

San José State University
School/Department
Computer Science 265: Cryptography and Computer Security, Fall 2017

Course and Contact Information

Instructor:	Auston Davis
Office Location:	MacQuarrie Hall 217
Telephone:	650-454-6044
Email:	auston.davis@sjsu.edu (preferred)
Office Hours:	Mon 6pm – 7pm (online only)
Class Days/Time:	Tu/Thu 6:00 – 7:15pm
Classroom:	MacQuarrie Hall 233
Prerequisites:	CS149 or instructor consent

Course Format

This is a traditional classroom lecture type format. Students will be required to bring a functional laptop to all quizzes, the midterm and final

Canvas

Course materials such as syllabus, handouts, notes, assignment instructions, etc. can be found on the [Canvas Learning Management System course login website](http://sjsu.instructure.com) at <http://sjsu.instructure.com>. You are responsible for regularly checking with the messaging system through [MySJSU](http://my.sjsu.edu) at <http://my.sjsu.edu> (or other communication system as indicated by the instructor) to learn of any updates.

Course Description

This course focuses on security mechanisms for protecting information in computer systems and networks. This 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.

Course Learning Outcomes

Upon successful completion of this course, students will be knowledgeable of the major technical security challenges in each of the following four areas: cryptography, access control, protocols, and software. In addition, students will have advanced knowledge in cryptanalysis, endpoint defense and software reverse engineering, as evidenced by work on the major projects.

Required Texts/Readings

Textbook

Information Security: Principles and Practice, 3rd Edition, Mark Stamp (Only available via classroom purchase)

San José State University
School/Department

Computer Science 265: Cryptography and Computer Security, Fall 2017

Other Readings

- ***A Bug Hunter's Diary: A Guided Tour Through the Wilds of Software Security***, Tobias Klein, No Starch Press, 2011. Lots of interesting real-world examples of vulnerable code.
- ***Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software***, Michael Sikorski and Andrew Honig, No Starch Press, 2012. An excellent book for information on reverse engineering (whether for malware analysis or other purposes). Includes many hands-on exercises.
- ***Software Reverse Engineering (SRE) website (<http://reversingproject.info/>)***. This website, which was created by a former masters student, includes lots of good information and detailed exercises with solutions.
- ***Network Security: Private Communication in a Public World***, second edition, Charlie Kaufman, Radia Perlman, and Mike Speciner, Prentice Hall, 2002, ISBN: 0-13-046019-2. This book provides good coverage of cryptography and excellent coverage of several security protocols.
- ***Security in Computing***, third edition, Charles P. Pfleeger and Shari Lawrence Pfleeger, Prentice Hall, 2003, ISBN: 0-13-035548-8. The strength of this book is its coverage of the security issues related to software. In particular, operating systems and some aspects of secure software engineering are covered well. This book also has some good, basic information on viruses.
- ***Applied Cryptography: Protocols, Algorithms and Source Code in C***, second edition, Bruce Schneier, John Wiley & Sons, Inc., 1995, ISBN: 0-471-11709-9. For better or for worse, in industry, this is the standard reference for all things cryptographic.
- ***Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses***, Ed Skoudis with Tom Liston, Prentice Hall, 2006, ISBN: 0-13-148104-5. There are many books that claim to provide information on how to foil hackers, but this is by far the best that I have seen. This is an updated version of the original Counter Hack, published in 2001.
- ***Computer Viruses and Malware***, John Aycock, Springer, 2006, ISBN: 0387302360. This book gives a good introduction to research topics related to malware. The book is well-written and surprisingly easy reading, given the technical nature of the material.

Course Requirements and Assignments

- **Lectures**: Students are strongly encouraged to attend all lectures. Any material presented in any lecture may be tested in any subsequent quiz, midterm or final exam. Quite a bit of material that is covered in class only will be necessary to successfully complete the projects, quizzes, mid-term and final.
- **Assignments**: There will be a total of 4 assignments due. Assignments are due no later than midnight the day they are due. No late homework will be accepted for any reason. Assigned problems typically require a solution and an explanation (or work) detailing how you arrived at your solution. Cite any outside sources used to solve a problem.

