CPSC 418 / MATH 318 Introduction to Cryptography

How to succeed in this course

This is a compilation of 8 recommendations, mainly **from students for students** that will help you succeed in this course. They are based on the remarkably consistent feedback we have received from students in this course over many years through teaching feedback surveys, supplemented by your instructor's observations.

1. **Know your course.** Familiarize yourself with the structure, expectations, policies, procedures, schedule (including exam and assignment due dates) and resources for this course. That way, you are prepared and avoid nasty surprises. Take time during our first week of classes to go through the entire course website and carefully read in particular the "home", "about" and "assignments" tabs. Be sure you have the necessary accounts (Piazza, Gradescope) and obtain other tools/environments you need (Python, LaTeX).
2. **Manage your time.** All assignment due dates and exam dates can be found on the course webpage. Budget your time accordingly, so you don't fall behind. Start the assignments early, take time to study, make time to attend lectures and (for CPSC 418) tutorials.
3. **Attend class and (for CPSC 418) tutorials.** Reading lecture slides, the textbook or tutorial materials is not a substitute for attendance, and most students learn much better from actually being there. It is my experience that there is in generally a strong correlation between attendance and performance.
4. **Prepare and review the material.** Preview and review the lecture slides. Review your marked assignments and consult the solution keys, so you detect potential knowledge gaps and learn from your errors. Same for marked exams.
5. **Do the assignments.** Irrespective of the portion of your final grade represented by homework, you learn the material by doing the assignments. Oh, and did I mention that you should start them early? They will take time, and there is a reason why they are posted at least 3 weeks in advance of the due date.
6. **Practice.** Cryptography sits squarely between math and computer science, so it requires skills from both disciplines. The "about" tab on our web page lists the body of knowledge and skills expected for this course. You learn math, programming and LaTeX the same way you learn a sport or a musical instrument: through practice, not by watching someone else (such as a professional athlete, virtuoso, instructor or TA) do it. For math, do the practice problems posted on the "handouts" tab of the course web page and review your MATH 271/273 or CPSC 351 materials. For programming, there are lots of Python online resources. More resources can be found on the "references" tab of our course website.
7. **Ask and answer questions**. Post your questions on Piazza, read the responses and look at related posts. Monitor Piazza regularly. Make an effort to answer questions posted by others: not only are you helping your fellow students, but answering questions is a great way to ascertain whether you know and understand material. Additionally, ask questions during lectures, tutorials and office hours.
8. **Make use of the available resources**. You have a wealth of resources at your fingertips: lectures, lecture notes and handouts to introduce you to the material, tutorials for more student-driven hands-on exploration, assignments and exams for applying your knowledge and deepening your understanding, practice problems for … well, practicing basic mathematical machinery, a website that has all this and more in one place, an online discussion forum for questions and exchange of ideas, and first-hand access to experts in the field. Use these resources to put your tuition fees to work and to get the maximum out of this course.

Good luck, and enjoy the course!