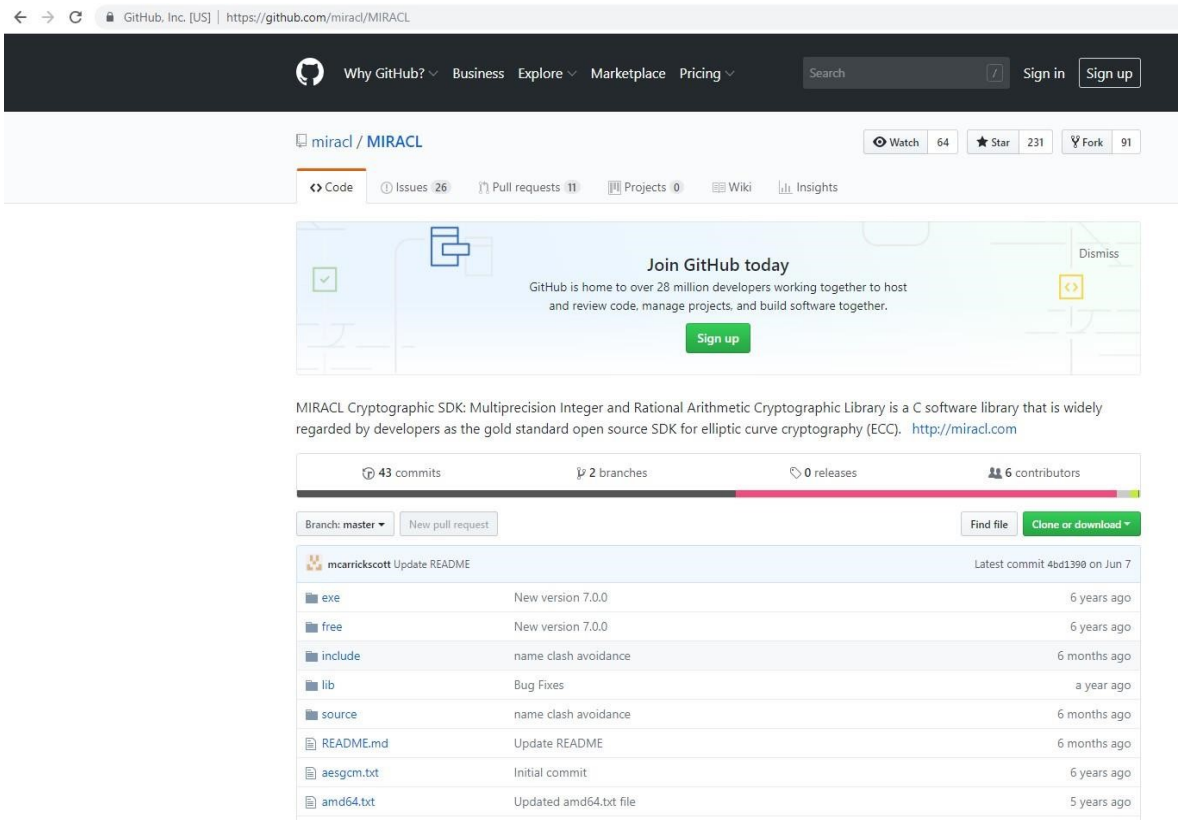
0. Compiling the MIRACL Library (.lib)

MIRACL [1] is an open source software library for implementing cryptographic algorithms, written in C. It can be used for writing C or C++ program that requires elliptic curve cryptography (ECC). It supports multi-precision arithmetic like modular multiplication, modular exponentiation, etc. These operations can work with very large integer (e.g., 1024-bit, 2048-bit, etc.) due to the efficient implementation in MIRACL. To use MIRACL in Windows, we need to first compile it as a static library (.lib), then link it to the program that we developed. The subsequent paragraphs walk you through the process of creating and linking the MIRACL library in the Visual Studio environment.

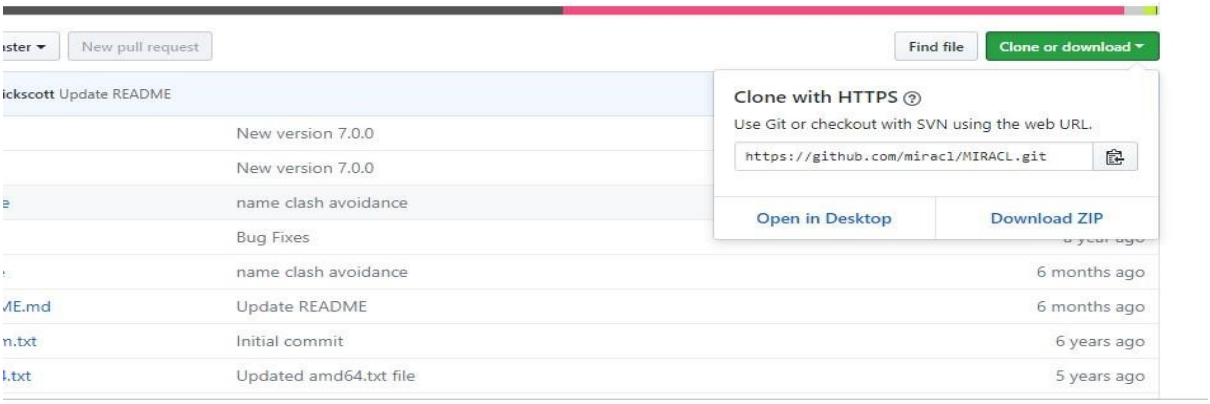
The program is compiled in Windows 10 using Visual Studio 2012.

- We will compile the Miracl library. We will use the library in our programs to build cryptographic schemes. To compile the library, perform the following steps.
- First of all, download the Miracl distribution. To download the Miracl distribution, go to the GitHub link given below:

