Computer Science CS 4/57221 Introduction to Cryptology
Call Numbers 12452 and 12470
SYLLABUS
Fall, 2012

Time and Place: Monday, Wednesday, 12:30 - 1:45 in room 121 MCS aka MSB;

Instructor: Michael Rothstein, 268 MSB, phone 330-672-9065. Email addresses: rothstei at cs.kent.edu . Though the university lists my email address as mrothste at kent.edu, that address will not be checked as frequently, so don't use it if you want a prompt response. (Substitute @ for " at ")

Web address: http://www.cs.kent.edu/ rothstei

Office Hours: Monday 2:00-5:00, Wednesday 2:00-7:00 Thursday 3:15-5:30. Also, you can always send email with questions and/or to set up an appointment. Usual turnaround will be a few hours during the day. Email use is to be preferred over voicemail, which will not be checked as often.

Textbook: Paar, Cristof, and Pelzl, Jan, *Understanding Cryptography*, Springer, 2010, ISBN 978-3-642-04100-6 or 978-3-642-04101-3

Goal of the course The goal of this course is to provide a basic understanding of the concepts and uses of cryptography and cryptanalysis; implementation and design of cryptographic algorithms is full of pitfalls, some of which will become apparent in the course, however, judicious use is relatively straightforward once the basic principles are understood.

Material to be covered We will cover the textbook in order, as far as time allows.

Attendance policy By initiative of the Provost of the University, I have been charged with keeping full attendance records, at least for the first ten weeks of the semester. Though I will not compute these records into your final averages, when I assign letter grades, I will give you a slightly better grade if you have a better attendance record. Notwithstanding the above, if you are absent, there may be material created, either spontaneously or in response to questions, and covered in the classroom; often there will not be any written notes of this material, so it might be a good idea to team up with somebody who keeps good notes to make sure you have all the material covered. Some of this material may show up in an exam.

Read the text. Only general reading assignments will be given. The class will mostly cover material in the same order as the text book, there may be exceptions however. It is the student's responsibility to maintain an awareness of the material in the text that is currently being covered.

Ask the instructor if you are unsure of the text material currently being covered.

The syllabus may be changed during the semester if necesary: changes will be announced in class; they will also show up on the instructor's website.

Class disruptions Disruptions should be kept to a minimum; these include (in increasing order of seriousness):

1. Early departure (if announced and done discreetly: please sit near the door so that as few people as possible notice.)
2. Late arrival
3. Use of electronic devices or other devices which may interfere with your or other student's participation. Laptops are acceptable for taking notes, however, please sit in the last row of the room so that your screen does not distract/block other students.
4. Conversation among students.
5. Aiding and/or abetting these or any other student's disruptive behaviors.

Guidelines pertaining to class disruptions are outlined in Chapter 4 of the University Policy Register in section 4 - 02.2.

Grading: Your grade will be based on one midterm, one final, assorted assigned exercises, and a "class participation grade", based on the number of relevant questions and comments: specially good questions or catching my mistakes get extra points. The weights are:

Class Participation	10%
Midterm (Due Oct 17 at 10 PM)	25%
Final (Due Dec 13 at 10 PM)	25%
Exercises	40%

The final will be comprehensive.

All submissions should be electronic, via email to rothstei at cs.kent.edu (substitute @ for " at ")

Test make-up policy: I will need signed documentation to verify *each* individual absence in order to provide make-ups; only university accepted reasons will be honored.

Grading scale: I will assign number grades during the session and only convert them to letter grades when I turn them in at the end of the session. No decision can be made regarding a converion table until the very last minute due to such imponderables as test difficulty, class attendance and participation, etc. which will influence the grade. However, I guarantee the following, worst case, table:

97-100	will convert into an A
94-96	will convert into at least an A-
91-93	will convert into at least a B+
88-90	will convert into at least a B
85-87	will convert into at least a B-
82-84	will convert into at least a C+
79-81	will convert into at least a C
76-78	will convert into at least a C-
73-75	will convert into at least a D+
66-72	will convert into at least a D

Special accommodations for Students with Disabilities: University policy 3342-3-01.3 requires that students with disabilities be provided reasonable accommodations to ensure their equal access to course content. If you have a documented disability and require accommodations, please contact the instructor at the beginning of the semester to make arrangements for necessary classroom adjustments. Please note, you must first verify your eligibility for these through Student Accessibility Services (contact 330-672-3391 or visit:
http://www.kent.edu/sas for more information on registration procedures).

Registration Requirement: The official registration deadline for this course is September 9, 2012. University policy requires all students to be officially registered in each class they are attending. Students who are not officially registered for a course by published deadlines should not be attending classes and will not receive credit or a grade for the course. Each student must confirm enrollment by checking his/her class schedule (using Student Tools in FlashFast) prior to the deadline indicated. Registration errors must be corrected prior to the deadline.

The last day to withdraw is November 4, 2012.

On cheating, plagiarism and other unethical behavior You are encouraged to discuss class problems with other students but required to work independently of anybody else except the instructors and/or tutor, unless otherwise indicated. Copying other people's work, allowing your work to be copied (even inadvertently!) and plagiarizing work will not be tolerated and will be dealt with according to University regulations, as described in the University policy register on cheating

Notes:

1. By default, the penalty for cheating in this course is an "F" in the course.
2. University regulations require me to notify Student Conduct in case of violations.
3. Cooperation is just as bad as the deed itself: so, deciding which of two is the original is a non-issue: both are equally guilty.