This sheet summarizes information for the course CSC 2414 F ("Topics in Applied Discrete Mathematics: Lattices in Computer Science") during the Fall session of 2011 on the St. George 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.utoronto.ca/~vinodv/COURSES/CSC2414-F11/`

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	*SF2301B*	`vinodv@cs.toronto.edu`	T 5:10-6:10pm in my office.

Please include [**CSC2414**] in *all* email communication about course-related matters.

Lecture: *Time:* T 3-5 *Place:* Bahen Center BA 4010

Textbook

There is no *required* textbook for this course. Instead, we will use material from the references given in the course web-page.

A *reference* textbook that covers the material in the first few lectures is: "Complexity of Lattice Problems: A Cryptographic Perspective" by Daniele Micciancio and Shafi Goldwasser (Available at the Mathematical Sciences Library and the University of Toronto bookstore).

Outline

This is an advanced graduate course. We will assume knowledge of basic math (linear algebra and probability) and introductory level algorithms (analysis of algorithms, polynomial time and NP-hardness). The following topics will be covered in this course, tentatively in the order listed.

- Introduction to the Theory of Lattices, Preliminaries and Definitions, Gram-Schmidt Orthogonalization, Successive Minima.
- Minkowski's Theorem and Applications.
- Computational Problems on Lattices, the Lenstra-Lenstra-Lovász algorithm for the Shortest Vector Problem.
- Applications of LLL – Small solutions to polynomial equations, Cryptanalysis of special cases of the RSA encryption, Integer Programming.
- Complexity of Lattice Problems, NP-hardness.
- Dual Lattices and the Smoothing Parameter.
- Average-case Hardness of Lattice Problems, Ajtai's Worst-case to Average-case Reduction, Introduction to Lattice-based Cryptography.
- Learning with Errors (LWE), Search and Decisional versions of LWE, Lattice-based Secret-key and Public-key Cryptography
- Fully homomorphic encryption and Applications

Grading Scheme

The workload for this course will be "moderate". Grades will be based on four assignments, scribing notes for 1-2 lectures, and class participation. We will use the following grading scheme.

Item	Weight
Assignments	80%
Lecture Scribing	15%
Class Participation	5%

Class attendance is mandatory, and you are encouraged to ask many questions in class!

Assignment Submission

Assignments:

- All assignments are due *no later than 11:59pm* on their due date.

Scribe notes:

- All scribe notes are due the Thursday after the week of the lecture at 11:59pm (approximately 10 days). For example, the scribe notes for the lecture on September 13 are due on September 22, Thursday.

All assignments and scribe notes should be e-mailed to the instructor. Include "[CSC2414]" in the subject of the e-mail. The submissions should be in pdf. You can find the appropriate Latex style files in the course website.

The primary considerations in grading the scribe notes will be accuracy and clarity. The notes should contain a clear exposition of the material taught in the class. A rule of thumb is: *the lecture notes should be better than the lectures, not worse!* If you have questions about the material, feel free to schedule an appointment with the instructor.

Lateness Policy

You have a quota of *120 "late hours"* for the course (including the problem sets and scribe notes) which you can use at your discretion. For example, you can submit the second problem set 48 hours (2 days) late and the third problem set 72 hours (3 days) late without penalties, but then you can't have any more late submissions.

Collaboration Policy

You are free to discuss the problem sets with others. However, the actual writeup of your assignments must be done in isolation from others (and without copying from notes or other sources!). In addition, you must acknowledge your sources and the discussions in your submission.

Please read the `Guidelines for Avoiding Plagiarism` page for full details of the course policies and the Faculty's rules. If you are having trouble with the course, come speak to me!

Courtesy: François Pitt and Mark Braverman.