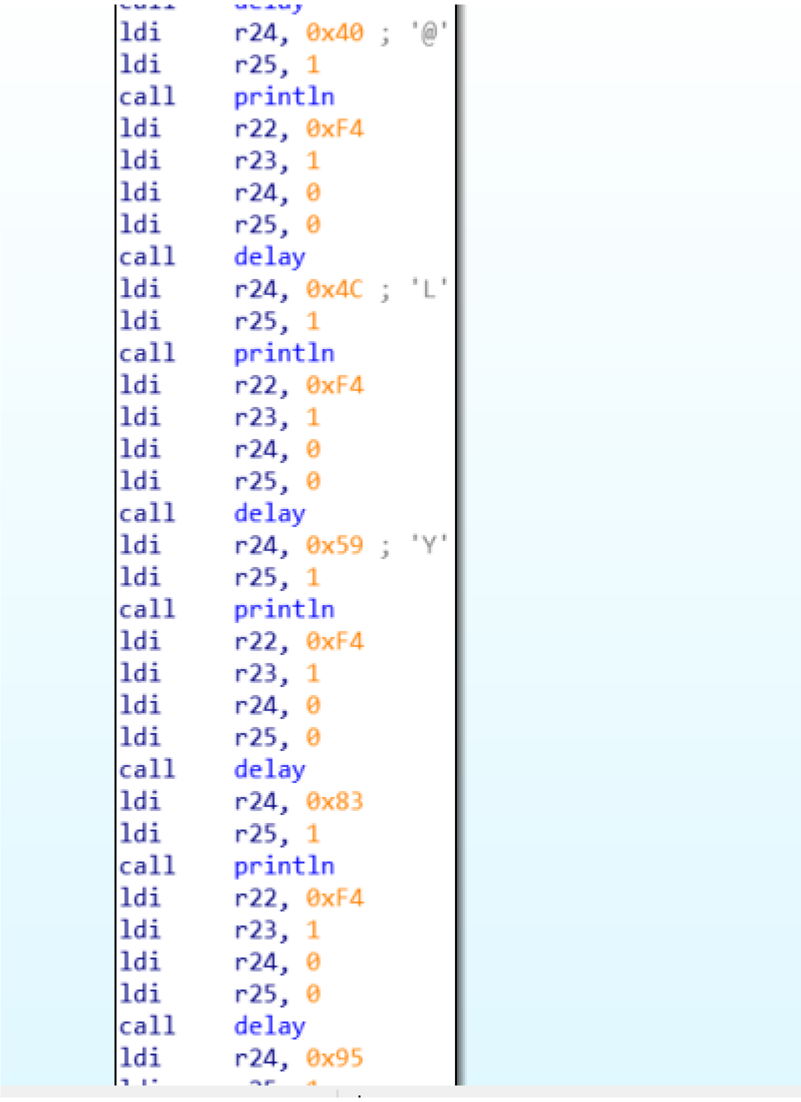
Hctf PolishDuck

由于出题人水平有限，给各位师傅带来的不必要困扰还请谅解。

Badusb 固件
先 hex2bin
Arduino Leonardo 芯片 atmega32u4
Github 上找到 32u4 的 datasheet，然后难度就降维了
https://gist.github.com/thecamper/18fa1453091be4c379aa12bcc92f91f0
有了 datasheet 可以直接 ida 分析
‘可以装 arduino ide 自己编译一个相关的固件对比函数，或者直接找到 keyboard 的库分析，都可以。
找到主函数



```
ldi     r24, 0x40 ; '@'
ldi     r25, 1
call    println
ldi     r22, 0xF4
ldi     r23, 1
ldi     r24, 0
ldi     r25, 0
call    delay
ldi     r24, 0x4C ; 'L'
ldi     r25, 1
call    println
ldi     r22, 0xF4
ldi     r23, 1
ldi     r24, 0
ldi     r25, 0
call    delay
ldi     r24, 0x59 ; 'Y'
ldi     r25, 1
call    println
ldi     r22, 0xF4
ldi     r23, 1
ldi     r24, 0
ldi     r25, 0
call    delay
ldi     r24, 0x83
ldi     r25, 1
call    println
ldi     r22, 0xF4
ldi     r23, 1
ldi     r24, 0
ldi     r25, 0
call    delay
ldi     r24, 0x95
```

