COURSE SYLLABUS: *CS 4/57221 Intro to Cryptology*

Term: Fall 2016
Section: 1
instructor: Michael Rothstein
Kent State University
College of A&S, Dept of Computer Science
Office: 251 Mathematical Sciences Building
Office Phone: 330-672-9023
Office Hours: Monday and Wednesday, 1:30-3:30 or by appointment.
Email: rothstei at cs.kent.edu or mrothste at kent.edu (replace at by @)
Delivery: 100% Web-based, Asynchronous.
Dates: August 29 to December 18 (Including finals week)

Course Information

Course Description This is a course on the modern science of Cryptology; that is, the process of hiding information by converting it, through a reversible process, into something unrecognizable. Of course, only the recipient should be able to reverse the "hiding" or encrypting process.

This course is part of the Security Concentration in Computer Science, and completes one third of the necesary credits of the concentration.

As far as usage in life is concerned, this course will help you to set up cryptosystems in many different environments. This skill is highly employable; from the NSA, to banks, to anybody who needs to encrypt information is looking for people with knowledge in Cryptology.

Course Times and Location This is a fully online, 15 week course. There will be no face-to-face meetings. All assignments have due dates; please refer to the course schedule located within the course.

Prerequisites: C in CS 33001 CS-2 Data Structures.
Knowledge of Python is suggested but not required.

Course Delivery: As mentioned before, This course is 100% online. Materials will be delivered through Blackboard Learn (https://learn.kent.edu). You will be reading the textbook, listening to lectures, doing exercises and submitting them through Blackboard. There will also be homework which will be submitted in the same manner.

Blackboard Discussion Forums will be available for your convenience, or you can submit questions via email.

The course is divided into fourteen units, all of them doable in a week. The first one is introductory; the first two cover chapter one, the remaining twelve cover chapters 2 through thirteen and are two covered in weeks 3 through 14 of term. Week 15 is reserved for review.

On the Email address: rothstei at cs.kent.edu or mrothste at kent.edu ; (Substitute @ for " at "). please do not send mail to both at once; I'll simply get it twice and think it is spam!

Best way to reach me is through email or during my office hours. I recommend you email me directly; you can also use Blackboard email, since that reaches me directly also.

I will try to answer email within 24 hours, but I cannot make any promises; please do not count on an instant response; I may be otherwise occupied. Also, some emails may not allow for a quick answer.

You can always send email with questions and/or to set up an appointment. As mentioned before, I try to answer email within 24 hours, but circumstances may not be in your favor; please be patient. Email use is to be preferred over voice-mail, which will not be checked as often.

Instructor's Web address: http://www.cs.kent.edu/˜rothstei This website will contain a copy of this syllabus.

Please Note: The syllabus may be changed during the semester if necessary: changes will be announced; they will also show up on Blackboard and the instructor's website.

Course Goals: By the end of this course, you will:

1. Know how classical, symmetric and asymmetric cryptography work.
2. Understand the principle behind elliptic curve cryptography.
3. Understand how digital signitarues, message authentication codes and key establsiment work.
4. Understand their weaknesses.

Course Learning Outcomes: By the end of the course, you will be able to:

1. Use cryptography to encode and decode text.
2. Use crytoanalytic techniques to decode text encrypted with classical techniques.
3. Calculate the necesary key length to provide the required security in cryptographic and security applications.
4. Design and implement cryptographic systems.
5. Use hashing applications, digital signature schemes and message authentication codes.
6. Evaluate key distribution protocols.

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

The textbook is available at the University Bookstore, or other bookstores.

Since there will be some programming, I recommend you have a good language and debugging guide handy.

Author's lectures (optional) One of the authors of the textbook (Chris Paar) recorded a series of lectures covering the whole textbook; they are available on youtube.

Textbook website There is a website, set up by the textbook authors, with the powerpoints (although I did edit them), another series of lectures, and exercises and problems. The address is: www.crypto-textbook.com

Technology Requirements and Skills: Students new to Kent State University should review Information Services Technology Viewbook (link available in the Preparing your computer section of the Getting Started in Your Online Course link within the Start Here folder). A personal computer with consistent, reliable Internet access is required:

1. A DSL or cable connection to the Internet; dial-up is not sufficient.
2. Laptop or desktop computer with a minimum of a 2 GHz processor and 2 GB of RAM

You will also need the following software:

1. If using Windows, you need at least Windows 7. Apple Mac computers need at least Mac OSX 10.6 or 10.7.
2. An office suite; LibreOffice is avalable free on the web www.libreoffice.org. Another alternative is Microsoft Office, available free to students. Instructions and information can be found on support.kent.edu.
3. Antivirus for Windows OS, Microsoft Security Essentials OR Antivirus for Mac OS, Sophos
4. A Blackboard Learn compatible browser, such as the latest version of Mozilla Firefox. Blackboard also supports Chrome and Safari. Internet Explorer is NOT a supported browser and should not be used.

