CS6377.001.13S Introduction to Cryptography
Spring 2013: Syllabus

Course Information

Course Number/Section:	CS6377.001.13S
Course Title:	Introduction to Cryptography
Term:	Spring 2013
Days & Times:	Tuesday & Thursday: 4:00pm – 5:15pm
Location:	ECSN 2.126

Professor Contact Information

Professor:	Dr. Yvo G. Desmedt
Office Phone:	(972) 883-4536
Email Address:	Yvo.Desmedt@UTDallas.edu **(not efficient: see further)**
Office Location:	ECS 4.411
Office Hours:	Wednesday 2pm – 3pm

TA Contact Information: to be announced

Course Prerequisites

CS 5333 and CS 5343 (or equivalent)

Course Description

This course covers the basic aspects of modern cryptography, including block ciphers, pseudorandom functions, symmetric encryption, Hash functions, message authentication, number-theoretic primitives, public-key encryption, digital signatures and zero knowledge proofs.

Course Goals and Objectives

The objective is that students become familiar with basic cryptography and *understand* how most of the US standards on cryptography work. The students will learn about:

- The range of security objectives.
- The different levels of security that are achieved.
- The available tools, including the types of cryptosystems, such as conventional cryptography, symmetric and asymmetric cryptography, and public key.

Required Textbooks and Materials

Required textbook: *Cryptography: Theory and Practice*, by D. R. Stinson, CRC, The Fourth Printing. **Note:** the 2nd edition is *not* allowed!
The course will also use **notes and material** from the following:

- *Introduction to Number Theory*, by L. K. Hua, Springer, 1992 (only the first three chapters will be used).
- "Encryption schemes," by Y. Desmedt, Chapter 10 in *Handbook of Algorithms and Theory of Computation: special topics and techniques*, M. Atallah and M. Blanton, editors, 2010, CRC. (This will be heavily used.)

Suggested Course Materials

- "Cryptographic Foundations," by Y. Desmedt, Chapter 9 in *Handbook of Algorithms and Theory of Computation: special topics and techniques*, M. Atallah and M. Blanton, editors, 2010, CRC. (Parts of this chapter will be used.)
- *Introduction to Modern Cryptography*, by Jonathan Katz and Yehuda Lindell.
- *Applied Cryptography*, by A. Menezes and P. van Oorschot and S. Vanstone, CRC 1996.

Students are *recommended* to read:

- Chapters 2–4 in Menezes-van Oorschot-Vanstone, and
- Chapter 9 in Handbook of Algorithms and Theory of Computation: special topics and techniques.

Students are encouraged to read the material before class time. However, students should be aware that there is no perfect book in the area of cryptography.

Assignments & Academic Calendar

Of above reference the students are **required** to read:

1. the first three chapters of Hua by February 14, 2013. Students who prefer to read a less dense introductory text on number theory than Hua can propose one to the instructor. Alternative books should cover the same material.
2. "Encryption Schemes" by February 19, 2013.

Large homework assignments will be given after these deadlines. Exams and other homeworks extensively use the aforementioned material.

Academic Calendar: Questions and interactions with students are welcome. Such interactions may be the start of a scientific paper(s). The schedule is therefore tentative and not etched in stone. For details see Table 1.

Grading Policy

The grade depends on the understanding of the material covered in class and on the correctness and the details given in answers to questions on exams and homeworks.

homeworks and possibly program assignments:	20%
midterm (April 2):	40%
final exam (cumulative):	40%

Day	Topic	Material	Sugg. Exc.
1/15	Syllabus & Introduction	Des Ch. 9, MOV pp. 1–6	
1/17	Intro, Levels & Types	Des Ch. 9, MOV pp. 25–32	
1/22	Perfect Secrecy[a].	Sti pp. 44–51, Des Ch. 9	Sti 2.1–2.2 & Notes
1/24	El Gamal Encryption	Sti pp. 162–164, Des Ch. 10	Sti 5.4
1/29	Number Theory 1	Des Ch. 10, Sti pp. 9–10, Hua	Sti 4.2
1/31	Number Theory 1	Des Ch. 10, Sti pp. 9–10, Hua	
2/05	RSA	Sti pp. 124-125, Des Ch. 10	
2/07	Computational Number Theory 1	Des Ch. 10, Sti pp. 116–119, 125–128	Sti 4.1
2/12	Number Theory 2	Des Ch. 10, Sti Ch. 5	Sti 4.4–4.5
2/14	Number Theory 2	Des Ch. 10, Sti Ch. 5	Sti 4.4–4.5
2/19	Computational Number Theory 2	Des Ch. 10, Sti Ch. 5	
2/21	Primality testing	Des Ch. 10, Sti Ch. 5	Sti 4.14
2/26	Probabilistic Encryption	Des Ch. 10, Sti pp. 381-384	
2/28	Some signature schemes	Sti pp. 203–210	
3/05	Some signature schemes	Sti pp. 203–210	
3/07	Block Ciphers & Hash functions	MOV Ch. 7 & 9, Sti Ch. 3 & 9, Not	
3/19	Block Ciphers & Hash functions	MOV Ch. 7 & 9, Sti Ch. 3 & 9, Not	
3/21	Key Distribution	Sti Ch. 8, MOV Ch. 12, Sti 8.3	
3/26	Key Distribution	Sti Ch. 8, MOV Ch. 12, Sti 8.3	
3/28	Certificates & PKI	Not, MOV Ch. 13	
4/02	Midterm		
4/04	Pseudo-random generators	Sti Ch. 12	
4/09	Zero-knowledge	Not, Sti Ch. 13	Sti 13.5
4/11	Zero-knowledge	Not, Sti Ch. 13	Sti 13.5
4/16	DSS	Not, Sti pp. 285–291, pp. 210–214	
4/18	Secret Sharing	Sti pp. 327–339	
4/23	Threshold Cryptography	Not	
4/25	Anonymity & e-voting	Not	
4/30	Authentication Code	Sti Ch. 10	
5/02	Tracing	Not	

