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

1. ECE 542 Computer Network Architectures and Protocols
   – S.-C. Chang, et al.
2. ECE 646 Cryptography and Computer Network Security
   – K. Gaj, J.-P. Kaps – lab, project
3. ECE 746 Advanced Applied Cryptography
   – J.P. Kaps, K. Gaj – lab, project
4. ISA 656 Network Security
   – D. McCoy, A. Stavrou,
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
Architecture and Protocols

ECE 542

CS 571

Performance
 analys

ECE 646

Network
Security

ECE 741

Statistical
Comm. Theory

ECE 528

Coding Theory

ECE 630

Digital Comm.

ECE 633

Satellite Comm.

ECE 730

Spread
Spectrum
Comm.

ECE 742

High-Speed
Networks

ECE 731

Mobile Comm.

ECE 737

ECE 739

Optoelectronics

ECE 565

EE core

ECE 672

CS 672

EE core

EE core

ECE 756

Performance Analysis & Evaluation

Homework

10 %

Midterm exam

20 %

Final Exam

25 %

Specification - 5 %

Results - 10 %

Oral presentation - 10 %

Written report - 8 %

Review - 2 %

Lecture

35 %

Laboratory

ECE 646

Project
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
  or HDL codes

✓ More time consuming
✓ Most time spent on debugging
✓ Relatively straightforward

✓ Typically less time consuming
✓ More thinking
✓ Little writing
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 22nd or October 29th

Final exam

- 2 hours 45 minutes
- Multiple choice + several problems

Tuesday, December 10
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**
  - 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, or analytical
  - may involve experiments
  - teams of 1-3 students

- **useful**

### 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
  
  *Tuesday, December 3*

  - contest for the best presentation
  - written report/article, IEEE style
    
    *due Saturday, December 7*

  - 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
  - reviews done by your colleagues
  - reviews due, Thursday, December 12
  - final version of the report due Saturday, December 14
Project (4)

- Project presentations (Tuesday, December 3, 7:20-10:00PM)
  - 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

“Typical” course

follow-up courses

<table>
<thead>
<tr>
<th>Cryptography and Computer Network Security</th>
<th>ECE 646</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Applied Cryptography</td>
<td>ECE 746</td>
</tr>
<tr>
<td>Digital System Design with VHDL</td>
<td>ECE 545</td>
</tr>
<tr>
<td>Cryptographic Engineering</td>
<td>ECE 899</td>
</tr>
<tr>
<td>Computer Arithmetic</td>
<td>ECE 645</td>
</tr>
<tr>
<td>Cryptography and Computer Network Security</td>
<td>Advanced Applied Cryptography</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>Modular integer arithmetic</td>
<td>Operations in the Galois Fields $\mathbb{GF}(2^n)$</td>
</tr>
<tr>
<td>• Historical ciphers</td>
<td>• AES</td>
</tr>
<tr>
<td>• Classical encryption (DES, IDEA, RSA)</td>
<td>• Stream ciphers</td>
</tr>
<tr>
<td>• Public key encryption (RSA, DH, DSA)</td>
<td>• Elliptic curve cryptosystems</td>
</tr>
<tr>
<td>• Hash functions and MACs</td>
<td>• Random number generators</td>
</tr>
<tr>
<td>• Digital signatures</td>
<td>• Smart cards</td>
</tr>
<tr>
<td>• Public key certificates</td>
<td>• Attacks against implementations (timing, power, fault analysis)</td>
</tr>
<tr>
<td>• Secure Internet Protocols</td>
<td>• Efficient and secure implementations of cryptography</td>
</tr>
<tr>
<td>- e-mail: PGP and S-MIME</td>
<td>• Security in various kinds of networks (IPSec, wireless)</td>
</tr>
<tr>
<td>- www: SSL/TLS</td>
<td>• Zero-knowledge identification schemes</td>
</tr>
<tr>
<td>• Cryptographic standards</td>
<td></td>
</tr>
</tbody>
</table>