Course Code | COMP586 | Course Title | Cryptography and Data Security
---|---|---|---
Academic Year | 2014-2015 | Academic Term | Spring | Course Credit | (3,0,0)3
Instructor(s) | Rza Bashirov, Prof. Dr. | e-mail and URL | rza.bashirov@emu.edu.tr | Office | 1250
| | | http://brahms.emu.edu.tr/rza/ |
Assistant(s) | |

Course Objectives

It is the purpose of this course to provide a survey of both the principles and practical techniques of cryptography and network security. The basic issues to be addressed by a network security capability are explored by providing a tutorial and survey of cryptography and network security technology. The course is self-contained. A background material will be provided as needed.

Weekly Schedule

1. Classical conventional encryption techniques: substitution techniques, Caesar’s cipher, monoalphabetic ciphers.
5. Block cipher design principles: number of rounds, F function, S-box design. International Data Encryption Algorithm (IDEA).
7. Term exam.
9. A few concepts from number theory: prime numbers, greatest common divisors, relatively prime numbers, Euler’s totient function, Euler’s theorem, review of primality test algorithms, AKS algorithm.
10. The RSA algorithm.
12. Presentation of homeworks.
13. Presentation of homeworks.

Textbook(s)/Required Reading

<table>
<thead>
<tr>
<th>Grading Criteria</th>
<th>Midterm exam</th>
<th>35%</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Homework</td>
<td>20%</td>
</tr>
<tr>
<td></td>
<td>Final exam</td>
<td>45%</td>
</tr>
</tbody>
</table>

**Academic Honesty**

Individual accountability for all individual work, written or oral. Copying from others or providing answers or information, written or oral, to others is cheating. Providing proper acknowledgment of original author. Copying from another student’s paper or from another text without written acknowledgement is plagiarism. According to University’s bylaws **cheating and plagiarism** are serious offences resulting in a failure from exam or project and disciplinary action (which includes an official warning may appear in student’s transcript or/and suspension from University for up to one semester).

**Additional Remarks**

1. Students are strongly encouraged to attend exams on exam date. One general make-up exam will be given at the end of the semester. Any student, who provides reasonable excuse for not attending the exam within three days following the exam date, will be allowed to sit for make-up exam.
2. Homeworks are essential part of the course. Each student is invited to select a homework subject among those published on the web page. Homeworks will be presented close to the end of semester (most probably during the last two weeks of the classes). Any student needs to submit a short report on the homework.