南京邮电大学CTF密码学部分Writeup

转载

weixin_30838921 于 2017-01-14 02:16:00 发布 351 收藏
文章标签： 密码学 php python
原文链接：http://www.cnblogs.com/Chesky/p/nuptzj_crypto_Writeup.html

异性相吸

> 1.xor
> 2.hex2binary
> 3.len(bin(miwen))==len(bin(mingwen))

```
# -*- coding:utf-8 -*-
file_de = open('decode1.txt')
file_en = open('ene.txt')
de = file_de.read()
en = file_en.read()

s = ''
for i, j in zip(de, en):
    s += chr(ord(i) ^ ord(j))
print s
file_de.close()
file_en.close()
```

MD5

> 明文:TASC?O3RJMV?WDJKX?ZM
> MD5 密文：e9032???da???08????911513?0???a2

查了下 Python MD5的库，发现是内置了一个模块的：
http://www.cnblogs.com/the4king/archive/2012/02/06/2340660.html

暴力猜明文缺失字符。

```
import hashlib
s1 = "TASC"
s2 = "O3RJMV"
s3 = "WDJKX"
s4 = "ZM"

dict = ['0','1','2','3','4','5','6','7','8','9','0','A','B','C','D','E','F','G','H','I','J','K','L','M','N'

for i in range(36):
    for j in range(36):
        for k in range(36):
            src = s1 + dict[i] + s2 + dict[j] + s3 + dict[k] + s4
            pre = hashlib.md5()
            pre.update(src)
            md5 = str(pre.hexdigest())
            if ('e9032' and 'da' and '911513') in md5 :
                print md5,'  ',src
```

easy&base64&n次base64&mixed_base64

这几道题都是一个类型的……

```
import base64
with open('string.txt') as f:
        s = f.read().replace('\n','')
while 1:
        try:
                s = base64.b16decode(s)
        except:
                try:
                     s = base64.b32decode(s)
                except:
                        s = base64.b64decode(s)
        if 'nctf' in s:
                print s
                break
```

KeyBoard

看键盘画图形，不过我没做对，想象力拙计……

骚年来一发吗

密文

```
iEJqak3pjIaZ0NzLiITLwWTqzqGAtW2oyOTq1A3pzqas
```

```
function encode($str){
    $_o = strrev($str);
    for($_0 = 0; $_0 < strlen($_o); $_0++){
        $_c = substr($_o, $_0, 1);
        $__ = ord($_c) + 1;
        $_c = chr($__);
        $_ = $_.$_c;
    }
    return str_rot13(strrev(base64_encode($_)));
```

没学过这种世界上最好的语言。去搜索了下 $ 貌似是“xx变量”的意思，暂且当成 CPP 来看了……然后直接搜一些函数语法：

```
substr() 返回字符串
strrev(string)      反转字符串
ord(string)    返回字符串中第一个字符的 ASCII 值
chr(ascii)  从指定 ASCII 值返回字符
(.)         PHP 并置运算符,将两个字符串连接起来
```

执行完函数后得到一个字符串 $_
然后将这个字符串 base64 再反转再 ROT13 。
ROT13 实际上是凯撒加密的变体。,不过神奇的是，PHP 竟然自带 rot13 的函数。
解密的时候逆过来操作就好了。
我感到了智商缺陷，最开始在逆向操作 `return`那一行时从内层到外层写的……

```
import codecs
import base64

with open('rot13decode.txt') as f:
    s = f.read().replace('\n', '')
flag = ""
s = codecs.encode( s,"rot13" )
s = s[::-1]
s = base64.b64decode(s)
for i in s:
    s = s + chr(ord(i) - 1)
s = s[::-1]
print s
```

Vigenere

> It is said that Vigenere cipher does not achieve the perfect secrecy actually :-)
> Tips:
> 1.The encode pragram is given;
> 2.Do u no index of coincidence ?
> 3.The key is last 6 words of the plain text(with "nctf{}" when submitted, also without any interpunction)

code is here(without '
'):

```
F96DE8C227A259C87EE1DA2AED57C93FE5DA36ED4EC87EF2C63AAE5B9A7EFFD673BE4ACF7BE8923CAB1
DA3DA44FCF7AE29235A24C963FF0DF3CA3599A70E5DA36BF1ECE77F8DC34BE129A6CF4D126BF5B9A7CFE
50D37CF0C63AA2509A76FF9227A55B9A6FE3D720A850D97AB1DD35ED5FCE6BF0D138A84CC931B1F121B44
6C032BD56C33FF9D320ED5CDF7AFF9226BE5BDE3FF7DD21ED56CF71F5C036A94D963FF8D473A351CE3FE
84DDB71F5C17FED51DC3FE8D732BF4D963FF3C727ED4AC87EF5DB27A451D47EFD9230BF47CA6BFEC12AE
2E29224A84CDF3FF5D720A459D47AF59232A35A9A7AE7D33FB85FCE7AF5923AA31EDB3FF7D33ABF52C33F
551D93FFCD33DA35BC831B1F43CBF1EDF67F0DF23A15B963FE5DA36ED68D378F4DC36BF5B9A7AFFD121B
FEDC73BE5DD27AFCD773BA5FC93FE5DA3CB859D26BB1C63CED5CDF3FE2D730B84CDF3FF7DD21ED5ADF
6BE1EDB79E5D721ED57CE3FE6D320ED57D469F4DC27A85A963FF3C727ED49DF3FFFDD24ED55D470E69E7
3FE5DA3ABE1EDF67F4C030A44DDF3FF5D73EA250C96BE3D327A84D963FE5DA32B91ED36BB1D132A31ED8
A255DF71B1C436BF479A7AF0C13AA14794
```

http://www.cnblogs.com/Chesky/p/Vigenre_cipher_note.html

转载于:https://www.cnblogs.com/Chesky/p/nuptzj_crypto_Writeup.html