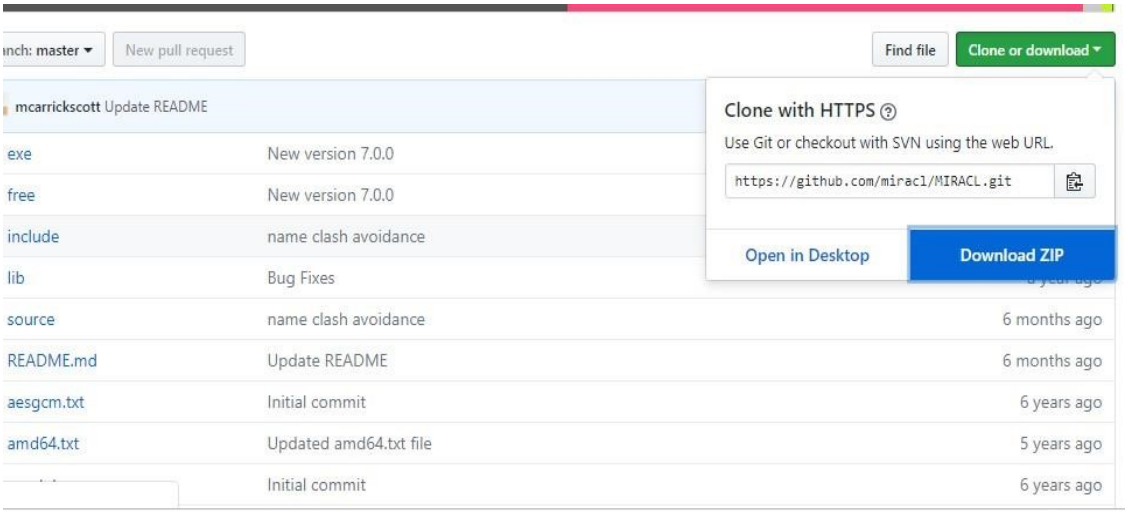
  https://github.com/miracl/MIRACL



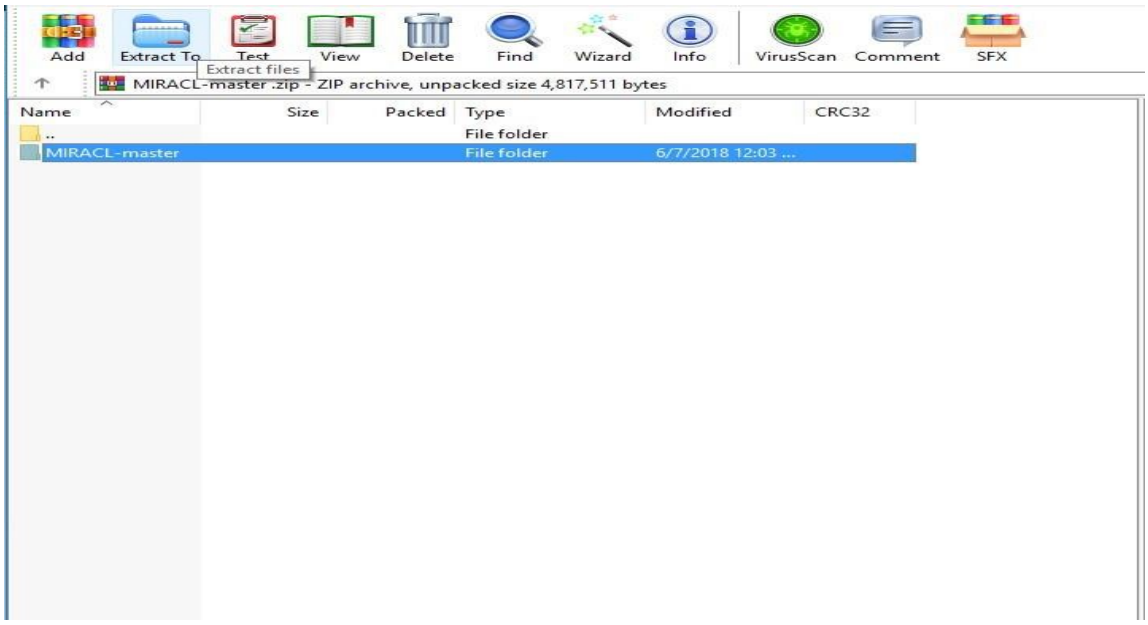
- Now click on “Clone or download” as follows.

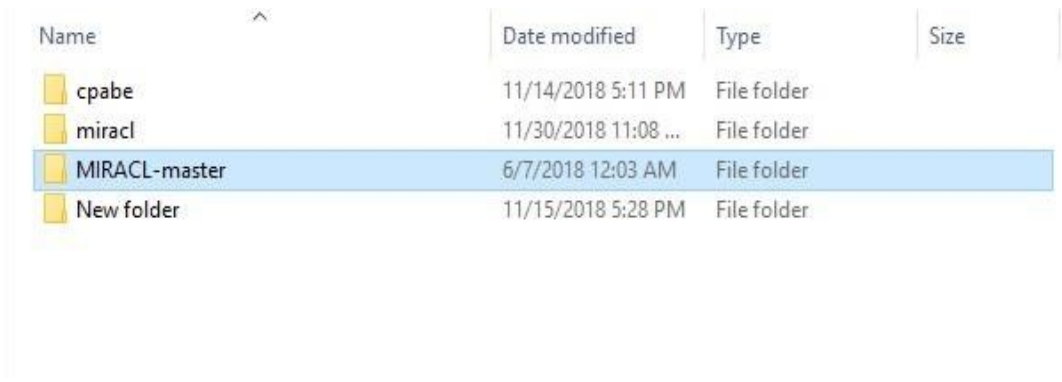


- Click on “Download Zip”



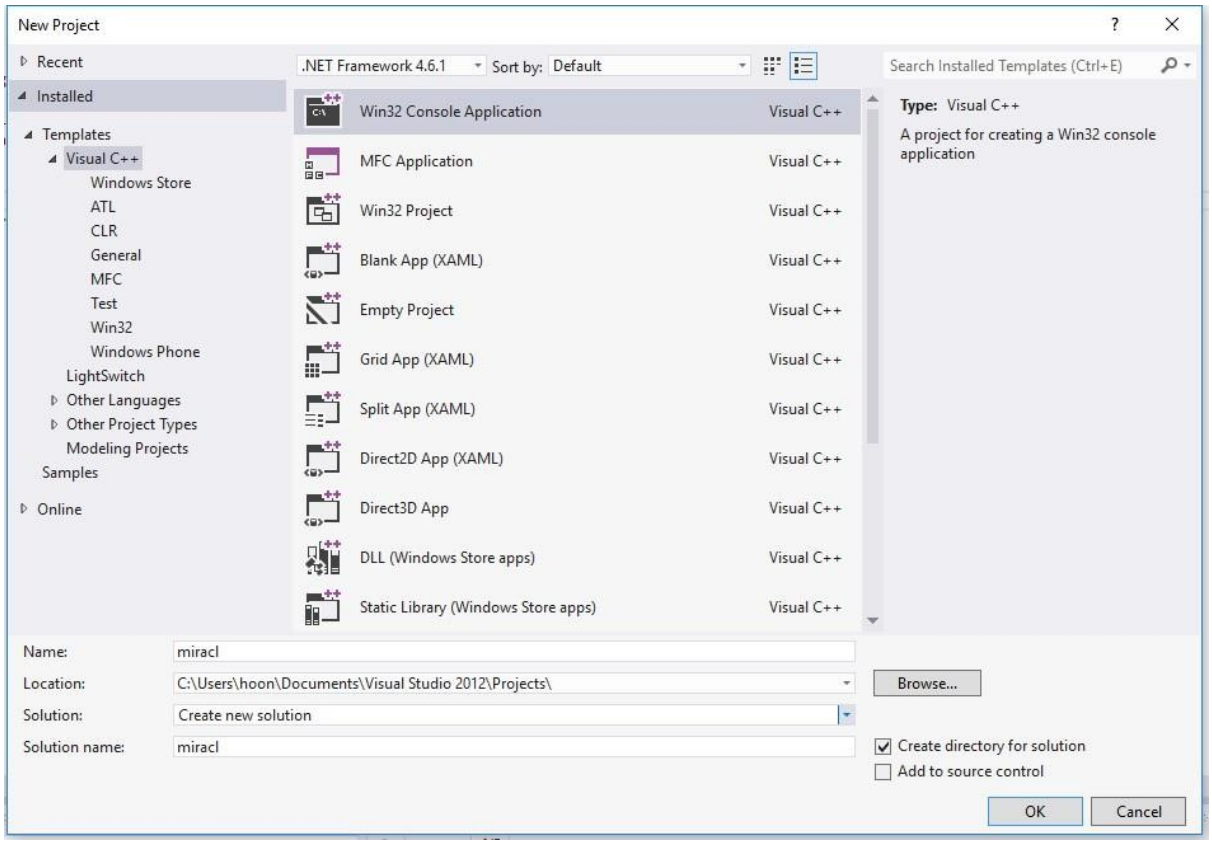
- Open the downloaded “MIRACL-master.zip file ” and extract the Miracl-master folder as follows.





