Teknis Perkuliahan

Kriptografi [INF1.62.4002]

Universitas Negeri Padang (UNP)

Dosen Pengampu:

Dr. Sandi Rahmadika, M.T., M.Eng.

Profil Dosen

Academic Background

- **2017.9 – 2021.8 (Ph.D.) – Pukyong National University (PKNU), South Korea**
  Dept. of Information Security, Graduate School
- **2015 – 2016 (Master of Engineering) – Pukyong National University (PKNU), South Korea**
  Dept. of Information Security, Graduate School
  *(*Double degree program between PKNU & ITB)*
- **2014 – 2016 (Master Degree) – Institut Teknologi Bandung (ITB), Indonesia**
  Dept. of Information Security, Graduate School
  *(*Double degree program between PKNU & ITB)*
- **2009 – 2013 (Bachelor Degree) – Universitas Bengkulu (UNIB), Indoensia**
  Electrical Engineering – Instrumentation and Control

Dr. Sandi Rahmadika, M.T., M.Eng.

Phone / WA : +82 10 6717 7551
Email : sandika@pukyong.ac.kr
ndiikaa@gmail.com

Current Affiliation

- **Postdoctoral Researcher**
  Soonchunyang University and Wonkwang University, South Korea
- **Lecturer**
  Padang State University, Indoensia

Prerequisites

Quick Recall …

- Basic Number Theory
- Computer Networks
- Algorithms / Data Structures / Complexity
- Basic Probability Theory

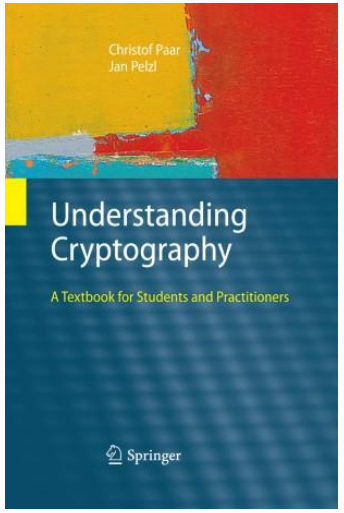
However, you don't need to be scared, because you are able to understand through this lecture even you are beginners at those areas

Class Information

- Days: Monday
- Time: 15.00 – 17.10 WIB
- Places: *Tentative (online and offline class)
- Lecture Processing Format
  - Introduction Slides (by Instructor)
  - Interaction
- Browse the course materials in Website: Portal UNP
  - Check it regularly
  - All news and lecture nodes (in PDF) will be there

Course Contents for Readings

Springer Link Search Menu



© 2010

Understanding Cryptography

A Textbook for Students and Practitioners

Authors (view affiliations)

Christof Paar, Jan Pelzl

This book is uniquely designed for students of engineering and applied computer science, and engineering practitioners

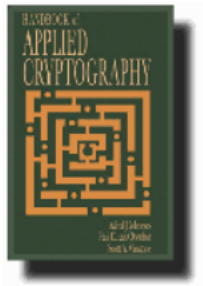
Authors' website (http://www.crypto-textbook.com/) provides extensive notes, slides, video lectures

Authors' YouTube channel (https://www.youtube.com/channel/UC1usFRN4LCMcfIV7UjHNuQg) includes video lectures

Includes supplementary material: sn.pub/extras

Textbook

384 Citations 47 Mentions 1.8m Downloads



Handbook of APPLIED CRYPTOGRAPHY

Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone

CRC Press
ISBN: 0-8493-8523-7
October 1996, 816 pages

Fifth Printing (August 2001)

The Handbook was reprinted (5th printing) in August 2001. The publisher made all the various minor changes and updates we submitted. You can identify the 5th printing of the book by looking for "5 6 7 8 9 0" at the bottom of the page that includes the ISBN number.

You can order the handbook today from any one of these online bookstores:

- Amazon Books (amazon.com) (Price as of May 9, 2016: US $**84.10**).
- Amazon.ca (for Canadian orders) (Price as of May 9, 2016: Cdn $**118.22**).
- CRC Press (Price as of May 9, 2016: US $**97.95**).

