hw1

0410788 CHING-WEN CHENG

October 7, 2017

Contents

1 Homework1

1.1 hw1 [100]

we have the encrypt flag & the encryption program, so first we dump the object file

```
objdump -d -Mintel hw1 | tail -n104 | head -n56
```

```
08048550 <encrypt>:
 8048550: 55                    push   ebp
 8048551: 57                    push   edi
 8048552: 56                    push   esi
 8048553: 53                    push   ebx
 8048554: 31 db                 xor    ebx,ebx
 8048556: 83 ec 24              sub    esp,0x24
 8048559: 68 60 86 04 08        push   0x8048660
 804855e: 68 63 86 04 08        push   0x8048663
 8048563: e8 48 fe ff ff        call   80483b0 <fopen@plt>
 8048568: 83 c4 10              add    esp,0x10
 804856b: 89 c7                 mov    edi,eax
 804856d: 8b 44 24 34           mov    eax,DWORD PTR [esp+0x34]
 8048571: 8d 6c 24 0c           lea    ebp,[esp+0xc]
 8048575: 85 c0                 test   eax,eax
 8048577: 74 4c                 je     80485c5 <encrypt+0x75>
 8048579: 8d b4 26 00 00 00 00  lea    esi,[esi+eiz*1+0x0]
 8048580: 8d 4b 02              lea    ecx,[ebx+0x2]
 8048583: b8 cd cc cc cc        mov    eax,0xcccccccd
 8048588: 8d 73 01              lea    esi,[ebx+0x1]
```

```
804858b: f7 e1                mul    ecx
804858d: c1 ea 03             shr    edx,0x3
8048590: 8d 04 92             lea    eax,[edx+edx*4]
8048593: 89 f2                mov    edx,esi
8048595: 01 c0                add    eax,eax
8048597: 29 c1                sub    ecx,eax
8048599: 8b 44 24 30          mov    eax,DWORD PTR [esp+0x30]
804859d: d3 e2                shl    edx,cl
804859f: 0f be 04 18          movsx  eax,BYTE PTR [eax+ebx*1]
80485a3: 89 f3                mov    ebx,esi
80485a5: 0f af c2             imul   eax,edx
80485a8: 05 33 23 00 00       add    eax,0x2333
80485ad: 89 44 24 0c          mov    DWORD PTR [esp+0xc],eax
80485b1: 57                   push   edi
80485b2: 6a 01                push   0x1
80485b4: 6a 04                push   0x4
80485b6: 55                   push   ebp
80485b7: e8 d4 fd ff ff       call   8048390 <fwrite@plt>
80485bc: 83 c4 10             add    esp,0x10
80485bf: 3b 74 24 34          cmp    esi,DWORD PTR [esp+0x34]
80485c3: 75 bb                jne    8048580 <encrypt+0x30>
80485c5: 83 ec 0c             sub    esp,0xc
80485c8: 57                   push   edi
80485c9: e8 b2 fd ff ff       call   8048380 <fclose@plt>
80485ce: 83 c4 10             add    esp,0x10
80485d1: 83 c4 1c             add    esp,0x1c
80485d4: 5b                   pop    ebx
80485d5: 5e                   pop    esi
80485d6: 5f                   pop    edi
80485d7: 5d                   pop    ebp
80485d8: c3                   ret
80485d9: 66 90                xchg   ax,ax
80485db: 66 90                xchg   ax,ax
80485dd: 66 90                xchg   ax,ax
80485df: 90                   nop
```

we find the encrypt function, the write a similar function that do the same encryption.

```
function encrypt(S)
  for i = 2:length(S)+1
    k = fld(0xcccccccd * i, 2^32 ) >> 3
    k = 2*(k + 4k)
    s = i - k
    println(hex(((i-1) << s) * Int(S[i-1]) + 0x2333))
  end
end
```

then decrypt the flag by

```
f = open("flag")
i = 2
while !eof(f)
  S = read(f,Int32)
  k = fld(0xccccccccd * i, 2^32 ) >> 3
  k = 2*(k + 4k)
  s = i - k
  S = Char(   (S - 0x2333)/((i-1) <<s)     )
  print(S)
  i+=1
end

> FLAG{Iost4SXskSmu53CbCAI5e52FBJkj1JKl}
```