COMP434/ECOE534
Computer and Network Security
Spring 2011 Syllabus

Instructor
Öznur Özkasap, Associate Professor of Computer Engineering
Office: Eng144, Phone: x1584, oozkasap@ku.edu.tr
Office hour: Tue, Thu 15:30-16:30 (or by appointment)

Teaching Assistant
Damla Kılıçarslan
Office: Eng147, dkilicarslan@ku.edu.tr

Course web page
http://home.ku.edu.tr/~oozkasap/comp434

Course material
(Storage server) F:\COURSES\UGRADS\COMP434

Description

Prerequisite
Good knowledge of C or Java programming

Textbook

Reference books

Outline
Overview
Symmetric Ciphers:
- Classical Encryption Techniques
- Block Ciphers and DES (Data Encryption Standard)
- Basics of Finite Fields
- AES (Advanced Encryption Standard)
- Contemporary Symmetric Ciphers
- Confidentiality Using Symmetric Encryption
Public-Key Encryption and Hash Functions:
- Basics of Number Theory
- Public-Key Cryptography and RSA
- Key Management
- Message Authentication and Hash Functions
- Hash Algorithms
- Digital Signatures and Authentication Protocols

Network Security Practice:
- Authentication Applications
- Electronic Mail Security
- IP Security
- Web Security

System Security:
- Intruders
- Malicious Software
- Firewalls

**Assignments, project and exams**

There will be programming and written assignments related to concepts covered in class. Course project consists of investigating a given research topic in computer and network security area and building a prototype implementation. Students are required to prepare a term paper and presentation/demonstration of their projects. In addition, there will be two midterm exams.

**Grading**

<table>
<thead>
<tr>
<th>Component</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assignments</td>
<td>15%</td>
</tr>
<tr>
<td>Project</td>
<td>30%</td>
</tr>
<tr>
<td>Midterm I</td>
<td>20%</td>
</tr>
<tr>
<td>Midterm II</td>
<td>30%</td>
</tr>
<tr>
<td>Class participation</td>
<td>5%</td>
</tr>
</tbody>
</table>

These weights are subject to minor adjustments.

**Attendance**

The students are required to attend classes **on time**. Attendance may be taken, and late comers will not be allowed.

**Exam schedule**

- Midterm-1: March 29, Tuesday
- Midterm-2: May 24, Tuesday

**Academic Honesty**

The students taking this course are expected to submit their own work in all assignments, project and exams. Academic dishonesty includes using other people's words or ideas without acknowledgement, cheating on exams, projects, and assignments. In case any of the academic dishonesties are disclosed, disciplinary action and/or reduction of the final letter grade will follow.