wechall Training: Crypto - Digraphs (Crypto, Training)

原创

hhhhhorz 于 2019-05-10 11:05:01 发布 820 收藏
分类专栏： wechall 文章标签： ctf

本文链接：https://blog.csdn.net/qq_23997471/article/details/90053519

Crypto - Digraphs

This time I am using a digraph crypto scheme to encrypt one letter into two characters.
With only 26 different letters I am able to encrypt up to 26*26 different characters.
The big problem again is sharing the key, but the cipher is easily broken anyway.
The message is in the current language, is written with correct case and punctuation. There are no line breaks.

Good luck!

ierkvkllhwhardjzaahardsxrkvknqlf cxrkjz dynywxhwuvnordnydy rdhvsxnq frnynqnqhallny nqjzwxwxnynqnqrvjzaaaauvlf nthanq vkrkrd rdrkrk dysxrvrvsxwxjzaard nysxrdhvnyhwce hhhanq sxrdav ntnyaaaace llrkrkdy qirkwllf abvkrdnyhw rdhvsxnq asnyuvhhrkhwdy hanq nqrkaajzrdsxrkvknj nynydydyfrrkhawlaanqrvrvlf

解题思路：

题中说明两个字符是一个字母，首先猜测ierkvkllhwhardjzaahardsxrkvknqlf是Congratulations（说实话我没猜出来.....）

python编程，将密文每两个字符分开，根据猜测到的明密文对应关系建立部分明密文字典，先解一次密，再根据解密结果猜测其他的明密文对应关系。

```
#字符串每两个进行分隔，建立字典
miwen = "ierkvkllhwhardjzaahardsxrkvknqlf cxrkjz dynywxhwuvnordnydy rdhvsxnq frnynqnqhallny nqjzwxwxnynqnqr
miwen1 = miwen.split(" ")

dic = {'ie':'C','rk':'o','vk':'n','ll':'g','hw':'r','ha':'a','rd':'t','jz':'u','aa':'l','sx':'i','nq':'s','
for i in miwen1:
    a =[]
    for j in range(0,len(i),2):
        a.append(i[j:j+2])        #密文字符串每两个分开
    print(a)
    b = []
    for k in a:
        if k in dic:
            b.append(dic[k])      #解密
        else:
            b.append(' ')         #解不出来的用空格填充
    txt = ''.join(b)
    print(txt)
```

运行结果：

```
['ie', 'rk', 'vk', 'll', 'hw', 'ha', 'rd', 'jz', 'aa', 'ha', 'rd', 'sx', 'rk', 'vk', 'nq', 'lf']
Congratulations
['cx', 'rk', 'jz']
you
['dy', 'ny', 'wx', 'hw', 'uv', 'no', 'rd', 'ny', 'dy']
  r  t
['rd', 'hv', 'sx', 'nq']
t is
['fr', 'ny', 'nq', 'nq', 'ha', 'll', 'ny']
 ssag
['nq', 'jz', 'wx', 'wx', 'ny', 'nq', 'nq', 'rv', 'jz', 'aa', 'aa', 'uv', 'lf']
su   ss ull
['nt', 'ha', 'nq']
as
['vk', 'rk', 'rd']
not
['rd', 'rk', 'rk']
too
['dy', 'sx', 'rv', 'rv', 'sx', 'wx', 'jz', 'aa', 'rd']
i  i ult
['ny', 'sx', 'rd', 'hv', 'ny', 'hw', 'ce']
it  r
['hh', 'ha', 'nq']
as
['sx', 'rd', 'av']
it
['nt', 'ny', 'aa', 'aa', 'ce']
 ll
```


猜测补充单词，继续扩充字典

最终密码是：eeddmoablsff

注意：密文空间中包括标点符号，大小写区分