

# 基于 DES 算法的测发控系统无线通讯加密方案

范峻豪,柴 波,成 龙

(西安微电子技术研究所,陕西 西安 710054)

**摘 要:** 针对无线通讯应用于导弹地面测发控系统时,可能造成信息泄露等问题,提出了一种基于 DES 算法的加密方案.该方案在明文数据中加入可变的冗余码,保证了加密可靠性;在加密后的密文数据包之间嵌入随机标识码,使得通讯数据的结构有效隐藏,并为接收端恢复数据提供支持.分析可知,该方案易于实现,保密性好,适合应用于导弹测发控系统中.

**关键词:** 测发控系统;无线通讯;DES 算法;加密方案

**中图分类号:** V55

**文献标识码:** A

**文章编号:** 1000-7180(2018)11-0134-05

## Encryption Scheme of Wireless Communication in Missile Launch Control System Based on DES Algorithm

FAN Jun-hao, CHAI Bo, CHENG Long

(Xi'an Microelectronics Technology Institute, Xi'an 710054, China)

**Abstract:** Aiming at the problems of information disclosure when the wireless communication is applied to the missile launch control system, an encryption scheme based on DES algorithm is proposed. The scheme adds redundant code in sending data, which ensures the reliability of encryption. It uses random identification code in received data to effectively hide the data structure of ciphertext, and provides support in data recovery at receiving end. Analysis shows that the scheme is easy to implement and good in security, suitable for use in missile launch control system.

**Key words:** missile launch control system; wireless communication; DES algorithm; encryption scheme

### 1 引言

导弹地面测发控系统一般包含前端测试设备和后端控制设备<sup>[1]</sup>.传统的前后端通讯采用物理总线,需临时铺设电缆网,在执行任务时十分不便,而无线通讯无需电缆,发射效率高,有利于保障发控人员的安全.但是无线通讯由于其开放性面临着很多信息安全上的风险,例如弹上参数信息泄露,发射程序被敌方劫持等.数字加密技术可以解决无线通讯安全上的问题,发挥无线通讯的优势.

DES(Data Encryption Standard)算法<sup>[2]</sup>是一种经典分组加密算法,安全性高,能够应对各种破解方式,且易于实现.但是 DES 算法在应用于地面测发控系统时,由于同样的命令整体作为明文加密将产生同样的密文,容易遭受概率统计等方式的攻击,另

外,作为分组密码,密文中每 1 bit 的缺失或错位都会导致其恢复出错<sup>[3]</sup>.

针对上述不足之处,本文提出了一种基于 DES 算法的无线通讯加密方案.该方案通过在明文加入冗余码以及在通讯码流中嵌入随机标识码序列等措施,既有效保证了通讯数据的安全,又能进行简单的身份认证,非常适合应用于导弹地面测发控系统中.

### 2 基于 DES 算法的加密方案

#### 2.1 DES 算法的加密过程

DES 算法的加密过程包括初始置换 IP, 16 轮迭代,逆初始置换 IP 以子密钥产生等.其流程图如图一所示.

#### 2.2 冗余码的设计

在使用 DES 算法加密之前,我们将连续 56 bit

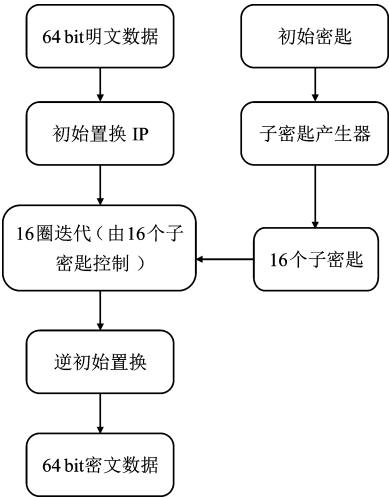


图 1 DES 算法加密流程

的有效通讯数据分为一组,每组在最后加入 8 bit 冗余码,形成 64 bit 的明文分组后再进行加密.冗余码从二进制 0000 0000 到 1111 1111 依次循环递增使用.其原理如图 2 所示.

