This sheet summarizes information for the course MAT 302 S ("Algebraic Cryptography") during the Spring session of 2012 on the Mississauga campus at the University of Toronto. By the end of the first week of classes, you should have read and become familiar with the contents of this information sheet.

Course Website

`http://www.cs.toronto.edu/~vinodv/COURSES/MAT302-S12/`

The course website will be available at the start of the first week of classes and it will always contain the most up-to-date information possible regarding the course. *You are responsible for all announcements posted on the course web site*, so please check the `Schedule` and `Announcements` sections of the page frequently (at least once a week). You are also responsible for all announcements made in lectures: make a friend in class and get their notes if you miss class.

Instructor and Lectures Info

Instructor	**Office**	**Email**	**Office Hours**
Vinod Vaikuntanathan	*3073 CCT*	`vinod.vaikuntanathan@utoronto.ca`	TBD.

Please include [**MAT302**] in *all* email communication about course-related matters.

Lecture: *Time:* M 1-2pm *Place:* Instructional Building IB 370
W 1-3pm *Place:* Instructional Building IB 379

Tutorial: *Time:* F 10-11am *Place:* Instructional Building IB 360

Textbook

We have a recommended textbook that we will more or less follow through the course. In cases where the material taught is not readily available online, I will try to provide course notes or other online references.

- **Recommended:** Christof Paar and Jan Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners, Springer, 2nd Ed. *Available online via the UofT Libraries!*
- **Reference:** Victor Shoup, A Computational Introduction to Number Theory and Algebra, Available online at http://shoup.net/ntb/ntb-v2.pdf
- **Reference:** Thomas Cormen, Charles Leiserson and Ronald Rivest, Introduction to Algorithms, The MIT Press.

Outline

The course will take students on a journey through the methods of algebra and number theory in cryptography, from Euclid to Zero Knowledge Proofs. A tentative list of topics include:

- Block ciphers and the Advanced Encryption Standard (AES);
- Algebraic and Number-theoretic techniques and algorithms in Cryptography, including methods for primality testing and factoring large numbers;
- Encryption and Digital Signature systems based on RSA, Factoring, Elliptic Curves and Integer Lattices; and
- Zero-Knowledge Proofs.

Pre-requisites for this course are: MAT223H5 Linear Algebra I, MAT224H5 Linear Algebra II, MAT301H5 Groups and Symmetries. *If you have not taken these courses, please contact the instructor.*

Grading Scheme

Item	Worth
Problem Sets (5)	35%
Midterm (1)	20%
Final exam	40%
Class Participation	5%

Assignment Submission

All assigments are due *no later than 1pm* on their due date. All assignments must be submitted in class. If you must be late to a lecture due to circumstances beyond your control, please contact me and (ideally) have another student submit the problem set on your behalf.

However, if you require special consideration for one of your assignments, please follow the "Policy on Special Consideration" given on the `Main Webpage`: hand in your assignment directly to your instructor along with any supporting documentation.

Lateness Policy

All assignments are due *by 1pm* on their due date (always on Mondays). Late assignments will be accepted up to four days after this deadline, with the following penalties.

Submission time	Penalty
by 1pm on Monday	none
by 1pm on Wednesday	-25%
by 10am on Friday	-50%
after 10am on Friday	-100%

Late assignments must be submitted in the beginning of the class (on Wednesdays) or the tutorial (on Fridays), unless you require special consideration (see the section above for details). **Please write the submission time on your assignment if you are submitting late. The late policy is strictly enforced.**

Plagiarism

Plagiarism is a form of academic fraud and is treated very seriously. **The assignments you hand in must not contain anyone else's work or ideas, without proper attribution.** I encourage you to work together on the problem sets. However, the actual writeup of your assignments must be done in isolation from others (and without copying from notes or other sources). This ensures that your solution is truly your own, that you understand the course material, and that your grade reflects your own understanding.

Although the internet is a great resource, I urge you to use it wisely. In particular, I ask you not to search for the problems appearing on the assignments. **The rule of thumb: looking up definitions is OK, looking up solutions is not.**

When using ideas which are not your own, please indicate your source. You will not be penalized for collaborating with someone else, unless: (1) your work is identical to that appearing elsewhere; or (2) you explicitly use an idea without attributing the source. Both (1) and (2) may have serious consequences. See

`http://www.utoronto.ca/writing/plagsep.html`

for further information.

Courtesy: François Pitt, Mark Braverman and Leo Goldmakher.