R_{i-1}$。

3)输入的右组 32 位比特经过扩展置换(E 盒)变为 48 位比特码组，扩展置换有专门的置换表可查。

4)经过扩展置换(E 盒)输出的 48 位比特与本轮的子密钥 Ki (48 位比特)进行异或运算，输出的 48 位比特，把它们分为 8 组，每组 6 位。

5)上步骤的输出按组进行密表(S 盒)替代，产生每组 4 位比特信息，其置换法则是输入的 6 位比特的第 1、6 两位所组成一个两位数，这个数字决定密表内所要选择的行数，其余 4 位所组成的一个四位数，这个数字决定密表内的列数，通过这个 6 位输入确定的行号和列号所对应位置的值作为该组的 4 位输出。

6)把上步骤的输出(8 组)合并为 32 位比特信息，经过置换运算(P 盒)的简单换位后，得到 32 位比特的输出，然后与本次乘积变换输入左组进行异或运算，即可得到第 i 轮 F 函数作用的右 32 位输出 R_i。如图 3 所示。

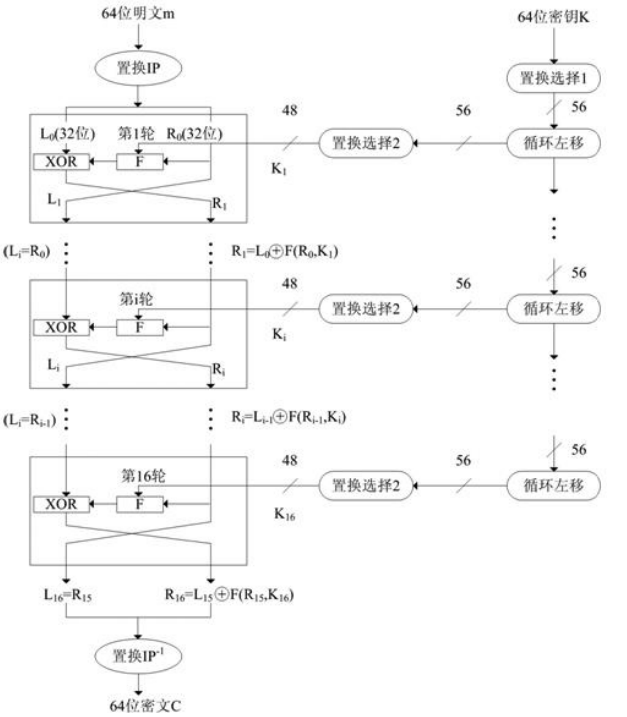

图 2　DES 的基本结构

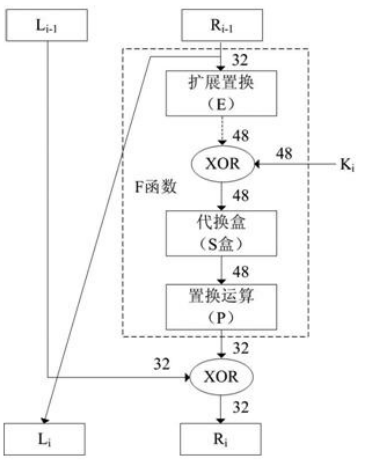

图 3　EDS 的一轮迭代过程

假设 B_i 是第 i 轮迭代的结果，L_i 和 R_i 是 B_i 的左半部分和右半部分，K_i 是第 i 轮的 48 位子密钥，子密钥是初始密钥经过一定算法的输出，且 F 是实现扩展置换(E 盒)、密表替代(S 盒)及置换运算(P 盒)的函数，那么每一轮算法可以简单的描述为：

$L_0R_0 \leftarrow IP$(64 位明文)

对于 i=1,2,…,16,

$L_i \leftarrow R_{i-1}$

$R_i \leftarrow L_{i-1} \oplus F(R_{i-1},K_i)$

(64 位密文)$\leftarrow IP^{-1}(R_{16}L_{16})$

2.2 DES 解密算法

DES 的解密算法是加密算法的逆运算，数学公式表达如下：

$R_{16}L_{16} \leftarrow IP$(16 位密文)

对于 i=16,15,…,1,

$R_{i-1} \leftarrow L_i$

$L_{i-1} \leftarrow R_i \oplus F(L_i,K_i)$

(64 位明文)! $IP^{-1}(R_0L_0)$

DES 算法的解密算法与加密算法相同，只是各子密钥的顺相反，即为 $K_{16},K_{15},\cdots,K_1$。

2.3 DES 算法特点及安全性

DES 算法具有以下特点：

1)DES 算法公开，信息的保密性完全依赖密钥的管理，传输等保密环节。

2)在目前水平下，在不知道密钥的情况下，如果想在一定的时间内破译 DES(即析出密钥 K 或明文)是不太可能的，因为想要实现，至少要建立 256 或 264 个的表，这是现有硬件与软件资源难以实现的。

3)明文或密钥的微小变化都会导致密文的巨大变化，即 DES 显示出很强的"雪崩效应"，使攻击者无法分而破之。

而 DES 也总有不足之处，强密钥长度为 56 个，显得有些短；其次，存在弱密钥，第三，S 盒的设置变化显得略微简单。

3 DES 的完善与发展展望

自 DES 产生的二十多年里，对它最有效的攻击仍然是穷举攻击方式，1999 年 1 月"DES 破译者"在分布式网络的协同工作下，用 22 小时 15 分钟找到了 DES 的密钥，这意味着 DES 已经达到了信任重点，但为了充分利用有关 DES 的现有软件和硬件资源，人

