

---

Home Computer Instructions for **MATH2068/2988 Number Theory and Cryptography**

---

If you are enrolled in MATH2068/2988, you can download the student version of MAGMA to install on your own computer. This would allow you to do some of the computer laboratories (as well as the computer parts of the assignments) on your own computer, in your own time, meaning you would not have to attend the corresponding timetabled laboratory sessions. It would also allow you to continue the lab exercises after your scheduled session, or do your own further experimentation. The disadvantage of working outside the labs, of course, is that you will not have a tutor to help you, and we cannot guarantee that everything will work the same way. The steps are as follows:

1. To download the student version of MAGMA, go to:

<http://www.maths.usyd.edu.au/u/dhowden/loc/>

You will need to log in with your UniKey. Follow the instructions for download and installation appropriate to your computer. **Important note: you may see instructions to email your MAC address to obtain a passfile; ignore this, it is no longer required.**

2. Create a new directory (or folder) called something like “MATH2068” to store all your MATH2068-related files. Then download the MAGMA add-on packages designed for MATH2068/2988, listed as “MAGMA start-up file 1” and “file 2” in the Resources Table on the MATH2068/2988 webpage (under Week 1), as well as the data file(s) needed for the labs you want to do, listed as “Lab 2 data file”, etc. Save these in your MATH2068 directory, being **careful not to change the file names**<sup>1</sup> (which are MagmaProcedures.txt and m2068crypto.m for the start-up files and tut2data.txt, etc., for the data files).
3. To start MAGMA, open a terminal or command prompt and navigate so that MATH2068 is the current directory. Then type `magma`. (If you accidentally start MAGMA from the wrong directory, you can use the command `GetCurrentDirectory()`; to see which directory is the current one, and `ChangeDirectory("MATH2068")`; to change to the MATH2068 directory.)
4. To work on the MATH2068/2988 exercises away from the computer lab, you will need to type `load "MagmaProcedures.txt"`; as your first MAGMA command. This defines certain additional functions, and causes the further package `m2068crypto.m` to be attached. Then you should type any further commands such as `load "tut2data.txt"`; as instructed on the lab exercises sheet (which you can find on the MATH2068/2988 webpage, of course).
5. The other difference from working in the laboratories is that a log file of your MAGMA session will not be automatically created. To create a log file (which you will need to do, for instance, if you want to complete the computer part of the assignment at home), use a command such as `SetLogFile("comptut2.log")`;
6. Otherwise, you should be able to follow the lab exercises sheet just as if you were in the laboratories. If you get stuck in the absence of a tutor, you should consult the commented log file (also on the MATH2068/2988 webpage) to see if it resolves your question; otherwise, you can post a question on the Ed forum or email [dzmitry.badziahin@sydney.edu.au](mailto:dzmitry.badziahin@sydney.edu.au). Please give a full description of the problem, including any relevant commands and output, and details of your computer and software. However, a solution is not guaranteed.

---

<sup>1</sup>The file listed as “file 2” is named `m2068crypto.m`, the `.m` extension being traditional for objective C files but unfamiliar to some operating systems; your computer may automatically add another extension to the file name, in which case you will have to manually change it back.