COM 5335 Network Security – Syllabus

Course Description

The course intends to provide a practical, state-of-the-art introduction to network security. This course is basically divided into two parts. Part I covers the basic theory of cryptography. Preliminary knowledge in **abstract algebra** and **number theory**, although not required, will greatly help understand the core ideas of this part much more deeply. Students with such background (usually Math major students) will have the potential to fine-tune these cryptographic algorithms in the future. Part II is very practical. We will view network security from an engineering angle. At least some knowledge in programming (at least one of C/C++, Python, Java, or others) is required, as we will have 4 **programming assignments**.

Part I includes the following topics.

1. Introduction
2. Block and Stream Ciphers
    - DES and RC4
3. Basic Finite Fields
4. Advanced Encryption Standard (AES)
5. Public-Key Cryptography
    - RSA, Rabin, ElGamal
6. Digital Signatures
    - RSA, Rabin, ElGamal, DSA
7. Hash and MAC
8. Elliptic Curve Cryptography
    - EC-ElGamal, ECDSA

Part II includes the following topics.

1. X.509 Certificates, Identification
2. Email security, Web security, SSL/TLS, Malicious Softwares
3. Wireless LAN security, IP security, VPN, Firewalls, Intrusion detection
4. Blockchain and Cryptocurrency

Prerequisites

There are no prerequisites for this course even if this is quite a Math-intense course (especially in Part I). All mathematical tools will be taught in-class. It is possible get good grades even if s/he has no backgrounds in Math (not that easy though! but definitely not impossible). However, we will heavily use many basic results in abstract algebra as well as number theory. Some knowledge about them (even partial knowledge) will not only greatly help you understand the topic in cryptography but will also help you understand other related courses (such as Error-Correcting Codes I & II) at a much deeper level. Apart from mathematical knowledge, basic programming skills are necessary. There will be 4 programming assignments, which contribute to 40% of the total grade.

Textbooks

No required textbooks. Lecture notes and related research papers will be 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/

Assessment

- Midterm 35%, in-class, closed books/notes (*Lots of Math!*)
- 4 assignments: 40% (*You'll have problems if you don't know programming at all!*)
- Final Project: 25%

Final Project

You can choose to do either one of the following tasks:

1. Theoretical studies: Paper reading and theoretical analysis. I will assign topics. Students are required to write a study report as final project. No programming is required.
2. Practical studies: Implementing a programming project related to network security. No theory/Math is required.

Course webpage

On iLMS. http://lms.nthu.edu.tw/