广西首届网络安全选拔赛 CRYPTO Writeup

原创

zrools 于 2016-02-03 18:22:45 发布 8773 收藏 5

分类专栏： CTF 文章标签： 网络安全 密码学 ctf

密码学相关(CRYPTO)

> CRYPTO 是密码学的缩写，这一类的题目通常以破解密文为主，加密算法有可能是古典加密算法，也有可能是现代的加密算法，甚至有些是出题者杜撰的加密算法。

大帝的秘密武器

- 分值：100
- 附件：55ed7caf2936e.txt

公元前一百年，在罗马处上了一位对世界影响巨大的人物，他是当时罗马三巨头之一。在执政生涯中，传言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，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：FRPHEVGL。答案为非常规形式。

接触过密码学从前面两句话应该猜到是“凯撒密码”了(从第二题凯撒大帝也能得到提示)，加密方式是位移，这就好办了，a-z首尾相连进行替换，那么就有26种位移方法，用python循环一下：

```python
#! /usr/bin/env python
# -*- coding: utf-8 -*-

def translateMessage(key, message, mode):
    LETTERS = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'
    translated = ''

    for symbol in message:
        if symbol.upper() in LETTERS:
            num = LETTERS.find(symbol.upper())
            if mode == 'encrypt':
                num = num + key
            elif mode == 'decrypt':
                num = num - key

            if num >= len(LETTERS):
                num = num - len(LETTERS)
            elif num < 0:
                num = num + len(LETTERS)

            if symbol.isupper():
                translated = translated + LETTERS[num]
            elif symbol.islower():
                translated = translated + LETTERS[num].lower()

        else:
            translated = translated + symbol

    return translated


if __name__ == '__main__':

    # key     = 13
    mode    = 'decrypt'
    message = 'FRPHEVGL'

    for key in xrange(0,26):
        print(str(key)+':'+translateMessage(key,message,mode).lower())
```

输出结果：

```
0:frphevgl
1:eqogdufk
2:dpnfctej
3:comebsdi
4:bnldarch
5:amkczqbg
6:zljbypaf
7:ykiaxoze
8:xjhzwnyd
9:wigyvmxc
10:vhfxulwb
11:ugewtkva
12:tfdvsjuz
13:security
14:rdbtqhsx
15:qcaspgrw
16:pbzrofqv
17:oayqnepu
18:nzxpmdot
19:mywolcns
20:lxvnkbmr
21:kwumjalq
22:jvtlizkp
23:iuskhyjo
24:htrjgxin
25:gsqifwhm
```

第14个：security，附件中的密文是：ComeChina，解出即得到答案

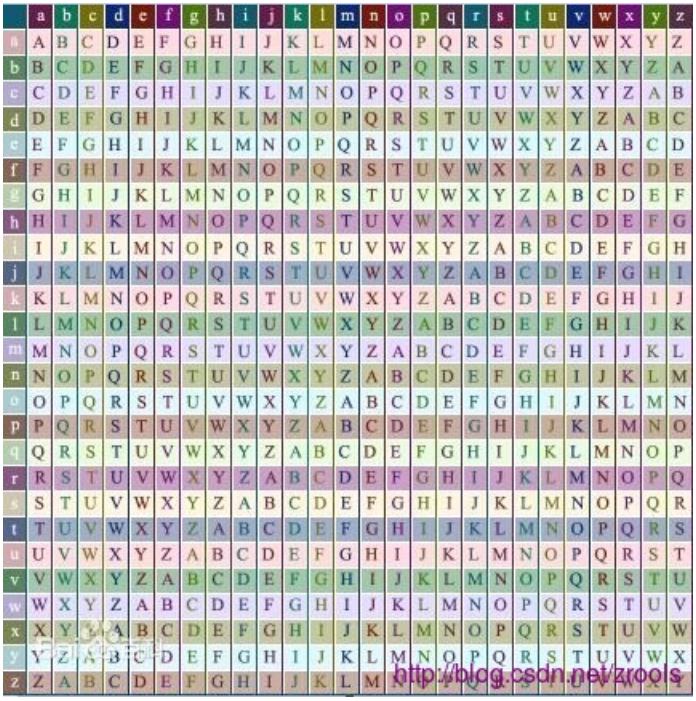
> flag:PbzrPuvan

其实很简单

- 分值：500
- 附件：55ed7caf2ed33.jpg

在学习了凯撒大帝使用的神奇密码后，密码前辈们有创造出了更为奇异的加密方法。本题出题者喜欢用helloworld当密钥，密文如下：dlpcsegkshrij,请破解后提交。附录是一张似乎有用的表。答案为非常规形式。