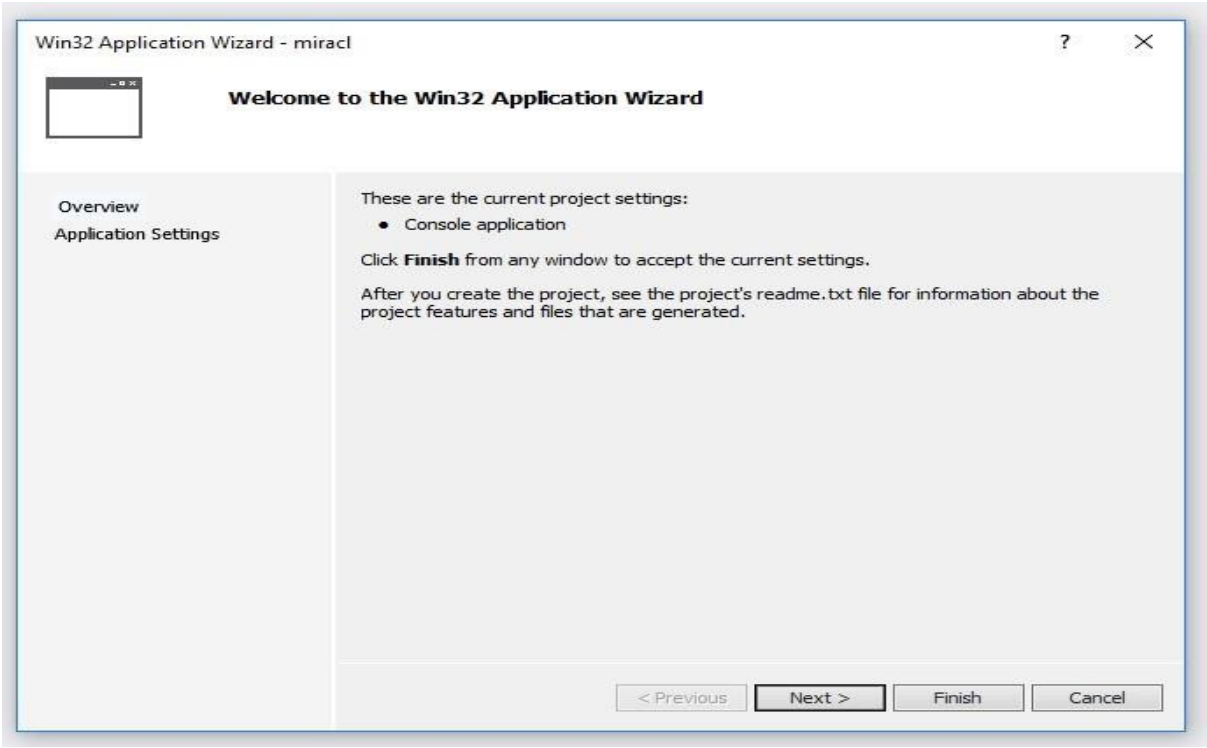
- The steps below describe how to start compiling the MIRACL library (miracl.lib).

1. Select New Project, Console Application

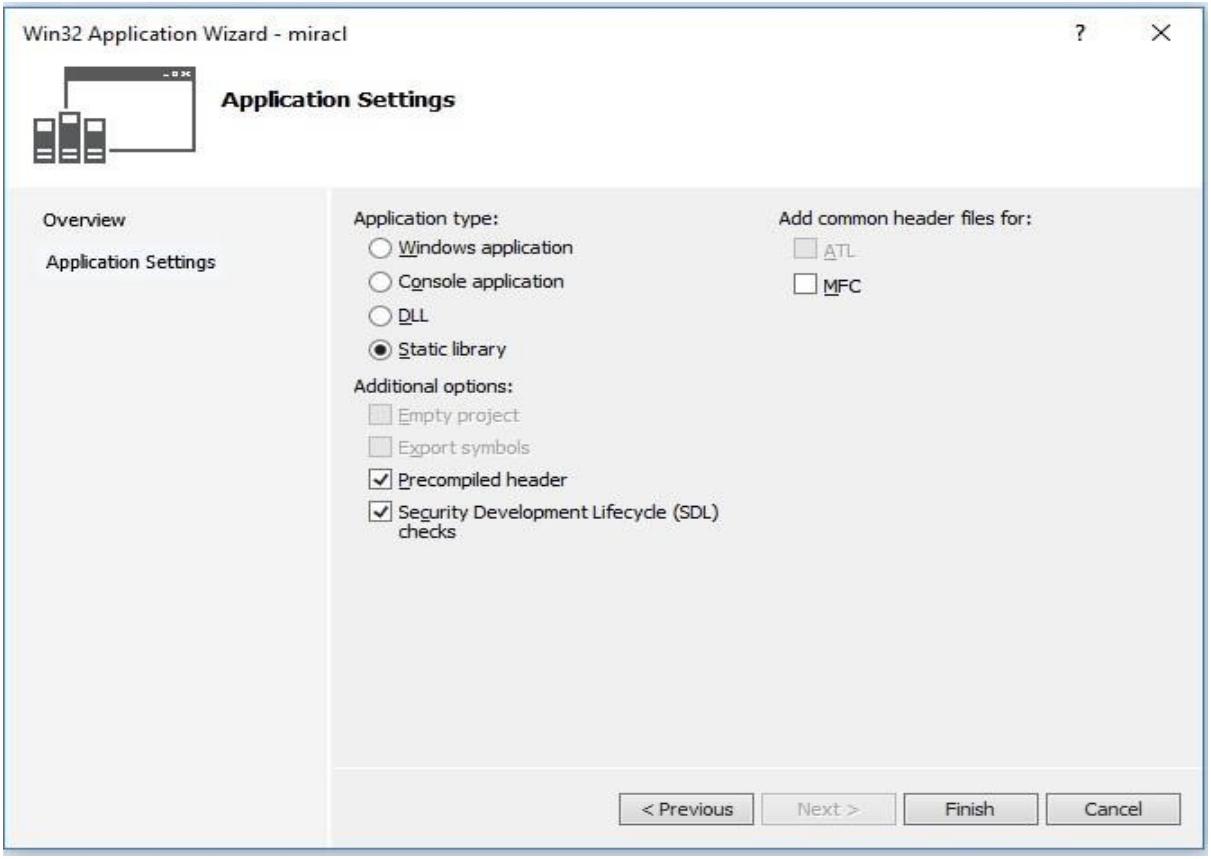


2. Name: miracl (it is important to name the project as “miracl” because we will be later using miracl key word to include it in other program for cryptographic schemes)
3. Location: “C:\Users\hoon\Documents\VIisual Studio 2012\Projects\”. Note “hoon” in this case is user name, like if the user name is “xxx” location will be “C:\Users\xxx\Documents\Visual Studio 2012\Projects\”
4. Solution name: miracl
5. Click OK.