Save your homework to a Zip file named cs265hmk<assignment#><last name><last 4 of student number>.zip. Upload this file to the corresponding assignment in Canvas.

San José State University
School/Department

Computer Science 265: Cryptography and Computer Security, Fall 2017

- Quizzes: Students will have 6 quizzes. Quizzes will be open-book and administered in class via the Respondus LockDown Browser. The student is responsible for ensuring their browser is functional. Makeup quizzes will only be given in cases of a verifiable emergency and at the discretion of the professor. Be aware, makeup quizzes tend to be significantly more difficult.
- Projects: Students are expected to complete two projects over the course of the semester. The Cryptology Project (Project #1) and Spoofing Project (Project #2) information is provided in separate documents and posted to Canvas
- Midterm Exam: The midterm exam will be held on Oct 17th. The midterm will be in-class, closed-book, and comprehensive. Makeup midterm exams will only be given in cases of a verifiable emergency and at the discretion of the professor.
- Final Exam: Tuesday, Dec 19: 5:15 PM – 7:30 PM. Makeup final exams will only be given in cases of a verifiable emergency and at the discretion of the professor.

Grading Information

In addition to the stipulations provided above, grading will be based on the following:

Assignments: 15%
Quizzes: 21%
Projects: 30%
Midterm: 15%
Final: 21%

Grading Scale:

Percentage	Grade
92 and above	A
90 - 91	A-
88 - 89	B+
82 - 87	B
80 - 81	B-
78 - 79	C+
72 - 77	C
70 - 71	C-
68 - 69	D+
62 - 67	D
60 - 61	D-
59 and below	F

**San José State University
School/Department**

Computer Science 265: Cryptography and Computer Security, Fall 2017

Classroom Protocol

- No extra credit is anticipated
- Wireless laptop is required. Your laptop must remain closed and not on your desk. You will be informed when it is needed for a particular activity
- Cheating will not be tolerated
- Student must be respectful of the teacher and other students
- No disruptive or annoying talking
- Turn off cell phones
- Class begins on time
- Class is not over until I say it's over
- A valid picture ID is required at all times

University Policies

Per University Policy S17-9, university-wide policy information relevant to all courses, such as academic integrity, accommodations, etc. will be available on Office of Graduate and Undergraduate Programs' [Syllabus Information web page](http://www.sjsu.edu/gup/syllabusinfo/) at <http://www.sjsu.edu/gup/syllabusinfo/>"

Course Schedule

This schedule is subject to change with fair notice. Notifications will be made via Canvas

Week	Date	Topics, Readings, Assignments, Deadlines
1	Aug 24	Introduction to the Course
2	Aug 28	<i>[Assignment #1 due]</i>
2	Aug 29	Cryptology - Introduction to Cryptography and Data Security <i>[Collect \$ for Textbook]</i>
2	Aug 31	Cryptology - Crypto Basics. (READING: Chapter 1 - 2 - Stamp)
3	Sep 5	Cryptology – Symmetric Key Crypto. <i>Cryptography Project Topic Due.</i> (READING: Chapter 3.3 - Stamp)

