

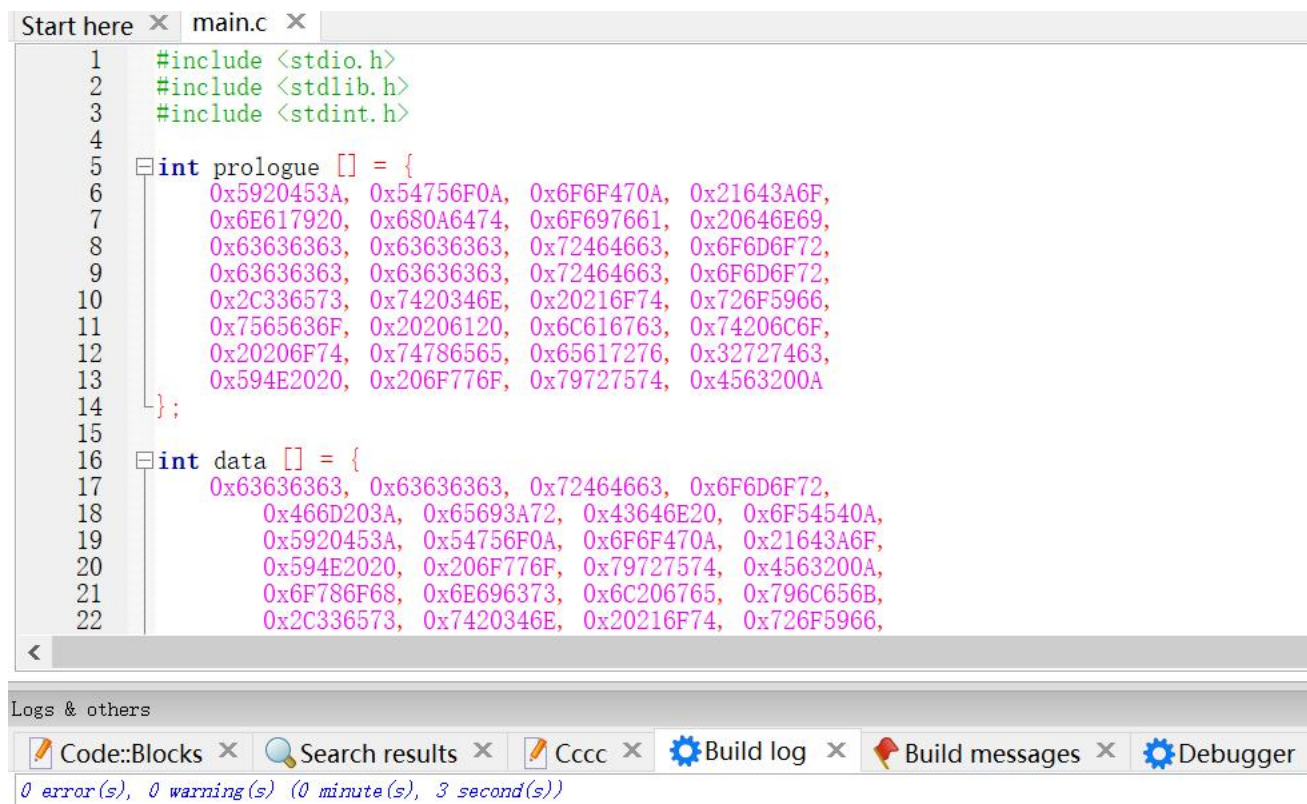
Decoding Lab

1. Objectives:

For this exercise, you have to compile a program as attached and supply four secret keys to determine the contents. This is the guide to solve the problem. The details are as follows.

2. Start the program

Create a new project and import the main.c with Code:Blocks. Compile the program without any bug.



```
1  #include <stdio.h>
2  #include <stdlib.h>
3  #include <stdint.h>
4
5  int prologue [] = {
6      0x5920453A, 0x54756F0A, 0x6F6F470A, 0x21643A6F,
7      0x6E617920, 0x680A6474, 0x6F697661, 0x20646E69,
8      0x63636363, 0x63636363, 0x72464663, 0x6F6D6F72,
9      0x63636363, 0x63636363, 0x72464663, 0x6F6D6F72,
10     0x2C336573, 0x7420346E, 0x20216F74, 0x726F5966,
11     0x7565636F, 0x20206120, 0x6C616763, 0x74206C6F,
12     0x20206F74, 0x74786565, 0x65617276, 0x32727463,
13     0x594E2020, 0x206F776F, 0x79727574, 0x4563200A
14 };
15
16 int data [] = {
17     0x63636363, 0x63636363, 0x72464663, 0x6F6D6F72,
18     0x466D203A, 0x65693A72, 0x43646E20, 0x6F54540A,
19     0x5920453A, 0x54756F0A, 0x6F6F470A, 0x21643A6F,
20     0x594E2020, 0x206F776F, 0x79727574, 0x4563200A,
21     0x6F786F68, 0x6E696373, 0x6C206765, 0x796C656B,
22     0x2C336573, 0x7420346E, 0x20216F74, 0x726F5966,
23 };
24
25 int main()
26 {
27     return 0;
28 }
```

Logs & others

Code::Blocks x Search results x Cccc x Build log x Build messages x Debugger

0 error(s), 0 warning(s) (0 minute(s), 3 second(s))

