

攻防世界 Crypto 高手进阶区 4分题 Decode_The_File

原创

思源湖的鱼 于 2020-12-28 13:35:57 发布 247 收藏

分类专栏: [ctf](#) 文章标签: [ctf](#) [攻防世界](#) [crypto](#) [base64](#)

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/weixin_44604541/article/details/111835754

版权

CTF

[ctf 专栏收录该内容](#)

200 篇文章 23 订阅

[订阅专栏](#)

前言

继续ctf的旅程

攻防世界Crypto高手进阶区的4分题

本篇是Decode_The_File的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

解题过程

得到一堆base64

1a351e90fb2b476a929d1e2666d7c511 - 记事本

那感觉就不像是base64本身解码得到什么

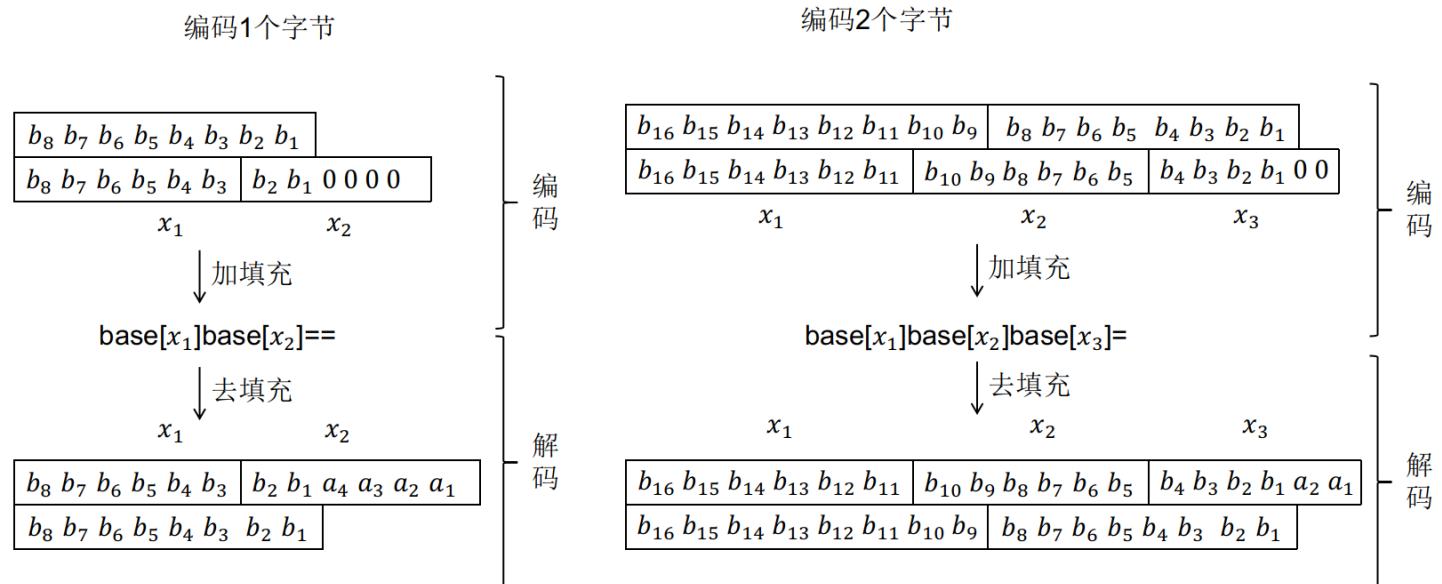
而是base64编码过程中隐藏了什么

尝试解码几个

确实没得到什么有效信息

而考虑base64编码过程中隐藏信息

那就要看等号



即使 $a_i \neq 0$, 解码过程也能正确进行

从而可以使用ai传递一些信息

因此，将编码中的 a_i 提取出来

```
from base64 import b64decode
from string import uppercase,lowercase,digits
from Crypto.Util.number import long_to_bytes

def solve():
    with open('encode','r') as f:
        codes=f.read()
    Lc=codes.split('\n')[:-1]
    base=uppercase+lowercase+digits+'/'
    re2=[]
    for code in Lc:
        if '==' in code:
            re2.append(bin(base.find(code[-3]))[2:].rjust(6,'0')[2:])
        elif '=' in code:
            re2.append(bin(base.find(code[-2]))[2:].rjust(6,'0')[4:])
    ret=''.join(re2)
    return long_to_bytes(long(ret[:ret.rfind('1')+1],2))

if __name__=='__main__':
    print solve()
```

得到flag: ROIS{base_GA_caN_b3_d1ffeR3nT}

结语

base64编码隐藏信息