

# COSC413 Advanced Topics in Algorithms

## Course Outline, 2012 Second semester

Course supervisor: Professor T. Takaoka  
Department of Computer Science  
Email:tad, phone 7773, room 302

January, 2012

### Course aims

We learn cryptography and complexity theory in this course. This course will give a clear explanation of NP-completeness theory. Then algorithms on number theory needed for the RSA cryptosystem will be given in detail. The advanced topic of random algorithms will also be discussed. COSC262, MATH220 and MATH324 are good preparation for this course. Topics will be drawn from:

- Non-deterministic Turing machine
- The classes P and NP
- Cook's Theorem
- Satisfiability Problem is NP-complete
- Hamilton cycle is NP-complete
- Colorability is NP-complete
- Knapsack problem is NP-complete
- Public-key cryptosystem by Diffie and Hellman
- RSA cryptosystem by Rivest, Shamir and Adelman
- Probabilistic primality test algorithm in polynomial time
- Number theoretic algorithms in multiple precision

### Lectures and Lecturer

Lecture times and location will be announced later. Lecturer is the supervisor given above.

## Assessment

Part	Type	Worth	Due date
Assignment 1	Cryptography	25%	Single Precision August 17 Multiple Precision September 7
Assignment 2	Complexity Theory	25%	September 28
Exam		50%	TBA

The Computer Science department has the following grading policy. In order to pass a course you must meet two requirements:

- a) The university has adopted a common scale for converting marks to grades. According to this scale, an average mark of 50% is sufficient to pass the course (i.e. to achieve a C-), with an average mark of 55% a C grade is achieved and so forth. We apply this conversion scale to the average marks students achieve over all assessment items.
- b) You must achieve an average mark of at least 45% on invigilated assessment items.

Marks are sometimes scaled to achieve consistency between courses from year to year.

The test is an open book one. Important documents are posted to the COSC413 area on Learn. Please read all such notices and documents.

## Recommended Reading

- Hopcroft and Ullman (recommended text), *Design and Analysis of Computer Algorithms*, Addison-Wesley, 1974.
- D. E. Knuth, *The Art of Programming, Vol 2 : Seminumerical Algorithms*, Addison-Wesley, 1997

## Other important documents

There are several important documents available online about departmental regulations, policies and guidelines at the following site. We expect all students to be familiar with these. <http://www.cosc.canterbury.ac.nz/regulations/>

Notices about this class will be posted to the class forum in the Learn system ([learn.canterbury.ac.nz](http://learn.canterbury.ac.nz)). COSC students will also be made members of “CSSE Notices”, where general notices will be posted that apply to all classes (such as information about building access or job opportunities).