攻防世界 base64stego

原创

『铁躯电芯』 于 2021-06-07 00:32:51 发布 200 收藏 2

base64stego：

首先根据题目下载得到一个加密文件：

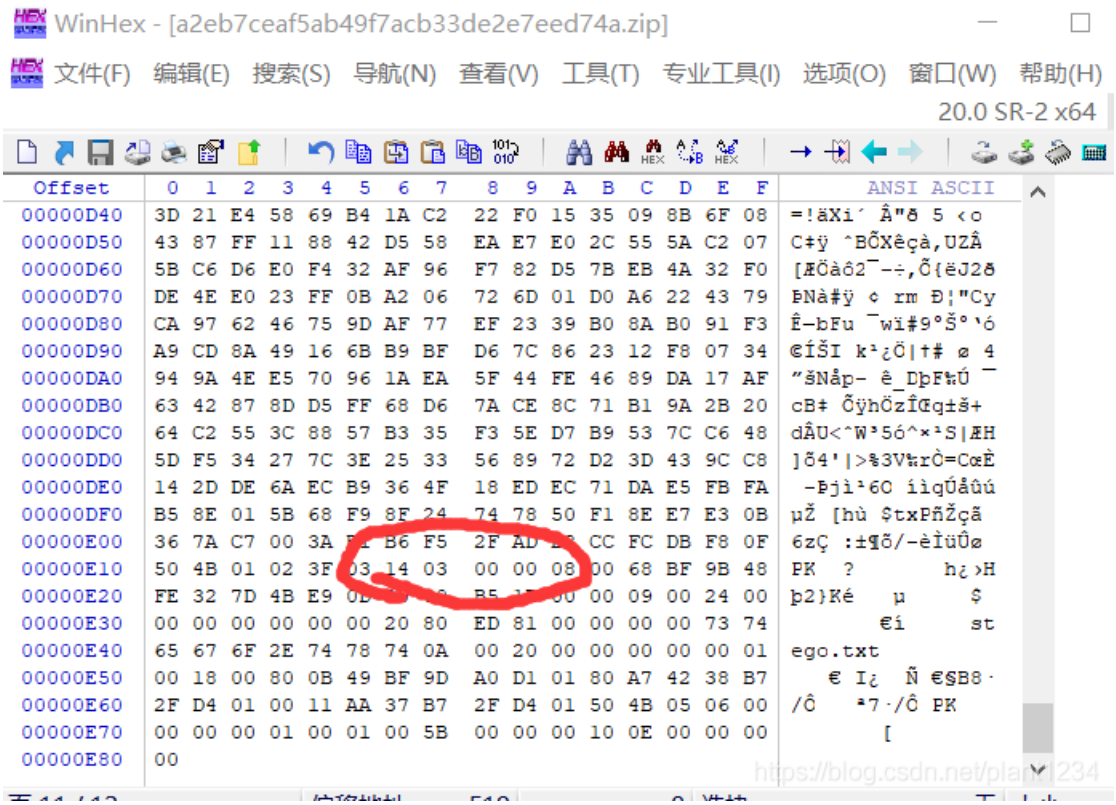
首先我想到的是伪加密,这里提供一下加密文件的知识：

0x00:ZIP伪加密

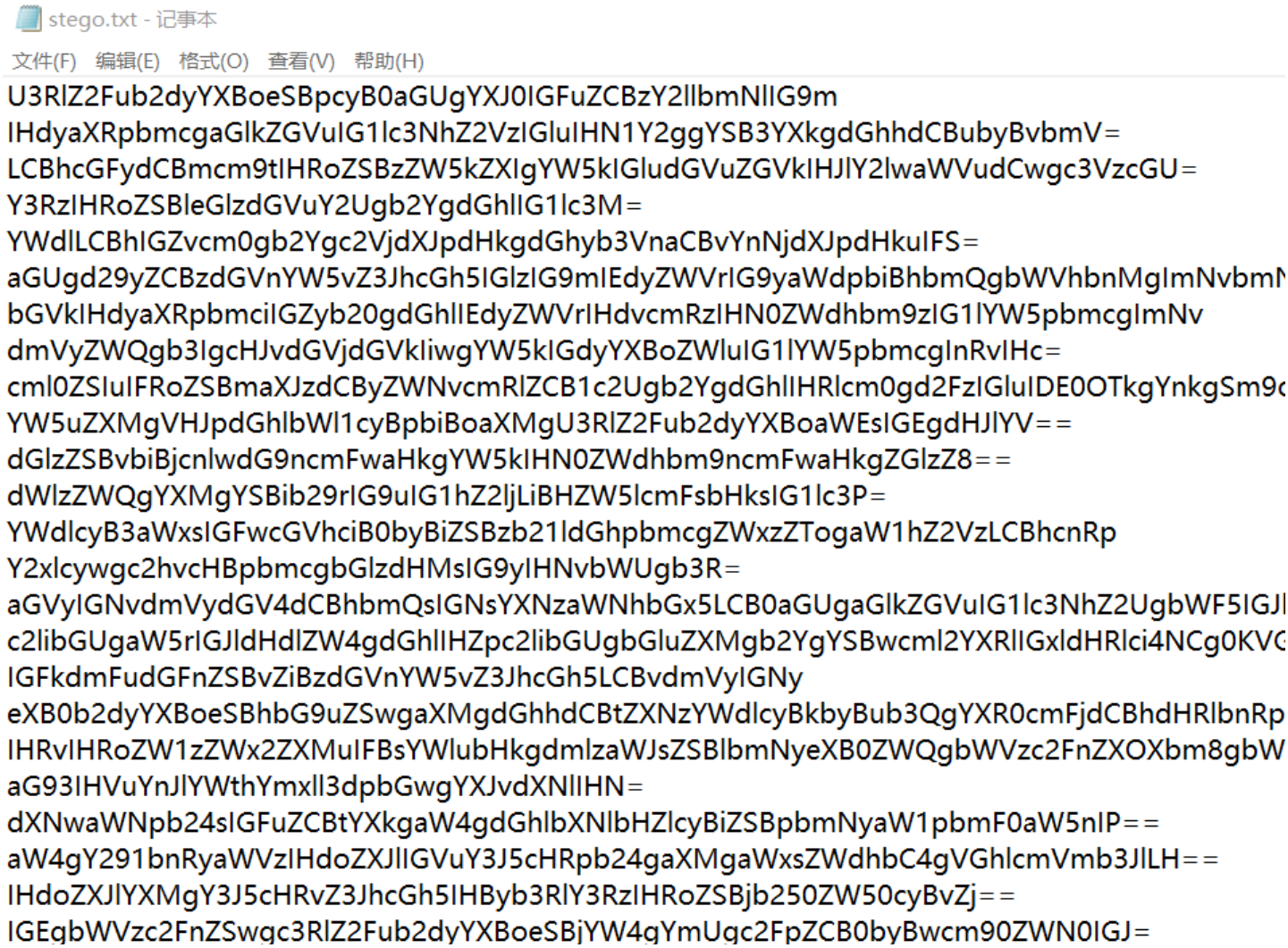
一个ZIP文件由三个部分组成：压缩源文件数据区+压缩源文件目录区+压缩源文件目录结束标志。
伪加密原理：zip伪加密是在文件头的加密标志位做修改，进而再打开文件时识被别为加密压缩包。

1.无加密
压缩源文件数据区的全局加密应当为00 00
且压缩源文件目录区的全局方式位标记应当为00 00
2.假加密
压缩源文件数据区的全局加密应当为00 00
且压缩源文件目录区的全局方式位标记应当为14 03 09 00
3.真加密
压缩源文件数据区的全局加密应当为14 03 09 00
且压缩源文件目录区的全局方式位标记应当为14 03 09 00

所以用把末尾改09 00为00 00 :



打开发现：



b3RoIG1lc3NhZ2VzIGFuZCBjb21tdW5pY2F0aW5nIHBhcnRpZXMuDQoNCIN0ZWdhbm9ncmFwaHkg

全是bas64解码，于是我们就利用python写个脚本来解码得到：

```python
import base64
a = open("stego.txt", "rt")
b = a.readlines()
data=[]
for i in b:
    c = base64.b64decode(i.encode("utf-8"))
    data.append(c)

a.close()

m = open("jiema","wb")
for i in data:
    m.write(i)

m.close()
```


得到一篇英文，

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. The word steganography is of Greek origin and means "concealed writing" from the Greek words steganos meaning "covered or protected", and graphein meaning "to write". The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography disguised as a book on magic. Generally, messages will appear to be something else: images, articles, shopping lists, or some other covertext and, classically, the hidden message may be in invisible ink between the visible lines of a private letter.

