San José State University
Department of Electrical Engineering

EE 209, Internet Security & Cryptography,
Section 2, Spring 2020

Instructor: Jalel Rejeb
Office Location: ENG 367
Telephone: (408) 924-4007
Email: jalel.rejeb@sjsu.edu
Office Hours: Tu.16:30-17:30, We. 15:00-16:00, by an appointment, or whenever my office door is open.
Class Days/Time: Tu.Th. 15:00 - 16:15PM
Classroom: ENG 341
Course Website: All course handouts, assignments and announcements are posted on SJSU Canvas Website

Prerequisite: EE281/CMPE206 and programming skills, or instructor’s permission.

Course Objectives:
Internet security architectures and protocols are examined. Symmetric and public-key encryption schemes are discussed and their mathematical foundations are examined in details. Alternative for the hardware implementations of for Galois field and modern crypto operations are discussed. Authentication, hash functions, and key management schemes are also covered and their impacts on computer security are compared.

Course Learning Objectives:

• Learn to identify and define the different threats to network systems: secrecy, authentication and data integrity.
• Learn Cryptography Principles: mathematical foundations (number theory) for commonly used crypto –algorithms are discussed.
• Learn Symmetric-Key Algorithms which include Data Encryption Standard (DES), RC4, and Advanced Encryption Standard (AES) are discussed and their performances are compared.
• Learn the Different types of encryption mode are explained and their pros and cons 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.
• 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.
• 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.
• Learn IPsec (IKE)/ EKE: Here we use IKE as study case for security association (SA), authentication and key management schemes.
• SSL and HTTPS, security association (SA), authentication and key management schemes.
• Blockchain Technology (Bitcoin) as an emerging application to cryptography schemes.

Outcomes Assessment:
• Two midterm examinations and a final examination
• Project: consists of hands-on programming assignments and oral presentations
• Pop Quizzes and periodic homework assignments
• Class participation & bonus

Textbook:
1. Handouts/classnotes posted on SJSU Canvas

References:

Grading Information:
The overall course grades (letter-grades) will be assigned based on the cumulative outcome assessment results. The weights of class assignments and the project are as listed below.

<table>
<thead>
<tr>
<th>Assignment</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Midterm Exam 1</td>
<td>15%</td>
</tr>
<tr>
<td>Midterm Exam 2</td>
<td>20%</td>
</tr>
<tr>
<td>Pop Quizzes</td>
<td>20%</td>
</tr>
<tr>
<td>Homework</td>
<td>20%</td>
</tr>
<tr>
<td>Project</td>
<td>20%</td>
</tr>
<tr>
<td>Final Exam</td>
<td>25%</td>
</tr>
</tbody>
</table>

Note: Curving is used to adjust the overall average in case it is lower than 83%
Examinations:

- There will be two midterm exams and a final examination. Exams are closed book and notes.
- Exams cover
  - assigned reading materials from the textbook
  - discussed materials in the lectures
  - class handouts and notes
  - Homework and practice problems
- Exams will be announced at least one week prior to administration.
- There will be no make-up exams (in very special circumstances, written excuse and official proofs are required for make-up exams).
- Final Exam Date: Thursday, May 14, 14:45-17:00

Pop Quizzes

- Quizzes are given on timely fashion. They are based on the most two recent homework assignments, the material and relevant examples discussed on the two most preceding class lectures and homework. There will be at least four quizzes.
- There is no make up for the quiz.
- Only the best four quiz scores are considered.

Homework:

Homework assignments will be given periodically and are not collected, unless it involves paper review or otherwise specified. Quizzes are closely based on homework problems. Homework solutions will be made available online.

Please refer to the class Canvas for handout, homework solutions and announcements. You are responsible for all material posted on Canvas website.

Project:

- Provides hands-on experience to reinforce and *extend* security concepts discussed in class through the implementations and analysis of real-world network security protocols and mechanisms. It is based on client/server platform and socket programming (Unix, BSD Sockets) and requires programing knowledge of C or python.
- The instructor will provide all the necessary specifications, advising and resource, however one of the project objective requires you to learn and do research in your own.
- The project includes presentation and discussion of relevant technical papers and demo of your work to the rest of the class.
# Course Outline

Based on the material of chapters 1-to-13 of the textbook and literature handout and papers.