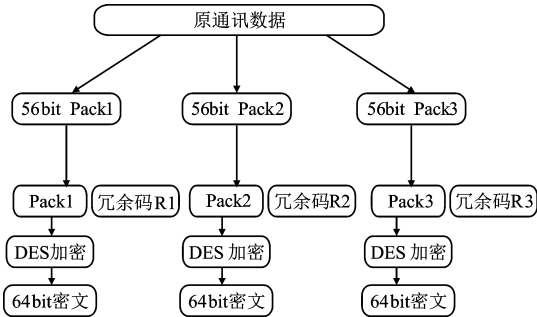


图 2 冗余码设计原理

初始密钥由 DES 密钥产生器产生,分别交给发送和接收端.发送端将初始密钥经过置换选择 PC-1、循环移位运算、置换选择 PC-2 后,产生 16 个子密钥用于加密程序的 16 圈迭代.下面给出了一个加密示例:

将一组数据 Pack:B5 D8 C3 E6 B2 E2 B7 加入不同的冗余码后使用相同密钥加密.

1、Pack 加入冗余码 0000 0001 作为明文 1:  
B5 D8 C3 E6 B2 E2 B7 01

加密得到密文 1:B8 43 E3 F9 01 75 8D 52

2、Pack 加入冗余码 0000 0010 作为明文 2:  
B5 D8 C3 E6 B2 E2 B7 02

加密得到密文 2:D8 FF E9 AE 17 3B B3 5B

3、Pack 加入冗余码 0000 0011 作为明文 3:  
B5 D8 C3 E6 B2 E2 B7 03

加密得到密文 3:99 38 AA 6E F9 CA F3 65

如上例所示,在不同分组中,即使有效数据完全一样,加入冗余码后组成的明文经过加密后所得的密文也会完全不同.冗余码取值从 0x00~0xFF 依次递增,256 次一循环,相同数据使用相同冗余码的概率极低.虽然加入冗余码会产生一定的数据扩展,但其扩展率只有  $64/56=1.1429$ ,并不会对通讯效率造成太大影响.

冗余码的添加可以在牺牲少许通讯效率的条件下,极大的消除明文和密文的统计相关性,确保了加密的可靠性.由于冗余码是按照循环递增的关系依次填入明文中,在接收端使用解密算法得到明文后,既可以通过前后数据包冗余码的比较判断通讯的质量(数据包丢失的状况),进而选择进行丢包反馈和重传等操作,也可以将冗余码作为一种数字签名来认证数据发送方的身份,避免通讯被劫持.

2.3 随机标识码序列设计

DES 算法中加密和解密均为 64 bit 数据一组.接收端将密文恢复前,需要将同组密文挑出,整体进行解密处理.为了方便解密分组,数据在发送前需要在每一组密文之间插入一个 8 位标识码,作为一组数据的结束和新一组数据的开始,如图 3 所示.但是标识的存在无疑将密文数据格式暴露在攻击者面前,方便了攻击者的数据分析.为了隐藏通讯数据流的数据结构,本文采用一种随机标识码,代替固定的标识码.实现过程如下:

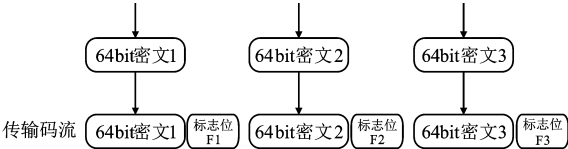


图 3 密文标识码示意图

```
(1)使用计算机产生随机码序列,代码如下:  
intrandomflag(char radflag[256])  
{  
    int rad;  
    char mid;  
    for(int i=0;i<256;i++)  
    {  
        memcpy(&radflag[i],&i,1);  
        //初始化序列表  
    }  
    srand((unsigned)time( NULL ));  
    //使用系统当前时刻作为初始种子  
    for(int i=0;i<256;i++)
```

```
{
rad=rand()%255;    //生成随机数
mid=radflag[i];
radflag[i]=radflag[rad]; //换位操作
radflag[rad]=mid;
}
return 0;
}
```

该程序将 256(0x00~0xFF)个 8bit 数按顺序放入一个包含 256 个元素的表中,然后从第一个元素开始依次与其他元素随机互换位置,从而产生一张随机码序列表。

