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. Alternatively, you can take one of the methods or algorithms we discussed in class and implement the method in a programming language of your choice.

You can work either alone or in pairs. If you decide to learn about a new cryptographic method, you will provide both a write up and a short presentation. If you decide to write computer code, you will have to submit your code and provide a short presentation on what your code does.

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 or computer code). The following sheet will guide you through this project.

TOPIC: If you decide not to code, 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). If you are doing a computer programming project, you should explain how your code would use this passage as input.

WRITE UP: If you are doing a written project, 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`

CODING: If you are doing a computer project, you will need to send me an electronic copy of your code, as well as some documentation on how your code works. You can use any programming language you wish. (If you are up to the challenge, you can also trying to make an app for your phone!)

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 or code 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 or code.
>
> 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.