某IC卡加密方法初探

原创

PUZZER_Ball 于 2020-11-22 15:32:16 发布 1489 收藏 9

本文链接：https://blog.csdn.net/qq_39712148/article/details/109954751

1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*	
A2	69	5E	06	05	96	00	00	00	00	34	00	00	34	00	2F	16.30
9A	69	63	06	00	96	00	00	00	00	33	00	00	33	00	31	16.35
7E	8D	82	06	05	72	00	00	00	00	31	00	00	31	00	11	16.66
02	07	F5	0D	05	F8	00	00	00	00	29	00	00	29	00	A7	35.73
94	73	20	4E	05	8C	00	00	00	00	10	00	00	10	00	6D	200.00

1. 3和4字节反位转为十进制即为卡金额，HEX(08BD)=DEC(2237)，HEX(08CE)=DEC(2254)，
2. 第11,14字节为刷卡次数，每在刷卡机上刷卡一次，都将数据加1，
3. 第2字节为3 4 5字节数据之和(CC=BD+8+7，DF=CE+8+9)，
4. 第5字节功能未知，不过看了两张卡不是00就是05
5. 第6字节为2字节和 FF 异或(33=CC xor FF，20=DF xor FF)，
6. 第16字节为2到14字节相加和取反（需要注意不要累加，舍弃高位，69+96=FF,FF+5E=5D（不进位），5D+06+05+34+34=D0，取反=2F）
7. 1字节为2至14字节所有数据的异或(B2=CC xor BD xor 8 xor 7 xor 33 xor FF)。

2.开水卡加密逻辑

```
00000380  01 14 65 00 13 88 EB F1  FF FF FF FF FF FF FF FF
00000390  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000003A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000003B0  77 F5 DB 80 33 90 FF 07  80 69 FF FF FF FF FF FF
```

13 88(H)为余额，EB为校验位，计算方法：EB=01 XOR 14 XOR 65 XOR 13 XOR 88

3.工具网站

异或计算：http://www.ip33.com/bcc.html

进制转换：https://tool.oschina.net/hexconvert/

4.参考文章

https://www.cnblogs.com/undezhi/p/9099694.html