Department of Computer Science

nue I
Academic Building One

Huntsville, Texas
P.O. Box 2090 • 77341-2090

(936) 294-3846
Fax • (936) 294-4312

DFSC 3316-01: Cryptography and Network Security, CID: 21890
Course Syllabus
Spring 2018 – Jan 17, 2018 – May 10, 2018

Lectures: 11:00 AM - 11:50 AM M, W, F. AB I, Room 209.

General Information

Instructor: Dr. Narasimha Karpoor Shashidhar
Office: AB1 216B
Phone: 936 294 1591
Email: karpoor@shsu.edu

Course Title: Cryptography and Network Security
Course Code: DFSC 3316.01
Office Hours: M,W,F 8 AM to 10 AM, 1 PM to 2 PM.

Course Description:

This course is an introduction to modern cryptography and network security. Cryptography, broadly speaking, is about communicating in the presence of an adversary, with goals like preservation of privacy and integrity of communicated data. We will cover symmetric (aka. private key) and asymmetric (aka. public key) cryptography, including block ciphers, modes of operation, hash functions, digital signatures, asymmetric encryption, RSA, the discrete logarithm problem, public-key infrastructure, key distribution, and various applications. The course will emphasize rigorous mathematical formulations of security goals in the style of "provable security," and aim to train students in spotting weaknesses in designs.

There is no text book for this course. We will be using course handouts, slides and lecture notes posted on Blackboard. Homework assignments and other related material will be posted on Blackboard as well. On occasion, we will refer to the Introductory Cryptography Lecture Notes by Goldwasser and Bellare available on Blackboard.

As a broad overview of the course, we will be discussing topics on:

- Chapter 1: Introduction to modern cryptography
- Chapter 2: Classical encryption
- Chapter 3: Block ciphers
- Chapter 4: Pseudorandom functions
- Chapter 5: Symmetric encryption
- Chapter 6: One-way and collision-resistant functions
- Chapter 7: Message authentication
- Chapter 8: Authenticated encryption
- Chapter 9: Computational number theory
- Chapter 10: Number-theoretic primitives
- Chapter 11: Asymmetric encryption
- Chapter 12: Digital Signatures
- Chapter 13: Password-based login
- Chapter 14: Applications
- Chapter 15: The birthday problem

- Chapter 16: Reverse Engineering

Blackboard will be the only source of all course related material including homework problem sets and notes. Hardcopies of these items will not be distributed. Please familiarize yourselves with the Blackboard environment.

While I will try to provide all the prerequisite mathematical foundations required for the course, students are expected to possess a certain level of mathematical maturity and the desire to learn new concepts.

Additional department goals supported by this course include: a) developing a strong technical foundation in the computational sciences, b) an understanding and sensitivity for professional ethics, c) appreciation for the need to pursue professional and related learning activities for life. Students are expected to: a) employ quantitative (mathematical) evaluations in seeking optimal problem solutions, b) maintain and increase their professional knowledge/skill sets, c) develop their ability to express abstractions in the form of algorithms in the frame work of established software engineering practice and d) to extend the discipline through original cognitive processes.

You are encouraged to please drop by my office to ask questions, get help, or otherwise talk about the material. You could of course email me anytime, but you will soon realize that it is much harder to make yourself understood over email, with the result that at times you may be asked to come see me instead.

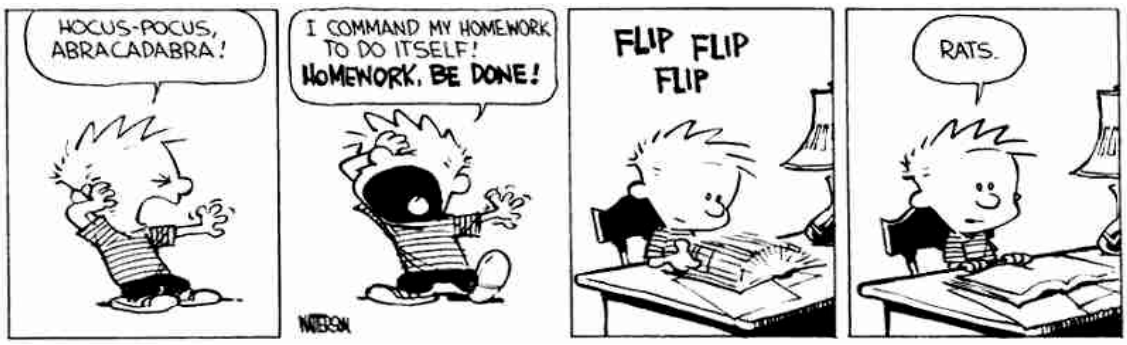
Attendance:

Attendance is required. We will complete group and individual in class assignments and conduct discussions on a regular basis. If you are not in class when an in class assignment is done, then you will not receive credit for that assignment. Exceptions to this rule are on a case by case basis and must include a scheduled meeting with me along with an official note from a doctor, coach or other person in some official capacity to justify the absence. The same applies to absences in general. If you know you must be absent on a particular day, you must provide me with official documentation of the reason for the absence in order to prevent absence penalties.

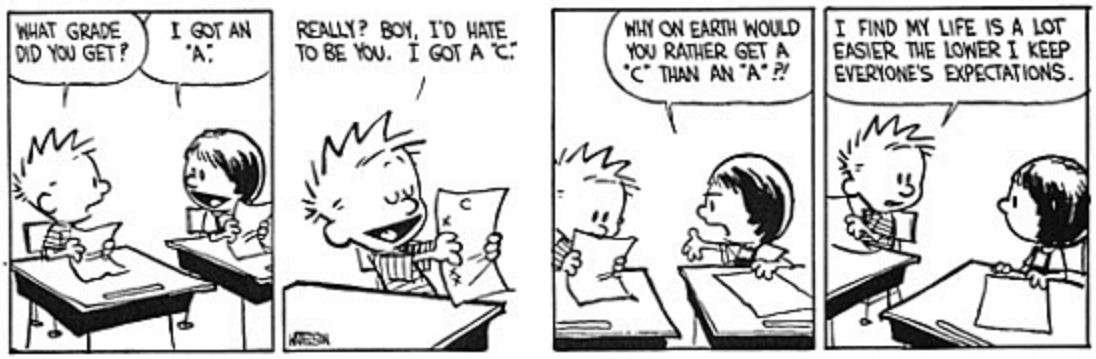
IMPORTANT – Your final course grade will be lowered one letter grade for 5 absences and by 2 letter grades for 10 absences and so on. Do not get into this situation as it applies no matter what your grades are.

Assignments:

I will assign homework as necessary throughout the semester. Homework is an opportunity to demonstrate your knowledge. I expect clear, comprehensive explanations of processes and concepts in written homework assignments. All homework must be neat and must have your name, class and assignment name on the first page. Turn in neat, readable, typeset solutions. If you have more than one sheet, they should be stapled together, not clipped or folded at the corner. If not, points will be deducted. If your name is not on your sheet, points will also be deducted. Deviation from this standard will result in a loss of some or all points. If I cannot read your work you will receive few if any points. In doing homework assignments, you are forbidden from referring to any resources other than your own course notes, the class notes or other material suggested by me. In particular, you are not allowed to consult books. You are not allowed to use materials from previous years of this course, and you are not allowed to use the Internet to "find" solutions.