(2)以上方法产生的随机码序列表前端和后端各一份;

(3)发送端从随机码序列表中依次取出各元素作为标识码嵌入数据流的加密分组之间。

其中随机码序列表中每一个元素都是随机的,其随机性主要靠两方面来保证:rand()函数随机数的产生和换位操作的普遍性。

rand()函数是以一个数(称其为种子)为基准,以某个递推公式推算出来一系列数,只要每次运用不同的种子值,就可以产生不可预见的随机序列<sup>[4]</sup>。本文使用 srand()函数调用系统的当前时刻作为初始种子,每次调用的时刻都具有不可预见性和随机性,可以很好地作为 rand()函数产生随机序列的种子,从而保证了函数运行结果的随机性。

每一个元素在表中的次序都会经历一次或多次随机换位操作。例如初始次序表中第 10 位为 00001010,在第十次换位操作中会和表中第  $rad_{10}$  位的数据主动换位( $rad_{10}$  为 rand()函数第十次产生的随机数)。除此之外,00001010 也有可能在其他换位操作中被动换位。序列表中每一个数的位置都会改变,这样能够最大程度的保证序列表的混乱度。

图 4 为序列表生成实例(部分):

序列表中每一位数的值单独来看都是 0x00 到 0xFF 中随机的一个,并且每一个数都不重复,所以相互之间没有线性关系。用其作为密文分组的标志位,在只有通讯双方掌握相同随机码序列表的情况下,接受端才可以有效获取完整的密文分组,进而进行解密运算。并且标识位的随机性能够很好地隐藏通讯码流的数据结构,使攻击者的分析行为无法进行,增强了通讯的安全性。随机序列码表产生方便,可以频繁更换,对于防范暴力破解具有极大的优势。

|                                          |
|------------------------------------------|
| 0x28,0x63,0x7e,0x2c,0x62,0x41,0x37,0x3f, |
| 0xe6,0x42,0x26,0x40,0x73,0x2d,0x3b,0x39, |
| 0xee,0x9e,0x78,0x46,0x8f,0xea,0x0b,0xec, |
| 0x6c,0x4a,0x58,0xda,0x92,0x96,0x4f,0x21, |
| 0x01,0x76,0x53,0xdh,0x9c,0x3c,0x9f,0xae, |
| 0x8d,0x08,0xa2,0xef,0xf3,0xf1,0xe2,0x98, |
| 0xf9,0x93,0xdd,0xab,0xfb,0x00,0xbb,0x9d, |
| 0x15,0xa5,0x4b,0x85,0xe4,0xd2,0x24,0x2b, |

图 4 序列表生成实例

2.4 加密方案总体流程

综上所述,本文提出的基于 DES 算法的加密过程可用图 5 所示流程图表示:

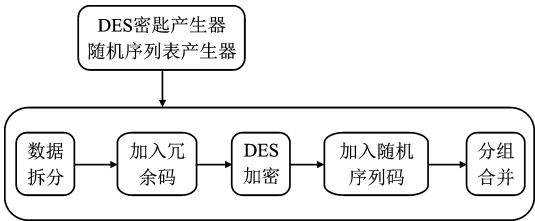


图 5 加密流程图

3 解密流程

解密是把物理信道获得码流经过密文分组提取、DES 解密、剔除冗余码等操作得到有效明文的过程。其流程图如下图所示:

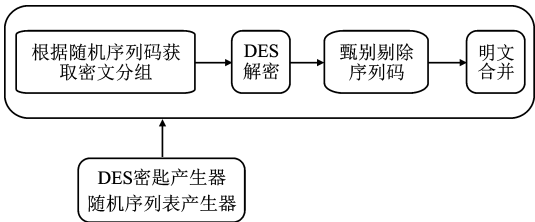


图 6 解密流程图

3.1 获取密文分组

随机码序列表由生成器生成后,交给接收端作为分组依据。接收端从序列表中依次提取元素数作为标识码,从收到的码流中寻找标识码作为密文分组开始的标志。其实现代码如下:

```
int (char recvdata[],int num)
{
int posinow=0;    //检索位置
char miwen[64]={0}; //存放提取的密文
while (posinow<num)
```

```
{
    posinow = searchflag (recvdata, posinow, rad-
flag[flagnow])
    /* 检索函数,从 posinow 开始返回第一个标识
位位置,全局变量 radflag 为随机码序列表,flag-
now 当前标识码序号 */memcpy (miwen,
&recvdata[posinow+1],64); //提取密文分组
    posinow=posinow+65;
    jiemi(miwen); //后续解密操作
    flagnow=flagnow<255? flagnow+1:0;
    //更新标识码
}
return posinow;
}
```