Blackboard (Bb) Learn This class will use Blackboard (Bb) Learn, the official learning management system (LMS) used by Kent State University to deliver course materials to university students. ALL course materials and activities will take place in Bb Learn.

In order to login to the online Bb Learn LMS, students will need a Kent State FlashLine User Name ID and password. You can login to Bb Learn either through a student FlashLine account or via a direct link to the login page: https://learn.kent.edu.

For help using the Blackboard (Bb) Learn system use the Bb Learn Tutorials for Students link in the main navigation of your course.

In general, Bb Learn works best using the latest version of most major web browsers, including Firefox (recommended), Chrome, and Safari.

Technology Help Guidelines

1. 30-Minute Rule: When you encounter struggles with technology, give yourself 30 minutes to figure it out. If you cannot, then post a message to the discussion board; your peers may have suggestions to assist you. You are also directed to contact the KSU Helpdesk 24/7. As a last resort, contact me. However, do not expect an immediate reply, and I cannot guarantee that I will be able to help with any and all technology issues.
2. When posting or sending email requesting help with technology issues, whether to the Helpdesk or me, use the following guidelines:
   - (a) Include a descriptive title for the subject field that includes 1) the name of course 2) the issue. Do NOT just simply type Help into the subject field or leave it blank.
   - (b) List the steps or describe the circumstance that preceded the technical issue or error. Include the exact wording of the error message.
   - (c) When possible, always include a screenshot(s) demonstrating the technical issue or error message.
   - (d) Also include what you have already tried to do to remedy the issue (rebooting, trying a different browser, etc.).

Policies and Expectations

Online Attendance Policy

Online courses are conducted on the premise that regular attendance requires students to log into the Bb Learn learning management system (LMS). Attendance is measured both by virtual presence in the online course and student interaction with course learning materials and assignments. Students are expected to check their Kent State e-mail and to log into the system multiple times (at least every other day) during the week.

All actions by students in the Bb Learn LMS can be tracked. At any time during the course, an instructor may generate a report that indicates when and how long individual students have been logged into the LMS, or engaged with any course materials or course tools.

Students who anticipate an absence from the online course due to technical or medical reasons should consult with the instructor individually. An absence due to illness or injury requires verification from a medical professional and should be presented to the instructor.

Communication Policy

1. Email course questions and personal concerns, including grading questions, to me privately using your @kent.edu email. *Do NOT submit posts of a personal nature to the discussion board.*
2. Email will be checked at least twice per day Monday through Friday; Saturday and Sunday, email is checked once per day. During the week, I will respond to all emails within 24 hours; on weekends and holidays, allow up to 48 hours. If there are special circumstances that will delay my response, I will make an announcement to the class. However, special circumstances, specially questions requiring research or thought may cause a delay in the answer.
3. Student Forum/Q&A discussion boards will be checked twice per day Monday through Friday; Saturday and Sunday, these discussion boards will be checked once per day.
4. Another 30 minute rule: If you have difficulty with a concept, mull it over; try to listen to the lecture again; if after thirty minutes you are still having difficulties, please contact the instructor (email or in person). Please do not expect an immediate answer. Maybe It is not as easy as I think either!
5. For questions related to technology, please contact: 330-672-HELP for 24/7 support.

Online Student Conduct

and (N)etiquette. Communicating appropriately in the online classroom can be challenging. In order to minimize this challenge, it is important to remember several points of internet etiquette that will smooth communication for both students and instructors:

1. Read first, Write later. Read the ENTIRE set of posts/comments on a discussion board before posting your reply, in order to prevent repeating commentary or asking questions that have already been answered.
2. Avoid language that may come across as strong or offensive. Language can be easily misinterpreted in written electronic communication. Review email and discussion board posts BEFORE submitting. Humor and sarcasm may be easily misinterpreted by your reader(s). Try to be as matter-of-fact and professional as possible.
3. Follow the language rules of the Internet. Do not write using all capital letters, because it will appear as shouting. Also, the use of emoticons can be helpful when used to convey nonverbal feelings.
4. Consider the privacy of others. Ask permission prior to giving out a classmate's email address or other information.

5. Keep attachments small. If it is necessary to send pictures, change the size to an acceptable 250kb or less (there are several programs you can use to do this such as: Photoshop, Paint, GIMP, and picresize.com).
6. No inappropriate material. Do not forward virus warnings, chain letters, jokes, etc. to classmates or instructors. The sharing of pornographic material is forbidden.

NOTE: The instructor reserves the right to remove posts that are not collegial in nature and/or do not meet the Online Student Conduct and Etiquette guidelines listed above. University Use Of Electronic Email A university-assigned student e-mail account is the official university means of communication with all students at Kent State University. Students are responsible for all information sent to them via their university-assigned e-mail account. If a student chooses to forward information in their university e-mail account, he or she is responsible for all information, including attachments, sent to any other e-mail account. To stay current with university information, students are expected to check their official university e-mail account and other electronic communications on a frequent and consistent basis. Recognizing that some communications may be time-critical, the university recommends that electronic communications be checked minimally twice a week.

