把res 替换成自己的就可以了

ida 直接检索字节序列 unk\_7FF7899C0010

#RC4加密

def rc4(key, ciphertext):

# 初始化S盒

sbox = list(range(256))

j = 0

for i in range(256):

j = (j + sbox[i] + (key[i % len(key)])) % 256

sbox[i], sbox[j] = sbox[j], sbox[i]

# 生成密钥流

i = 0

j = 0

keystream = []

flag = []

for byte in ((ciphertext)):

i = (i + 1) % 256

j = (j + sbox[i]) % 256

sbox[i], sbox[j] = sbox[j], sbox[i]

k = sbox[(sbox[i] + sbox[j])%256]

keystream.append(k)

print("key1:",(keystream))

# pause()

# 解密密文

plaintext = []

for i in range(len(ciphertext)):

m = ciphertext[i] ^ keystream[i]

plaintext.append(m)

print("res:",plaintext)

print(bytes(plaintext).decode("latin-1"))

key= b"SecretKey"

res = [

0x1C, 0xB8, 0x2E, 0x47, 0xDD, 0x72, 0x1C, 0xA2, 0xDE, 0x13,

0x52, 0x46, 0x82, 0xF0, 0x62, 0x81, 0xB2, 0xE6, 0xCC, 0xEE,

0x2E, 0x9A, 0x1E, 0x28, 0x16, 0x6B, 0xAB, 0xE8, 0x9C, 0x24,

0xFD, 0x3F, 0xD0, 0x15, 0x3E, 0x17, 0xCA, 0x91, 0xC0, 0xFE,

0x35, 0x74 # 最后一个非零字节是 0x74

]

res2 = []

for i in range(0,len(res)):

if i %2 ==0:

res2.append(res[i]^0x41)

else :

res2.append(res[i])

print((res2))

print(len(res))

plaintext = rc4(key, res2)

print()