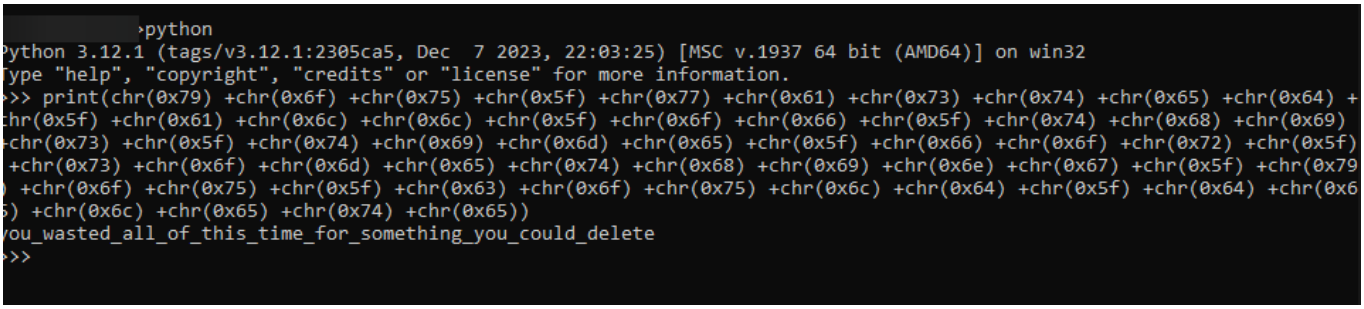
Password Please - Writeup

Starting with the script, the user has an incredibly long cipher text and also an encrypt function. Reading through the purpose of this we can hopefully realise that the function iterates through each letter of the message the user wanted to encrypt and adds as many random letters as the value "key" is, which is the other value the user has provided. For example, if the user passed the string "hello" and the key "5" then the output would look something like the following:

- "h" into "hA5S2B" as 5 random characters have been appended onto the actual character.
- "e" into "eDH12N" etc.

Knowing this, we can move onto our next problem, the incredibly long password. Well, it's not actually relevant to the program but for those who decided to solve the password, you could have manually figured out what each value converted to, or made life easy and ran it in Python.



So we know how the encryption function works but the key could be anything, luckily we know the flag format so that doesn't matter as long as we look at the results. We can use a neat for loop in our decrypt function to reverse the process and then iterate the key until we find an output that indicates we have found the correct key.

```
original_text = ''.join([ciphertext[i] for i in range(0, len(ciphertext),
step)])
```

This for loop iterates through each letter of the `ciphertext` variable and, for every letter that occurs every `step` letters in the ciphertext, appends it to the `original_text` variable. We can now create some kind of automation for the key, with the method I chose to simply by increasing it in the main function and iterating through until it found a string that started with "HACKSOC" with our final code looking like:

```
def decrypt(ciphertext, key):
    original_text = ''.join([ciphertext[i] for i in range(0, len(ciphertext),
key)])
    return original_text
```

```python
def main():
    ciphertext = input("Input the text: ")
    key = 0
    for i in range(100):
      key = key + 1
      decrypted_text = decrypt(ciphertext, key)
      print(decrypted_text)
      if (decrypted_text[:7] == "HACKSOC"):
         print (decrypted_text)
         break
      else:
         continue

if __name__ == "__main__":
  main()
```

If we then input our encrypted flag, we'll get the decrypted version and have our flag!