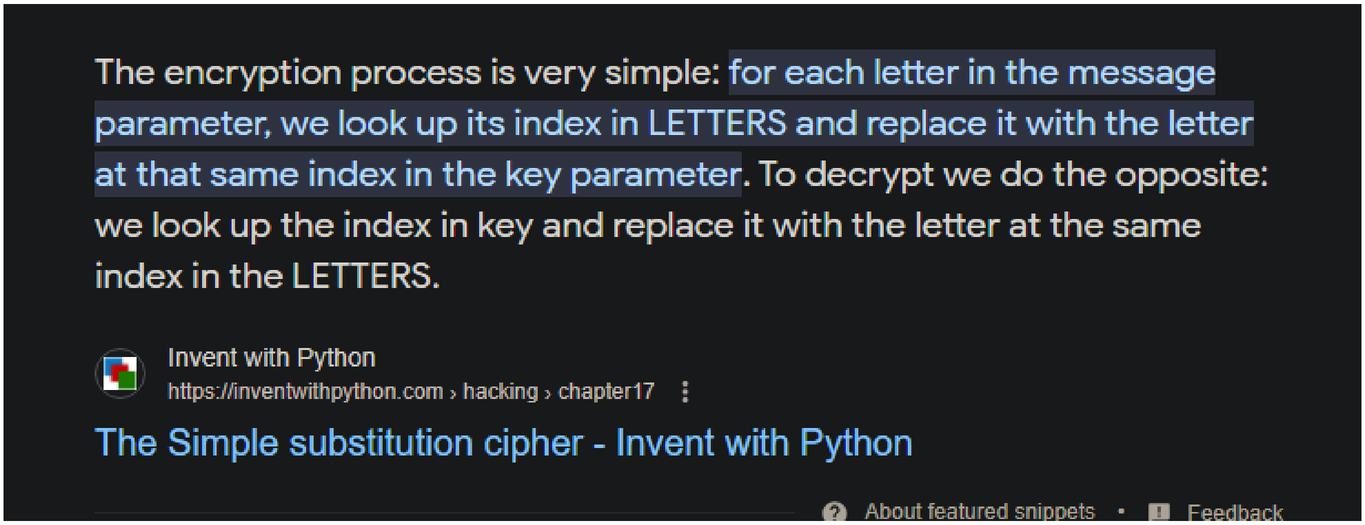
Alphabet Soup Writeup

The user starts with the script which contains three variables, alphabet, key and output. It is hoped that later in the CTF these three variables will help the user find the necessary documentation to get the flag. The program then also contains one function, decrypt which takes two inputs, cipher and key, which is a further hint about what needs to be included for this challenge, although is not actually necessary as the variables are global variables and thus can be mentioned in the function.

The original hint for this challenge is "I can't remember what this cipher was called but something to do with the alphabet being equal to a different letter", with this hoping to be a reference for the user to a substitution cipher. If we Google "substitution cipher python" we find more information about the cipher:



The encryption process is very simple: for each letter in the message parameter, we look up its index in LETTERS and replace it with the letter at that same index in the key parameter. To decrypt we do the opposite: we look up the index in key and replace it with the letter at the same index in the LETTERS.

Invent with Python
https://inventwithpython.com › hacking › chapter17

The Simple substitution cipher - Invent with Python

And also a StackOverflow link for code implementing the necessary functions in this program. The only reply documents the necessary information to be implemented into this code, so if you are interested in understanding how it works then continue to work on, otherwise, feel free to skip down.

```
keyIndices = [key.index(k) for k in cipher]
return ''.join(alphabet[keyIndex] for keyIndex in keyIndices)
```

We start by creating a list called "keyIndicies" which contains the position of each character in the encrypted text related to the key - `key.index(k)` is responsible for getting the indexed position with the latter section - `for k in cipher` being a "for" loop that executes throughout the string.

We then perform our decryption by iterating through each position in the key and retrieving the character in the alphabet that correlates with the character stored at the same position in the key. These are joined together which eventually gives the decrypted string.

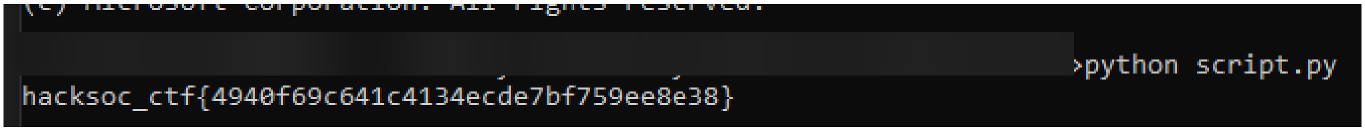
From here, we can alter our script to include the necessary lines, and then run the script for our flag.

```python
import random

alphabet = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz1234567890}_{"
key = "PIRfjL7cksiO2pZhH_zY}AUSxl0DCQTeMwVBbyn9JKq1oavrt53F8Gd{ENWuX46gm"
output = "w0CboJCgCaem{X{4eNXCN{8C{8d{TCQTWDeWEXTTuTdu6"

def decrypt(cipher, key):
    keyIndices = [key.index(k) for k in cipher]
    return ''.join(alphabet[keyIndex] for keyIndex in keyIndices)

final_output = decrypt(output, key)
print(final_output)
```



```
(c) Microsoft Corporation. All rights reserved.

[redacted]>python script.py
hacksoc_ctf{4940f69c641c4134ecde7bf759ee8e38}
```