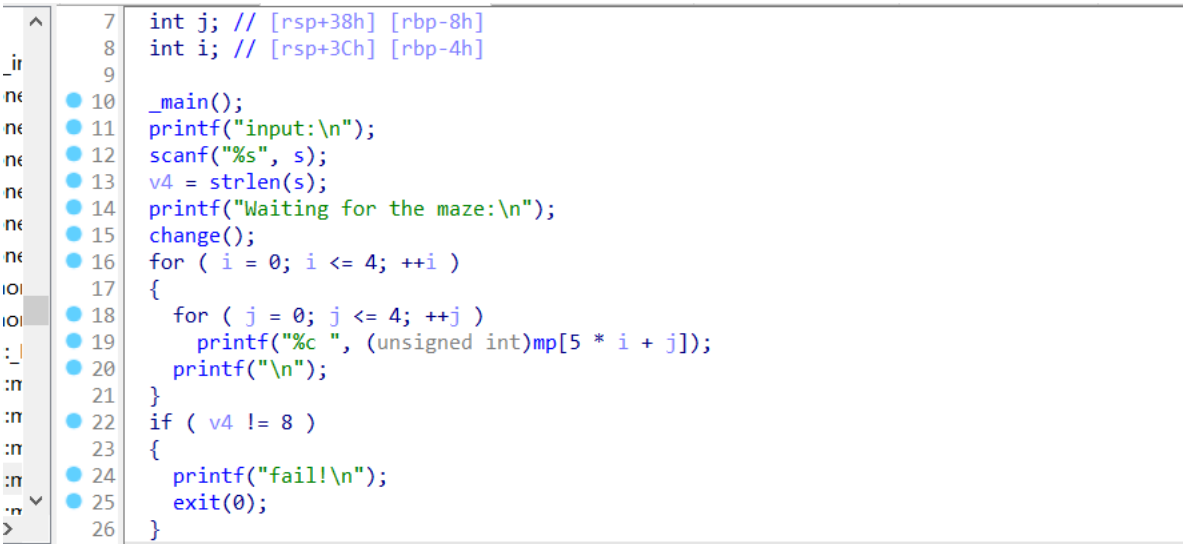
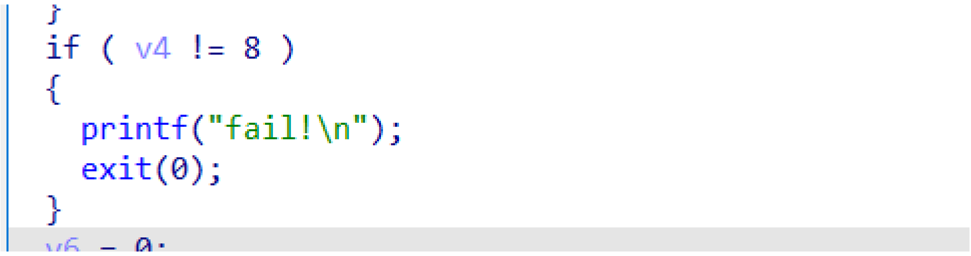


```
int j; // [rsp+38h] [rbp-8h]
int i; // [rsp+3Ch] [rbp-4h]

_main();
printf("input:\n");
scanf("%s", s);
v4 = strlen(s);
printf("Waiting for the maze:\n");
change();
for ( i = 0; i <= 4; ++i )
{
  for ( j = 0; j <= 4; ++j )
    printf("%c ", (unsigned int)mp[5 * i + j]);
  printf("\n");
}
if ( v4 != 8 )
{
  printf("fail!\n");
  exit(0);
}
```

