Error 1:

Isolation:

Function: int arithmetic_operations()

Line 51-64

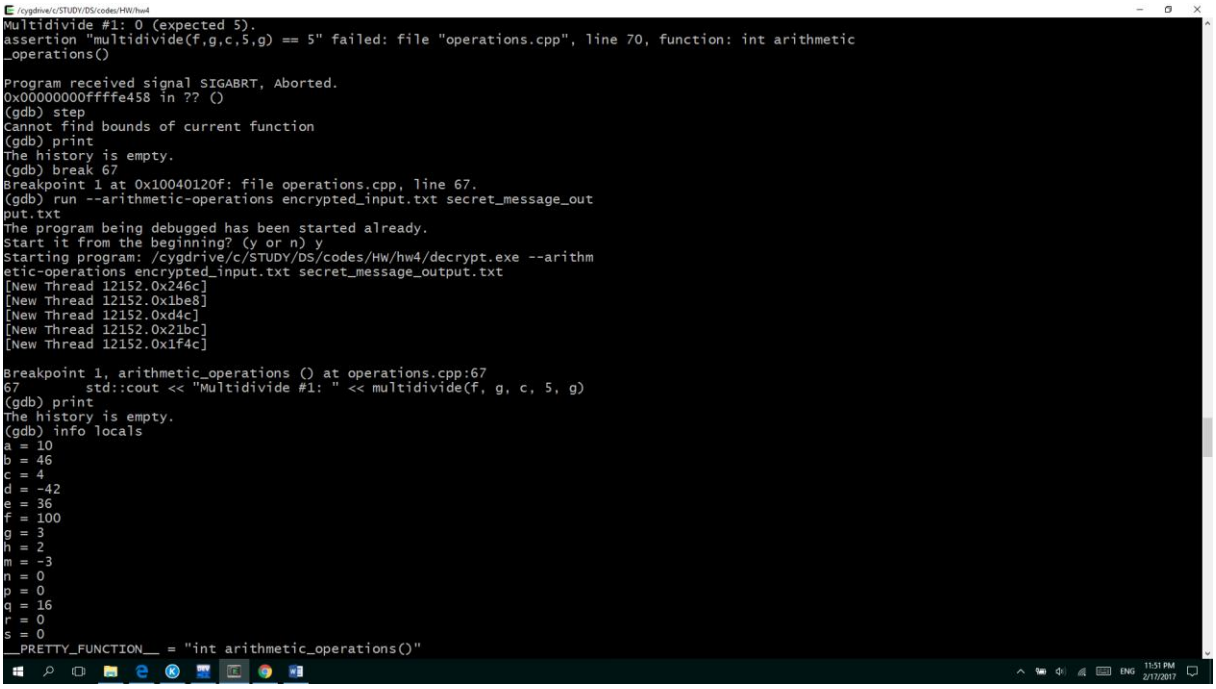
Description:

Unexpected assignment to local variables (e, g, h, m, n, p, r, s) causing return false to “assert” function (assertion fail) and stop the program.

Process:

1. Run program using gdb, which shows that assertion fail at line 70.
2. set a break point at line 70, run program again, and use “info locals” to print out all local variables. Because the reason for assertion fail is that the “==” operator return false. In this case, only those local variables should be taken into account, thus checking the correctness of local variables.

Debugger use:



Error 2:

Isolation:

Function: int arithmetic_operations() step in

multidivide(int numerator, int d1, int d2, int d3, int d4)

Line 91 step in Line 359

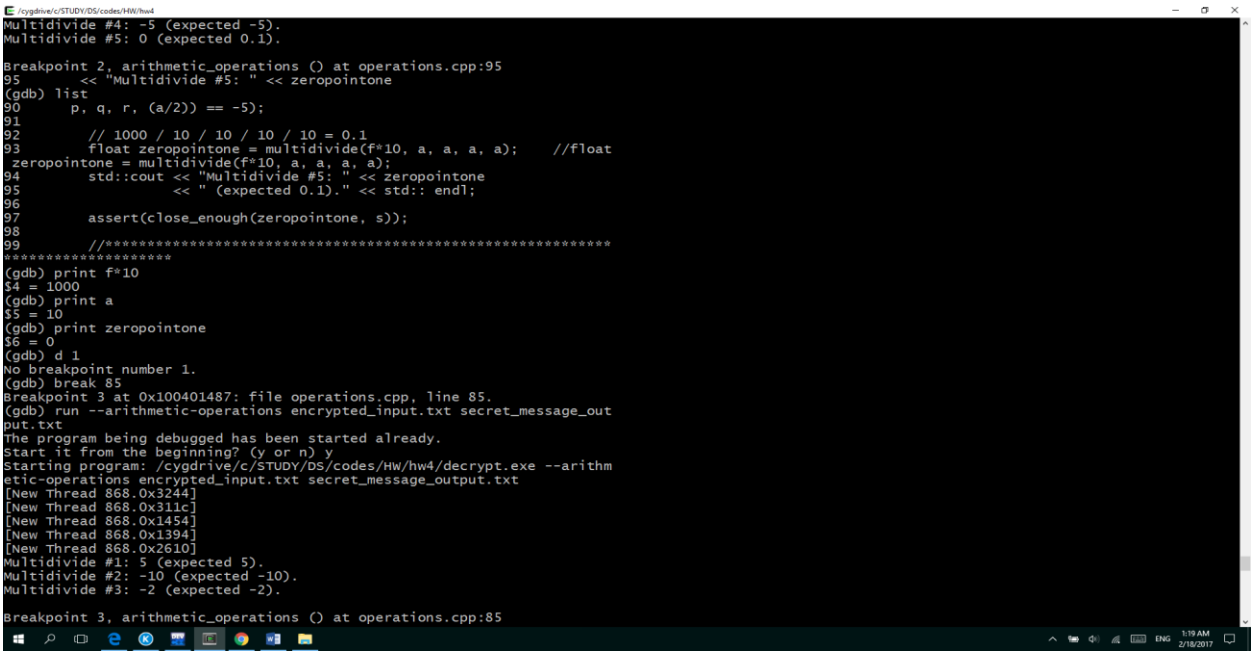
Description:

