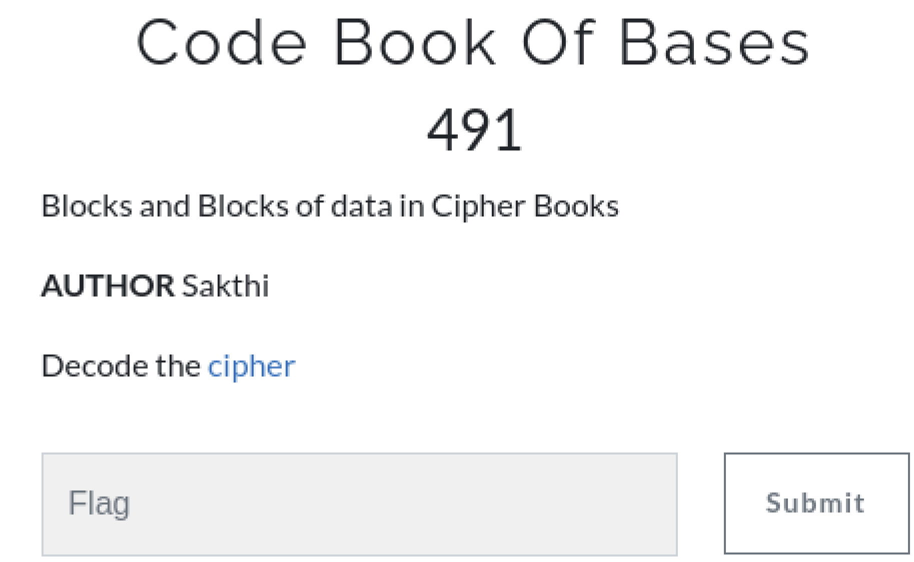
CHALLENGE : Code Book Of Bases

CATEGORY : Crypto

AUTHOR : 0xsakthi

LEVEL : EASY



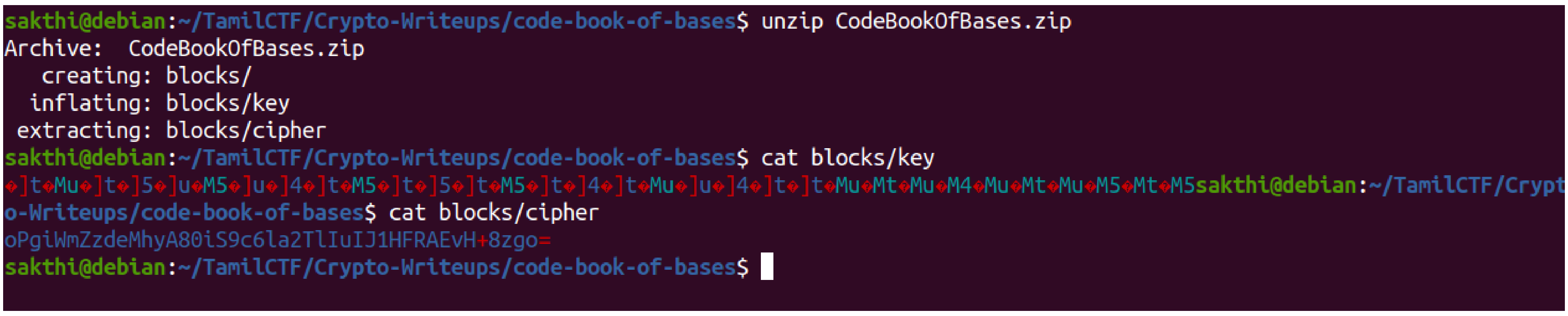
Code Book Of Bases

491

Blocks and Blocks of data in Cipher Books

AUTHOR Sakthi

Decode the cipher

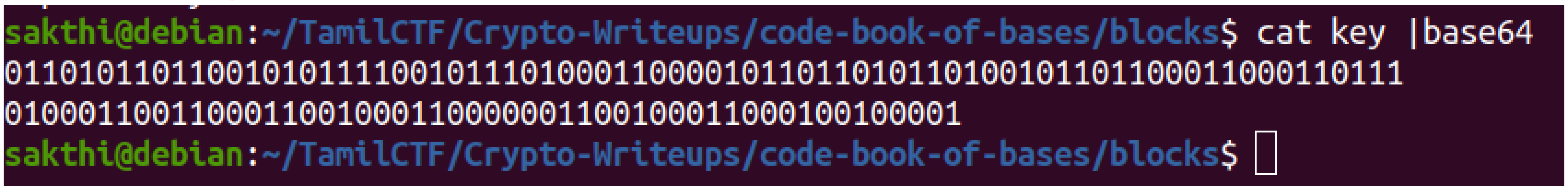


```
sakthi@debian:~/TamilCTF/Crypto-Writeups/code-book-of-bases$ unzip CodeBookOfBases.zip
Archive:  CodeBookOfBases.zip
   creating: blocks/
  inflating: blocks/key
 extracting: blocks/cipher
sakthi@debian:~/TamilCTF/Crypto-Writeups/code-book-of-bases$ cat blocks/key
�]t�Mu�]t�]5�]u�M5�]u�]4�]t�M5�]t�]5�]t�M5�]t�]4�]t�Mu�]u�]4�]t�]t�Mu�Mt�Mu�M4�Mu�Mt�Mu�M5�Mt�M5sakthi@debian:~/TamilCTF/Crypt
o-Writeups/code-book-of-bases$ cat blocks/cipher
oPgiWmZzdeMhyA80iS9c6la2TlIuIJ1HFRAEvH+8zgo=
sakthi@debian:~/TamilCTF/Crypto-Writeups/code-book-of-bases$ 
```

