修士課程科目でのシラバス情報例： Electrical Engineering & Computer Science、 MIT School of Engineering から

MIT では、学士・修士・博士共通の電子シラバスシステム (WebSIS) に掲示されたシラバス概要に加えて、各科目ごとに詳細シラバスが提供されている。基本的に詳細シラバスは Web に掲載されている。(URL が付記されており、殆どの場合外部から自由に参照可能である。)
以下に、修士向けの科目での具体例を示す。
なお、科目番号については、仮想の番号としてある。

トップページには、各必要項目ページへのリンクを置き、簡素化

(1) X.XXX Network and Computer Security

General Information
Lectures and Handouts
Calendar
Term Projects
References
Mail Archive
Anonymous Feedback
Textbook Errata
Previous Years

News

Please provide feedback on the course!

Quiz 2 Solutions [PDF, PS] are available.

Homework templates: LaTeX Microsoft Word

X.XXX Course Announcement -
Tuesdays and Thursdays, 2:30 - 4:00
Room 6-NNN
3-0-9

This is an upper-level undergraduate, first-year graduate course on network and computer security. It fits within the Computer Systems and Architecture Engineering Concentration. Topics covered include (but are not limited to) the following:

- Techniques for achieving security in multi-user computer systems and distributed computer systems
- Cryptography: secret-key, public-key, digital signatures
- Authentication and identification schemes
- Intrusion detection: viruses
- Formal models of computer security
- Secure operating systems
- Software protection
- Security of electronic mail and the World Wide Web
- Electronic commerce: payment protocols, electronic cash
- Firewalls
- Risk assessment

Underground Review (available with MIT Personal Certificates only): 2002 2001 1999 1998 1997 1996

前提科目

Prerequisites
X.XXY and X.XYZ. Limited Enrollment.

講義スタッフの情報

Staff

Lecturer

Mr.AAA aaa@xxx.yyy.mit.edu Bill no. Extention no.

Course Secretary

Mr. BBB bbb@xxx.yyy.mit.edu Bill no. Extention no.

Teaching Assistants

Mr. CCC ccc@yyy.mit.edu Bill no. Extention no

Mr. DDD ddd@yyy.mit.edu Bill no. Extention no023

TA のオフィスアワー

Course staff mailing list: *X.XXX-staff@mit.edu*
Use this mailing list to contact the X.XXX staff members.
TA Office Hours

Mr CCC Wednesday, 3-5pm, in Bill no. xxx

Mr. DDD Tuesdays, 10:15-12:00noon, in **Bill no. yyy** (note new location)

X.XXX Lectures and Handouts

Below are links to material relevant to our lectures. Students are responsible for knowing the contents of the assigned reading, the handouts, the lecture notes, and any other items that are starred. In contrast, related readings are provided for your own interest, and are optional.
To suggest the addition of a hyperlink or paper, email *6.857-staff@mit.edu*

以下、毎回の講義で渡される資料と、読むべき教科書、参考資料のリスト

Lecture 01 (Th 9/04/2003): Introduction

- **Handouts:**
  - Handout 01: (Course information) [PDF, PS]
  - Handout 02: ("Why Johnny Can't Encrypt"/Whitten) [PDF, PS, HTML]
  - Handout 03: (Cookies/Fu): [PDF, PS]
  - Handout 04: ("Analysis of an Electronic Voting System"): [PDF]

Lecture 02 (Tu 9/9/2003): User Authentication Overview, Passwords, Hashing

- **Handouts:** None today
- **Reading:** Section 10.3 of the textbook
- **Lecture Notes:**
  - Lecture 02 notes from Fall 2002: [PDF, PS]
  - Lecture 04 notes from Fall 2001: [PDF, PS]
- **Related (Optional) Reading:**
  - Menezes et al. *Handbook of Applied Cryptography*, pages 321--327. [hash functions and MACs]
  - "Risks of Passwords" by Peter Neumann. Page 126, Communications of the ACM, April 1994, Vol 37, No. 4. [MIT-only pdf]
  - "User Authentication Scheme Not Requiring Secrecy in the Computer" Arthur Evans, Jr., William Kantrowitz, and Edwin Weiss. pages 437--442, Communications of the ACM, August 1874, Vol 17, Number 8. [MIT-only pdf]
  - FIPS Standard for Password Usage
- **Related (Optional) Links:**
  - Web Cookies: Not Just a Privacy Risk [HTML, MIT-only PDF]

第 2 回講義での、参考資料のリスト。毎回指定。

Lecture 03 (Th 9/11/2003): Hash Functions

- **Handouts:**
  - Handout 05: Problem Set 1 [PDF, PS]
- **Related (Optional) Reading:**
  - SHA-1
  - Collision in part of MD5 (the compression function)
  - Tripwire
  - HMAC
  - A file system using Merkle's hash trees for integrity

