Syllabus

Instructor

Jens-Peter Kaps
Engineering Building, 3222
Phone: (703) 993-1611
jkaps@gmu.edu
http://ece.gmu.edu/~jkaps
Office Hours: Tuesday 4:30pm–5:30pm, Thursday 1:00pm–2:00pm, or by appointment.

Date & Time & Place

Tuesdays & Thursdays, 10:30am–11:45am, Blue Ridge 128

Course Web Page

The course web page is accessible via http://ece.gmu.edu/~jkaps/courses/cyse476 The latest announcements, handouts, assignments, source code and useful/interesting web links will be posted on the course page on myMason.

Textbooks

- Christof Paar and Jan Pelzl, *Understanding Cryptography*, Springer-Verlag, 2009, ISBN: 978-3-642-04101-3.
  The lecture follows to some extend this book. The book can be accessed through the GMU Library https://link-springer-com.mutex.gmu.edu/book/10.1007/978-3-642-04101-3.
- William Stallings, *Cryptography and Network Security: Principles and Practice*, Prentice Hall; 7th edition, 2016, ISBN: 978-0134444284.
- 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 http://cacr.uwaterloo.ca/hac/.

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

Prerequisites

CYSE 101 and CYSE 330 with a grade C or better or ECE 465 with a grade C or better as well as a strong math background and practical programming skills in Python.

Homework

There will be weekly homework assignments. These will include reading assignments, questions, and programming exercises. The homework will not be collected or graded. The homework questions will be posted on Mondays, the solutions will be posted on Fridays. The following Tuesday, will be an inclass quiz based on the homework. The quizzes will be collected and graded. For maximum benefit of these homework assignments you are encouraged to try to solve the questions before the

solutions are published. You should discuss your work with other students in the class. Once the solutions are published, try to learn from them and see where you went wrong.

Quizzes
There will be up to 12 quizzes during the course. The quizzes will be given on Tuesdays at the beginning of class and take approximately 15 minutes. No extra time will be given for late arrivals. The questions will be similar to the previous weeks homework. The quizzes will be closed book and closed notes.

Projects
Laboratory exercises will involve getting familiar with selected implementations of cryptographic algorithms and protocols. Based on this knowledge and your own experiments, you will be asked to solve a set of simple problems, and prepare a short report including answers to the questions included in the instruction.

Examinations
There will be two exams during the course, a midterm exam and a final exam. The exams will be closed book and closed notes and contain a multiple choice test and short problems. The questions will range from mild to difficult. One letter size page with notes on one side will be allowed for the midterm and notes on both sides will be allowed for the final exam.

- **Midterm Exam:** October 18th
- **Final Exam:** December 18th

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

- 15% Quizzes
- 30% Projects
- 25% Midterm Examination
- 30% Final Examination

Schedule of Lectures (subject to change)
The course schedule is provided in a separate document on myMason and the class website.

Honor Code
All rules of the GMU Honor Code system will be in effect. You must review the rules and be familiar with them. You are encouraged to discuss homework problems and projects with other students and/or obtain the assistance of the instructor. Nevertheless, you must write down your own homework solutions which represent your understanding of the material. Projects must be completed individually. No part of a project submission can be copied from another person of the class or any other source. Duplicating someone elses work such as but not limited to quizz solutions, hard-ware/software designs, diagrams, source code, project reports, and exam notes, is considered cheating. If you use material from other sources such as but not limited to the web, books, journals,

data sheets, etc. you must reference the source. Honor code violations will be followed up with full force.

Classroom Etiquette
Cellphones, pagers have to be put into silent mode. If you have an emergency need to answer a call please quietly leave the room BEFORE answering the call. Lectures may not be recorded without express written permission from the instructor.

Students with Disabilities
If you need special assistance, please inform the instructor within the first 3 weeks of classes so that we can work something out.

The course syllabus is subject to change