LASSONDE SCHOOL OF ENGINEERING | YORK U

Electrical Engineering and Computer Science

EECS3481 – Applied Cryptography

Ruba Al Omari

Fall 2024

1. Important Dates

Classes Start	Classes End	Last day to drop a course without receiving a grade	Fall Study Day (No classes)	Final Exam Period
Sept. 4, 2024	Dec. 3, 2024	Nov. 8, 2024	Dec. 4, 2024	Dec. 5-20, 2024

2. Course Schedule

Type	Day	Time	Location	Cat #
Lecture	Tuesday Thursday	2:30 pm – 4:00 pm	DB 0005 Keele	K10W01

3. Instructor Contact Information & Office Hours

Instructor Name	Office	Office Hour (Starting Week 2)	Email
Ruba Alomari	Lassonde 2013	Thursdays 4:15-5:15 PM	alomari@yorku.ca

Laboratory/Teaching Assistant Name	Office	Office Hour	Email

4. Course Description:

An overview of cryptographic algorithms and the main cryptosystems in use today, emphasizing the application of cryptographic algorithms to designing secure protocols.

Topics covered include:

1) Foundation: Security goals, the communication model, and classification of attacks.
2) Classical Cryptography: Classical ciphers, diffuse and confuse, information theory and entropy, and cryptanalysis.
3) Symmetric Cryptography: Perfect secrecy, block and stream ciphers, random number generation, and key distribution.
4) Asymmetric Cryptography: Public/private key pairs, primality testing, and key pair generation.
5) Cryptographic Hash Functions: Properties and construction methods; message integrity; digest, MAC, and signatures.
6) Selected Topics (If time permits): Key Distribution, and Quantum Cryptography.

5. Expected Learning Outcomes

By the end of the course, the students are expected to be able to:

1) Explain the workings of fundamental cryptographic algorithms in classical, symmetric, and asymmetric settings, and apply them programmatically.
2) Attack a given communication pattern using exhaustive as well as cryptanalytic techniques such as meet-in-the-middle, man-in-the-middle, or birthday, or by exploiting an algorithmic vulnerability.
3) Analyze a given communication pattern to achieve a certain security goal by identifying vulnerabilities, threats, and risks, and recommending hardening mechanisms.
4) Apply cryptographic primitives in advanced settings such as secret sharing, zero-knowledge, and key distribution.
5) Discuss the impact of advances in computing power, algorithm complexities, and quantum computing, on the strength of cryptographic algorithms.

6. Required Textbook/Readings

- Cryptography and Network Security: Principles and Practice by William Stallings, 8th Edition, Pearson (2019). Author website: http://williamstallings.com/Cryptography/

Recommended:

- Internet Security: A Hands-on Approach (3rd ed., 2022), by Wenliang Du, ISBN: 978-17330039-6-4.

Additional readings may be assigned or recommended during the course.

7. Schedule

Week	Week Of	Tue	Thu	Topics	Readings*
1	Sept. 2	–	Lecture	**About Cryptography**	Ch. 1 & 2
2	Sept. 9	Lecture	Lecture	**Classical Cryptography** Foundational Concepts and Techniques	Ch. 3
3	Sept. 16	Lecture	Lecture		
4	Sept. 23	Lecture	Lecture	**Symmetric Cryptography** Stream & Block Ciphers The Unbreakable Cipher: OTP	Ch. 4, 6, 7 & 8
5	Sept. 30	Lecture	Lecture		
6	Oct. 7	Lecture	Lecture		
	Oct. 14-Oct. 18	Reading Week – No Classes			
7	Oct. 21	Lecture	**Test # 1**	**Asymmetric Cryptography** Primality & Factoring Public Key Infrastructure	Ch. 9 & 10
8	Oct. 28	Lecture	Lecture		
9	Nov. 4	Lecture	Lecture	**Hash Functions** Digital Signatures Authentication	Ch. 11, 12, & 13
10	Nov. 11	Lecture	Lecture		
11	Nov. 18	Lecture	Lecture	**Selected Topics** Key Management Quantum Cryptography	Ch. 14
12	Nov. 25	Lecture	**Test # 2**		
13	Dec. 2	Lecture	–		
	Dec. 4	Fall Study Day – No Classes			

* All chapters refer to the Cryptography and Network Security textbook.

8. Assessment

- Assessment is based on two assignments, two tests, and a final exam with weights as follows:

    - **20% - Assignments 1 & 2 @10%**
      Each is due as shown in its document.
    - **40% - Tests 1 & 2 @20%**
      Dates specified in the schedule section.
    - **40% Final Exam**
      Scheduled by the registrar's office.

