|  |
| --- |
| **CMSE 491 Selected Topics in Software Engineering I**  |
| **Department:**   Computer Engineering   |
| **Instructor Information****Name:** Assoc. Prof. Dr. Alexander Chefranov**E-mail:** Alexander.chefranov@emu.edu.tr**Office:** CMPE 219**Office Tel:** 0 392 630 1190                                   |
| **Assistant Information****Name:  TBD****E-mail:** **Office:** **Office Tel:**                 |
| **Meeting times and places**Tuesday, 10.30-12.20, CMPE036, LectureThursday, 10.30-14.20, CMPE036, LectureFriday, 08.30-10.20, CMPE134, Lab |
| **Program Name:**  FORMTEXT Computer Engineering  | **Program** **Code:** 25 |
| **Course Code** CMSE 491 | **Credits** 4  | **Year/Semester**2019-2020 Fall |
|  FORMCHECKBOX   Required Course          FORMCHECKBOX   Elective Course |
|  **Prerequisite(s):**  |
| **Catalog Description**  This course is to be arranged as seminar course. Students and faculty members participate in studying recent articles published on the research interests of the department. (4'th year standing). (Prerequisite: none) **Aims & Objectives**Teaching the basic concepts of software engineering with specific emphasis on the practical issues involved in software project management through the use of a one-semester design project.The students will work in teams on projects of interest to industry and will be involved in analysis of requirements, architecture and design, implementation, testing & validation, project management, software process, software maintenance, and software re-engineering.  |
|  **Course Web Page** http://cmpe.emu.edu.tr/en/CourseLoad.aspx?id=CMSE492 |
| **Textbook(s)**   |
| **Indicative Basic Reading List:**  |
| **Topics Covered and Tentative Class Schedule****(4 hours of lectures per week)**

|  |  |  |
| --- | --- | --- |
| **Week  1** | Cryptography security methods and attacks on them |   |
| **Week  2** | NTRU-like methods |   |
| **Week  3** | NTRU-like methods | . |
| **Week  4** | Lattices, LLL method |   |
| **Week  5** | Use of LLL for NTRU attacking |   |
| **Week  6** | RSA method |   |
| **Week  7**  | Use of LLL for RSA attacking |   |
| **Weeks  8, 9**  | MIDTERMS |   |
| **Week 10** | Steganography methods and attacks on them |   |
| **Week 11** | Steganography methods |   |
| **Week 12** | Steganography methods |   |
| **Week 13** | Steganalysis methods |   |
| **Week 14** | Steganalysis methods |   |
| **Weeks 15-17** | FINAL EXAMS |   |

  |
|   |   |   |   |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Lab Schedule (Tentative)**

|  |  |
| --- | --- |
| **Weeks 3-4** | Implementation of NTRU for integers |
| **Weeks 5-6**  | Implementation of NTRU for polynomials |
| **Weeks 6-7** | LLL attack on NTRU for integers |
| **Weeks 10-11** | LLL attack on NTRU for polynomials |
| **Weeks 12-13** | RSA |

  |
| **Course Learning Outcomes** Upon successful completion of the course, students are expected to have the following competencies:1. To know NTRU-like methods
2. To know lattices and LLL method
3. Be able to apply LLL to attack NTRU-like methods
4. Know RSA method
5. Be able to apply LLL for RSA attacking
6. To know spatial steganography and watermarking methods
7. To know transformation domain steganography and watermarking methods
8. To know secret sharing methods
9. To know steganalysis methods
10. Work on the Term project in a team
11. Participate in the seminars on the course topics
 |
| **Assessment** | **Method** | **No** | **Percentage** |
| Midterm Exam(s) | 1 | 20% |
| Final Examination | 1 | 30% |
|  | Seminar work | 6-7 | 20% |
|  | Attendance | - | 0% |
|  | Labs | 5 | 10% |
|  | Term project | 1 | 20% |
|  **Attendance grade:**No grade will be given. However, it is compulsory |
| **Policy on makeups:** For eligibility to take a makeup exam, the student should bring a doctor's report within 3 working days of the missed exam. |
| **Policy on the NG grade:** If more than 20% of classes missed and/or poor performance is shown in assignments (including exams), NG grade may be given.  |
| **Policy on missed seminars and labs:** There will be no makeup for missed seminars and labs.  |
|  **Relationship of the course to Student Outcomes**The course has been designed to contribute to the following student outcomes:1.  an ability to identify, formulate, and solve complex engineering problems by applying principles of engineering, science, and mathematics2. an ability to apply engineering design to produce solutions that meet specified needs with consideration of public health, safety, and welfare, as well as global, cultural, social, environmental, and economic factors3. an ability to communicate effectively with a range of audiences5. an ability to function effectively on a team whose members together provide leadership, create a collaborative and inclusive environment, establish goals, plan tasks, and meet objectives |
| **Prepared by:** Assoc.Prof. Dr. Alexander Chefranov | **Date Prepared:** 23 September 2019 |
|   |   |   |   |   |