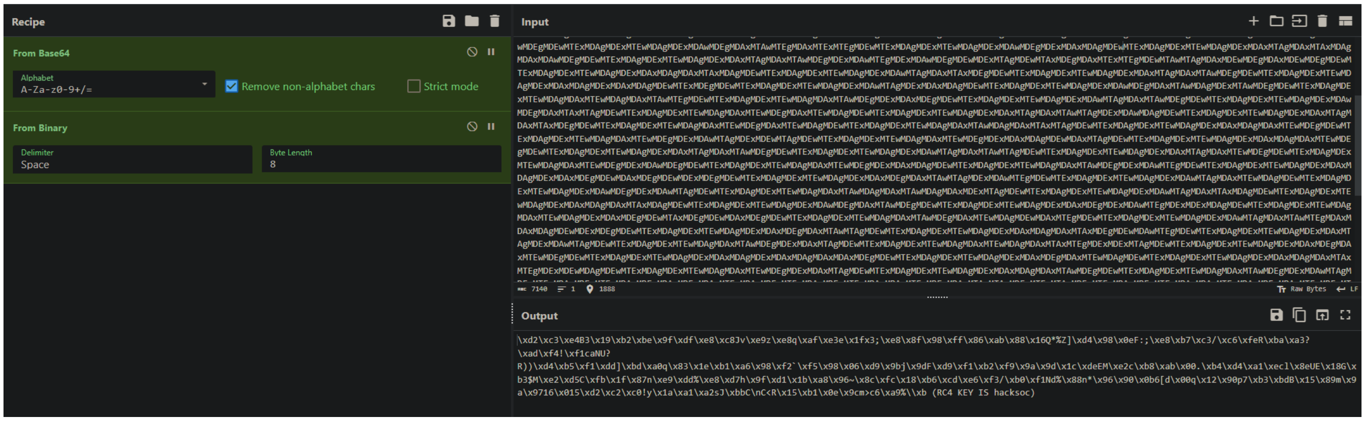
RC4 Writeup

The user starts with a text file containing a random piece of string, with the only hint being a tail on the end (=). Placing the text into CyberChef reveals some binary code, which, once passed through CyberChef again reveals a set of characters with some cleartext at the end.



