GSIS
Graduate School of Information Sciences,
TOHOKU University
東北大学 大学院情報科学研究科
Graduate School of Information Sciences.TOHOKU University

specialty choice | subject choice | top page

Syllabus 2017 System Information Sciences

Cryptology

Japanese

Basic information

held this year:	yes
instructor(s)	Hiroki SHIZUYA, Masao SAKAI, Shuji ISOBE
room	206 Lecuture Hall, GSIS building
schedule	The latter period (Thursday) 10:30-12:00
begins on:	10/05

Objectives and outline

The purpose of this class is to overview the fundamental theory of cryptography and information security.
We first study some preliminary theory including the elementary number theory, algebra and computational complexity.
After that, we study the main topics of this class: that includes number-theoretic public-key cryptographic schemes such as RSA and Diffie-Hellman's key exchange, and zero-knowledge proofs.

Class plan

1. Course Overview
2. Introduction to Cryptology
3. Algebra (1) (Fundamentals of algebraic structure)
4. Algebra (2) (Fundamentals of algebraic structure)
5. Algebra (3) (Elementary Number theory)
6. Algebra (4) (Some Cryptographic Primitive Problems)
7. Public-Key Cryptography: Discrete Logarithm-Based Schemes (1)
8. Public-Key Cryptography: Discrete Logarithm-Based Schemes (2)
9. Public-Key Cryptography: Factoring-Based Schemes (1)
10. Public-Key Cryptography: Factoring-Based Schemes (2)
11. Security Notions
12. Zero-Knowledge Proofs
13. Current Topics on Information Security (1)
14. Current Topics on Information Security (2)
15. Term Paper Assignments

Evaluation

The course grade will be evaluated by the term paper.
Attendance records will not be taken into consideration.

Textbook(s)

There is no specific textbook for the class.
Literatures strongly related to this course will be introduced at the first lecture.
Some handouts on selected subjects will be provided.

Web site

Office hours

Although regular office hour are not arranged, you can send e-mail to the specified address for your question.
Visit by appointment is possible. The e-mail address will be given at the first lecture.

Other information

↑Top

Copyright (C) 2005-2007 Graduate School of Information Sciences, Tohoku University. All rights reserved.