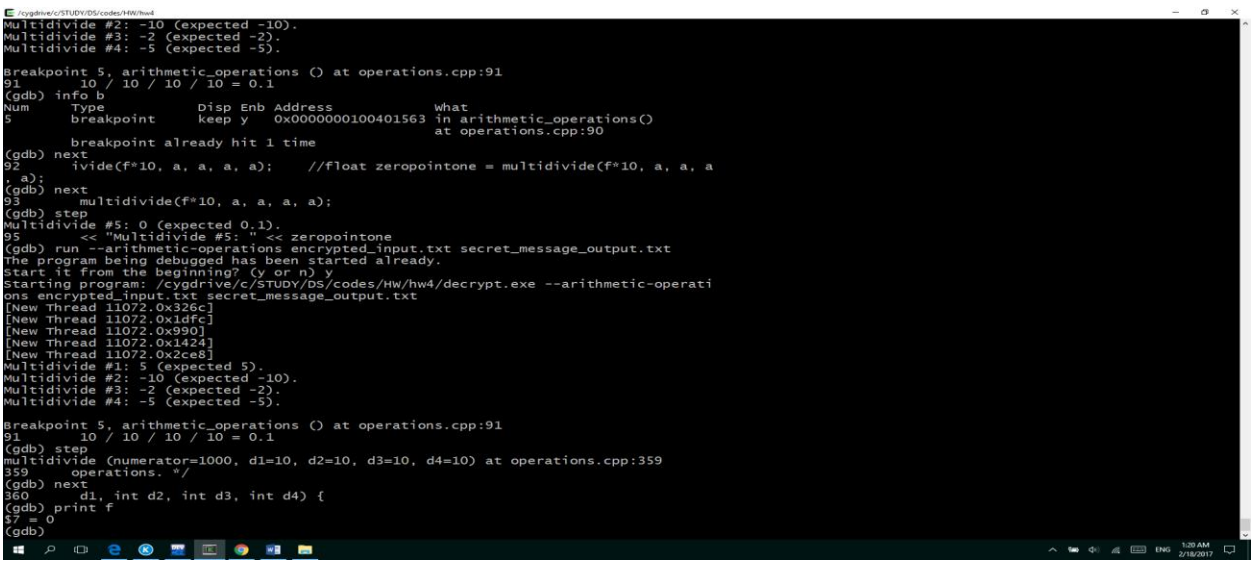
the expected value of variable " zeropointone" is 0.1, while the precision error in function multidivide (line 359) assigned 0 to " zeropointone", thus function "close_enough" (line 95) evaluate false causing the assertion fail.

Process:

1. error is found at line 95, function "close_enough" return a false
2. set break point at 91 check the value of " zeropointone" which is passed into function "close_enough", and found the value of " zeropointone" is 0 (should be 0.1)
3. step in function multidivide(f*10, a, a, a, a) which assigned value to " zeropointone", print f*10, a, and return value f. It shows that the input variables are fine, while the return value f is 0(should be 0.1). Considering all in put values are int type, I convert the type to float while calculating.

Debugger use:





Error 3:

Isolation:

Function: main() step in

file_operations(int argc, char** argv, char*& returned_buffer, int& retlen)

Line 602 step in Line 309

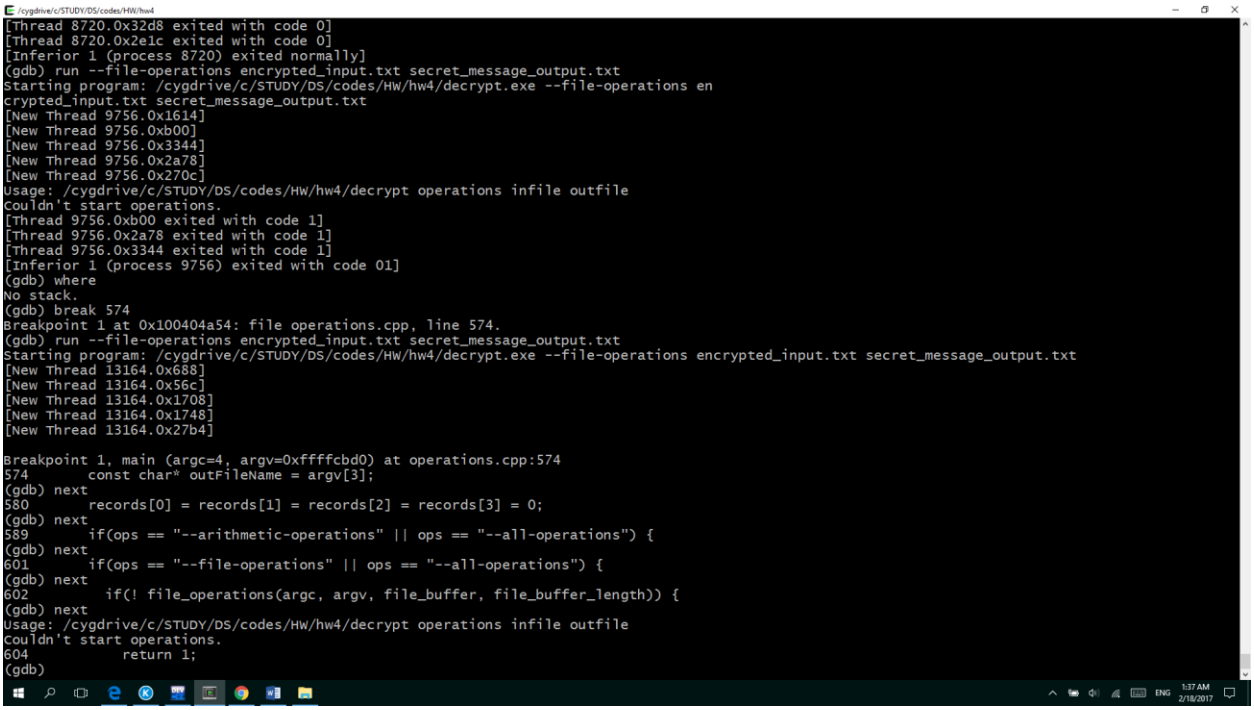
Description:

the function “file_operations” return false at line 602, causing main function directly return 1. And inside the function “file_operations” at line 306, argc is evaluate to be equal to 4 (it should be), thus stepping into the if statement and return false.

Process:

1. error is found at line 604 first. Function “file operations” return false stop all the program.
2. Set break point 601, and step into Function “file operations”, using “next” fond function returns false at line 309.
3. Set break point at 306 which check if return false, and print “argc”. The value is exactly 4 causing the function return false. Because there are 3 arguments, so the “argc” should be exactly 4, and the if statement is checking the correctness of the arguments. I estimate the if statement should be if (argc!=4).