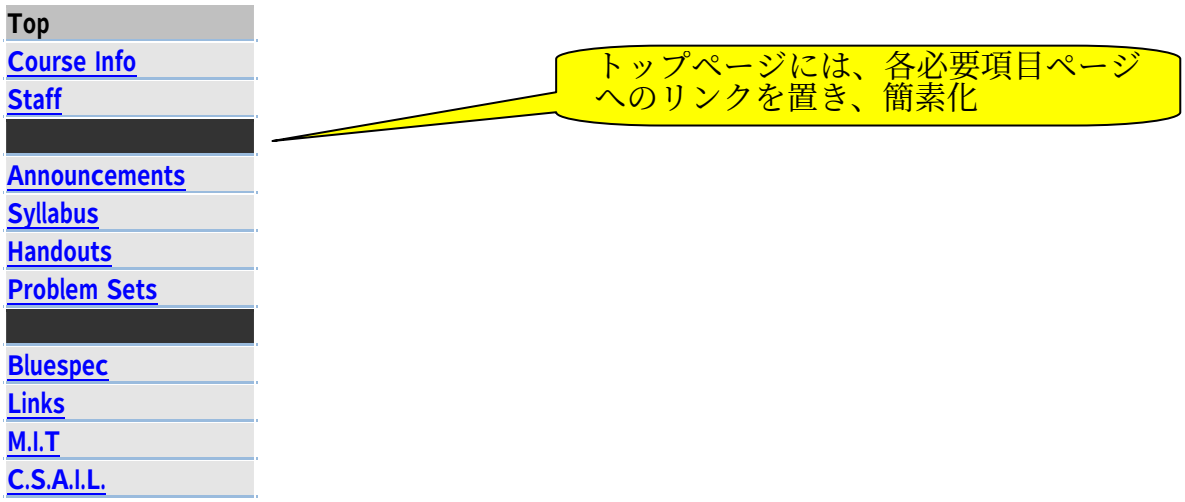
Lecture 04 (Tu 9/16/2003): More Hashing Applications, Unconditional Security

- **Handouts:**
  - Handout 06: Lamport's One-Time Passwords [MIT-only PDF]
- **Reading:** Chapter 4 of the textbook
- **Lecture Notes:** Unconditional Security [PDF, PS]
- **Related (Optional) Reading:**
  - NSA VENONA Project
  - Hash cash (Adam Back)
  - One-time passwords and an implementation

以下、Lecture05－26 は省略。

（2） X.YYY Multithreaded Parallelism: Languages and Compilers

(Revised content with new emphasis on hardware descriptions)



(Information on this website is preliminary and subject to change)

Instructor: Mr EEE
Lectures: MW9:30-11AM, 26-314
Units: 3-0-9, H-level, Grad Credit, 4 EDP

Hardware modeling provides one of the richest areas for multithreaded and parallel programming these days. Hardware operations at a low level are inherently parallel, and hardware description languages, whether for modeling, synthesis or verification, need to be able to describe fine-grain parallel operations. This subject will show a new way of describing hardware based on functional languages and atomic actions. the first third of the subject will focus on functional languages (Haskell and pH) and the lambda calculus, the second third on atomic actions and their concurrent scheduling (Bluespec). The last part of the course will cover miscellaneous topics dealing with programs analysis and implementation of these languages. Following is a partial list of topics that are likely to be covered:

- Languages and compilers to exploit multithreaded parallelism.
- Implicit parallel programming using functional languages and their extensions.
- Higher-order functions, non-strictness, and polymorphism..
- The Lambda calculus and Term Rewriting Systems.
- Atomic actions for hardware descriptions.
- Concurrent scheduling of atomic actions.
- Statics analysis and compiler optimizations.

Students may have the opportunity to program FPGA' using Bluespec.

This subject is intended for Graduate Students and Seniors. Some mathematical maturity (e.g., 6.042) and basic knowledge of programming languages and architectures (6.001, 6.004) will be assumed.

Course Information

Lectures: **Lectures will be from 9:30 AM to 11:00 AM every Monday and Wednesday in room 26-314.**

成績の付け方の記述

Office Hours: Wed 4:30-6:30, Bill no. NNN

Grading: Grades will be based on homeworks, a midterm exam and final project. The base grade will be determined by exam performance (40% midterm and 60% final). This grade will be adjusted based on homework performance. A satisfactory grade on homework will be neutral. Excellent performance on homeworks can raise grade by half a point. Poor performance can reduce the grade by up to one grade point.

Problem Sets	25%
Midterm Exam	25%
Course Project	50%

In addition, we have instituted the requirement that every student must help grade at least one problem set over the course of the semester. Failure to assist in grading will result in up to half a grade deduction (e.g. B to B-).