Title(Code book) directly refers its a Electronic Code Book(one of the aes algorithm)ECB

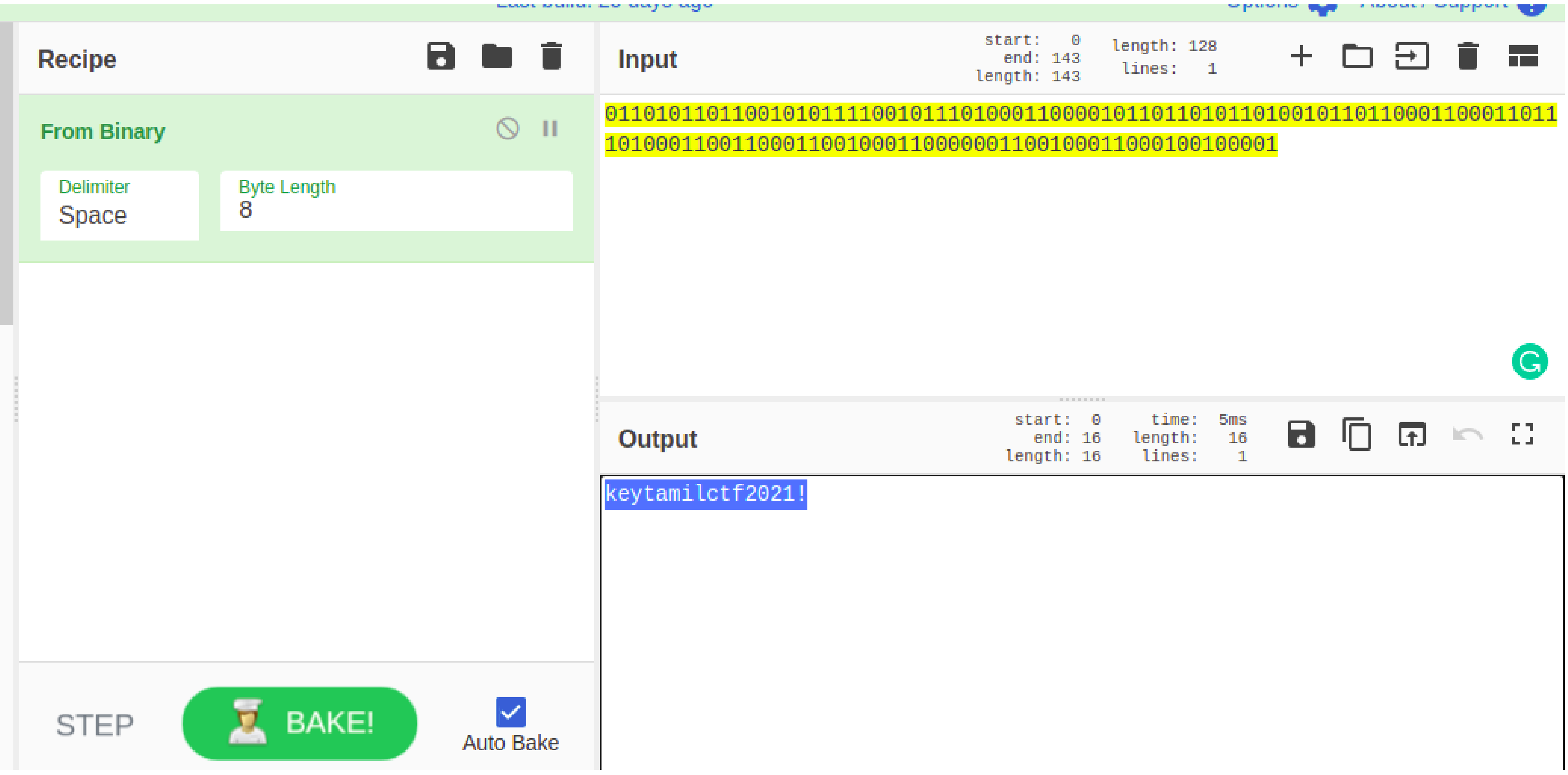
We have cipher where is the key?(the key looks like unknown bytes)

Booom!
when iam ***encrypted*** *the key(unknown bytes) via base64 it will returned a binary values :)*



```
sakthi@debian:~/TamilCTF/Crypto-Writeups/code-book-of-bases/blocks$ cat key |base64
0110101101100101011110010111010001100001011011010110100101101100011000110111
0100011001100011001000110000001100100011000100100001
sakthi@debian:~/TamilCTF/Crypto-Writeups/code-book-of-bases/blocks$ 
```

Decode the binary via cyberchef!