**Table 1: Course Schedule (Tentative, for reference only)**

<table>
<thead>
<tr>
<th>Week of (Monday)</th>
<th>Topics, Readings, Assignments, Deadlines</th>
</tr>
</thead>
</table>
| 1 1/27 | **Introduction**  
  - Security attacks and security terminology: Trudy, Bob, Alice…  
  - Encryption model and techniques  
  - Block Cipher design principles and modes |
| 2 2/3 | **Symmetric-Key Algorithms**  
  - Symmetric, Substitution, transposition techniques  
  - Steganography  
  - Data Encryption Standard (DES) |
| 3 2/10 | **Symmetric-Key Algorithms**…  
  - Finite Fields— A First Look: GF(2^n)  
  - Encryption modes Electronic Code Book Mode, Cipher Block Chaining Mode, Cipher Feedback Mode, Stream Cipher and Counter Modes. |
| 4 2/17 | **Symmetric-Key Algorithms**…  
  - Advanced Encryption Standard (AES)  
  - Efficient Hardware implementation of GP(p)  
  - Other symmetric ciphers: RC4 and RC5 |
| 5 2/24 | Review… *Exam1* |
| 6 3/2 | **Public-Key Algorithms**  
  - Principles of Public-key cryptosystems  
  - Finite Fields— A Second Look: Prime number, Fermat’s and Euler’s Theorems, Chinese Remainder, Discrete log  
  - Principles of Public-key cryptosystems |
| 7 3/9 | **Public-Key Algorithms**…  
  - RSA algorithm  
  - Key management  
  - Diffie-Hellman key exchange |
| 8 3/16 | Hash Function  
  - MD5  
  - SHA |
| 9 3/23 | Review… *Exam2* |
| 10 3/30 | **Spring Break** |
| 11 4/6 | **Authentication and Digital Signatures**  
  - Authentication protocols using symmetric-keys,  
  - key distribution, Traffic confidentiality. |
| 12 4/13 | **Authentication and Digital Signatures**…  
  - Authentication protocols using public-keys  
  - Digital signatures, and key management |
| 13 4/20 | **Blockchain and Cryptocurrency**  
  - Bitcoin block  
  - Hash and mining in BTC |
| 14 4/27 | **Real World Protocol**  
  - EKE  
  - SSH  
  - SSL exchanged messages (HTTP) |
### Week of (Monday) | Topics, Readings, Assignments, Deadlines
---|---
15 | 5/4 | Project Presentations and Demos
16 | 5/11 | Final Exam  *May 14, 14:45-17:00*

---

**Other Classroom Protocols**

- **University Policies**
  Per [University Policy S16-9](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](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.

  Per [University Policy S16-9](http://www.sjsu.edu/senate/docs/S16-9.pdf) “Success in this course is based on the expectation that students will spend, for each unit of credit, a minimum of 45 hours over the length of the course (normally three hours per unit per week) for instruction, preparation/studying, or course related activities, including but not limited to internships, labs, and clinical practica. Other course structures will have equivalent workload expectations as described in the syllabus.”

---

**EE@SJSU**

**Honesty and Respect for Others and Public Property**

**EE HONOR CODE**

The Electrical Engineering Department will enforce the following Honor Code that must be read and accepted by all students.

“I have read the Honor Code and agree with its provisions. My continued enrollment in this course constitutes full acceptance of this code. I will NOT:

- Take an exam in place of someone else, or have someone take an exam in my place
- Give information or receive information from another person during an exam
- Use more reference material during an exam than is allowed by the instructor
- Obtain a copy of an exam prior to the time it is given
• Alter an exam after it has been graded and then return it to the instructor for re-grading
• Leave the exam room without returning the exam to the instructor.”

Measures Dealing with Occurrences of Cheating
• Department policy mandates that the student or students involved in cheating will receive an “F” on that evaluation instrument (paper, exam, project, homework, etc.) and will be reported to the Department and the University.

A student’s second offense in any course will result in a Department recommendation of suspension from the University