

CTF-Crypto题目分析_2

原创

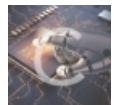
建议密码为123456 于 2021-04-23 20:33:58 发布 244 收藏

分类专栏: [ctf-crypto题目分析](#) 文章标签: [字符串](#) [加密解密](#) [base64](#) [leetcode](#) [ssl](#)

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/a6b6c6d5488/article/details/115635294>

版权



[ctf-crypto题目分析](#) 专栏收录该内容

3 篇文章 0 订阅

订阅专栏

CTF-Crypto题目分析_2

以下所有题目提交flag的格式为SeBaFi{}
第六题: 考察base64

1. 题目描述

base64?



实训描述: TO BE NO.64

下载可得: U2VCYUZpJTdCNDlyYjZkZjJlZGlzNzY5MyU3RA==

2. 解题思路: 由实训描述, 猜测是base64编码

3. 解题过程: 通过base64解密

在线base64编码解码

全屏

代码

明文:

SeBaFi%7B422b6df2edb37693%7D

编码 >

<解码

BASE64:

U2VCYUZpJTdCNDlyYjZkZjJlZGlzNzY5MyU3RA==

4. 求出flag, 得到SeBaFi%7B422b6df2edb37693%7D,

可得SeBaFi{422b6df2edb37693}

第七题：考察base编码

1. 题目描述

Base全家桶？



实训描述： Base全家桶

实训附件：

下载

<https://blog.csdn.net/a6b6c6d5488>

下载可得：

```
;DD3<e`=#K*cHL;(sjp<S&f..AX<E.^m;D;m4;FO>V=):c*=&_dl;_`mC<'N[69e]l5<,><!;DDr@<e`@=);PA;H-7h<)keS=)2;"=):c.<GY90;DDs5<^h++<A7Tl:/t%U:fK,/:f0A=
```

2. 解题思路

题目给了提示： flag->16->32->64->85

解密就需要反过来， 85->64->32->16->flag

3. 解题过程

1. 原字符串 ;DD3<e`=#K*cHL;(sjp<S&f..AX<E.^m;D;m4;FO>V=):c*=&_dl;_`mC<'N[69e]l5<,><!;DDr@<e`@=);PA;H-7h<)keS=)2;"=):c.<GY90;DDs5<^h++<A7Tl:/t%U:fK,/:f0A=

2. base85解密

后R1VaVE1OSIVHSTNEQ05CV0dZNFRPUVJVR0kzRENOWIRHWTJUS1JSVUdZM0RDTINFR1k0VE1RWlhIRTJVTU5S
Wkc0WIRLUIJXR1kzVEtOU0ZHNUNBPT09PQ==

3. base64解密

后GUZTMNJUGI3DCNBWGY4TOQRUGI3DCNZTGY2TKRRUGY3DCNSEGY4TMQZXHE2UMNRZG4ZTKRRWGY3TKNS
FG5CA====

4. base32解密后

5365426146697B426173655F46616D696C795F69735F66756E7D

5. base16解密后

SeBaFi{Base_Family_is_fun}

4. flag

SeBaFi{Base_Family_is_fun}

第八题：bacon培根

1. 题目描述

bacon？



实训描述： bAcon iS a MEaT prodUcT prePared frOm a pig and UsuALLy cURed.

<https://blog.csdn.net/a6b6c6d5488>

2.解题思路

题目名字是bacon，中文翻译就是培根。题目描述给出了一段英文介绍，但是中间的个别字母被人为强行大写了。猜测是培根加密算法。

3.解题过程

简单介绍一下培根密码。培根密码，又名倍康尼密码（英语：Bacon's cipher）是由法兰西斯·培根发明的一种隐写术。加密时，明文中的每个字母都会转换成一组五个英文字母。转换如下表：

第一种方式			
A aaaaa	H aabbb	O abbba	V babab
B aaaab	I abaaa	P abbbb	W babba
C aaaba	J abaab	Q baaaa	X babbb
D aaabb	K ababa	R baaab	Y bbaaa
E aabaa	L ababb	S baaba	Z bbaab
F aabab	M abbaa	T baabb	
G aabba	N abbab	U babaa	
第二种方式			
a AAAAA	g AABBA	n ABBAA	t BAABA
b AAAAB	h AABBB	o ABBAB	u-v BAABB
c AAABA	i-j ABAAA	p ABBBA	w BABAA
d AAABB	k ABAAB	q ABBBB	x BABAB
e AABAA	l ABABA	r BAAAA	y BABBA
f AABAB	m ABABB	s BAAAB	z BABBB

把题目给出的描述按照5个字母一组划分。

b4con iSaME aTpro dUcTp rePar edfrO mapig andUs uALLy cUReD

小写换成a，大写换成b

abaaa ababb abaaa ababa aabaa aaaab aaaaa aaaba abbba abbab

对照表中第一种方式

abaaa > l

ababb > L

abaaa > l

ababa > K

aabaa > E

aaaab > B

aaaaa > A

aaaba > C

abbba > O

abbab > N

连在一起:ILIKEBACON

4.flag

SeBaFi{ILIKEBACON}大写提交失败

转换为小写，进行尝试，发现小写是flag ——>SeBaFi{i like bacon}



[创作打卡挑战赛 >](#)

[赢取流量/现金/CSDN周边激励大奖](#)