DOI:10.16184/j.cnki.comprg.2009.04.012

DES 算法原理及实现

管莹，敬茂华
（东北大学秦皇岛分校计算机工程系，秦皇岛 066004）

摘 要： DES 算法是一种通用的计算机加密算法，主要用于民用加密。本文深入地剖析了 DES 算法的原理及运算过程，并给出了该算法 C 语言实现的代码解析，最后简要说明了其安全性。

关键词： DES；加密；原理；密钥

The Principle and Implement of DES Algorithm

GUAN Ying, JING Maohua
（Computer Engineering Department of Northeastern University at Qinhuangdao, Qinhuangdao 066004）

Abstract: DES is the most popular encryption Algorithm, it is used mostly in popular encryption. This paper analyzes and Research of the principle and the implement of DES Algorithm, and analyzes it's program script of C. At last, it presents the security of DES Algorithm.

Key words: DES; encryption; principle; security

1 引言

随着计算机网络的飞速发展，产生了大量的电子数据。这些电子数据在网络的传输过程中受到了很多威胁。现代密码学的应用保证了电子数据的保密性、完整性和真实性。

未作任何处理的消息称为明文，用某种方法伪装消息以隐藏其内容的过程称为加密，加密后的消息称为密文。将密文转换为明文的过程称为解密。密码算法也称密码函数，是用于加密和解密的数学函数。如果算法本身是保密的，这种算法称为受限算法。受限算法不可能进行质量控制或标准化。现代密码学利用密钥解决了加密算法的受限性。

基于密钥的算法的安全性在于其密钥的安全性，其算法本身是公开的。基于密钥的算法通常有两类：对称算法和公开密钥算法。对称算法又称为传统密码算法。对称算法的对称性体现在加密密钥能够从解密密钥推算出来，反之亦然。在大多数对称算法中，加解密的密钥是相同的。可见，对称密钥算法的加解密密钥都是保密的。而公开密钥算法的加密密钥是公开的，解密密要是保密的。

对称密钥算法又分为两种：分组密码和流密码。分组密码将明文分割为若干个定长的数据块（称为一个分组），每次对一个分组进行处理；流密码又称序列密码，依次对输入每个元素进行处理。

DES 算法是一种最通用的对称密钥算法，属于分组密码算法。DES 主要用于民用敏感信息的加密。该算法是 IBM 公司于 1975 年研究成功并公开发表的，于 1977 年 7 月 15 日得到美国国家标准局的正式许可，作为联邦信息处理标准 46 号，供商业界和非国防性政府部门使用。

2 DES 算法剖析

2.1 DES 算法加解密过程

DES 算法的加密由四部分完成，分别为：初始置换函数 IP、子密钥 Ki 及获取、密码函数 F、末置换函数 IP^{-1}。

DES 的分组长度为 64 位（比特）。初始置换函数 IP 接受长度为 64 位的明文输入，末置换函数 IP-1 输出 64 位的密文。在子密钥的获取过程中，通过密钥置换 PC-1 获取从 K1 到 K16 共 16 个子密钥，这 16 个子密钥分别顺序应用于密码函数的 16 次完全相同的迭代运算中。如图 1 所示。

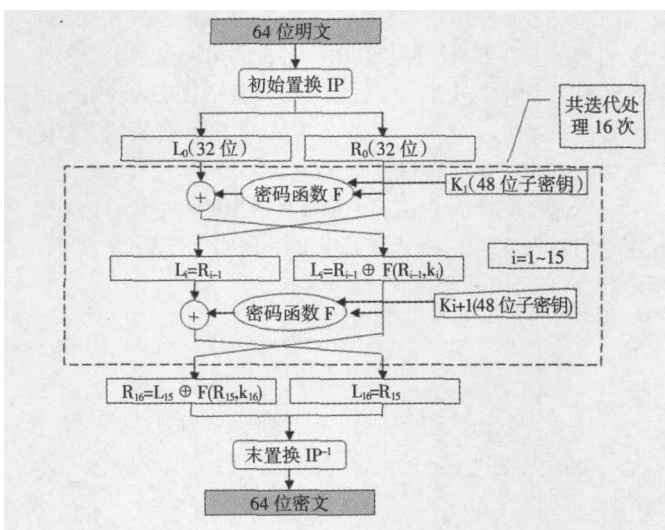

图 1 DES 加密过程

DES 的解密算法与加密算法完全相同，只需要将密钥的应用次序与加密时相反应用即可。即解密过程是初始置换函数 IP 接受长度为 64 比特的密文输入，将 16 个子密钥按照 K16 到 K1 的顺序应用与函数 F 的 16 轮迭代运算中，然后将迭代的结果经由末置换函数 IP-1 得到 64 位的明文输出。