3.2 DES 解密

DES 是一种对称加密算法,其加解密算法相同,使用同一套代码,只需将子密匙的使用顺序颠倒即可<sup>[5]</sup>. 例如,加密的时候 16 圈迭代使用的子密匙依次是 k1,k2,...,k16,那么解密时进行 16 圈迭代时依次使用 k16,k15,k14,...,k1. 对得到的 64 bit 密文分组整体进行解密运算后得到 64 bit 明文分组.

3.3 剔除冗余码

经过 DES 解密后得到的明文分组还包含 8 位冗余码. 冗余码在添加的时候是按照顺序添加的,所以可以通过前后冗余码的比较判断数据包的缺失. 与前后冗余码没有线性关系的数据包可以作为虚假包丢弃,以防止敌方伪装的数据包混入,对通讯进行劫持,造成发射事故. 剔除冗余码后的明文重新组合在一起作为解密接收的最终结果.

4 方案验证

以下为一组需要传输的数据:

发送数据:BB F9 D3 DA 44 45 53CB E3 B7 A8 B5 C4 B2E2 B7 A2 BF D8 CF B5CD B3 CE DE CF DF CDCB E3 B7 A8 B5 C4 B2A8 D1 86 BC D3 C3 DCB7 BD B0 B8 CE F7 B0B2 CE A2 B5 E7 D7 D3CB E3 B7 A8 B5 C4 B2BC BC CA F5 D1 D0 BEBF CB F9 B1 A3 C3 DCCB E3 B7 A8 B5 C4 B2

初始密匙 KEY:B3 F5 CA BC C3 DC B3 D7

随机标志位序列表: 31 5D 79 61 7f 10 69 1A DF 6B D0 27 65 .....

加密过程:

(1)先对以上数据进行分组得到下列数据组:

Pack1:BB F9 D3 DA 44 45 53 Pack2:CB E3 B7 A8 B5 C4 B2 Pack3:E2 B7 A2 BF D8 CF B5 Pack4:CD B3 CE DE CF DF CD Pack5:CB E3 B7 A8 B5 C4 B2 Pack6:A8 D1 86 BC D3 C3 DC Pack7:B7 BD B0 B8 CE F7 B0 Pack8:B2 CE A2 B5 E7 D7 D3 Pack9:CB E3 B7 A8 B5 C4 B2 Pack10:BC BC CA F5 D1 D0 BE Pack11:BF CB F9 B1 A3 C3 DC Pack12: CB E3 B7 A8 B5 C4 B2

(2)每组数据添加冗余码作为密文并加密(冗余码用□标注)

