San José State University
College of Engineering/Electrical Engineering Department
EE 282, Internet Security, Section 1, Spring 2012

Instructor:	Chao-Li Tarng, Ph.D.
Office Location:	ENG 383
Telephone:	(408) 924-3656
Email:	chaoli.tarng@sjsu.edu
Office Hours:	Wed 6:00pm – 7:00pm
Class Days/Time:	Mon/Wed 7:30 – 8:45pm
Classroom:	ENG 403
Prerequisites:	EE281, or instructor's permission. Background in internetworking design is a plus.

Faculty Web Page and MYSJSU Messaging (Optional)

Copies of the course materials such as the syllabus, major assignment handouts, etc. may be found on my faculty web page at <TBD>.

You are responsible for regularly checking with the messaging system through MySJSU (or other communication system as indicated by the instructor).

Course Description

The course provides the underlying principles and practices of modern network security. Network security architectures and protocols are examined and emphasis is given to their performance and implementation aspects. Symmetric and public-key encryption schemes are discussed in details. Authentication, hash functions, and key management schemes are also covered and their impacts on computer network security are compared. Several aspect of Network Security related topic to today's implementation like OSI Security, IP Security, etc. would also be discussed.

Course Goals and Student Learning Objectives

1. Learn to identify and define the different threats to network systems: secrecy, authentication and data integrity.
2. Learn Symmetric-Key Algorithms which include Data Encryption Standard (DES), RC4, and Advanced Encryption Standard (AES) are discussed and their performances are compared.

3. Learn the Different types of encryption mode are explained and their pros and con s are discussed and their hardware implementation impacts on performance: Electronic Code Book Mode, Cipher Block Chaining Mode, Cipher Feedback Mode, Stream Cipher and Counter Modes.
4. Learn public-Key Algorithms Key Distribution: Detailed implementations of the RSA algorithm is provided and when it is more practical to implement Public-Key algorithms is discussed.
5. Learn electronic Digital Signatures: are defined using symmetric-key and public-key approaches. Message Digest, MD5, as alternative solutions to digital signature are also discussed.
6. Learn IPsec (IKE): Here we use IKE as study case for security association (SA), authentication and key management schemes.

Required Texts/Readings

Textbook

W. Stallings, Cryptography and Network Security: Principles and Practice, 5th Ed., Prentice Hall 2011 (Required)

Other readings

Kaufman, Network Security – Private Communication in Public World, 2nd Ed., Prentice Hall 2002
S. Singh, The Code Book – The Science of Secrecy from Ancient Egypt to Quantum Cryptography, Anchor Books, 1999

Handouts either posted on the web page or distributed in class.

Classroom Protocol

Students will turn their cell phones off or put them on vibrate mode while in class. They will not answer their phones in class. Students whose phones disrupt the class and do not stop when requested by the instructor will be referred to the Judicial Affairs Officer of the University.

Dropping and Adding

Students are responsible for understanding the policies and procedures about add/drop, grade forgiveness, etc. Refer to the current semester's Catalog Policies section at http://info.sjsu.edu/static/catalog/policies.html. Add/drop deadlines can be found on the current academic calendar web page located at http://www.sjsu.edu/academic_programs/calendars/academic_calendar/. The Late Drop Policy is available at http://www.sjsu.edu/aars/policies/latedrops/policy/**.** Students should be aware of the current deadlines and penalties for dropping classes.

Information about the latest changes and news is available at the Advising Hub at http://www.sjsu.edu/advising/.

Assignments and Grading Policy

Homework & Quiz	10%
Class discussions	5%
Project	20%
Midterm exam 1	20%
Midterm exam 2	20 %
Final exam	25 %
Total	100%

Grade	Overall Score
A+	95-100
A	90-94
B+	85-89
B	80-84
C+	75-79
C	70-74
D+	65-69
D	60-64
F	0-59

Notes:
a. All exams are closed book and notes.
b. Homework assignments will be given regularly and are due one week from the assigned date. Late homework will not be accepted.

University Policies

Academic integrity

Your commitment as a student to learning is evidenced by your enrollment at San Jose State University. The University's Academic Integrity policy, located at http://www.sjsu.edu/senate/S07-2.htm, requires you to be honest in all your academic course work. Faculty members are required to report all infractions to the office of Student Conduct and Ethical Development. The Student Conduct and Ethical Development website is available at http://www.sa.sjsu.edu/judicial_affairs/index.html.

Instances of academic dishonesty will not be tolerated. Cheating on exams or plagiarism (presenting the work of another as your own, or the use of another person's ideas without giving proper credit) will result in a failing grade and sanctions by the University. For this class, all assignments are to be completed by the individual student unless otherwise specified. If you would like to include your assignment or any material you have submitted, or plan to submit for another class, please note that SJSU's Academic Policy S07-2 requires approval of instructors.

Campus Policy in Compliance with the American Disabilities Act

If you need course adaptations or accommodations because of a disability, or if you need to make special arrangements in case the building must be evacuated, please make an appointment with me as soon as possible, or see me during office hours. Presidential

Directive 97-03 requires that students with disabilities requesting accommodations must register with the Disability Resource Center (DRC) at http://www.drc.sjsu.edu/ to establish a record of their disability.

EE 282: Internet Security and Cryptography, Semester: Sprint 2012, Course Schedule

The schedule is subject to change with 2-week notice.

Table 1 Course Schedule

			EE 282 (M/W 7:30pm - 8:45pm) ENG 403	
Week	**Mon**	**Wed**	**Topic**	**Stallings Chapters**
1		1/25	Overview	1
2	1/30	2/1	Symmetric Ciphers- DES	2,3
3	2/6	2/8	Number Theory, Finite Field	4
4	2/13	2/15	Symmetric Ciphers - AES, Block Ciphers	5,6
5	2/20	2/22	Midterm I - 2/22	
6	2/27	2/29	Pseudorandom Number Generation, More Number Theory	7,8
7	3/5	3/7	Public Key Crypto, RSA	9
8	3/12	3/14	Other Public Key Crypto	10
9	3/19	3/21	Crypto Hash Functions	11
10	3/26	3/28	Spring break	
11	4/2	4/4	MAC, Digital Signature	12,13
12	4/9	4/11	Midterm II - 4/9	
13	4/16	4/18	Key Management and Distribution	14
14	4/23	4/25	User Authentication Protocols	15
15	4/30	5/2	Transport-Level Security	16
16	5/7	5/9	Wireless Network Security	17,18
17	5/14	5/16	IP Security, Review	19
	5/21		**Final Mon 5/21 7:45pm - 10:00 pm**	