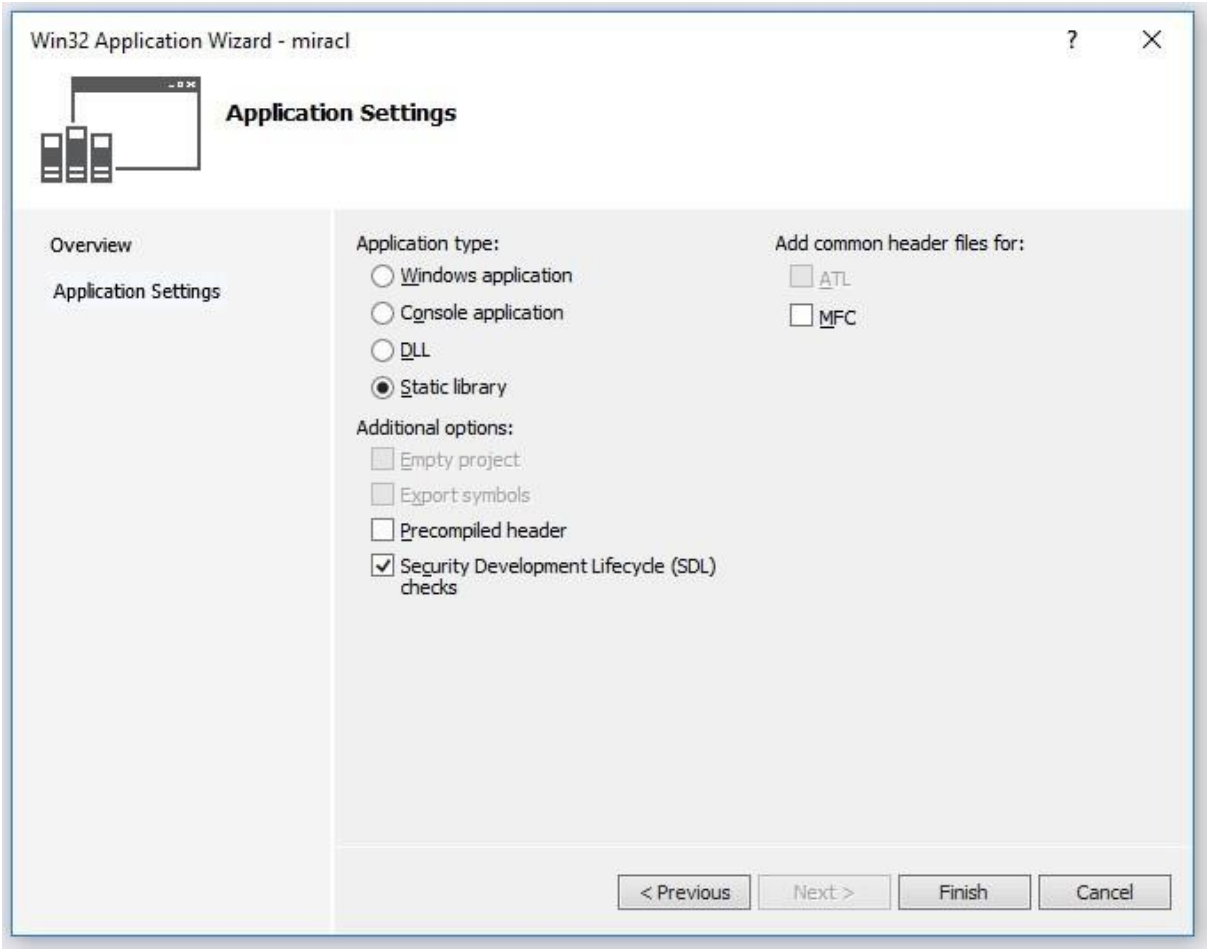
6. Click Application settings, then you can see the application settings in left panel as follows.



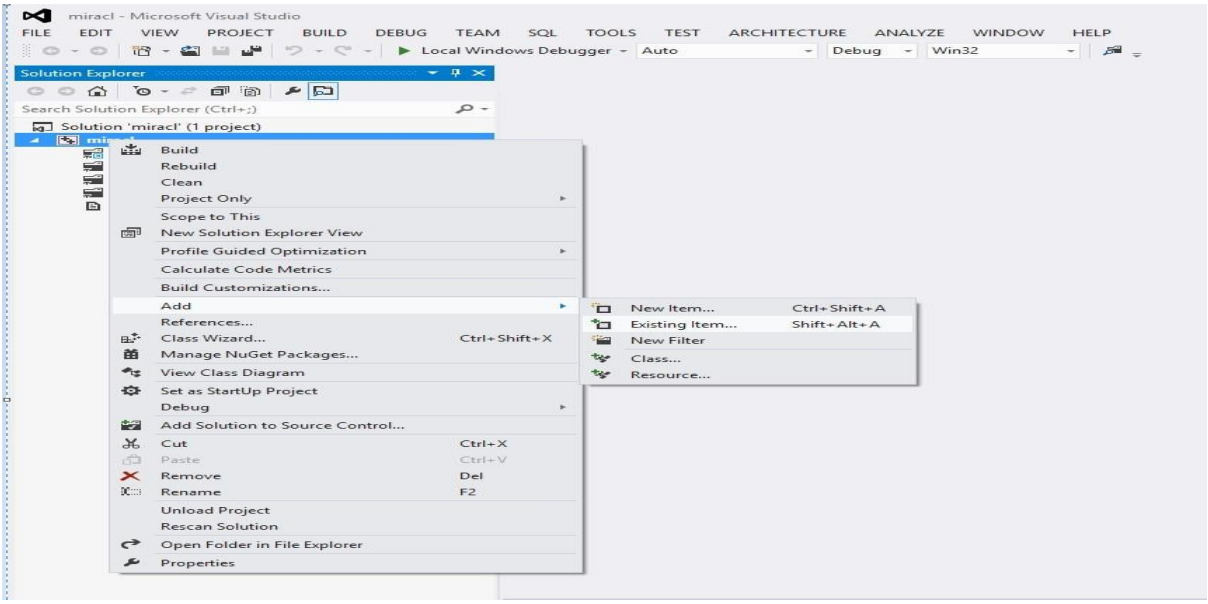
7. Click on Static library.