3. Set a breakpoint

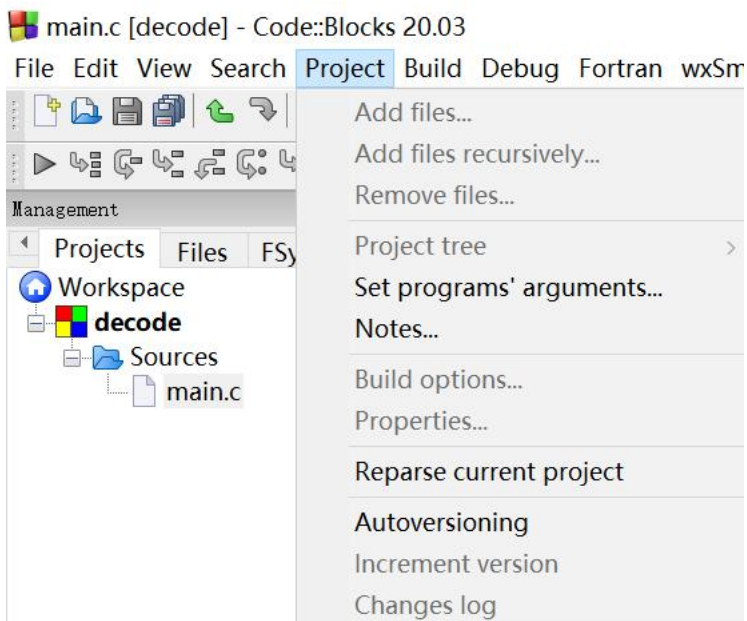
Set a breakpoint to force the program to break. A good programmer must know how to debug.

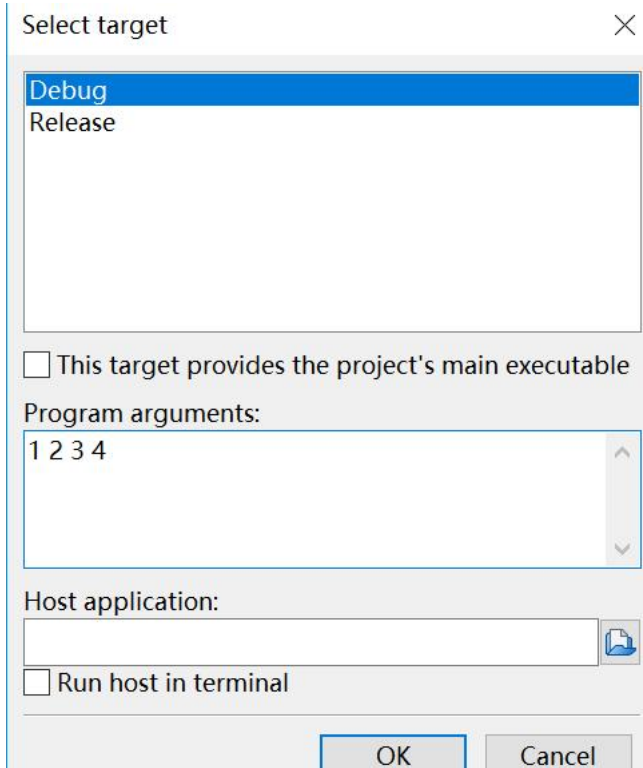
1) Setup a breakpoint at the location of int dummy under main(). Then Click Debug and choose **start debug** then **go, you will see the screen**

```
main.c x
76
77     for (i = 0, j = start;
78          *(((char *) data) + j) != '\0';
79          i++, j += stride)
80     {
81         message[i] = *(((char *) data) + j);
82     }
83     message[i] = '\0';
84     return message;
85 }
86
87 int main (int argc, char *argv[])
88 {
89     int dummy = 1;
90     int start, stride;
91     int key1, key2, key3, key4;
92     char * msg1, * msg2;
93
94     key3 = key4 = 0;
95     if (argc < 3) {
96         usage_and_exit(argv[0]);
97     }
98     key1 = strtol(argv[1], NULL, 0);
99     key2 = strtol(argv[2], NULL, 0);
```

It means the program stops at this location, You can now dummy the message to analysis the data.

You can enter the dummy arguments by select *Project -> Set programs' arguments...*





Find the address of data in main.c

Address of data is: _____ (hint: in hex, ox.....)

2) Find the value of data in ASCII from memory window. Write down the first 40 characters.

4. Determine start and stride

[Hint] Now you find that if you can extract the message, pick the start message and then the stride (after how many characters for the next), you can then guess how to determine it.

For example, 1234567890A

Start:0 and stride: 2, will produce 13579A

4Start:0 and stride: 3, will produce 1245780A

Start:0 and stride: 4, will produce 12356790A

Start:1 and stride: 3, will produce 235689A

1) If you choose the value properly, you will get:

```
From: Friend
To: You
Good! Now try choosing keys3,4 to force a call to extract2 and
avoid the call to extract1
```

Start value: in decimal in order to produce the above message is _____

Stride: length of next character (Hint: You have to refer to the program, the value is 2, 3 or 4 only) _____

2) Write down the address of dummy _____, and address of key1 _____, address of key2 _____

3) Try to understand the algorithm of function process_key12. It will try to change the value of dummy in order to get the right values of start and stride.

The value of key1 should be: The difference between dummy and key1,

The value of Key2 should be compute by start and stride.

Key1 = _____

Key2 = _____

5. Break the last two secret keys

You need to understand the algorithm of process_key34, and the detail of function call and function return process.

1) Write down the return address of function process_key34

Return address of process_key34: _____

2) Write down the stack frame of process_key34.

3) Is it possible to change the process_key34 return address value by process_key34? If so, which address number it should be in order to force a call to function extract2?

Return address after process_key34: _____

4) The value of key3 should be: The difference between &key3 and address to hold return address in function process_key34.

Key3 = _____

5) The value of key4 should be: the difference between original return address and the new return address.

Key4 = _____

6) Post the screen shot after break all secret keys.