ECE 646
Applied Cryptography
Fall 2019

Kris Gaj
Research and teaching interests:
• cryptographic engineering
• secure cryptographic protocols
• hardware security
• FPGA design and software/hardware codesign

Contact:
The Engineering Building, room 3225
kgaj@gmu.edu
Office hours: Monday, 6:00-7:00 PM
Wednesday, 7:30-8:30 PM
Friday, 6:00-7:00 PM, and by appointment

ECE 646
Part of:
MS in Computer Engineering
Recommended in particular for students pursuing
the following concentrations/specializations:
• Internet of Things & Network Security
• Hardware Security & Cryptographic Engineering
• Computer Networks
Elective course in the remaining specialization areas

MS in Electrical Engineering
Recommended in particular for students pursuing
the concentration/specialization:
• Communications and Networking
Elective course in the remaining specialization areas

ECE 646
Part of:
MS in Information Security and Assurance
Elective for the concentrations:
• Network and System Security
• Applied Cyber Security

MS in Cyber Security Engineering
Additional Core (subject to final approvals)

PhD in Electrical and Computer Engineering
PhD in Computer Science
PhD in Information Technology

Programs
MS in Computer Engineering MS CpE
IMMEDIATELY PROGRAMS
COMPUTER ARCHITECTURE
& EMBEDDED SYSTEMS
INTERNET OF THINGS
& NETWORK SECURITY
HARDWARE SECURITY
& CRYPTOGRAPHIC ENG.
COMPUTER NETWORKS
DIGITAL SYSTEMS DESIGN
DIGITAL SIGNAL PROCESSING

Specializations (since Fall 2020 Concentrations)

MS in Electrical Engineering MS EE
COMMUNICATIONS
& NETWORKING
SIGNAL PROCESSING
CONTROL & ROBOTICS
ELECTRONICS
SPACE-BASED SYSTEMS
BIOENGINEERING
**MSCpE Internet of Things & Network Security**

ECE 508 Internet of Things  
ECE 542 Computer Network Architectures and Protocols  

At least 3 courses from the following list:  
1. ECE 510 Real-Time Concepts  
2. ECE 511 Computer Architecture  
3. ECE 530 Sensor Engineering  
4. ECE 611 Advanced Computer Architecture  
5. ECE 612 Real-Time Embedded Systems  
6. ECE 633 Error Control Coding  
7. ECE 642 Design and Analysis of Computer Communication Networks  
8. ECE 646 Applied Cryptography  
9. ECE 746 Advanced Applied Cryptography  
10. ECE 747 Cryptographic Engineering  
11. SWE 619 Object-Oriented Software Specification and Construction  
12. SWE 681 Secure Software Design and Programming

*not on the list of courses for this specialization area*

**MSCpE Hardware Security & Cryptographic Engineering**

ECE 505 Hardware Security  
ECE 545 Digital System Design with VHDL  

At least 3 courses from the following list:  
1. ECE 511 Computer Architecture  
2. ECE 527 Learning From Data  
3. ECE 542 Computer Network Architectures and Protocols  
4. ECE 586 Digital Integrated Circuits  
5. ECE 615 Software/Hardware Codesign  
6. ECE 633 Error Control Coding  
7. ECE 645 Computer Arithmetic  
8. ECE 646 Applied Cryptography  
9. ECE 681 VLSI Design for ASICs  
10. ECE 682 VLSI Test Concepts  
11. ECE 746 Advanced Applied Cryptography  
12. ECE 747 Cryptographic Engineering

**MSCpE Computer Networks**

ECE 528 Introduction to Random Processes in Electrical and Computer Engineering  
ECE 542 Computer Network Architectures and Protocols  

At least 3 courses from the following list:  
1. ECE 508 Internet of Things  
2. ECE 531 Introduction to Wireless Communications and Networking  
3. ECE 633 Error Control Coding  
4. ECE 642 Design and Analysis of Computer Communication Networks  
5. ECE 643 Network Switching and Routing  
6. ECE 646 Applied Cryptography  
7. ECE 741 Wireless Networks  
8. ECE 742 High-Speed Networks  
9. ECE 746 Advanced Applied Cryptography
MSEE Communications and Networking

ECE 528 Introduction to Random Processes in Electrical and Computer Engineering
ECE 542 Computer Network Architectures and Protocols

