

攻防世界crypto部分fanfie的writeup

原创

[隐藏起来](#) 于 2020-04-10 11:50:55 发布 1769 收藏 1

分类专栏: [CTF # crypto](#)

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/dchua123/article/details/105429883>

版权



[CTF 同时被 2 个专栏收录](#)

20 篇文章 3 订阅

订阅专栏



[crypto](#)

15 篇文章 0 订阅

订阅专栏

这是BITSCTF 2017的原题。

1、首先对BITSCTF进行base32加密后得到的是:

```
IJEVIU2DKRDA=====
```

与密文前面几位进行对应, 发现:

```
MZYVMIWLG7C7IJOJQVOA3IN5BLYC3NHI
IJEVIU2DKRDA=====
```

M解密两次对应的都是I, 不同的字母对应的都是不同的解密字母, 那么猜测可能是根据某种规则进行了字母替换。

对字母表进行编码:

1	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 2 3 4 5 6 7
2	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

则有:

3 -> 11

4 -> 24

8 -> 12

20 -> 8

21 -> 21

25 -> 9

26 -> 22

那么，观察可得，这是仿射密码，这种密码相关介绍见：https://blog.csdn.net/x_yhy/article/details/83756908

仿射密码的 $a = 13$ 和 $b = 4$ ，对应表如下：

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	2	3	4	5	6	7
4	17	30	11	24	5	18	31	12	25	6	19	0	13	26	7	20	1	14	27	8	21	2	15	28	9	22	3	16	29	10	23
E	R	6	L	Y	F	S	7	M	Z	G	T	A	N	2	H	U	B	O	3	I	V	C	P	4	J	W	D	Q	5	K	X

则密文进行仿射解密得：

```
MZYVMIWLGBl7CIJOGJQVOA3IN5BLYC3NHI -> IJEVIU2DKRDHWUZSKZ4VSMTUN5RDEWTNPU
```

对 IJEVIU2DKRDHWUZSKZ4VSMTUN5RDEWTNPU进行base32解密得：

```
BITSCTF{S2VyY2tob2Zm}
```