

Syllabus

Instructor

Jens-Peter Kaps

Engineering Building, 3222

Phone: (703) 993-1611

jkaps@gmu.edu

<http://ece.gmu.edu/~jkaps>

Date & Time & Place

Thursdays, 4:30pm–7:10pm, Aquia Building 213

Course Web Page

The course web page will contain the latest announcements, handouts, assignments, source code and useful/interesting web links.

The web page is accessible via <http://ece.gmu.edu/~jkaps/courses/ece747>.

Textbooks

- **Course Text:** Çetin Kaya Koç, *Cryptographic Engineering* by Springer; 2009, ISBN: 978-0-387-71816-3.
- **Recommended:** Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, *Handbook of Applied Cryptography* by CRC Press, Inc.; 1996, ISBN: 0-84-938523-7.

Prerequisite

ECE 646 Cryptography and Computer Network Security or permission from the instructor.

Office Hours

Please check the class web page for the current office hour schedule. You should feel free to approach Dr. Kaps at any time if you need help in addition to the scheduled sessions. The best way to contact him is via email.

Description

Cryptographic Engineering is concerned with all aspects of implementing cryptographic algorithms in hardware and / or software. This ranges from high performance implementations to ultra-low power implementations of public key and secret key algorithms, fault tolerant implementations, attack resistant implementation and even implementations of attacks. This course will be taught partially as lecture to introduce cryptographic engineering and partially as seminar where the students explore in-depth cryptographic engineering problems that they are interested in or are engaged in research. The textbook *Cryptographic Engineering* will be the main resource for this course and serves as a thorough introduction to the topic areas. The class will be further enhanced by current research publications in the respective fields.

Presentations

Students make two one-hour presentations during this semester on a topic of their choosing. The first presentation serves as an introduction of the class to the specific topic. The second presentation explores one specific aspect of that topic in more depth.

Midterm Exam

There will be one midterm exam during the course. It will cover the introductory presentations of all topics selected for this class.

- Midterm Exam: March 29th

Participation

Students are expected to read the material ahead of class. The schedule of topics and presentations will be determined in the first class and then posted on the class webpage. Furthermore, the students are expected to participate in class discussions and provide constructive feedback to presentations by their fellow students.

Assignments

An important part of this course are the assignments. All assignments are to be completed individually. The very first assignment is to select a research topic. All following assignments are based on this topic. The schedule of assignments is shown below. The assignments are chosen to guide the student from a research topic to an overview of the research area, identification of open problems, selection of a research idea, and finally to formulate the research approach and defend the topic.

Final Report

The final report is the culmination of the assignments.

Grading

The following weight distribution will be used to calculate the final grade:

- 20% Presentations
- 10% Class Participation
- 30% Assignments
- 30% Midterm Exam
- 10% Final Report

Schedule of Assignments

- **Topic selection:** February 1st
- **Literature search results:** February 8th
- **Revised lit. search:** February 15th
- **Research matrix:** February 22nd
- **Revised research matrix:** March 1st
- **Open problems:** March 8th
- **Previous work:** March 22nd
- **Research ideas:** April 5th
- **Motivation:** April 12th
- **Research approach:** April 19th
- **Revised research approach:** April 26th
- **Final report:** May 10th

Topics

- True random number generator
- Finite field multiplication
- Arithmetic for hardware cryptography
- Elliptic and hyper elliptic curves
- Pairing based cryptosystems
- Post quantum cryptography
- Lightweight cryptography
- Efficient implementations
- Side-channel analysis (SCA)
- Countermeasures to SCA
- Fault attacks and fault Injection
- ...