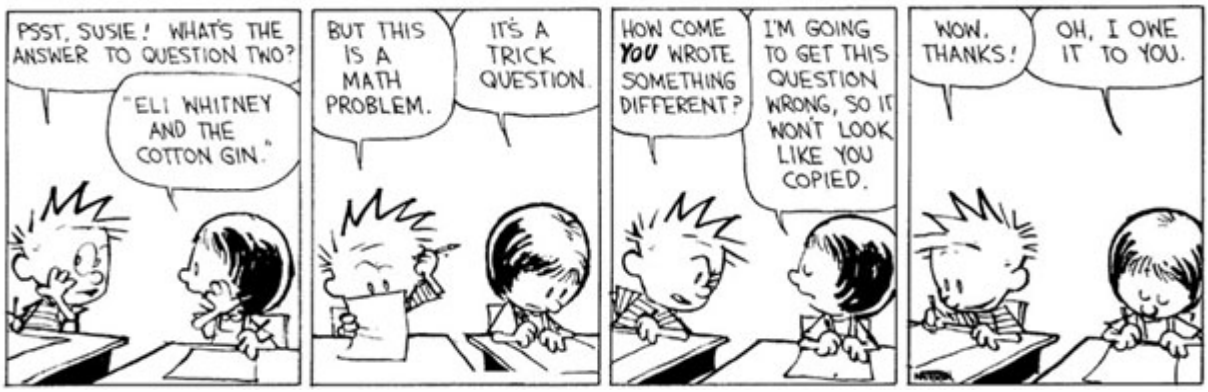
Grade-related questions: It is not possible to provide answers to questions such as the following during the course: "What scores do I have to get for the rest of this class in order to get such and such grade?" "What is the cutoff score for such and such a grade?" "What were the cutoff scores, or what was the grade distribution, in previous years the class was taught?"



Late work will not be accepted without a scheduled meeting with me along with an official note from a doctor, coach or other person in some official capacity to justify the reason for the late work.

Group Work: All assignments and in-class work are individual unless specifically stated otherwise. I will periodically allow work to be completed in groups, but I will specifically indicate which ones. Any violation of this policy will result in a zero on the assignment.

Cheating on homework WILL NOT be tolerated. A grade of "F" for the assignment/course and appropriate disciplinary action will be taken to any student caught cheating.



DO NOT:

Disrupt the class in any way.
Leave class early unless you have made prior arrangements.
Disrupt the class if you come in late (make every effort to be on time)

A 100 point grade reduction will be incurred for each instance of an above action.
Disruptive behavior will be reported to the Dean of Student Life, Campus Security or both.
Students who disrupt the class more than once will receive an "F" for the course

Grading:

Your final grade is computed as a percentage from the number of points earned divided by the number of points possible. The minimum percentage to earn an A is 90%, a B is 80%, a C is 70%, and a D is 60%.

There are no makeup exams under any circumstances whatsoever. The only acceptable reason to miss a quiz is that the student has a personal health problem at the time and can provide the instructor with adequate documentation to verify this. For a student with such a medical excuse, arrangements will be made to shift the weight of the quiz to the final.

I warmly welcome you all to this course and guarantee that you will learn much from it and enjoy it thoroughly. My only request is that you are prepared to work hard and sincerely.

Email: Email communication is the best way to communicate with me outside of my office hours during the semester. I will not respond to Email that does not follow appropriate etiquette. At a minimum, your email must include your name, and specifics of your question. It must not include common IRC chat lingo or shorthand. If your email does not conform to the above mentioned minimum requirements, then your email will not be answered. Please be professional in your communication. If you are missing a grade on Blackboard, you may email me a short note informing me of a possible mistake. I will file this note and check on it. I will not, however, discuss grades via email or any other electronic communication. If you have a question about a grade you received, you are required to make an appointment with me in my office so we can discuss it.

Exams: There will be 3 major exams and a final. The final exam will be comprehensive. Tests are writing intensive and require that you understand the material. Prepare to use the exam as an opportunity to demonstrate your mastery of the subject matter. Answers with little detail or that demonstrate a lack of mastery of the subject matter will result in few if any points.

Cheating on exams or homework WILL NOT be tolerated. A grade of "F" for the course and appropriate disciplinary action will be awarded to any student caught cheating.

Blackboard will be the only source of all course related material including homework problem sets and additional notes. Please familiarize yourselves with the course environment. While I will try to provide all the prerequisite foundations materials required for the course, students are expected to possess a certain level of computing maturity and the desire to learn new concepts and naturally willing to work hard in this process to succeed in the course
Additional goals supported by this course include: a) developing a strong technical foundation in the computational sciences, b) an understanding and sensitivity for security and professional ethics, c) appreciation for the need to pursue professional and related learning activities for life. Students are expected to: a) employ critical thinking in seeking optimal problem solutions, b) maintain and increase their professional knowledge/skill sets, c) develop their ability to express their skills using tools and related analysis techniques and d) to extend the discipline through original cognitive processes..

