Greensheet

CS 265: Cryptography and Computer Security | **San José State University**

Spring 2020, Section 01 | **Department of Computer Science**

Instructor Info

Instructor	**Ahmad Yazdankhah**	My name is difficult to pronounce!
Office Location	MH 212	MacQuarrie Hall, Room #212
Email	ahmad.yazdankhah@sjsu.edu	
Website *	Under construction!	Our official educational web tool is Canvas available at https://sjsu.instructure.com/
Phone	(408) 924-5060	Email is the best way to communicate with me!
Office Hours	TR 7:15pm – 9:15pm	By appointment please! I'll be in the class room DH 450.

* Course materials such as handouts, notes, assignment instructions, etc. can be found on *Canvas Learning Management System* available at http://sjsu.instructure.com. You are responsible for regularly checking with its messaging system (or other communication system as indicated by the instructor) to learn of any updates.

Class Info

	Section 01
Meeting Time	TR 6:00pm – 7:15pm
Classroom	DH 450
Course Number	27542

General Events of Semester

Description	**Day of Week**	**Month**	**Day #**	**Comment**
First day of instruction	Thursday	January	23	
Last day to drop	Tuesday	February	4	
Last day to add	Tuesday	February	11	
Daylight saving time	Sunday	March	8	
Spring Break	Mon-Fri	March-April	30 - 3	Recess
Last day of instruction	Monday	May	11	Thursday, May 7th for our class
Final Examinations	Wed-Fri, Mon-Tue	May	13-15, 18-19	Please look at the bottom of the syllabi at page 5 for the final exam info of this course
Grades due from faculty	Friday	May	22	End of semester

For academic events of this semester, please refer to the course syllabus at page 5.

Course Info

Catalog Description

Security mechanisms for protecting information in computer systems and networks. Includes cryptography and its applications to security services in distributed systems, mathematics of cryptography, access control, protection models, security policies, design of secure systems, firewalls, and intrusion detection.

Prerequisites

CS 149	Operating Systems	Grade C minus or better

The Department of Computer Science strictly enforces prerequisites.

If you are not already pre-enrolled, you must attend the first day of the class and let your instructor know and fill out the provided document. If the class is not full, the permission codes will be provided to the requesters based on the priorities. More information will be given in the first day of the class.

Please note that any student who does not show up during the first two class meetings, may be dropped by the instructor.

Required Text

There is no required text for this course. My lecture notes contain all required materials.

Further Readings

1. Stamp, Mark and Low, Richard M., "Applied Cryptanalysis: breaking ciphers in the real world," John Wiley & Sons, Inc., New Jersey, USA, 2007
2. Stallings, William, "Cryptography and Network Security, Principles and Practice, 6th ed.," Pearson, USA, 2014
3. Paar, Christof, "Understanding Cryptography," Springer, Berlin, Germany, 2010
4. The references at the end of each lecture note.

Course Learning Outcomes (CLO)

Upon successful completion of this course, students would be able to:

1. Understand the major principles of cryptography for designing secure cipher systems.
2. Understand different classes of cipher systems such as: classical, stream, block, public-key.
3. Analyze and implement the major cipher systems including but not limited to:
   A5/1, ORYX, PKZIP, RC4 and RC6, CMEA, Akelarre, FEAL, DES, AES, TEA, Knapsack, RSA, and Diffie-Helman.
4. Analyze and implement the major hashing algorithms such as: message digest (MD4, MD5), secure hash algorithm (SHA), HMAC, digital signature, and so on.
5. Get familiar with major types of attacks such as: brute-force, statistical, chosen plaintext, ciphertext only, forward search, birthday, and so on.
6. Understand intrusion detection.
7. Understand the required mathematics for cryptography such as: modular arithmetic, prime numbers, random and pseudo-random numbers, GCD, Galois fields (GF), Knapsack problem, Birthday problem, and so on.
8. Understand the required hardware model for cryptography such as: linear feedback shift register (LFSR)

Examinations, Assignments, Term Project

- Every week, there would be a programming assignment.
- There would be a midterm, and a final exam.
- There would be a term project.
- All examinations would cover from the beginning of the semester.
- All conceptual examinations would be closed-all-materials.
- All practical examinations would be open-all-materials.

Grading Information

Assignments	50%
Term Project	25%
Midterm	10%
Final	15%
Total	**100%**

Nominal Grading Scale

From	To	Grade
97	100	A plus
93	96.99	A
90	92.99	A minus
87	89.99	B plus
83	86.99	B
80	82.99	B minus
77	79.99	C plus
73	76.99	C
70	**72.99**	**C minus**
67	69.99	D plus
63	66.99	D
60	62.99	D minus
0	59.99	F

To practice time management, late submissions will lose 20% of the total assignment score and an additional 20% for each 24-hour afterward.

