YALE UNIVERSITY
DEPARTMENT OF COMPUTER SCIENCE

CPSC 461b: Foundations of Cryptography *Handout #1*
Professor M. J. Fischer *January 11, 2009*

Syllabus (Spring 2009)

1 Official Yale course listing

CPSC 461 01 (23721) /
CPSC 561 01 (23722)
Foundations of Cryptography
Michael Fischer
TTh 2.30–3.45 AKW 200 [Changed to TTh 3.45–5.00 AKW 500]

Spring 2009
No regular final examination
Permission of instructor required

Foundations of modern cryptography and their application to computer and network security. Topics include randomized models of computation, indistinguishability, computationally hard problems, one-way and trapdoor functions, pseudorandom generators, zero-knowledge, secure computation, and probabilistic proofs.
After Computer Science 467a. (Not taught every year.)

2 Course Description

2.1 Nature and Purpose of the Course

This is an advanced seminar on cryptography and computer security. It assumes a basic knowledge of cryptography such as is covered in CPSC 467a/567a. The goal is to cover the background necessary for theoretical research in the area. Recent advances in computational complexity have transformed cryptography from a poorly-understood art to a rigorous scientific discipline in which security properties can be proved from explicit assumptions. Randomization and notions from probability, statistics, and complexity theory are central to these techniques.

2.2 Main Topics to be Covered

Topics include randomized models of computation, indistinguishability, computationally hard problems, one-way and trapdoor functions, pseudorandom generators, zero-knowledge, secure computation, and probabilistic proofs. Additional topics may be included if time permits.

3 Course materials

Primary readings: The first part of the course will be based on two books by Oded Goldreich.

1. *Foundations of Cryptography*, Volume 1, Basic Tools, published by Cambridge University Press. It may be awhile before copies are available at the Yale University Bookstore. In the meantime, a preliminary draft of the book is available for personal and classroom use on the author's web site. See also the author's web page for the published book for further information and errata.

2. *Foundations of Cryptography – A Primer*. This is a condensation of *Foundations of Cryptography* that attempts to give a more readable survey of the field. It is a good starting point for

the topics we will be discussing and contains an extensive bibliography to the literature. It is available free of charge as an Open Journal PDF file. A book version can be purchased for $50. It is the first issue in the new Foundations and Trends in Theoretical Computer Science series published by Now Publishers. The Yale Library subscribes to this series, so other issues may be downloaded for free from computers on the Yale network.

Other materials will be posted on the course web site from time to time during the term.

Website: I maintain a course website at http://zoo.cs.yale.edu/classes/cs461/2009/index.html. You should bookmark it in your browser and visit it often. It will grow as the term progresses and will contain announcements, handouts, homework assignments, programming hints, and links to documents in the course directory and elsewhere on the web. *Access may be restricted to machines on the Yale network.* If so, for off-campus use, you will need to follow the instructions for use of the Yale remote authentication proxy server.

4 Course Mechanics

Prerequisites: This course will be taught at the graduate level, but it is open to well-prepared advanced undergraduates as well. CPSC 467a is a prerequisite for undergraduates; graduate students should have an equivalent background. It also assumes a basic computer science background and familiarity with basic tools of mathematics as are covered in CPSC 202a and in elementary mathematics courses.

Requirements: This course will be taught as a seminar, and attendance is required. Each 75-minute class period will be devoted to the exploration of one topic. One person (student or instructor) will prepare the topic and act as discussion leader, but all will be expected to participate. Course requirements include written problem sets (which may on occasion involve some programming), a midterm exam, and a term paper. There is no final exam. Graduate students taking the course will be expected to perform at a higher level than undergraduates and may be required to do additional work.

Grading: The final grade in the course will be based on class participation, homework, midterm exam, and the term paper.

Assignments and other announcements: Course announcements will be posted from time to time on the course home page. Assignments and other materials will be posted on the handouts page. It is your responsibility to check these pages frequently.

Email: I am always available for email consultation at fischer-michael@cs.yale.edu. I can't always promise to respond right away, but I can often be reached by email when I am away from the office. Email is also the preferred way to arrange an appointment with me.

5 Policies

Late Policy: Late work will be accepted at the discretion of the instructor and/or TA and will generally be subject to a penalty unless accompanied by a Dean's excuse. Work will not be accepted after graded papers have been returned or solutions released. However, alternative means for making up missed work may be arranged on an individual basis with a Dean's excuse.

Please contact the instructor or TA as soon as you find out that you are unable to submit work on time or to attend a scheduled exam so that suitable makeup arrangements can be made.

Policy on Working Together: Work turned in under your name must be your own work. Plagiarism is unethical and will not be tolerated. You may neither copy from others nor permit your own work to be copied. Therefore, it is important that you keep your files protected so that others cannot read them and that you carefully guard your password. If you think your password may have been compromised, you should change it immediately.

You may of course discuss the lectures and readings with your classmates in order to improve your understanding of the subject. However, all written work must be your own. You are also always free (and encouraged) to come in and ask the TA or instructor for help about anything concerning the course. Please talk to me if you have any questions about this policy.

Policy on Computer Problems: The Yale College policy on "Use of Computers and Postponement of Work" in the Yale College Programs of Study applies to this course. It is reproduced below.

> "Problems that may arise from the use of computers, software, and printers normally are not considered legitimate reasons for the postponement of work. A student who uses computers is responsible for operating them properly and completing work on time. (It is expected that a student will exercise reasonable prudence to safeguard materials, including saving data on removable disks at frequent intervals and making duplicate copies of work files.) Any computer work should be completed well in advance of the deadline in order to avoid last-minute technical problems as well as delays caused by heavy demand on shared computer resources in Yale College."

Particularly relevant for this course are the cautions against leaving a programming assignment to the last minute when machines might be busy, printers broken, and so forth, and about safeguarding your data.

6 Computing Facilities

The Zoo: This course will be supported by the Computer Science Department's educational computing facility, otherwise known as the Zoo. This facility contains Pentium-based PC's running Linux. You will need to learn how to use these machines if you don't already know how in order to read email, browse course-related web pages, edit and compile C programs, and access the course directory. Look at

```
http://zoo.cs.yale.edu/help/
```

for information on getting started if you are new to the Zoo.

Your course account: You should request a course account for this course *even if you already have a Zoo account*, for otherwise you will be unable to submit work electronically. To obtain your account, go to

```
http://zoo.cs.yale.edu/help/accessing-zoo.shtml
```

and follow the instructions there.

Course directory: The shared course directory, `/c/cs461`, is located on the Zoo server. You can access it from your Zoo course account. It will contain any software needed for this course and miscellaneous documentation and files. It will also contain software to allow you to submit assignments electronically. Public files there can be accessed via the web as well as from a Zoo node. Your class account home directories will also be located there.