[a]Material to refresh before this course: probability theory and proof techniques.

Table 1: Tentative schedule. "Sti" means the book by Stinson, "Hua" means the book by Hua, "Des" means Chapters 9 and 10 in the Handbook of Algorithms and Theory of Computation, "Not" means personal notes, and "MOV" means the book by Menezes-van Oorschot-Vanstone.

Course & Instructor Policies

Class attendance: Students are strongly encouraged to attend class. Since the material is very mathematical students are strongly encouraged to do this. Besides the textbook, personal notes and other references are used during the class presentations. This implies that students have yet another benefit to attend classes.

Although there is a significant overlap with Stinson's book and the course, most material will be presented in a didactic way, different from Stinson's book. Students who regularly attend class may do better on the exam.

Students do *not* need to inform the instructor they will miss class. A student missing a class is strongly encouraged to ask for the notes of 2 students who did attend that class.

How to return homework: students need to return homework *on paper* by 4pm the day the homework is due. Students who miss this class, are encouraged to ask some other student to bring the homework to class.

Late work policy: Students who return their homework too late will be penalized as follows:

- If a student is late, but turns his/her answer in before the start of the next class the student's grade will be multiplied with 0.9.
- If a student waits longer, then the student receives no credit! His/her answer will be corrected. In case the student has trouble to pass the course, the non-credited homework be taken into consideration in favor of the student. (Hopefully not applicable.)

Student Conduct & Discipline

The University of Texas System and The University of Texas at Dallas have rules and regulations for the orderly and efficient conduct of their business. It is the responsibility of each student and each student organization to be knowledgeable about the rules and regulations which govern student conduct and activities. General information on student conduct and discipline is contained in the UTD publication, A to Z Guide, which is provided to all registered students each academic year.

The University of Texas at Dallas administers student discipline within the procedures of recognized and established due process. Procedures are defined and described in the Rules and Regulations, Board of Regents, The University of Texas System, Part 1, Chapter VI, Section 3, and in Title V, Rules on Student Services and Activities of the universitys Handbook of Operating Procedures. Copies of these rules and regulations are available to students in the Office of the Dean of Students, where staff members are available to assist students in interpreting the rules and regulations (SU 1.602, 972/883-6391).

A student at the university neither loses the rights nor escapes the responsibilities of citizenship. He or she is expected to obey federal, state, and local laws as well as the Regents Rules, university regulations, and administrative rules. Students are subject to discipline for violating the standards of conduct whether such conduct takes place on or off campus, or whether civil or criminal penalties are also imposed for such conduct.

Academic Integrity

The faculty expects from its students a high level of responsibility and academic honesty. Because the value of an academic degree depends upon the absolute integrity of the work done by the student for that degree, it is imperative that a student demonstrate a high standard of individual honor in his or her scholastic work.

Scholastic dishonesty includes, but is not limited to, statements, acts or omissions related to applications for enrollment or the award of a degree, and/or the submission as ones own work or material that is not ones own. As a general rule, scholastic dishonesty involves one of the following acts: cheating, plagiarism, collusion and/or falsifying academic records. Students suspected of academic dishonesty are subject to disciplinary proceedings.

Plagiarism, especially from the web, from portions of papers for other classes, and from any other source is unacceptable and will be dealt with under the universitys policy on plagiarism (see general catalog for details).

This course will use the resources of turnitin.com, which searches the web for possible plagiarism and is over 90% effective.

Email Use

Due to massive spam Email is no longer an efficient way to communicate. Therefore, students are *discouraged* to e-mail the instructor. Better ways to communicate with the instructor, are: immediately after class (when available) and during office hours.