Please note: This course will require a lot of extra work; all web courses/distance learning courses require a lot of self discipline to keep on track and a lot of work to keep up. I recommend you devote at least about 10 to 12 hours of weekly work to this course. Of course, if you get behind, these hours will add up, to the point where there will not be enough hours! (For example, if you are carrying 15 hours, that would mean that you need about 48 hours a week of study; if you goof off a couple of weeks, that will add up to a staggering 96 hours! Put another way: that is 8 12-hour days!)

Subject and Units Calendar This course is broken up into 14 units, which correspond to fourteen weeks of class; we will leave one week for slack, catch up, or extra material (there is a new cryptosystem which Google is testing already). The first two units comprise chapter 1, thereafter it is one chapter per week.

The table of subjects and units follows:

Week of	Unit	Source	Material
Aug 29	1	Chapter 1 (first half)	Introduction to Cryptography
Sep 5	2	Chapter 1 (second half)	Historical Ciphers
Sep 12	3	Chapter 2	Stream Ciphers
Sep 19	4	Chapter 3	Data Encryption Standard and Alternatives
Sep 26	5	Chapter 4	Galois Fields and the Advanced Encryption Standard
Oct 3	6	Chapter 5	More about Block Ciphers and Modes of Operation
Oct 10	7	Chapter 6	Introduction to Public-Key Encryption and Essential Theory
Oct 17	8	Chapter 7	The RSA Cryptosystem
Oct 24	9	Chapter 8	Cryptosystems based on the Discrete Logarithm Problem
Oct 31	10	Chapter 9	Elliptic Curve Cryptosystems
Nov 7	11	Chapter 10	Digital Signatures
Nov 14	12	Chapter 11	Hash Functions
Nov 21	13	Chapter 12	Message Authentication Codes (MACs)
Nov 28	14	Chapter 13	Key Establishment
Dec 4	RESERVED		
Dec 11	Final		

Grading: Your grade will be based on periodic exercises, 2 quiz grades, a midterm, and a final. In addition, an estimate grade will be added based upon your activity level on the discussion boards. The weights are:

Discussion estimate grade	10%
Exercises	30%
Quizzes (the total)	10%
Midterm	20%
Final (Finals Week)	30%

All quizzes and exams will be comprehensive. This includes the final.

All quizzes and tests will appear in Blackboard Learn; it will be clear which ones must be answered on the spot and which ones should be answered by a submission; the quizzes will be on the spot, the midterm is in flux (may have a part that is immediate and a part that is submitted) and the final will have to be submitted separately. At any rate, no quizzes or tests will require a lock-down browser or have a time limit. When taking tests in Blackboard, please do not refresh your browser. Also, remember that only the newer Firefox, Chrome or Safari will work.

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 conversion table until the very last minute due to such imponderables as test difficulty, class 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

In my experience, the scale slides downward substantially, and never by less than 3 points. However, I instituted that policy in a semester when everybody ended up averaging more than 90%!

University Policies Students are required to be aware of and follow all general and academic policies established by Kent State University. A list of the general academic policies is listed on the online version of the Kent State University Catalog. Specific policies related to the successful completion of this online course can be located and reviewed in your Blackboard Learn course. University policies are located in the Syllabus, Course Schedule and University Policies folder contained within the START HERE folder in your Blackboard Learn course.

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).

Blackboard Learn accessibility statement:
http://blackboard.com/Platforms/Learn/Resources/Accessibility/WebCT-Accessibility.aspx

Registration Requirement: University policy requires all students to be officially registered in each class they are attending, by the deadline published for the course. The official registration deadlines for this course are September 4 for adding and September 11 for dropping. 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 FlashLine) prior to the deadline indicated. Registration errors must be corrected prior to the deadline.

The last withdrawal date for this course is November 6, 2016.

On cheating, plagiarism and other unethical behavior: Students enrolled in the university, at all its campuses, are to perform their academic work according to standards set by faculty members, departments, schools and colleges of the university; and cheating and plagiarism constitute fraudulent misrepresentation for which no credit can be given and for which appropriate sanctions are warranted and will be applied.

For more information see the Kent State policy on plagiarism in the University policies section of the Getting Started in Your Online Course link within the Start Here folder.

As far as this course is concerned, you are encouraged to discuss class problems with other students but required to work independently of anybody else except the instructors and/or tutor at all times; submissions which look similar, specially with name changes, are specially suspect. 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.

Notes:

1. I have the option of penalizing cheating in this course with 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. This means that if you do not guardyour work, you may be guilty of plagiarism.

Please note: this syllabus and course schedule may be subject to change. Changes will be communicated via email or the Blackboard Learn announcement tool. It is the responsibility of students to check email messages and course announcements to stay current in their online courses.