YALE UNIVERSITY
DEPARTMENT OF COMPUTER SCIENCE

CPSC 467b: Cryptography and Computer Security *Handout #1*
Professor M. J. Fischer *January 6, 2012*

Syllabus (Spring 2012)

1 Official Yale course listing

CPSC 467 01 (21632) /CPSC 567 01 (20820)	Final exam scheduled (Group 36)
Cryptography and Computer Security	05/03/2012 Th 9.00
Michael Fischer	Skills QR
MW 1.00–2.15 AKW 400	

A survey of such private and public key cryptographic techniques as DES, RSA, and zero-knowledge proofs, and their application to problems of maintaining privacy and security in computer networks. Focus on technology, with consideration of such societal issues as balancing individual privacy concerns against the needs of law enforcement, vulnerability of societal institutions to electronic attack, export regulations and international competitiveness, and development of secure information systems.
Some programming may be required. After CPSC 202 and 223.

2 Course Description

This course is about cryptography and its applications to information and computer security. Privacy and security are central to our emerging "information society", and cryptography is a key technology for achieving them. It is also a fascinating field of study in its own right.

Information security, broadly defined, involves controlling the dissemination of information. It includes issues of privacy, data integrity, authenticity, and authority. Privacy refers to preventing information flow to unintended recipients. Data integrity properties insure that information is correct and undamaged. Authenticity identifies information with a source. Authority describes what actions are permitted by whom. Because of the ease with which information can be copied and transmitted, traditional physical means of control are of limited efficacy. Cryptography gives a way to build logical controls on the flow of information that are largely independent of the physical properties of the devices used to transmit and store information.

Computer security relies on cryptography for access control and protection of sensitive data, but computer security also includes topics such as physical security, access restrictions, activity monitoring, and control of software defects that go way beyond what will be covered in this course.

Cryptography lies at the center of this course, but we will be approaching the subject broadly. On the one end, we'll look at problems of computer and information security and see how cryptographic tools can be used to solve them. We'll also touch on some social issues surrounding the use of cryptography. At the other end, we'll explore the mathematical structures from which cryptographic primitives are built.

Security properties cannot be verified through testing since there is no way to test all possible attacks. Instead, they must be verified analytically through security modeling, or empirically through the test of time. Analytic verification means establishing plausible mathematical models in which security properties can be formally stated and proved.

Tentative topic outline:

1. Introduction (0.5 lecture)
2. Classical cryptography (1.5 lectures)
3. Symmetric key cryptography and cryptanalysis (4 lectures)
4. Number theory (1 lecture)
5. Public key cryptography and cryptanalysis (3 lectures)
6. Elliptic curve cryptography (1 lecture)
7. Digital signatures (2 lectures)
8. Encryption with special properties (1 lecture)
9. Key distribution (1 lecture)
10. Message integrity (2 lecture)
11. Authentication (4 lectures)
12. Pseudo random number generation (1 lecture)
13. Protocols (2 lectures)
14. Secure multiparty computation (1 lecture)

This represents somewhat of a departure from the way this course has been taught in the past, where a greater emphasis was placed on number theory and less on current directions in the field. The time estimates are only guesses and are subject to revision as the term progresses.

3 Course materials

Required textbooks:

1. Shafi Goldwasser and Mihir Bellare,
   Lecture Notes on Cryptography. Available online without charge.
2. Wade Trappe and Lawrence C. Washington,
   Introduction to Cryptography with Coding Theory, Second Edition, Pearson, 2006, ISBN-10: 0131862391, ISBN-13: 9780131862395. Suggested retail price: $126.67. Google product search lists a variety of sellers of new and used copies at varying prices.

Website: I maintain a course website at http://zoo.cs.yale.edu/classes/cs467/2012s/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, lecture notes, revisions to homework assignments, programming hints, and links to documents in the course directory and elsewhere on the web. *Access to this and other Yale web sites may be restricted to machines on the Yale network.* If you find it is, you will need to configure your browser to use the Yale remote authentication proxy server, or set up your machine to use a Yale VPN connection.

4 Course Mechanics

Prerequisites: This course will be taught at an advanced undergraduate/graduate level and assumes a basic computer science background. Some C/C++ programming will be required. CPSC 202a and 223b are prerequisites. Graduate students should have an equivalent background.

Requirements: Course requirements include written problem sets and programming assignments (∼30%), a midterm exam (∼25%), and a final exam (∼45%). The approximate weights of each in determining the course grade are shown following in parentheses. Graduate students taking the course will be expected to perform at a higher level than undergraduates and may be required to do additional work.

Assignments and other announcements: Written problem sets and programming assignments will posted on the handouts page of the course website from time to time during the course. Other course announcements will be posted on the course home 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 know that you will be unable to submit work on time or to attend a scheduled exam so that suitable makeup arrangements can be made.

Policy on Cheating, Plagiarism, and Documentation: Students in this course are subject to Yale's policies on cheating, plagiarism, and documentation. For undergraduates, the policies are documented in the Undergraduate Regulations under Cheating, Plagiarism, and Documentation. For graduate students, the policies are documented under Professional Ethics. It is your responsibility to become familiar with these regulations and to abide by them. Penalties for violation can be severe, including possible expulsion from the university.

With so much information available on the internet, it is particularly important that you cite the sources of any materials (including computer source code) that you use in your own work. It is okay to use of other people's work as long as you make clear what work is not your own and you give it proper attribution.

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, expect for parts that are explicitly quoted from and attributed to others. You are also always free (and encouraged) to come in or email 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 using 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/cs467`, is located on the Zoo server. You can access it from your Zoo course account. It will contain software that you will be using for this course and miscellaneous documentation and files. It will also contain the software that you will use when submitting 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.