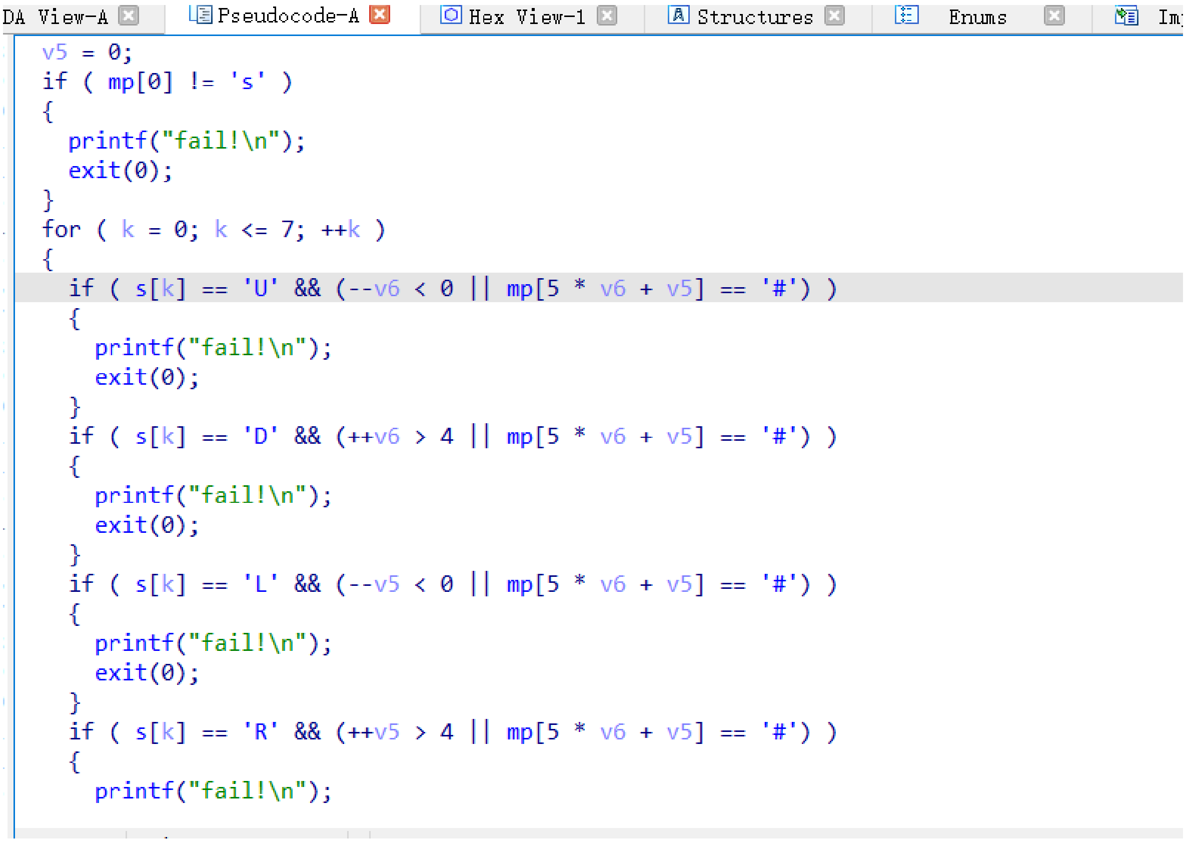
根据这个printf("Waiting for the maze")猜测是个迷宫题

这个双重循环猜是个5*5大小的迷宫



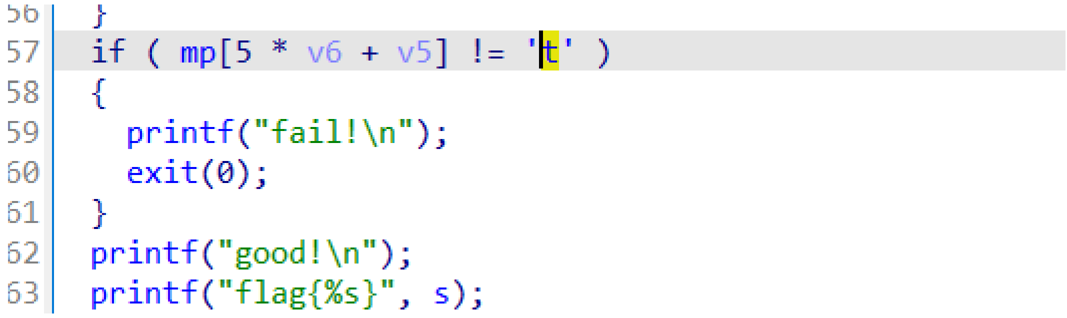
```
}
if ( v4 != 8 )
{
  printf("fail!\n");
  exit(0);
}
v6 = 0;
```