Exams: There will be a midterm exam less than half way through the term covering the material from the lectures, assigned readings, and class notes.

Final Project: There will be a final project presentation which will take place on the last day of classes and final reports will also be due then. All projects will involve programming in Bluespec. More details will be provided later in the term.

Homework: There will be 4 homework assignments. Homework assignments are due at the beginning of class on the due date. To facilitate grading, each problem must be stapled separately. Contact TAs in advance to request an extension. No homeworks will be accepted once solutions are handed out.

Collaboration and Academic Honesty Policy: The course policy on collaboration and the use of past course materials is as follows:

For problem sets, students are encouraged to work in pairs. A pair needs to hand in only one copy of the solution to a problem set. Pairs need not remain the same throughout the course. Students in different groups are not allowed to collaborate on a problem set.

Collaboration amongst students to understand the course material and the statement of problems sets is always encouraged.

Referring to course bibles (e.g. old problem sets and solutions) is strictly forbidden. Normal ethics dictate that, if you have been exposed to an old solution through any means, you should explicitly state this fact on the first page of an affected problem set submission.

If you have any questions about the above policy, please consult one of the TAs.

Course Reading Materials: *Implicit Parallel Programming in pH* by Rishiyur S. Nikhil and Arvind is the main textbook used in this course. This book is available at Quantum Books for around $65. This book will be useful for approximately half the course. Bluespec material will be available from the Bluespec site free of charge.

Facilities: Programming assignments for the course will be implemented in two programming languages: Haskell (Hugs implementation) and Bluespec. A Hugs compilers will be available.

教科書の指定

Home Page: The home page for the course is: http://ddd.yyy.mit.edu/X.YYY/. Here you will find course related information like handouts, manuals, problem set hints, etc... Make sure you refresh this page frequently, as it will change often and caching in your Web browser may prevent you from seeing the latest version.

Computer Communication: The TAs can be reached for questions, etc., via email at X.YYY-ta@ddd.yyy.mit.edu. We will mail all announcements, clarifications to assignments, answers to common questions, etc., to the course email list - X.YYY-students@ddd.yyy.mit.edu.

（3） X.ZZZ/HST.WWW Medical Computing　Spring 2002

Medical science and practice in the age of automation and the genome: Present and Future

Instructors: Mr. MMM, MD, PhD, Mr. LLL, MD, PhD, Mr. KKK, PhD

The text is

Shortliffe EH, Perreault LE, Wiederhold G and Fagan LM, *Medical Informatics: Computer Applications in Health Care and Biomedicine, 2nd Edition.* Springer 2001.
Sold online at: Barnes & Noble Fatbrain Amazon Quantum

Link To Course Schedule, Readings & Problem Sets

Please hand in problem set answers via electronic submission to: qqq@mit.edu

Solutions to Problem Set 1 are now (belatedly) posted.

Problem Set 2 due April 30. ***(Note postponement.)***

Project topic suggestions

Here are a few relevant links:

- Microsoft Access version of a small subset of the Children's Hospital database, from about five years ago. These data have been "scrubbed", so that specifically identifying information has been altered or removed. Nevertheless, please treat the data with sensitivity, because you know from our discussion of medical data confidentiality that even innocuous-seeming data can help re-identify. The database is accessible via the same security as papers for the class. If you need it in a form different from MS Access, please email the instructors. Note: This database is about 45MB in size. Via a cable modem, it takes over 10 minutes to download. By dial-up phone line, it is probably impractical.
- MySQL version of the above database. If you don't have access to MS Access, you might try this.
- CWS database tab-delimited text flatfiles if all else fails...
- NLM's PubMed interface to the MEDLINE search engine. This indexes all the biomedical literature, holds abstracts for most papers, and full text for a few.
- Note that if you find a citation, you can probably find the paper on-line through the MIT Library's subscription to electronic journal databases. Harvard-affiliated students should have similar access through the Harvard library system. Access to both is limited to those associated with the particular institution.
- NLM's links to other useful databases. Note especially the link to NCBI, which holds many interesting genomic data.
-

Fundamentals -- Links and Readings:

Conceptual Modeling & UML

- Brief Introduction to Conceptual Graphs
- Conceptual graph examples
- Introduction to the use of conceptual graphs for medical databases

教科書、参考書の指定

教科書、参考書の指定

- Paper on tradeoff in the modeling of large clinical databases (pdf)
- Introduction to UML - the most commonly used conceptual modeling formalism

Structured Query Language (SQL) and Relational Algebra

- Very basic introduction to SQL
- More on SQL
- Even more on SQL
- More detail regarding the Oracle implementation of SQL (pdf)
- In depth view of one of the two languages behind relational database operations: relational algebra (pdf)
- A web-oriented view of data modeling and databases
- A good, short book on SQL: Teach Yourself SQL in 10 Minutes
- A pdf on MS Access SQL.