Debugger use:



```
Breakpoint 2, main (argc=4, argv=0xffffcbd0) at operations.cpp:601
601       if(ops == "--file-operations" || ops == "--all-operations") {
(gdb) next
602         if(! file_operations(argc, argv, file_buffer, file_buffer_length)) {
(gdb) step
file_operations (argc=4, argv=0xffffcbd0, returned_buffer=@0xffffcb38: 0x1802e5880 <new_categories+64> "C",
    at operations.cpp:306
306       if(argc == 4) {
(gdb) print argc
$1 = 4
(gdb)
```

Error 4:

Isolation:

Line 604 main function step in function “file_operations” (line 318)

Description:

line 318 “If statement” fail to check if the file is open, thus returning opposite bool value to main function causing program stop.

Process:

1. The program fail at line 342 (assertion fail). Because assertion fail is caused by return a false, I doubt that the infile.gcount() does not match length, I print out length which shows it was 0.
   So, it must the fail of tellg() function or gcount() function.
2. Because the most possible reason for those function fail is that the file does not open. So I make a break point on line 318, which is used to check if the file open. But program did not step into if statement.
3. And there are 2 possible situations: first, the file did open, second, the bool value fail. I checked the bool value “infile” which should represent the file is open, but inside the if statement, code is for not-opening the file. So I change if(infile) to if(!infile)
4. Run program again. The gdb outputs that the file does not open. To check if the argv[2] is exactly the file name, I set breakpoint at line 315. And argv[2] is exactly the file name
5. Finally, I found there is no such file called “encrypted_input.txt” in the folder….

Debugger use:

```
Reading symbols from decrypt.exe...done.
(gdb)  run --file-operations encrypted_input.txt secret_message_output.txt
Starting program: /cygdrive/c/STUDY/DS/codes/HW/hw4/decrypt.exe --file-operations encrypted_input.txt secret_message_output.txt
[New Thread 8028.0x920]
[New Thread 8028.0x33c4]
[New Thread 8028.0x185c]
[New Thread 8028.0x3208]
[New Thread 8028.0x318c]
Successfully opened the input file.
Successfully read in 0 bytes of data.
assertion "infile.gcount() == length" failed: file "operations.cpp", line 342, function: bool file_operations(int, char**, char*&, int&)

Program received signal SIGABRT, Aborted.
0x00000000ffffe458 in ?? ()
```

```
Successfully opened the input file.

Breakpoint 1, file_operations (argc=4, argv=0xffffcbd0, returned_buffer=@0xffffcb38: 0x1802e5880 <new_categories+64> "C", retlen=@0xffffcb34: 73)
    at operations.cpp:327
327       char* buffer = new char[length];
(gdb) next
331       infile.seekg(0, infile.end);
(gdb) print length
$1 = 0
```

```
Starting program: /cygdrive/c/STUDY/DS/codes/HW/hw4/decrypt.exe --file-operations encrypted_input.txt secret_message_ouput.txt
[New Thread 5188.0x2c64]
[New Thread 5188.0x29e8]
[New Thread 5188.0x289c]
[New Thread 5188.0x2cec]
[New Thread 5188.0xa1c]
That file could not be opened!
[Thread 5188.0x289c exited with code 1]
[Thread 5188.0x29e8 exited with code 1]
[Thread 5188.0xa1c exited with code 1]
[Thread 5188.0x2cec exited with code 1]
```

```
Breakpoint 1, file_operations (argc=4, argv=0xffffcbd0, returned_buffer=@0xffffcb38: 0x1802e5880 <new_categories+64> "C", retlen=@0xffffcb34: 73)
    at operations.cpp:315
315       std::ifstream infile(argv[2], std::ifstream::binary);
(gdb) print argv[2]
$1 = 0xffffcc37 "encrypted_input.txt"
```

Error 5:

Isolation:

Function: array_operations() line 128 for loop

Description:

Wrong judgement condition, x >= size, y>=size will allow program step into for loop

Process:

1. Run ./decrypt.exe --array-operations encrypted_input.txt secret_message_output.txt. program fail at line 128 which is an assertion fail. So check the value of array[1][2], shows that array[1][2]=0, but it should be -1. The error might happen when assigned values to array.
2. Set break point to line 122 which is the last nearest assignment. According to gdb, program does not get through the for loop and assign values to array.
3. Check the judgement condition of for loop. Print out the value of size which is 25.Because x=1 initially, thus program can never step into for loop. So I change >= to <=. And for the second for loop, same mistake has been made.

Debugger use:

```
(gdb) run --array-operations encrypted_input.txt secret_message_output.txt
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program: /cygdrive/c/STUDY/DS/codes/HW/hw4/decrypt.exe --array-operations encrypted_input.txt secret_m
essage_output.txt
[New Thread 6076.0x1c04]
[New Thread 6076.0x2d44]
[New Thread 6076.0x2f44]
[New Thread 6076.0x2f54]
[New Thread 6076.0x2f50]
assertion "array[1][2] == -1" failed: file "operations.cpp", line 128, function: int array_operations()

Program received signal SIGABRT, Aborted.
0x00000000ffffe458 in ?? ()
(gdb)
```

```
Breakpoint 2, array_operations () at operations.cpp:128
128       assert(array[1][2] == -1); // no triple exists
(gdb) print array[1][2]
$3 = 0
```

```
Breakpoint 3, array_operations () at operations.cpp:122
122       for(int x=1; x>=size; ++x) {
(gdb) next
128       assert(array[1][2] == -1); // no triple exists
(gdb) print size
$4 = 25
```

Error 6:

Isolation:

Call function “pythagoras(x, y)” fail: line 124

assertion fail: line 128, line 129, line 130

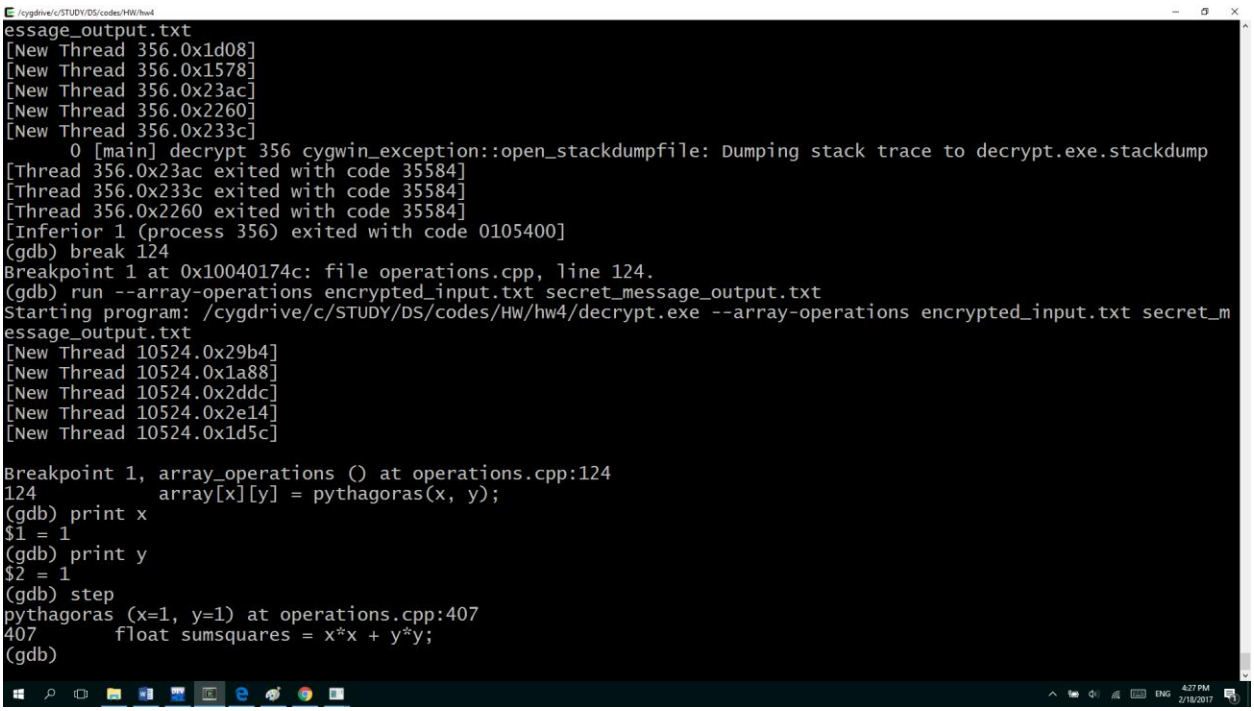
Description:

1. Pythagoras has no return value for those not satisfy (step in to) if statement.
2. Does not assign absolute value to “diffsquares” (line 413), causing the compare in if statement (line 415) fail.
3. Assign value to uninitial pointer (line 403) causing assignment fail.

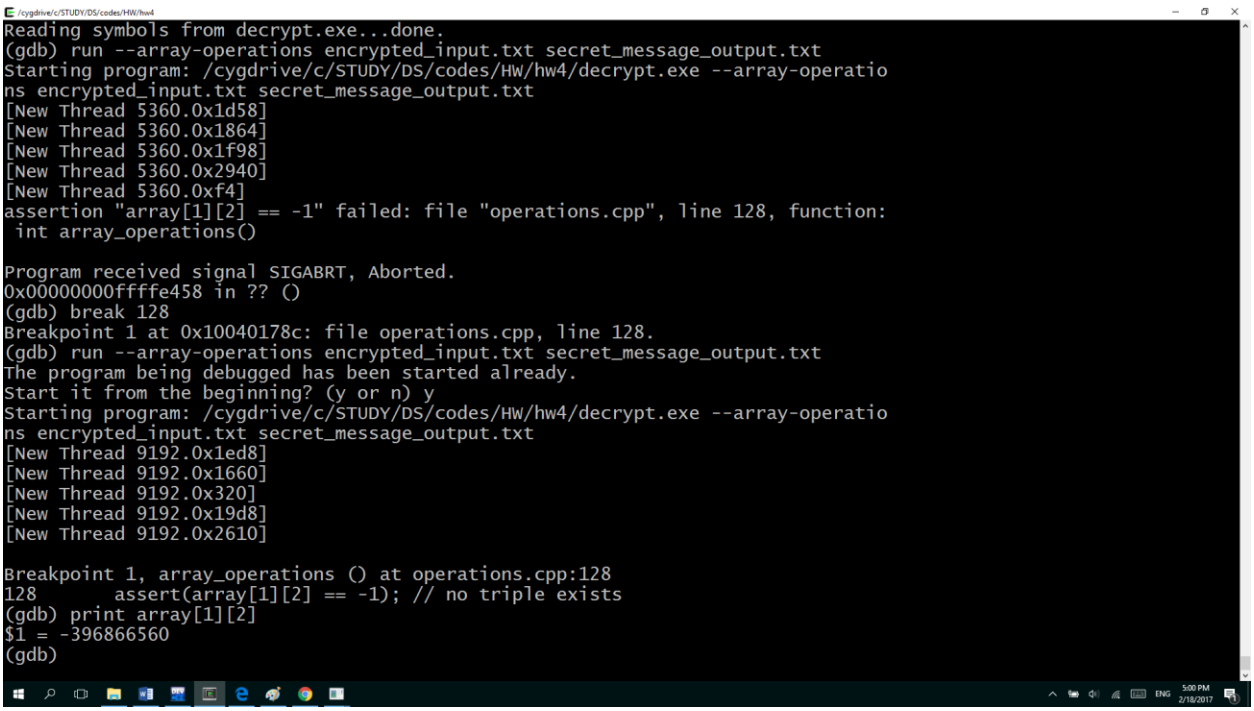
Process:

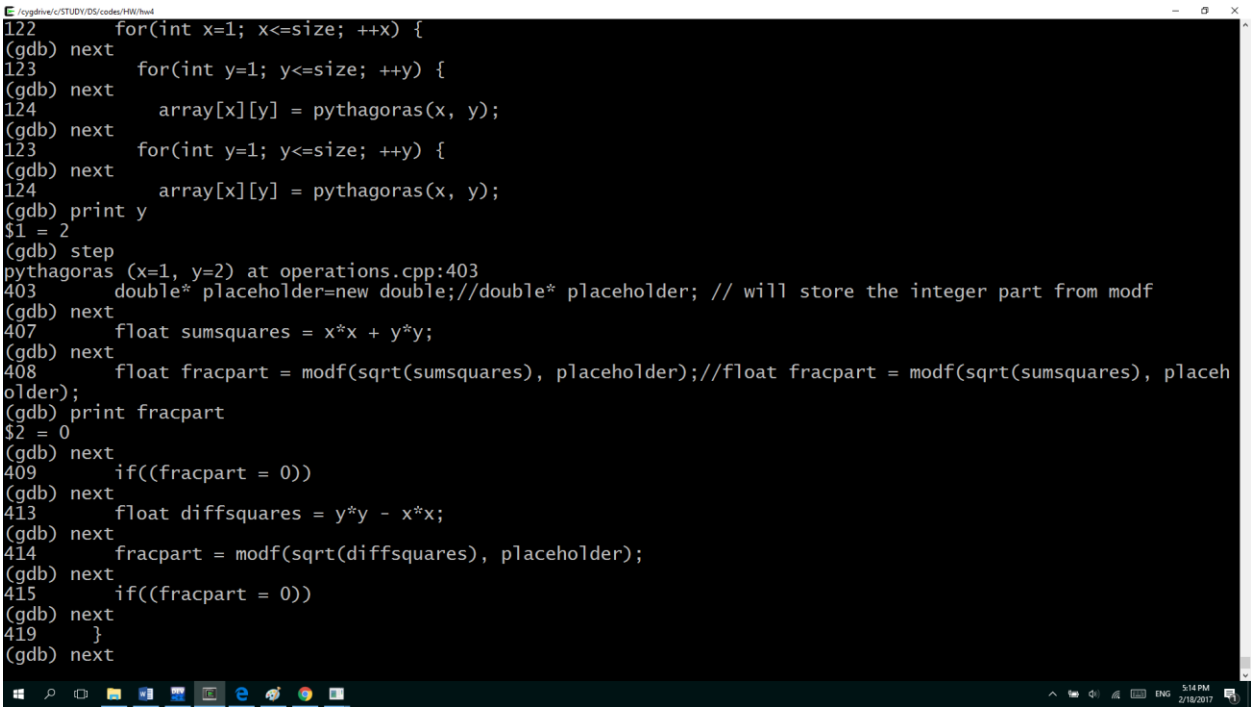
1. Run ./decrypt.exe --array-operations encrypted_input.txt secret_message_output.txt. program dumping stack. Set several break point before each for loop in array_operations().
2. Run each check point, error happen at line 124 when function “pythagoras(x, y)” be called. Step in Pythagoras function.
3. Using next go through the Pythagoras function, I found the error happen at line 408 when “modf” function be called. According to reference, reference(address) should be passed to “modf”.
4. *Because a pointer is passed to “modf” function, according to C++ reference, it should be pass by reference. Change the pointer to double placeholder and pass in modf function by refernce;
5. Run the program again, error appear at line 128, which is assertion fail. Print out the value of array[1][2], found a strange number.
6. Step in “pythagoras” when x=1,y=2, and found program did not step into any if statement thus returning nothing. According to the requirement, “pythagoras” should return -1 if do not fit any of the requirement in “if”.
7. Assertion fail at line 129. Print value of array [3][4] which is -1. Step in “pythagoras” when x=3,y=4. GDB shows that program does not step in if statement. Fix the syntax of that part.
8. Assertion fail at line 130. Print value of array [5][4] which is -1. Step in “pythagoras” when x=5,y=4. GDB shows that program does not step in if statement (ideally should step in the second “if”). Print out the variable “diffsquares” which shows a negative number. Add “abs” to change negative to positive.

Debugger use:




```
Breakpoint 1, array_operations () at operations.cpp:124
124           array[x][y] = pythagoras(x, y);
(gdb) print x
$1 = 1
(gdb) print y
$2 = 1
(gdb) step
pythagoras (x=1, y=1) at operations.cpp:407
407       float sumsquares = x*x + y*y;
(gdb) next
[New Thread 10524.0x1d70]
408       float fracpart = modf(sqrt(sumsquares), placeholder);
(gdb) next
[New Thread 10524.0x1ed4]
     0 [main] decrypt 10524 cygwin_exception::open_stackdumpfile: Dumping stack
 trace to decrypt.exe.stackdump
[Thread 10524.0x1ed4 exited with code 35584]
[Thread 10524.0x2e14 exited with code 35584]
[Thread 10524.0x1a88 exited with code 35584]
[Thread 10524.0x2ddc exited with code 35584]
[Thread 10524.0x1d70 exited with code 35584]
[Inferior 1 (process 10524) exited with code 0105400]
(gdb)
```





Error 8:

Isolation:

Function “vector_sum(std::vector<int> inVec)” Line 369.

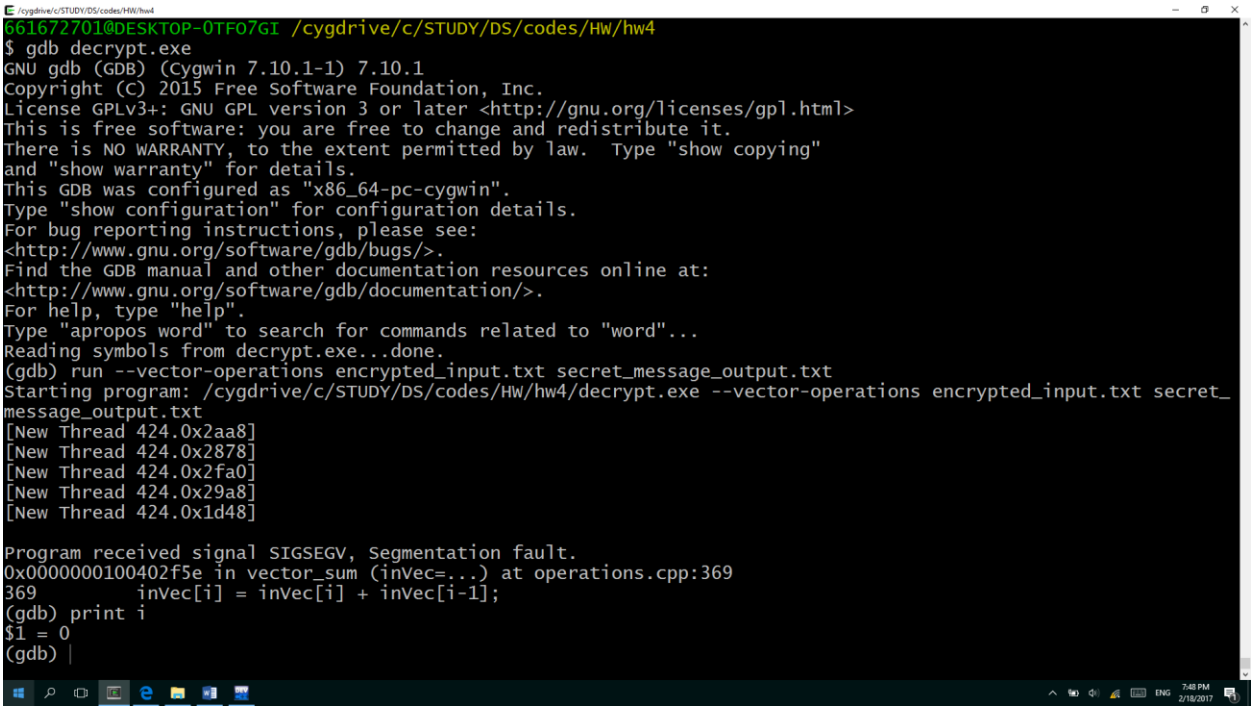
Description:

invalid access to array: index of vector out of bond (line 369)

Process:

1. Run --vector-operations encrypted_input.txt secret_message_output.txt, GDB shows segment fault at line 369.
2. Print out the value of I, it shows that i-1=-1, which is an invalid index of vector. Thus changing the initial value of I in for loop to be 1 and maximum bond to i< inVec.size(). (line 368)

Debugger use:



Error 9:

Isolation:

Line 196 assertion fail.

Line 371 function ”vector_sum”

Description:

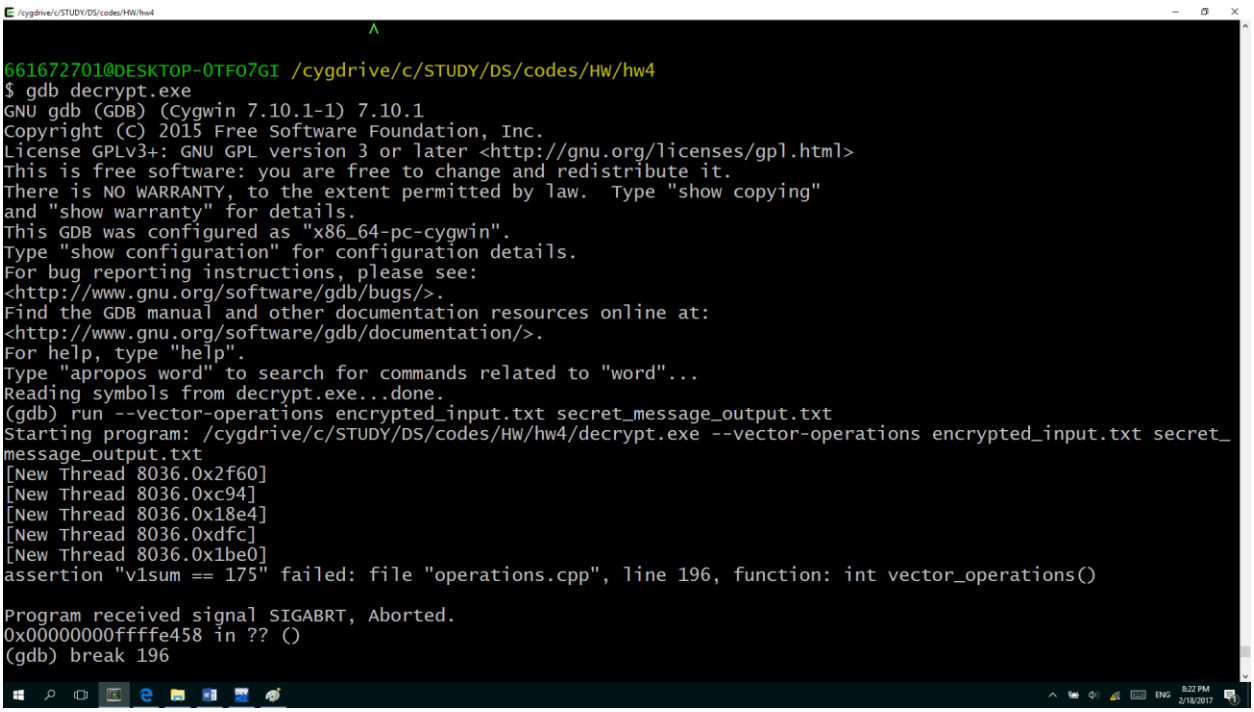
Line 371 function ”vector_sum” using an invalid index cause program dumped and assertion fail.

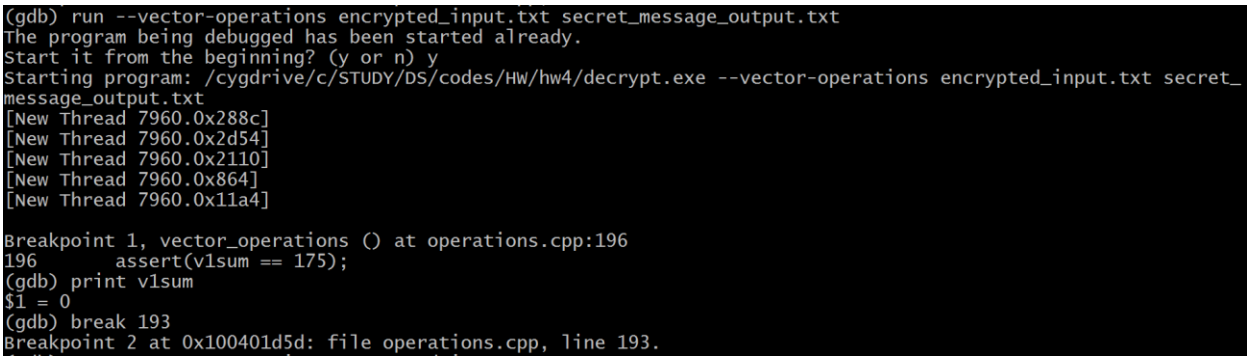
Process:

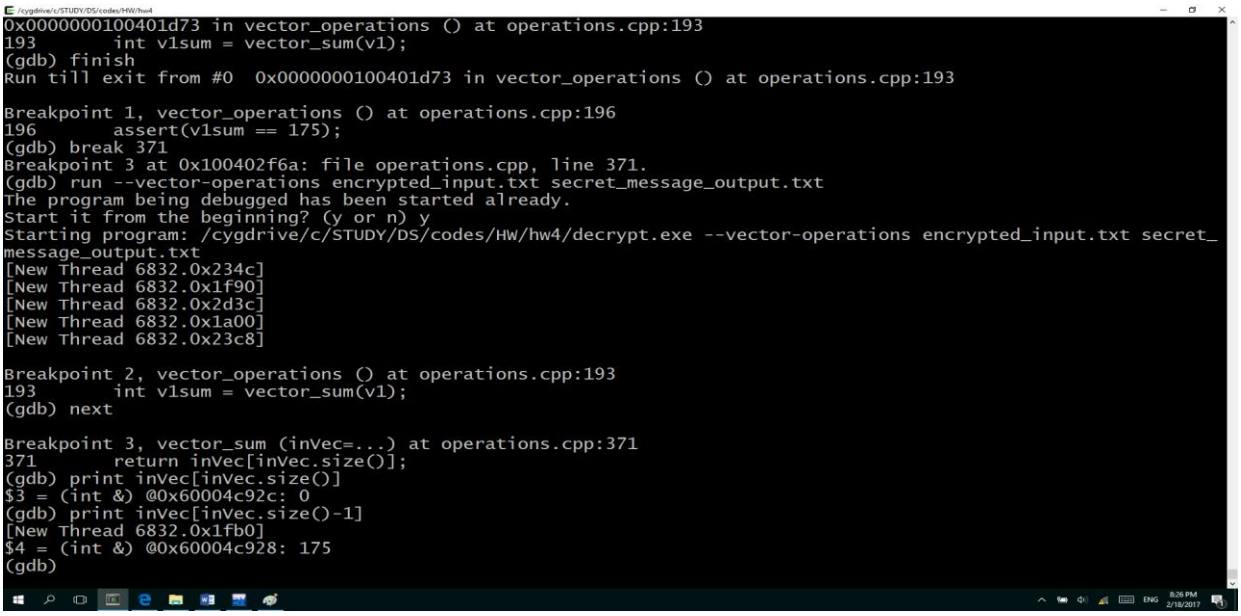
1. Run --vector-operations encrypted_input.txt secret_message_output.txt. GDB shows insertion fail and program dumped at line 196.

2. Because the variable “v1sum” is assigned by function “vector_sum”, set break point in the function.
3. Print the return value (line 371) in gdb, which shows the value is 0, and found the problem on the index. Index should be inVec.size()-1.

Debugger use:







Error 10:

Isolation:

Line 197 assertion fail. Line 367(line 29(clarification))

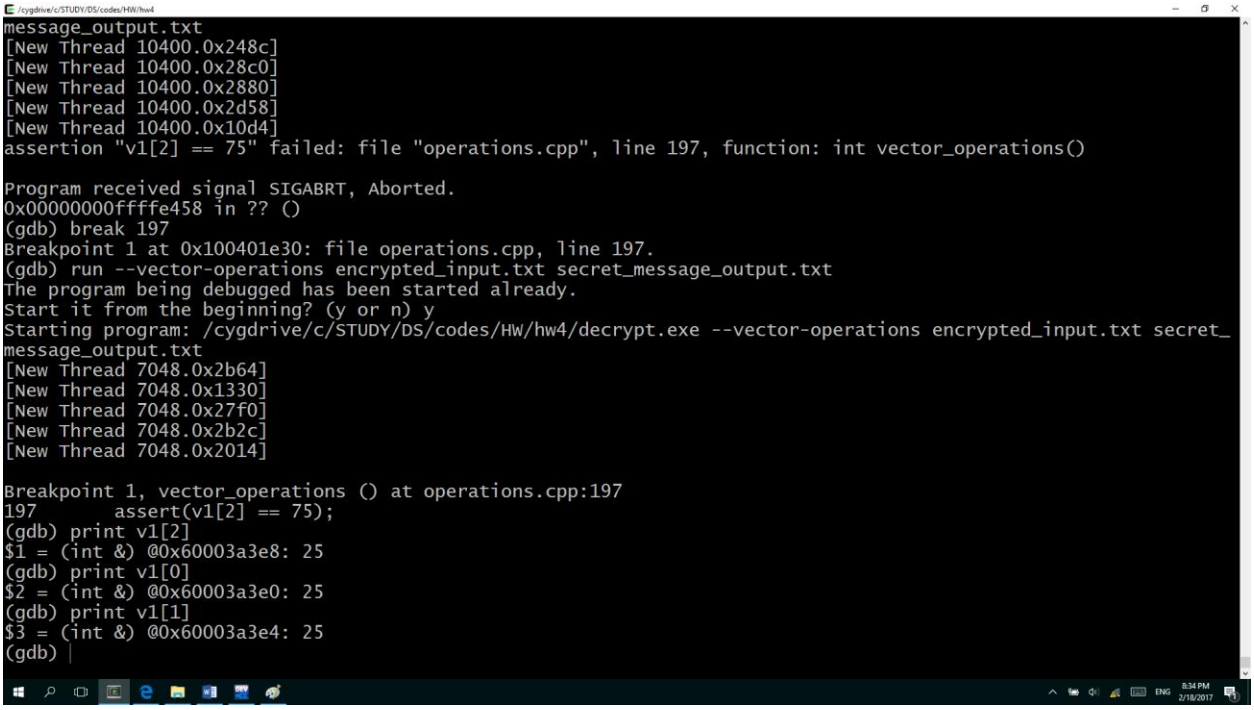
Description:

function “vector_sum” does not “pass by reference” thus changing nothing of the vector.

Process:

1. Set break point at 197. And try to print out several value in v1. They shows that after function “vector_sum”, the values in v1 does not change.
2. In order to make function “vector_sum” to change values in vector, pass by reference. (line 29, line 367)

Debugger use:



Error 11: line 183

Error 12: line 211 unitialized variable

Error 13: line 381 compare false

Error 14: line 268 infinite loop

Error 15: line 272, false push_back (index)

Line 269, compare with index

Error 16: line 271, uinitialized counter

Error 17: line 279, unsinged int can not less than 0

Error 18:line 447, list iterator stuff..