v4是上面出入的字符串的长度，预计走八步



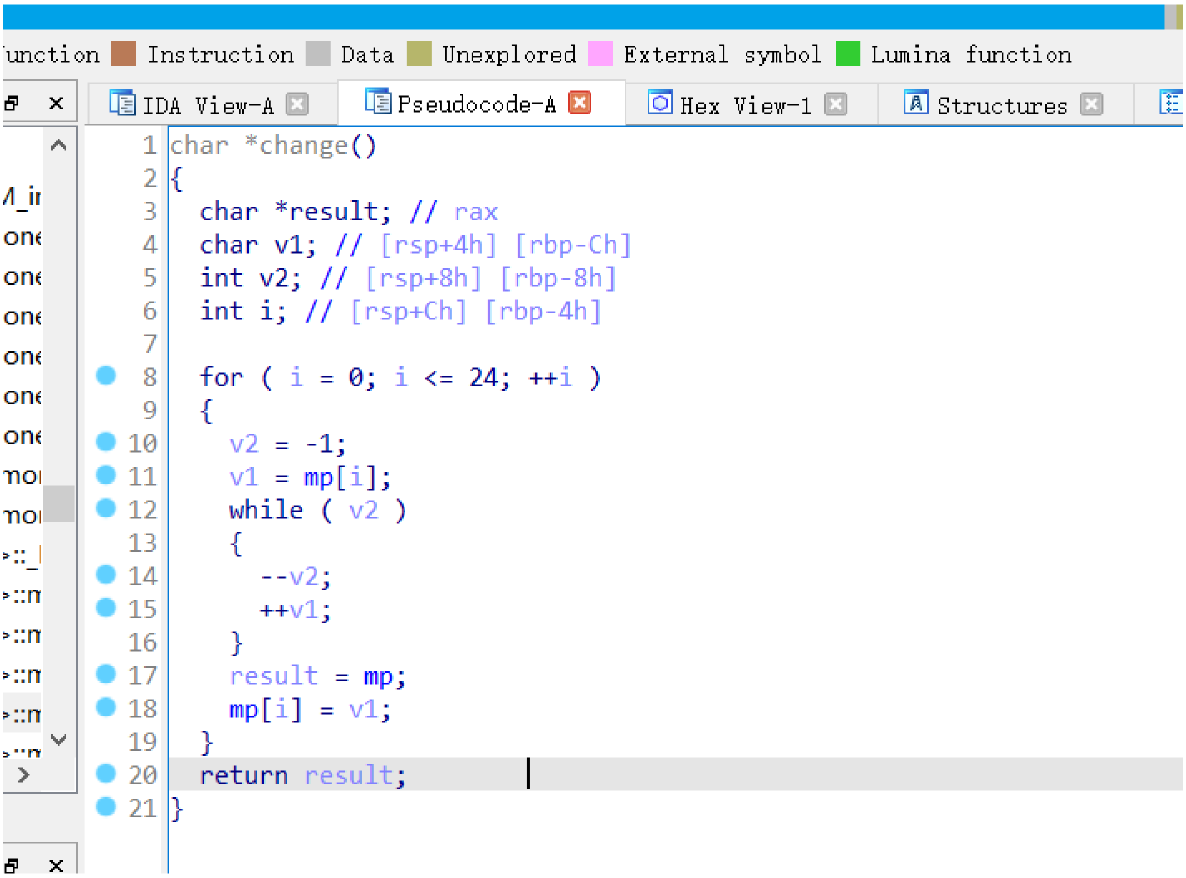
```
v5 = 0;
if ( mp[0] != 's' )
{
  printf("fail!\n");
  exit(0);
}
for ( k = 0; k <= 7; ++k )
{
  if ( s[k] == 'U' && (--v6 < 0 || mp[5 * v6 + v5] == '#') )
  {
    printf("fail!\n");
    exit(0);
  }
  if ( s[k] == 'D' && (++v6 > 4 || mp[5 * v6 + v5] == '#') )
  {
    printf("fail!\n");
    exit(0);
  }
  if ( s[k] == 'L' && (--v5 < 0 || mp[5 * v6 + v5] == '#') )
  {
    printf("fail!\n");
    exit(0);
  }
  if ( s[k] == 'R' && (++v5 > 4 || mp[5 * v6 + v5] == '#') )
  {
    printf("fail!\n");
```

