RIT Department of Computer Science

Syllabus ----- Schedule

CSCI-462 Introduction to Cryptography Syllabus

Catalogue Description

This course provides an introduction to cryptography, its mathematical foundations, and its relation to security. It covers classical cryptosystems, private-key cryptosystems (including DES and AES), hashing and public-key cryptosystems (including RSA). The course also provides an introduction to data integrity and authentication. (MATH-190 or equivalent and CSCI-243)

Course Outcomes

- Students will be able to implement and cryptanalyze classical ciphers. *Evaluation: Assessed by homeworks.*
- Students will be able to describe modern private-key cryptosystems and ways to cryptanalyze them. *Evaluation: Assessed by homeworks and exams.*
- Students will be able to describe modern public-key cryptosystems and ways to cryptanalyze them. *Evaluation: Assessed by homeworks and exams.*
- Students will be able to explain the mathematical concepts underlying modern cryptography. *Evaluation: Assessed by homeworks and exams.*
- Students will be able to describe the field of cryptography and its relation to security. *Evaluation: Assessed by homeworks and exams.*

Instructor Contact

Stanisław P. Radziszowski, Ph.D.
Office: 70-3657
Phone: 475-5193
email: spr@cs.rit.edu
website: www.cs.rit.edu/~spr

Course Policies

N/A

Required Materials

Christof Paar and Jan Pelzl, *Understanding Cryptography,* SpringerLink, 2010.

Additional Resources

Douglas R. Stinson, *Cryptography: Theory and Practice,* CRC Press, third edition 2006.
A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *CRC Handbook of Applied Cryptography,*, CRC Press 1996.

Grading

Component	Weight
Homeworks	45%
Midterm exam	20%
Final exam	30%
Class participation	5%

CS Common Course Policies Include:

- **Rescheduling an Exam**
- **Course Withdrawal**
- **Disability Services**
- **Academic Integrity**

---

updated: Fri Jan 18 20:22:46 EST 2013