ECE 646
Cryptography and Computer Network Security

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

Kris Gaj
Research and teaching interests:
• cryptography
• network security
• computer arithmetic
• FPGA & ASIC design and testing
Contact:
Science & Technology II, room 223
kgaj@gmu.edu
Office hours: Wednesday 6:00-7:00 PM
Tuesday, Thursday, 4:30-5:30 PM

ECE 646
Part of:
MS in CpE
Network and System Security (required)
Computer Networks (elective)
MS in EE
Communications & Networks (elective)
Ph.D. in Electrical and Computer Engineering
MS in Information Security & Assurance
MS in E-Commerce
Certificate in Information Systems Security
Ph.D. in Information Technology
NETWORK AND SYSTEM SECURITY
Concentration advisors: Jens-Peter Kaps, Kris Gaj

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, D. Hwang – lab

3. ECE 746 Advanced Applied Cryptography
   – K. Gaj, D. Hwang – lab, project: C/C++, VHDL, or analytical

4. ISA 656 Network Security
   – A. Stavrou

Grading Scheme

- Homework 20%
- Labs 20%
- Quizzes 10%
- Midterm Exam 20%
- Final Exam 30%

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 (1)

• reading assignments
• theoretical problems (may require basics of number theory or probability theory)
• problems from the main textbook
• short programs
• literature surveys

Homework (2)

• 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 30 minutes
✓ multiple choice test + short problems
✓ open-books, open-notes
✓ practice exams available on the web
✓ midterm exam review session - optional

Tentative date:

Wednesday, October 29th
Quizzes

- 10-15 minutes
- one-two questions related to the most recent lectures
- closed-books, closed-notes
- unannounced

Final exam

2 hours 45 minutes
Multiple choice + several problems

Wednesday, December 10
7:30 – 10:15 PM

Laboratory

- 5-6 labs
- based on the GMU educational software, public domain cryptographic programs & libraries, or evaluation versions of commercial products
- 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)
Tentative list of laboratory topics

1. Secure e-mail: PGP – Pretty Good Privacy
2. Historical ciphers
3. Properties of classical cryptosystems
4. Properties of public key cryptosystems
5. Secure e-mail: S/MIME

Follow-up courses

Cryptography and Computer Network Security
ECE 646

Advanced Applied Cryptography
ECE 746

Digital System Design with VHDL
ECE 545

Computer Arithmetic
ECE 645

Cryptography and Computer Network Security
Advanced Applied Cryptography

Modular integer arithmetic

• Historical ciphers
• Classical encryption (DES, IDEA, RC5, AES)
• Public key encryption (RSA, DHL, DSA)
• Hash functions and MACs
• Digital signatures
• Public key certificates
• Secure Internet Protocols - e-mail: PGP and S/MIME - www: SSL
• Cryptographic standards

Operations in the Galois Fields GF(2^n)

• 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
"Typical" course

<table>
<thead>
<tr>
<th>difficulty</th>
<th>time</th>
</tr>
</thead>
</table>

This course

<table>
<thead>
<tr>
<th>difficulty</th>
<th>time</th>
</tr>
</thead>
</table>