2.2 DES 算法运算过程

DES 主要采用置换和移位运算来实现加解密，接下来深入剖析 DES 每个部分运算的实现过程。

（1）初始置换函数 IP

本文收稿日期：2008 年 10 月 26 日

64 位的明文分组 x 首先经过一个初始置换函数 IP 进行置换运算，产生一个 64 位的输出 x0，该输出被分成两个分别为 32 位的左半部分 L0 和右半部分 R0，用于 F 函数的 16 轮迭代运算的首次迭代的初始输入。

初始置换函数 IP 实际上就是一张 8×8（8 行 8 列）的迭代表，如表 1 所示。明文分组中的 64 位按照表中的规定重新进行排序，其排列顺序为从左到右，从上到下。按表 1 所示，明文中的第 58 位被放置在 x0 的第 1 位，第 50 位防止在第 2 位，依次类推。

表 1 初始置换函数 IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

L_0 R_0

(2) 获取子密钥 Ki

子密钥的获取主要通过置换和移位运算来实现。

DES 加密算法的密钥长度为 56 位，由用户提供，是 DES 算法的输入之一。但用户输入的密钥是 64 位的，按 8 行 8 列从左到右从上到下地排列，其中，每行的第 8 位用于奇偶校验。在 DES 加密算法中，子密钥获取过程中，DES 经过一系列的置换和移位运算，得到 K1 到 K16 共 16 个子密钥，每个子密钥长 48 位。其实现过程如下：

首先将输入的 64 位密钥去掉最后一列的 8 个校验位，然后用密钥置换函数 PC-1 对剩下的 56 位密钥进行置换，如表 2 所示。

表 2 密钥置换函数 PC-1

57	49	41	33	25	17	9	
1	58	50	42	34	26	18	C_0
10	2	59	51	43	35	27	
19	11	3	60	52	44	36	
63	55	47	39	31	23	15	
7	62	54	46	38	30	22	D_0
14	6	61	53	45	37	29	
21	13	5	28	20	12	4	

由表 2 可知，用户输入的 64 位密钥中，第 8、16、24、32、40、48、56、64 共 8 个校验位被去掉。剩余的 56 位按表 2 所示排放：第 57 位放在第 1 位，第 49 位放在第 2 位，依次类推。

经过 PC-1 置换后，将其置换的输出再分为前 28 位 C0 和后 28 位 D0 和两部分，上一轮置换得到的输出的两部分经过循环左移 1 位或 2 位后，每轮按表 3 进行移位，然后将两部分合并成 56 位，之后经过压缩置换 PC-2 后得到当前这轮置换的 48 位子密钥。压缩置换 PC-2 如表 4 所示。

表 3 每轮移动的位数

轮数	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
位数	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

表 4 压缩置换 PC-2

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

PC-2 置换为压缩置换，即置换后的输出数据的位数要比置换前输入的位数要少，即某些位的数据在置换的过程中被去掉了。由表 4 可知，在压缩置换过程中，原来的 7 行 8 列共 58 位数据被压缩成 8 行 6 列的 48 位数据。在压缩置换过程中，第 9、18、22、25、35、38、43、54 共 8 位数据被丢掉。

同时，将上一轮移位后得到的两部分再按表 3 进行移位，作为下一个子密钥产生的 PC-2 置换的输入。依次经过 16 次循环左移和 16 次置换得到 16 个子密钥。其产生过程如图 2 所示。

