C&O 487/687: APPLIED CRYPTOGRAPHY **Winter 2013**

INSTRUCTOR: **David Jao**
Office: MC 5038, email: djao@uwaterloo.ca
Office hours: Tuesday 12:30pm–1:30pm, Wednesday 2:00pm–3:00pm

TEACHING ASSISTANTS: **Gabriel Gauthier**, `g3gauthi`, MC 6093, Office hours: Friday 2:30pm–4:30pm
Yik-Siong Kok, `yskok`, MC 5147, Office hours: Wednesday 3:00pm–4:00pm
Brandon Weir, `bweir`, MC 5161, Office hours: Thursday 4:30–5:30pm

WEB PAGE: `http://www.math.uwaterloo.ca/~djao/co487/`
The web page contains basic administrative information. Course materials such as slides and notes, assignments and handouts, lecture summaries, and references will be posted on LEARN (`http://learn.uwaterloo.ca`).

PREREQUISITES: MATH 135, STAT 230, and 3rd-year standing or higher. It is assumed that you know all the elementary number theory from Math 135 (divisibility, greatest common divisors, Extended Euclidean algorithm, prime numbers, Fermat's Little Theorem, congruences, the integers modulo n, finding inverses modulo n, Chinese Remainder Theorem, ...).

COURSE OUTLINE: Cryptography is concerned with the mathematical, algorithmic, and implementational aspects of information security. It is one of the core technologies for securing the emerging information infrastructure. Its applications range from (conceptually) simple tasks such as encryption, authentication, and key management to sophisticated tasks such as Internet security, electronic cash payments, and electronic voting.

This course is a comprehensive introduction to modern cryptography that is aimed primarily at those interested in applications. The topics discussed will include an introduction to classical cryptography: encryption algorithms, hash functions, and message authentication codes. In the area of public-key cryptography, topics will include an overview of specific systems (Diffie-Hellman, RSA, DSA, etc.) and a few advanced protocols. The security of these schemes and the use of public-key techniques for generating digital signatures will be described. An emphasis will be placed on tools that are currently being used to secure the Internet and enable secure electronic commerce.

Topics to be covered will be drawn from the following partial list.

- *Symmetric-key encryption*: Classical ciphers, one-time pad, stream ciphers (RC4), Feistel networks, DES, AES, modes of operation.
- *Hash functions and data integrity*: Hash functions (SHA-1), parallel collision search, message authentication codes (CBC-MAC, HMAC).
- *Public-key encryption*: RSA, ElGamal, Elliptic curves.
- *Signature schemes*: RSA, DSA, ECDSA.
- *Key establishment*: Key transport and key agreement, symmetric and asymmetric techniques.
- *Pseudorandom bit generation*: Random numbers, cryptographically strong pseudorandom bit generators.
- *Key management*: Merkle authentication trees, certification authorities, public-key infrastructures.
- *Deployed cryptography*: Kerberos, Pretty Good Privacy (PGP), Secure Sockets Layer (SSL and TLS), IPsec, IEEE 802.11, Clipper chip, privacy-enhancing technologies, digital payment systems (SET, anonymous cash, micropayments).

COURSE TEXTBOOKS (OPTIONAL): The material covered in this course is rather broad, and we will not have the chance to study any topic in great depth. The following books are good sources of supplementary information for the material covered in class. Copies of these books have been placed on 3-hour reserve in the Davis Centre Library.

- A. Menezes, P. van Oorschot and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997. Available online at `http://www.cacr.math.uwaterloo.ca/hac/`.
- D. Stinson, *Cryptography—Theory and Practice*, 3rd edition, CRC Press, 2006. QA268.S75 2006.
- B. Schneier, *Applied Cryptography*, Wiley, 2nd edition, 1996. QA76.9.A25.S35.
- W. Stallings, *Cryptography and Network Security: Principles and Practice*, Prentice-Hall, 4th edition, 2003. TK5105.59.S713.

EVALUATION

Assignments:	30%
Midterm test:	20%
Final exam:	50%

POLICIES

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.
