# CS378 Introduction to Cryptology, Syllabus

## Spring 2016, Tuesday, Thursday 3:30-4:45 PM

## Room 203-RGAN

**Web Site:** http://www.cs.uky.edu/~klapper/cs378-s16.html

**Instructor:** Professor Klapper, 307 Marksbury Building; phone: x7-6743;

e-mail: klapper@cs.uky.edu; web: http://www.cs.uky.edu/~klapper/

**Office Hours:** Tuesday, 1-2; Thursday, 11-12, and by appointment.

**Course Description:** The study of privacy in digital systems. Methods of keeping information secure from classical systems dating from ancient times to modern systems based on modern mathematics. Basic methods of encryption using public key systems, block ciphers, and stream ciphers. The mathematical tools for the design and analysis of such systems. Topics will include classical cryptography, modern methods of public and private key encryption, authentication and digital signatures, hashing, and passwords. Number theory, abstract algebra, combinatorics, and complexity theory necessary for the design and analysis of cryptographic systems.

**Prerequisites:** You are expected to be familiar with the content of CS 275, CS 315 and STA 281. If it has been a while since you took these courses, you are encouraged to review them. Cryptology is a very mathematical subject, depending heavily on combinatorics (from CS275), analysis of algorithms (from CS315), probability (from STA281), number theory (to be learned in CS 378), and abstract algebra (to be learned in CS 378). Substantial time in the course will be spent developing the tools we need from these areas.

**Text:** Introduction to Cryptography with Coding Theory, second edition, by Wade Trappe, Lawrence Washington. Publisher: Prentice Hall. ISBN-10: 0131862391, ISBN-13: 978-0131862395.

**Learning Outcomes:** Successful students will:

1. Learn basic issues of security in communication and computing.
2. Learn basic approaches to solving security problems.
3. Learn mathematical tools for analyzing cryptographic protocols, including the basic number theory.
4. Become familiar  with a variety of protocols for providing security in digital systems.

5. Experience implementing security protocols.

**Exams and Homework:** There will be regular homework; one midterm exam, on March 8; a Programming Project due on April 21; and a comprehensive final exam on May 3 at 3:30PM. Some of the homework may also include short programming tasks. Homework will be due in class on the due date at most 5 minutes after the scheduled start of class. Assignments will be available from the class web site. Late homework will not be accepted without a compelling excuse ("I could not find a parking space" or "aliens ate my cat" are not compelling excuses).

You are strongly encouraged to ask questions by e-mail or come to my office hours for help if you are stuck on the homework problems or have any questions about the material we are covering. No appointment is necessary for my office hours. If you cannot attend my office hours but want to see me in person, make an appointment by e-mail. You will make every reasonable effort to arrive before class begins. Cell phones must be turned off before class starts.

**Grades:** Final course grades will be based on the breakdown: homework: 20%; midterm: 20%; Programming project 10%; final exam: 40%; attendance: 10%. Letter grades will be assigned based on the scale: A: 80-100; B: 65-80; C: 50-65; D: 40-50.

**Approximate Syllabus:**

1. Introduction to cryptography: classical approaches: Chapters 1, 2 (5 classes, January 14-28)
2. Mathematical tools: basic number theory: Chapter 3 (5 classes, February 2-16)
3. Block ciphers - DES and Rijndael: Chapters 4, 5 (3 classes, February 18-25)
4. Midterm exam: March 8
5. Public key cryptography - RSA and discrete log systems: Chapters 6, 7 (5 classes, March 1-24)
6. Hash functions: Chapter 8 (2 classes, March 29-31)
7. Authentication and signature schemes: Chapter 9 (2 classes, April 5-7)
8. Cryptographic protocols: Chapters 12, 13 (3 classes, April 12-19)
9. Error correcting codes: Chapters 18 (3 classes, April 21-28)
10. Final exam: May 3, 3:30-5:30PM

**Academic Integrity:** Per university policy, students shall not plagiarize, cheat, or falsify or misuse academic records. Students are expected to adhere to University policy on cheating and plagiarism in all courses. The minimum penalty for a first offense is a zero on the assignment on which the offense occurred. If the offense is considered severe or the student has other academic offenses on their record, more serious penalties, up to suspension from the university may be imposed.

Plagiarism and cheating are serious breaches of academic conduct. Each

student is advised to become familiar with the various forms of academic dishonesty as explained in the Code of Student Rights and Responsibilities. Complete information can be found at the following website: www.uky.edu/Ombud. A plea of ignorance is not acceptable as a defense against the charge of academic dishonesty. It is important that you review this information as all ideas borrowed from others need to be properly credited.

Part II of *Student Rights and Responsibilities* (available online www.uky.edu/StudentAffairs/Code/part2.html) states that all academic work, written or otherwise, submitted by students to their instructors or other academic supervisors, is expected to be the result of their own thought, research, or self-expression. In cases where students feel unsure about the question of plagiarism involving their own work, they are obliged to consult their instructors on the matter before submission.

When students submit work purporting to be their own, but which in any way borrows ideas, organization, wording or anything else from another source without appropriate acknowledgement of the fact, the students are guilty of plagiarism. Plagiarism includes reproducing someone else's work, whether it be a published article, chapter of a book, a paper from a friend or some file, or something similar to this. Plagiarism also includes the practice of employing or allowing another person to alter or revise the work which a student submits as his/her own, whoever that other person may be.

Students may discuss assignments among themselves or with an instructor or tutor, but when the actual work is done, it must be done by the student, and the student alone. When a student's assignment involves research in outside sources of information, the student must carefully acknowledge exactly what, where and how he/she employed them. If the words of someone else are used, the student must put quotation marks around the passage in question and add an appropriate indication of its origin. Making simple changes while leaving the organization, content and phraseology intact is plagiaristic. However, nothing in these Rules shall apply to those ideas which are so generally and freely circulated as to be a part of the public domain (Section 6.3.1).

Please note: Any assignment you turn in may be submitted to an electronic database to check for plagiarism.

**Accommodations due to disability:** If you have a documented disability that requires academic accommodations, please see me as soon as possible during scheduled office hours. In order to receive accommodations in this course, you must provide me with a Letter of Accommodation from the Disability Resource Center (Room 2, Alumni Gym, 257-2754, email address: jkarnes@email.uky.edu) for coordination of campus disability services available to students with disabilities.

**Excused Absences:** Attendance will only be excused with a compelling excuse. Please do NOT come to class if you have a contagious disease. Your absence will

be excused.

Students need to notify the professor of absences prior to class when possible. S.R. 5.2.4.2 defines the following as acceptable reasons for excused absences: (a) serious illness, (b) illness or death of family member, (c) University-related trips, (d) major religious holidays, and (e) special circumstances found to fit "reasonable cause for nonattendance" by the professor.

Students anticipating an absence for a major religious holiday are responsible for notifying the instructor in writing of anticipated absences due to their observance of such holidays no later than the last day in the semester to add a class. Information regarding dates of major religious holidays may be obtained through the religious liaison, Mr. Jake Karnes (859-257-2754).

Students are expected to withdraw from the class if more than 20% of the classes scheduled for the semester are missed (excused or unexcused) per university policy.

Students may be asked to verify their absences in order for them to be considered excused. Senate Rule 5.2.4.2 states that faculty have the right to request "appropriate verification" when students claim an excused absence because of illness or death in the family. Appropriate notification of absences due to university-related trips is required prior to the absence.