Spring 2005

CS6260 - **Applied Cryptography**
Syllabus

Time: Tu, Th: 3:05-4:25pm.
Place: CoC 102.
Instructor: Alexandra (Sasha) Boldyreva
Email: aboldyre@cc.gate.... Please include "CS6260" in the subject.
Office hours: Tuesday 4:45-5:45pm, Wednesday 2-3pm, in CoC 254.
TA: Ashok Ponnuswami, pashok@cc

Textbook and notes. There is no required textbook. Lecture notes, slides and additional references are available online and the links are given on the class web page.

Content. This is a 3-credit graduate-level introduction to modern cryptography course. We consider the classical goals of cryptography such as data privacy, authenticity and integrity. Topics include pseudorandom functions and permutations, block ciphers, symmetric encryption schemes, security of symmetric encryption schemes, hash functions, message authentication codes (MACs), security of MACs, PKI, public-key (asymmetric) encryption, digital signatures, security of asymmetric encryption and digital signature schemes. Time permitting, we also study commitment schemes, secret sharing, threshold cryptography, Zero-knowledge proofs.

You will learn how various cryptographic schemes work. But the main objective is more fundamental. The goal is to build the understanding of what "secure" is and how to evaluate and measure security. We try to understand what it means for a cryptographic scheme to be "secure" by studying definitions of security of various primitives. You will learn how to analyze security of a cryptographic scheme and determine whether or not it is secure.

Cryptography is only one part of a much broader area of computer security. There are many topics that are beyond the scope of cryptography and will not be covered in this course, such as viruses, worms, buffer overflow and denial of service attacks, access control, intrusion detection and etc. We do not consider implementation issues. Students interested in these topics are advi sed to take Network Security (CS6262) and Advanced Systems and Network Security (CS8803) courses. Foundations of Cryptography (CS8803) course studies complementary, more theoretical topics of cryptography. Students can take the latter course as well as the Applied Cryptography course in any order.

Prerequisites. No previous knowledge of cryptography is necessary. This course is about applying theory to practical problems, but it is still a theory course. The main requirement is basic "mathematical maturity". You have to be able to read and write mathematical definitions, statements and proofs. I expect that you took basic graduate -level algorithms and complexity theory classes. In particular, you have to know how to measure the running time of an algorithm and understand the notion of reducing one problem to another. You also have to know very basic probability theory. All necessary elements of number theory will be presented in class. No programming will be required. If you have doubts whether you have the right background please come to see me.

Requirements. There will be weekly (and sometimes bi-weekly) homeworks (50%), a midterm (20%) and a final (30%). An approximate day for the midterm is March 1st.

Rules. Georgia Tech and College of Computing academic Honor Code applies. Homeworks are announced in class and are posted on the class web page. You can work on the homeworks individually or in pairs, but you have to write and turn in your own solutions and indicate the name of your collaborator, if any. You cannot search the Internet to find the solutions. Homework solutions should be turned in in class, before the lecture starts, on a due day (usually Thursday). If you are unable to attend a lecture when a homework is due, you can email me a postscript or a PDF file with your solutions before the time of the class. No late homeworks will be accepted. During exams you can use the on-line lecture notes and slides posted on the class web page and your own notes.