Error 19: line 494,list iterator stuff..

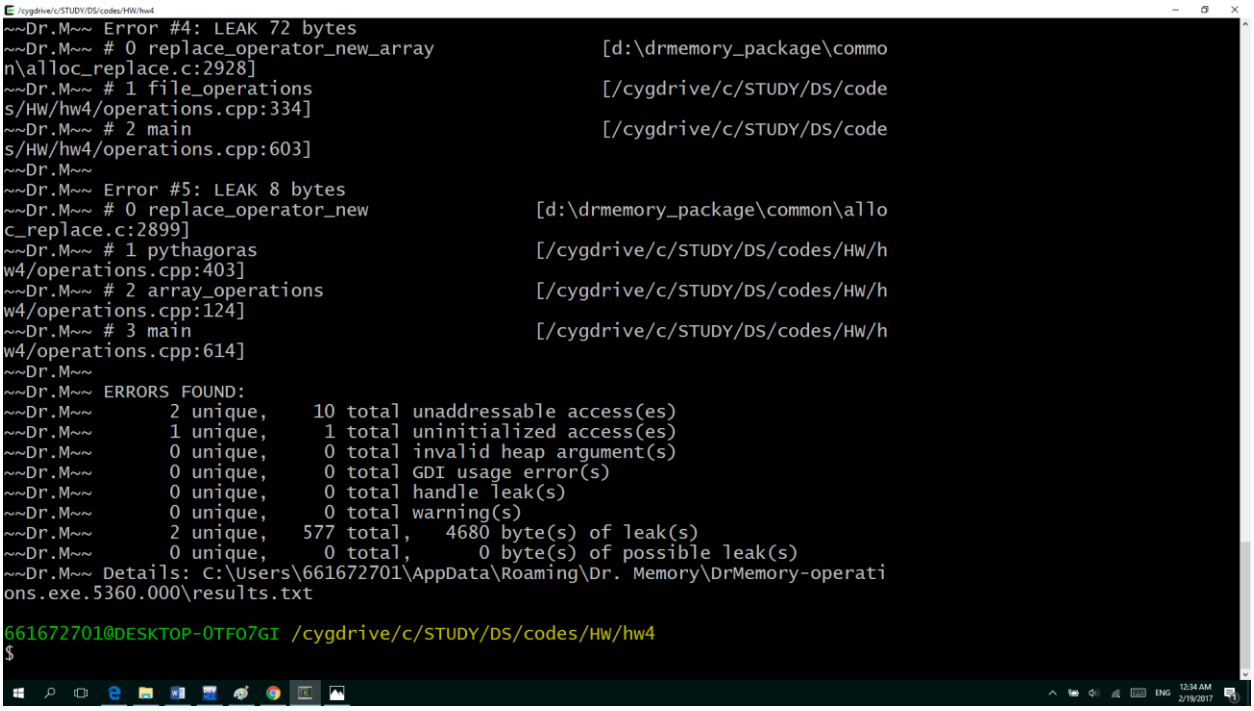
Error 20: assertion fail 524 ,line 428, order of list

Error 21: line 517, break stops all for loop

Error 22:line 446, bool false

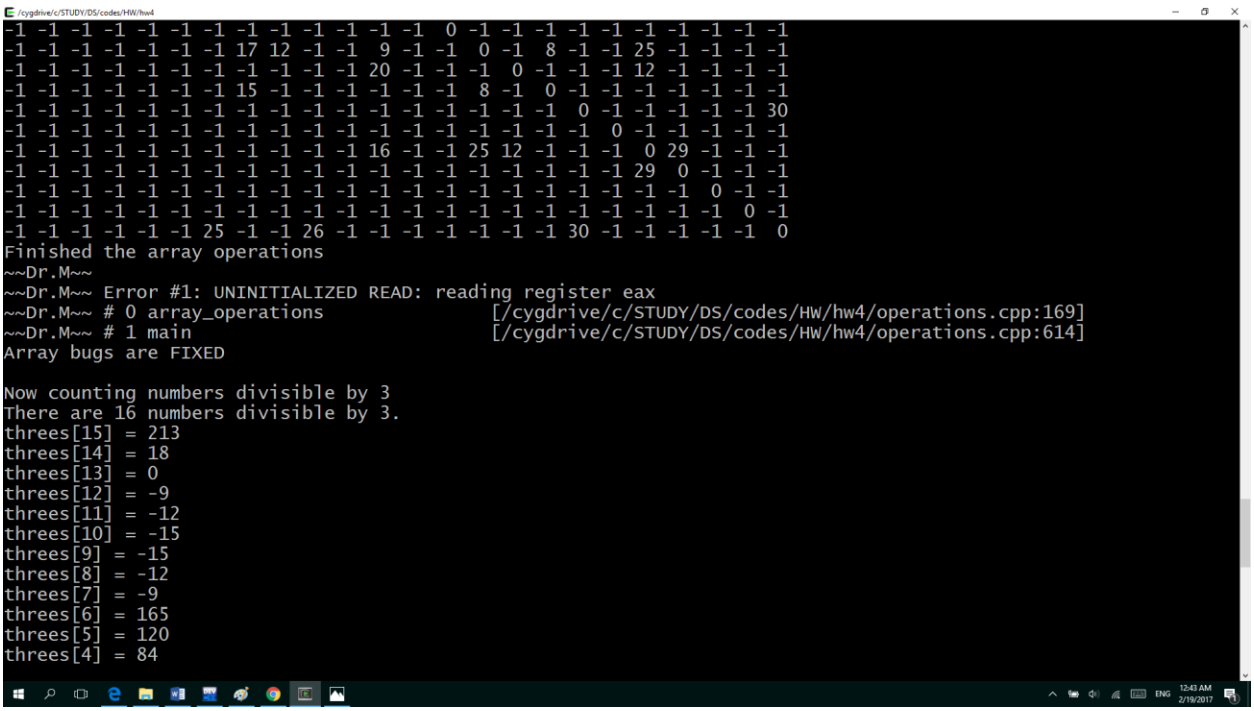
Error 23:line 324, assignment before initialize

Error 24: with drmemory



Line 381: what if size of v2<v1? Array out of bond

Error 25: with drmemory



Line 168: because the first row of array not initialized, thus cannot be delete as an array

Error 25: with drmemory

Memory leak:

Line 644 and line 647 added delete for buffer