

# classical--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](#)

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\\_41676901/article/details/84197029](https://blog.csdn.net/weixin_41676901/article/details/84197029)

版权



[凯撒](#) 同时被 3 个专栏收录

2 篇文章 0 订阅

订阅专栏



[base64](#)

1 篇文章 0 订阅

订阅专栏



[词频分析](#)

1 篇文章 0 订阅

订阅专栏

打开文件看到一段奇怪的英文:

```
Ld hcrakewcfaxr, f hofjilhfo hlaxuc lj f krau ev hlaxuc kxfk zfj tjui xijkeclhfoor gtk dez xfj vfooud, vec kxu pejk afck, ldke iljtju. Ld hedkcfjk ke peiucd hcrakewcfaxlh foweclxpxj, pejk hofjilhfo hlaxucj hfd gu acfhklhfoor hepatkui fdi jeoyui gr xfdi. Xezuyuc, OrmkO3vydJCoe2qyNLmcN2qIpJXnM3SxM2Xke3q9 kxur fcu foje tjtfoot yucr jlpaou ke gcufn zlkx peiucd kuhxdeoewr. Kxu kucp ldhotiuj kxu jlpaou jrjkupj tjui jldhu Wcuun fdi Cepfd klpuj, kxu uofgecfku Cudfljfdhu 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, **LjytL3fvnSRlo2xvKljrK2ximSHkJ3ZhJ2Hto3x9** 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：

```

OyGmgl
KgGqGcwR Sz hM Oh+ -Kr*Kd x=V+]Wz_
o h_Q+
[Shl $nOrkOd] x)Z; [z 0 h U; Wh 4 Sr Sd x x ^K z @ kh
YK [h D Wr Wd kx b \ c("hQ2oi") \ i U1[s.[e
oy=flag[classical_cipher_so_easy] {pqwi e} gi lu csc ce wy
{t {i } i p gs ge y
&x } j & } j 3 t t 2 f $ z = | g | j g j Z x ts
fe z } & } | } j } t } & z } g } | } o j } e } j } ^
t } g } z } v } k } 7 } k } u } { } = } v } a } k } G
k ^ } u } { } * # w } k } X ( } k } ! } u } a } { } ' } k' w m } k

```

```

MzkuM3gwoTSmp2ywLjksL2yjnTIkK3AiK2Iup3y9
NalvN3hxpUTnq2zxMKltM2zkoUJmL3BjL2Jvq3z9
ObmwO3iyqVUor2ayNLmuN2alpVKnM3CkM2Kwr3a9
PcnxP3jzrWVps2bzOMnvO2bmqWLoN3DIN2Lxs3b9
QdoyQ3kasXWqt2caPNowP2cnrXMpO3EmO2Myt3c9
RepzR3lbtYXru2dbQOpXQ2dosYNqP3FnP2Nzu3d9
SfqaS3mcuZYsv2ecRPqyR2eptZOrQ3GoQ2Oav3e9
TgrbT3ndvAZtw2fdSQrzS2fquAPsR3HpR2Pbw3f9
UhscU3oewBAux2geTRsaT2grvBQtS3lqS2Qcx3g9
VitdV3pfxCBvy2hfUStbU2hswCRuT3JrT2Rdy3h9
WjueW3qgyDCwz2igVTucV2itxDSvU3KsU2Sez3i9

```

看到flag了吗!!! 这就是答案!