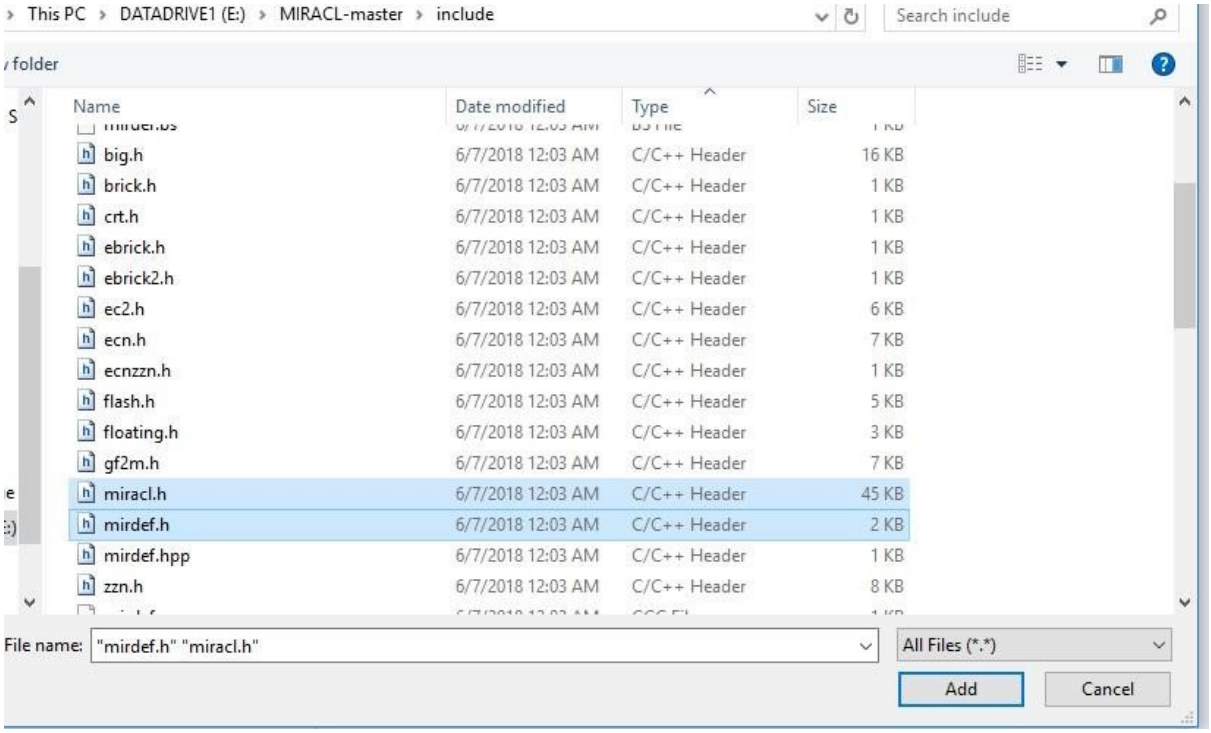
8. Disable precompiled header.



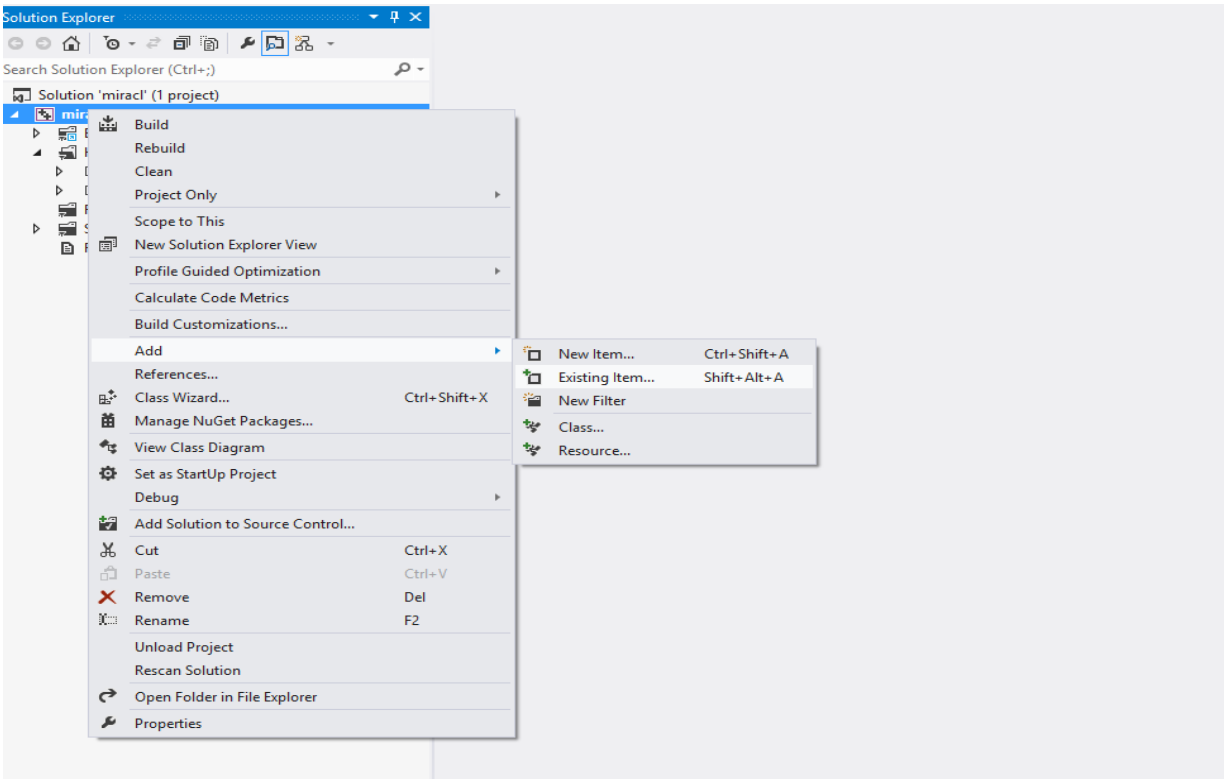
9. Click on Finish.
10. Click on Project (in this case it is “miracl” in the left panel as shown in figure), and go to Add→Existing Item.