Delimiter: Space
Byte Length: 8

Input
```
start:   0   length: 128
  end: 143    lines:   1
length: 143
01101011011001010111100101110100011000010110110101101001011011000110001101110100011001100011001000110000001100100011000100100001
```

Output
```
start:  0     time:  5ms
  end: 16   length:  16
length: 16   lines:   1
keytamilctf2021!
```

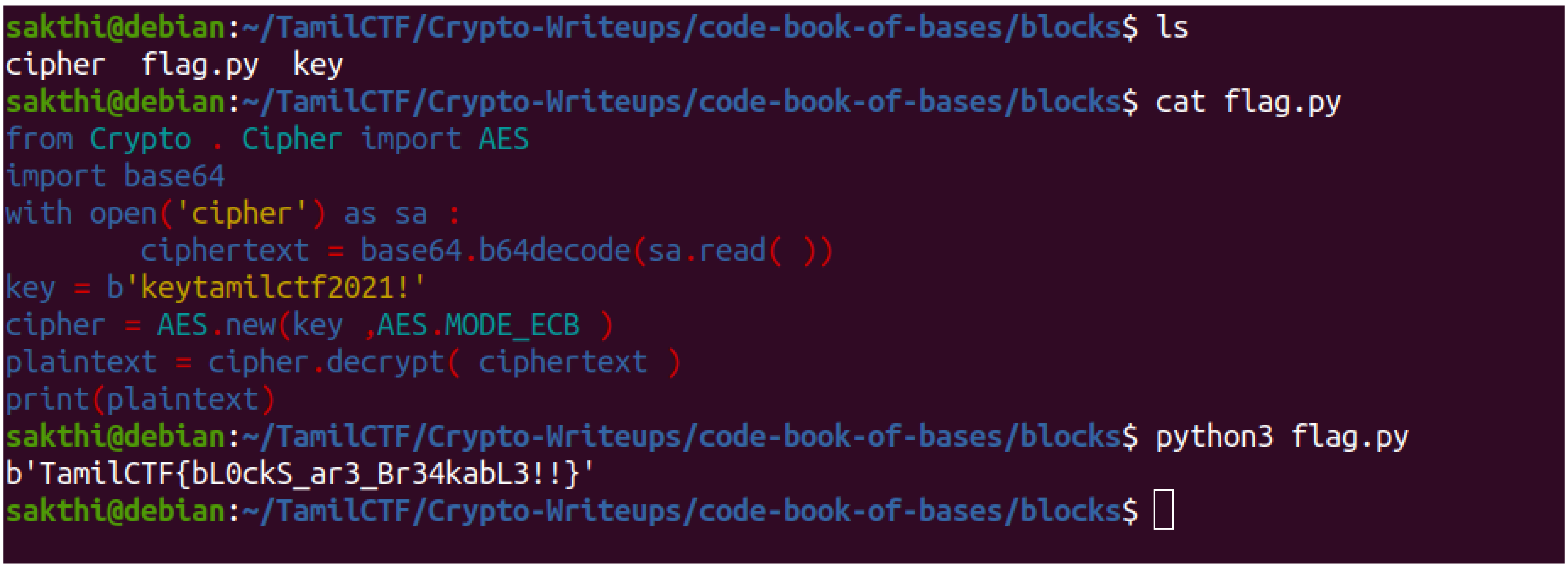
now we have a key

```
keytamilctf2021!
```

Decoding AES-ECB

flag.py

```
from Crypto . Cipher import AES
import base64
with open('cipher') as sa :
    ciphertext = base64.b64decode(sa.read( ))
key = b'keytamilctf2021!'
cipher = AES.new(key ,AES.MODE_ECB )
plaintext = cipher.decrypt( ciphertext )
print(plaintext)
```



```
sakthi@debian:~/TamilCTF/Crypto-Writeups/code-book-of-bases/blocks$ ls
cipher  flag.py  key
sakthi@debian:~/TamilCTF/Crypto-Writeups/code-book-of-bases/blocks$ cat flag.py
from Crypto . Cipher import AES
import base64
with open('cipher') as sa :
        ciphertext = base64.b64decode(sa.read( ))
key = b'keytamilctf2021!'
cipher = AES.new(key ,AES.MODE_ECB )
plaintext = cipher.decrypt( ciphertext )
print(plaintext)
sakthi@debian:~/TamilCTF/Crypto-Writeups/code-book-of-bases/blocks$ python3 flag.py
b'TamilCTF{bL0ckS_ar3_Br34kabL3!!}'
sakthi@debian:~/TamilCTF/Crypto-Writeups/code-book-of-bases/blocks$ 
```

Flag

```
TamilCTF{bL0ckS_ar3_Br34kabL3!!}
```

First Blood : Cyberlandsholdet