ECE 8372 / CS 8352 CRYPTOGRAPHY & DATA SECURITY

Course Syllabus **Professor Jim Dunham**
17 Jan 2020 **Spring 2020**

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 or studied.

Prerequisite: STAT/CS 4340 *Statistical Methods for Engineers and Applied Scientists*, or ECE 3360 *Statistical Methods in Electrical and Computer Engineering* or equivalent. Ability to program.

Credit: 3 Term-Credit Hours (TCH)

Textbook: *Understanding Cryptography: A Textbook for Students and Practitioners*, Paar and Pelz, Springer-Verlag Berlin Heidelberg 2010 , ISBN 978-3-642-04100-6 e-ISBN 978-3-642-04101-3. (Free Download)

Lectures: Tu, Th 3:30 PM – 4:50 PM Caruth Hall 183

Office Hours: Tu, Th, 1:00 PM – 2:20 PM By Appointment

Office Location: Junkins Building 321
Office Phone 214-768-3112
Email james.dunham@lyle.smu.edu
Class Web Site https://s2.smu.edu/~jgd/

University Calendar:

Monday	January 17	First Day of Instruction
Monday	January 20	University Holiday – MLK Day
	March 16-22	Spring Break
Tuesday	April 7	Last Day to Drop a Course (Grade W)
Friday	April 10	University Holiday – Good Friday
Friday	April 24	Last Day to Withdraw from the University
Monday	May 4	Last Day of Instruction (Friday Schedule)
Tuesday	May 5	Reading Day
Thursday	May 7	Final Exam 3:00 PM – 6:00 PM
Saturday	May 16	Commencement

Grading Policy:

Homework	40 %
Presentation	20 %
Paper/Project	40%

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 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. I reserve the right to administer a different, but comparable, make-up examination.

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 reserve the right to begin pro-rating the homework at the rate of a TBD rate 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:

Students needing academic accommodations for a disability must first register with Disability Accommodations & Success Strategies (DASS). Students can call 214-768-1470 or visit http://www.smu.edu/Provost/ALEC/DASS to begin the process. Once registered, students should then schedule an appointment with the professor as early in the semester as possible, present a DASS Accommodation Letter, and make appropriate arrangements. Please note that accommodations are not retroactive and require advance notice to implement.

Religious Observance:

Religiously observant students wishing to be absent on holidays that require missing class should notify their professors in writing at the beginning of the semester, and should discuss with them, in advance, acceptable ways of making up any work missed because of the absence. (See "Religious Holidays" under University Policy No. 7.22).

Excused Absences for University Extracurricular Activities:

Students participating in an officially sanctioned, scheduled University extracurricular activity should 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 the instructor prior to any missed scheduled examination or other missed assignment for making up the work. (See 2018-2019 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' 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.

Assessment

The course is subject to SACS assessment. In particular, the following Student Learning Outcomes (SLOs) are subject to assessment:

SACS Outcome I: An ability to use the techniques, skills, and modern tools necessary for practice in the discipline.

SACS Outcome II: An ability to apply knowledge of mathematics and science to applications.

SACS Outcome III: An ability to identify, formulate, and solve problems.

SACS Outcome IV: Ability to communicate effectively.

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
4. Encryption – Symmetric Techniques
   A. Modern Algebra Review
   B. Binary Fields – GF(2^n) – Construction
   C. Data Encryption Standard (DES) Algorithm
   D. Advanced Encryption Standard (AES) Algorithm
   E. Attacks on DES and AES
5. Computational Complexity
   A. Introduction
   B. Turing Machines
   C. Complexity Classes
   D. Applications to Cryptography
6. Encryption – Asymmetric Techniques
   A. Background
   B. RSA Public-Key Cryptosystem
   C. Factoring Integers
   D. Efficient Exponentiation
   E. RSA Cryptanalysis
7. Key Exchange Protocols
   A. Diffie-Hellman
   B. Computing Discrete Logarithms
8. Hash Function & Algorithms
9. Elliptic Curve Cryptography
   A. Elliptic Curves Basics
   B. Chinese Remainder Theorem
   C. NIST Elliptic Curves
   D. Applications
10. Quantum Cryptography
11. Blockchain