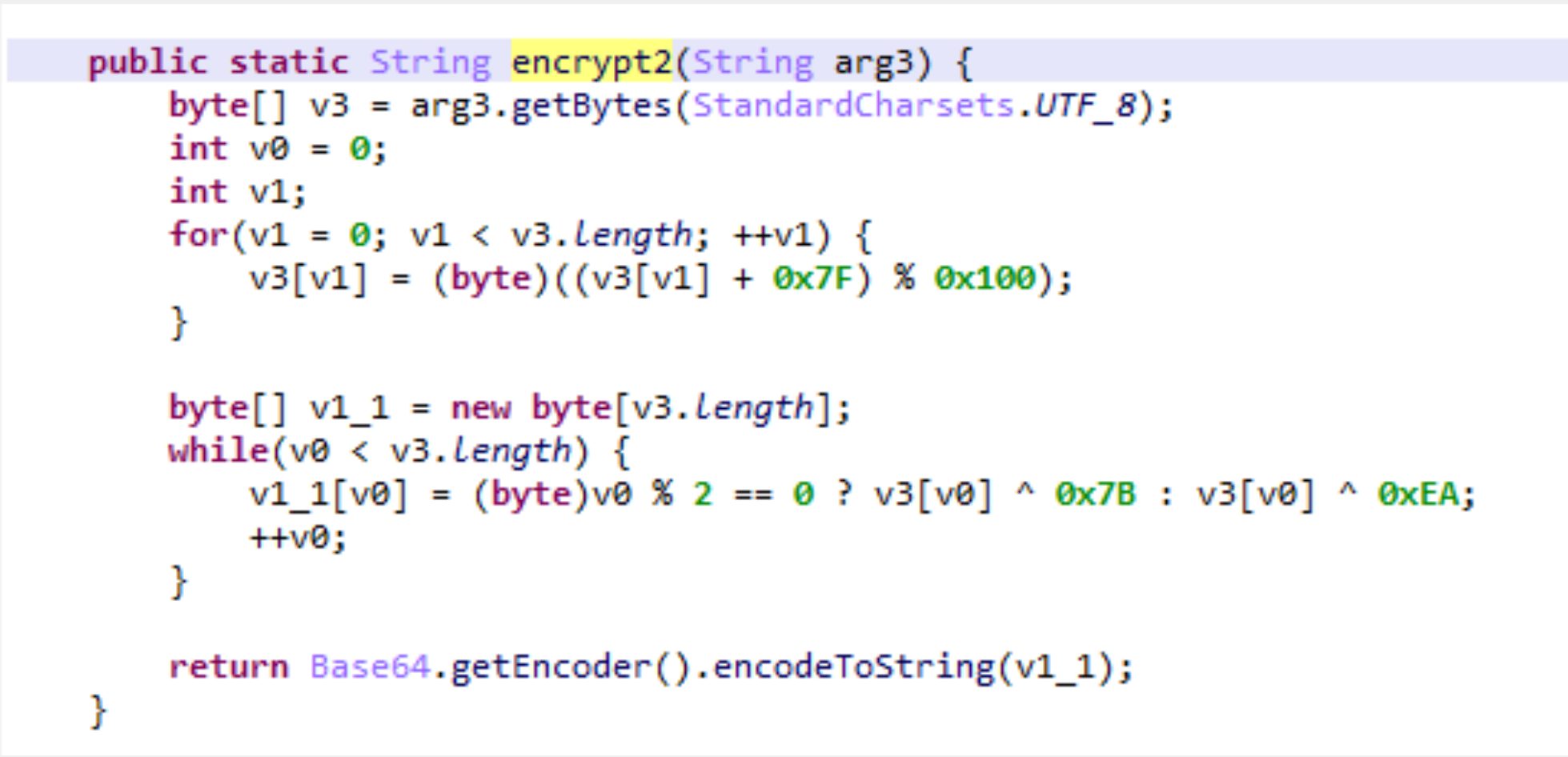
Nebu1ea 韩磊 [1504895347@qq.com](mailto:1504895347@qq.com)

Mobile:Puzzle\_Game

解题思路：



上方图片是主要的加密函数，有个array是随机出来的，根据函数推断随机数种子是0xd7c，根据随机数的性质，我们可以利用随机序列的固定性跑出来一个数组，之后按照加法和异或逻辑写exp就能解出来flag，exp如下

Exp:

from ctypes import c\_uint8

import base64

def convert\_to\_ord(string):

    return [ord(char) for char in string]

def convert\_to\_uint8(list):

    return [c\_uint8(num).value for num in list]

def encode\_base64(byte\_array):

    return base64.b64encode(bytes(byte\_array)).decode()

def xor\_operation(data, key):

    return [data[i] ^ key[i % len(key)] for i in range(len(data))]

def add\_and\_mask(data):

    return [(num + 0x7f) & 0xff for num in data]

def xor\_with\_condition(data):

    return [num ^ 0x7b if i & 1 == 0 else num ^ 0xea for i, num in enumerate(data)]

def generate\_encoded\_string(input\_str, key):

    encoded\_str = xor\_operation(convert\_to\_ord(input\_str), convert\_to\_uint8(key))

    combined\_list = [num % 256 for num in (key + encoded\_str)]

    encoded\_str2 = add\_and\_mask(convert\_to\_ord(encode\_base64(combined\_list)))

    final\_encoded\_str = xor\_with\_condition(encoded\_str2)

    return "ISCC{%s}" % encode\_base64(final\_encoded\_str)[:32]

input\_str = "04999999gwC9nOCNUhsHqZm"

key = [-67, 55, 95, -42, -24, 94, -98, 56, 115, 17, 97, -46, -89, 122, -18, -25]

print(generate\_encoded\_string(input\_str, key))

上方的key值就是由伪随机数逻辑跑出来的数组