附件图片是这样：



图片下面有个百度水印，那么直接扔百度识图(`http://shitu.baidu.com/`)得到是“维吉尼亚密码”

python解密得到答案

```python
#! /usr/bin/env python
# -*- coding: utf-8 -*-

def translateMessage(key, message, mode):
    LETTERS = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'
    translated = []

    keyIndex = 0
    key = key.upper()

    for symbol in message:
        num = LETTERS.find(symbol.upper())
        if num != -1:
            if mode == 'encrypt':
                num += LETTERS.find(key[keyIndex])
            elif mode == 'decrypt':
                num -= LETTERS.find(key[keyIndex])

            num %= len(LETTERS)

            if symbol.isupper():
                translated.append(LETTERS[num])
            elif symbol.islower():
                translated.append(LETTERS[num].lower())

            keyIndex += 1
            if keyIndex == len(key):
                keyIndex = 0
        else:
            translated.append(symbol)

    return ''.join(translated)

if __name__ == '__main__':

    key     = 'helloworld'
    mode    = 'decrypt'
    message = 'dlpcsegkshrij'

    print(translateMessage(key,message,mode))
```

> flag:whereisthekey

还原大师

- 分值：500

我们得到了一串神秘字符串：TASC?O3RJMV?WDJKX?ZM,问号部分是未知大写字母，为了确定这个神秘字符串，我们通过了其他途径获得了这个字串的32位MD5码。但是我们获得它的32位MD5码也是残缺不全，E903???4DAB????08?????51?80??8A?,请猜出神秘字符串的原本模样，并且提交这个字串的32位MD5码作为答案。

`TASC?O3RJMV?WDJKX?ZM`只有三个未知字母，且均为大写，直接写三个循环就OK；`E903???4DAB????08?????51?80??8A?`这个玩意匹配前4位就够了，MD5碰撞概率可以无视，如果出现多个输出再人工看一下，python跑以下得到答案

```python
#! /usr/bin/env python
# -*- coding: utf-8 -*-

import string
import hashlib

# TASC?O3RJMV?WDJKX?ZM
# E903???4DAB???P08?????51?80??8A?

for w1 in string.uppercase:
    for w2 in string.uppercase:
        for w3 in string.uppercase:
            s1 = 'TASC'+w1+'O3RJMV'+w2+'WDJKX'+w3+'ZM'
            m = hashlib.md5()
            m.update(s1)
            p = m.hexdigest().upper()
            # print p
            if p[0:4]=='E903':
                # print(s1)
                print(p)
```

> flag:E9032994DABAC08080091151380478A2

Alice与Bob

- 分值：100

密码学历史中，有两位知名的杰出人物，Alice和Bob。他们的爱情经过置换和轮加密也难以混淆，即使是没有身份认证也可以知根知底。就像在数学王国中的素数一样，孤傲又热情。下面是一个大整数:98554799767,请分解为两个素数，分解后，小的放前面，大的放后面，合成一个新的数字，进行md5的32位小写哈希，提交答案。

分解为素数，没啥好说的，素因子分解算法的话，直接跑到`98554799767`的开根，我比较喜欢用算法，得到`101999`和`966233`，组合md5得到答案

```python
#! /usr/bin/env python
# -*- coding: utf-8 -*-

from random import randint
from fractions import gcd
from math import *

def PollardRho(n):
    i=0;
    xi=randint(0,n-1);
    k=2
    y=xi
    while i< n:
        i=i+1
        xi=((xi^2)-1)%n
        d=gcd(y-xi,n)
        if d!=1 and d!=n:
            print(d)
        if i==k:
            y=xi
            k=2*k

PollardRho(98554799767)
```

> flag:d450209323a847c8d01c6be47c81811a

残缺的哈希值

- 分值：300

小明一直将电脑密码的哈希值写在纸上，结果一不小心将墨水撒在了上面，只看得到前10位是c2979c7124，小明只记得密码是4位的数字加字母，你能帮小明恢复密码的哈希值吗？（提示：flag为密码的哈希值）

排列组合以下匹配前10位，直接跑一会可以得到答案

```python
#! /usr/bin/env python
# -*- coding: utf-8 -*-

import string
import hashlib
import itertools

def md5(cstr):
    m = hashlib.md5()
    m.update(cstr)
    return m.hexdigest().lower()

ls = list(string.lowercase) + list(string.uppercase) + list(string.digits)

s = 'c2979c7124'
for l in list(itertools.permutations(ls,4)):
    p = ''.join(l)
    if md5(p)[0:len(s)] == s:
        print md5(p)
        exit(0)
```

flag:c2979c71244dec2befc6e369941c6546