* **解题文档**
* **关键技术**

解题主要掌握已知明文攻击分析，古典密码算法分析，密码编码认知，难点是分析已知明文密文对，推测密码算法进而写出解密脚本。

* **解题思路**

1. 解密password.enc
2. 解密flag.enc

* **解题步骤**

1. 解密password.enc



known.txt给出了明文密文对，根据题目意思需要解密password.enc获得解压密码，获得的解压密码之后解压level2.7z进入第二层。

根据掌握的编码密码知识，通过对明文密文对的分析，推测密文最外层使用了base64编码，尝试进行解码：





解码发现有不可显字符，说明base64编码之前还做了加密，推测是异或加密，于是进行验证。



经过简单的验证，发现密文是通过明文与密钥生成的，而所有加密都使用了同一个密钥，根据题目意思推测解出密钥再与加密的解压密码异或便能得到明文的解压密码，于是编写脚本解密password.enc：

*from* base64 *import* b64decode  
*from* Crypto.Util.strxor *import* strxor  
  
*def* decrypt\_data(*ciphertext*):  
 cipher = "JFK63wT1zksfFnACSd93c5WzN5PURZNH"  
 *print* '[!] Cipher:' + cipher  
 plaintext = strxor(b64decode(*ciphertext*), cipher)  
 *return* plaintext  
  
*with* open("password.enc", 'r') *as* f:  
 *print* '[!] Password:' + decrypt\_data(f.read())



1. 解密flag.enc



根据掌握的编码密码知识，通过对明文密文对的分析，发现明文密文中都有大小字母和数字，且长度都相等，推测是替换加密，通过对多组明文密文对的对比分析，发现存在下面的替换关系：

明文：{abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789}

密文：XmQavYuUbsgqAnpZVoCySjrJORBlGTEhPWLNftwciHMDzxFIdKek}{6470513298

于是尝试编写解密脚本：

*import* string  
  
*def* decrypt\_data(*ciphertext*):  
 orig = '{' + string.letters + string.digits + '}'  
 cipher = "XmQavYuUbsgqAnpZVoCySjrJORBlGTEhPWLNftwciHMDzxFIdKek}{6470513298"  
 transl = string.maketrans(cipher, orig)  
 result = *ciphertext*.translate(transl)  
 *print* '[!] Flag:' + result  
  
*with* open('flag.enc', 'r') *as* f:  
 decrypt\_data(f.read())



* **结果提交**

flag{Y0uG0tKn0wnPl4inT3xt4tt4ck}