第三周周报

工业大赛的题：

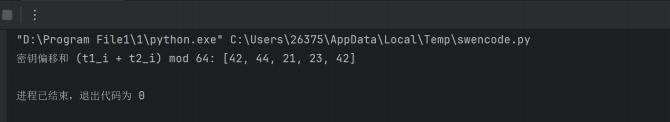
**题目名称：**三维维吉尼亚赛题

**题目答案：flag** **{c3692979a5992a13d06eb094ccf69e1b}**

**解题过程：**

1.根据 py 解读代码，是一个三维查表加密函数。它根据输入字符串 p 和两个密钥 串 t1 、 t2 ， 通 过 字 母 表 偏 移 的 方 式 映 射 成 密 文 。 密 文 是 S0vAeRotMHuuMPqwMHvoGSltRQlwHRx}JOzoOh，

2.找到偏移和



3.再暴力破解

**s** **=** **"ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789abcdefghijklmnopqrstuvwxyz\_** **{}"** **n** **=** **len(s)**

**ciphertext** **=** **"S0vAeRotMHuuMPqwMHvoGSltRQlwHRx}JOzoOh"**

**key\_sums** **=** **[42,** **44,** **21,** **23]** **#** **只用前** **4** **个，后面第** **5** **个是重复**

**def** **idx(c)** **:**

**return** **s.index(c)**

**def** **decrypt\_with\_keys(ciphertext,** **t1,** **t2)** **:**

**res** **=** **""**

**for** **i,** **c** **in** **enumerate(ciphertext)** **:**

**c\_idx** **=** **idx(c)**

**t1\_idx** **=** **t1[i** **%** **4]**

**t2\_idx** **=** **t2[i** **%** **4]**

**p\_idx** **=** **(c\_idx** **-** **t1\_idx** **-** **t2\_idx)** **%** **n**

**res** **+=** **s[p\_idx]**

**return** **res**

**from** **itertools** **import** **product**

**count** **=** **0**

**for** **t1\_candidate** **in** **product(range(n),** **repeat=4)** **:**

**#** **对应** **t2**

**t2\_candidate** **=** **tuple((key\_sums[i]** **-** **t1\_candidate[i])** **%** **n** **for** **i** **in** **range(4))**

**decrypted** **=** **decrypt\_with\_keys(ciphertext,** **t1\_candidate,** **t2\_candidate)**

**if** **decrypted.startswith("flag** **{")** **:**

**print("找到可能密钥！")**

**print("t1** **索引:",** **t1\_candidate)**

**print("t2** **索引:",** **t2\_candidate)**

**print("解密结果:",** **decrypted)**

**break**

**count** **+=** **1**

**if** **count** **%** **1000000** **==** **0** **:**

**print(f"已尝试** **{count}** **种** **t1** **组合")**

**else** **:**

**print("穷举结束，没有找到匹配结果")**

得 到

flag



**Python:**

本周我学习了有关python的知识点（在b站上）

1. 下载pycharm
2. 基本语法：

大小写敏感 ：name 和 Name 是两个不同的变量

使用缩进来划分代码块（推荐使用 4 个空格）

eg：if 5 > 2:

print("5 大于 2") # 这行有缩进，属于if语句块

print("这行没有缩进，不属于if语句块")

单行注释：用 # 开头

多行注释：用三引号 """ 或 ''' 包裹等等

1. 循环：

for 循环：

for 变量 in 序列: # 循环体

Eg：

# 打印1到5

for i in range(1, 6):

print(i)

# 打印1到10的偶数

for i in range(2, 11, 2):

print(i)

break 语句

continue 语句

else 子句

简单代码：

①打印九九乘法表

for i in range(1, 10):

for j in range(1, i+1):

print(f"{j}×{i}={i\*j}", end="\t")

print()

②计算 1 到 100 之间所有偶数的和

total = 0

for num in range(1, 101):

if num % 2 == 0:

total += num

print(f"1到100之间所有偶数的和是：{total}")

4.函数：

def 函数名(参数列表):

# 函数体

return 返回值 # 可选

函数的调用以及传参，参数这里不再一一列举

代码示例：

实现一个简单的计算器

def calculator(a, b, operator):

if operator == '+':

return a + b

elif operator == '-':

return a - b

elif operator == '\*':

return a \* b

elif operator == '/':

if b == 0:

return "错误：除数不能为0"

return a / b

else:

return "错误：不支持的运算符"

# 使用计算器

print(calculator(10, 5, '+'))

print(calculator(10, 5, '-'))

print(calculator(10, 5, '\*'))

print(calculator(10, 5, '/'))

print(calculator(10, 0, '/'))

print(calculator(10, 5, '^'))