ECE 646
Cryptography and Computer Network Security

Course web page:
ECE web page → Courses → ECE 646

Kris Gaj
Research and teaching interests:
• cryptography
• network security
• computer arithmetic
• FPGA & ASIC design and testing

Contact:
The Engineering Building, room 3225
kgaj@gmu.edu

Office hours: Tuesday, 6:00-7:00 PM
Thursday, 7:30-8:30 PM

MS CpE: NETWORK AND SYSTEM SECURITY
Advisors: Kris Gaj, Jens-Peter Kaps, Kai Zeng
3. ECE 746 Advanced Applied Cryptography – J.P. Kaps, K. Gaj – lab, project
4. ISA 656 Network Security – R. Simon, A. Stavrou, D. McCoy
5. ECE 899 Cryptographic Engineering – J.-P. Kaps

MS CpE: COMPUTER NETWORKS
Advisors: Brian Mark, Bijan Jabbari, S.C. Chang
1. ECE 528 Introduction to Random Processes in ECE
2. ECE 542 Computer Network Architectures and Protocols
3. ECE 642 Design and Analysis of Comp. Comm. Networks
4. ECE 646 Cryptography and Computer Network Security
5. ECE 741 Wireless Networks
6. ECE 742 High-Speed Networks

MS EE: COMMUNICATIONS AND NETWORKING
Comp. Network
Architectures and Protocols

EE core
EE 565
EE 528
ECE 646
ECE 630
ECE 633
ECE 642
ECE 731
ECE 732
ECE 733
ECE 734
ECE 735
ECE 736
ECE 737
ECE 738
ECE 739

Course web page:
ECE web page → Courses → ECE 646

ECE 646
Cryptography and Computer Network Security

Course web page:
ECE web page → Courses → ECE 646

Kris Gaj
Research and teaching interests:
• cryptography
• network security
• computer arithmetic
• FPGA & ASIC design and testing

Contact:
The Engineering Building, room 3225
kgaj@gmu.edu

Office hours: Tuesday, 6:00-7:00 PM
Thursday, 7:30-8:30 PM

Kris Gaj
Research and teaching interests:
• cryptography
• network security
• computer arithmetic
• FPGA & ASIC design and testing

Contact:
The Engineering Building, room 3225
kgaj@gmu.edu

Office hours: Tuesday, 6:00-7:00 PM
Thursday, 7:30-8:30 PM
**Bonus Points for Class Activity**

- Based on class exercises during lecture
- “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>Rank</th>
<th>Name</th>
<th>Small Points</th>
<th>Big Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Alice</td>
<td>40</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>Bob</td>
<td>36</td>
<td>4.5</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>28</td>
<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 (CryptoBytes, RSA Data Security Conf., CHES, CRYPTO, etc.)
- Web sites - Crypto Resources
  - Standards, FAQs, surveys

**Homework**

- Optional assignments
  - Short programs vs. analytical problems
- More time consuming
- Typically less time consuming
- More thinking
- Little writing

**Getting Help Outside of Office Hours**

**Piazza**

- 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 2013 = 1.1 hour
- You can submit your questions anonymously
- You can ask private questions visible only to the instructors

**Midterm exam**

- 2 hours 40 minutes
- Multiple choice test + short problems
- Open-books, open-notes
- Practice exams (with solutions) available on the web

Tentative date:

Tuesday, October 28th
Final exam

2 hours 45 minutes
Multiple choice + several problems

Tuesday, December 16
7:30 – 10:15 PM

Laboratory

• labs based on two major software packages
  ✓ CrypTool
  ✓ GnuPG for Windows or GnuPG for Linux

• 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

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 due Saturday, Dec. 6
  - reviews done by your colleagues
  - reviews due, Thursday, Dec. 11
  - final version of the report due Saturday, Dec. 13

Mixed Projects
Project (4)

- Project presentations
  Tuesday, December 9, 5:00-10:00PM
  - conference style
  - open to general public (in particular, students from previous years), ECE seminar credit
  - 10 minutes for the presentation + 5 minutes for Q&A
  - time strictly enforced
  - audience votes in the contest for the best project

Contest for the best project

Two independent categories:

- Results
- Presentation

Scale:

0 = very poor to 10 = excellent

Results

- Meeting Project goals
- Efficiency & security of the proposed/selected design/scheme
- Original & Correct
  - analysis
  - implementation & testing scheme
- Useful
  - for other students
  - & other members of the cryptographic community

Presentation

- Quality of viewgraphs
- Answering questions
- Discussion of encountered problems
- Conclusions
- Logical organization of the talk
- Clear and Concise presentation of main results
- Motivation & background

Awards

(separate in each category)

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

Types of Projects Typically Winning the Contest

<table>
<thead>
<tr>
<th></th>
<th>Fall 2013</th>
<th>Fall 2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>HW</td>
<td>SW</td>
<td>HW-AN</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>SW-AN</td>
<td>HW</td>
<td>AN</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Fall 2011</th>
<th>Fall 2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>AN</td>
<td>HW</td>
<td>HW-SW</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>HW</td>
<td>AN</td>
<td>AN</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
Combining Projects from Two Different Courses

- ECE 646 & ECE 545
  - ECE 545 project: Hardware implementation of authenticated ciphers competing in the CAESAR contest
  - ECE 545 project can be extended into an ECE 646 project by adding additional ciphers, architectures, key sizes, modes of operation, etc.
- ECE 646 & ECE 797/798/799/998
  - ECE 646 project can be extended into a Scholarly Paper, Research Project, Master’s Thesis, PhD Thesis

"Typical" course

- difficulty

This course

- difficulty

Follow-up courses

Cryptography and Computer Network Security
ECE 646

Advanced Applied Cryptography
ECE 746

Digital System Design with VHDL
ECE 545

Cryptographic Engineering
ECE 899

Computer Arithmetic
ECE 645

Cryptography and Computer Network Security

- Historical ciphers
- Classical encryption (DES, AES, cipher modes)
- Public key encryption (RSA, Diffie-Hellman)
- Hash functions and MACs
- Digital signatures
- Public key certificates
- Secure Internet Protocols
  - e-mail: PGP and S-MIME
  - www: SSL/TLS
- Cryptographic standards

Advanced Applied Cryptography

- AES
- Stream ciphers
- Elliptic curve cryptosystems
- Random number generators
- Smart cards
- Attacks against implementations (timing, power, fault analysis)
- Efficient and secure implementations of cryptography
- Security in various kinds of networks (IPSec, wireless)
- Zero-knowledge identification schemes

Modular integer arithmetic
Operations in the Galois Fields GF(2^n)