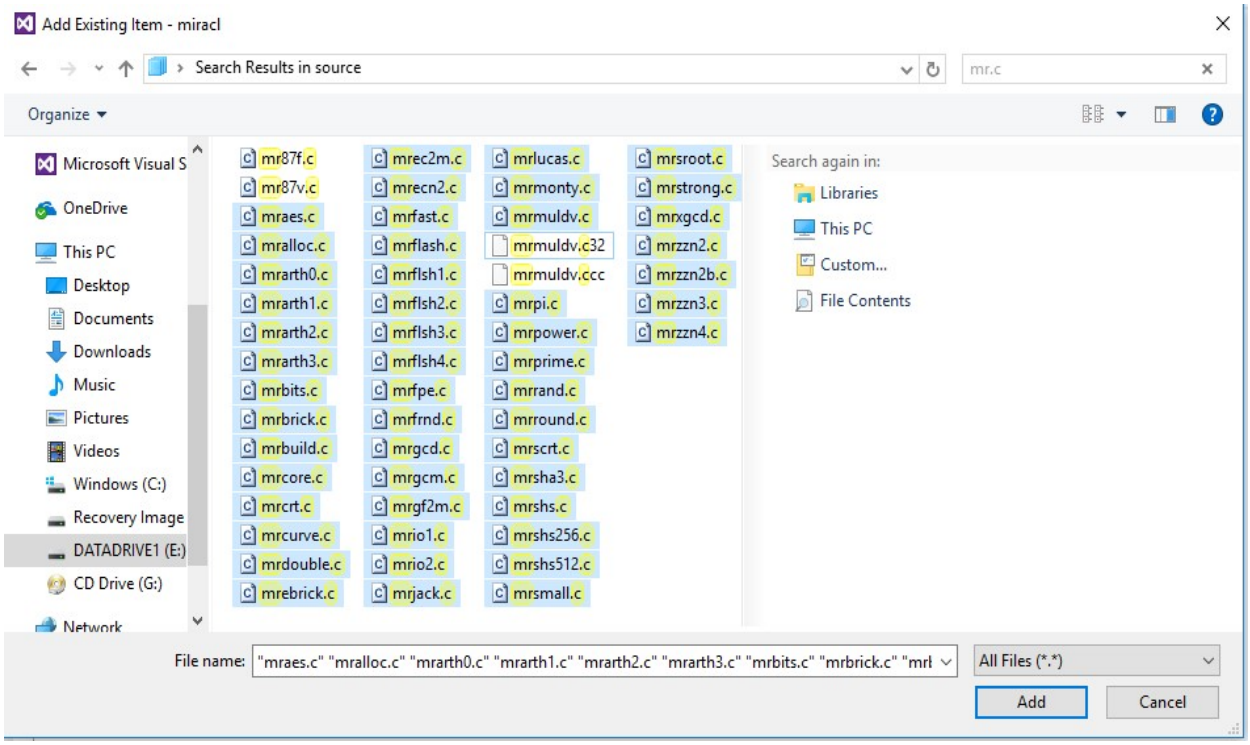
11. Add miracl.h and mirdef.h from wherever you have unzipped the miracl distribution.