- The default and only acceptable way of submission for assessments in this course is through e-class, unless otherwise specified. Email submissions are void for all assessments.
- The weight of any missed work is transferred to the final exam.
- Conversion of the overall numeric mark to a letter grade:

F	E	D	D+	C	C+	B	B+	A	A+
<40	>= 40	>= 50	>= 55	>= 60	>= 65	>= 70	>= 75	>= 80	>= 90

For a full description of York grading system see the York University Undergraduate Calendar - https://calendars.students.yorku.ca/2022-2023/grades-and-grading-schemes

Student Expectations & Course-Specific Policies

9. Missed Assessments

Students who miss the due date for assignments 1 or 2, can still submit within 48 hours with a 25% late submission penalty. Students who fail to submit within 48 hours, must submit a request for consideration with supporting documentation to the instructor in writing within 3 days of the missed assignment (late submission penalty still applies).

Students who miss the midterm must submit a request for consideration with supporting documentation to the instructor in writing within 5 days of the missed midterm.

For missed final exams, students must submit a petition through the department to write a deferred exam.

If a student misses coursework and does not follow the procedures listed above, the student will receive zero marks for the missed coursework.

11. Grade Appeals

If you believe there is an error, follow the instructions in the test results announcement on submitting a reappraisal request online. It is essential that you present logical arguments as to why the work should be re-marked; otherwise, it will not. Note that the entire work will be re-marked, and your mark may be increased or decreased, or it may stay unchanged. Note also that the deadline for re-marking is **5 business days** after the marks are posted. No re-marking request will be considered after that deadline.

12. Asking Questions

1. Use the course forum to ask any course-related questions. This is the best and fastest way to get answers. You are also encouraged to answer posted questions as this is a great way to learn. To use the forum, you must adhere to the **forum protocol**:

    - Do not ask a question that has already been asked or whose answer has already been posted. To that end, use the search facility to look for keywords related to your question.
    - Be clear and specific. This applies to the post title as well as to its body. For example, "Please Help" is not a good title, and "My code is not working" is not useful --instead, provide the exception message and the code.
    - Do not mix topics. If while answering a question, you think of a different question, then post it in a separate topic.
    - Be professional in terms of language and tone.

2. For questions related to private matters requiring confidentiality, either use my office hour or send me an email (alomari@yorku.ca). The **email protocol** is as follows:

    - Put "EECS 3481/X" in the subject line where X is your PPY (Passport York) username.
    - Include your full name in the message body. Do not include your York ID.
    - Email messages not meeting these guidelines, or not requiring confidentiality, will **not** be answered.

13. Recording

Students may **not** record any portion of a lecture, class discussion, or other learning activity without the prior knowledge and written consent of the instructor.

14. Academic Honesty Policy

Students are expected to act with integrity. For assignments, projects, and activities, students may discuss the questions with others, may ask questions on forums, and may look for ideas online, but once they understand the approach, they must compose and submit their own answers. By submitting any assessment, you acknowledge that you are

aware of these rules and that we may enforce them in a variety of ways; e.g., monitor network traffic, use video cameras, mine for patterns, administer multiple versions, etc. Violators (whether committing or aiding) will be charged with academic dishonesty whose penalty may reach expulsion from the University.

Students are expected to read and understand the **Senate Policy on Academic Honesty** available at https://www.yorku.ca/secretariat/policies/policies/academic-honesty-senate-policy-on/

and **Academic Conduct Policy and Procedures** available at https://www.yorku.ca/secretariat/policies/policies/academic-conduct-policy-and-procedures/

Note that if the links are not active, you can google "Senate Policy on Academic Honesty York University" and "Academic Conduct Policy and Procedures" to find an alternate link.

15. Access/Disability

York University is committed to principles of respect, inclusion, and equality of all persons with disabilities across campus. The University provides services for students with disabilities (including physical, medical, learning, and psychiatric disabilities) needing accommodation related to teaching and evaluation methods/materials. These services are made available to students in all Faculties and programs at York University. Students in need of these services are asked to register with disability services as early as possible to ensure that appropriate academic accommodation can be provided with advance notice. You are encouraged to schedule a time early in the term to meet with each professor to discuss your accommodation needs. Please note that registering with disabilities services and discussing your needs with your professors is necessary to avoid any impediment to receiving the necessary academic accommodations to meet your needs.

