CS6377.001.22F Introduction to Cryptography
Fall 2023: Syllabus: Version 1 (Draft)

Course Information

Course Number/Section:	CS6377.001.23F
Course Title:	Introduction[1]to Cryptography
Term:	Fall 2023
Days & Times:	Monday & Friday: 2:30pm-3:45pm
Location:	AD 2.232

Professor Contact Information

Professor:	Dr. Yvo G. Desmedt
Office Phone:	(972) 883-4536[2]
Email Address:	y.desmedt@cs.ucl.ac.uk **(not efficient: see further)**
Office Location:	ECS 4.411
Office Hours:	Monday 10:00am – 11:00am (see further for details)

Course Prerequisites

CS 5333 and CS 5343 (or equivalent)

Warning

This course is very mathematical. Students should not be mislead by the word "introduction" in the title. Students who are not good in mathematics should not take this course to avoid ending up with an F grade.

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.
- Basic encryption techniques.

[1] See Section: Warning

[2] This is no longer a real telephone, but has been replaced by MS Teams.

- Message authentication techniques.
- Number theory for cryptography.
- Public key cryptography digital signatures.
- Cryptographic proof techniques.
- Practical applications of cryptography.

Textbooks and Materials

There is *no* required textbook. The course will use **notes and material**, e.g., from the following:

- "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 and is available via eLearning.)
- *Introduction to Number Theory*, by L. K. Hua, Springer, 1992 (only the first three chapters will be used and are available via eLearning.).

Recommended textbooks:

- *Cryptography: Theory and Practice*, by D. R. Stinson, CRC, Third Edition. **Note:** the 2nd edition is *not* allowed!
- *Cryptography Made Simple*, by N. Smart, Springer
- *Applied Cryptography*, by A. Menezes and P. van Oorschot and S. Vanstone, CRC 1996 (This text is only recommended for limited material.)

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.

Students are *recommended* to read:

- 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.

Students should *avoid* reading chapters on cryptography in books on Computer Security.

Assignments

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

- "Encryption Schemes" by September 18, 2023.

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

Students are *recommended* to read:

- the first three chapters of Hua by September 25, 2023.

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:	20%
quiz:	40%
final exam (cumulative):	40%

The exact date of the quiz will be announced well before the exam.

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.

How to return homework: students need to return homework by the start of class the day the homework is due. The delivery method will be decided by the TA/grader.

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

- If a student is late, but turns the homework 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! The homework will be corrected.

Recommendations

- **Homeworks:** Students copying other students homeworks will be ill prepared for the quiz and for the final. To avoid this, students should make their own homework.
- **e-mail:** UTD has recently moved to Microsoft's Outlook, resulting in several complains from students. Microsoft states:

  > Email messages in your Microsoft Outlook 2010 Inbox and other mail folders can be organized by date and arranged by Conversation. When Conversations is turned on, messages that share the same subject appear as Conversations that can be viewed expanded or collapsed. You can quickly review and act on messages or complete Conversations.

  To turn this off (and get the by date option), see:
  https://support.office.com/en-us/article/View-email-messages-by-conversation-0eeec76c-f59b-4834-98e6-05cfdfa9fb07
  The instructor strongly recommends students to use the date option.

Draft 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.

Day	Topic	Material	Sugg. Exc.
8/21	Syllabus & Introduction	**Des Ch. 9**, MOV pp. 1–6	
8/25	Intro, Levels & Types	**Des Ch. 9**, MOV pp. 25–32	
8/28	Historic Systems & Perfect Secrecy[a].	Sti pp. 48–54, **Des Ch. 9**	Sti 2.3–2.7 & Notes
9/1	El Gamal Encryption	Sti pp. 233–235, **Des Ch. 10**	Sti 6.4
9/8	Number Theory 1	**Des Ch. 10**, Sti pp. 8–11, Hua	Sti 4.2
9/11	Number Theory 1	**Des Ch. 10**, Sti pp. 8–11, Hua	
9/15	RSA	Sti pp. 173–174, **Des Ch. 10**	
9/18	Computational Number Theory 1	**Des Ch. 10**, Sti pp. 163–166, 171–172	Sti 5.3–5.4
9/22	Number Theory 2	**Des Ch. 10**, Sti Ch. 5	Sti 5.5–5.7
9/25	Computational Number Theory 2	**Des Ch. 10**, Sti Ch. 5	
9/29	Primality testing	**Des Ch. 10**, Sti Ch. 5	
10/2	Probabilistic Encryption	**Des Ch. 10**, Sti pp. 344-349	
??/??*	Quiz		
10/9	Some signature schemes	**Sti pp. 282–283**	
10/13	Key Distribution & Key Agreement	**Sti Ch. 10–11**, MOV Ch. 12	Sti 11.2
10/16	Key Distribution & Key Agreement	**Sti Ch. 10–11**, MOV Ch. 12	Sti 11.2
10/20	Certificates & PKI	**Not**, MOV Ch. 13, Sti Ch. 12	
10/23	Zero-knowledge	**Not**, Sti pp. 367–387	Sti 9.13
10/27	DSS	**Not, Sti pp. 293–296**	
10/30	Secret Sharing	**Not**. Sti pp. 481–491	
11/3	Threshold Cryptography	**Not**	
11/6	Anonymity & e-voting	**Not**	
11/10	Research topics(+), Post-quantum, Error-correcting (intro), McEliece	**Not** & WWW	
11/13	Block Ciphers & Hash functions	MOV Ch. 7 & 9, Sti Ch. 3 & 4, **Not**	
11/17	Block Ciphers & Modes of operation	MOV Ch. 7 & 9, Sti Ch. 3 & 4, **Not**	
11/27	Authentication Code & Elliptic Curves & Pseudo-random	**Not, Sti pp. 143-145**	
12/1	Topic class	**Not**	
12/4	Topic class	**Not**	

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

Table 1: Tentative schedule. Information about any potential rescheduling will be e-mailed to all students.
(+) includes: attribute-based encryption, fully homomorphic encryption, functional encryption, identity based cryptography, searchable encryption, and secure multiparty computation.
*: the dates of the quiz have not yet been finalized.

"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 (some as slides), and "MOV" means the book by Menezes-van Oorschot-Vanstone. Boldface indicates the preferred source of the material.

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 university's 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, 972/882-6391).

A student at the university neither loses the rights nor escapes the responsibilities of citizenship. The student 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 the student's 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 one's own work or material that is not one's 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 university's 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 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 the 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.

Office Hours

Office hours will be held in-person. Note that office hours may be canceled occasionally.

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 university's 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 respondent's 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 Dean's 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 semester's 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 student's responsibility to notify the professor 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 the 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.