12. Click on Project (in this case it is “miracl” in the left panel as shown in figure), and go to Add→Existing Item.

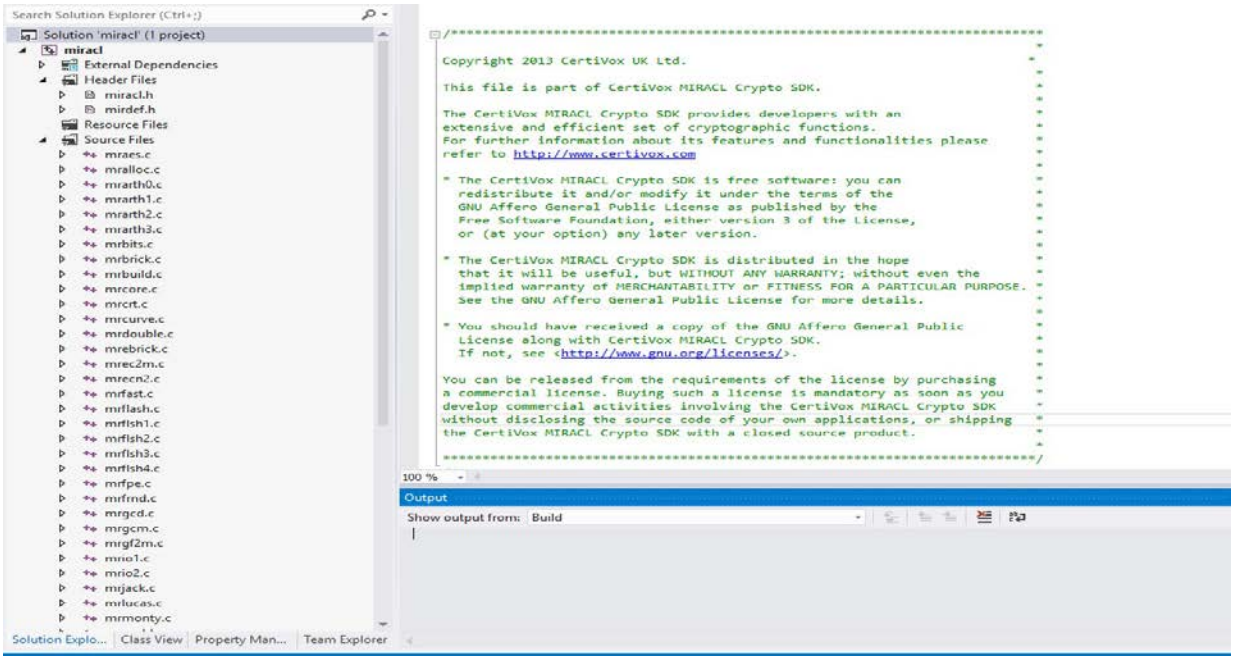


13. Add the following miracl source files from the miracl distribution to the project.

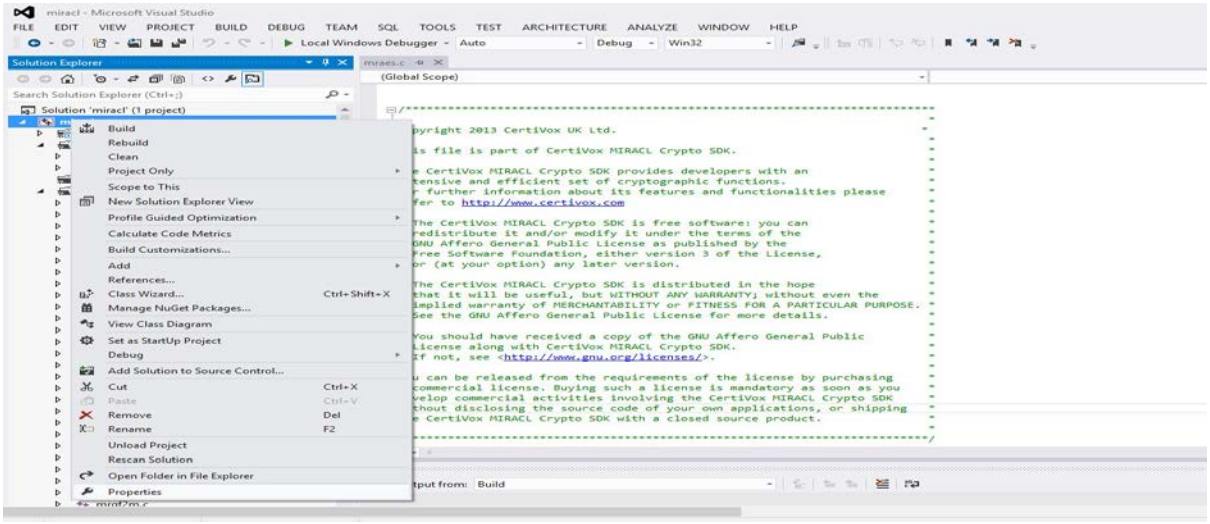


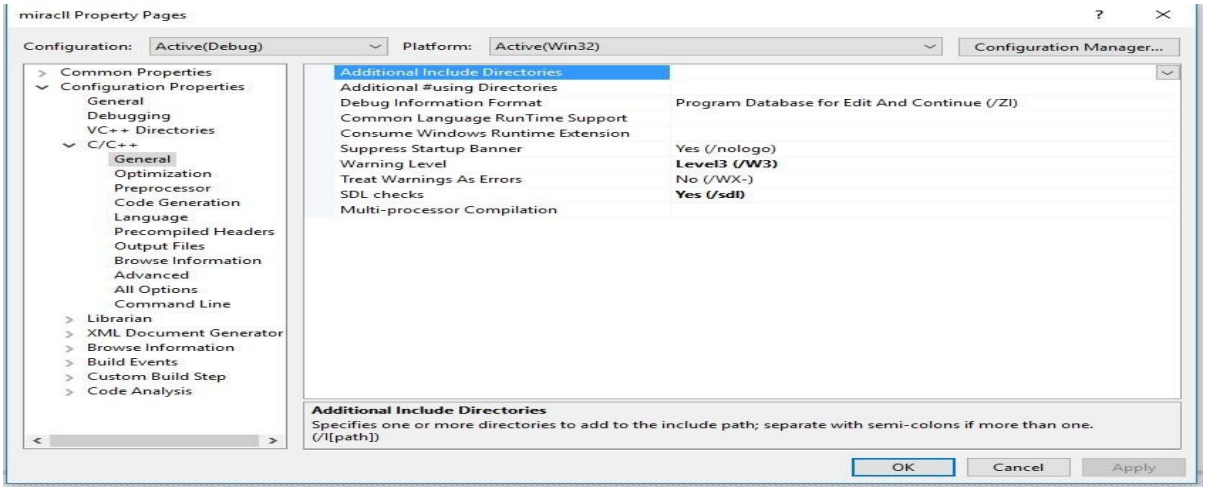
- mraes.c
- mralloc.c
- mrarth0.c
- mrarth1.c
- mrarth2.c
- mrarth3.c
- mrbits.c
- mrbrick.c
- mrbuild.c
- mrcore.c
- mrcrt.c
- mrcurve.c
- mrdouble.c
- mrebrick.c
- mrec2m.c
- mrgf2m.c
- mrfast.c
- mrflash.c
- mrflsh1.c
- mrflsh2.c
- mrflsh3.c
- mrflsh4.c

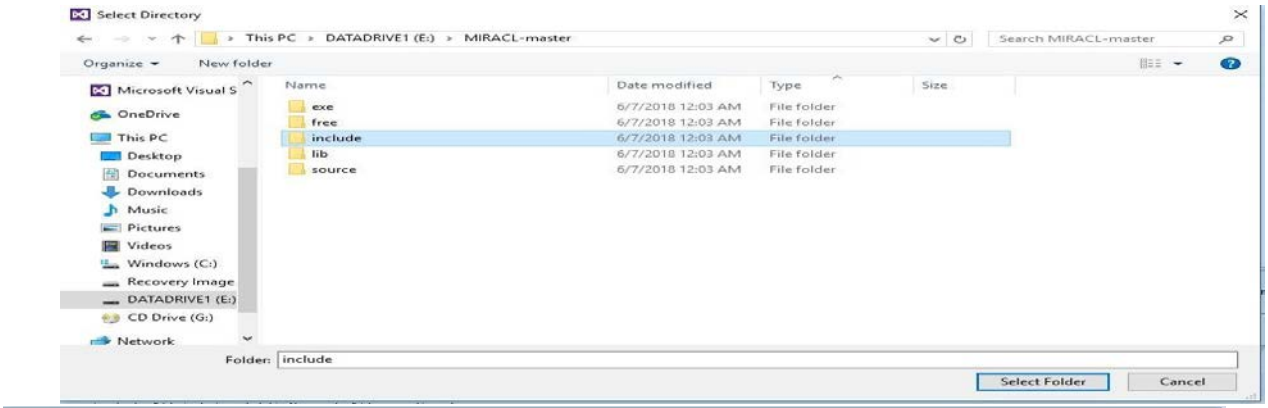
- mrfrnd.c
- mrgcd.c
- mrgcm.c
- mrio1.c
- mrio2.c
- mrjack.c
- mrlucas.c
- mrmonty.c
- mrmuldv.c
- mrpi.c
- mrpower.c
- mrprime.c
- mrrand.c
- mrround.c
- mrscrt.c
- mrshs.c
- mrshs256.c
- mrshs512.c
- mrsmall.c
- mrsroot.c
- mrstrong.c
- mrxgcd.c
- mrecn2.c
- mrzzn2b.c
- mrzzn3.c
- mrzzn2.c
- mrzzn4.c

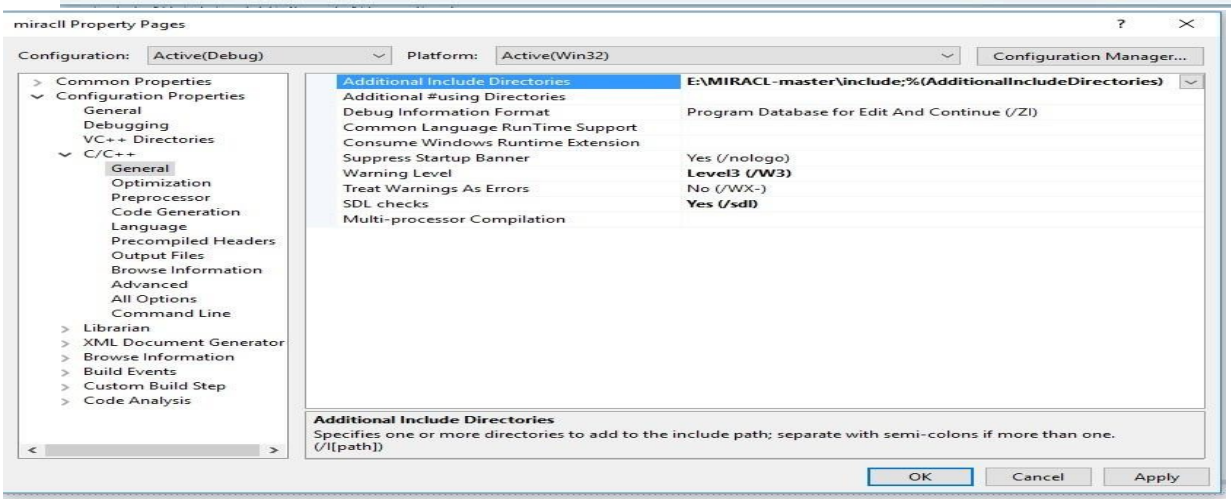


14. Right click on the miracl in the left panel and go to the properties→C/C++→General →Additional Include directories. Then select the include folder from miracle distribution as show in below figure.

