ECE/CS 578: Cryptography and Data Security

When: Mondays 6:00 – 8:50 pm, starting August 29
Where: AK 233
Instructor: Thomas Eisenbarth (teisenbarth@wpi.edu), (508) 831-5914; Office: AK 307
TA Contact: Mohit Hopani (mkhapani@wpi.edu)

Course description

This course is an introductory course to modern cryptography and information security. It focuses on *how* cryptographic algorithms and protocols work and how to use them. The course covers the following topics:

1. Principles of cryptography, classical ciphers and general cryptanalysis
2. Symmetric primitives: Modern encryption methods and secure hashing
3. Public key cryptography: Key exchange, asymmetric encryption and digital signatures
4. Advanced applications: protocols, key management and special cryptographic services

Throughout the course we will develop a good understanding of all commonly used encryption schemes and other services that can be provided by modern cryptography.

Recommended Background: Interest in the subject matter and good standing in CS courses as well as some background in discrete mathematics.

Target Audience

The course is suited for students with a ECE, CS, or similar background. Interested undergraduate students are also welcome. The course targets students interested in cryptography or other security related fields such as trusted computing, network and OS security, or general IT security.

Course Outcomes

After attending the course you will understand why today's secure cryptosystems have been designed the way they are. You will further know how to perform basic attacks on cryptography and how to avoid common pitfalls when integrating cryptography in practical applications.

Course Outline

The following is a tentative course outline.

Symmetric Cryptography

1 - Principles of Cryptography, historical ciphers and their cryptanalysis
2 - Randomness, Stream Ciphers and One-time Pad

3 - Block Ciphers: AES, basics, functionality and security
4 - Block Ciphers: Modes of operation
5 - Hash functions and MACs

Asymmetric Cryptography

6 - Mathematical Foundations and Diffie-Hellman Key Exchange
7 - Asymmetric Encryption: ElGamal and RSA
8 - Digital Signatures
9 - Elliptic Curve Cryptography

Applications of Cryptography

Select topics such as:
Principles of key management, Secret Sharing, Zero-Knowledge Proofs

Textbook

The course will loosely follow the text book by Nigel Smart [1], which is recommended as a reference. Further material will be provided through myWPI.

[1] (recommended) Nigel Smart: *Cryptography: An Introduction*, Mcgraw-Hill College, The text was made available by the author for free download at:
http://www.cs.bris.ac.uk/~nigel/Crypto_Book/

[2] (optional)Paar, Pelzl: *Understanding Cryptography: A Textbook for Students and Practitioners.* 1st edition, Springer, 2009
http://link.springer.com/book/10.1007%2F978-3-642-04101-3

[3] (optional) Katz, Lindell*: Introduction to Modern Cryptography: Principles and Protocols.* 2nd edition, Chapman & Hall/CRC, 2014

[4] (reference) Menezes, van Oorschot, Vanstone: *Handbook of Applied Cryptography*. CRC Press. 5th printing 2001. Downloads for academic purposes are available from: *www.cacr.math.uwaterloo.ca/hac*

[5] (further reading) David Kahn, *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet.* Scribner, 1996

Grading

Grading is based on projects, one MidTerm exam and final presentations. Exam will be in-class, take-home or a mix of both. The weights for the final grade are as follows:

Projects	**50%**
MidTerm Exam (Nov. 7)	**30%**
Presentation	**20%**

The following grading scale will be used:

Cumulative Performance	Grade
>90%	A
>80% - 90%	B
>65% - 80%	C
55% - 65%	D
<55%	F

Honor Code

Students at WPI are expected to maintain the highest ethical standards. Academic dishonesty, including cheating and plagiarism, is considered a serious breach of these ethical standards, because it interferes with the university mission to provide a high quality education in which no student enjoys an unfair advantage over any other. Academic dishonesty is also destructive of the university community, which is grounded in a system of mutual trust and places high value on personal integrity and individual responsibility. Harsh penalties are associated with academic dishonesty. For more information, see:
http://www.wpi.edu/offices/policies/judicial/sect5.html

Students with Disabilities

If you need course adaptations or accommodations because of a disability, or if you have medical information to share with me, please make an appointment with me as soon as possible. If you are entitled to accommodation in accord with documentation on file at the Disabilities Service Office, let me know as soon as possible so I can arrange for the accommodation.

This syllabus is subject to reasonable changes at the discretion of the instructor.