COMP 7120/8120 – Cryptography and Data Security

Instructor:

Kan Yang (kan.yang@memphis.edu, 901-678-3139)

Lectures:

Monday/Wednesday, 2:20 pm - 3:45 pm, Dunn Hall 109

Office Hours:

By appointment only (Please arrange by email 2-3 days in advance)

Course Website:
http://www.cs.memphis.edu/~kanyang/COMP7:8120-sp20.html

Course Description:

This course is an introduction to the basic concepts and mechanisms of applied cryptography and data security. It will cover both cryptographic primitives (symmetric encryption, public encryption, MACs, Digital Signatures, Authenticated Encryption, etc.) to cope with the data confidentiality and data integrity. It also emphasizes on how to apply and implement cryptography in practice. (The content and syllabus are subject to adjustment during the semester.)

Prerequisites: The course is self-contained, however a basic understanding of probability theory and modular arithmetic will be helpful.

Recommended Texts (not mandatory):

- *Introduction to Modern Cryptography* by J. Katz and Y. Lindell. UofM library available.
- *Handbook of Applied Cryptography* by A. Menezes, P. Van Oorschot, S. Vanstone. Free!
- *A Graduate Course in Applied Cryptography* by D. Boneh and V. Shoup. Free!

Evaluation:

Grading: Your final grade will come from the following sources: class attendance (CA), homework assignments (HA), in-class presentations (IP), one in-class exam (IE). Here is the grading formula:

$$Grade = 0.1 * CA + 0.2 * HA + 0.3 * IP + 0.4 * IE$$

Grading Scale: A: 85 – 100, B: 70 – 84, C: 60 – 69, D: 50 – 59, F: 49 and below. **(**Plus/minus grading will be used).

Course Policies:

- **Late Policy:** Without prior request, no late work will be accepted. All late submission maybe accepted at a penalty of 15% per day for no more than THREE days.

- **Testing Policy:** The exam given is closed book/note/laptop/neighbor. But students are allowed to bring one cheat sheet (letter-sized 8.5-by-11) for quick reference. There will NOT be any makeup exams unless there is a documented emergency.
- **Homework Assignment and Project Report Policy:** It is recommended that students use a word processing software (e.g., Word or LaTeX) to type their homework solutions or project report, then submit well-formatted PDF files.

Plagiarism/Cheating Policy:

Plagiarism or cheating behavior in any form is unethical and detrimental to proper education and will not be tolerated. All work submitted by a student (projects, programming assignments, lab assignments, quizzes, tests, etc.) is expected to be a student's own work. The plagiarism is incurred when any part of anybody else's work is passed as your own (no proper credit is listed to the sources in your own work) so the reader is led to believe it is therefore your own effort. Students are allowed and encouraged to discuss with each other and look up resources in the literature (including the internet) on their assignments, but appropriate references must be included for the materials consulted, and appropriate citations made when the material is taken verbatim.

If plagiarism or cheating occurs, the student will receive a failing grade on the assignment and (at the instructor's discretion) a failing grade in the course. The course instructor may also decide to forward the incident to the University Judicial Affairs Office for further disciplinary action. For further information on U of M code of student conduct and academic discipline procedures, please refer to: http://www.people.memphis.edu/~jaffairs/

Your written work may be submitted to Turnitin.com, or a similar electronic detection method, for an evaluation of the originality of your ideas and proper use and attribution of sources. As part of this process, you may be required to submit electronic as well as hard copies of your written work, or be given other instructions to follow. By taking this course, you agree that all assignments may undergo this review process and that the assignment may be included as a source document in Turnitin.com's restricted access database solely for the purpose of detecting plagiarism in such documents. Any assignment not submitted according to the procedures given by the instructor may be penalized or may not be accepted at all.

Topics:

Introduction

- o Introduction to Cryptography and Data Security

Data Confidentiality

- Symmetric Cryptography
  - o One Time Pad and Perfect Secrecy
  - o Stream Cipher
  - o Semantic Security
  - o Block Cipher – The Data Encryption Standard (DES)
  - o Block Cipher – The Advanced Encryption Standard (AES)
  - o How to use Block Cipher (one-time key)
  - o How to use Block Cipher (many-time key)

- Public Key Cryptography
    - Basic Key Exchange
    - Some Number Theory
    - Hard problems and Public Key Encryption
    - Public Key Encryption - RSA
    - Public Key Encryption - ElGamal

Data Integrity

- Message Integrity - Message Authentication Codes
- Collision Resistance and HMAC
- Digital Signature

Data Confidentiality & Integrity

- Authenticated Encryption I
- Authenticated Encryption II

Modern Cryptography

- Cloud Security and Attribute-based Encryption