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 2019 / WINTER 2020

Last Modified Date: 08/01/2019

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 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

COURSE TOPICS
1. **Foundation** - Security goals, the communication model, 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, key distribution.
4. **Asymmetric Cryptography** - public/private key pairs, primality testing and key pair generation, discrete logs, key agreement protocols.
5. **Cryptographic Hash Functions** - Properties and construction methods; message integrity; digest, MAC, and signatures.
6. **Selected Topics** - May include secret sharing, zero-knowledge proofs, quantum cryptography, and digital cash.

COURSE LEARNING OUTCOMES
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, person 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, quantum key distribution, and digital cash.
5. Discuss the impact of advances in computing power, algorithm complexities, and quantum computing, on the strength of cryptographic algorithms.

COURSE TEXTBOOK
None

RECOMMENDED RESOURCES

COURSE ASSESSMENT
20% - Activities
25% - Test #1
25% - Test #2
30% - Final Exam

ACADEMIC INTEGRITY LINKS
• Senate Policy on Academic Honesty - http://secretariat-policies.info.yorku.ca/policies/academic-honesty SENATE POLICY ON ACAD HONESTY
• 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/
• Student Accessibility Services (SAS) - https://accessibility.students.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 care 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 peaceably 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