CO 485/685: The Mathematics of Public-Key Cryptography — Fall 2012

Lectures: TR 2:30–3:50 p.m. in MC 2017

Instructor: **Edlyn Teske**
Email: `eteske@uwaterloo.ca`
Office: MC 4030. Phone: x33473
Office hours: Tuesdays and Fridays 12 noon–1 p.m.

Teaching Assistant: **Gabriel Gauthier-Shalom**
Email: `g3gauthi@uwaterloo.ca`
Office: MC 6093. Phone: x36680
Office hours: Wednesdays 2–3 p.m.

Course website: `http://learn.uwaterloo.ca`, look for CO 485/CO 685 - Fall 2012.

Prerequisites (CO 485 only). One of PMATH 334, 336, 345, 346. Cumulative overall average of at least 80%.

Course Outline. An in-depth study of public-key cryptography and number-theoretic problems related to the efficient and secure use of public-key cryptographic schemes. Topics to be covered will be drawn from the following list.

- *Algorithmic number theory*: primality testing, integer factorization problem, discrete logarithm problem, elliptic curve discrete logarithm problem.
- *Public-key encryption*: RSA, ElGamal.
- *Signature schemes*: RSA, Schnorr, ECDSA.
- *Key establishment*: Diffie-Hellman and variants.
- *Pairing-based cryptography*: Bilinear pairings, identity-based encryption.
- *Provable security*: Security definitions, security models, security proofs.

CO 485/685 has only little overlap with CO 487 (Applied Cryptography) and CS 758 (Cryptography/Network Security), which are offered in the Winter semester.

References. The course textbook is:

- J. Hoffstein, J. Pipher, and J. Silverman, *An Introduction to Mathematical Cryptography*, Springer-Verlag, QA268.H64 2008 (available online via `http://lib.uwaterloo.ca/`).

You might also find the following books interesting or useful.

- D.R. Stinson, *Cryptography: Theory and Practice*, 3^{rd} Edition, CRC Press, QA268.S75 2006.
- N. Koblitz, *A Course in Number Theory and Cryptography*, Springer-Verlag, 2nd edition, QA241.K672 1994.
- E. Bach and J. Shallit, *Algorithmic Number Theory, Volume I: Efficient Algorithms*, MIT Press, QA241.B1085 1996.
- R. Crandall and C. Pomerance, *Prime Numbers. A Computational Perspective*, Springer, 2nd edition, 2008.
- J. Buchmann, *Introduction to Cryptography*, Springer-Verlag, QA268.B83 2004.

Copies of these books have been placed on reserve in the Davis Centre Library.

Lecture Summaries. Lecture summaries (keywords only) will be posted on the course website on a weekly basis.

Assignments. There will be four assignments to be handed in. Assignments are to be handed in to the instructor on their due date **before** the lecture. The assignments and their solutions will be posted on the course website. Students are expected to do the assignments on their own.

Midterm test. The midterm test is on **Thursday, Oct 18, 2012, 2:30–4p.m.**

Project. Students of CO 685 will need to do a written project report. Details will be issued in early October.

Discussion Board. There is a discussion board on the Piazza site, see `piazza.com/uwaterloo.ca/fall2012/co485685`. The instructor will visit the board on a regular basis and will try to answer course-related questions in a timely manner. Note that it is not acceptable to discuss the assignments on any other discussion board, and solutions to questions must not be discussed on the Piazza site prior to an assignment's due date.

Marking scheme.

	CO 485	**CO 685**
Assignments (4):	30%	20%
Midterm test:	20%	15%
Final exam:	50%	35%
Written project:	—	30%

Policy on INC Grades. A grade of INC (incomplete) will be only awarded to students who cannot write the final exam for reasons acceptable to the instructor, such as a medical certificate by a recognized medical professional. In addition such students need to be in good standing prior to the final exam. To be in good standing a student must

- achieve a passing grade in the assignments,
- write and pass the midterm exam, and
- attend classes regularly.

Academic Integrity. In order to maintain a culture of academic integrity, members of the University of Waterloo community are expected to promote honesty, trust, fairness, respect and responsibility.
Check the details under 'Academic Integrity' under Course Information on the course website. (Just under 'Course Outline').

Note for students with disabilities. The Office for Persons with Disabilities (OPD), located in Needles Hall, Room 1132, collaborates with all academic departments to arrange appropriate accommodations for students with disabilities without compromising the academic integrity of the curriculum. If you require academic accommodations to lessen the impact of your disability, please register with the OPD at the beginning of each academic term.