Course Syllabus
18 Aug 2005

Course Description: Cryptography is the study of mathematical systems for solving two kinds of security problems on public channels: privacy and authentication. Covers the theory and practice of both classical and modern cryptographic systems. The fundamental issues involved in the analysis and design of a modern cryptographic system will be identified and studied.

Prerequisite: STAT/CSE 4340 Statistical Methods for Engineers and Applied Scientists, or EE 3360 Statistical Methods in Electrical Engineering or equivalent. Ability to program.

Credit: 3 Term-Credit Hours (TCH)


Lectures: TuTh 2:00 p.m. – 3:20 p.m.
Caruth 218

Office Hours: TuTh 1:00 p.m. – 2:00 p.m. and W 2:00 p.m. – 3:00 p.m.
By Appointment

Office Location: Junkins Building 321
Office Phone 214-768-3112
Email jgd@engr.smu.edu
Web http://www.engr.smu.edu/~jgd

Calendar:

Thursday August 18 First Day of Instruction
Friday September 2 Last Day to Declare Pass/Fail
Monday September 5 University Holiday – Labor Day
October 10-11 Fall Break
Wednesday November 2 Last Day to Drop a Course
Monday November 18 Last Day to Withdraw from the University
November 24-25 University Holiday – Thanksgiving
Thursday December 1 Last Day of Instruction (Monday Schedule)
Tuesday December 6 Final Exam 3:00 p.m. – 6:00 p.m.

Grading Policy: Homework 50%
Paper/Project 50%
Class Policies:

Lateness: Please enter from the back of the classroom and quietly take a seat so as not to disturb the class.

Attendance: I do not take daily attendance. I do reserve the right to drop a student administratively for non-attendance combined with failure to submit graded materials.

Make-Ups: Please let me know in advance if you are unable to submit graded materials by the scheduled due date so an alternative due date can be arranged.

Late Homework: Students are encouraged to submit homework by the scheduled due date. I will accept late homework up to the time homework solutions are posted on the class web site. If a pattern of late homework submissions develops, I do reserve the right to begin pro-rating the homework at the rate of a 5% decrease per day.

Class Disruption: Please turn off mobile phones and beepers during class. You may use a computer in class, but please do disturb others with your usage of the computer. Also, be sure to mute the computer’s speakers.

Disability Accommodations: If you need academic accommodations for a disability, you must first contact Ms. Rebecca Marin, Coordinator, Services for Students with Disabilities (214-768-4557) to verify the disability and to establish eligibility for accommodations. Then you should schedule an appointment with me so that appropriate arrangements can be made. (Refer to University Policy No. 2.4.)

Religious Observance: Religiously observant students wishing to be absent on holidays that require missing class should notify me in writing at the beginning of the semester, and should discuss with me, in advance, acceptable ways of making up any work missed because of the absence. (Refer to University Policy No. 1.9.)

Excused Absences for University Extracurricular Activities: Students participating in an officially sanctioned, scheduled University extracurricular activity will be given the opportunity to make up class assignments or other graded assignments missed as a result of their participation. It is the responsibility of the student to make arrangements with me prior to any missed scheduled examination or other missed assignment for making up the work. (Refer to University Undergraduate Catalogue)

Incomplete Policy: An Incomplete (I) may be given if the majority of the course requirements have been completed with passing grades but for some justifiable reason, acceptable to the instructor, the student has been unable to complete the full requirements of the course. Before an (I) is given, the instructor should stipulate, in writing, to the student the requirements and completion date that are to be met and the grade that will be given if the requirements are not met by the completion date. The maximum period of time allowed to clear the Incomplete grade is 12 months (except for graduate thesis and dissertation courses). If the Incomplete grade is not cleared by the date set by the
instructor or by the end of the 12-month deadline, the (I) may be changed to an F or to another grade specified by the instructor. The grade of (I) is not given in lieu of an F, WP, or other grade, each of which is prescribed for other specific circumstances. If the student's work is incomplete and the quality has not been passing, an F will be given. The grade of (I) does not authorize the student to attend the course during a later semester. Graduation candidates must clear all Incompletes prior to the deadline in the official University Calendar, which may allow less time than 12 months. Failure to do so can result in removal from the degree candidacy list and/or conversion of the (I) to the grade indicated by the instructor at the time the (I) was given.

