#include<stdio.h>

#include<string.h>

#include<stdint.h>

#include<stdlib.h>

//标准RC4

void rc4(unsigned char\* key, int key\_Len, unsigned char\* data, int data\_Len) //加解密

{

int i = 0, j = 0, t = 0;

unsigned char s[256] = { 0 };

unsigned char tmp = 0;

for (i = 0; i < 256; i++) {

s[i] = i;

}

for (i = 0; i < 256; i++) {

j = (j + s[i] + key[i % key\_Len]) % 256;

tmp = s[i];

s[i] = s[j]; //交换s[i]和s[j]

s[j] = tmp;

}

int q = 0;

i = j = 0;

for (q = 0; q < data\_Len; q++) {

i = (i + 1) % 256;

j = (j + s[i]) % 256;

tmp = s[i];

s[i] = s[j]; //交换s[x]和s[y]

s[j] = tmp;

t = (s[i] + s[j]) % 256;

data[q] ^= s[t];

}

}

int main()

{

unsigned char flag[42] = {

//密文替换在这里

};

char\* key = "SecretKey";

rc4(key, strlen(key), flag, 42);

for (int i = 0; i < 42; i++)

{

if (flag[i] >= 'a' && flag[i] <= 'z')

{

flag[i] = (flag[i] - 'a' + 26 - 3) % 26 + 'a';

}

else if (flag[i] >= 'A' && flag[i] <= 'Z')

{

flag[i] = (flag[i] - 'A' + 26 - 3) % 26 + 'A';

}

}

for (int i = 0; i < 42; i+=2)

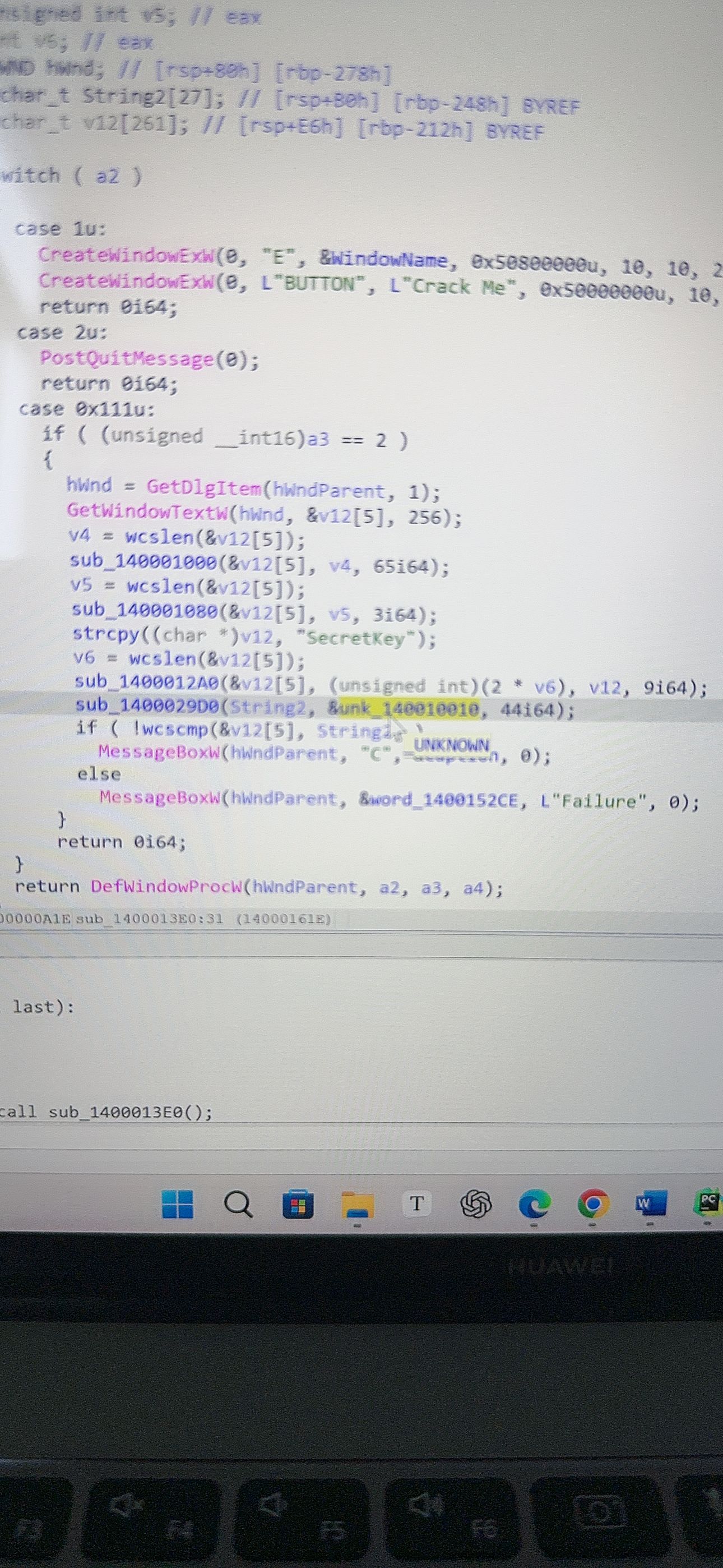
{

printf("%c", flag[i] ^ 65);

}

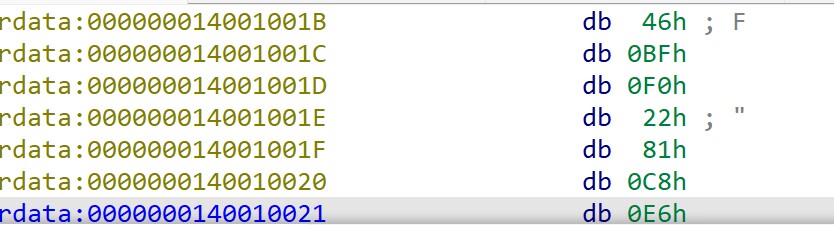
return 0;

}



进去 sub1400013e0函数

42个0x



从1ch开始选到下面

shift e 导出就行