往下看，字符串UDLR对应着上下左右



```
}
if ( mp[5 * v6 + v5] != 't' )
{
  printf("fail!\n");
  exit(0);
}
printf("good!\n");
printf("flag{%s}", s);
```

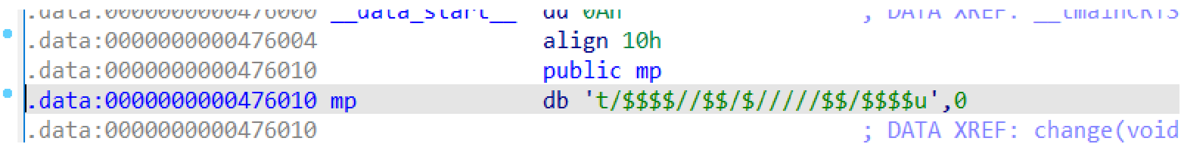
t是终点，flag是我们的输入



```
char *change()
{
  char *result; // rax
  char v1; // [rsp+4h] [rbp-Ch]
  int v2; // [rsp+8h] [rbp-8h]
  int i; // [rsp+Ch] [rbp-4h]

  for ( i = 0; i <= 24; ++i )
  {
    v2 = -1;
    v1 = mp[i];
    while ( v2 )
    {
      --v2;
      ++v1;
    }
    result = mp;
    mp[i] = v1;
  }
  return result;
}
```

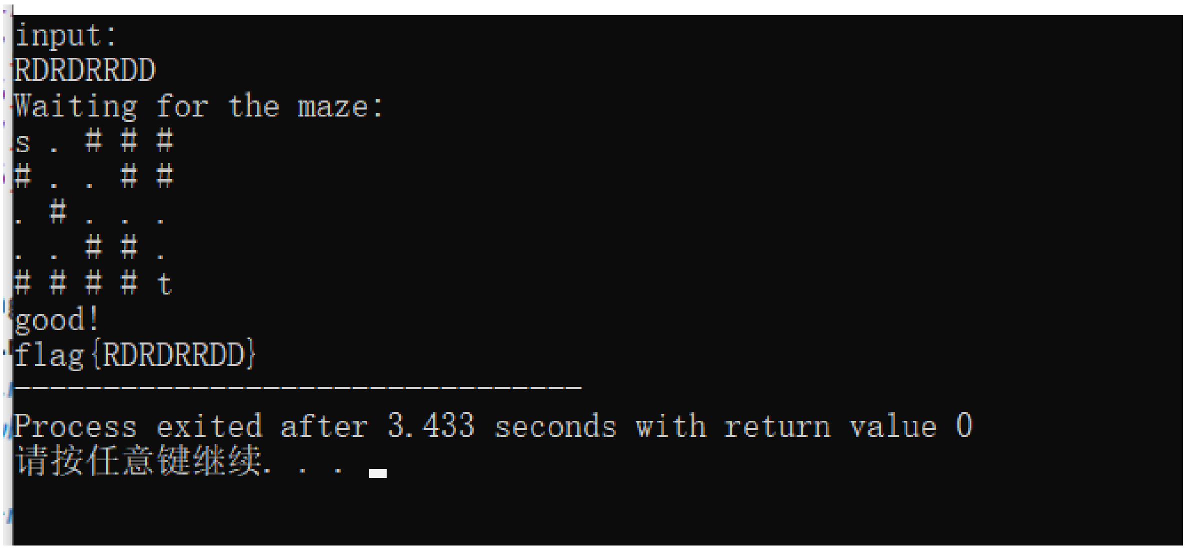
观察这个函数，发现对于每个mp[i]，都进行了mp[i]=mp[i]-1的操作



```
.data:0000000000476000 __data_start__   dd 0Ah                  ; DATA XREF: __tmainCRTS
.data:0000000000476004                  align 10h
.data:0000000000476010                  public mp
.data:0000000000476010 mp               db 't/$$$$//$$/$/////$$/$$$$u',0
.data:0000000000476010                                          ; DATA XREF: change(void
```

而mp长这样

所以迷宫为



```
input:
RDRDRRDD
Waiting for the maze:
s . # # #
# . . # #
. # . . .
. . # # .
# # # # t
good!
flag{RDRDRRDD}
--------------------------------
Process exited after 3.433 seconds with return value 0
请按任意键继续. . .
```