网络传输中的数据保护软件 WDES

吴 维 （*Memorex Telex* 公司北京代表处）

摘要：本文介绍一个防止网络数据泄密的加密软件。

一、引言

网络作为商业通信手段，往往要传送如财务数据、员工记录和公司分类产品资料等敏感和私人数据。随着网络在企业通信上的角色日益重要，现今局域网规模日趋庞大，以至于连接大型广域网络，使得网络保密性问题成为公众的焦点。

针对这个问题，美国联邦标准局公布第 46 号信息数据加密标准，防止出现在以太网上偷盗信息和其它没经授权用户获取不应获取的信息。该标准用于美国非联邦政府组织，并被鼓励在商业和私人组织中使用。基于此标准，作者实现了加密软件 WDES，该软件用于 DOS、UNIX 联网环境，它把以太网的开放存取、广播方式转换为个人与个人之间的联系。目前，在 1994 年 4 月开业的、由中国国家外汇管理局主管的全国外汇交易中使用。该软件可对文本文件、运行文件进行加密。加密方法是通过用户给出的 8 个字符的口令，经过一系列变换达到加密目的，被加密的文件变成不可视文件，其长度增长 8 个字节，因为口令也用同样的方法加密，并存放到被加密文件的前面。解密时，根据给出的口令是否正确，以决定是否解密。

该软件通过 8 个字节的口令，即 64 位的数据块对文件进行加密和解密。加密和解密都要用同样的关键字，但过程相反。要加密的数据块首先通过一个初步矩阵变换 IP，然后是一个复杂的基于口令的矩阵变换；最后是逆初步矩阵变换 IP−1。基于口令的矩阵变换由加密／解密函数 f 和口令置换矩阵 K_1、…、K_{16} 构成。下面将分别描述加密过程，解密过程，以及所用到的加密函数 f 和口令置换矩阵 K_1、…、K_{16}。

定义：对于给定的两个位块 L 和 R，LR 表示首先是块 L 的位，然后是块 R 的位。

例如：8 位块 L 是 01100110，8 位块 R 是 10011001，则 LR 为 16 位块，即 0110011010011001。

WDES 把需要加密或解密的文件分成一系列 8 个字节的数据块，即一系列 64 位数据块，每个数据块做为一个加密单元进行加密或解密。不足 8 个字节的剩余数据不做任何处理。

注：在本文中，L_0，…，L_{16}，R_0，…，R_{16} 是 32 位数据块，K_1，…，K_{16} 是 48 位数据块。

二、加密

图 1 表示加密计算的流图：

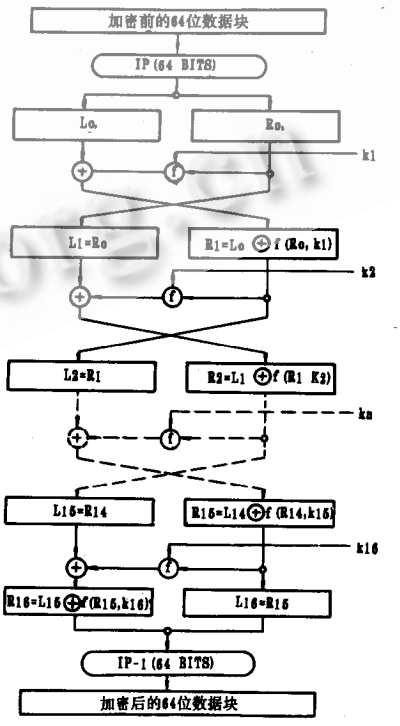

图 1 数据加密过程

原始初步矩阵置位 IP 如下:

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

例如，设 A，B 为 64 位数据块，即 1 * 64 矩阵，且 B=IP(A)

则 B[1]=A[58], B[2]=A[50], 等等。以下同此。

加密／解密函数 f，口令置换矩阵 $K_1, \cdots, K_{16}$ 分别在第四和第五部分描述。

逆原始初步矩阵置位 IP-1 如下:

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
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

三、解密

解密计算如图 2 所示:

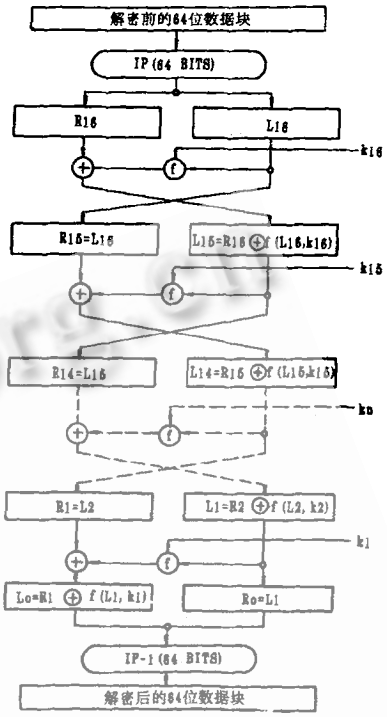

图 2　数据解密过程

四、加密／解密函数 f

图 3 描述加密／解密函数 f 的运算过程:

其中:矩阵 E 如下

E 位选择表

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

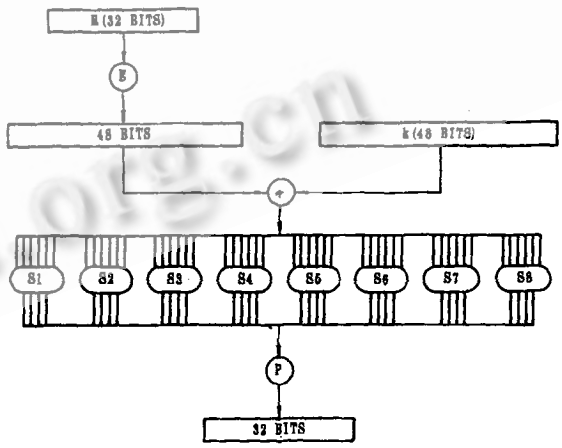

图 3　加密／解密函数 f 的运算过程

选择函数 S1-S8 如下:

对于 6 位数据块 B(b1 b2 b3…b6)和函数 S1，有

S1(B)=S1[(b1 × 2+b6),(b2 × 8+b3 × 4+b4 × 2+b5)]

例如:B=b1 b2 b3 b4 b5 b6=011011

则:b1=0, b2=1, b3=1, b4=0, b5=1, b6=1

S1(B)=S1[1,13]=5

S2 至 S8 的变换同 S1。

置换函数 P 如下:

P			
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

由以上可以看出:

$B1\ B2\cdots B8 = E(R) \oplus Kn$

$f(R,K_n) = P(S1(B1).S2(B2)\cdots S8(B8))$

其中: E(R)的值是 48 位数据块, R 是 32 位数据块,

Kn 为口令置位矩阵 K_1、…、K_{16},

B1、B2…、B8 为 6 位数据块,可得 B1 B2…B8 为 48 位数据块。

五、口令置位矩阵 K_1、…、K_{16}

图 4 描述口令置位矩阵 K_1、…、K_{16} 的计算方法:

由图 4 可以看出,口令字通过置换矩阵,Pc-1, Pc-2 及一系列左移,可得到 K1, …, K16。

数据块 Cn, Dn 的左移次数 LS 如下:

n=	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
LS=	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

六、结论

该软件 WDES 目前已经商品化,并在实际中运用。理论上讲所有加密工具都可以被破释,WDES 也存在这种可能,但其被破译的可能性是 7×10^6 分之一。希望 WDES 能对国内信息界提供良好的保护。

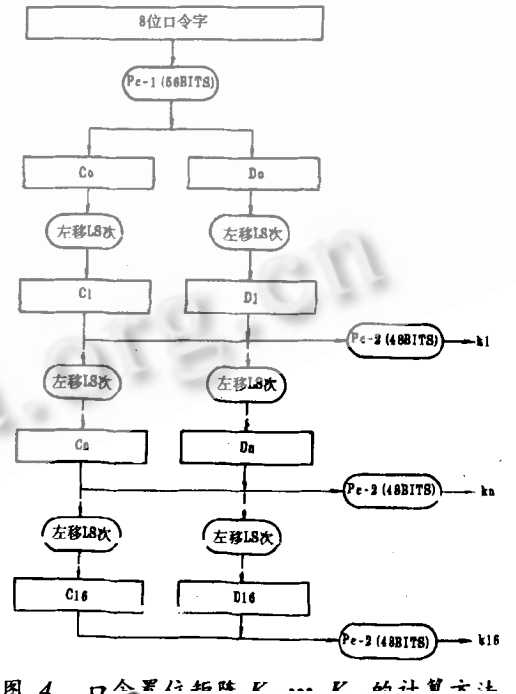

图 4 口令置位矩阵 K_1、…、K_{16} 的计算方法