COMPSCI 759, Data Security

University of Wisconsin-Milwaukee
Spring, 2019

Class meetings:
Lecture Time: Monday, Wednesday: 5:30–6:45 pm
Classroom: EMS E150

Instructor: Guangwu Xu;
Office: EMS 1239;
Phone: (414) 229-5731;
Email: gxu4uwm@uwm.edu;
Office hours: 1:30pm-3:00pm, Monday, Wednesday. (or by appointment).


Topics: Modern symmetric key cryptography, block ciphers, stream ciphers; cryptographic hash functions; asymmetric key cryptography; network security, operating system security; database security.

Course Outline:
1. Overview; Some probabilities and entropies (weeks 1-2)
2. Symmetric-key ciphers (weeks 2-4)
3. Stream ciphers (week 5)
4. Data integrity and cryptographic hash functions (weeks 6-7)
5. Some basic number theory (week 8)
6. Asymmetric-key ciphers (weeks 9-10)
7. Digital signatures (weeks 10-11)
8. Network security and authentication (weeks 12-14)
9. System security (weeks 14-15)

Assignments: There will be a total of four assignments (three homework assignments and one programming assignment) in the course.
• Homework assignments will involve algorithm analysis and problem solving. These assignments cover material presented in lecture and the readings. They are to be completed individually.

• Programming assignment will involve implementation of some cryptographic routines in C/C++, or Java. Programs should be well designed, and use good coding practice.

• Programming assignment should be submitted to the D2L dropbox. It is due by Midnight CST on the due date.

**Exams:** There will be a midterm test and a comprehensive final exam. They are all close-book. The format of questions will be multiple choice and some longer problems. Exam questions will be based on material covered in the book and/or in lecture.

**Grading:**

• Assignments (4): 9% + 9% + 9% + 9%
• Midterm test: 30%
• Final exam: 34%

**Midterm Test Date:** Monday, March 11.
**Final Exam Date Time:** Monday, May 13, 5:30 – 7:30pm.

**UWM Policies:** Policies for students with disabilities, religious observances, incomplete, academic misconduct, grade appeal procedures, final examination policy, students called to military service, discriminatory conduct, and complaint procedures can be found at
www.uwm.edu/Dept/SecU/SyllabusLinks.pdf