정보보호 개론(Introduction to Information Security)

Spring 2011

Professor: Prof. Kwangjo Kim

 Room 2215@N5

 (042) 350-3550, 010-9414-1386, kkj@kaist.ac.kr

Class Hours and Classroom: 10:30 – 12:00 (Tue, Thu.)

Class Code: CS448

**Class Web Page**: **http://caislab.kaist.ac.kr/lecture/2011/spring/cs448/**

TA: Yi Jae Park

Textbook: Handouts

References:

1. Wade Trappe, Lawrence C. Washington, “[Introduction to Cryptography with Coding Theory](http://www-users.math.umd.edu/~lcw/book.html)”, 2nd Ed, 2005, Prentice Hall ISBN 0-13-186239-1
2. Richard A. Mollin, “[An Introduction to Cryptography](http://math.ucalgary.ca/~ramollin/cryptopref.html)”, Chapman & Hall/CRC, 2001, ISBN 1-58488-127-5
3. Mark Stamp, “[Information Security: Principles and Practices](http://as.wiley.com/WileyCDA/WileyTitle/productCd-0471738484.html)”, ISBN:978-0-471-73848-0, 2005 Oct. Wiley International(한국어 “정보보안 이론과 실제”, 안태남 등 번역), and others*.*

Grading Policy: Midterm (35%), Final (35%), Quiz (10%), HW (10%), Attendance (10%)

Objective:

*This course introduces the fundamental understanding on information security to build for any secure system covering the design and breaking of classical, symmetric and asymmetric cryptosystem with mathematical background. We also deal with the cryptographic protocols and their applications to authentication and identification. After finishing this class, the students are expected to understand the broad spectrum on information security and cryptography to advance their challenging research.*Course Schedule

|  |  |  |
| --- | --- | --- |
| Week | Topic | Remark |
| 1 | Introduction I  | 2/8, 2/10  |
| 2 | Introduction II, Basic Terms |  2/15, 2/17 |
| 3 | Classical Ciphers I, II | 2/22, 2/24, Quiz#1 |
| 4 | Block Cipher, DES  | 3/1(off) , 3/3  |
| 5 | AES  | 3/8, 3/10 |
| 6 | Mode of Operation | 3/15, 3/17  |
| 7 | Cryptanalysis of Block Cipher, Summary I | 3/22, 3/25 Programming HW #1 |
| 8 | Mid-term Exam | 3/29, 3/31(off) |
| 9 | Public Key Cryptosystem, Number Theory | 4/5, 4/7 |
| 10 | Digital Signatures | 4/12, 4/14, Quiz#2 |
| 11 | Hash Functions | 4/19, 4/21 |
| 12 | Cryptographic Protocol  | 4/26, 4/28  |
| 13 | Secret Sharing Protocol  | 5/3, 5/5 (off) |
| 14 | Identification Protocol  | 5/10(off), 5/12 |
| 15 | Special talk, Summary II | 5/17, 5/19 Programming HW #2 |
| 16 | Final Exam | 5/24, 5/26(off) |

\* Schedule can be subject to change slightly.