**San José State University
School/Department**

Computer Science 265: Cryptography and Computer Security, Fall 2017

Week	Date	Topics, Readings, Assignments, Deadlines
3	Sep 7	Cryptology - Advanced Encryption Standard (AES). <i>[Quiz #1]</i> (READING: Chapter 3.3 – 3.5 - Stamp)
4	Sep 12	Cryptology - Introduction to Public-Key Cryptography, RSA, Diffe-Heilman (READING: Chapter 4.1 – 4.4 - Stamp)
4	Sep 14	Cryptology – Uses for Public-Key Cryptography. Public-Key Infrastructure (PKI) (READING: Chapter 4.6 – 4.9 - Stamp)
5	Sep 19	Cryptology – Hash Functions. Birthday Attack. Non-Crypto Hashing. Tiger Hash. (READING: Chapter 5.1 – 5.8 - Stamp)
5	Sep 21	Cryptology – Visual Cryptography. Information Hiding. Steganography. <i>[Quiz #2]</i> (READING: Chapter 5.9.1.2 – 5.10 - Stamp)
6	Sep 26	Cryptology – Section Review (READING: Up through Chapter 6 - Stamp)
6	Sep 28	[Cryptography Test] , Access Control - Passwords. (READING: Chapter 7.1 – 7.4 - Stamp)
6	Sep 30	<i>[Assignment #2 due] – Crypto Programming</i>
7	Oct 3	Access Control – Authorization, Orange Book, EAL, Authentication vs Authorization, ACLs (READING: Chapter 8.1 – 8.6 - Stamp)
7	Oct 5	Access Control - Biometrics. Cookies. Single Sign On (SSO). Federated Access. (READING: Chapter 7.4 – 7.8 - Stamp) <i>[Quiz #3]</i>
8	Oct 10	Access Control – Multilevel Security Models, Bell-LaPadula. Compartments. Covert Channel (READING: Chapter 8.7 – 8.8 - Stamp)
8	Oct 12	Access Control - Inference Control, CAPTCHA. 2-Factor Authentication, Access Control Section Review. <i>Cryptography Project (Project #1) Due</i> (READING: Chapter 9.1 – 9.2 - Stamp)
9	Oct 17	MIDTERM – Cryptology – Access Control (READING: Up through Chapter 9.2 - Stamp)
9	Oct 19	Protocols – Network Basics, Simple Protocols. (READING: Chapter 9.3 – 9.4 - Stamp)
10	Oct 24	Protocols - Authentication Protocols. Authentication and TCP. <i>[Quiz #4]</i> (READING: Chapter 9.3 – 9.4 - Stamp)
10	Oct 26	Protocols – Real World Security Protocols: SSH. SSL. IPSEC (READING: Chapter 10.1 – 10.4 - Stamp)

**San José State University
School/Department**

Computer Science 265: Cryptography and Computer Security, Fall 2017

Week	Date	Topics, Readings, Assignments, Deadlines
11	Oct 31	Protocols – Real World Security Protocols: Kerberos. WEP, (Section Review) (READING: Chapter 10.5 - 10.6 - Stamp)
11	Nov 2	[Protocols Test] Software Security - Software Flaws. (READING: Chapter 11.1 - Stamp)
12	Nov 7	Software Security - Buffer Overflow. Stack Smashing Defense. Input Validation Incomplete Mediation. Race Conditions (READING: Chapter 11.2 - Stamp)
12	Nov 9	Software Security – Networking Refresher. Firewalls. Application Proxy. Intrusion Detection Systems, Anti-Virus v. Whitelisting. Anomaly Detection. Defense-in- Depth [<i>Quiz #5</i>] (READING: Chapter 8.9 – 8.11 - Stamp)
13	Nov 14	Software Security – Malware. Trojans. Botnets. Ransomware (READING: Chapter 11.3 – 11.5 - Stamp)
13	Nov 16	Software Security – Reverse Engineering. Secure Software Development. Malware and Defense (READING: Chapter 12.4 – 12.5 - Stamp)
13	Nov 18	<i>[Assignment #3 due] – Security Architect for a Day</i>
14	Nov 21	Software Security – Trusted Operating System. Next Generation Secure Computing Base. <i>Spoofed Email Project (Project #2) Due [Quiz #6]</i> (READING: Chapter 13.1 – 13.5 - Stamp)
14	Nov 23	NO CLASS – THANKSGIVING HOLIDAY
15	Nov 28	Software Security - Software Security (Section Review)
15	Nov 30	[Software Security Test] Computer Forensics – The Forensic Process. Volatile v. Stagnant Data Types.
17	Dec 5	Computer Forensics – Anti-Forensics. [Guest Speaker] – Careers in Information Security
17	Dec 7	Finals Review
17	Dec 9	<i>[Assignment #4 due] – Digital Forensic Investigation (Programming)</i>
Final Exam	Dec 19	TBD