

This repository | Search

Pull requests | Issues | Gist

ctfs / write-ups-2014

Watch

219

Star

1,279

Fork

457

<> Code

Issues 15

Pull requests 0

Projects 0

Pulse

Graphs

Branch: master | write-ups-2014 / tinyctf-2014 / safer-than-rot13 /

Create new file

Upload files

Find file

History

abpolym Add several writeup links for 31c3, 9447, asis-finals, hacklu, tinyctf Latest commit e819e3c on Mar 25 2015

..

README.md Add several writeup links for 31c3, 9447, asis-finals, hacklu, tinyctf 2 years ago

cry100.zip tinyCTF 2014: add placeholders 3 years ago

README.md

tinyCTF 2014: Safer than rot13

Category: Crypto Points: 100 Description:

[Download file](#)

Write-up

Let's extract [the provided cry100.zip file](#):

```
$ unzip cry100.zip
Archive:  cry100.zip
  inflating: cry100
```

The extracted cry100 file is a text document:

```
$ file cry100
cry100: ASCII text, with CRLF line terminators
```

It contains the following ciphertext:

```
XMVZGC RGC AMG RVMG HGFGMQYCD VT VWM BYNO, NSVWDS NSGO RAO XG UWFN AF
HACDGMVWF. AIRVFN AII AMG JVRVC-XVMC, FYR BIG TVIZ ESV SAH CGQGM XGGC
RVMG NSAC A RYIG TMVR NSG SVWFG ESGMG NSGO EGMG XVMC WCNYI NSG HAO
FVRG IVMH JARG MVWCH NV NAZG NSGR VTT NV EAM. OVWM TIAD YF "CV NSYF
YF CVN JMOBNV RO HGAM", YC IVEGMJAFG, EYNS WCHGMFJVMGF YCFNGAH VT
FBAJGF, FWMVWCHGH XO NSG WFWAI "TIAD" NAD ACH JWMIO XMAJGF. GCUVO.
```

This string is encoded using a substitution cipher. Specifically, it is a [cryptogram](#), a cipher in which each letter is replaced by some other letter. One way to identify a substitution cipher is to run [character frequency analysis](#) on the ciphertext.

Using a cryptogram solver like [quipqiup.com](#) (and assuming that the cleartext is in English) reveals that the key is AXJHGTD SYUZIRC VBPMFNWQEKOL . The cleartext is:

```
BROKEN MEN ARE MORE DESERVING OF OUR PITY, THOUGH THEY MAY BE JUST AS
DANGEROUS. ALMOST ALL ARE COMMON-BORN, SIMPLE FOLK WHO HAD NEVER BEEN
MORE THAN A MILE FROM THE HOUSE WHERE THEY WERE BORN UNTIL THE DAY
SOME LORD CAME ROUND TO TAKE THEM OFF TO WAR. YOUR FLAG IS "NO THIS
IS NOT CRYPTO MY DEAR", IN LOWERCASE, WITH UNDERSCORES INSTEAD OF
SPACES, SURROUNDED BY THE USUAL "FLAG" TAG AND CURLY BRACES. ENJOY.
```

The flag is `flag{no_this_is_not_crypto_my_dear}` .

Other write-ups and resources

- <http://sugarstack.io/tinyctf-cry-100.html>
- <https://github.com/evanowe/TinyCTF2014-writeups/blob/master/README.md#safer-than-rot13>
- <https://github.com/jesstess/tinyctf/blob/master/rot13/rot13.md>
- <http://barrebas.github.io/blog/2014/10/03/tinyctf/>

