CO 487/687: APPLIED CRYPTOGRAPHY — Winter 2021

INSTRUCTOR:

Alfred Menezes, Email: ajmeneze@uwaterloo.ca
Office hours: Please see LEARN and the Assignments.

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

Valerie Gilchrist (vgilchri)
Elvis Iam (hciam)
Mary Kate MacPherson (mkmacphe)
Connor Paul-Paddock (cpaulpad)
Matthew Sullivan (m8sulliv)
Philip Hodges (pwhodges)
Andrew Jena (ajjena)
Kazuhiro Nomoto (knomoto)
Evelyne Smith-Roberge (e2smithr)

WEB PAGE: `learn.uwaterloo.ca`
The course web page will contain video lectures; slides; assignments and solutions; handouts; optional readings; and quizzes.

LECTURES: Video lectures for the week will be posted on LEARN by 7:00 pm each Sunday.

PIAZZA: PASSWORD:
You are encouraged to use Piazza to ask questions about the video lectures and to discuss the course material. *You may ask for general clarification about assignment questions. However, please do not discuss solutions to assignment questions on Piazza, or make posts that reveal part of a solution.* In particular, please do not ask for hints of Pizza. Instead, please see the instructor or one of the TAs during their office hours.

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.

SYLLABUS: 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, secure messaging, secure cloud computing, and electronic cash payments.

This course is a comprehensive introduction to modern cryptography that is aimed primarily at those interested in applications. An emphasis will be placed on tools that are currently being used to secure the Internet and enable secure electronic commerce. The following topics will be covered:

- *Symmetric-key encryption*: Classical ciphers, one-time pad, stream ciphers (RC4, ChaCha20), block ciphers (Triple-DES, AES), modes of operation.
- *Hash functions and data integrity*: Hash functions (SHA256), 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 (ECDH).
- *Key management*: Certification authorities, public-key infrastructures.

- *Deployed cryptography*: IEEE 802.11 WEP, IEEE 802.11 WPA2, Google's Key Management Service, GSM security, FIDO Universal 2nd Factor Authentication (U2F), Transport Layer Security (TLS), Bluetooth security, Signal protocol (WhatsApp), cryptocurrencies (Bitcoin).

LEARNING OUTCOMES: On successful completion of this course, students will:

1. Understand the fundamental cryptographic tools of symmetric-key encryption, message authentication, authenticated encryption, hash functions, public-key encryption, and signatures;
2. Appreciate the challenges with assessing the security of these tools;
3. Gain exposure to how these cryptographic tools are used to secure large-scale applications;
4. Understand why key management is an essential process that underpins the security of many applications.

EVALUATION

Assignments (5):	50%	Due dates: **11:30 am** on Jan 29, Feb 12, Mar 5, Mar 26, Apr 9
Quizzes (2) :	15% or 7.5% or 0%	Feb 26, Mar 19
Final assessment:	35% or 42.5% or 50%	Date: TBD

Notes:

1. Assignments will be submitted using Crowdmark.
2. *Assignments are not weighted equally.* The total marks received on assignments will be added at the end of the course.
3. The five assignments are due at 11:30 am on the stated Friday. However, if you are pressed for time, you can take advantage of the following deadline extensions (without penalty):
   - Assignment #1: Jan 29 (11:30 am) $\longrightarrow$ Jan 30 (1:00 pm).
   - Assignment #2: Feb 12 (11:30 am) $\longrightarrow$ Feb 16 (1:00 pm).
   - Assignment #3: Mar 5 (11:30 am) $\longrightarrow$ Mar 6 (1:00 pm).
   - Assignment #4: Mar 26 (11:30 am) $\longrightarrow$ Mar 27 (1:00 pm).
   - Assignment #5: Apr 9 (11:30 am) $\longrightarrow$ TBD.
4. The two quizzes, which are in lieu of a midterm test, will be administered via LEARN, and will be time-limited. The questions will be of the following kind: multiple choice, True/False, fill in the blanks, short answers. The quizzes will be open book (but not open internet). Further instructions will be provided later in the course.
5. The date for the final assessment will be set by the Registrar's Office. The final assessment will be open book (but not open internet), and will be time-limited. Further instructions will be provided later in the course.
6. Your lowest and second lowest quiz marks will be replaced by your final assessment mark, if either of the quiz marks is lower than the final assessment mark. So, in principle, you have the option of not attempting quizzes without penalty. However, you are discouraged from exercising this option since the final assessment is expected to be significantly more challenging than the quizzes.
7. There is no requirement to pass the final assessment in order to pass the course.
8. I will not be using any kind of proctoring software for the quizzes and the final assessment.

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 *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:
  `http://www.springer.com.proxy.lib.uwaterloo.ca/gp/book/9783642041006`.
  Optional 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 `http://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.

POLICIES

1. **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 video lectures and course material and for general discussions on anything related to cryptography and security.
2. **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.
3. **Readings**. I will provide some suggestions for *optional* readings on the course website. These readings supplement the lectures and slides. If you would like to learn more about a topic covered in class, please ask me to provide additional optional readings. For the quizzes and final assessment, you will be responsible for all material covered in lectures. You will *not* be responsible for any of the optional readings.
4. **Collaboration on assignments**.

   One or two questions on each assignment will permit no collaboration of any kind; more details will be provided on the assignment. For the remaining questions, you are welcome (and encouraged) to collaborate on assignments with other students presently enrolled in CO 487. However, *solutions must be written up by yourself.* If you do collaborate, you must *acknowledge your collaborators in the write-up for each problem.* You are *not* permitted to solicit help from websites such as Course Hero and Chegg, online discussion groups, or solutions from previous offerings of the course.

5. **Assignment deadlines**. The material for each assignment problem will be covered well in advance of the assignment due date, so you will have adequate time to work on assignment problems. 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.
6. **Grade appeals**. If you have any concerns with the marking of assignment questions, please send me an email together with a *clear and detialed* description of your appeal(s). If your marked assignment 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.

7. **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://uwaterloo.ca/academic-integrity/` for more information.]
8. **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://tinyurl.com/UWPolicy70`. When in doubt please be certain to contact the department's administrative assistant who will provide further assistance.
9. **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, `http://tinyurl.com/UWPolicy71`. For typical penalties check Guidelines for the Assessment of Penalties, `http://tinyurl.com/UWPenalties`.
10. **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://tinyurl.com/UWpolicy72`.
11. **Note for students with disabilities**. AccessAbility Services, located in Needles Hall, Room 1401 (`http://uwaterloo.ca/accessability-services/`), 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.
12. **Mental Health Support**. The Faculty of Math encourages students to seek out mental health support if needed.

    On-campus Resources

    - Campus Wellness: `https://uwaterloo.ca/campus-wellness/`
    - Counselling Services: counselling.services@uwaterloo.ca / 519-888-4567 ext 32655.
    - 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
13. **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 us of 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.
