COURSE INFORMATION
MATH 3375 (Theory of Cryptology) – Fall 2013

Math 3375 is a mathematical introduction to the theory of cryptography (making secret messages) and cryptanalysis (decrypting secret messages). Mathematically, the course requires basic number theory, probability, counting, and linear algebra. The prerequisite for this course is Math 1271 (Discrete Mathematics).

Time	Class: TTh 8:30-10:00
Place	Class: Ryan Building 2047
Instructor	Adam Van Tuyl
	Office: RB 2015
	Office Hours: TBA
Text	*Cryptological Mathematics* by Robert Edward Lewand
Email	`avantuyl@lakeheadu.ca`
Web Page	`http://flash.lakeheadu.ca/~avantuyl/courses/2013_math3375.html`

Contact Information. The best way to contact me is via email. The class webpage is also a good source of information. I update the webpage after every class.

Outline. Math 3375 is a one semester long course. Our goal is to cover all the material presented in the textbook.

Marking Scheme. The evaluation is composed of four components.

1. Homework (15%) A homework assignment will be given out every Thursday. It will be due the following Thursday at the *beginning* of class. There will be nine homework assignments. The homework assignment with the lowest grade will not be counted. Some of the solutions will be posted on ERES, the electronic reserve of Lakehead Library, once the assignments have been handed in (a link is on the webpage).

Homework questions will be a combination of questions taken from the text book and original questions. Exercises will be marked out of 2 or 4 points, depending upon the level of difficulty.

Questions out of 2 points will be graded as follows:

[2 pts] Near perfect or perfect solution. A near perfect solution is a solution that is correct up to the final stage with possible mistake or sign error at the last step.
[1 pt] The solution shows some of the needed ideas, but fails to have the final solution.
[0 pts] Little or no progress is made toward the solution.

Questions out of 4 points will be graded as follows:

[4 pts] Near perfect or perfect solution. A near perfect solution is a solution that is correct up to the final stage with possible mistake or sign error at the last step.
[3 pts] Most of the needed ideas are present, but misses a key point, or is poorly written.
[2 pt] The solution shows some of the needed ideas, but fails to have the final solution.
[1 pt] One or two initial steps are made.
[0 pts] Little or no progress is made toward the solution.

Further notes on homework:

- Every assignment must contain the course number, the assignment number, your name, and your student ID, and the instructor's name. (Every week, hundreds of math assignments are turned in - make sure your assignment gets to the right person!)
- Homework must **always** be stapled together (no paper-clips, folding the pages, folders, etc. will be accepted). Failure to do this will result in **10 points deducted** from the assignment. (Paper-clipped assignments have the tendency to fall apart; assignments in folders make more work for the grader.)
- Late homework will have **10 points deducted** for every day (the weekend is counted as one day) that is late. Once the solutions have been posted, you may no longer submit an assignment.
- The copying of assignments will result in a mark of 0 for both assignments.
- Homework may be handed in early by either giving it to me or by placing it under my office door. Do **not** bring your assignment to the math office.

2. Tests (1 Midterm, 25%) There will be one midterm. The (provisionally) date of the midterm is:
October 17, 2013 - Midterm 1

3. Presentations (15%) You will have to do a presentation. See the next sheet for more details.

4. Exams (Final Exam 45%) Your final exam will consist of two parts. The first part will be a take home component. You will be given an encrypted text and asked to decrypt it. The second part will be a cumulative final exam. The exact date and further details will be given once the exam schedule is posted.

A friendly piece of advice: do not book your plane ticket home until you are certain about the exam schedule. A flight is not an acceptable excuse for missing an exam.

Class Policies. Attendance is not mandatory; however, it is strongly recommend that you come to class. We will do a lot of hands on examples. I would appreciate the fact that you show up on time if you do decide to come to class. Arriving late disturbs both me and your fellow classmates. Also, please **turn off** your phone while in class, and **no texting**.

Changing Marks. If you disagree and/or have a problem with a particular mark on an assignment or exam, please use the following procedure. First, check your assignment/exam against the solutions. If this does not clear up any problems, on the front of the assignment/exam, please write the question number you want re-graded, and why it should be re-graded. Then hand it back it in. I will then take a look at the assignment/exam and see if the mark needs to be adjusted. If there is simply an addition error with the marks, please hand it back in to me with the correct number at the top.

