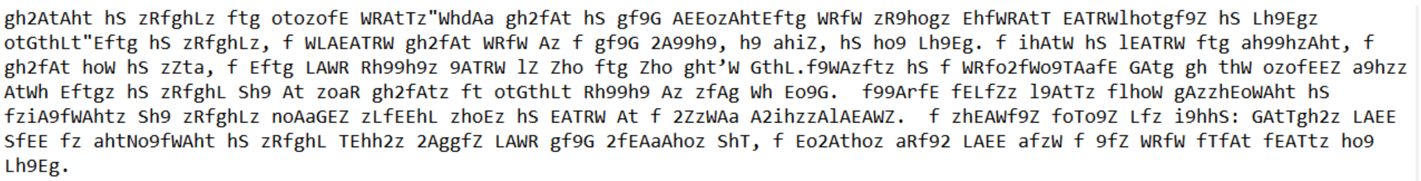
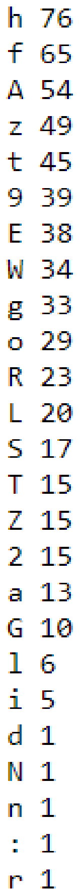
Norman Zhao
Offensive Security Write Up
SwampCTF: Orb of Light 1: Secret [477]



```
gh2AtAht hS zRfghLz ftg otozofE WRAtTz"WhdAa gh2fAt hS gf9G AEEozAhtEftg WRfW zR9hogz EhfWRAtT EATRWlhotgf9Z hS Lh9Egz
otGthLt"Eftg hS zRfghLz, f WLAEATRW gh2fAt WRfW Az f gf9G 2A99h9, h9 ahiZ, hS ho9 Lh9Eg. f ihAtW hS lEATRW ftg ah99hzAht, f
gh2fAt hoW hS zZta, f Eftg LAWR Rh99h9z 9ATRW lZ Zho ftg Zho ght'W GthL.f9WAzftz hS f WRfo2fWo9TAafE GAtg gh thW ozofEEZ a9hzz
AtWh Eftgz hS zRfghL Sh9 At zoaR gh2fAtz ft otGthLt Rh99h9 Az zfAg Wh Eo9G.  f99ArfE fELfZz l9AtTz flhoW gAzzhEoWAht hS
fziA9fWAhtz Sh9 zRfghLz noAaGEZ zLfEEhL zhoEz hS EATRW At f 2ZzWAa A2ihzzAlAEAWZ.  f zhEAWf9Z foTo9Z Lfz i9hhS: GAtTgh2z LAEE
SfEE fz ahtNo9fWAht hS zRfghL TEhh2z 2AggfZ LAWR gf9G 2fEAaAhoz ShT, f Eo2Athoz aRf92 LAEE afzW f 9fZ WRfW fTfAt fEATtz ho9
Lh9Eg.
```



```
h 76
f 65
A 54
z 49
t 45
9 39
E 38
W 34
g 33
o 29
R 23
L 20
S 17
T 15
Z 15
2 15
a 13
G 10
l 6
i 5
d 1
N 1
n 1
: 1
r 1
```

Downloading the file yields a zip with 2 files: a story.txt that has some background story within the DnD universe, and a secret_message.txt. The secret message is a jumble of characters. After counting the amount of characters in the secret message and ordering the by frequency, there are only 24 letters (one of the characters was a colon, which I will assume to remain as is). This indicates that the message is probably encrypted using a substitution cypher. The deciphered text will be in all lowercase for increased readability.

The first clue was that the letter **f** showed up by itself, and occurred the second most frequently, meaning it can be the letter *a* or *I*. Since some of the instances had longer words coming after it, it seemed unlikely to be *I*, leading me to decipher the first letter as *a*.

The next clue was that **hS** showed up together often, and **h** by itself occurred the most frequently. Using letter frequency tables showed that **e**, **t**, **a** and **o** occurs the most, and of those, **t** and **o** can be meant that **hS** is **to** or **of**. Because **S** doesn't show up that often, I went with *of*, as **f** occur less often than **o**.

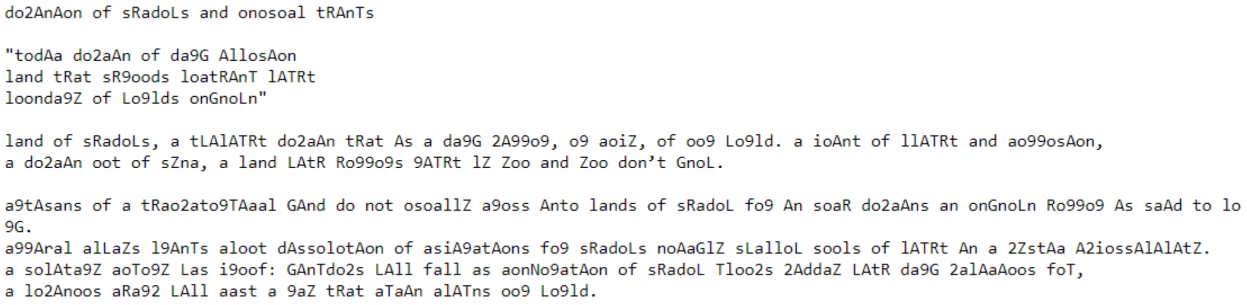
The letter *z* occurs pretty often at the end of words, leading me to substitute it as **s**.

The letters *ftg* also shows up often and since I know that *f* is **a**, this leads me to believe that *ftg* is **and**.

There are also a lot of pairings of **EE**, and an occurrence of **Eftg**. Since I'm substituting **ftg** to and, then **E** has to be a pairing of the same letter that should show up before and. This leads me to believe that **E** is *l* so **Eftg** is *land*.