源码里可以看到 println 是根据地址取字符串
根据 ldi 地址位置，推算出字符串位置
String 能看出来是 notepad.exe 里输入东西。

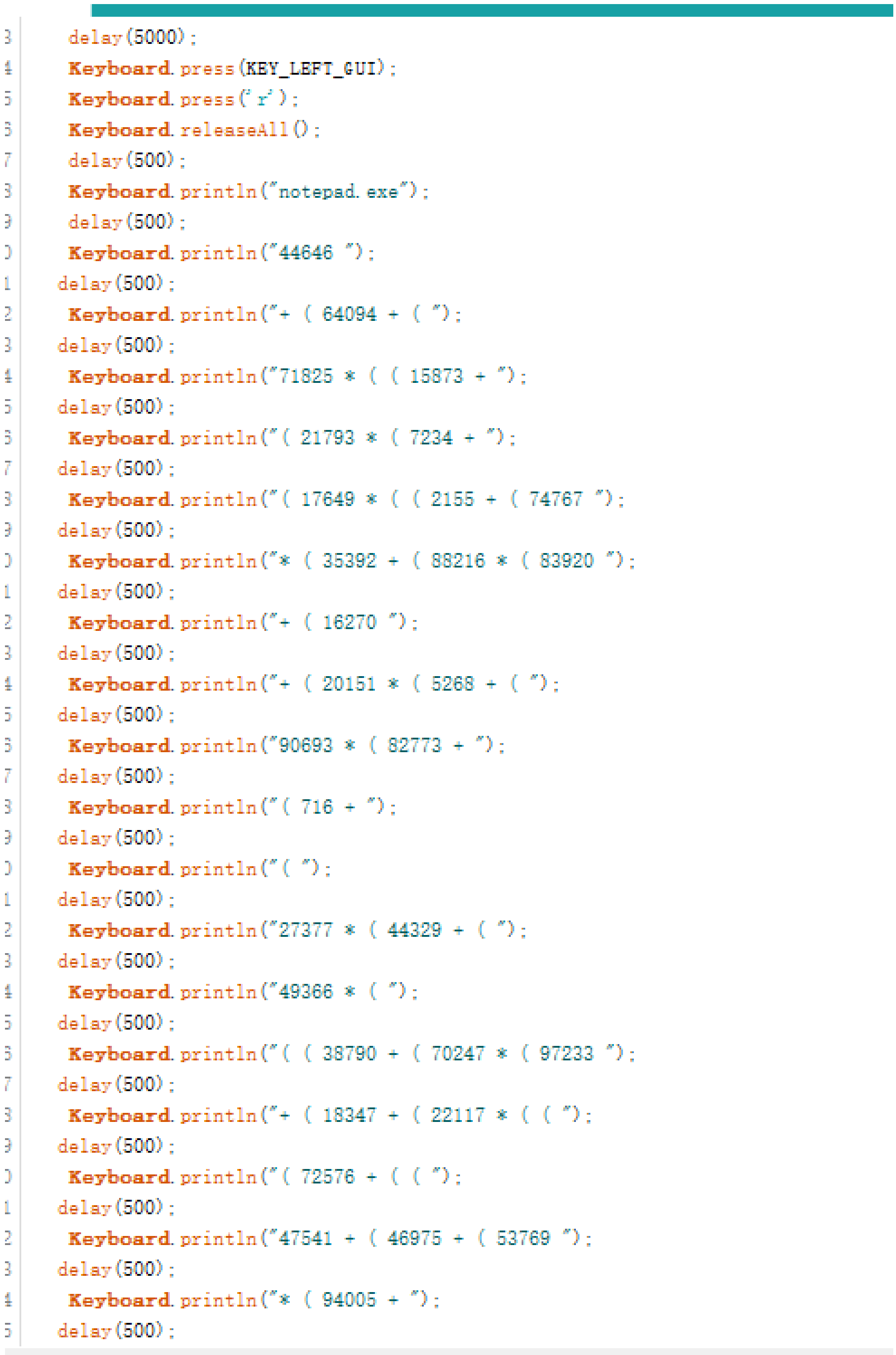
这里引用一下Nu1L战队师傅的脚本

```
index_table=[320,332, 339, 354, 375, 395, 425, 456, 467, 491, 510, 606, 519, 540, 551, 582,
609, 624, 651, 664, 675, 689, 604, 698, 709, 720, 727, 754, 775, 784, 606, 807,
838, 988, 845, 868, 883, 911, 934, 947, 959, 976, 991, 1007, 1024, 1099, 1043, 1068, 1083,
1103, 1106, 1168, 1119, 1132, 1149, 1166, 1175, 1182, 1205, 1227,
  1093, 1093, 1238, 1101, 1101, 1172, 1253, 1103]

import ida_bytes,idaapi

def my_get_str(ea):
    #print(hex(ea))
    res = ''
    i = 0
    while True:
        tt = ida_bytes.get_byte(ea+i)
        if tt ==0 or tt & 0x80 != 0:
            break
        res += chr(tt)
        i += 1
    return res

guess_offest = [6480]

for offest in guess_offest:
    res = ''
    for i in index_table:
        res += my_get_str(i+offest)
        res += '\n'
    print(res+'\n')

