**EASTERN MEDITERRANEAN UNIVERSITY  
CMPE 553 Fall 2022 COURSE OUTLINE**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **COURSE CODE** | CMPE 553 | **COURSE LEVEL** | | Graduate | |
| **COURSE TITLE** | Cryptography and Network Security | | | | |
| **COURSE TYPE** |  | | | | |
| **LECTURER(S)** | Prof. Alexander Chefranov | | | | |
| **ASSISTANTS** |  | | | | |
| **CREDIT VALUE** | 3 | | **ECTS VALUE** | |  |
| **PREREQUISITES** |  | | | | |
| **COREQUISITES** | None | | | | |
| **DURATION OF COURSE** | 1 Semester | | | | |
| **CLASSES TIME** | Tuesday, 10.30-12.20, CMPE126 Lecture; Wednesday, 12.30-13.20, CMPE127; All the classes are face to face | | | | |
| **WEB LINK** | https://staff.emu.edu.tr/alexanderchefranov/en/teaching/cmpe553 | | | | |
| **CATALOGUE DESCRIPTION**This the course on Cryptography and Network Security, objectives are: Classical encryption techniques, Block ciphers and the Data Encryption Standard, Basics of finite fields, Advanced Encryption Standard, Contemporary symmetric ciphers, Confidentiality using symmetric encryption, Basics of number theory, Key management, Public key cryptosystems, Message authentication, Hash functions and algorithms, Digital signatures and authentication protocols, Network security practice, Applications, E-Mail, IP and web security, System security, Intruders, Malicious software, Firewalls | | | | | |
| **AIMS & OBJECTIVES**The aim of the course is to introduce the student to the fundamentals of cryptography and network security. | | | | | |
| **GENERAL LEARNING OUTCOMES (COMPETENCES)**On successful completion of this course, all students will have developed knowledge and understanding of:  Classical encryption techniques, Block ciphers and the Data Encryption Standard, Basics of finite fields, Advanced Encryption Standard, Contemporary symmetric ciphers, Confidentiality using symmetric encryption, Basics of number theory, Key management, Public key cryptosystems, Message authentication, Hash functions and algorithms, Digital signatures and authentication protocols, Network security practice, Applications, E-Mail, IP and web security, System security, Intruders, Malicious software, Firewalls    On successful completion of this course, all students will have developed their skills in: the programming of symmetric and/or asymmetric ciphers and their use in the networks.  On successful completion of this course, all students will have developed their appreciation of and respect for values and attitudes regarding the issues of: Cryptography; Block and stream ciphers; Symmetric and asymmetric ciphers; Network security;  Cooperation and teamwork ; Unsupervised learning | | | | | |
| **GRADING CRITERIA**Will be decided according to student performance. | | | | | |
|  |  |  |  |  |  |

|  |
| --- |
| **RELATIONSHIP WITH OTHER COURSES**The course is based on the majority of the undergraduate courses related to algorithms, programming, computer organization, and networking |
| **LEARNING / TEACHING METHOD**Mainly through lectures, using Power-point slides and the whiteboard, and  term project for getting experience. |
| **ASSIGNMENTS**There will be a term project. |
| **METHOD OF ASSESSMENT**•**30% Midterm**•**45% Final**•2**0% Assignment**•**5% Quizzes** |
| **ATTENDANCE** NG grade may be given in the case of poor attendance (unexcused missing of more than 20% of the class hours) and/or a failure to complete assigned work (including exams).. |
| **TEXTBOOK**W. Stallings, Cryptography and Network Security, Principles and Practices, 3rd Ed., Prentice Hall, 2003, ISBN 0-13-111502-2 |
| **INDICATIVE BASIC READING LIST**None |
| **EXTENDED READING LIST**None |
| **SEMESTER OFFERRED**2022-23 Fall Semester |

**CONTENT & SCHEDULE**

* Classical encryption techniques,
* Block ciphers and the Data Encryption Standard,
* Basics of finite fields,
* Advanced Encryption Standard,
* Contemporary symmetric ciphers,
* Confidentiality using symmetric encryption,
* Basics of number theory,
* Key management,
* Public key cryptosystems,
* Message authentication,
* Hash functions and algorithms,
* Digital signatures and authentication protocols,
* Network security practice,
* Applications, E-Mail, IP and web security, System security, Intruders, Malicious software, Firewalls

**PLAGIARISM AND OTHER FORMS OF CHEATING**

Plagiarism is intentionally failing to give credit to sources used in writing regardless of whether they are published or unpublished. Plagiarism (which also includes any kind of cheating in exams) is a disciplinary offence and will be dealt with accordingly. Copying will also be dealt with similarly.

**DEPARTMENTAL POLICY ON TAKING MAKEUP EXAMS**

You can take a make-up for a mid-term  exam *only if*you have valid excuses (e.g., you are sick) and provide material evidence for it (e.g., a doctor’s report which must be issued/approved by EMU Health Center) within 3 working days of the exam.

**ANY OTHER USEFUL INFORMATION**

Please check course web site **http://cmpe.emu.edu.tr/courses/cmpe553**for slides, lecture notes, study materials, and announcements regarding labs, assignments and grades.

Last modified 02/10/2022