At least 3 courses from the following list:
1. ECE 508 Internet of Things
2. ECE 531 Introduction to Wireless Communications and Networking
3. ECE 567 Optical Fiber Communications
4. ECE 630 Statistical Communication Theory
5. ECE 631 Software-Defined Radio
6. ECE 633 Error Control Coding
7. ECE 642 Design and Analysis of Computer Communication Networks
8. ECE 643 Network Switching and Routing
9. ECE 646 Applied Cryptography
10. ECE 728 Random Processes in Electrical and Computer Engineering
11. ECE 731 Digital Communications
12. ECE 732 Mobile Communication Systems
13. ECE 734 Detection and Estimation Theory
14. ECE 741 Wireless Networks
15. ECE 742 High-Speed Networks
16. ECE 751 Information Theory
17. ECE 781 Information Theory

New Degree Requirements
(for students with a catalog year 2020/2021 or later)

1. No core courses
2. Concentrations instead of specialization areas
   • 2 required courses
   • 3 concentration electives (min. 2 upper-level)
3. Upper-level course requirement
   • 3 upper-level (including concentration electives)
   • MSEE: other than ECE 698, 798, 799
   • MSCpE: other than ECE 799
4. ECE course requirement
   • MSEE: max. 2 non-ECE
   • MSCpE: max. 2 non-ECE + 2 CFRS, CS, ISA, or SWE

Advantages of Concentrations vs. Specializations

For students:
• Concentration appears on a student’s transcript
• Concentration can be declared at the time of application to a program (starting in Fall 2020)
• Progress of study easy to follow using Degree Works

For instructors & staff:
• Statistics how many students follow each concentration
• Statistics how many students graduate with a given concentration
• Concentration requirements easily enforceable using Degree Works

New Degree Requirements
(for students with a catalog year 2020/2021 or later)

In order to follow the New Degree Requirements it is sufficient to change the Catalog Year by filling the form Change of Program (Graduate) available at https://ece.gmu.edu/graduate/forms and https://registrar.gmu.edu/forms

However, you will be able to do it only in Fall 2020.

Transfer between Programs

• possible only after one semester of studies at GMU
• requires permission from the directors of the proposed and the current programs
• especially easy within the ECE Department, i.e., between the MS EE and MS CpE programs
For more information about the Master-level programs offered by ECE please check ECE website → Graduate Studies Orientation for MSEE and MSCpE Students

A few words about You

1 PhD
ECE

11 MS CpE

6 MS EE

3 MS ISA

1 PhD
ECE

Getting Help Outside of Office Hours

• System for asking questions 24/7
• Answers can be given by students and instructors
• Student answers endorsed (or corrected) by instructors
• Average response time in Fall 2017 = 45 minutes
• You can submit your questions anonymously
• You can ask private questions visible only to the instructors

ECE 646

Lecture Lecture Laboratory Project

Homework 10 % 10 % 35 %

Midterm exam 20 %
Final Exam 25 %

Specification - 5 %
Results - 10 %
Oral presentation - 10 %
Written report - 8 %
Review - 2 %

Bonus Points for Class Activity

• Based on class exercises during lectures & activity on Plazza
• “Small” points earned each week posted on Blackboard
• Up to 5 “big” bonus points
• Scaled based on the performance of the best student

For example:

<table>
<thead>
<tr>
<th></th>
<th>Small points</th>
<th>Big points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>40</td>
<td>5</td>
</tr>
<tr>
<td>Bob</td>
<td>36</td>
<td>4.5</td>
</tr>
<tr>
<td>…</td>
<td>…</td>
<td>…</td>
</tr>
<tr>
<td>Charlie</td>
<td>8</td>
<td>1</td>
</tr>
</tbody>
</table>
Lecture
• viewgraphs / whiteboard
• viewgraphs available on the web (please, extend with your notes)
• books
  1 required (Stallings)
  1 optional (all chapters available on the book web page)
• articles (PQCrypto, CHES, CRYPTO, EUROCRYPT, etc.)
• web sites - Crypto Resources
  standards, FAQs, surveys

Homework
• optional assignments
  short programs vs. analytical problems
  More time consuming
  Most time spent on debugging
  Relatively straightforward
  Typically less time consuming
  More thinking
  Little writing

Midterm exam
✓ 2 hours 40 minutes
✓ 10-12 problems
✓ open-books, cheat sheet
✓ practice exams (with solutions) available on the web
Tentative date:
  Wednesday, October 30

