## 思路：

```
  sub_402230();
  printf("Give me your code:\n");
  sub_40E5F0("%s", Str);
  if ( strlen(Str) != 33 )
  {
    printf("Wrong!\n");
    system("pause");
    exit(0);
  }
  for ( i = 0; i <= 32; ++i )
  {
    byte_414040[i] = Str[dword_40F040[i]];
    byte_414040[i] ^= LOBYTE(dword_40F040[i]);
  }
  for ( j = 0; j <= 32; ++j )
  {
    if ( byte_40F0E0[j] != byte_414040[j] )
    {
      printf("Wrong!\n");
      system("pause");
      exit(0);
    }
  }
  printf("Right!Good Job!\n");
  printf("Here is your flag: %s\n", Str);
  system("pause");
  return 0;
}
```

可以看到check的字符串在0x40f0e0处，0x414040处的字符串为输入经过变换的。

对输入进行逆变换（即对0x40f0e0的字符串返回输入flag）
首先对0x40f0e0处进行异或处理。
然后再进行位置转换。

File Edit Format Run Options Window Help

```
from idc_bc695 import *
addr = 0x40f0e0
check =[]
for i in range(33):
    check.append(Byte(addr+i))

addr = 0x40f040
index = []
for i in range(33):
    index.append(Byte(addr+4*i))
print(index)
for i in range(33):
    check[i] ^= index[i]
print(check)
flag=[]
for i in range(33):
    flag.append(0)

for i in range(33):
    flag[index[i]] = check[i]

print(bytes(flag))
```

```
[9, 10, 15, 23, 7, 24, 12, 6, 1, 16, 3, 17, 32, 29, 11, 30, 27, 22, 4, 13, 19, 20, 21, 2, 25, 5, 31, 8, 18, 26, 28, 1
[110, 115, 116, 104, 114, 51, 48, 84, 82, 105, 84, 79, 125, 95, 112, 51, 49, 112, 70, 115, 95, 67, 108, 67, 114, 123,
b'MRCTF{Tr4nsp0sltiON_Clph3r_1s_3z}'
```