

## CS 4821: Computer Security (4)

### Catalog Description:

Entropy and the underlying statistical characteristics of text. Encryption-basic techniques based on confusion and diffusion and modern day encryption. Access, information flow and inference control. Program threats and intrusion detection. Network and internet security. Firewalls, trusted systems, network authentication.

**Textbook:** Pfleeger, *Security in Computing*, 2<sup>nd</sup> Ed., Prentice Hall, 2000.

### References:

### Course Goals:

Computer security today consists largely of defensive methods to detect and thwart potential intruders. In this course, we learn about entropy and the statistical characteristics which underlie the processing of natural language text, making it possible to obscure its meaning so that only authorized persons may understand it (encryption). We examine public and private key encryption and basic and secure systems (DES, RSA, etc.). We study attacks on computing systems and the protective measures designed to thwart them. Database, program, operating systems and network security are examined. As time permits, ethics (as it pertains to these issues) will be explored.

### Prerequisites by Course & Topic

CS 2511: Software Analysis & Design – proficiency in object-oriented design and coding, a systematic approach to testing and debugging

CS 2521: Computer Organization & Architecture – understanding how programs and data are stored and represented in a computer system

Math 3355: Discrete Mathematics – functions

### Major Topics Covered in the Course

- Statistical Characteristics of Text and Entropy
- Encryption—Basic Building Blocks
- Encryption—Modern Techniques
- Database and Operating System Security
- Program Security
- Network Security

**Class/Laboratory Schedule:** Lecture: 3 hours per week, Laboratory: 1

### Laboratory Projects

- Calculate/compare the average entropy per character of a message encoded as single characters, digrams, and characters whose probabilities of occurrence are unknown. (1)
- Simple Problems using the Basic Building Blocks of Encryption (2)
- Advanced Encryption Techniques (2)
- RSA, PGP, and SSH (2)
- Encryption, Database and Program Security (2)
- Network Security and Authentication (2)

### Course Contribution to Program Objectives and Outcomes:

1. Understand (1) the statistical characteristics of text that underlie all text processing (compression, encryption, information retrieval) and (2) the concept of entropy and its relationship to the binary representation of information. (*d*)
2. Recognize the basic building blocks of encryption (substitution, permutation, polyalphabetic substitution, stream and block ciphers). (*d*)
3. Understand (1) the differences between symmetric and asymmetric encryption and (2) the mathematical foundations and methods of public key encryption. (*d*)
4. Understand both historical encryption (Hagelin, Enigma, DES) and current day methods (Clipper and key escrow, PEM and PGP). (*d*)
5. Understand how to provide security in database and operating systems. (*d*)
6. Understand how to provide program security. (*d*)

### Estimate CSAB Category Content

	CORE	ADVANCED		CORE	ADVANCED
Data Structures			Computer Organization and Architecture		1
Algorithms		1	Concept of Programming Languages		
Software Design					

### Oral and Written Communications

Every student is required to submit at least \_\_\_\_\_ written reports (not including exams, tests, quizzes, or commented programs) of typically \_\_\_\_\_ pages and to make 2 oral presentations of typically 20 minutes duration. Include only material that is graded for grammar, spelling, style, and so forth, as well as for technical content, completeness, and accuracy.

Each student makes two oral presentations during the semester. The subjects are chosen by the student (the first is cryptography-related, the second is any area of computer security).

### Social and Ethical Issues

Privacy (databases, key escrow) is covered each semester. Other ethical issues are discussed as time permits. (2)  
Grading: homework, test questions

### Theoretical Content

Applications of mathematics (entropy and its relationship to binary representation) (3)  
Applications of group theory, combinatorics and number theory in cryptography and authentication (6)

### Problem Analysis

For various problems related to cryptography, decompose the problem and understand how to encrypt/decrypt a message. For specific problems, determine public and private key information.

### Solution Design

Design algorithms and write code to implement the solutions to various cryptographic problems, check out and ensure that the code executes correctly.

**Coordinator/Prepared by:** C. Crouch