

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: C. Pfleeger and S. Pfleeger, *Security in Computing*, 4th Ed., Prentice Hall, 2006.

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

CS 3512 - proficiency in object-oriented design and coding, a systematic approach to testing and debugging (due to CS 3512 prereq of CS 2511), functions, asymptotic analysis

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

Course 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.
 - a. Given a body of text, compute the average entropy of the message in terms of bits per character.
 - b. Given probability distributions (characters, bigrams, Zipf, etc.) compute the average entropy of the message when probabilities are both known and unknown and compare the results.
2. Recognize the basic building blocks of encryption (substitution, permutation, polyalphabetic substitution, stream and block ciphers).
 - a. Write programs to encode and/or decode messages using these basic methods.
3. Understand (1) the differences between symmetric and asymmetric encryption and (2) the mathematical foundations and methods of public key encryption.
 - a. Solve problems using the most frequently used methods of symmetric encryption (RSA, knapsacks, etc.).
 - b. Correctly identify the components with respect to both public and private key data.
4. Understand both historical encryption (Hagelin, Enigma, DES) and current day methods (Clipper and key escrow, PEM and PGP).
 - a. Reveal an understanding of how historical ciphers work (the basic building blocks upon which they are constructed).
 - b. Download and utilize PGP to send and receive encoded messages; demonstrate the ability to use SSH.
5. Understand how to provide security in database and operating systems.

- a. Demonstrate an understanding of the particular parts of an operating system provided to improve/ensure security.
- b. Demonstrate knowledge of the techniques designed to provide security in database systems.
- 6. Understand the methods of program and network security.
 - a. Demonstrate an ability to recognize various program threats, how they work, and how to combat them.
 - b. Display a knowledge of how antiviral systems are built and operate.

Relationship to Program Outcomes

In order to take CS 4821, a student must have successfully completed discrete math, computer organization and architecture, and systems analysis & design. This course contributes to meeting the following program outcomes:

- 1. *Students understand mathematics and statistics that underlie scientific applications.*
Students utilize basic statistics, mathematics (group theory) to calculate entropy and solve cryptographic problems (one-way functions, knapsacks). Course outcomes 1-4 map to this program outcome.
- 3. *Students understand the fundamentals of computer organization and architecture, data structures and related algorithms, and programming languages.*
Students utilize their basic knowledge of machine organization to design and implement basic encryption techniques. Their proficiency in algorithms is increased through the understanding of the basic foundations of cryptography. All course outcomes map to this program outcome.
- 4. *Students can apply computer science principles and practices to a variety of problems.*
This course increases a student’s knowledge of encryption and its mathematical underpinnings. Students implement basic cryptographic techniques and utilize advanced methods of cryptography. All course outcomes map to this program outcome.
- 6. *Students can communicate effectively both orally and in writing.*
Students improve their communication skills by researching and presenting with appropriate visual aids reports related to computer security. Course outcomes 5-6 map to this program outcome.
- 7. *Students understand social, professional and ethical issues related to computing.*
Additional ethical issues are explored including computer system theft, privacy and the law, and ethics related to databases, data mining, and security. Course outcomes 4-6 map to this program outcome.

Assessment Plan for Course:

This course is assessed every third year by the instructor and a course assessment document covering all of the course outcomes and their effect on the program outcomes is prepared.

Estimate CSAB Category Content

	CORE	ADVANCED		CORE	ADVANCED
Data Structures			Computer Organization and Architecture		2
Algorithms		1	Concept of Programming Languages		
Software Design		1			

Coordinator/Prepared by: C. Crouch