## Course Information

**Course Name:** Special Topic on Implementation (I)

**Course Code:** EE3900-00

**Instructor:** Kenjiro Kato

**Office:** 310

**Contact Information:**

### Topics

1. Software implementation of a private key cryptosystem
2. Implementation of a computer cluster
3. Mathematical analysis of pseudorandom sequences

### Special Topic Types

- [ ] Component Design
- [ ] Circuit Design
- [x] Software Design
- [ ] System Implementation
- [ ] Measurement Experiment
- [ ] System Operation and Analysis
- [ ] Other (In Project 2, assemble and examine a PC cluster system)

### Number of Participants

- Minimum 2
- Maximum 3

### Background Knowledge or Recommended Courses

- Probability
- Discrete Math
- Programming

### Synopsis

1. **Basics:**
   - Private key and Public key cryptosystems
   - Block cipher and Stream cipher
   - Software implementation of a private key cryptosystem
   - Evaluation of the system

2. **Basics:**
   - Cluster computing
   - SCore and Linux
   - Implementation of a computer cluster by SCore.
   - Evaluation of the system

3. **Basics:**
   - Pseudorandom number sequences and Linear Feedback Shift Registers
   - Randomness Test by NIST standards

### Expected Outcomes

1. **Basics:**
   - Understand a framework of private key cryptosystems
   - Understand how to use and evaluate a private key cryptosystem

2. **Basics:**
   - Understand cluster computing/parallel computing
   - Understand how to operate a cluster system

3. **Basics:**
   - Understand the design methods of pseudo-random number generators.
   - Understand how to evaluate pseudorandom numbers