Alaska47 / RC3CTF-2016-Writeups

Watch 5 Star 1 Fork 0

Code Issues 0 Pull requests 0 Projects 0 Pulse Graphs

Branch: master ▾ RC3CTF-2016-Writeups / crypto / 100-Salad / Create new file Find file History

pwang00 committed on GitHub Add solution script for 100-Salad Latest commit 3b1a2bd on 24 Nov 2016

..

README.md	Add writeup for 100-Salad	4 months ago
Salad.py	Add solution script for 100-Salad	4 months ago

README.md

#100 - Salad

##Problem Statement

“The fault, dear Brutus, is not in our stars, but in ourselves.” (I.ii.141) Julius Caesar in William Shakespeare’s Julius Caesar
Cipher Text: 7sj-ighm-742q3w4t

##Overview

Decrypt a Caesar cipher with a custom alphabet

##Solution

From the problem statement, we can reasonably infer that the ciphertext is to be decrypted in a manner similar to that of a caesar cipher. However, since the flag has to begin with uppercase "RC3-2016", we conclude that a custom alphabet was used for encryption. We take a look at the charset of the ciphertext (excluding the dashes - those don't get shifted), and find that it fits within

```
abcdefghijklmnopqrstuvwxyz0123456789
```

Our next step is to find out the correct shift. This python snippet does just that, and prints out the message if it contains "RC3-2016".

```
import string

alphabet =  string.ascii_lowercase + string.ascii_uppercase + string.digits

ctext = "7sj-ighm-742q3w4t"

def shift(n):
    message = ""
    for index, char in enumerate(ctext):
        if char == "-":
            message += char
        else:
            message += alphabet[(alphabet.index(ctext[index])+n)%len(alphabet)]
    return message.upper()

for i in range(len(alphabet)):
    message = shift(i)
    if "RC3" in message:
        print(message)
```

Running it returns the flag:

RC3-2016-ROMANGOD

##Flag

```
RC3-2016-ROMANGOD
```