COURSE: Cyber Security				
CODE: CENG440	**SEMESTER:** FALL OR SPRING			
LANGUAGE: ENGLISH	**TYPE:** ELECTIVE			
PRE-REQUISITES: CENG101 , CENG301, CENG304 **CO-REQUISITES:**	**THEORY**	**PRACTICAL**	**CREDIT**	**ECTS**
WEEKLY HOURS:	3	0	3	5

CONTENT OF THE COURSE:
In this course, students will be introduced to real-world cybersecurity challenges that organisations face, and learn to apply knowledge and skills gained through other Computer Science courses to address them. This course provides also basic definitions of cyber security, overview of cyber threats. Cryptology, Symmetric/asymmetric cryptography, PKI, CA trust model, SSL/TLS (HTTPS, SFTP etc.). In order to build a solid background about authentication and secure protocols some topics will be covered in this course such as: Message authentication, digital signature, digital certificates, authentication and Hash Functions. The course also will also introduce cyber security management concepts, including security operations, risk management, security engineering. Other topics such as: cyber threat prevention mechanisms, network forensics, and web application security will be covered in this course.

OBJECTIVE OF THE COURSE:
To enable the students to apply the knowledge and skills to analyze cybersecurity and digital forensics problems and design appropriate solution to solve relevant engineering problems

WEEKLY SCHEDULE	
Week	**Topics**
1	Basic definitions of cyber security, overview of cyber threats
2	Symmetric cryptography
3	Asymmetric cryptography
4	Network attacks, security of basic network services, cyber threat prevention mechanisms
5	Network forensics
6	Hash functions
7	Penetration testing methodologies and tools
8	**Mid Examination Week**
9	Message authentication code and digital signature
10	Secure transport and application layers protocols Wireless security
11	E-mail security
12	Attacks and Malicious software
13	Risk management and security policy
14	Project presentations and discussion

TEXTBOOK:
Cybersecurity Leadership: Powering the Modern Organization 3rd Edition (2014)

by Mansur Hasib
REFERENCE BOOKS:
Andreasson, Kim J., ed. *Cybersecurity: public sector threats and responses*. CRC press, 2011.
Stallings, W. (2006). *Cryptography & Network Security: Principles and Practices* (4th ed.). New Jersey: Pearson.
Stallings, W. (2007). *Network Security Essentials* (3rd ed.).New Jersey: Pearson.

EVALUATION SYSTEM:		
IN-TERM STUDIES	**QUANTITY**	**PERCENTAGE (%)**
Midterm Exam	1	30%
Homework	2	20%
Laboratory works		
Quiz	2	10%
Final Exam	1	40%
TOTAL	**6**	**100%**
CONTRIBUTION OF INTERM STUDIES TO OVERALL GRADE	5	60%
CONTRIBUTION OF FINAL EXAMINATION TO OVERALL GRADE	1	40%
TOTAL	6	100%

COURSE CATEGORY:	PERCENTAGE (%)
Mathematics and Basic Sciences	30%
Engineering	50%
Engineering Design	10%
Social Sciences	10%

TABLE OF ECTS / WORKLOAD:			
Activities	**QUANTITY**	**Duration (Hour)**	**Total Workload**
Course Duration	13	3	39
Hours for off-the-classroom study (Pre-study, practice)	14	6	84
Laboratory works			
Mid-term	1	2	2
Final examination	1	2	2
Homework	2	3	6
Quiz	2	1	2
Total Work Load			**135**
Total Work Load / 30			**4,5**
ECTS Credit of the Course			**5**

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**
LO1	1	1	2	2	1	0	0	1	2	1	2
LO2	2	3	2	3	2	1	0	1	1	1	2
LO3	3	3	2	2	2	1	0	1	1	1	1

LO4	2	2	2	3	2	1	0	1	2	1	2
LO5	3	3	2	2	2	1	0	1	1	1	1
	PO: Program Outcomes | LO: Learning Outcomes Values: 0: None | 1: Low | 2: Medium | 3: High										

INSTRUCTOR(S):	Asst. Prof. Dr. Mohammed Madi
FORM PREPARATION DATE:	22.05.2019

LEARNING OUTCOMES OF THE COURSE:	**PROGRAM OUTCOMES:**
LEARNING OUTCOMES OF THE COURSE: **LO1: Get introduced to IT security forensics and ethics** **LO2: Describe the role of an information security in an organisation, and main components of information security management frameworks.** **LO3: Evaluate the different techniques and protocols used in wireless security.** **LO4: Demonstrate basic skills in computer forensic analysis.** **LO5: Explain wide range of security mechanisms**	**PO1:** Adequate knowledge in mathematics, science and engineering subjects pertaining to the relevant discipline; ability to use theoretical and applied knowledge in these areas in complex engineering problems. **PO2:** Ability to identify, formulate, and solve complex engineering problems; ability to select and apply proper analysis and modeling methods for this purpose. **PO3:** Ability to design a complex system, process, device or product under realistic constraints and conditions, in such a way as to meet the desired result; ability to apply modern design methods for this purpose. **PO4:** Ability to devise, select, and use modern techniques and tools needed for analyzing and solving complex problems encountered in engineering practice; ability to employ information technologies effectively. **PO5:** Ability to design and conduct experiments, gather data, analyze and interpret results for investigating complex engineering problems or discipline specific research questions. **PO6:** Ability to work efficiently in intra-disciplinary and multi-disciplinary teams; ability to work individually. **PO7:** Ability to communicate effectively in Turkish, both orally and in writing; knowledge of a minimum of one foreign language; ability to write effective reports and comprehend written reports, prepare design and production reports, make effective presentations, and give and receive clear and intelligible instructions. **PO8:** Recognition of the need for lifelong learning; ability to access information, to follow developments in science and technology, and to continue to educate him/herself. **PO9:** Consciousness to behave according to ethical principles and professional and ethical responsibility; knowledge on standards used in engineering practice. **PO10:** Knowledge about business life practices such as project management, risk management, and change management; awareness in entrepreneurship, innovation; knowledge about sustainable development. **PO11:** Knowledge about the global and social effects

	of engineering practices on health, environment, and safety, and contemporary issues of the century reflected into the field of engineering; awareness of the legal consequences of engineering solutions.