QwQ3

(用VSCode的Markdown扩展编译吧。)
多文件多密码打包成一个文件，即变成单文件多密码。给一个密码，只能提取对应文件。
同时你可以生成多个只包括部分真密码的密码序列，使得就算有人拿枪顶着你的脑袋让你解码，你也可以隐藏想要隐藏的文件。

Encode many files with different passwords into one large file. When decoding the large file, each password can be used, but only the corresponding file can be extracted. In this way, even if someone holds a gun to your head and asks you to decode it, you can still hide the files you want to hide.

开源协议

0.该协议是我临时现编的，适用于本人在GitHub上的所有文件。
1.你可以以任意非盈利合法方式使用我的代码。
2.如果用我的代码的idea发表文章，请给予我一个作者位。(PS:我在想peach)
3.如果发表文章与我的代码相关，请给予我一个引用位。(PS:我又在想peach)
4.如果盈利与我的代码相关，请给我钱。(PS:我还在想peach)

算法介绍

理想状态的函数

$$\mathrm{F}(\mathrm{psw}_1,\cdots,\mathrm{psw}_\mathrm{n},\mathrm{file}_1,\cdots,\mathrm{file}_\mathrm{n})=\mathrm{bigfile},$$

$$\mathrm{G}(\mathrm{psw}_\mathrm{x},\mathrm{bigfile})=\mathrm{file}_\mathrm{x}.$$

且 $\mathrm{bigfile}$ 就算在知道了源码和部分 psw 的情况下，还是只能爆破。

异或值

其实没啥用，要是算法没开源的话还有点用。
几乎没有加密效果，仅用作混淆。要加密的话自己先拿个现有常用加密算法跑一跑就好了。

密码序列要求

编码过程中，需要用每个 psw_x 生成无限长度下标序列 l_x, 满足

$$\mathrm{l_i[k]}\neq\mathrm{l_j[k]},\mathrm{l_i[k]}\in\mathbb{N}\cap[0,\mathrm{n}),\ \forall\mathrm{i}\neq\mathrm{j}.$$

可见这个要求还是很苛刻的，所以我们采用让程序自生成密码的方式。

下标序列生成

密码字符串 $\rightarrow$ 整数 $\rightarrow$ n 进制数字符串 $\rightarrow$ 转无限长度序列(用环状结构实现)

bigfile 文件结构

记文件 x 的第 i 个bit位为 $\mathrm{x[i]}$, 则

$$\mathrm{bigfile[(k-1)*n+l_x[k]]=file_x[k].}$$

当娶不到 $\mathrm{file_x[k]}$, 随机生成即可。
更不像人话的人话:

大文件bigfile的第k段连续的n个bit位中的第i个，

恰好是小文件$\mathrm{file_x}$的第k位.

暴力破解所需时间

已知算法和 k 个密码。
密码长度为 l, 文件数量为 n.
则下标序列的最大最小循环节长度为 $m=[\log_n 95^l]+1=[l\frac{\ln 95}{\ln n}]+1$, 遍历所有可能密码

$$O((n-k)^m)\simeq O((\frac{n-k}{n})^m 95^l).$$

其它可能的破解方式

对方知道里面存的其中一个文件的一段bit位和异或值，但不知道文件数量、任何密码或密码长度，于是可以暴力对比出此文件对应的密码。所需时间的数学期望仅为 $m^2 n\log n$.

安全性证明

不会证。

接口介绍

_psw.key_maker

函数定义

```
def key_maker(pth:str,n:int=None,len_psw:int=None,lst_psw:list=None,xor8:int=0)->list:
```

变量介绍

名称	类型	解释
pth	str	将信息输出到文件 pth+'.json'
n	int	文件(及密码)数量
len_psw	int	密码长度
lst_psw	list	许愿密码序列
xor8	int	异或值，生成密码时用不到
返回值	list	下标序列

功能介绍

给出需要的密码长度和个数，生成合法的密码序列。
若许愿密码序列不为空，将在生成密码序列前检查其是否合法，将合法的密码加入到生成密码序列中。
需要生成真假密码混合序列时，将真密码作为许愿密码即可。

np.mian

函数定义

```
def mian(pth:str,_files_name:list,_n:int=None,len_psw:int=None,lst_psw:list=None,xor8:int=0):
```

变量介绍

名称	类型	解释
pth	str	bigfile 保存为文件 pth+'.qwq3'
_files_name	list	文件名
_n	int	文件(及密码)数量
len_psw	int	密码长度
lst_psw	list	许愿密码序列
xor8	int	异或值
返回值	None	无

功能介绍

调用了 `_psw.key_maker` 来生成密码。
`_n` 允许且建议大于实际文件数量，多余位将以随机bit位填充。

_p.mian

函数定义

```
def mian(_psw:str,in_pth:str,out_pth:str=None,_n:int=None,xor8:int=0):
```

变量介绍

名称	类型	解释
`_psw`	`str`	提取密码
`in_pth`	`str`	bigfile `in_pth`
`out_pth`	`str`	输出文件 `out_pth`
`_n`	`int`	文件(及密码)数量
`xor8`	`int`	异或值
返回值	`None`	无

功能介绍

一个密码只能解压对应的一个文件。