Exams and tests must be taken on the date assigned, except if there are medical or family emergencies. In these cases, the relevant Lakehead policies need to be followed.

Important Dates.

Sept.9, 2013 - First semester begins
Oct. 14, 2013 - Thanksgiving (No classes)
Oct. 17, 2013 - Midterm 1
Nov. 4, 2013 - Last day to drop without academic penalty
Dec. 19, 21 and 26, 2013 - Presentations
Dec. 2, 2013 - First semester ends
Dec. 5-17, 2013 - Final Exams

OVERVIEW: There are many, many different cryptological methods. As part of this course, you will independently learn about a method not discussed in the textbook and present it to the class.

Either working alone or in pairs, you will give a short presentation and provide a write up on your cryptological method. The presentations will be during the last week of classes. This project will be worth 15% of your final mark (half of the mark will be based on your presentation, and the other other half will be on your write up). The following sheet will guide you through this project.

TOPIC: You must pick a method in cryptology not covered in class. A good place to get your feet wet is the wiki page:

`http://en.wikipedia.org/wiki/Cryptography`

Or you could try the library. Check out journals like the American Mathematical Monthly, the Mathematics Magazine, or the College Math Journal. The last two can be searched at:

`http://www.math.hmc.edu/journals/journalsearch2/`

Find something that interests you. Please note that all methods need to be cleared with me first. When you come to clear the method with me, you must show me what resources (journals, textbooks, web pages, etc.) that you plan to use.

PRESENTATION: You are required to give at most a 10 minute presentation on your topic. Please keep this in mind when picking your topic. Your goal is to explain to the other students in the class the main points of your method. Note that you are not limited to using the chalkboard. If you feel a power-point presentation (or interpretative dance!) would be better, please do so. However, I will need to know about any A/V needs in advance. Presentations will be graded upon your knowledge of the material, your delivery, and your ability to handle questions. As part of your presentation, you will explain how your method would encode a passage from *Pride and Prejudice* (see the appendix).

WRITE UP: You will also be required to write up a summary of your method. This summary should be at most four pages and it is required to be typed (LaTeX is preferred). The write up will be due on the first day of the presentations. Written work will be graded on the mathematical content, as well as the clarity of the exposition. As part of your write up, you will explain how your method would encode a passage from *Pride and Prejudice* (see the appendix).

In your write up, I will expect you to include correct mathematical references. Here are

some samples. The first is for a journal, the second is for a book:

1. A. Van Tuyl, The defining ideal of a set of points in multi-projective space. J. London Math. Soc. (2) **72** (2005), 73–90.

2. R. H. Villarreal, *Monomial algebras.* Marcel Dekker, Inc., New York, 2001.

Web pages are a little bit more complicated. For a complete list of possibilities, see:
`http://www.virtualsalt.com/mla.htm`

TIME-LINE: The following schedule will be used:

> October 17, 2013 – Topic picked, with evidence of references, cleared by me. If you are working in pairs, I need to know who is working with whom.
>
> November 19, 2013 - Write up due
>
> November 19, 21, 26, 2013 – Presentations given.

GRADING: You will be graded on this presentation as follows:

> 10% Topic picked on time, with references.
>
> 45% Write up.
>
> 45% In-class presentation.

You will lose 10% per day for every day you miss a deadline.

APPENDIX: Use the following passage from *Pride and Prejudice* by Jane Austen to illustrate your cryptological method. I will put a "clean" copy on the class webpage. The clean copy will strip out the punctuation.

> It is a truth universally acknowledged, that a single man in possession of a good fortune, must be in want of a wife.
>
> However little known the feelings or views of such a man may be on his first entering a neighbourhood, this truth is so well fixed in the minds of the surrounding families, that he is considered the rightful property of some one or other of their daughters.
>
> "My dear Mr. Bennet," said his lady to him one day, "have you heard that Netherfield Park is let at last?"
>
> Mr. Bennet replied that he had not.