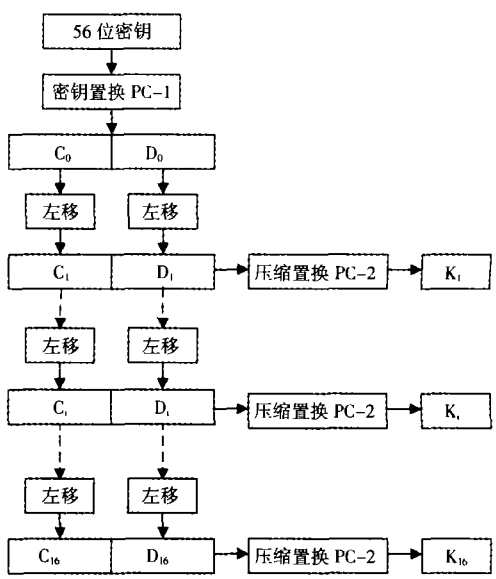

图 2 子密钥 Ki 的产生

(3) 密码函数 F

密码函数 F 接收两个输入：32 位的数据和 48 位的子密钥。函数 F 的运算过程为：

1) 先将数据的右半部分 Ri 通过扩展置换 E 从 32 位扩展为 48 位。之所以称为扩展置换，是因为置换后的数据比置换前的数据的位数要多。扩展置换（E）通过将原 32 位数据中的某些位重复出现达到扩展的目的。其置换函数如表 5 所示。

扩展置换也称位选择函数，俗称 E 盒。

由表 5 可以看出，扩展置换（E）通过将第 32、1、4、5、8、9、12、13、16、17、20、21、24、25、28、29 共 19 位分别放置在两个位置，从而将 32 位的数据扩展为 48 位。

表 5 扩展置换（E）

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

2）接着将扩展置换后的 48 位输出 E（Ri）与压缩置换后的 48 位密钥 Ki 作异或运算。

3）将异或运算得到的 48 位结果数据分成 8 个 6 位的块，将每一块通过对应的一个 S 盒产生一个 4 位的输出。每个 S 盒实际上是一张 4（0~3）行 16（0~15）列的置换表，注意，S 盒的行列编号都是从 0 开始的。显然，需要 8 个 S 盒，每个 S 盒如表 6 所示。

S 盒接收 6 位的输出，经过置换输出 4 位的数据，其具体置换过程为：将 6 位输入中的第 1 位和第 6 位取出来形成一个 2 位的二进制数 x（从 0~3），该数得出 S 盒的行数，然后将 6 位输入的中间 4 位构成另一个二进制数 y（从 0~15），该数为 S 盒的列数，然后查出 S 的 x 行 y 列所对应的整数，将该整数转换为一个 4 位的二进制数，即为 S 盒的输出。例如，假设输入数据中的第一个 6 位数字块为 010111，则需要通过查 S1 盒。先取出 010111 中的第 1 位和第 6 位，组成二进制数 01，则行数 x=1，然后取出中间的 4 位 1011，则得列数为 y=11，在 S1 盒中，第 1 行第 11 列的整数为 11（表 6 中灰色背景处），转换为二进制为 1011，则输出 1011，即用 4 位的 1011 代替 6 位的 010111。

4）将 3）中 8 个 6 位数据的置换结果连在一起，形成一个 32 位的输出，输出结果再通过一个 P 盒置换产生一个 32 位的输出。P 盒置换如表 7 所示。

最后，P 盒置换的结果与左半部分进行异或运算，然后将左右两半部分交换，之后进入下一轮迭代。在完成完全相同的 16 轮运算后，将得到的两部分数据合在一起，再经过一个末置换函数 IP-1 即可得到 64 位的密文。

末置换函数 IP-1 是初始置换 IP 的逆运算，如表 8 所示。

3 DES 算法的安全性

DES 算法具有相当高的复杂性，起密码函数 F 的非线性性质非常好，起到的“扰乱”效果非常显著，并且还遵循了严格雪崩准则（SAC）和比特独立准则（BIC），这使得要破译它的开销要超过可能获得的利益。再加上其便于理解掌握，经济有效，因此，得到了广泛的应用。

表 6 S 盒

S1 盒	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S2 盒	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S3 盒	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S4 盒	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S5 盒	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S6 盒	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S7 盒	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S8 盒	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

表 7 P 盒置换

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

DES 算法具有极高的安全性，到目前为止，除了用穷举搜索法对 DES 算法进行攻击外，还没有发现更有效的办法。

（下转到 13 页）

第 12 条测试通过 (√) :期望值是:*baa,实际值是 *baa
第 13 条测试通过 (√) :期望值是:null,实际值是 null
第 14 条测试通过 (√) :期望值是:null,实际值是 null
第 15 条测试通过 (√) :期望值是:null,实际值是 null
第 16 条测试通过 (√) :期望值是:,实际值是
第 17 条测试通过 (√) :期望值是:,实际值是
共执行测试用例 17 笔;成功 15 笔; 失败 2 笔;

