# Syllabus

Welcome to Cryptography Fundamentals. In this course you will be introduced to algorithms and techniques that make modern secure communication possible. You will learn the mathematical background required for understanding the algorithms and security estimates. This course also covers modern secret-key stream and block ciphers, modes of operation, and public key cryptosystems such as RSA, elliptic curve, and post quantum cryptography. It discusses popular cryptographic modules, such as True Random Number Generators and Physical Unclonable Functions, used for key generation and device authentication. You will explore historical ciphers, limits of key management for public key ciphers, as well as attack implementations of cryptographic algorithms in hardware using side-channel analysis through hands-on projects. The projects are based on educational and open-source software and a physical side-channel analysis setup that can be accessed through the web.

**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).

**Date & Time & Place**

Tuesdays & Thursdays, 3:00pm–4:15pm, Music and Theater Building 1006. 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 `https://people-ece.vse.gmu.edu/~jkaps/courses/ece476/`
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. 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 `https://cacr.uwaterloo.ca/hac/`.

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

**Course Schedule**
The course schedule is provided in a separate document on MyMason.

**Prerequisites**
ECE 301, ECE 231, or ECE 331 with a grade C or XS or better as well as a strong math background and practical programming skills in Python.

**Reading Assignments**
The reading assignments are shown in the class calendar in the rightmost column and in the homework. They refer to sections in the Paar and Pelzl (P&P) or the Stallings (Stall.) text that need to be read by the beginning of the week.

**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 Tuesdays, 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**
Projects 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. Projects submitted after the deadline will receive a late penalty of 5% per day for up to one week late. Projects submitted more than one week after the deadline will receive 0 points.

**Discussion Board**
All questions about the material covered in this course, including questions about the class, homework assignments, exams, and projects, will be addressed using the discussion board on myMason.

Please subscribe to each of the forums – you will then receive an email each time a question or response is posted to one of the forums.

Class-related questions will not be addressed via email. Instead, all questions should be posted to the appropriate forum of the discussion board. Always check the forum before posting your question. The same,or a similar, question may have already been posted (and answered). Furthermore, you may post a "follow-up" question to an existing thread to foster additional discussion and/or to request a more detailed answer.

The Instructor will do his best to respond to all questions posted on the discussion board forums. In addition, you may provide a response to any question posted on one of the forums.Any questions or concerns regarding a personal matter should be emailed to the instructor directly. Do not post such comments on the discussion board.

**Examinations**
There will be two exams during the course, a midterm exam and a final exam. The questions will be similar to the homework questions and will contain mathematical problems and essay questions ranging from mild to difficult.

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:** March 10th
- **Final Exam:** May 16th

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

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