密文 1:BB F9 D3 DA 44 45 53 □01明文 1:18 8A E1 7E 8B A6 AF 0F

密文 2:CB E3 B7 A8 B5 C4 B2 □02明文 2:3C 5B F0 9C 25 E9 C0 0F

密文 3:E2 B7 A2 BF D8 CF B5 □03明文 3:B4 CA 7B 8F 92 58 66 6B

密文 4:CD B3 CE DE CF DF CD □04明文 4: 3E E3 ED E4 45 19 51 93

密文 5:CB E3 B7 A8 B5 C4 B2 □05明文 5:59 E5 35 98 DD DE C1 C7

密文 6:A8 D1 86 BC D3 C3 DC □06明文 6:DF 6D CB AF 9A 09 3B AC

密文 7:B7 BD B0 B8 CE F7 B0 □07明文 7: 62 B0 64 23 E9 02 5B 74

密文 8:B2 CE A2 B5 E7 D7 D3 □08明文 8:C3 3D 41 15 E1 7F 7D 1F

密文 9:CB E3 B7 A8 B5 C4 B2 □09明文 9: F2 24 81 00 7B 7D 5B 1F

密文 10:BC BC CA F5 D1 D0 BE □0A明文 10: D2 F7 03 C0 43 73 74 12

密文 11:BF CB F9 B1 A3 C3 DC □0B明文 11: F2 E6 F2 35 2F 5A E9 93

密文 12: CB E3 B7 A8 B5 C4 B2 □0C明文 12: FC 38 17 AA 18 B4 DC 47

(3)添加随机码后合并(随机码用□标注) 合并明文:

□31 18 8A E1 7E 8B A6 AF 0F □5D 3C 5B F0 9C 25 E9 C0 0F □79 B4 CA 7B 8F 92 58 66 6B □61

3E E3 ED E4 45 19 51 93 7F 59 E5 35 98 DD DE  
C1 C7 10 DF 6D CB AF 9A 09 3B AC 69 62 B0  
64 23 E9 02 5B 74 1A C3 3D 41 15 E1 7F 7D 1F  
DF F2 24 81 00 7B 7D 5B 1F 6B D2 F7 03 C0 43  
73 74 12 D0 F2 E6 F2 35 2F 5A E9 93 27 FC 38  
17 AA 18 B4 DC 47 65

解密过程:

(1)从随机码序列表中读取第一个字节 31 作为标识位,在明文中查找从而得到上述明文 1,依次类推依次得到上述明文 2、3…;

(2)依次对明文 1、2、3、…、12 进行 DES 解密运算,得到上述密文 1、2、3、…、12;

(3)将密文 1、2、3、…、12 剔除最后一个字节后分别得到 Pack1、Pack2、Pack3、…、Pack12,将其按顺序连接得到接受数据。

接收数据:BB F9 D3 DA 44 45 53CB E3 B7 A8  
B5 C4 B2E2 B7 A2 BF D8 CF B5CD B3 CE DE CF  
DF CDCB E3 B7 A8 B5 C4 B2A8 D1 86 BC D3 C3  
DCB7 BD B0 B8 CE F7 B0B2 CE A2 B5 E7 D7  
D3CB E3 B7 A8 B5 C4 B2BC BC CA F5 D1 D0  
BEBF CB F9 B1 A3 C3 DCCB E3 B7 A8 B5 C4 B2

将接收数据与发送数据进行对比,发现两组数据完全一致并无异同,说明数据经过该方案加密和解密操作后不会影响数据的真实性。

实例表明该方案能够达到保证通讯安全的目的,并且容易实现,能够很好满足测发控系统的

要求.

5 结束语

本文针对导弹地面测发控系统中前后端设备无线通讯存在的问题,以 DES 算法为基础,引入了冗余码和随机序列码,设计了一种新的加密方案.通过文中分析及实例验证可知,该方案实现简单,在提高算法的保密性能的同时,增强了通讯的纠错能力,使之更适合地面测发控系统前后端无线通讯的数据特征和应用环境.

参考文献:

[1] 杜诚谦, 潘洁伦. 新一代运载火箭地面测试发控系统一体化设计概述[J]. 航天控制, 2004, 22(1):55-57.  
[2] Shneier B. 应用密码学:协议、算法与 C 源程序[M]. 吴世忠等,译. 北京:机械与工业出版社,2000.  
[3] 庄春兴, 刘渊. 利用 DES 算法实现软件加密的方法[J]. 计算机与现代化, 2002(6):21-23.  
[4] 谢宇, 周建儒. 探寻 C 语言随机数生成函数的实现原理[J]. 自动化与仪器仪表, 2016(2):219-220.  
[5] 汪翼, 沈海斌, 何乐年, 等. DES 算法的高速流水线实现[J]. 微电子学与计算机, 2003, 20(8):158-160.

作者简介:

范峻豪 男,(1994),硕士研究生. 研究方向为计算机控制技术. E-mail:1013218565@qq. com.  
柴 波 男,(1963),博士,研究员. 研究方向为计算机控制技术.  
成 龙 男,(1977),男,硕士. 研究方向为地面测发控系统