(下转第 309 页)

没有防火墙也提供了对网内主机天然的保护。所以潜在的可能是其它恶意主机通过 ipv6 网络能直接的绕过天然的屏障攻击你，一些自动隧道建立方式能在你不知情的情况下创建对外通道。所以对网络管理员来讲必须定义好安全边界，在必要的边界路由器上设置好安全和过滤规则。IPv6 不会改变运行在传输层之上的任何应用。目前，在 IPv4 应用上存在的威胁在 IPv6 应用上也同样存在。例如，你的双栈 Web 服务器很容易受跨站脚本攻击，那么当使用 IPv6 作为 Layer 3 协议时也仍然是会受到攻击的。下一代的 Internet 协议 IPv6 主要是为了引进一个更大型的地址空间，但是在 Web 安全性方面几乎没有任何提高。主要的原因是 Web 安全性是一个与应用安全性相关的（这些攻击包括 SQL 注入，跨网站脚本等等）；同时，应用安全性是在部署了新的 IPv6 后仍然与网络层完全独立的。

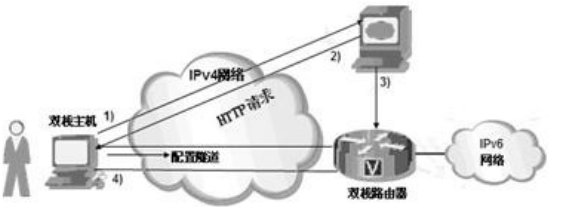

图 3 主机和 ipv6 网络连接常用的方式

3）NAT-PT 技术：NAT-PT 技术通过 SIIT 协议转换技术和 IPV4 网络中的动态地址转换技术与应用层网关相结合，实现纯 IPV4 节点与纯 IPV6 节点间的通信。NAT-PT 作为通信的中间设备，可在 IPV4 与 IPV6 网络间转换 IP 报头的地址（NAT），同时根据协议不同对分组做相应的语义翻译（PT），从而使纯 IPV4 与纯 IPV6 节点间进行透明的通信。

3 结束语

我们需要采取相应的措施，配套完善的安全组织和策略体系，积极拓展以 IPv6 为基础的网络安全业务，提升 IPv6 网络整体安全水平，达到网络安全纵深防御的目标，形成安全可管可控的 IPv6 网络架构，推动下一代网络安全应用的发展。

参考文献：

[1] 李津生.下一代 Internet 网络技术[M].北京:人民邮电出版社,2001.
[2] 中国教育和科研计算机网[EB/OL].http://www.cernet.edu.cn.
[3] 郭洪涛.IPv6 网络的安全技术研究[D].南京:南京理工大学,2007:19-21,40-43.

（上接第 296 页）

们开始提出针对 DES 的各种改进方案，一种简单的方案是使用多重 DES 加密算法。3DES 算法（3 重 DES 算法）是扩展 DES 密钥长度的一种方法，可使加密密钥长度扩展到 128 比特（其中有 112 比特是有效位）或 192 比特（其中 168 比特是有效位），从而大大提高 DES 的安全性与有效性。

使用 3DES 可以很好地抵抗中途相遇攻击。3DES 有 4 种模式：

1）DES-EEE3 模式：在该模式中共使用 3 个不同密钥，顺序使用 3 此 DES 加密算法。

2）DES-EDE3 模式：在该模式中共使用 3 个不同密钥，一次用加密-解密-加密算法。

3）DES-EEE2 模式：在该模式中共使用 2 个不同密钥，顺序使用 3 次 DES 加密算法，其中第一次和第三次加密使用的密钥相同。

4）DES-EDE2 模式：在该模式中共使用 2 个不同的密钥，一次使用加密-解密-加密算法，其中加密算法使用的密钥相同。

但 3DES 的缺点是加、解密速度比 DES 慢。

总之，基于 DES 的加密算法，其设计思想与理念非常严谨，精密，它的诞生对密码技术是个重要的突破与贡献，在最近几十年的现代信息安全中起到重大作用，但随着芯片的运算速度不断加快，针对 DES 攻击为主要目的的专用密码破译机在不断的升级，信息安全领域存在着前所未有的挑战，尽管 AES 已经取代了 DES，但 DES 仍是迄今为止世界上使用最广泛的分组加密算法。它的基本理论和设计思想仍有重要的参考价值，这就要求我们在原有 DES 算法的基础上，不断地加以探索、研究、创新。

参考文献：

[1] 刘晓敏.网络环境下信息安全的技术保护[J].情报科学,1999,17(2).
[2] 张焕国,冯秀涛,覃中平,等.演化密码与 DES 的演化研究[J].计算机学报,2003,26(12).
[3] 沈昌祥,张焕国,冯登国,等.信息安全综述[J].中国科学(E 辑:信息科学),2007(2).
[4] 谷利泽,郑世慧,杨义先.现代密码学教程[M].北京:北京邮电大学出版社,2009.