CIS 553 and 753 – Applied Cryptography
Spring 2015

Course Syllabus

Instructor: Xinming Ou, xou@ksu.edu

TA: Sathya Chandran Sundaramurthy

Office Hours: Simon: Friday 3-5 in Nichols 316C
Sathya: TBD in Nichols 127

Course Webpage: http://people.cis.ksu.edu/~xou/crypto15/

Lecture: TU 11:30-12:45 in Nichols 236

Required Textbook: “Cryptography and Network Security” by Forouzan

Prerequisite: CIS 300 and MATH 510. Students should be comfortable writing large programs in a high-level language with minimal guidance. They should be familiar with data structures such as stacks, binary trees, and hash tables. Finally, students should have the mathematical maturity and familiarity with proofs that comes with completing MATH 510.

Objectives: Learn the fundamentals of cryptography, including mathematical background, classical ciphers, DES, AES, RSA, ElGamal, cryptographic hash functions, and basic network security. Students will also learn the weaknesses of each crypto technique.

The following topics will be covered:
- Mathematical background
- Information theory
- Classical ciphers and attacks
- Block and stream ciphers
- DES and AES
- RSA and the Rabin cryptosystem
- Elliptic curve cryptosystem
- Message integrity
- Cryptographic hash functions
- Digital signatures
- Entity authentication
- Key management
- PGP and SSL

Programming Language: Students are welcome to use any programming language of their choosing. However, you must include instructions for how to build and run each of your projects.
Graded Work:
   Exams and quizzes ........................................ (50%)
   Homeworks and programming projects ..........(50%)

All Assignments: Written homework assignments and programming projects will be available on course website. Each assignment will be announced during class or by e-mail. (Course announcements will be sent to your K-State e-mail address.) Late homework assignments and programming projects will not be accepted without authorization. All assignments are to be completed individually.

Graduate and Undergraduate Grading: Students in CIS 553 (undergraduate) and CIS 753 (graduate) will be graded separately throughout the course. CIS 753 students may have to do extra work on assignments, and they will be subject to a different grading rubric from the CIS 553 students.

Course Policies

Prerequisite Policy: This course's prerequisites are CIS 300 and MATH 221, and if you have not taken them, the Engineering College might drop you from this course without notice.

Drop Policy: It is your responsibility to drop the course if you are enrolled but decide not to complete the course --- there are no “automatic” drops due to nonattendance.

Honor System: Kansas State University has an Undergraduate Honor System based on personal integrity which is presumed to be sufficient assurance in academic matters one's work is performed honestly and without unauthorized assistance. Undergraduate students, by registration, acknowledge the jurisdiction of the Undergraduate Honor System. The policies and procedures of the Undergraduate Honor System apply to all full and part-time students enrolled in undergraduate courses on-campus, off-campus, and via distance learning.

A component vital to the Honor System is the inclusion of the Honor Pledge which applies to all assignments, examinations, or other course work undertaken by undergraduate students. The Honor Pledge is implied, whether or not it is stated: “On my honor, as a student, I have neither given nor received unauthorized aid on this academic work.” A grade of XF can result from a breach of academic honesty. An XF would be failure of the course with the X on the transcript indicating failure as a result of a breach of academic honesty.

Academic Honesty: Kansas State University has an Honor System based on personal integrity, which is presumed to be sufficient assurance that, in academic matters, one's work is performed honestly and without unauthorized assistance. Undergraduate and graduate students, by registration, acknowledge the jurisdiction of the Honor System. The policies and procedures of the Honor System apply to all full and part-time students enrolled in undergraduate and graduate courses on-campus, off-campus, and via distance learning. The honor system website can be
reached via the following URL: www.ksu.edu/honor. A component vital to the Honor System is the inclusion of the Honor Pledge which applies to all assignments, examinations, or other course work undertaken by students. The Honor Pledge is implied, whether or not it is stated: "On my honor, as a student, I have neither given nor received unauthorized aid on this academic work." A grade of XF can result from a breach of academic honesty. The F indicates failure in the course; the X indicates the reason is an Honor Pledge violation.

**Attendance Policy:** You are responsible for all material presented in class. If you must be absent, please ask the instructor or a fellow student what was covered. Makeup exams may be considered, but only if you contact the instructor before the class period.

**Collaboration Policy:** Every line of work on all submitted assignments must be your own. If you do discuss details of an assignment with another student, then you should document this in your submission.

**Academic Accommodations for Disabled Students:** Any student with a disability who needs a classroom accommodation, access to technology or other academic assistance in this course should contact Disability Support Services (dss@k-state.edu) and/or the instructor. DSS serves students with a wide range of disabilities including, but not limited to, physical disabilities, sensory impairments, learning disabilities, attention deficit disorder, depression, and anxiety.