Plaid CTF 2014: twenty

Category: Crypto Points: 20 Description:

> It's so far in the past, computers haven't even been imagined, let alone used. But somehow The Plague has already been here, building an evil army of hackers. Can you find his secret message?

Write-up

After extracting the tarball we end up with a file named `twenty.txt` with the following contents:

```
fvoxoxfvwdepagxmwxfpukleofxhwevefuygzepfvexwfvufgeyfryedojhwffoyhxcwgmlxeylawfxfurwfvoxecfezfvwbecpfpeejuyg
```

The string is encoded using a Vigenère cipher: each letter of the alphabet represents a number from 0 to 25. The key is added to the original message to form the decoded message. Since the message is usually longer than the key it is necessary to duplicate the key until it reaches the length of the original message. To decode the message, the key is subtracted from the decoded message to obtain the original message.

`cipher_solver.py` uses an implementation of the hill climbing algorithm to calculate the key. It is assumed that the key is a permutation of all the letters of the alphabet. The algorithm starts with the key `ABC…Z` and calculates the decoded message. The `ngram_score` module is used to calculate the score of this decoded string. `ngram_score` uses `quadgrams.txt` which is a file that lists all combinations of 4 characters and their occurence frequency in the English language.

By searching the decoded string for these n-grams it is possible to calculate a score for the decoded string. If this decoded strings score is higher (resembled the English language better) than the previous score, this key is presumed to be closer to the final key and it will be used in the next iteration of the hill climbing algorithm.

For each iteration, two characters are swapped and the previously explained process is repeated until the user stops the program or the score of the decoded string exceeds `maxscore`.

This delivered the correct decoded string which contained the flag.

The flag is `sincenewcryptomighthavensabackdoorsiuseoldcrypto`.

Other write-ups and resources

- https://ucs.fbi.h-da.de/writeup-plaidctf-2014-twenty/

- https://docs.google.com/a/google.com/document/d/1WthFuKx3sAtqTVPOklVJt12MMS3lrxITGglskPKNtL8/edit
- http://csrc.tamuc.edu/css/?p=169
- Source code for this challenge, released after the CTF
- https://github.com/hackerclub/writeups/blob/master/plaidctf-2014/twenty/WRITEUP-arthurdent.md
- Indonese