Recipe

From Base64

Alphabet A-Za-z0-9+/= ☑ Remove non-alphabet chars □ Strict mode

From Binary

Delimiter Space Byte Length 8

Input

wMDEgMDEwMTExMDAgMDExMTEwMDAgMDExMDAwMDEgMDAxMTAwMTEgMDAxMTExMTEgMDEwMTExMDAgMDExMTEwMDAgMDExMDAwMDEgMDExMDAxMDAgMDEwMTExMDAgMDExMTEwMDAgMDExMDAxMTAgMDAxMTAxMDAg
MDAxMDAwMDEgMDEwMTExMDAgMDExMTEwMDAgMDExMDAxMTAgMDAxMTAwMDEgMDExMDAwMTEgMDExMDAwMDEgMDEwMDExMTAgMDEwMTAxMDEgMDAxMTExMTEgMDEwMTAwMTAgMDAxMDEwMDEgMDAxMDEwMDEgMDEwM
TExMDAgMDExMTEwMDAgMDExMDAxMDAgMDAxMTAxMDAgMDEwMTExMDAgMDExMTEwMDAgMDExMDAwMTAgMDAxMTAxMDEgMDEwMTExMDAgMDExMTEwMDAgMDExMDAxMTAgMDAxMTAwMDEgMDEwMTExMDAgMDExMTEwMD
AgMDExMDAxMDAgMDExMDAxMDAgMDEwMTExMDEgMDEwMTExMDAgMDExMTEwMDAgMDExMDAwMTAgMDExMDAxMDAgMDEwMTExMDAgMDExMTEwMDAgMDExMDAwMDEgMDAxMTAwMDAgMDExMTAwMDEgMDEwMTExMDAgMDE
xMTEwMDAgMDAxMTEwMDAgMDAxMTAwMTEgMDEwMTExMDAgMDExMTEwMDAgMDAxMTAwMDEgMDExMDAxMDEgMDEwMTExMDAgMDExMTEwMDAgMDExMDAwMTAgMDAxMTAwMDEgMDEwMTExMDAgMDExMTEwMDAgMDExMDAw
MDEgMDAxMTAxMTAgMDEwMTExMDAgMDExMTEwMDAgMDAxMTEwMDEgMDAxMTEwMDAgMDEwMTExMDAgMDExMTEwMDAgMDExMDAxMTAgMDAxMTAwMTAgMDExMDAwMDAgMDEwMTExMDAgMDExMTEwMDAgMDExMDAxMTAgM
DAxMTAxMDEgMDEwMTExMDAgMDExMTEwMDAgMDAxMTEwMDEgMDAxMTEwMDAgMDEwMTExMDAgMDExMTEwMDAgMDAxMTAwMDAgMDAxMTAxMTAgMDEwMTExMDAgMDExMTEwMDAgMDExMDAxMDAgMDAxMTEwMDEgMDEwMT
ExMDAgMDExMTEwMDAgMDAxMTEwMDEgMDExMDAwMTAgMDExMDEwMTAgMDEwMTExMDAgMDExMTEwMDAgMDAxMTEwMDEgMDExMDAxMDAgMDEwMDAxMTAgMDEwMTExMDAgMDExMTEwMDAgMDExMDAxMDAgMDAxMTEwMDE
gMDEwMTExMDAgMDExMTEwMDAgMDExMDAxMTAgMDAxMTAwMDEgMDEwMTExMDAgMDExMTEwMDAgMDExMDAwMTAgMDAxMTAwMTAgMDEwMTExMDAgMDExMTEwMDAgMDExMDAxMTAgMDAxMTEwMDEgMDEwMTExMDAgMDEx
MTEwMDAgMDAxMTEwMDEgMDExMDAwMDEgMDEwMTExMDAgMDExMTEwMDAgMDAxMTEwMDEgMDExMDAxMDAgMDEwMTExMDAgMDExMTEwMDAgMDAxMTAwMDEgMDExMDAwMTEgMDEwMTExMDAgMDExMTEwMDAgMDExMDAxM
DAgMDExMDAxMDEgMDEwMDAxMDEgMDEwMDExMDEgMDEwMTExMDAgMDExMTEwMDAgMDExMDAxMDEgMDAxMTAwMTAgMDExMDAwMTEgMDEwMTExMDAgMDExMTEwMDAgMDExMDAwMDEgMDAxMTEwMDEgMDEwMTExMDAgMD
ExMTEwMDAgMDExMDAwMDEgMDExMDAwMTAgMDEwMTExMDAgMDExMTEwMDAgMDAxMTAwMDAgMDAxMTAwMDAgMDAxMDExMTAgMDEwMTExMDAgMDExMTEwMDAgMDExMDAwMDEgMDAxMTAxMDEgMDEwMTExMDAgMDExMTE
wMDAgMDExMDAxMDAgMDAxMTAxMDAgMDEwMTExMDAgMDExMTEwMDAgMDExMDAwMDEgMDAxMTAwMDEgMDEwMTExMDAgMDExMTEwMDAgMDExMDAxMDEgMDExMDAwMTEgMDExMDExMDAgMDEwMTExMDAgMDExMTEwMDAg
MDAxMTEwMDAgMDExMDAxMDEgMDEwMTAxMDEgMDEwMDAxMDEgMDEwMTExMDAgMDExMTEwMDAgMDAxMTAwMDEgMDAxMTEwMDAgMDEwMDAxMTEgMDEwMTExMDAgMDExMTEwMDAgMDExMDAwMTAgMDAxMTAwMDEgMDAxM
DAxMDAgMDEwMDExMDEgMDEwMTExMDAgMDExMTEwMDAgMDExMDAxMDEgMDAxMTAwMTEgMDEwMTExMDAgMDExMTEwMDAgMDExMDAxMDAgMDAxMTAxMDEgMDEwMDAwMTEgMDEwMTExMDAgMDExMTEwMDAgMDExMDAxMT
AgMDExMDAwMTAgMDEwMTExMDAgMDExMTEwMDAgMDAxMTAwMDEgMDExMDAxMTAgMDEwMTExMDAgMDExMTEwMDAgMDAxMTEwMDAgMDAxMTAxMTEgMDExMDAxMTAgMDEwMTExMDAgMDExMTEwMDAgMDExMDAxMDEgMDA
xMTEwMDEgMDEwMTExMDAgMDExMTEwMDAgMDExMDAxMDAgMDExMDAxMDAgMDAxMDAxMDEgMDEwMTExMDAgMDExMTEwMDAgMDExMDAxMDEgMDAxMTEwMDEgMDEwMTExMDAgMDExMTEwMDAgMDExMDAxMDAgMDAxMTAx
MTEgMDExMDEwMDAgMDEwMTExMDAgMDExMTEwMDAgMDAxMTEwMDEgMDExMDAxMTAgMDEwMTExMDAgMDExMTEwMDAgMDExMDAxMDAgMDAxMTAwMDEgMDEwMTExMDAgMDExMTEwMDAgMDAxMTAwMDEgMDExMDAwMTAgM

