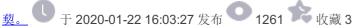
BUUCTF Crypto 4



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/weixin 45897326/article/details/104069305

版权

传统知识+古典密码

题目:

小明某一天收到一封密信,信中写了几个不同的年份 辛卯, 癸巳, 丙戌, 辛未, 庚辰, 癸酉, 己卯, 癸巳。 信的背面还写有"+甲子",请解出这段密文。

key值: CTF{XXX}

先把 辛卯, 癸巳, 丙戌, 辛未, 庚辰, 癸酉, 己卯, 癸巳 转为数字, 再加上甲子, 最终得**88** 90 83 68 77 70 76 90 转ascii得 XZSDMFLZ

之后就是很多尝试

[*]offset21--SHUANGYU

古典密码能用栅栏和凯撒,但是没有提示几栏,只能找合适的,最终找到个 提交呗。

SHUANGYU 双鱼?

传感器

题目:

5555555555555A65556AA696AA666666955

这是某压力传感器无线数据包解调后但未解码的报文(hex)

己知其ID为0xFED31F,请继续将报文完整解码,提交hex。

提示1: 曼联

一开始是没有头绪的,后来学习到这是曼彻斯特编码,但是曼彻斯特编码又分为两种:

第一种G. E. Thomas, Andrew S. Tanenbaum1949年提出的,它规定0是由低-高的电平跳变表示,1是高-低的电平跳变。

第二种IEEE 802.4(令牌总线)和低速版的IEEE 802.3(以太网)中规定,按照这样的说法,低-高电平跳变表示1,高-低的电平跳 变表示0。

关于曼彻斯特编码还有一个差分曼彻斯特

这道题用的是第二种IEEE的方法(都试了一遍),

0x5=0101 编码为11

0x6=0110 编码为10

0x9=1001 编码为01

0xA=1010 编码为00

把5555555555555A65556AA696AA666666955转为二进制编码后得到

转为十六进制0xffff7fcbf8260aaa9f

但是不包括题目0xFED31F,后来才知道需要8位翻转

(8位翻转 我理解的就是镜像翻转 比如01010101 反转后 10101010),

转为十六进制0xffffed31f645055f9

包含0xFED31F

转大写提交即可。

大帝的密码武器

题目:

公元前一百年,在罗马出生了一位对世界影响巨大的人物,他生前是罗马三巨头之一。他率先使用了一种简单的加密函,因此这种加密方法以他的名字命名。

以下密文被解开后可以获得一个有意义的单词: FRPHEVGL

你可以用这个相同的加密向量加密附件中的密文,作为答案进行提交。

密文: ComeChina



明摆了凯撒密码,解密FRPHEVGL在

得到security, 把ComeChina解(加)密得到

[*]offset13——PbzrPuvan

注意大写小写, 提交即可。

windows系统密码

🗐 pass.hash - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

ctf:1002:06af9108f2e1fecf144e2e8adef09efd:a7fcb22a88038f35a8f39d503e7f0062:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

SUPPORT 388945a0:1001:aad3b435b51404eeaad3b435b51404ee:bef14eee40dffbc345eeb3f58e290d56:::

md5一个个解密,有几个是空密码,

📗 pass.hash - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

ctf;1002:06af9108f2e1fecf144e2e8adef09efd;a7fcb22a88038f35a8f39d503e7f0062;x

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

SUPPORT 388945a0:1001:aad3b435b51404eeaad3b435b51404ee:bef14eee40dffbc345eeb3f58e290d56:::

https://blog.csdn.net/weixin_45897326

这个解密就是flag。

权限获得第一步

跟上一个题一样的。

■ 8789fff6-9169-4185-967d-bbc2a90774bd.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

Administrator:500:806EDC27AA52E314AAD3B435B51404EE:F4AD50F57683D4260DFD48AA351A17A8:::

md5解密得结果。