

2017信息安全大赛 crypto 传感器2

原创

[DDragon321](#) 于 2019-07-26 16:38:27 发布 864 收藏 2

分类专栏: [CTF](#) 文章标签: [CTF](#) [网络安全](#) [计算机](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_43165101/article/details/97395191

版权



[CTF 专栏收录该内容](#)

4 篇文章 0 订阅

订阅专栏

题目

已知ID为0x8893CA58的温度传感器未解码报文为: 3EAAAAA56A69AA55A95995A569AA95565556

为伪造该类型传感器的报文ID (其他报文内容不变), 请给出ID为0xDEADBEEF的传感器1的报文校验位 (解码后hex), 以及ID为0xBAADA555的传感器2的报文校验位 (解码后hex), 并组合作为flag

解题过程

根据传感器1的结果，可以分析出来，编码的可以分为0024D {ID}41{校验位}

0024D 8893CA58 41 81

0024D 8845ABF3 41 19

由于校验位是8位二进制所以猜测是CRC8

找到在线测试CRC编码工具，测试结果如下

CRC (循环冗余校验) 在线计算

Hex Ascii

需要校验的数据:

输入的数据为16进制, 例如: 31 32 33 34

参数模型 NAME:

宽度 WIDTH:

式 POLY (Hex): 例如: 3D65

始值 INIT (Hex): 例如: FFFF

OROUT (Hex): 例如: 0000

输入数据反转 (REFIN) 输出数据反转 (REFOUT)

计算结果 (Hex):

高位在左低位在右, 使用时请注意高低位顺序!!!

计算结果 (Bin):

https://blog.csdn.net/qq_43165101

然后将题目给出的两个iD放入进行校验生成

0024D DEADBEEF 41

0024D BAADA555 41

校验得到结果分别是B5和15