CO 487/687: APPLIED CRYPTOGRAPHY — Winter 2019

(Updated on Jan 9 with the Math Faculty's statement on mental health (#16) and diversity (#17).

INSTRUCTOR: Alfred Menezes

Email: ajmeneze@uwaterloo.ca
Office hours: Monday 2:30–5:30 pm (MC 5026)
Wednesday 2:30–5:30 pm (MC 5026)

TEACHING ASSISTANTS: (Office hours will be listed on the assignments)

Sam Jaques
Christopher Leonardi (MC 5494)
Luis Ruiz-Lopez (MC 5486)
Caelan Wang (MC 6313)
Elena Bakos Lang (MC 5474)
Mary Kate MacPherson (MC 5481)
Alexander Stoll (MC 6022)
Sam Winnick (QNC 0204)

WEB PAGE: `learn.uwaterloo.ca`
The course web page will contain slides; assignments and solutions; handouts; and references for required, recommended and optional readings.

PIAZZA: `piazza.com`
You are encouraged to use Piazza to discuss the course material.

PREREQUISITES: MATH 135, STAT 230, and 3rd-year standing or higher. I will assume 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, and the Chinese Remainder Theorem). A handout that summarizes this material is available on the course web site.

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, electronic voting, and secure cloud computing.

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 symmetric-key cryptography: encryption algorithms, hash functions, and message authentication codes. In the area of public-key cryptography, topics will include an overview of RSA and elliptic curve cryptography (ECC) 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 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, SHA-2), parallel collision search, message authentication codes (CBC-MAC, HMAC).
- *Authenticated encryption*: Encrypt-then-MAC, AES-GCM.
- *Public-key encryption*: RSA, elliptic curves.
- *Signature schemes*: RSA, ECDSA, quantum-safe signature schemes.

- *Key establishment*: Elliptic curve Diffie-Hellman key agreement.
- *Key management*: Certification authorities, public-key infrastructures.
- *Deployed cryptography*: IEEE 802.11 WEP, IEEE 802.11 WPA2, Secure Sockets Layer (SSL/TLS), Google's Key Management Service, cryptocurrencies (Bitcoin), Fast IDentity Online (FIDO), Signal protocol (WhatsApp), privacy-enhancing technologies (Tor, OTR).

EVALUATION

CO 487		**CO 687**	
Assignments (5):	25%	Assignments (5):	25%
Midterm test:	25% (6:30-8:00 pm, March 8, Friday)	Midterm test:	20%
Final exam:	50% (TBA)	Final exam:	35%
		Project:	20%

Note that assignments are not weighted equally. The total marks received on assignments will be added at the end of the course.
Grades for CO 487 students will be computed using the formula

$$\text{Final grade} = \text{MAX}(0.25 * A + 0.25 * M + 0.5 * F,\ \ 0.25 * A + 0.10 * M + 0.65 * F).$$

There is no requirement to pass the midterm test and/or final exam in order to pass the course.

COURSE TEXTBOOKS (OPTIONAL): The material covered in this course is rather broad, so we will not have the opportunity to study any topic in great depth. The following books are good sources of supplementary information for the material covered in class. The web site provide suggestions for *required*, *recommended* and *optional* readings from the first book.

- C. Paar and J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*, Springer, 2009.

  Available for free download from the UW library website: `tinyurl.com/PaarPelzl`. Recommended readings from this book are provided on the course website.

- A. Menezes, P. van Oorschot and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

  Available for free download from `cacr.uwaterloo.ca/hac/`. An extensive reference book on cryptography. Out-dated, but a useful reference for older material. The presentation is terse and there are no exercises or proofs.

CROWDMARK: Assignments will be submitted using Crowdmark. The assignments will be due at **3:00 pm** on Jan 25 (Fri), Feb 8 (Fri), Mar 1 (Fri), Mar 22 (Fri), and Apr 5 (Fri). Further instructions will be included with Assignment #1.

POLICIES

1. **Attendance**. Since lectures will *not* follow the optional textbook(s) very closely, you are *strongly* encouraged to attend all lectures.
2. **Class etiquette**. Out of courtesy to your classmates, please refrain from talking during class. If you have any questions about the lecture, you can ask me during class, or after class, or during my office hours, or on Piazza.

