CSL 866: Cryptography **Date:** January 10, 2011
Instructor: Ragesh Jaiswal

Course Information

Description: Cryptography has a very long history and there are evidences to suggest its existence even around 4000 years back. Classical cryptography deals mainly with secret communication and in fact, the dictionary meaning of cryptography is the art of hiding information. Classical cryptography mainly consisted of an endless "design-break-design" cycle making it more of an art rather than science. In the past few decades, the field has been greatly revolutionized. It has been given a solid mathematical and computational grounding and cryptography has now transitioned into being a scientific discipline. Furthermore, with the advent the internet and digital revolution, the scope of the subject has expanded enormously. No more is cryptography just about secret communication nor is it just restricted to the millitary and intelligence domains. Cryptography now deals with varied issues like authentication, digital signatures, digital cash and much more. It is in use every time you make a payment for a book bought on the internet, login to your machine, set-up a yahoo account, use wifi on your laptop and so many more places.

This course will mainly be about the mathematical and computational foundations on which modern cryptography has been built. We will see how provably secure protocols are constructed using problems that are believed to be computationally hard to solve. We will see how security goals can be formalized and cryptographic protocols can be shown to be provably secure. Some of the topics covered will be private key encryption, hash functions (SHA1, MD5), message authentication (HMAC), pseudorandom permutations (AES, DES), one-way functions, pseudorandom generators, public key encryption (RSA), digital signatures (El Gamal, Rabin), key distribution etc. We will decide on more advanced topics as the course progresses.

Lecture:
Place: IIA 501 (CSE Seminar Room)
Time: Wednesday 1:30-3:00pm and Thursday 3:00-4:30pm.

Office hours: Send email to setup time.

Course Web Page: http://www.cse.iitd.ac.in/∼rjaiswal/csl866/.
The page will contain course information, references, problem sets, and announcements. Please check this page regularly.

Pre-requisites: This course requires knowledge of algorithms and probability theory. Since the course will be theoretical in nature, you should be comfortable with reading/writing mathematical proofs.

Textbook: There is no single textbook that covers all the material intended for this course. I will try to provide pointers to lecture notes and other reference material. Most of them will be available on the internet. However, most of the basic material can be found in:

- *Introduction to Modern Cryptography* by Katz and Lindell.

Requirements, policies and grades: There are no projects in this course. You will be given 4-5 problem sets that are supposed to be solved individually. There will be a Mid-term exam and final exam (that will have a take-home component). The weightage of the problem sets (collectively) will be around 35%. The mid-term exam will have 15% weight and the final exam will have the remaining 50% weightage.

Grading policies: You must write solutions on your own. In case you find material that will help you in solving some problems, you should mention the source in your writeup. Class participation will be taken into account when assigning grades at the end of the course. You will be writing mathematical proofs in this course and the grades will depend on both mathematical clarity and correctness. Links to some nice expositions on mathematical writing will be provided on the course webpage. **Finally, cheating and academic dishonesty cases will be severely punished.**