Discrete Mathematics

Syllabus Number 3C221

Special Subjects
Elective 2 credit

MORI, Takuo

1. Course Description

In the modern information society, the information security technique is one of the indispensable techniques. Cryptography is the basis of the information security technique.

This course aims at understanding the RSA cryptosystem, which is the first public key cryptosystem in the world, and learning the basis of number theory and abstract algebra, which are the fundamentals of the RSA cryptosystem. This course aims at not only understanding mathematical theorems through their proofs, but also understanding them as algorithms or programs. To that end, this course aims at understanding them from the algorithmic point of view.

To describe algorithms, we use the Ruby language, by which large integers used in the cryptography can be easily managed.

This course relates to the diploma policy DP3, DP4C and DP4M.

2. Course Objectives

The goal of this class is that students master the following abilities;

Students can read and execute programs written by ruby.
Students can write programs of simple algorithms by ruby.
Students can explain the Euclidean algorithm and the extended Euclidean algorithm.
Students can explain the definition and the fundamental property of prime numbers, and explain the relation between prime numbers and pseudoprimes.
Students can implement algorithms of basic factorization and primality tests.
Students can explain the definition of modular arithmetics and calculate four arithmetics operations including remainder operation and power residue operation with respect to modular arithmetics.
Students can explain the Chinese Remainder theorem, solve basic systems of linear congruences.
Students can explain the definition and basic property of Groups, subgroups and cyclic subgroups.
Students can explain the process of key generation, encryption and decryption of the RSA cryptosystem.

3. Grading Policy

Grading policy: Midterm report(50%), Examination(50%).

The way of feedback: Answers for questions or feedback for the contents of class, worksheets, and examination will be given in a class, through LMS or in office hours.

4. Textbook and Reference

Textbook
S. C. コウチーニョ 著、林彬訳　暗号の数学的基礎　丸善出版、ISBN- 13: 978- 4621062869
S.C. Coutinho　The Mathematics of Ciphers: Number Theory and RSA Cryptography　A K Peters/CRC Press, ISBN-13: 978-0367447601
Reference
五十嵐邦明、松岡 浩平著　ゼロからわかる Ruby 超入門 (かんたんIT基礎講座)　技術評論社、ISBN- 13: 978-4297101237

5. Requirements(Assignments)

Before each class, materials related to the class will be published through LMS. Students should download them to their own devices or print them to make it possible to refer to or to taking notes.
Students should read these materials and grasp what they do not understand and they understand in an hour.
After each class, student should review the class through tests on the LMS in half an hour.

6. Note

Students can hardly earn credits not submitting the mid-term report. Thus, it is expected students to observe the deadline.
As for the self-learning support students are expected to utilize materials, such as slides, handouts and quizzes on the LMS.
In each class, students should concentrate on not taking notes but understanding explanations and solving exercises.
Before taking this course, students should take the following courses;
Mathematical Logic, Programming 1, Linear Algebra, Programming 2 and Exercises in Programming 1

At the same semester with this course, students should take take the following courses;
Computer Science Programming 1, Exercises in Programming 2 and Data Structure and Algorithms.

After taking this course, students should take the following courses;
Information Theory and Information Security.

7. Schedule

[1] Introduction, Cryptography, Ruby

[2] Fundamental Algorithms
[3] Unique Factorization
[4] Prime Numbers
[5] Modular Arithmetic
[6] Induction and Felmat
[7] Pseudoprimes
[8] Systems of Congruences
[9] Groups
[10] Cyclic Subgroups
[11] Mersenne and Felmat
[12] Primality Tests
[13] Primality Tests and Primitive Roots
[14] The RSA Cryptosystem
[15] Summary and Examination