

逻辑很简单，如下图

```
IDA View-A  Pseudocode-A  Hex View-1  Structures  Enums  Imports
1 __int64 __fastcall main(int a1, char **a2, char **a3)
2 {
3     char v4[32]; // [rsp+0h] [rbp-A8h] BYREF
4     char v5[104]; // [rsp+20h] [rbp-88h] BYREF
5     unsigned __int64 v6; // [rsp+88h] [rbp-20h]
6
7     v6 = __readfsqword(0x28u);
8     __printf_chk(1LL, "Please give me the key string:", a3);
9     scanf("%s", v5);
10    if ( sub_860(v5) )
11    {
12        sub_C50(v5, v4);
13        __printf_chk(1LL, "Judgement pass! flag is actf{%s_%s}\n", v5);
14    }
15    else
16    {
17        puts("False key!");
18    }
19    return 0LL;
20 }
```

可以看到输入的v5满足sub_860的条件即可获得flag

进入sub_860

```
IDA View-A  Pseudocode-A  Hex View-1  Structures  Enums  Imports  Exports
15 v1 = a1[1];
16 v2 = *a1;
17 v3 = a1[2];
18 v4 = a1[3];
19 v5 = a1[4];
20 v6 = a1[6];
21 v7 = a1[5];
22 v8 = a1[7];
23 v9 = a1[8];
24 result = 0;
25 if ( -85 * v9 + 58 * v8 + 97 * v6 + v7 + -45 * v5 + 84 * v4 + 95 * v2 - 20 * v1 + 12 * v3 == 12613 )
26 {
27     v11 = a1[9];
28     if ( 30 * v11 + -70 * v9 + -122 * v6 + -81 * v7 + -66 * v5 + -115 * v4 + -41 * v3 + -86 * v1 - 15 * v2 - 30 * v8 == -54400
29         && -103 * v11 + 120 * v8 + 108 * v7 + 48 * v4 + -89 * v3 + 78 * v1 - 41 * v2 + 31 * v5 - (v6 << 6) - 120 * v9 == -10283
30         && 71 * v6 + (v7 << 7) + 99 * v5 + -111 * v3 + 85 * v1 + 79 * v2 - 30 * v4 - 119 * v8 + 48 * v9 - 16 * v11 == 22855
31         && 5 * v11 + 23 * v9 + 122 * v8 + -19 * v6 + 99 * v7 + -117 * v5 + -69 * v3 + 22 * v1 - 98 * v2 + 10 * v4 == -2944
32         && -54 * v11 + -23 * v8 + -82 * v3 + -85 * v2 + 124 * v1 - 11 * v4 - 8 * v5 - 60 * v7 + 95 * v6 + 100 * v9 == -2222
33         && -83 * v11 + -111 * v7 + -57 * v2 + 41 * v1 + 73 * v3 - 18 * v4 + 26 * v5 + 16 * v6 + 77 * v8 - 63 * v9 == -13258
34         && 81 * v11 + -48 * v9 + 66 * v8 + -104 * v6 + -121 * v7 + 95 * v5 + 85 * v4 + 60 * v3 + -85 * v2 + 80 * v1 == -1559
35         && 101 * v11 + -85 * v9 + 7 * v6 + 117 * v7 + -83 * v5 + -101 * v4 + 90 * v3 + -28 * v1 + 18 * v2 - v8 == 6308 )
36     {
37         result = 99 * v11 + -28 * v9 + 5 * v8 + 93 * v6 + -18 * v7 + -127 * v5 + 6 * v4 + -9 * v3 + -93 * v1 + 58 * v2 == -1697;
38     }
39 }
```

解方程

于是乎可以用z3求解方程

```

from z3 import *

s = Solver()
v1 = Int('v1')
v2 = Int('v2')
v3 = Int('v3')
v4 = Int('v4')
v5 = Int('v5')
v6 = Int('v6')
v7 = Int('v7')
v8 = Int('v8')
v9 = Int('v9')
v11 = Int('v11')

s.add(-85 * v9 + 58 * v8 + 97 * v6 + v7 + -45 * v5 + 84 * v4 + 95 * v2 - 20 * v1 + 12 * v3 == 12613)
s.add(30 * v11 + -70 * v9 + -122 * v6 + -81 * v7 + -66 * v5 + -115 * v4 + -41 * v3 + -86 * v1 - 15 * v2 - 30 * v8 == -54400)
s.add(-103 * v11 + 120 * v8 + 108 * v7 + 48 * v4 + -89 * v3 + 78 * v1 - 41 * v2 + 31 * v5 - (v6 * 64) - 120 * v9 == -10283)
s.add(71 * v6 + (v7 * 128) + 99 * v5 + -111 * v3 + 85 * v1 + 79 * v2 - 30 * v4 - 119 * v8 + 48 * v9 - 16 * v11 == 22855)
s.add(5 * v11 + 23 * v9 + 122 * v8 + -19 * v6 + 99 * v7 + -117 * v5 + -69 * v3 + 22 * v1 - 98 * v2 + 10 * v4 == -2944)
s.add(-54 * v11 + -23 * v8 + -82 * v3 + -85 * v2 + 124 * v1 - 11 * v4 - 8 * v5 - 60 * v7 + 95 * v6 + 100 * v9 == -2222)
s.add(-83 * v11 + -111 * v7 + -57 * v2 + 41 * v1 + 73 * v3 - 18 * v4 + 26 * v5 + 16 * v6 + 77 * v8 - 63 * v9 == -13258)
s.add(81 * v11 + -48 * v9 + 66 * v8 + -104 * v6 + -121 * v7 + 95 * v5 + 85 * v4 + 60 * v3 + -85 * v2 + 80 * v1 == -1559)
s.add(101 * v11 + -85 * v9 + 7 * v6 + 117 * v7 + -83 * v5 + -101 * v4 + 90 * v3 + -28 * v1 + 18 * v2 - v8 == 6308)
s.add(99 * v11 + -28 * v9 + 5 * v8 + 93 * v6 + -18 * v7 + -127 * v5 + 6 * v4 + -9 * v3 + -93 * v1 + 58 * v2 == -1697)

if s.check() == sat:
    result = s.model()

print(result)

```