2.2.6 修整

根据测试结果，对程序进行修改，直到测试用案例全部通过，即测试完成。

使用 JUnit 通过测试驱动的开发来实现单元测试时，是以测试失败为开端的，这是意料之中的结果。如果它不失败，那就意味着测试的设计或实现出了问题。测试类会逐一运行已经设计好的全部测试用例，如果有测试用例运行失败，整个测试也将失败，失败的原因反应的就是工具类的缺陷，需根据失败原因再对工具类进行修改，当所有测试用例全部运行通过，工具类的实现也随之完成。

2.3 数据说明

表 1 中的“实际结果”项是测试驱动执行后测试驱动程序自动填入的，测试驱动自动比较“预期结果”和“实际结果”是否相等，如何相等则在“比较结果说明”中填“√”，不相等则在“比较结果说明”中填“×”。所以，测试人员对测试结果的检查只要查看测试用例表的执行结果就可以了。

3 结语

测试是开发过程中的重要阶段，测试工具对软件测试的有效性、成本、时间、可靠性等方面起到关键作用。而测试工具又有商业和开源之分，许多开源的测试工具功能强大并且具有非常好的开放性，但测试人员需要经过不断的摸索和研究，才能很好的运用。JUnit 给开发者的单元测试带来了极大的方便，但是大多使用者对其应用掌握不深。本文分析了利用 JUnit 进行单元测试的全过程，并结合实例研究了测试驱动的开发，起到抛砖引玉的作用。

作者简介

杜庆峰，男（1968-），同济大学副教授，研究方向：软件项目管理与质量控制、软件测试。

韩梅，女，同济大学软件学院软件工程专业研究生。

（上接第 7 页）

而 56 位长的密钥的穷举空间为 256，这意味着如果一台计算机的速度是每一秒种检测一百万个密钥，则它搜索完全部密钥就需要将近 2285 年的时间。然而，这并不等于说 DES 是不可破解的。而实际上，随着硬件技术和 Internet 发展，其破解的可能性越来越大，而且，所需要的时间越来越少。

表 8 末置换函数 IP-1

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

为了克服 DES 密钥空间小的缺陷，人们又提出了三重 DES 的变形方式。

此外，DES 算法也存在一些漏洞，比如，DES 算法中只用到 64 位密钥中的其中 56 位，而第 8、16、24、.....64 位 8 个位并未参与 DES 运算，即 DES 的安全性是基于除了 8、16、24、.....64 位外的其余 56 位的组合变化 256 才得以保证的。因此，在实际应用中，应避开使用第 8、16、24、.....64 位作为有效数据位，而使用其他的 56 位作为有效数据位，才能保证 DES 算法安全可靠地发挥作用。如果不了解这一点，把密钥 Key 的 8、16、24、.....64 位作为有效数据使用，将不能保证 DES 加密数据的安全性，对运用 DES 来达到保密作用的系统产生数据被破译的危险，这正是 DES 算法在应用上的误区，留下了被人攻击、被人破译的极大隐患。

4 总结

本文介绍了 DES 算法的原理和运算过程，以 C 语言程序代码为例介绍了该算法的实现，并分析了 DES 算法的安全性。

尽管 DES 存在有一些不足，但作为第一个公开密码算法的密码体制，它成功地完成了它的使命。并且，由于破解 DES 算法的花费可能远远要大于破解其的收益，因此，在民用电子数据的加密上，DES 算法依旧是一个理想的选择。

参考文献

[1] 胡建伟. 网络安全与保密. 北京：西安电子科技大学出版社，2003.
[2] 石志国. 计算机网络安全教程. 北京：清华大学出版社，北京交通大学出版社，2004.
[3] Susan Yong Dave Aitel. The Hacker’s Handbook The Strategy behind Breaking into and Defending Networks.北京:机械工业出版社，2006.
[4] 牛少影，江为强. 网络的攻击与防范一理论与实践. 北京：北京邮电大学出版社，2006.
[5] 刘远生. 计算机网络安全. 北京：清华大学出版社，2006.

作者简介

管莹，女（1979-），东北大学秦皇岛分校计算机工程系讲师，主要研究方向：计算机网络。

敬茂华，女（1977-），东北大学秦皇岛分校计算机工程系讲师/硕士，主要研究方向：计算机网络及信息安全技术，数据库应用。