Department of Computer Science

1803 Avenue I
Suite 214, Academic Building One

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

(936) 294-3846
Fax • (936) 294-4312

COURSE SYLLABUS
Cryptography and Network Security
DFSC 3316-01 Fall 2017

Location: Academic Building 1, Room 209
Time: Tuesdays and Thursdays, 12:30-1:50 pm
Instructor: Dr. Umit Karabiyik (Preferred to be called **Dr. K)**
Office: Academic Building 1, Room 212E
E-mail: umit@shsu.edu
Phone: (936) 294-4785 (leave VM if unanswered)
Office hours: Tuesdays/Thursdays 9:30am - 11:00 am, or by appointment
TA Name/email: Naciye Celebi – nxc038@shsu.edu
TA Hours: TBA

Course description: This course involves the study of both the theory and practice of cryptography and computer and network security, and focuses on the security aspects of the web and the internet. It surveys cryptographic tools used to provide security, such as shared key encryption, public key encryption, key exchange, and digital signature algorithms. It then reviews how these tools are used in the current Internet protocols and network security applications. System security issues, such as viruses, worms, intrusion, and firewalls may also be discussed. **Prerequisite:** DFSC 2316 and MATH 2395. **Credit:** 3 hours.

Department Goals: 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 and d) to extend the discipline through original cognitive processes.

Instructor's Objectives:

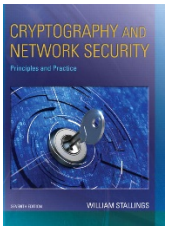
Essential: Learning fundamental principles, generalizations, or theories.

Important: Learning to apply course material (to improve critical thinking, problem solving, and decisions)

Required Text:

Cryptography and Network Security: Principles and Practice, 7th Edition by William Stallings

ISBN-10: 1285060032
ISBN-13: 978-1285060033



Course Requirements:

Assignments:

- There will be multiple and various assignments including homework and programming labs. Assignment due dates will be posted along with the assignments files and course Blackboard page.
- Most assignments are writing intensive and require that you understand the material thoroughly. Answers with little detail or that demonstrate a lack of mastery of the subject matter will result in few if any points.
- Lab assignments may require students to develop programs related to course content. This will allows students to understand the real life implementation of current state of the art cryptosystems.

- Each homework assignment contains a number of questions relevant to the course content (including textbook and lectures) as well as possible research components which require students to conduct individual research and possible lab exercises.
- All type of assignments must be typed in Microsoft Word document and submitted to the relevant **BLACKBOARD PAGE** by due dates. The name of all submitted assignment files must be in this format **"[first&last_name] - DFSC 3316 A2"** which indicates Assignment 2 submission of a student for this course.
- In doing any of your 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 your friends. You are not allowed to use materiel from previous years of this course, and you are not allowed to use the Internet to "find" partial/complete solutions if the instructor does not explicitly direct you.
- **Copying and plagiarism is prohibited** (*read related document on Blackboard*). Assignments must be done individually by each student unless specified otherwise. Cheating on homework **WILL NOT** be tolerated. A grade of **"F"** for the assignment/course and appropriate disciplinary action will be awarded to any student caught cheating.
- All assignment documents should contain the name of student and the date on which assignment was submitted. Failure on this will cause point deduction.
- If any programming is required in the assignments, codes/scripts must be provided in the submission.

Quizzes:

Extended-length quizzes (considering it as mini-exams) will be given regularly throughout the course. It covers contents in the slides and the lectures. This form of quizzes has shown (in my previous courses) to be an effective way of learning as it promotes timely review of course materials. Date and scope of the quizzes will be announced in class. There will be absolutely no make-up for the quizzes.

Course Project:

Students are required to complete a significant course project. The project should be cryptography and security related, but not limited to network security. For example, the topics such as operating system security, virtualization security, or mobile security are all welcomed. Students should try to come up project ideas that are suitable to their skills and schedule. Otherwise, a list of project ideas will be provided in the course Bb page for students to choose from. The project idea should be discussed and approved by the instructor. Each project will have two members (at most) with shared responsibility. With the instructor's permission, a student can complete the project by him-/her-self. No extra credit will be given because of this.

The schedule and deliverable of the project are:

Sep 14th: Form a team, discuss with the instructor about the project idea (each team twenty minutes), submit a one page project proposal.

Oct 26th: Mid-semester project report, submit a three-page report.

Nov 30th: In class project presentation. Schedule will be announced.

Dec 5th: Final project due, submit source code and five-page final project report.

The writing should follow the IEEE (template) format. See PDF example here! If different format is used, 10% penalty will be applied.