Final Grade

- Your final grade might be adjusted depending upon your level and quality of participation in the class activities. Note that "participation" is NOT equal to "attendance".
- If the FINAL grades of the class at the end of the semester are not normal, then I might curve the grades. So, it is not the case that I'd curve all exams and assignments individually.
- More details about final exam can be found in University policy S17-1 available at http://www.sjsu.edu/senate/docs/S17-1.pdf.

Course Requirements and Workload

- A wireless laptop is required for the activities in the class.
- Java is the standard programming language for this course.
- Success in this course is based on the expectation that students will spend at least 6 – 10 hours per week for:
  - working on the assignments.
  - preparation for the exams.
  - working on the term project.

- More details about student workload can be found in University Policy S16-9 available at http://www.sjsu.edu/senate/docs/S16-9.pdf.

Course Format

This will be a combination of lecture-lab format course. Therefore, students will be required to bring a laptop to all sessions.

Classroom Protocol

- Be on time! Coming late is disruptive for the other students and the instructor.
- My classes are always interactive. So, participate in the class' activities as much as you can.
- Ask good questions and answer the others' questions (in class and/or in the Canvas discussion) and get extra credit!
- Cell phones should be in silent mode and should be kept in your pocket or backpack, and should NOT be used during the lectures.
- Laptops should remain closed until I inform you that it is needed for a particular activity.
- Instant messaging, e-mailing, texting, tweeting, etc. are strictly forbidden in my classes.
- Attendance is highly recommended, but is not mandatory, except for exam dates.
  - NOTE that University policy F69-24 available at http://www.sjsu.edu/senate/docs/F69-24.pdf states that:
    "Students should attend all meetings of their classes, not only because they are responsible for material discussed therein, but because active participation is frequently essential to insure maximum benefit for all members of the class. Attendance per se shall not be used as a criterion for grading.
    If a student has been out of school for one or more days, he/she should report to his instructors upon his/her return to inquire about making up the work. Students who know in advance that they will miss one or more classes should inform their instructors about their plans."

Consent for Recording of Class and Public Sharing of Instructor's Material

- Common courtesy and professional behavior dictate that you notify someone when you are recording him/her.
- You must obtain the instructor's permission to make audio or video recordings in this class. Such permission allows the recordings to be used for your private, study purposes only.
- The recordings are the intellectual property of the instructor; you have not been given any rights to reproduce or distribute the material.

University Policies

Per University Policy S16-9 available at http://www.sjsu.edu/senate/docs/S16-9.pdf, relevant university policy concerning all courses, such as student responsibilities, academic integrity, accommodations, dropping and adding, consent for recording of class, etc. and available student services (e.g. learning assistance, counseling, and other resources) are listed on Syllabus Information web page available at http://www.sjsu.edu/gup/syllabusinfo, which is hosted by the Office of Undergraduate Education. Make sure to visit this page to review and be aware of these university policies and resources.

Course Schedule

Note: this is a tentative schedule and is subject to change but with fair notice.

Day#	Date	Lec#	Topics	Assignments
1	01/23	1	Greensheet; A big picture of the course; Who is your professor?	
2	01/28	2	Security terminologies; **Preparing development environment**	
3	01/30	3	Classical ciphers (part 1);	#1
4	02/04	4	Classical ciphers (part 2);	
5	02/06	5	Mathematical preliminaries for cryptography; linear feedback shift register (LFSR)	#2
6	02/11	6	Stream ciphers: A5/1; **Finalizing enrollments;**	
7	02/13	7	Stream ciphers: ORYX	#3
8	02/18	8	Stream ciphers: PKZIP	
9	02/20	9	Stream ciphers: RC4	#4
10	02/25	10	Block ciphers: Feistel model, CMEA	
11	02/27	11	Block ciphers: Akelarre	#5
12	03/03	12	Block ciphers: FEAL	
13	03/05	13	Block ciphers: TEA	#6
14	03/10	14	Block ciphers: DES	
15	03/12	15	Block ciphers: AES (part 1)	#7
16	03/17	16	Block ciphers: AES (part 2)	
17	03/19		Midterm	
18	03/24	17	Public key ciphers: Mathematical preliminaries	
19	03/26	18	Public key ciphers: Knapsack	#8
20	03/31		Spring Break	
21	04/02		Spring Break	
22	04/07	19	Public key ciphers: RSA (part 1)	
23	04/09	20	Public key ciphers: RSA (part 2),	#9
24	04/14	21	Diffie-Hellman Key Exchange; Digital signature	
25	04/16	22	Hashing: MD Family algorithms	#10
26	04/21	23	Hashing: SHA Family algorithms	
27	04/23	24	Access control and Protocols (part 1)	#11
28	04/28	25	Access control and Protocols (part 2)	
29	04/30		Students presentations	
30	05/05		Students presentations	
31	05/07		Students presentations; Study guide for final; **Pizza party!**	

Final exam	**Section 01 (TR 6:00pm – 7:15pm)**
Date and Time	Thursday, May 14 @ 5:15pm
Venue	DH 450