Course Project Information Sheet

Overview: All students are required to complete a course project; for undergraduate students the project will be completed in groups. Each group or graduate student will choose a different project topic related to cryptography from the list below. The project must be focused on material not discussed in class. Undergraduates will propose group members – there should be 3 groups of 3 members each and 1 group with 4 members for a total of 4 groups. Each project will include both a short written paper and a presentation made to the class. All participants in a group will receive the same grade, so it is important that each person in the group participate fully and equally. You will be graded on correctness, completeness, and creativity. The project will count 15% of your final course grade.

Written Component: Each project must include a written paper. Each group will hand in 1 paper. Your paper should be 4 to 5 pages long (typed using single-spacing with 1 inch margins and 11 point font size with respectable font type). Quality is more important than quantity. Have something to say and say it clearly and concisely. If you are presenting the results of your investigation of some journal article or textbook chapter, you should fill in the missing parts of each argument or proof and do any problems left to the reader. It would be better to go into a small part of some topic in depth and detail, rather than try to cover a large area superficially. This is your opportunity to show that you can read some mathematics on your own and then explain it in writing to your reader. All papers must include a list of references. References should be to either journals or books. You may use the internet to find sources, but references themselves should not be to websites. *Please do not copy any references - appropriately cite these.*

Presentations: You will have 20 minutes to enlighten your colleagues about the topic you have researched. Your presentation should be clear and to the point. Choose your examples carefully to illustrate the points you want to make. In a group presentation, all members in the group should have a role and all should be able to answer any questions which arise. You should rehearse your presentation in advance on some fellow students and leave some time for questions and interruptions. Class presentations always take more time than you think they will. Rehearsal will help you to better gauge how much you can accomplish. *Much effort is invested in course projects – please make every effort to attend all presentations to support your classmates.*

Important Dates: We will adhere to the following deadlines. As stated on the course syllabus, no extensions will be granted for the project papers and presentations will only be rescheduled for unavoidable, documented circumstances.

- By 9:00 a.m. on Friday, February 26 you need to submit the course project proposal.
- By noon on Monday, February 29 the groups, topics, and presentations schedule will be announced and finalized.
- The short project paper is due at the beginning of class on Monday, April 18.
- The graduate presentations will be given in-class on Friday, April 29.
- There will be 1 undergraduate group presentation each class on Monday, May 2 and Wednesday, May 4. There will be 2 undergraduate presentations in-class on Friday, May 6.

The Topics:

- Zero-Knowledge Proofs
- Hash Functions
- Identification Schemes
- DES and AES
- Digital Cash
- Number Field Sieve
- Pseudo-primes (Lucas, Fibonacci, Frobenius test)
- Probabilistic Encryption

Resources: Most of the topics are discussed to some extent in your textbook. You may also want to browse through some books and journals on cryptography. As mentioned above, the internet has many good sites dealing with the above topics and any of the standard search engines should produce helpful sources. However, references themselves should not be to websites.