

Syllabus

Instructor

Jens-Peter Kaps

Engineering Building, 3222

Phone: (703) 993-1611

jkaps@gmu.edu

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

Office Hours: Monday 3:30pm–4:30pm, Tuesday 1:30pm–2:30pm, or by appointment.

Assistance

If you need assistance outside of class and office hours contact me via e-mail. Always start the subject line with "ECE 746" so that I can quickly find your e-mail in my inbox.

Date & Time & Place

Tuesday, 4:30pm – 7:10pm, Exploratory Hall L111

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/ece746>

Textbooks

- William Stallings, *Cryptography and Network Security: Principles and Practice* by Prentice Hall; 7th edition, 2016, ISBN: 978-0134444284.

If you already own an earlier edition, or can get the 6th edition at a good price you don't have to buy the 7th edition for this course. When you use an edition earlier than the 6th, it is your responsibility to make sure that you read the corresponding material and that errors in the earlier edition do not create wrong results in assignments.

- A. J. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1997, ISBN: 0-84-938523-7.

(all chapters of this book can be downloaded from the books web page)

You can find links to more interesting books on the class home page.

Prerequisite

- ECE 646 Cryptography and Computer-Network Security or permission from Instructor
- Strong math background. Practical programming skills in Python, Perl, C or C++

Homework

There will be weekly homework assignments. These will include questions, and programming

exercises. Homework must be handed in on time. If you can't make it to the class, please e-mail it me. Homework handed in after solutions are posted will receive zero credit.

Project

An important part of this course is the semester project. The project should be an in-depth study of a topic in cryptography (e.g. side channel attacks, identity based encryption, efficient implementations, etc.) and will result in a report and a presentation. A list of possible project topics will be provided. Each project will be completed either alone or in a group of two. You are required to perform a literature study on the topic you have chosen, perform experiments, implement functions, or analyze several resources and write a journal style report. Towards the end of the semester, you will be required to give a final presentation of your project.

- **Draft Project Paper Due:** April 25th
- **Project Presentation:** May 5th
- **Final Project Paper Due:** May 9th

Examinations

There will be two exams during the course, a midterm exam and a final exam. The exams will be open book and open notes and contain multiple choice and short problems. The questions will range from mild to difficult.

- **Midterm Exam:** March 7th
- **Final Exam:** May 16th

Grading

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

- 15% Homework
- 40% Project
- 20% Midterm Examination
- 25% Final Examination