# 一、题目描述

题目链接：https://buuoj.cn/challenges#zip

题目来源平台：buuctf

题目名称：zip

题目描述：crc32碰撞

题目类型：MISC

题目附件：

FLAG：flag{nev3r\_enc0de\_t00\_sm4ll\_fil3\_w1th\_zip}

# 二、解题工具

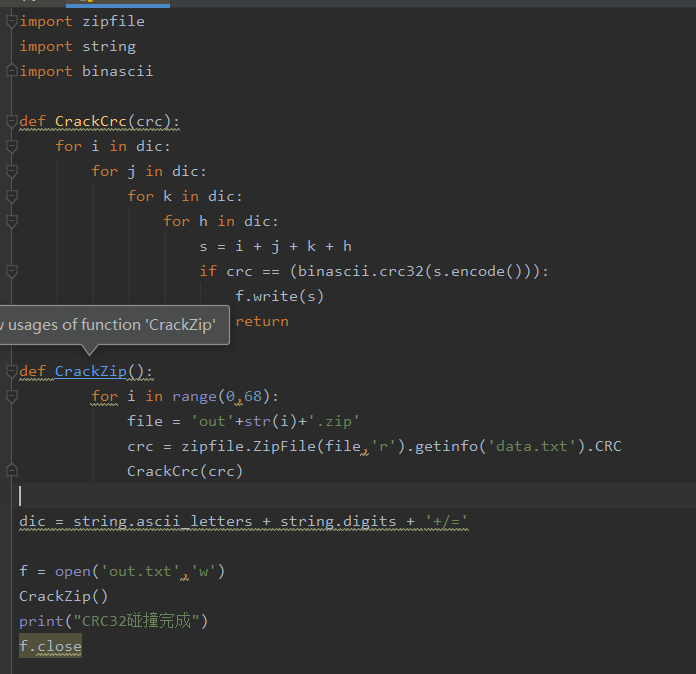
|  |  |  |  |
| --- | --- | --- | --- |
| 工具类型 | 工具名称 | 版本 | 备注 |
| 基础环境 | Windows | 10 |  |
|  |  |  |
| 工具 | Winhex | 19.6 |  |
| WinRAR |  |  |
| 脚本 | Crc32碰撞校验 |  | 用于py3下进行crc碰撞解密 |
|  |  |  |
|  |  |  |

