Greensheet

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

Fall 2021, Section 02 | **Department of Computer Science**

Instructor Info

Instructor	**Ahmad Yazdankhah**	My name is difficult to pronounce!
Office Location	Online	Physically it is MH 411 but we won't use it at all.
Email	ahmad.yazdankhah@sjsu.edu	Please email me via Canvas
Website *		Our official educational web tool is Canvas available at https://sjsu.instructure.com/
Phone		Email is the best way to communicate with me!
Office Hours	Thurs 16:00 – 18:00	By appointment please!

* Course materials such as handouts, notes, assignment instructions, etc. can be found on *Canvas Learning Management System* available at http://sjsu.instructure.com. Students 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

Meeting Time	MW 17:45 – 19:00
Classroom	Online - Zoom
Course Type	Online

General Events of Semester

Description	**Day of Week**	**Month**	**Day #**	**Comment**
First day of instruction	Thursday	August	19	Monday August 23 for MW classes
Last day to drop	Tuesday	August	31	
Holiday	Monday	September	6	Labor Day – Campus Closed
Last day to add	Wednesday	September	8	
Daylight saving time	Sunday	November	1	
Holiday	Wednesday	November	24	Non-Instructional Day for Thanksgiving
Last day of instruction	Monday	December	6	
Final Examinations	Wed-Fri, Mod-Tue	December	8 - 10 13 - 14	Please look at the syllabi at page 5 for the final exam info
Grades due from faculty	Friday	December	17	End of semester
Grades Viewable on MySJSU	Saturday	December	18	

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 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.
7. 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 computer with microphone and camera is required for this course.
- 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 course will be taught in online format. The lectures will be recorded and provided before the lecture time and students should watch it before attending the class. In each lecture meeting, the lecture will be summarized, last week assignment and quiz will be solved, and students' questions will be responded.

Online Classroom Protocol

- All microphones will be muted automatically when you join the meeting. If you have a question, you need to unmute it or type your question in the chat room.
- The chat room will be private and instructor reads your questions loudly and answer them.
- We won't use camera during the lectures but will use it during the exams. Therefore, you need to get dressed appropriately. **Dressing code** is "**Business Casual**".
- Attendance is highly recommended, but is not mandatory, except for exam times.

  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	08/23	0	Greensheet; A Big Picture of the Course	
2	08/25	1	Enter Cryptology! **Preparing Development Environment**	
3	08/30	2	Classical Ciphers (part 1)	
4	09/01	3	Classical Ciphers (part 2); **Term Project Assignment**	
5	09/06		Holiday: Labor Day	
6	09/08	4	Classical Ciphers (part 3);	#1
7	09/13	5	Stream Ciphers (part 1): A5/1;	
8	09/15	6	Stream Ciphers (part 2): ORYX	#2
9	09/20	7	Stream Ciphers (part 3): PKZIP	
10	09/22	8	Stream Ciphers (part 4): RC4	#3
11	09/27	9	Block Ciphers (part 1): Feistel Model, CMEA	
12	09/29	10	Block Ciphers (part 2): FEAL	#4
13	10/04	11	Block Ciphers (part 3): TEA	
14	10/06	12	Block Ciphers (part 4): DES	#5
15	10/11	13	Block Ciphers (part 5): AES	
16	10/13	14	Block Ciphers (part 6): Wrapping Up	#6
17	10/18		Review, Study Guide, Q & A	
18	10/20		Midterm	#7
19	10/25	15	Public key Ciphers (part 1): Mathematical Preliminaries 1	
20	10/27	16	Public key Ciphers (part 2): Mathematical Preliminaries 2	
21	11/01	17	Public key Ciphers (part 3): Knapsack	
22	11/03	18	Public key Ciphers (part 4): Mathematical Preliminaries 3	#8
23	11/08	19	Public key Ciphers (part 5): RSA	
24	11/10	20	Diffie-Hellman Key Exchange; Digital Signature	#9
25	11/15	21	Hashing: Mathematical Preliminaries	
26	11/17	22	Hashing: MD and SHA Family Algorithms	#10
27	11/22		Students Presentations	
28	11/24		Holiday: Thanksgiving Day	
29	11/29		Students Presentations	
30	12/01		Students Presentations	
31	12/06		Review, Study Guide, Q & A	

Final exam	Section 02 (MW 17:45 – 19:00)
Date and Time	Wednesday, December 08 @ 17:15
Venue	Online