ECE 480X: Introduction to Cryptography and Communication Security

When: Mondays and Thursdays, 3:00 – 4:50 pm, starting Mar. 17
Where: Goddard Hall 227
Instructor: Thomas Eisenbarth
email: teisenbarth@wpi.edu, phone: (508) 831-5914, office: AK 216

Course description

This course provides an introduction to modern cryptography and communication security. It focuses on *how* cryptographic algorithms and protocols work and how to use them. The course covers the concepts of block ciphers and message authentication codes, public key encryption, digital signatures, and key establishment, as well as common examples and uses of such schemes, including the AES, RSA-OAEP, and the Digital Signature Algorithm. Basic cryptanalytic techniques and examples of practical security solutions are explored to understand how to design and evaluate modern security solutions.

Recommended background:
ECE 2049 Embedded Computing in Engineering Design or CS 2301 Systems Programming for Non-Majors or equivalent

Suggested background:
CS 2022/MA2201 Discrete Mathematics

Target Audience

The course is suited for 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 basic principles of cryptography and general cryptanalysis
- Be acquainted with the concepts of symmetric encryption and authentication
- As well as public key encryption, digital signatures, and key establishment.
- know and understand common examples and uses of cryptographic schemes, including the AES, RSA-OAEP, the Digital Signature Algorithm, and the basic Diffie-Hellman key establishment protocol, and know how and when to apply them.
- Be able to compose, build and analyze simple cryptographic solutions.

Course Outline

The following is a tentative course outline.

- Week 1: Historical encryption schemes and the one-time pad
- Week 2: Block Ciphers and their usage in practice
- Week 3: Hash functions and message authentication
- Week 4: Public key cryptography and key exchange
- Week 5: Public key encryption
- Week 6: Digital Signatures
- Week 7: Usage of cryptography in practical protocols

Textbook

The course will loosely follow the text book by Paar and Pelzl [1], which is recommended as a reference. Further material will be provided through Blackboard.

[1] (recommended)Paar, Pelzl: *Understanding Cryptography: A Textbook for Students and Practitioners.* 1st edition, Springer, 2009

[2] (optional) Nigel Smart: *Cryptography: An Introduction*, Mcgraw-Hill College, 2004
The text was made available by the author for free download at:
http://www.cs.bris.ac.uk/~nigel/Crypto_Book/

[3] (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*

[4] (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 hands-on projects, homework, and quizzes; no midterm/final exams are planned. The weights for the final grade are as follows:

Projects + Homework	**60%**
Quizzes	**40%**

The following grading scale will be used:

Cumulative Performance	Grade
>90%	A
>75% - 90%	B
60% - 75%	C
<60%	NR

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.