cassical--CTF（Crypto）

原创

--Xc 于 2018-11-18 12:05:26 发布 678 收藏 2
分类专栏： 凯撒 base64 词频分析 文章标签： 密码学 CTF

本文链接：https://blog.csdn.net/weixin_41676901/article/details/84197029

打开文件看到一段奇怪的英文：

Ld hcrakewcfaxr, f hofjjlhfo hlaxuc lj f krau ev hlaxuc kxfk zfj tjui xljkeclhfoor gtk dez xfj vfooud, vec kxu pejk afck, ldke iljtju. Ld hedkcfjk ke peiucd hcrakewcfaxlh foweclkxpj, pejk hofjjlhfo hlaxucj hfd gu acfhklhfoor hepatkui fdi jeoyui gr xfdi. Xezuyuc, OrmkO3vydJCoe2qyNLmcN2qlpJXnM3SxM2Xke3q9 kxur fcu foje tjtfoor yucr jlpaou ke gcufn zlkx peiucd kuhxdeoewr. Kxu kucp ldhotiuj kxu jlpaou jrjkupj tjui jldhu Wcuun fdi Cepfd klpuj, kxu uofgecfku Cudfljjfdhu hlaxucj, Zecoi Zfc LL hcrakewcfaxr jthx fj kxu Udlwpf pfhxldu fdi guredi. F btlhn gcezd veq mtpa eyuc kxu ofsr iew.

猜测应该是古典密码，先用词频分析：https://quipqiup.com/

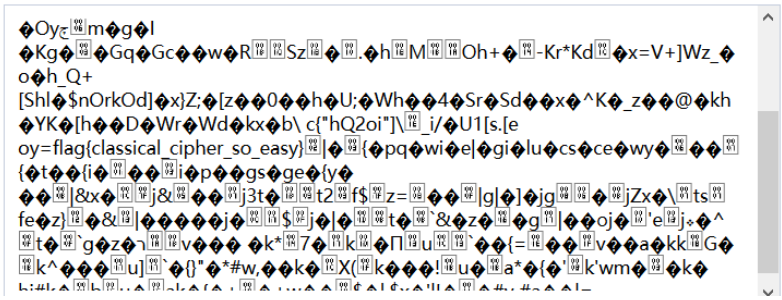
得出来的明文：

In cryptography, a classical cipher is a type of cipher that was used historically but now has fallen, for the most part, into disuse. In contrast to modern cryptographic algorithms, most classical ciphers can be practically computed and solved by hand. However, **LyjtL3fvnSRlo2xvKljrK2ximSHkJ3ZhJ2Hto3x9** they are also usually very simple to break with modern technology. The term includes the simple systems used since Greek and Roman times, the elaborate Renaissance ciphers, World War II cryptography such as the Enigma machine and beyond. A quick brown fox jump over the lazy dog.

发现一句诡异的英文，应该就是答案了，先提取出来，一开始先用base64解码出来发现是乱码，先试试凯撒密码，由于不知道偏移量，就全部情况都列出来：

```
a='abcdefghijklmnopqrstuvwxyz'
b='ABCDEFGHIJKLMNOPQRSTUVWXYZ'
s=input("请输入明文:")
len=len(s)
for k in range(1,26):
    t=[]
    for i in range(0,len):
        n=a.find(s[i])
        m=b.find(s[i])
        if n==-1 and m==-1:
            t.append(s[i])
            continue
        elif n==-1:
            t.append(b[(m+k)%26])
        elif m==-1:
            t.append(a[(n+k)%26])
    for i in range(0,len):
        print(t[i],end="")
    print("")
a=input()
```

解出来后没有发现有flag的，全部再base64一下：



看到flag了吗！！！这就是答案！