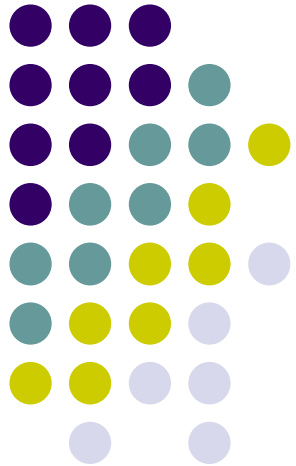
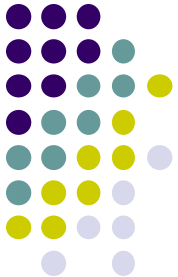
컴퓨터공학특론1:
Course Orientation



Instructor:
Sangwon Hyun (현상원)



Assistant Professor in Department of Computer Engineering, Myongji University

- Education
  - ✓ Ph.D. in Computer Science, North Carolina State Univ.
- Experiences
  - ✓ Assistant Professor, Myongji University (Sep. 2019 ~)
  - ✓ Assistant Professor, Chosun University
  - ✓ Senior researcher, Samsung DMC Research
  - ✓ Senior researcher, Samsung Advanced Institute of Technology
- Research interests:
  - ✓ Network security, applied crypto
  - ✓ Mobile security
  - ✓ Software forensic analysis

Office: Room 5737
Office hours: 10~11:50am Tuesday
Email: shyun@mju.ac.kr

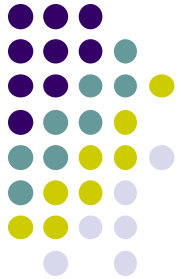
Please include [컴공특론1] in the subject of your e-mail

Course Information

- Course title: 컴퓨터공학특론1
  - Overview of information security
  - In-depth study of cryptography
    - Symmetric key crypto, public key crypto, cryptographic hash algorithm etc.
  - Time: Tuesday 13:00~15:50

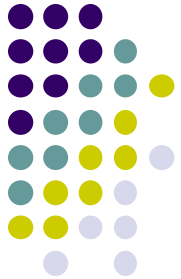
- PPT slides written in English

Intended audience



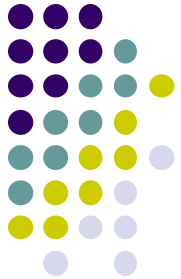
- 4th year undergraduate students who
  - are interested in information security
  - want to gain in-depth knowledge in information security

Prerequisite



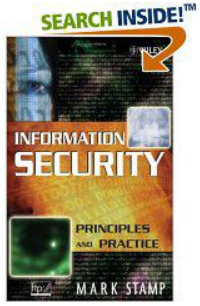
- Students should
  - have taken basic courses in computer engineering
    - e.g., Data Structures, Algorithm, Computer Network, etc.
  - be familiar with C programming
  - SW development experiences in Linux is also preferred.

Reference



- Mark Stamp, Information Security: Principles and Practice – 2nd edition, Wiley
- W. Stallings, Cryptography and Network Security, Pearson
- Charlie Kaufman, Radia Perlman, and Mike Speciner. Network Security: Private Communication in a Public World, 2nd edition. Prentice Hall

Textbook

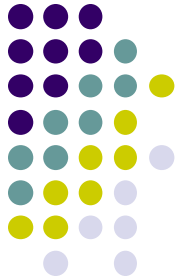


Information Security: Principles and Practice

- Introduction
- Chapter 1
- Cryto
  - Chapter 2: Crypto Basics
  - Chapter 3: Symmetric Key Crypto
  - Chapter 4: Public Key Crypto
  - Chapter 5: Hash Functions and Other Topics
  - Chapter 6: Advanced Cryptanalysis
- Access Control
  - Chapter 7: Authentication
  - Chapter 8: Authorization
- Protocol
  - Chapter 9: Simple Authentication Protocols
  - Chapter 10: Real-World Security Protocols
- Software
  - Chapter 11: Software Flaws and Malware
  - Chapter 12: Insecurity in Software
  - Chapter 13: Operating Systems and Security

번역서: *정보보안 이론과 실제, 안태남, 손용락, 이광석 역, 한빛출판*

Class schedule 1st

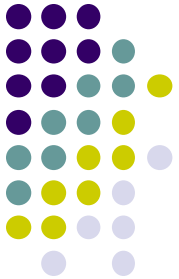


Week	Topic
1	Course orientation & Introduction to information security
2	Cryptographic basics: classical cryptographic algorithms, key concepts for information hiding
3	Major categories of cryptography
4	Typical threat model assumed in cryptanalysis
5	Symmetric key crypto: stream ciphers, A5/1, RC4
6	Symmetric key crypto: block ciphers, DES, 3DES, AES
7	Symmetric key crypto: modes of operations, ECB, CBC, CTR
8	Mid term exam

Class schedule 2nd

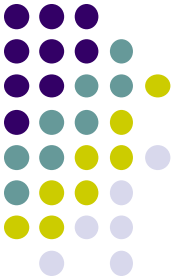
Week	Topic
9	Number theory basics
10	Public key crypto: Knapsack crypto
11	Public key crypto: RSA, Diffie-Hellman key exchange algorithm
12	Public key crypto: Elliptic curve crypto, ECDH
13	Cryptographic hash: major requirements, birthday problem
14	Cryptographic hash: MD5, SHA
15	Final term exam

Evaluation



- Attendance (10%)
  - Three times of late = one absence
  - "성적은 수업일수 5분의 4 이상을 출석한 자에 한하여 인정한다" (수업 일수는 학기당 15주 이상)
- Mid term exam (40%)
- Final term exam (40%)
- Assignments (10%)

Evaluation- Assignments



- 3~4 assignments for each major subject
- 1~2 programming assignments
- No late submission!!

Questions?