```

开始的内容本来是逆波兰表达式, 但在减法写成了 ‘负数加‘ 不满足中缀表达式 所以符号比数字多，这种脑洞没有必要，所以后期更新了附件，变成了常规的中缀表达式。

给各位师傅带来的困扰还请海涵。

Source code example



```
     delay(5000);
     Keyboard.press(KEY_LEFT_GUI);
     Keyboard.press('r');
     Keyboard.releaseAll();
     delay(500);
     Keyboard.println("notepad.exe");
     delay(500);
     Keyboard.println("44646 ");
    delay(500);
     Keyboard.println("+ ( 64094 + ( ");
    delay(500);
     Keyboard.println("71825 * ( ( 15873 + ");
    delay(500);
     Keyboard.println("( 21793 * ( 7234 + ");
    delay(500);
     Keyboard.println("( 17649 * ( ( 2155 + ( 74767 ");
    delay(500);
     Keyboard.println("* ( 35392 + ( 88216 * ( 83920 ");
    delay(500);
     Keyboard.println("+ ( 16270 ");
    delay(500);
     Keyboard.println("+ ( 20151 * ( 5268 + ( ");
    delay(500);
     Keyboard.println("90693 * ( 82773 + ");
    delay(500);
     Keyboard.println("( 716 + ");
    delay(500);
     Keyboard.println("( ");
    delay(500);
     Keyboard.println("27377 * ( 44329 + ( ");
    delay(500);
     Keyboard.println("49366 * ( ");
    delay(500);
     Keyboard.println("( ( 38790 + ( 70247 * ( 97233 ");
    delay(500);
     Keyboard.println("+ ( 18347 + ( 22117 * ( ( ");
    delay(500);
     Keyboard.println("( 72576 + ( ( ");
    delay(500);
     Keyboard.println("47541 + ( 46975 + ( 53769 ");
    delay(500);
     Keyboard.println("* ( 94005 + ");
    delay(500);
```

中缀计算得 16 进制:
0x686374667b50306c3173685f4475636b5f546173743735f44336c3163693075735f44305f555f5468316e6b3f7d
Decode 得 flag：hctf{P0l1sh_Duck_Tast3s_D3l1ci0us_D0_U_Th1nk?}

没有 Polish 的 PolishDuck XD，出题人已自裁。