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 / defkthon-ctf / crypto-100 /   Create new file   Upload files   Find file   History

mathiasbynens Normalize headers   Latest commit a7ab67c on Oct 14 2014

..

README.md	Normalize headers	3 years ago

README.md

DEFKTHON CTF: Crypto 100

Description:

> ucoizsbtkxhtadcg

Write-up

During the CTF, a hint for this challenge was provided:

> [Crypto 100] Clue: Vinegar

Since this is crypto challenge, the clue could be an indication that this is a Vigenère cipher.

Let's fire up a Windows VM, open Cryptool 1, enter the ciphertext `ucoizsbtkxhtadcg`, and do some analysis. Go to *Analysis → Symmetric Encryption (Classic) → Vigenère (Analysis according to Schroedel…)* and click *Start analysis*. The analysis takes a few minutes. Once it's finished, click *Show analysis results*, and exactly 9011 possible encryption keys and deciphered texts are presented:

```
CrypTool: Ciphertext-only analysis according to Schroedel against Vigenère cipher
Time needed to perform analysis:758 seconds
Length of analyzed ciphertext: 16 characters
Keyword language(s): English
Ciphertext language: English

Ciphertext:
UCOIZSBTKXHTADCG

…
```

At this point I guessed that either the encryption key or the deciphered text would contain `FLAG` so I searched the result set for that. It turned out that many of the deciphered texts started with `FLAGIS`, so I decided to focus on those first:

```
$ grep -B3 'FLAGIS' results.txt
114. Possible key:
PROCRASTINATIONS
Found cleartext:
FLAGISJACKHASPPO
--
418. Possible key:
PROCRASTINATING
Found cleartext:
FLAGISJACKHASQWR
--
419. Possible key:
PROCRASTINATION
Found cleartext:
```

```
FLAGISJACKHASPPR
--
420. Possible key:
PROCRASTINATORS
Found cleartext:
FLAGISJACKHAMMKR
--
836. Possible key:
PROCRASTINATED
Found cleartext:
FLAGISJACKHAWANP
--
837. Possible key:
PROCRASTINATES
Found cleartext:
FLAGISJACKHAWLNP
--
838. Possible key:
PROCRASTINATOR
Found cleartext:
FLAGISJACKHAMMNP
--
1493. Possible key:
PROCRASTINATE
Found cleartext:
FLAGISJACKHAWOLS
```

At this point I tried entering `JACKHASPPO` , `JACKHASQWR` , etc. as the flag, but none of them were accepted. Looking through the list again, one of the cleartexts stood out:

```
420. Possible key:
PROCRASTINATORS
Found cleartext:
FLAGISJACKHAMMKR
```

`JACKHAMMKR` wasn't accepted either, and neither was `JACKHAMMER` . However, since the ciphertext was originally in lowercase instead of uppercase, I figured the expected cleartext was probably in lowercase too. So I guessed `jackhammer` was the flag, which turned out to be correct!

P.S. With the knowledge that `jackhammer` is the correct flag, we can figure out the encryption key that was originally used: `PROCRASTINATORY` . (Apparently this word is not included in the English dictionary used by Cryptool.)

Other write-ups and resources

- none yet