# 三、解题过程

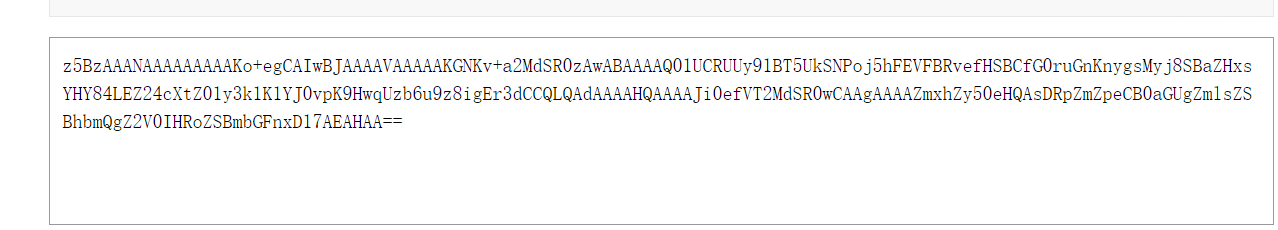
（详细说明CTF赛题的解题过程，分步骤说明）

### 步骤1

### 由题目名称判断可能是crc32碰撞，因此抛入脚本跑一遍，

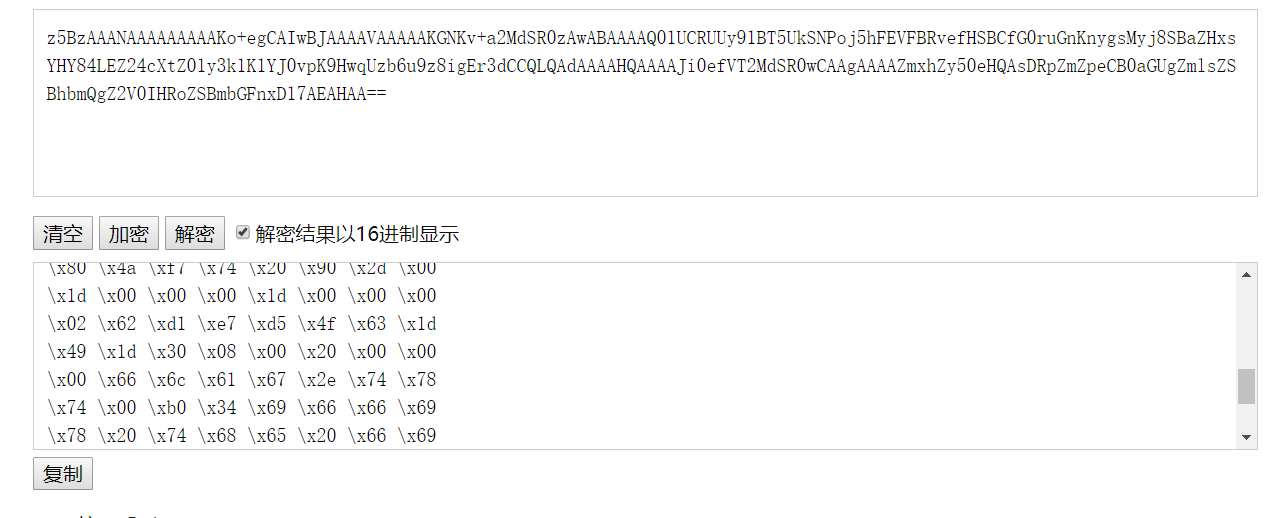


得到字符拼接后的文本文件：



### 步骤2

题目给出提示，将得到的字符放到base64中解密：

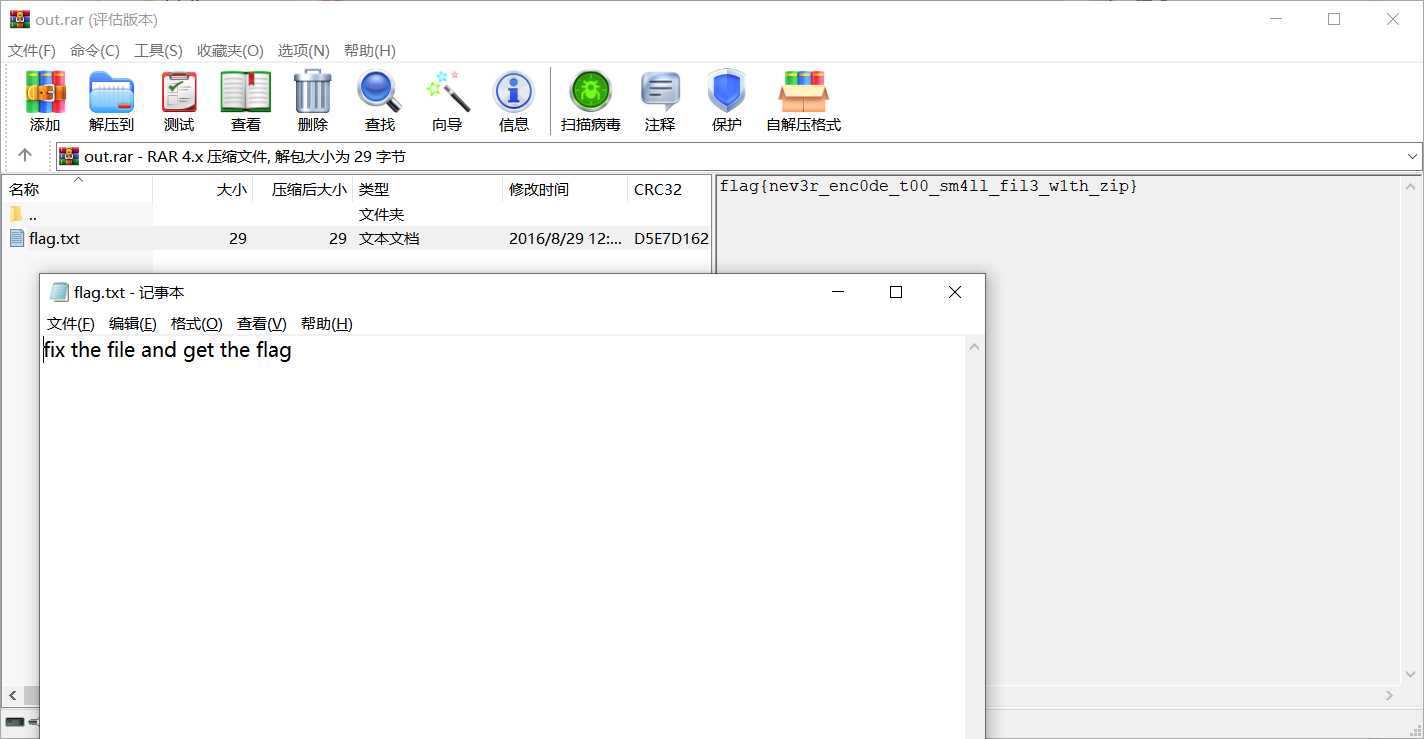


### 步骤3

### 对解码后的数据进行处理，看到CF 90字段，联想到压缩文件头crc的校验值，判断可能不是zip后缀，加上52 61 72 21 1A 07 00 ，（具体结构在压缩包总结中有写）将后缀修改为.rar，拖入winhex中处理：

### 

打开压缩包得到：



### （在这里可以看到压缩软件直接将flag爆破出来了，填写flag试一试是正确的）