Academic Honesty:

Academic dishonesty may be defined broadly as a student's misrepresentation of his or her academic work or of the circumstances under which the work is done. This includes plagiarism in all papers, projects, take-home exams, or any other assignments in which the student represents work as being his or her own. It also includes cheating on examinations, unauthorized access to test materials, and aiding another student to cheat or participate in an act of academic dishonesty. Failure to prevent cheating by another may be considered as participation in the dishonest act.

The Honor Code of Southern Methodist University

Intellectual integrity and academic honesty are fundamental to the processes of learning and evaluating academic performance; maintaining them is the responsibility of all members of an educational institution. The inculcation of personal standards of honesty and integrity is a goal of education in all the disciplines of the University.

The faculty has the responsibility of encouraging and maintaining an atmosphere of academic honesty by being certain that students are aware of the value of it, that they understand the regulations defining it, and that they know the penalties for departing from it. The faculty should, as far as is reasonably possible, assist students in avoiding the temptation to cheat. Faculty must be aware that permitting dishonesty is not open to personal choice. A professor or instructor who is unwilling to act upon offenses is an accessory with the student offender in deteriorating the integrity of the University.

Students must share the responsibility for creating and maintaining an atmosphere of honesty and integrity. Students should be aware that personal experience in completing assigned work is essential to learning. Permitting others to prepare their work, using published or unpublished summaries as a substitute for studying required materials, or giving or receiving unauthorized assistance in the preparation of work to be submitted are directly contrary to the honest process of learning. Students who are aware that others in a course are cheating or otherwise acting dishonestly have the responsibility to inform the professor and/or bring an accusation to the Honor Council.
Students and faculty must mutually share the knowledge that any dishonest practices permitted will make it more difficult for the honest students to be evaluated and graded fairly, and will damage the integrity of the whole University. Students should recognize that their own interest, and their integrity as individuals, suffer if they condone dishonesty in others.

The Honor System

All undergraduate students at SMU are under the jurisdiction of the Honor Code, and as such will be required to sign a pledge to uphold the Honor Code. The Honor Council is composed of 22 students appointed by the Student Senate to represent the undergraduate schools and classes of the University. The Council's responsibility is to maintain and promote academic honesty.

Students are required to warn or to report to the Honor Council or faculty any student suspected of violating the Honor Code, and to inform the instructor of a course in which violations are suspected that he or she may not be achieving an atmosphere conducive to academic honesty. Suspected violations reported to the Honor Council by a student or by an instructor will be investigated and, if the evidence warrants it, a hearing will be held by a Board composed of five members of the Honor Council. Suspected cases of academic dishonesty may be either handled privately by the appropriate faculty member in whose class the alleged infraction occurred, or referred to the Honor Council.

Appeals of actions by the Honor Council shall be submitted to the All-University Judicial Council in writing no later than three class days after the hearing. Appeals of actions taken by instructors independently of the Honor Council may be made through the traditional academic routes.
Course Topics:

1. Introduction

2. Classical Cryptographic Systems
   A. Analog Systems
   B. Steganography
   C. Substitution Ciphers
   D. Transposition Ciphers
   E. Code Book Systems
   F. Cracking Classical Systems

3. Shannon Theory
   A. Background
   B. Questionnaire Schemes and Passwords
   C. Perfect and Ideal Security
   D. Random Cipher Model

4. Computational Complexity
   A. Introduction
   B. Turing Machines
   C. Complexity Classes
   D. Applications to Cryptography

5. Encryption – Symmetric Techniques
   A. Data Encryption Standard (DES) Algorithm
   B. Modern Algebra Review
   C. Binary Fields – GF(2^n) – Construction
   D. Vector Spaces
   E. Advanced Encryption Standard (AES) Algorithm
   F. Attacks on DES and AES

6. Encryption – Asymmetric Techniques
   A. Background
   B. RSA Public-Key Cryptosystem
   C. Factoring Integers
   D. Efficient Exponentiation
   E. RSA Cryptanalysis

7. Data Integrity Techniques
   A. Cryptographic Hash Functions
   B. SHA-1

8. Key Exchange Protocols
   A. Diffie-Hellman
   B. Computing Discrete Logarithms
   C. Group Selection (Focus on Elliptic Curve Groups)