ECE 596C
Cryptography for Secure Communications with Applications to Network Security
Spring 2007
University of Arizona

Instructor: Loukas Lazos
Office Hours: T TH: 1:00 – 2:00 PM and by appointment
Office: ECE 357
Email: llazos@ece.arizona.edu

Lecture Time and Location: T TH 11:00 PM – 12:15 PM, HARV 303

Course Description:
This course provides an introduction to the fundamental principles of cryptography and its applications on the network security domain. Students will become familiar with cryptographic techniques for secure (confidential) communication of two parties over an insecure (public) channel; verification of the authenticity of the source of a message; verification of the integrity of the messages transmitted via an insecure channel and unique identification of the originator of any message. Cryptanalysis attacks against the cryptographic techniques, and attack models will be presented. Furthermore, it will be illustrated how network security and management mechanisms employ cryptography to prevent, detect, and mitigate security threats against the network.


Course Objectives:
Upon the completion of this course, students should have achieved the following objectives:
- Have a fundamental understanding of the objectives of cryptography and network security.
- Become familiar with the cryptographic techniques that provide information and network security.
- Be able to evaluate the security of communication systems, networks and protocols based on a multitude of security metrics.

More specifically, students will gain fundamental understanding of the following (tentative) topics:

Introduction to Information Security - Classical Cryptosystems and Cryptanalysis
- Information security objectives
- Schematic of a secure communication system
- Formal definition of a cryptosystem
- The shift cipher, the substitution cipher, the affine cipher, the permutation cipher, the Hill cipher, the Vigenere cipher, stream ciphers
- Cryptanalysis – attack models, attacks on different ciphers
Shannon’s Approach to Cryptography

- Measures of security
- Perfect secrecy
- Definition of entropy
- One-time pad

Symmetric Key Cryptography

- The notion of a symmetric key cryptography
- The Data Encryption Standard (DES) and differential cryptanalysis
- The Advanced Encryption Standard (AES)

Cryptographic Hash Functions

- Definition of hash functions and properties
- The birthday problem
- Unkeyed hash functions
- Keyed hash functions
- Message Authentication Codes (MAC)
- The Random Oracle Model (ROM)

Authentication

- Definition of authentication
- A simple authentication protocol and possible attacks
- Strong password protocols
- BM Encrypted Key Exchange (EKE)
- Key Distribution Centers (KDC)
- Certification authorities and certificate revocation
- KDC based authentication protocols

Public Key Cryptosystems

- Fundamentals of Public-key Cryptography
- Background on number theory
- The RSA public key cryptosystem
- The ElGamal public key cryptosystem and discrete logs

Digital Signatures

- An RSA based signature scheme
- The ElGamal based signature scheme
- The Schnorr signature scheme
- The Digital Signature Algorithm (DSA)

Key Distribution and Key Agreement Protocols

- Key Predistribution
- Diffie-Hellman key Exchange
- The MTI key Exchange

Network Security

- TCP/IP threats
- The IPSEC protocol
- The SSL and TLS protocols
- Firewalls and Virtual Private Networks (VPNs)
- Electronic mail security
- Worms
- DDoS attacks
- BGB and security considerations

Course Website: www.ece.arizona.edu/~ece596
Important Dates:

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tue Feb 12th</td>
<td>Last day to drop a course so it does not appear on the record of enrollment.</td>
</tr>
<tr>
<td>Tue Feb 12th</td>
<td>First Midterm</td>
</tr>
<tr>
<td>Tue Mar 11th</td>
<td>Last day to drop a course with a withdrawal of “W.” Students must be passing the course in order to withdraw at this time. Signature of the Instructor is required.</td>
</tr>
<tr>
<td>Thur. Apr 3rd</td>
<td>Second Midterm</td>
</tr>
<tr>
<td>Tue May 13th</td>
<td>Final exam 11AM – 1:00 PM HARV 303</td>
</tr>
</tbody>
</table>

Course Assignments and Exams:
There will be weekly homework assignment on the topics covered in class, with an approximate 10 homework assignments. There will also be two midterm exams, one final project and a final exam. Final exam will be held on Tuesday May 13th, 11:00 AM – 1:00 PM.

The grading distribution for the course assignments and exams is as follows:

- Homework Assignments: 20%
- Midterm 1 (tentatively on Feb 12th): 20%
- Midterm 2 (tentatively on Apr 3rd): 20%
- Final Project: 20%
- Final Exam (May 13th): 20%

Course Grading Policies:
Homework is due at the time that it is specified in the homework handout (all homework handouts will be posted on the class website). Late homework will not be accepted, and will receive 0 points.

Make-up exams: A make-up exam may only be given under extraordinary circumstances. The student requesting a make-up exam should contact the instructor well in advance and provide written documentation for the reason that he/she will not be able to attend the regularly scheduled exam. It is up to the discretion of the Instructor to accept the justification provided by the student.

SALT Center:
Students eligible to use the services of the Strategic Technology Center, or with alternative educational needs, may see the Instructor at any time to discuss proper accommodations. Make sure that such a request is set forth at least 2 weeks before the first exam to allow sufficient time for any preparations that may be needed.

Plagiarism Policy:
The University’s Code of Academic Integrity (Section 2.1a) is based on the guiding principle that a student’s submitted work must be the student’s own. In ECE 596, this policy will be applied to all work submitted for a grade, including exams, quizzes, homework, and projects. Copying previously posted solutions or solution manuals is strictly forbidden; anyone violating this policy will receive zero credit for homework for the entire semester. All work must be original. The minimum penalty for submitting work that is not your own is an E grade. Repeated violations may result in expulsion from the university.