

Master Course Syllabus
School of Engineering and Computer Science
Washington State University Vancouver

CS 427
Computer Security
3 Semester Hours
(3 lecture hours)

Catalog Description

Computer security concepts, models and mechanisms; encryption technology, formal models, policy and ethical implications.

Prerequisite Courses

CS 360 – Systems Programming
MATH 216 – Discrete Structures

Prerequisite Topics

- Abstract Algebra, Probability Theory
- Proficient in at least one high level programming language.
- Implementation of common data structures for lists, trees, and graphs
- Use of UNIX or Windows environment for coding, compilation, debugging and testing

Measured Course Outcomes

Students taking this course will:

1. Analyze computational problems related to cryptography and cryptanalysis using mathematical techniques. (*Contributes to performance criteria J-2*).
2. Explain at least one global issue that influences decisions affecting security technology. (*G-2*).

Required Textbooks

Cryptography and Network Security (Principles and Practices), Fourth Edition, William Stallings, Prentice Hall 2006.

Reference Material

Applied Cryptography (Second Edition), Bruce Schneier, Wiley Inc. 1996

Major Topics Covered in the Course

1. An examination of conventional encryption algorithms and related mathematical theory, as well as design principles, including a discussion of the use of conventional encryption for confidentiality.
2. An examination of public-key encryption algorithms, message authentication, integrity, non-repudiation, hash functions, digital signatures, risk analysis, policy issues, auditing, and public-key certificates.
3. An overview of network security tools and applications including PGP, S/MIME, IP Security and SSL.
4. Examine system-level security issues, including the threat of and countermeasures for intruders and viruses and use of firewalls and trusted systems.

Laboratory Projects

	Project Area	Weeks
Software Design		1
Programming		4

CSAB Category Content

	FUNDAMENTAL	ADVANCED		FUNDAMENTAL	ADVANCED
Data Structures	0	0	Computer Organization and Architecture	0	0
Algorithm & Software Design	0	3	Concepts of Programming Languages	0	0

Oral and Written Communications

This course introduces students to a wide variety of cryptography and network security topics. The student will choose one topic and write a term research paper on the subject (e.g. a student might research current Internet Key Exchange Protocols). The term paper should include a description of a current problem, a proposed solution, and an analysis of that solution.

Social and Ethical Issues

We discuss ethical issues surrounding computer enabled crime, intellectual property rights, and privacy.

Theoretical Content

Topic	Hours
Abstract Algebra, Number Theory	3.5
Modular and Polynomial Arithmetic	1

Problem Analysis

All student programming assignments require the student to analyze software requirements. Students will use mathematical techniques to analyze computational problems associated with encryption and decryption.

Solution Design

Students are required to design and implement at least one symmetric encryption-decryption algorithm and one asymmetric (public/private) key algorithm. The instructor analyzes problem solutions (both their own and the student's) in class.

CC2001

This course provides coverage of topics in the following areas (hours listed are minimums):

AL9. Cryptographic algorithms	15
SP8. Computer crime	1
NC3. Network security	15
OS7. Security and protection	11
SP6. Intellectual property	1
SP4. Professional and ethical responsibilities	1
SP7. Privacy and civil liberties	1

Course Coordinator: Orest Pilskalns
Last Updated: April 20, 2007 (Approved)
Syllabus Version Number: 1.1