Due to the massive spam, students sending e-mail should not expect an immediate reply. A reply may be given in class, or by e-mail typically *several days to a week* after the student sent his/her e-mail.

Moreover, email raises some issues concerning security and the identity of each individual in an email exchange. **The instructor considers email from students *only* if it originates from a UTD student account**. E-mail sent from Gmail, Hotmail, etc., will likely bounce. UTD furnishes each student with a free email account that is to be used in all communication with university personnel.

Withdrawal from Class

The administration of this institution has set deadlines for withdrawal of any college-level courses. These dates and times are published in that semester's course catalog. Administration procedures must be followed. It is the student's responsibility to handle withdrawal requirements from any class. In other words, I cannot drop or withdraw any student. You must do the proper paperwork to ensure that you will not receive a final grade of "F" in a course if you choose not to attend the class once you are enrolled.

Student Grievance Procedures

Procedures for student grievances are found in Title V, Rules on Student Services and Activities, of the universitys Handbook of Operating Procedures.

In attempting to resolve any student grievance regarding grades, evaluations, or other fulfillments of academic responsibility, it is the obligation of the student first to make a serious effort to resolve the matter with the instructor, supervisor, administrator, or committee with whom the grievance originates (hereafter called the respondent). Individual faculty members retain primary responsibility for assigning grades and evaluations. If the matter cannot be resolved at that level, the grievance must be submitted in writing to the respondent with a copy of the respondents School Dean. If the matter is not resolved by the written response provided by the respondent, the student may submit a written appeal to the School Dean. If the grievance is not resolved by the School Deans decision, the student may make a written appeal to the Dean of Graduate or Undergraduate Education, and the deal will appoint and convene an Academic Appeals Panel. The decision of the Academic Appeals Panel is final. The results of the academic appeals process will be distributed to all involved parties.

Copies of these rules and regulations are available to students in the Office of the Dean of Students, where staff members are available to assist students in interpreting the rules and regulations.

Incomplete Grade Policy

As per university policy, incomplete grades will be granted only for work unavoidably missed at the semesters end and only if 70% of the course work has been completed. An incomplete grade must be resolved within eight (8) weeks from the first day of the subsequent long semester. If the required work to complete the course and to remove the incomplete grade is not submitted by the specified deadline, the incomplete grade is changed automatically to a grade of F.

Disability Services

The goal of Disability Services is to provide students with disabilities educational opportunities equal to those of their non-disabled peers. Disability Services is located in room 1.610 in the Student Union. Office hours are Monday and Thursday, 8:30 a.m. to 6:30 p.m.; Tuesday and Wednesday, 8:30 a.m. to 7:30 p.m.; and Friday, 8:30 a.m. to 5:30 p.m.

The contact information for the Office of Disability Services is:
The University of Texas at Dallas, SU 22
PO Box 830688
Richardson, Texas 75083-0688
(972) 883-2098 (voice or TTY)

Essentially, the law requires that colleges and universities make those reasonable adjustments necessary to eliminate discrimination on the basis of disability. For example, it may be necessary to remove classroom prohibitions against tape recorders or animals (in the case of dog guides) for students who are blind. Occasionally an assignment requirement may be substituted (for example, a research paper versus an oral presentation for a student who is hearing impaired). Classes enrolled students with mobility impairments may have to be rescheduled in accessible facilities. The college or university may need to provide special services such as registration, note-taking, or mobility assistance.

It is the students responsibility to notify his or her professors of the need for such an accommodation. Disability Services provides students with letters to present to faculty members to verify that the student has a disability and needs accommodations. Individuals requiring special accommodation should contact the professor after class or during office hours.

Religious Holy Days

The University of Texas at Dallas will excuse a student from class or other required activities for the travel to and observance of a religious holy day for a religion whose places of worship are exempt from property tax under Section 11.20, Tax Code, Texas Code Annotated. The student is encouraged to notify the instructor or activity sponsor as soon as possible regarding the absence, preferably in advance of the assignment. The student, so excused, will be allowed to take the exam or complete the assignment within a reasonable time after the absence: a period equal to the length of the absence, up to a maximum of one week. A student who notifies the instructor and completes any missed exam or assignment may not be penalized for the absence. A student who fails to complete the exam or assignment within the prescribed period may receive a failing grade for that exam or assignment. If a student or an instructor disagrees about the nature of the absence [i.e., for the purpose of observing a religious holy day] or if there is similar disagreement about whether the student has been given a reasonable time to complete any missed assignments or examinations, either the student or the instructor may request a ruling from the chief executive officer of the institution, or his or her designee. The chief executive officer or designee must take into account the legislative intent of TEC 51.911(b), and the student and instructor will abide by the decision of the chief executive officer or designee.