To learn more about academic accommodation for students with disabilities policy visit: https://www.yorku.ca/secretariat/policies/policies/academic-accommodation-for-students-with-disabilities-policy/ and Counseling and Disability Services available at https://accessibility.students.yorku.ca/

16. York University's Support and Policy on Sexual Violence

The Centre for Sexual Violence Response, Support, and Education is the University office with the primary responsibility to assist community members affected by sexual violence. The Centre coordinates support and resources for those who have experienced sexual violence, receives disclosures and complaints, facilitates safety planning, and assists survivors through the complaint process.

To learn more about York University Policy on Sexual Violence, and existing Supports and Services for Students, visit https://www.yorku.ca/secretariat/policies/policies/sexual-violence-policy-on/

17. Copyright

Course materials are designed for use only in the course. Copying this material for distribution (e.g., uploading material to a commercial third-party website) may lead to a charge of misconduct under York's Code of Student Rights and Responsibilities and the Senate Policy on Academic Honesty and/or legal consequences if copyright law has been violated http://www.copyright.info.yorku.ca

18. Campus Policies

- Academic Integrity: http://www.yorku.ca/academicintegrity
- Student Code of Rights and Responsibilities: https://calendars.students.yorku.ca/2022-2023/code-of-student-rights-and-responsibilities
- Accommodations for Students with Disabilities: https://calendars.students.yorku.ca/2022-2023/academic-accommodation-for-students-with-disabilities
- Academic Policies and Regulations: https://calendars.students.yorku.ca/2022-2023/policies-and-regulations
- Ethics review process for research involving human participants: https://www.yorku.ca/research/research-ethics /
- Student conduct standards: https://calendars.students.yorku.ca/2022-2023/student-conduct-and-responsibilities
- Religious Accommodation: https://calendars.students.yorku.ca/2022-2023/religious-accommodation

19. Computer Session Monitoring During Labtest:

Labtest will be used when writing tests and exams in this course. Please ensure to read the disclaimer available at this link prior to writing your test: https://www.eecs.yorku.ca/teaching/docs/disclaimer-labtest-monitoring.pdf

Note that this monitoring is only being done during in-lab labtest, and only on department owned equipment (never on student personal equipment such as their desktops or laptops).

Students can email their concerns to: Tech support (tech@eecs.yorku.ca), undergraduate program director, Gene Cheung (genec@yorku.ca), or Lassonde's Associate Dean of Students, Mitchell Burnie (mitch.burnie@lassonde.yorku.ca)

DISCLAIMER: Computer Session Monitoring during Labtests

This disclaimer serves to inform all students participating in in-lab tests (labtests) that electronic proctoring may occur, and their computer session may be monitored by their instructor. By accessing and utilizing labtest, you acknowledge and accept the following terms and conditions: **1. Purpose of electronic proctoring:** The monitoring of computer sessions during labtest is carried out for the purpose of maintaining academic integrity, ensuring fairness in assessment, enabling electronic communication between students and instructors, and promoting a conducive learning environment.

2. Academic Integrity: Clear instructions and access to approved materials for the test are provided. The monitoring process aims to deter and detect any unauthorized activities that may compromise the integrity of the examination or violate Senate policy.

3. Remote Troubleshooting: In the event of technical difficulties or disruptions encountered during the labtest, authorized personnel may access and monitor your computer session to provide remote troubleshooting support, address technical issues promptly, and minimize any potential interruptions to your labtest experience.

4. Maintenance and Security: Monitoring may be conducted for the purposes of system maintenance, ensuring the security of the testing platform, and identifying and mitigating any potential vulnerabilities or threats.

5. Confidentiality and Data Protection: All monitoring activities will be carried out in accordance with applicable privacy laws and regulations.

6. Legal Compliance: By accessing and participating in computer-based tests, you agree to comply with all relevant laws, regulations, institutional policies, and codes of conduct. Failure to comply may result in disciplinary action, including but not limited to the nullification of test scores, academic penalties, or other appropriate consequences as determined by the Lassonde School of Engineering.

7. Liability Disclaimer: The educational institution and its authorized personnel shall not be held responsible for any technical issues, disruptions, data loss, or any other consequences arising from the monitoring activities conducted during the test.

8. Acceptance: By proceeding to use labtest, you acknowledge that you have read, understood, and agreed to the terms and conditions outlined in this disclaimer. If you have any concerns or questions regarding the monitoring process, please seek clarification from: tech@eecs.yorku.ca .