Instructional Methods
This course is designed to promote learner-centered activities and support the development of cognitive strategies and competencies necessary for effective task performance and critical problem solving. The course utilizes individual and some group learning activities, performance-driven assignments, problem-based cases, projects, and discussions. These methods focus on building engaging learning experiences conducive to development of critical knowledge and skills that can be effectively applied in professional contexts.

Suggested Learning Approach
In this course, you will be studying individually and within a group of your peers. As you work on the course deliverables, you are encouraged to share ideas with your peers and instructor, work collaboratively on projects and team assignments, raise critical questions, and provide constructive feedback. You are encouraged to actively participate in the discussion forums on Blackboard in an effort to learn from your classmates. I will periodically monitor these discussion forums and offer comments to facilitate discussions. This serves to enrich the "virtual" classroom and make the material more exciting, inviting and above all fun!
Use the following advice to receive maximum learning benefits from your participation in this course:

DO	DON'T
▪ Do take a proactive learning approach ▪ Do share your thoughts on critical issues and potential problem solutions ▪ Do plan your course work in advance ▪ Do explore a variety of learning resources in addition to the textbook ▪ Do offer relevant examples from your experience ▪ Do make an effort to understand different points of view ▪ Do connect concepts explored in this course to real-life professional situations and your own experiences	▪ Don't assume there is only one correct answer to a question ▪ Don't be afraid to share your perspective on the issues analyzed in the course ▪ Don't be negative towards the points of view that are different from yours ▪ Don't underestimate the impact of collaboration on your learning ▪ Don't limit your course experience to merely reading the textbook ▪ Don't postpone your work on the course deliverables – work on small assignment components every day

Class participation

In accordance with University Policy (http://www.shsu.edu/students/guide/polpro/attendance.html), regular attendance is required; however, no points will be awarded or subtracted based on your attendance. You are responsible for all material covered in every class, regardless of whether you attended or not. It is your responsibility to obtain notes, assignments, etc., from fellow class members if you miss a class.

Academic dishonesty

All students are expected to engage in all academic pursuits in a manner that is above reproach. Students are expected to maintain complete honesty and integrity in the academic experiences both in and out of the classroom. Any student found guilty of dishonesty in any phase of academic work will be subject to disciplinary action. The university and its official representatives may initiate disciplinary proceedings against a student accused of any form of academic dishonesty including, but not limited to, cheating on an examination or other academic work which is to be submitted, plagiarism, collusion and the abuse of resource materials. No cheating on an examination or assignments is allowed. A score of zero will be given to the student if such a case occurred.

Rules of conduct

Students will refrain from behavior in the classroom that intentionally or unintentionally disrupts the learning process and, thus, impedes the mission of the university. Please turn off or mute your cellular phone and/or pager before class begins. Students are prohibited from eating in class, using tobacco products, making offensive remarks, reading newspapers, sleeping, talking among each other at inappropriate times, wearing inappropriate clothing, or engaging in any other form of distraction. Inappropriate behavior in the classroom shall result in a, minimally, a directive to leave class or being reported to the Dean of Students for disciplinary action in accordance with university policy.

Visitors in the classroom

Occasional visiting of classes by responsible persons is allowed with prior arrangement with the instructor, as long as it does not interfere with the registered members of the class or the educational process.

Americans with Disabilities Act

According to University policy requests for accommodations must be initiated by the student. A student seeking accommodations should go to the Counseling Center and Services for Students with Disabilities (SSD) for instructions.

Religious Holidays

An institution of higher education shall excuse a student from attending classes or other required activities, including examinations, for the observance of a religious holy day, including travel for that purpose. A student whose absence is excused under this subsection may not be penalized for that absence and shall be allowed to take an examination or complete an assignment from which the student is excused within a reasonable time after the absence.