An easy substitution was made when I saw that there was a *don'***W**, meaning **W** had to be *t*, making the word *don't*.

After these substitution, the secret now reads

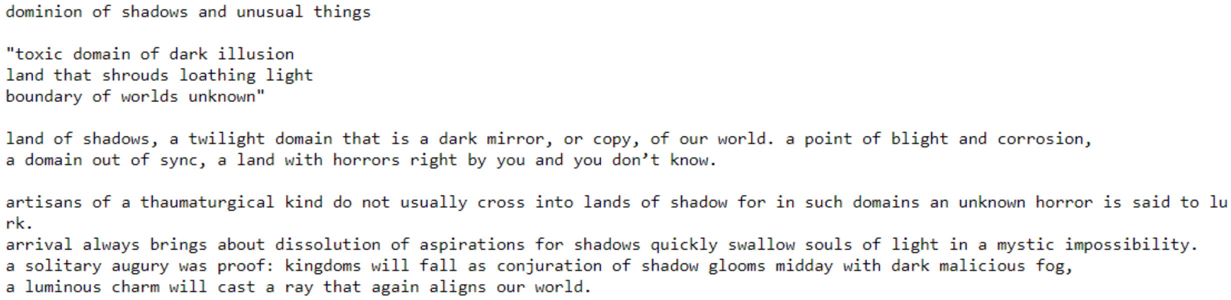


```
do2AnAon of sRadoLs and onosoal tRAnTs

"todAa do2aAn of da9G AllosAon
land tRat sR9oods loatRAnT lATRt
loonda9Z of Lo9lds onGnoLn"

land of sRadoLs, a tLAlATRt do2aAn tRat As a da9G 2A99o9, o9 aoiZ, of oo9 Lo9ld. a ioAnt of llATRt and ao99osAon,
a do2aAn oot of sZna, a land LAtR Ro99o9s 9ATRt lZ Zoo and Zoo don't GnoL.

a9tAsans of a tRao2ato9TAaal GAnd do not osoallZ a9oss Anto lands of sRadoL fo9 An soaR do2aAns an onGnoLn Ro99o9 As saAd to lo
9G.
a99Aral alLaZs l9AnTs aloot dAssolotAon of asiA9atAons fo9 sRadoLs noAaGlZ sLalloL sools of lATRt An a 2ZstAa A2iossAlAlAtZ.
a solAta9Z aoTo9Z Las i9oof: GAnTdo2s LAll fall as aonNo9atAon of sRadoL Tloo2s 2AddaZ LAtR da9G 2alAaAoos foT,
a lo2Anoos aRa92 LAll aast a 9aZ tRat aTaAn alATns oo9 Lo9ld.
```

Picking semi-completed words, I substituted:

-*s***R***ado***L***s* is probably *shadows*, meaning **R** and **L** are actually *h* and *w*
-*wo***9***ld* is probably *world*, meaning **9** is *r*
- **o***n***o***s***o***al* has 3 unknowns in the same word, meaning they're probably a vowel, leading me to believe that **o** is *u*
- **l***oundar***Z** of worlds *un***G***nown* is probably *boundary of worlds unknown*, so **l**, **Z** and **G** are *b*,*y* and *k* respectively
- *dom***A***n***A***on* and *doma***A***n* are similar and are all the same letters, and especially for *doma***A***n*, its highly likely **A** is *i*, making the words *dominion* and *domain*
- **a***orrosion* has to be *corrosion*, so **a** is *c*
- *thin**Ts* is probably *things*, so **T** is g
- *ioint* is most likely *point*, so **i** is *p*
-*arriral* is *arrival*, so **r** is *v*
-*todic* can be toric, toxic, tonic, but since r and n are solved, **d** is *x*
-*conNuration* is *conjuration*, since it fits with the theme and *j* hasn't mapped yet.

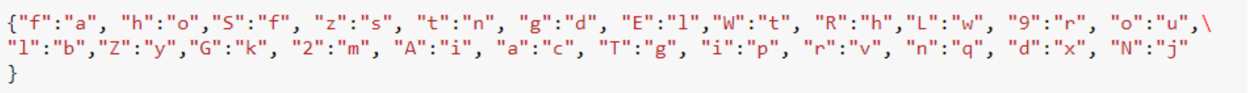
Substituting everything yields the full message:



```
dominion of shadows and unusual things

"toxic domain of dark illusion
land that shrouds loathing light
boundary of worlds unknown"

land of shadows, a twilight domain that is a dark mirror, or copy, of our world. a point of blight and corrosion,
a domain out of sync, a land with horrors right by you and you don't know.

artisans of a thaumaturgical kind do not usually cross into lands of shadow for in such domains an unknown horror is said to lu
rk.
arrival always brings about dissolution of aspirations for shadows quickly swallow souls of light in a mystic impossibility.
a solitary augury was proof: kingdoms will fall as conjuration of shadow glooms midday with dark malicious fog,
a luminous charm will cast a ray that again aligns our world.
```

…but no flag.

Looking at the keys though, yields something interesting:



```
{"f":"a", "h":"o","S":"f", "z":"s", "t":"n", "g":"d", "E":"l","W":"t", "R":"h","L":"w", "9":"r", "o":"u",\
"l":"b","Z":"y","G":"k", "2":"m", "A":"i", "a":"c", "T":"g", "i":"p", "r":"v", "n":"q", "d":"x", "N":"j"
}
```

f maps to a, l maps to b, a maps to c, and g maps to d. So flag decoded becomes abcd. After flipping the values and keys in the dictionary, sorting those keys, and printing them, I got the flag!

After adding the curly braces: flag{STRANGE2thin9zWorLdZ}, I submitted the flag.

Challenge completed!

I used https://www.math.cornell.edu/~mec/2003-2004/cryptography/subs/frequencies.html for letter frequencies.