trivial writeup 实验吧

原创

FrancisQiu 于 2019-02-23 19:47:00 发布 198 收藏

分类专栏： CTFwriteup crypto CTF 实验吧

本文链接：https://blog.csdn.net/qq_40737798/article/details/87896201


CTFwriteup 同时被 3 个专栏收录

8 篇文章 0 订阅

订阅专栏


crypto

5 篇文章 0 订阅

订阅专栏


CTF

7 篇文章 0 订阅

订阅专栏

trivial-writeup-实验吧

题目

> An unlocked terminal is displaying the following:
> Encryption complete, ENC(???,T0pS3cre7key) = Bot kmws mikferuigmzf rmfrxrwqe abs perudsf! Nvm kda ut ab8bv_w4ue0_ab8v_DDU
> You poke around and find this interesting file.
> 解题链接： http://ctf5.shiyanbar.com/crypto/trivial/encrypt.rar

解题

思路

下载解题链接之后，发现是个encrypt的py文件，打开发现以下代码：

```
#!/usr/bin/env python
import sys

alphaL = "abcdefghijklnmopqrstuvqxyz"
alphaU = "ABCDEFGHIJKLMNOPQRSTUVQXYZ"
num    = "0123456789"
keychars = num+alphaL+alphaU

if len(sys.argv) != 3:
  print "Usage: %s SECRET_KEY PLAINTEXT"%(sys.argv[0])
  sys.exit()

key = sys.argv[1]
if not key.isalnum():
  print "Your key is invalid, it may only be alphanumeric characters"
  sys.exit()

plaintext = sys.argv[2]

ciphertext = ""
for i in range(len(plaintext)):
  rotate_amount = keychars.index(key[i%len(key)])
  if plaintext[i] in alphaL:
    enc_char = ord('a') + (ord(plaintext[i])-ord('a')+rotate_amount)%26
  elif plaintext[i] in alphaU:
    enc_char = ord('A') + (ord(plaintext[i])-ord('A')+rotate_amount)%26
  elif plaintext[i] in num:
    enc_char = ord('0') + (ord(plaintext[i])-ord('0')+rotate_amount)%10
  else:
    enc_char = ord(plaintext[i])
  ciphertext = ciphertext + chr(enc_char)

print "Encryption complete, ENC(%s,%s) = %s"%(plaintext,key,ciphertext)
```

其中for循环那块是真正加密的过程。显然，这是个对称加密的过程。加密依赖一个一次同余式以及rotate_amount进行：

> rotate_amount=keychars.index(key[i%len(key)]
> enc_text[i]-C1 =（plaintext[i]+rotate_amount）mod C2 (其中C1、C2为常数）

因此考虑写个python脚本进行解密，依赖以下两个公式：

> rotate_amount=keychars.index(key[i%len(key)]
> plaintext[i] =[(enc_text[i]-C1-rotate_amount) mod C2]+ C1 (其中C1、C2为常数）

我的脚本代码：

> https://github.com/FrancisQiu/-shiyanbar_Crypto/pull/1/commits/067673eeab7d238307804f8ef01c6cbe2f6b7edd