7140 1 1888 Raw Bytes LF

Output

```
\xd2\xc3\xe4B3\x19\xb2\xbe\x9f\xdf\xe8\xc8Jv\xe9z\xe8q\xaf\xe3e\x1fx3;\xe8\x8f\x98\xff\x86\xab\x88\x16Q*%Z]\xd4\x98\x0eF:;\xe8\xb7\xc3/\xc6\xfeR\xba\xa3?
\xad\xf4!\xf1caNU?
R))\xd4\xb5\xf1\xdd]\xbd\xa0q\x83\x1e\xb1\xa6\x98\xf2`\xf5\x98\x06\xd9\x9bj\x9dF\xd9\xf1\xb2\xf9\x9a\x9d\x1c\xdeEM\xe2c\xb8\xab\x00.\xb4\xd4\xa1\xecl\x8eUE\x18G\x
b3$M\xe2\xd5C\xfb\x1f\x87n\xe9\xdd%\xe8\xd7h\x9f\xd1\x1b\xa8\x96~\x8c\xfc\x18\xb6\xcd\xe6\xf3/\xb0\xf1Nd%\x88n*\x96\x90\x0b6[d\x00q\x12\x90p7\xb3\xbdB\x15\x89m\x9
a\x9716\x015\xd2\xc2\xc0!y\x1a\xa1\xa2sJ\xbbC\nC<R\x15\xb1\x0e\x9cm>c6\xa9%\\xb (RC4 KEY IS hacksoc)
```

The hint for the next stage is in the plaintext "RC4 key is hacksoc", hinting at the encrypted text and the key for it. Some online tools may work for decoding this although the intended solution is through Python3.

Using Python3, there's a library called "arc4" which, following the simple documentation can reveal the flag for this challenge.

```python
from arc4 import ARC4

cipher =
b"\xd2\xc3\xe4B3\x19\xb2\xbe\x9f\xdf\xe8\xc8Jv\xe9z\xe8q\xaf\xe3e\x1fx3;\xe8\x
8f\x98\xff\x86\xab\x88\x16Q*%Z]\xd4\x98\x0eF:;\xe8\xb7\xc3/\xc6\xfeR\xba\xa3?
\xad\xf4!\xf1caNU?
R))\xd4\xb5\xf1\xdd]\xbd\xa0q\x83\x1e\xb1\xa6\x98\xf2`\xf5\x98\x06\xd9\x9bj\x9
dF\xd9\xf1\xb2\xf9\x9a\x9d\x1c\xdeEM\xe2c\xb8\xab\x00.\xb4\xd4\xa1\xecl\x8eUE\
x18G\xb3$M\xe2\xd5C\xfb\x1f\x87n\xe9\xdd%\xe8\xd7h\x9f\xd1\x1b\xa8\x96~\x8c\xf
c\x18\xb6\xcd\xe6\xf3/\xb0\xf1Nd%\x88n*\x96\x90\x0b6[d\x00q\x12\x90p7\xb3\xbdB
\x15\x89m\x9a\x9716\x015\xd2\xc2\xc0!y\x1a\xa1\xa2sJ\xbbC\nC<R\x15\xb1\x0e\x9c
m>c6\xa9%\\xb"
arc4 = ARC4(b'hacksoc')
cipher_decrypted = arc4.decrypt(cipher)
print (cipher_decrypted)
```

Running a successful script should output:

```
b'd1276b2d17b68db17267b61d267bd1276bd1276b8d1276bd216b1d827b61d27b612db7612d8b7612
```

`8db7162db16d72b76128d67b12dHACKSOC_CTF{RC4_IS_FUN}78fdh8h7d128h712d8h79127h912d8h7912d8h172d9h712d988h7192d8h7129dh8712dh7d\xda\xc5\x9d'` which contains the flag.