Math 311M Writing Project  
Fall 2011

Groups due by email: **October 25, 2011**  
2-3 page draft due: **November 16, 2011**  
Final version due: **December 2, 2011**

Students will work in groups consisting of \( n \) people, where \( 1 \leq n \leq 4 \). Each group will submit one typed report (approximately 5-6 pages in length, single spaced), including a cover page with project title and names of group members. All the group members will receive the same project grade. Each project should have a list of citations used at the end of the report. Note that Wikipedia is not itself an acceptable source, but can be useful to find other sources.

The group report will be graded out of 75 points. The report should be as self-contained as possible. It should comprise an introduction, a development of the necessary mathematical background (e.g. primitive roots), and a treatment of the main topic. Each part will be graded for mathematical detail and accuracy, clarity of writing and presentation, grammatical correctness, and appropriate use of notation, terminology, examples, etc. A good style guide for level of detail and type of writing is the mathematical part of the textbook.

Make sure to tell me via email who is in your group by October 25 (with Math 311M in the subject). A draft (2-3 pages) is due on November 16. The deadline to submit your completed project is Friday, December 2.

The topic is a more detailed development of public-key cryptography. You should write about the Diffie-Hellman key exchange. First develop any necessary mathematical background. Explain the purpose of the key exchange and how/why the Diffie-Hellman key exchange works. Then give a non-trivial, specific example. Make sure to discuss the strength/security of this method thoroughly: what makes it difficult to decode intercepted messages? Space permitting, you may describe applications (e.g. how Diffie-Hellman fits into a larger system).

Alternative topics are allowed if we discuss it beforehand (by October 25). For example, you might want to write about approaches to breaking encryption by factoring large integers via the number field sieve instead of the Diffie-Hellman key exchange. Another possible topic is how elliptic curves are used in the Diffie-Hellman key exchange. These topics, however, will be much more involved and difficult and will require more background learning on your part.