CO 485/685: The Mathematics of Public-Key Cryptography **Fall 2009**

Instructor: **David Jao**
djao@math.uwaterloo.ca
Office: MC 5038
Phone: x32493
Office hours: WTh 3:00–4:00
http://www.math.uwaterloo.ca/~djao/

Lectures: MWF 1:30–2:30 in DWE 3519

Prerequisites. Math 135, Math 235, Stat 230, and a course in abstract algebra (e.g. PMath 334 or PMath 336). CO 485/685 has only very little overlap with CO 487 (Applied Cryptography) and CS 758 (Cryptography/Network Security), which are offered in the Winter semester.

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.

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*, 3rd 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.
- J. Buchmann, *Introduction to Cryptography*, Springer-Verlag, QA268.B83 2004.

Copies of these books have been placed on reserve in the Davis Centre Library. Additional reading material and notes will be made available throughout the semester.

Marking scheme	**CO 485**	**CO 685**
Assignments:	30%	20%
Midterm exam:	20%	15%
Final exam:	50%	35%
Written project:	—	30%

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 `http://www.uwaterloo.ca/academicintegrity/` for more information.]

Grievance. A student who believes that a decision affecting some aspect of his/her university life has been unfair or unreasonable may have grounds for initiating a grievance. Read Policy 70, Student Petitions and Grievances, Section 4, `http://www.adm.uwaterloo.ca/infosec/Policies/policy70.htm`. When in doubt please be certain to contact the department's administrative assistant who will provide further assistance.

Discipline. A student is expected to know what constitutes academic integrity to avoid committing academic offenses and to take responsibility for his/her actions. A student who is unsure whether an action constitutes an offense, or who needs help in learning how to avoid offenses (e.g., plagiarism, cheating) or about "rules" for group work/collaboration should seek guidance from the course professor, academic advisor, or the undergraduate associate dean. For information on categories of offenses and types of penalties, students should refer to Policy 71, Student Discipline, `http://www.adm.uwaterloo.ca/infosec/Policies/policy71.htm`.
For typical penalties check Guidelines for the Assessment of Penalties,
`http://www.adm.uwaterloo.ca/infosec/guidelines/penaltyguidelines.htm`.

Appeals. A decision made or penalty imposed under Policy 70, Student Petitions and Grievances (other than a petition) or Policy 71, Student Discipline may be appealed if there is a ground. A student who believes he/she has a ground for an appeal should refer to Policy 72, Student Appeals, `http://www.adm.uwaterloo.ca/infosec/Policies/policy72.htm`.

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.