Final exam
2 hours 45 minutes
8-12 problems
Wednesday, December 11
4:30 – 7:15 PM

Laboratory
• labs based on two major software packages
  ✓ CrypTool
  ✓ GnuPG for Windows, Linux, or Mac
• done at home or in the ECE labs: software downloaded from the web
• based on detailed instructions
• grading based on written reports (answers to questions included in the instructions)
**Project (1)**

- original
- useful
- depth, originality
- based on additional literature
- you can start at the point where former students ended
- based on something you know and are interested in
- software, hardware, analytical, or mixed
- may involve experiments
- teams of 1-3 students

**Mixed Projects**

- HW 80%
- AN 20%
- HW 40%
- SW 40%
- SW 60%
- AN 40%

**Project (2)**

- about three weeks to choose a topic and write the corresponding specification
- regular meetings with the instructor
- a few oral progress reports based on Power Point slides
- draft final presentation due at the last progress report
- short conference-style oral presentations
- contest for the best presentation
- written report/article, IEEE style
- publication of reports and viewgraphs on the web

**Project (3)**

- Project reports/articles requirements
  - IEEE style
  - 15 pages maximum
  - appendices possible but do not influence the evaluation
- Review of project reports
  - initial version of the report
  - reviews done by your colleagues
  - final version of the report

**Contest for the best project**

**Two independent categories:**

- Results
- Presentation

**Scale:**

- 0 = very poor to 10 = excellent
Awards
(separate in each category)

I award - 5 points
II award - 3 points
III award - 1 point

Typical Approach to an Analytical Project

- Two or more alternative solutions to a certain problem.
- Clear evaluation criteria and their relative importance.
- Evaluation of all investigated solutions according to these criteria. Sometimes, there is a clear winner. In other cases, the winner depends on a particular application scenario.
- Mutual dependencies among various evaluation criteria.
- Critical analysis of previous literature, looking for any mistakes, inconsistencies, missing assumptions, or other flaws of previous work.
- Any remaining imperfections/disadvantages of the best currently available solution. Suggestions for possible improvements and future work.
Combining Projects from Two Different Courses

- ECE 646 & ECE 545
  - ECE 545 project: Hardware implementation of a selected Lightweight Cryptography algorithm
  - ECE 545 project can be extended into an ECE 646 project by adding additional algorithms, modes of operation, architectures, countermeasures against side-channel attacks, etc.

- ECE 646 & ECE 797/798/799/998
  - ECE 646 project can be extended into a Research Project, Master’s Thesis, PhD Thesis

Scholarly Paper (1)
After completing 18 credit hours of graduate work, a student
1. Chooses a 600-700 level course to fulfill his/her ECE 797 requirement
2. Registers for ECE 797 via Patriotweb by first requesting an override from the Academic Programs Coordinator, Ms. Patricia Sahs (psahs@gmu.edu), before the last day to add classes
3. Chooses a project topic in consultation with the instructor
4. Submits a single ECE 797 Entry Form, signed by the instructor and the student, to the Main Office by the end of the 5th week of classes in a given semester
5. Works on a project individually
6. Submits written report and gives short oral presentation
7. Asks the instructor to fill and sign the ECE 797 Evaluation Form, and submits this form to the main ECE Office

Scholarly Paper (2)
The paper and presentation must follow accepted standards for
- English
- technical merit
- literature analysis
- citation of references
- GMU Honor Code

In order to pass, the student cannot receive an Unacceptable score for any evaluated outcome

Students are encouraged to sign for ECE 797 in their last but one semester which guarantees at least two attempts

International Students’ Olympiad in Cryptography NSUCRYPTO - 2019
http://www.nsucrypto.nsu.ru
First Round: October 13, 2019
Duration: 4 hrs 30 min
Section B: for University students and professionals
Second Round: October 14-21, 2019
Team Round
Solving hard research and programming problems of crypto

Bonus points for the participation and solving the competition problems!

NSUCRYPTO - 2017
Round 2 (Professionals)

“Typical” course

This course
Follow-up courses

Applied Cryptography
ECE 646

Advanced Applied Cryptography
ECE 746

Digital System Design with VHDL
ECE 545

Cryptographic Engineering
ECE 747

Software/Hardware Codesign
ECE 615

Computer Arithmetic
ECE 645