- Cryptography fabulous resource.
  All chapters available for download at:

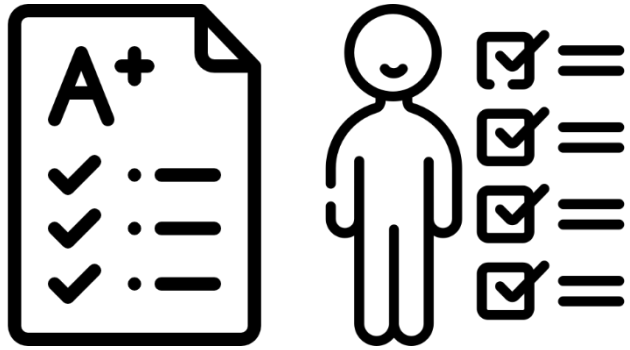
  https://cacr.uwaterloo.ca/hac/

Overall Contents

1. Overview of Cryptography
2. Streamchiphers
3. DES and Alternatives
4. AES
5. More about Block Ciphers
6. Intro to Public Key Crypto
7. RSA
8. Discrete Logarithm based Crypto
9. Elliptic Curve Cryptos
10. Digital Signatures
11. Hash Functions
12. Message Authentication Codes (MACs)
13. Key Establishment

Course Grading

- Absensi : 10%
- Tugas & Quiz : 20%
- Ujian Tengah Semester (UTS) : 30%
- Ujian Akhir Semester (UAS) : 40%



Remarks:

- I might curve (relative evaluation)
- I might assign grades of B and below …

… also

- You might even have fun
- Everybody will make mistakes
- I want your feedback!
- Please ask lots of discussions and questions
- *You are being used as “guinea pigs”*

Focus of the Class

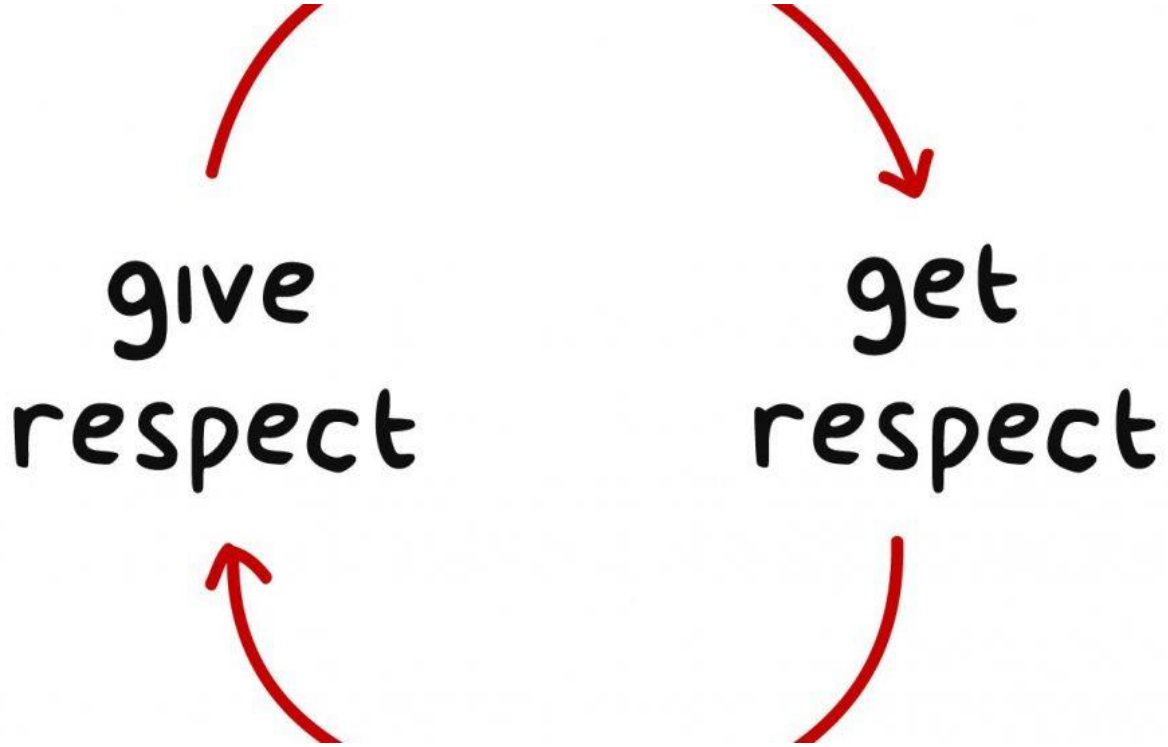
- Recognize basic cryptography
- Learn basic mathematical backgrounds for cryptographic primitives
- Appreciate how much remains to be learned after this course

Remarks:

- You will (I hope) be interested to study further in cryptography and information security

Teknis Perkuliahan (selected …)

- Semua aturan Tata tertib yang termaktub di peraturan akademik
- Total Pertemuan : **~16 x pertemuan**
  - Kehadiran minimal 75% dari seluruh tatap muka
  - Toleransi keterlambatan 15 menit
  - Bertingkah laku baik dan sopan
- Menggunakan dua Bahasa: **Indonesia dan English**
- Makul ini bersifat *"Weekly Course"* - Cek *E-Learning*
- Aturan lain yang diperlukan bagi terciptanya suasana kelas yang kondusif dapat ditentukan kemudian


give
respect
get
respect

Thank You!

Questions?

✉ sandika@pukyong.ac.kr