COM 5335 Network Security Admin

Scott CH Huang

Class Information

- Instructor: Scott C.-H. Huang 黃之浩
- Class Time:
  - Mon 2, Thur 23
- Venue:
  - Delta 210

Prerequisite

- Required
  - Basic C programming.
- Recommended
  - Discrete Mathematics
  - Abstract Algebra
  - Data Structure
  - Algorithms

Course Objectives

- Learning the mathematical background for cryptography.
- Understanding cryptographic techniques and how to use them in a proper way.
- Implementing/Simulating important cryptographic algorithms/protocols.
- Learning the implementation as well as hardware issues of important cryptographic algorithms/protocols.

Textbook/Reference books

- No required textbooks
  - Lecture notes/slides are sufficient.
- Reference books
  - Cryptography and Network Security: Principles and Practices, William Stallings, 4ed
  - Handbook of Applied Cryptography by Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone (Editor), CRC Press, ISBN 0849385237, Available on-line at http://www.cacr.math.uwaterloo.ca/hac/
- Other related research papers.

Assessment

- Written exam 30%, in-class, closed books/notes
- 4 assignments: 10% each
- Research Paper Presentation: 30%

Deadlines (Tentative)

	Overall %	Topic	Deadlines
#1	10%	Big Number	**3/6**
#2	10%	AES	3/27
#3	10%	RSA, ElGamal, & Rabin	4/24
#4	10%	Primality Test & ECC	5/15
Written Exam	30%		**5/25**
Presentation	30%	students choose	5/15~6/9

Academic Dishonesty

- Plagiarism: It is a serious fraud to plagiarize other's work. Suspected plagiarism cases may be handled by the relevant disciplinary body of the university.
- Cheating/Impersonating in the exam: Such cases will be reported to the Academic Regulations and Records Office, and the Disciplinary Procedures in the Code of Student Conduct will be followed.

Late Policy

- Within 72 hrs after the deadline– 10% off per day
- Submission after 72 hrs past the deadline will NOT be accepted.

To Reach Me

- Please send emails to chhuang (at) ee.nthu.edu.tw
- Your email title is suggested to start with [COM5335] .
  - e.g. “[COM5335] Assignment#1 Question.”
- This way I usually reply on the same day, otherwise I may not be able to notice your email and reply quickly because I receive too many emails.