Syllabus

Instructor
Jens-Peter Kaps
Engineering Building, 3222
Phone: (703) 993-1611
E-Mail: jkaps@gmu.edu, **Web:** http://ece.gmu.edu/~jkaps
Office Hours: Tuesday 1:00pm–2:00pm, Thursday 11:00am–noon, or by appointment. Office hours will be conducted in-person in my office and via Zoom (link on our myMason course page).

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
Monday, 4:30pm – 7:10pm, Engineering Building 2608. If we have to switch to on-line learning, we will be using Blackboard Collaborate Ultra which will be linked on our myMason page as "Online Lectures." All **on-line** lectures will be recorded and available on myMason.

Course Web Page
The course web page is accessible via http://people-ece.vse.gmu.edu/~jkaps/courses/ece746. The latest announcements, handouts, assignments, source code and useful/interesting web links will be posted on the course page on myMason.

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 by 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 https://cacr.uwaterloo.ca/hac/.
- Christof Paar and Jan Pelzl, *Understanding Cryptography*, Springer-Verlag, 2009, ISBN: 978-3-642-04101-3. The book can be accessed through the GMU Library
  https://link-springer-com.mutex.gmu.edu/book/10.1007/978-3-642-04101-3.

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.

Laboratory Exercises
There will be up to five laboratory exercises this semester in which the students will get partical exposure to side-channel attacks. Each exercise will require a short written report.

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, efficient implementations, etc.) and will result in a report and a presentation. A list of possible project topics will be provided. All projects will be individual projects. 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 2nd
- **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:

- 10% Homework
- 10% Laboratory Exercises
- 40% Project
- 20% Midterm Examination
- 20% Final Examination

Safe Return to Campus
All students taking courses with a face-to-face component are required to follow the university's public health and safety precautions and procedures outlined on the university Safe Return to

Campus webpage (`https://www2.gmu.edu/safe-return-campus`). Similarly, all students in face-to-face and hybrid courses must also complete the Mason COVID Health Check daily, seven days a week. The COVID Health Check system uses a color code system and students will receive either a Green, Yellow, Red, or Blue email response. Only students who receive a "green" notification are permitted to attend courses with a face-to-face component. If you suspect that you are sick or have been directed to self-isolate, please quarantine or get testing. Faculty are allowed to ask you to show them that you have received a Green email and are thereby permitted to be in class.

Students are required to follow Mason's current policy about facemask-wearing. As of August 11, 2021, all community members are required to wear a facemask in all indoor settings, including classrooms. An appropriate facemask must cover your nose and mouth at all times in our classroom. If this policy changes, you will be informed; however, students who prefer to wear masks either temporarily or consistently will always be welcome in the classroom.

Course Materials and Student Privacy
All course materials posted to Blackboard or other course site are private to this class and must not be shared with anyone not enrolled in this class. That applies to lecture slides, homework, quizzes, exams, labs as well as to material posted by students.

Videorecordings – whether made by instructors or students – of class meetings that include audio, visual, or textual information from other students are private and must not be shared outside the class.

Live video conference meetings (e.g. Collaborate or Zoom) that include audio, textual, or visual information from other students must be viewed privately and not shared with others in your household or recorded and shared outside the class.

If we have to switch back to on-line learning, then all of our synchronous meetings in this class will be recorded to provide necessary information for students in this class. Recordings will be stored on Blackboard and will only be accessible to students taking this course during this semester.

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 else's work such as but not limited to quiz 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.

For more information about the Mason Honor Code and about the Honor Committee, please visit the website for the Office of Academic Integrity (`http://oai.gmu.edu/`).

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.

GMU E-mail Accounts
Students must use their Mason email account to receive important University information, class-related messages, and to communicate with the professor and the teaching assistants. See `http://masonlive.gmu.eduformoreinformation`.

Students with Disabilities
If you are a student with a disability and require special accommodations, please contact the instructor and the Office of Disability Services as soon as possible. All special accommodations must be arranged through ODS.

Office of Disability Services (ODS): (703) 993 – 2474; `http://ods.gmu.edu`

Other Useful Campus Resources

- Writing Center: A114 Robinson Hall; (703) 993-1200; `http://writingcenter.gmu.edu`
- University Libraries: "Ask a Librarian" `http://library.gmu.edu/mudge/IM/IMRef.html`
- Counseling and Psychological Services (CAPS): (703) 993-2380; `http://caps.gmu.edu`
- The University Catalog: `http://catalog.gmu.edu`
- University Policies: `http://universitypolicy.gmu.edu`

The course syllabus is subject to change