Math 115F: Cryptography, Fall 2010
Essay #2 – Expository Paper

In this paper, you'll be asked to explore the origin, use, and (where available) decryption of a particular code or cipher (one not covered in detail in the course) or some other aspect of cryptography with a focus on clear explanations of the mathematics and cryptography involved. All papers will be posted on the course blog, and each student will be asked to read and comment on two of his or her classmates' papers.

We'll spend time looking at some of the more popular and interesting codes and ciphers from history in this course. However, there are many more codes and ciphers we won't have time to explore in detail, as well as other aspects of cryptography on which we'll spend relatively little time. This paper provides you with a chance to explore an area of cryptography on your own—one that interests you personally—and to share that exploration with your classmates.

The focus on explanations is an important part of this paper. If your explanation of something is very clear and effective, then you typically have a solid understanding of the topic. Furthermore, since you'll be sharing your papers with your peers, it is important that they be able to understand your work so that they can expand their understanding of cryptography.

Your paper should be about 5 pages long (typed in 11 or 12 point font, double-spaced), but the amount and type of mathematics and cryptography notation may result in some longer papers. Please ask me if you need help finding ways to represent non-textual content in your paper. You will be graded primarily on the clarity of your explanations. Accuracy, grammar, and presentation will be factored into your grade to a lesser extent. See the rubric for this assignment for more details on my expectations.

A first draft of your paper is due at the start of class on **Thursday, October 28th**. Bring a paper copy, since you'll spend that class session providing feedback on each other's papers. Failure to do so will reduce your grade on this assignment by two letter grades.

Your expository paper will contribute 15% of your overall course grade. The final draft, as an email attachment, please, is due at the start of class on **Tuesday, November 2nd**.

SELECTING A TOPIC

You are encouraged to select a cipher or code for your paper, one not covered in detail in this course. Use the Singh book as your guide here—if the cipher or code is discussed in detail in Singh, then it's off limits for this paper. If it's mentioned briefly or not at all, then it's fair game. I have and will continue to discuss codes and ciphers in class not mentioned in Singh. Once I know your paper topic, I'll make sure to avoid any lengthy discussion of that topic in class until after your paper has been submitted.

You might be interested in focusing on some aspect of cryptography in your paper that isn't strictly a code or cipher. I'm open to other approaches to this paper, however, your idea should have some mathematical, code-making, or code-breaking aspect that you can explain clearly in your paper.

Either way, please let me know your topic by **Thursday, October 21st**. That will give me an opportunity to provide you with feedback on your topic, discussing the feasibility of your proposed paper and suggesting ideas for enhancing your paper.

Where to find topic ideas? Here are some sources:

- Check our course's Delicious feed for ideas.
- The Barr textbook describes a number of codes and ciphers we won't be studying in depth in this course.
- Wikipedia's coverage of cryptography is fairly broad and accurate. You might start with the Wikipedia article on the history of cryptography and look for topic ideas.
- The Vanderbilt Library has a number of books on cryptography.
- *Cryptologia* is an academic journal devoted to cryptography with an emphasis on the history of the subject.

RESPONDING TO OTHER PAPERS

After you submit your paper, I'll post it on the course blog. Each paper will receive its own post, making it easy for you to comment on other students' papers. You'll be asked to select two papers that look interesting to you, read them, and comment on them. Here are some questions you might address in your comments:

- What did you find most interesting about this project?
- What aspect of the topic was most clearly explained and why?
- What questions do you still have about this topic?
- What connections do you see between this topic and other topics in this course?

Your comments must be made by the beginning of class on **Tuesday, November 9th**.

CITING YOUR SOURCES

You must cite your sources appropriately, and a list of references must appear at the end of your paper or embedded in your video. It does not matter which formatting style you use (APA, MLA, etc.), but you should be consistent in your formatting. Be sure to format your citations (footnotes, endnotes, etc.) correctly according to the formatting style you choose. For guidelines on documenting sources, avoiding plagiarism, and other relevant writing topics, please see the Vanderbilt Writing Studio's list of resources for students.

Make clear what references you use and how you use them. Did most of your project come from a single journal article? If so, then there is no need to cite it repeatedly, but you should explain your use of the article clearly in your project and cite direct quotations from the article. Did your project come from a variety of sources? Make it clear what ideas (facts, computations, analysis, etc.) came from which sources through proper citations. That is the spirit of not plagiarizing—making it clear where you obtained your ideas. The Vanderbilt Undergraduate Honor Council's "What Is Plagiarism?" page is another very useful source of information on how to quote and cite your sources.

DEADLINES

October 21st – Topic selection
October 28th – Drafts due
November 2nd – Papers due
November 9th – Comments due