Exams:

There will be two midterms for this course. The midterms will be scheduled as the semester progresses and related information will be discussed in class and be available on Blackboard. Generally speaking, no make-up for the exams will be provided. Students with legitimate excuses should contact the instructor before the midterm (giving in advance notice), with appropriate document, to arrange a make-up exam. No final exam will be schedule for the course. Instead, the students are expected to complete a significant course project. According to the SHSU registrar, the final exam is scheduled on Tuesday (12/05/2014) 1pm - 3pm. Since we do not have final exam, this time slot might be used for the make-up exam of midterm for excused students. **Note that your final paper submission due is on your scheduled final day by 3pm**. Absolutely no extension will be given for the final paper.

Late Policy:

Late submission to the homework will be accepted **up to two days** after the deadline with a penalty of 10% of the assignment each day. Students with legitimate excuses should contact the instructor before the deadline, if possible, and submit appropriate document afterwards to be exempted from this rule. Submission page for the assignments will be unavailable on the third late day since **it's too late.**

Grading plan:

Assignments	30%	(Tentatively 4 homework & 2 Labs)
Midterms	40%	(2 Exams)
Course Project	20%	(Paper and presentation)
Quizzes	10%	

Grading Criteria:

>= 90	A
>= 80 but < 90	B
>= 70 but < 80	C
>= 60 but < 70	D
< 60	F

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?"

Email

Email communication is naturally the best way to communicate with me outside of my office hours. Please understand that I will not respond to an 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 (Read the note on Professor's office door). 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 try to respond to your emails as promptly as possible.

Online Course Resources

All course materials can be found on Blackboard at https://blackboard.shsu.edu/webapps/login/. All students must check their SHSU email accounts regularly because instructor may send important announcements via email.

Class participation

In accordance with University Policy (http://www.shsu.edu/dotAsset/b719129b-9593-424f-9d5a-920e2eda6890.pdf), 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, discussion material etc., from fellow class members if you miss a class. Instructor will be using student attendance frequency to identify the borderline grades.

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 (if you still have one) 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.

Students with disabilities policy
It is the policy of Sam Houston State University that individuals otherwise qualified shall not be excluded, solely by reason of their disability, from participation in any academic program of the university. Further, they shall not be denied the benefits of these programs nor shall they be subjected to discrimination. Any student with a disability that affects his/her academic performance should contact the Office of Services for Students with Disabilities in the SHSU Lee Drain Annex (telephone 936-294-3512, TDD 936-294-3786) to request accommodations. They should then make arrangements with their individual instructors so that appropriate strategies can be considered and helpful procedures can be developed to ensure that participation and achievement opportunities are not impaired.

SHSU adheres to all applicable federal, state, and local laws, regulations, and guidelines with respect to providing reasonable accommodations for students with disabilities. If you have a disability that may affect adversely your work in this class, then I encourage you to register with the SHSU Services for Students with Disabilities and to talk with me about how I can best help you. All disclosures of disabilities will be kept strictly confidential. NOTE: No accommodation can be made until you register with the Services for Students with Disabilities. For a complete listing of the university policy, see: http://www.shsu.edu/dept/academic-affairs/documents/aps/students/811006.pdf

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.

Syllabus Chance Policy
Except for changes that substantially affect implementation of the evaluation (grading) statement, this syllabus is a guide for the course and is subject to change with in advance notice.

Tentative Class Schedule

Week	Date	Reading Assignments & Information	Information on Homework Assignments, Tests and Course Project
1		Chapter 1	Study syllabus and study Ch. 1 Computer and Network Security Concepts
2		Chapter 2	Study Ch. 2 Introduction to Number Theory,
3		Chapter 3 & 4	Study Ch. 3 Classical Encryption Techniques and Ch. 4 Block Ciphers and the DES
4		Chapter 6 & 7	Study Ch. 6 Advanced Encryption Standard and Ch. 7 Block Cipher Operation, **Submit your project Proposal and Complete Assignment 1**
5		Chapter 8 & 9	Study Ch. 8 Random Bit Generation and Stream Ciphers and Ch. 9 Public-Key Cryptography and RSA
6		Chapter 10 & 11	Study Ch. 10 Other Public-Key Cryptosystems and Study Ch. 11 Cryptographic Hash Functions
7		Exam Review	**Complete Assignment 2**
			Midterm Exam 1
8		Chapter 12	Study Ch. 12 Message Authentication Code, **Complete Lab Assignment 1**
9		Chapter 13 & 14	Study Ch. 13 Digital Signatures and Ch. 14 Key Management and Distribution
10		Chapter 15	**Submit your mid-semester project report** and study Ch. 15 User Authentication, **Complete Assignment 3**
11		Chapter 16	Study Ch. 16 Network Access Control and Cloud Security
12		Chapter 17	Study Ch. 17 Transport-Level Security, **Complete Lab Assignment 2**
13		Chapter 18	Study Ch. 18 Wireless Network Security and Ch. 19 Electronic Mail Security **Complete Assignment 4**
		Exam Review	
14			**Midterm Exam 2**
		No Class	**Happy Thanksgiving!**
15		Research Presentations	**Presenting your course project**
16		Project Paper	Research Paper Due