# Information Security

MORI, Takuo

### 1. Course Description

Information security techniques are becoming one of the indispensable techniques and are much more important as an infrastructure of networked societies.

The term "information security" covers very broad fields, from foundational theories such as elementary number theory, algebraic systems, cryptography, and computer science to cryptographic protocols or network protocols in general. In this course, we mainly deal with the latter fields.

Students acquire skills related to the diplomatic policy 2 and 3 of Department of Information Science Correspondence Course.

### 2. Course Objectives

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

Students can explain the basics of elemental number theory and abstract algebraic systems which construct public key crypto systems and explain the meanings of mathematical expression used in the public key crypto systems.
Students can explain the basic features of secret key or public key crypto systems, block cipher modes of operation and Hash functions, and can process encryption/decryption as for basic crypto systems.
Students can explain the purpose and summaries of information security, cryptographic protocols and network protocols, and explain or execute the processes of basic protocols.
Students can classify malware which is one of the factors of the illegal accesses, and explain the countermeasures against illegal accesses.
Students can explain the summaries, the purposes and the problems of identification, biometric identification.
Students can explain the security evaluation and its standardization.

### 3. Grading Policy

Grading policy:
Examination(100%).

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

### 4. Textbook and Reference

Textbook
宮地充子,菊池浩明編著　IT Text 情報セキュリティ　オーム社、ISBN-13: 978-4274132841

### 5. Requirements(Assignments)

In order to earn credits of this course, students must submit two reports and get 60% points for each report before taking an examination.

Before taking this course, students should take the following courses;
Mathematical Logic, Discrete Mathematics, Computer Networks and Introduction to the theory of automata and computation.

At the same semester with this course, students should take the following courses;
Information Theory, Information Systems and Operating System.

After taking this source, students should take all the courses related to digital communications.

### 6. Note

### 7. Schedule

| | |
|---|---|
| [1] | Information security, introduction to the information security, threats against information security, countermeasures against threats, cipher systems |
| [2] | Secret key cryptography, cipher systems, block/stream cipher, the evaluation of ciphers. |
| [3] | Basic theory of Public key cryptography, digital signature |
| [4] | Basic theory of Public key cryptography, digital signature 2, cryptographic primitives, a public key cryptography based on the factoring problem. |
| [5] | Public key cryptography/Digital Signature |
| [6] | Public key cryptography/Digital Signature, signature schemes with a hash function, signature schemes without a hash function, secret sharing schemes |
| [7] | Cryptographic Protocols, multi-party protocol, distributed decryption of RSA, group-signature and multi-signature. |