The advantage of steganography, over cryptography alone, is that messages do not attract attention to themselves. Plainly visible encrypted messages巽o matter how unbreakable椤ill arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. As a simple example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

The first recorded uses of steganography can be traced back to 440 BC when Herodotus mentions two examples of steganography in The Histories of Herodotus. Demaratus sent a warning about a forthcoming attack to Greece by writing it directly on the wooden backing of a wax tablet before applying its beeswax

翻译一下：

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. The word steganography is of Greek origin and means "concealed writing" from the Greek words steganos meaning "covered or protected", and graphein meaning "to write". The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography disguised as a book on magic. Generally, messages will appear to be something else: images, articles, shopping lists, or some other covertext and, classically, the hidden message may be in invisible ink between the visible lines of a private letter.

The advantage of steganography, over cryptography alone, is that messages do not attract attention to themselves. Plainly visible encrypted messages帛o matter how unbreakable椤ill arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. As a simple example, a sender might

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. The word steganography is of Greek origin and means "concealed writing" from the Greek words steganos meaning "covered or protected", and graphein meaning "to write". The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography disguised as a book on magic. Generally, messages will appear to be something else: images, articles, shopping lists, or some other covertext and, classically, the hidden message may be in invisible ink between the visible lines of a private letter.
隐写术是一门书写隐藏信息的艺术和科学，除了发送者和接收者之外，没有人怀疑信息的存在，这是一种通过隐晦来实现安全的形式。隐写术一词起源于希腊语，意思是“隐藏的写作”，而隐写术一词来自希腊语，意为“覆盖或保护”，graphenin意为“写作”。有记载的第一次使用这个术语是在1499年，约翰内斯特里希米斯在他的《隐写术》（Steganographia）中，这是一本关于密码学和伪装成魔法书的隐写术的论文。一般来说，信息看起来是其他的东西：图像、文章、购物清单或其他一些covertext，而经典的是，隐藏的信息可能是在私人信件的可见行之间的隐形墨水中。
The advantage of steganography, over cryptography alone, is that messages do not attract attention to themselves. Plainly visible encrypted messages帛o matter how unbreakable椤ill arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal. Therefore, whereas cryptography protects the

根据翻译是，隐写术，又想到题目base64,应该是base64隐写

于是查看大佬的博客，
知道base64隐写链接：https://www.tr0y.wang/2017/06/14/Base64steg/

在利用python跑一个base64的隐写脚本：

```
# -*- coding: cp936 -*-
import base64
b64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
with open('stego.txt', 'rb') as f:
    bin_str = ''
    for line in f.readlines():
        stegb64 = str(line, "utf-8").strip("\n")
        rowb64 =  str(base64.b64encode(base64.b64decode(stegb64)), "utf-8").strip("\n")
        offset = abs(b64chars.index(stegb64.replace('=','')[-1])-b64chars.index(rowb64.replace('=','')[-1]))
        equalnum = stegb64.count('=') #no equalnum no offset
        if equalnum:
            bin_str += bin(offset)[2:].zfill(equalnum * 2)
    b=''.join([chr(int(bin_str[i:i + 8], 2)) for i in range(0, len(bin_str), 8)]) #8 位一组
    data=""
    m="flag{"+b+"}"
    m = m.replace("\x00", "")
    print(m)
```

得到flag：

```python
import base64
b64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
with open('stego.txt', 'rb') as f:
    bin_str = ''
    for line in f.readlines():
        stegb64 = str(line, "utf-8").strip("\n")
        rowb64 = str(base64.b64encode(base64.b64decode(stegb64)), "utf-8").strip("\n")
        offset = abs(b64chars.index(stegb64.replace('=','')[-1])-b64chars.index(rowb64.replace('=','')[-1]))
        equalnum = stegb64.count('=') #no equalnum no offset
        if equalnum:
            bin_str += bin(offset)[2:].zfill(equalnum * 2)
    b=''.join([chr(int(bin_str[i:i + 8], 2)) for i in range(0, len(bin_str), 8)]) #8 位一组
    data=""
    m="flag{"+b+"}"
    m = m.replace("\x00", "")
    print(m)
```

Run: jiema (1)

```
flag{Base_sixty_four_point_five}
```