Syllabus

Instructor
Jens-Peter Kaps
Engineering Building, 3222
Phone: (703) 993-1611
jkaps@gmu.edu
http://ece.gmu.edu/∼jkaps
Office Hours: Tuesday 2:00pm–3:00pm, Wednesday 4:30pm–5:30pm, or by appointment.

Teaching Assistant
Rabia Shahid
rshahid@gmu.edu
Office Hours: Monday 2:00pm–4:00pm in ENGR 3204, Wednesday 11:00am–1:00pm in ENGR 3203

Assistance
If you need assistance outside of class and office hours use our Piazza board.

Date & Time & Place
Tuesdays, 7:20pm–10:00pm, 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/ece646

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 6$^{\text{th}}$ edition at a good price you don't have to by the 7$^{\text{th}}$ edition for this course. When you use an edition earlier than the 6$^{\text{th}}$, 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 542 (can be taken concurrently) or permission of instructor as well as a strong math background and practical programming skills in 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 to the TA. Homework handed in after solutions are posted will receive zero credit.

Laboratory Exercises
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.

Project
An important part of this course is the semester project which can be done in a team of 1–3 students. A list of possible project topics will be provided but you can also suggest your own. Four types of projects are possible: software, hardware, analytical, or mixed. All types of projects may involve some experiments. You will be asked to perform a literature search, write project specifications, deliver regular progress reports, give a project presentation, and write a journal style report.

- **Project Specification Due:** September 20th
- **1st Progress Report:** Week of October 10th
- **2nd Progress Report:** Week of November 7th
- **Draft Presentation Due:** Week of November 28th
- **Draft Report Due:** December 2nd
- **Report Reviews Due:** December 7th
- **Presentation:** December 9th
- **Report Due:** December 16th

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 a multiple choice test and short problems. The questions will range from mild to difficult.

- **Midterm Exam:** October 25th
- **Final Exam:** December 13th

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

- 14% Homework
- 6% Laboratory Exercises
- 30% Project
- 25% Midterm Examination
- 25% Final Examination

Schedule of Lectures (subject to change)
Please visit the class webpage for the most up-to-date schedule.

1. Introduction and basic concepts of cryptology. (08/30/16)
2. Implementation of security services. (09/06/16)
3. Key Management and secure e-mail. (09/13/16)
4. Mathematical background: Modular arithmetic. (09/20/16)
5. Historical Ciphers. (09/27/16)
6. Data Encryption Standard. (10/04/16)
7. Modes of operation of block ciphers. (10/18/16)
8. Advanced Encryption Standard. (11/01/16)
9. RSA – Genesis, operation, and security. Factoring. (11/08/16)
10. RSA – Efficient implementations, key generation (11/15/16)
11. Message Authentication Codes, Digital Signatures (11/22/16)
12. Modern cryptographic algorithms, key sizes, standards (11/29/16)
13. Random Number Generators, Physical Unclonable Functions (12/06/16)

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 by each group individually. No part of a project submission can be copied from another group of the class or any other source. Duplicating someone elses work such as but not limited to homework 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.