

ECE 646, Cryptography and Computer Network Security Fall 2008

Instructor

Dr. Kris Gaj
S&T II, room 223
Office hours: Tuesday, Thursday, 4:30-5:30 PM
Wednesday, 6:00-7:00 PM

Lecture

Wednesday, 7:20-10:00 PM, Robinson Hall A, room 106

Web page

<http://ece.gmu.edu> → Courses → Course Web Pages → ECE 646

Prerequisite

ECE 542 or permission of instructor.

Grading

Homework	20%
Laboratory	20%
Quizzes	10%
Midterms Exam	20%
Final Exam	30%

Schedule (subject to possible modifications):

1. Security services. 08/27/2008
2. Basic concepts of cryptology. 09/03/2008
3. Types of cryptosystems. Implementation of security services. 09/03/2008
4. Key management. Pretty Good Privacy. 09/10/2008, 09/17/2008
5. Mathematical background: Modular arithmetic. 09/24/2008
6. Historical ciphers. 10/01/2008, 10/08/2008
7. Towards modern ciphers. DES and its extensions. 10/15/2008
8. Modes of operation of block ciphers. RC5, IDEA, AES. 10/22/2008
9. Midterm Exam 10/29/2008
10. RSA – Genesis, operation & security. Factorization records. 11/05/2008
11. RSA Implementation: Efficient encryption, decryption & key generation. 11/12/2008
12. Hash functions & MACs. 11/19/2008
13. Secure Protocols. Cryptographic Standards. 12/03/2008

Literature

Required Texts

William Stallings, *Cryptography and Network Security: Principles and Practice*, 4th ed., Prentice Hall, 2005, ISBN: 0-13-187316-4.

Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Inc., 1996, ISBN: 0-84-938523-7.