EXPANDED COURSE DESCRIPTION
ELECTRICAL ENGINEERING AND COMPUTER SCIENCE
Lassonde School of Engineering
Electrical Engineering Computer Science
LE / EECS 3481 3.0 SECTION A
APPLIED CRYPTOGRAPHY
FALL 2018 / WINTER 2019

Last Modified Date: 08/20/2018

COURSE CALENDAR DESCRIPTION
An overview of cryptographic algorithms and the main cryptosystems in use today, emphasizing the application of cryptographic algorithms to designing secure protocols. Prerequisites: cumulative GPA of 4.50 or better over all major EECS courses (without second digit “5”); LE/EECS 2030 3.00 or LE/EECS 1030 3.00; LE/EECS 2011 3.00.

INSTRUCTOR(S)

<table>
<thead>
<tr>
<th>Name</th>
<th>Section / Format / Term</th>
<th>Contact Email</th>
<th>Contact Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Roumani, Hamzeh</td>
<td>Sec. A / LECT / F</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ADDITIONAL INFORMATION
This course provides an overview of cryptographic primitives in the context of computer security and looks at how they are applied to protect communication patterns. The emphasis is on the applied aspects as used in software to protect applications and build secure protocols.

COURSE TOPICS
• Foundation: security goals, the communication model, classification of
• Classical Cryptography: classical ciphers, diffuse and confuse, information theory, and
• Modern Cryptography: modern symmetric ciphers, perfect secrecy, block and stream ciphers, modern asymmetric
• Hash Functions: message integrity, digital signatures, certificate authorities, key distribution
• Advanced topics and applications: May include secret sharing, zero-knowledge proofs, quantum cryptography, and digital

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

RECOMMENDED COURSE RESOURCES
GRADING SCHEME
• 20% - Programming and Subject Test #1
• 30% - Programming and Subject Test #2
• 30% - Programming and Subject Test #3
• 20% - Programming and Subject Test #4

WEEKLY SCHEDULE
1. Crypto Basics
2. Classical Ciphers
3. Cryptanalysis
4. Stream & Block Cipher Information Theory
5. Symmetric Cryptography
6. Authentication & Integrity
7. Asymmetric Cryptography
8. Public Key Generation
9. Cryptographic Hash Functions
10. Cryptographic Protocols I
11. Cryptographic Protocols II
12. Advanced Topics

ACADEMIC INTEGRITY LINKS
• Senate Policy on Academic Honesty - http://secretariat-policies.info.yorku.ca/policies/academic-honesty-senate-policy-on/
• Academic Integrity - http://lassonde.yorku.ca/academic-integrity

STUDENT LINKS
• Student Rights and Responsibilities - http://oscr.students.uit.yorku.ca/student-conduct
• Religious Observance - https://w2prod.sis.yorku.ca/Apps/WebObjects/cdm.woa/wa/regobs
• Academic Accommodation for Students with Disabilities - http://secretariat-policies.info.yorku.ca/policies/academic-accommodation-for-students-with-disabilities-policy/
• Counselling and Disability Services - http://cds.info.yorku.ca/
• York University’s Policies on Sexual Violence - http://secretariat-policies.info.yorku.ca/policies/sexual-violence-policy-on/
• York University’s Policies on Gender/LGBTQ*/Positive Space - http://rights.info.yorku.ca/lgbtq/

LAND ACKNOWLEDGEMENT
• We acknowledge our presence on the traditional territory of many Indigenous Nations. The area known as Tkaronto has been taken by the Anishinabek Nation, the Haudenosaunee Confederacy, the Huron-Wendat, and the Métis. It is now home to many Indigenous Peoples. We acknowledge the current treaty holders, the Mississaugas of the New Credit First Nation. This territory is subject of the Dish With One Spoon Wampum Belt Covenant, an agreement to peacefully share and care for the Great Lakes region.
• The Indigenous Framework for York University: A Guide to Action can be found here: http://indigenous.info.yorku.ca/
• Meaning of a land acknowledgement: http://healthydebate.ca/opinions/indigenous-land-acknowledgements

Many courses utilize Moodle, York University’s course website system. If your course is using Moodle, click here to access it.
Moodle @ York University