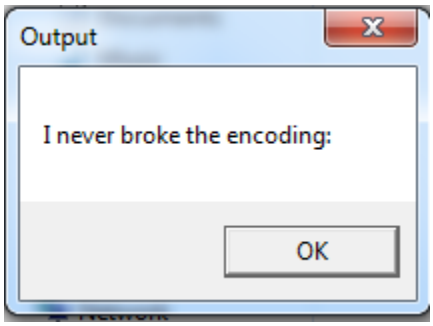
Overlong

Chạy thử chương trình ta thấy:



Đây là đoạn code xử lý của chương trình khi mở trên IDA Pro, ta thấy ebp+Text là nơi chứa chuỗi in ra màn hình, và ebp+Text từng được sử dụng trong hàm sub_401160

```
push    ebp
mov     ebp, esp
sub     esp, 84h
push    1Ch
push    offset unk_402008
lea     eax, [ebp+Text]
push    eax
call    sub_401160
add     esp, 0Ch
mov     [ebp+var_4], eax
mov     ecx, [ebp+var_4]
mov     [ebp+ecx+Text], 0
push    0               ; uType
push    offset Caption  ; "Output"
lea     edx, [ebp+Text]
push    edx             ; lpText
push    0               ; hWnd
call    ds:MessageBoxA
xor     eax, eax
```

Check hàm sub_401160 ta thấy hàm có 3 tham số:

```
sub_401160      proc near

var_8           = dword ptr -8
var_4           = dword ptr -4
arg_0           = dword ptr  8
arg_4           = dword ptr  0Ch
arg_8           = dword ptr  10h
```

Kiểm tra unk_402008 ta có 1 mảng:

```
unk_402008      db 0E0h ; à
                db  81h
                db  89h ; ‰
                db 0C0h ; À
```

Và unk_402008 có tổng cộng 0xAF bytes, ta có thể đoán đây là mảng chứa chuỗi bị mã hóa, và tham số còn lại push 0x1C là chiều dài của chuỗi được giải mã, ta mở chương trình bằng x64dbg và sửa lại lệnh push này thành 0xAF và chạy tiếp thì ta có Flag là: