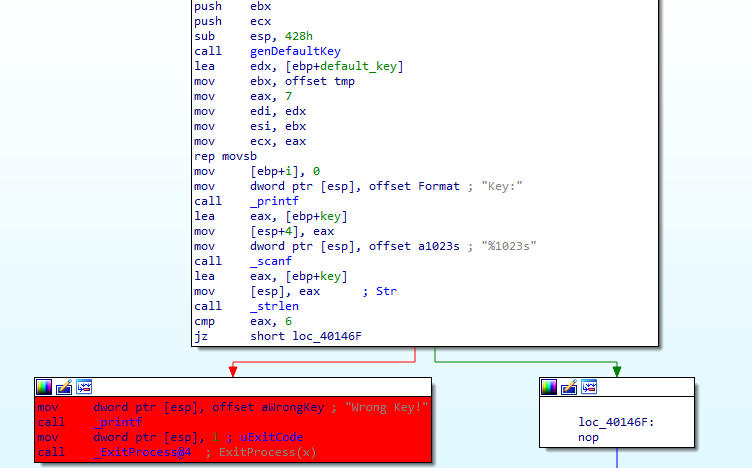
We got a x86 PE file.

Throw it into IDA

we get

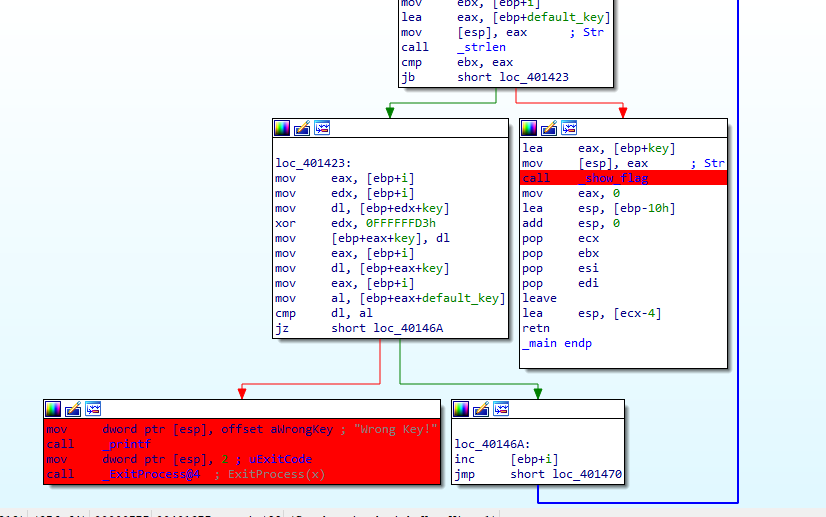


First it generate a default\_key

Then initialize i = 0

Then it require enter a Key, which must have length equals to 6

After that it check the key with simple xor byte algorithm

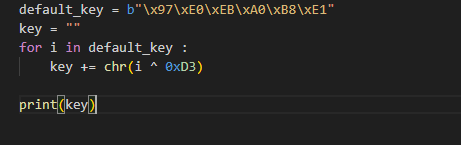


it just xor each byte of key with 0xD3 then compare with this byte with correspond byte in default key

->> get each byte in default\_key then xor with 0xD3 you get the key

If it is correct key, you get the FLAG

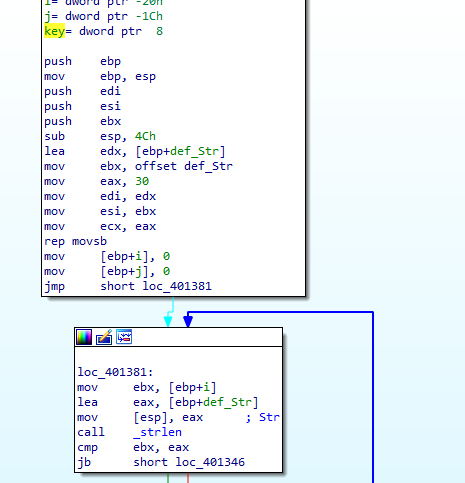
python Script for key



Now you have 2 choices: run app with the key and get the FLAG

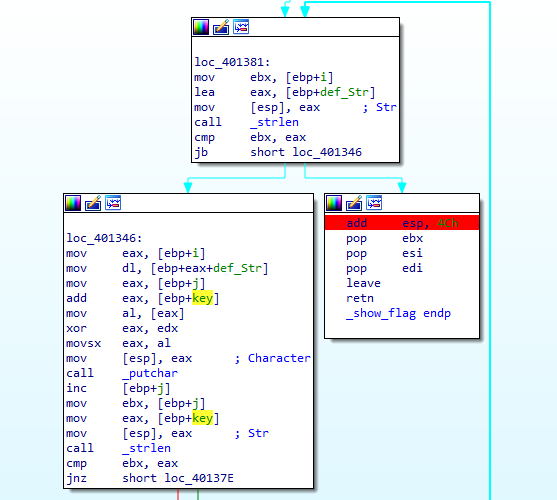
Or reverse show\_flag function

if you reverse show\_flag function



first it have a default String which has length equal to 30

then again xor stub



kind of easy for python script

-Because i run the program then get the flag so it can just give you a hint for it:

python way:

for i in range(len(def\_Str)):

flag += chr(ord(def\_Str[i]) ^ ord(key[i%6]))