3. **Class etiquette**. Out of courtesy to your classmates, *please arrive to class on time* and please do not leave class until I have finished lecturing. (Exceptions for emergency situations are permitted, of course!)
4. **Office hours**. Please make use of TA and instructor office hours and Piazza throughout the semester. Besides asking for assistance on assignment problems, you should use office hours to ask questions about the course material and slides and for general discussions on anything related to cryptography and security.
5. **Email queries**. Please restrict your email queries to questions that have short (e.g., YES/NO) answers. Questions that may have longer answers are best handled in person during office hours or on Piazza. I will also generally be available to answer your questions immediately after class.
6. **Readings**. I will provide numerous suggestions for *required*, *recommended* and *optional* readings on the course website. You are encouraged (but not required) to do the recommended readings in order to supplement the class notes. If you would like to learn more about a topic covered in class, please ask me to provide additional optional readings. For the midterm and final exam, you will be responsible for all material covered in class, and for all the required readings. You will *not* be responsible for recommended and optional readings.
7. **Collaboration on assignments**. You are welcome to collaborate on assignments with other students presently enrolled in CO 487. However, *solutions must be written up by yourself.* If you do collaborate, please *acknowledge your collaborators* in the write-up for each problem. *If you obtain a solution with help from a book, research paper, a website, or elsewhere, please acknowledge your source.* **You are not permitted to solicit help from online bulletin boards, chat groups, newsgroups, or solutions from previous offerings of the course.**
8. **Assignment deadlines**. Late assignments will *not* be accepted except in *very* special circumstances (usually a documented illness of a serious nature). High workloads because of midterms and assignments in other courses will *not* qualify as a special circumstance.
9. **Exams**. This course is not a traditional textbook course. That is, lectures will not closely follow any textbook, and much of the material covered will not be testable. There are no good sources of practice problems, as a result of which the content of exams does not have a predictable pattern. In addition to technical questions, there will be many short-answer questions on exams that will require you to clearly and concisely explain some concepts. These questions will test your ability to identify the important concepts introduced in lectures, and your understanding of them. (In contrast, assignment questions will only cover the technical aspects of the course.) A midterm test and a final exam from past offerings of the course are available on the course website.
10. **Grade appeals**. If you have any concerns with the marking of assignment or midterm questions, please send me an email together with a *clear* description of your appeal(s). If your marked assignment/midterm was returned to you on day X, then you should email appeals to me by the end of day $X + 7$ (and no later). Solutions to assignments will be posted on the course website shortly after the assignment submission deadline.
11. **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 uwaterloo.ca/academic-integrity/ for more information.]
12. **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, `tinyurl.com/UWPolicy70`. When in doubt please be certain to contact the department's administrative assistant who will provide further assistance.
13. **Discipline**. A student is expected to know what constitutes academic integrity [check uwaterloo.ca/academic-integrity/] to avoid committing an academic offence, and to take responsibility for

his/her actions. A student who is unsure whether an action constitutes an offence, or who needs help in learning how to avoid offences (e.g., plagiarism, cheating) or about "rules" for group work/collaboration should seek guidance from the course instructor, academic advisor, or the undergraduate Associate Dean. For information on categories of offences and types of penalties, students should refer to Policy 71, Student Discipline, `tinyurl.com/UWPolicy71`. For typical penalties check Guidelines for the Assessment of Penalties, `tinyurl.com/UWPenalties`.

14. **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) `tinyurl.com/UWPolicy72`.
15. **Note for students with disabilities**. AccessAbility Services (uwaterloo.ca/accessability-services/), located in Needles Hall, Room 1401, 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 AccessAbility Services at the beginning of each academic term.
16. **Mental Health**. If you or anyone you know experiences any academic stress, difficult life events, or feelings like anxiety or depression, we strongly encourage you to seek support.

    On-campus Resources

    - Campus Wellness: https://uwaterloo.ca/campus-wellness/
    - Counselling Services: counselling.services@uwaterloo.ca / 519-888-4567 ext 32655 / Needles Hall North 2nd floor, (NH 2401)
    - MATES: one-to-one peer support program offered by Federation of Students (FEDS) and Counselling Services:mates@uwaterloo.ca
    - Health Services service: located across the creek from Student Life Centre,519-888-4096.

    Off-campus Resources

    - Good2Talk (24/7): Free confidential help line for post-secondary students. Phone: 1-866-925-5454
    - Here 24/7: Mental Health and Crisis Service Team. Phone: 1-844-437-3247
    - OK2BME: set of support services for lesbian, gay, bisexual, transgender or questioning teens in Waterloo. Phone: 519-884-0000 extension 213
17. **Diversity**. It is our intent that students from all diverse backgrounds and perspectives be well served by this course, and that students' learning needs be addressed both in and out of class. We recognize the immense value of the diversity in identities, perspectives, and contributions that students bring, and the benefit it has on our educational environment.Your suggestions are encouraged and appreciated. Please let us know ways to improve the effectiveness of the course for you personally or for other students or student groups. In particular:

    - We will gladly honour your request to address you by an alternate/preferred name or gender pronoun. Please advise us of this preference early in the semester so we may make appropriate changes to our records.
    - We will honour your religious holidays and celebrations. Please inform of us these at the start of the course.
    - We will follow AccessAbility Services guidelines and protocols on how to best support students with different learning needs.