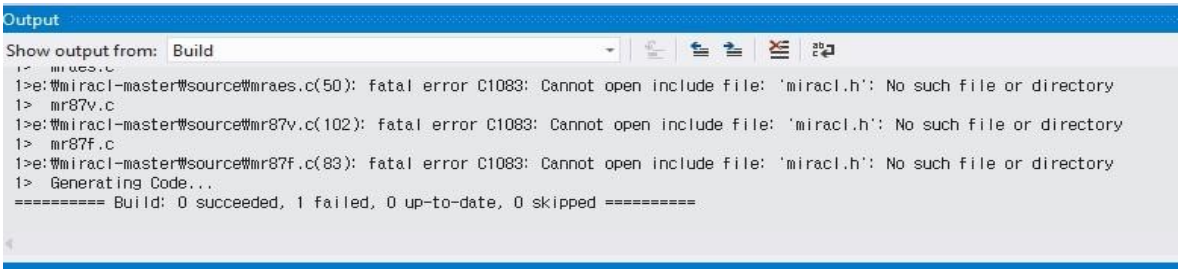






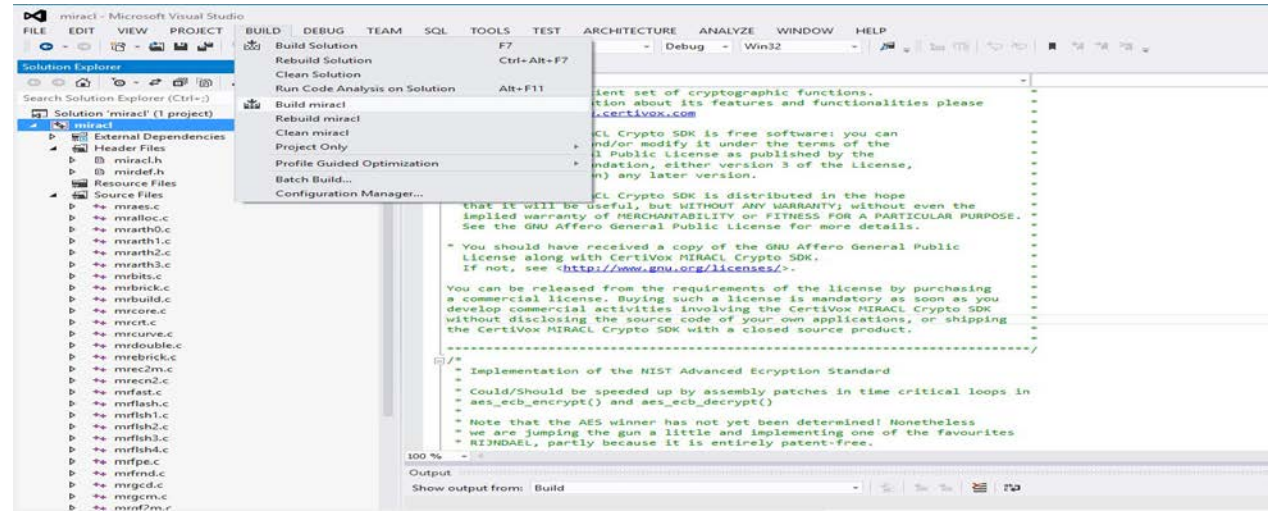


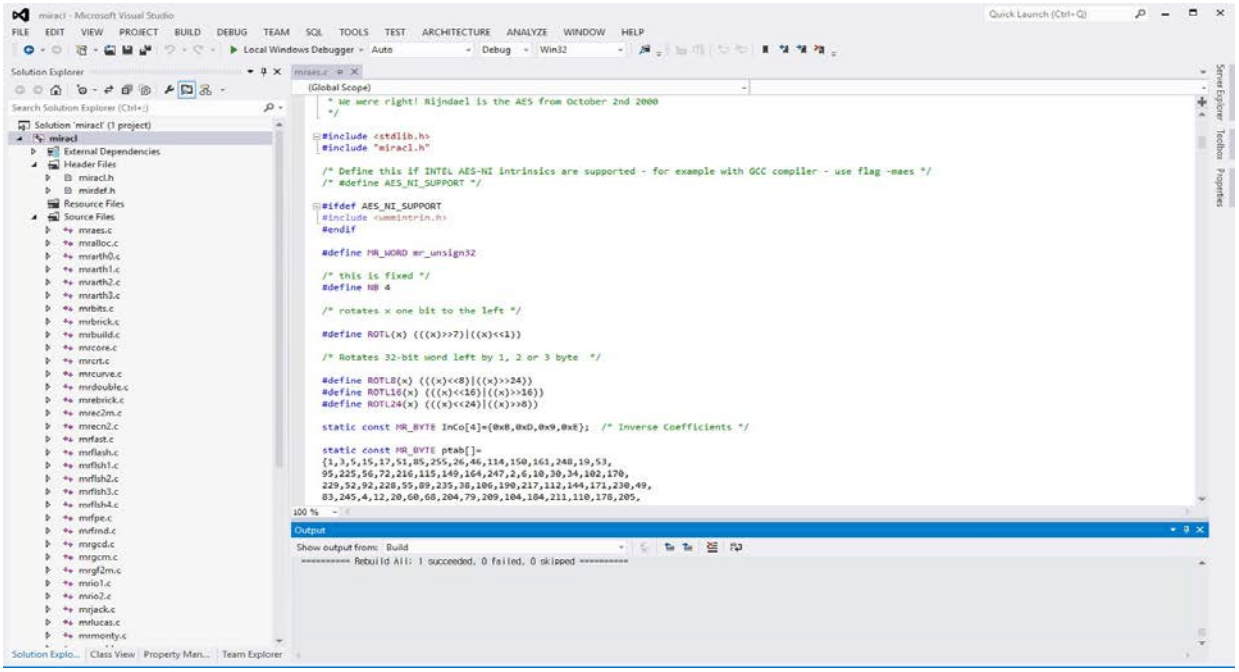
- Note: if you will not include the “include” directory of miracl distribution, the compiler cannot build the program, prompting the following errors.



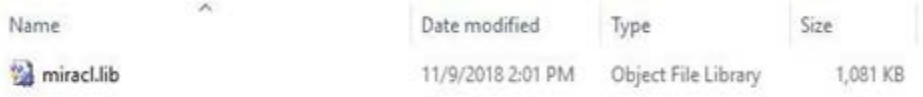
To avoid the error, you must include the “include directory of miracl distribution”.

- Then Click on Build miracl. The library is created in the directory.





- Go to the location where you built the project. For example, in this case: In the location "C:\Users\hoon\Documents\Visual Studio 2012\Projects\miracl\debug\miracl.lib", you will find the "maricl.lib" file. Note "hoon" in this case is user name, like if the user name is "xxx" then you can find the file in "C:\Users\xxx\Documents\Visual Studio 2012\Projects\miracl\debug\miracl.lib".



References:

1. Multiprecision Integer and Rational Arithmetic Cryptographic Library (MICARL), https://github.com/miracl/MIRACL