ECE 646, Cryptography and Computer Network Security
Fall 2014

Instructor

Dr. Kris Gaj
The Nguyen Engineering Building, room 3225
Office hours: Tuesday 6:00-7:00 PM, Thursday 7:30-8:30 PM,
and by appointment

Lecture

Tuesday, 7:20-10:00 PM, Aquia Building, room 219

Web page

http://ece.gmu.edu → Courses → ECE 646

Prerequisite

ECE 542 (can be taken concurrently) or permission of instructor.

Grading

Homework	10%
Laboratory	10%
Project	35%
Midterms Exam	20%
Final Exam	25%

Schedule (subject to possible modifications):

1. Organization of the course. Basic concepts of cryptology. 08/26/2014
2. Steganography. 09/02/2014
3. Types of cryptosystems. Implementation of security services. 09/09/2014
4. Key management. 09/16/2014
5. Secure e-mail. 09/23/2014
6. Mathematical background: Modular arithmetic. 09/30/2014
7. Historical ciphers. 10/07/2014
8. DES and its extensions. Modes of operation of block ciphers. 10/21/2014
9. Midterm exam. 10/28/2014
10. AES. Hash functions & MACs. 11/04/2014
11. RSA – Genesis, operation, and security. Factorization records. 11/11/2014
12. RSA Implementation: Efficient encryption, decryption. RSA key generation. 11/18/2014
13. Digital Signature Schemes. Secure Protocols. 11/25/2014
14. Cryptographic Standards. Companies Developing Cryptographic Hardware. 12/02/2014

Lab

Laboratory classes will involve getting familiar with selected open-source 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 questions included in the corresponding instruction. All exercises can be done at home, at your own speed, or in the ECE computing labs.

Project

Project can be done in a team of 1-3 students. You can choose a project topic from the list of topics suggested by the instructor, posted on the course website. You can also suggest a project topic by yourself. Your project can be of different type: software, hardware, analytical, or mixed. All types of projects may involve some experiments. You will be asked to write a project specification, deliver bi-weekly project reports, give a project presentation, and develop a comprehensive project report.

Literature

Required Texts

William Stallings, *Cryptography and Network Security: Principles and Practice*, 6th ed. Prentice Hall, 2013, ISBN-13: 978-0133354690, or 5th ed., Prentice Hall, 2010, ISBN-13: 978-0136097044.

Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Inc., 1996, ISBN: 0-84-938523-7 (available on line at http://cacr.uwaterloo.ca/hac/).