

<b>Course title</b>	<b>Code</b>	<b>semester</b>	<b>T+U</b>	<b>credit</b>	<b>ECTS</b>
	YM506	6	3+0	3	4
<b>Prerequisite Courses</b>	None				
<b>Language of the Course</b>	English				
<b>Course Level</b>	Undergraduate				
<b>Type of Course</b>	Optional				
<b>Course Coordinator</b>					
<b>Instructors</b>					
<b>Course Assistants</b>					
<b>The aim of lesson</b>	To enable students to apply their knowledge and skills to analyze cyber security and forensic problems and to design appropriate solutions to solve related engineering problems.				
<b>Course Content</b>	It will introduce the real-world cybersecurity challenges organizations face and use the knowledge and skills gained through other Computer Science courses to address them. Basic definitions of cyber security, an overview of cyber threats. Cryptology, Symmetric / asymmetric encryption, PKI, CA trust model, SSL / TLS (HTTPS, SFTP, etc.). Building a solid background on authentication and secure protocols. Message authentication, digital signature, digital certificates, authentication and Hash Functions.				
<b>Course Learning Outcomes</b>	<p>Students who successfully complete this course;</p> <ol style="list-style-type: none"> <li>1. Basic definitions of cyber security, an overview of cyber threats</li> <li>2. They will learn network attacks, security of basic network services, and cyber threat prevention mechanisms.</li> <li>3. Will be able to build a solid background on authentication and secure protocols.</li> </ol>				
<b>Weeks</b>	<b>Topics</b>				
one	Introduction to Web Security				
2	Basic definitions of cybersecurity, an overview of cyber threats				
3	Symmetric encryption				
4	Asymmetric encryption				
5	Network attacks, security of essential network services, cyber threat prevention mechanisms				
6	network computing				
7	Penetration testing methodologies and tools				
8	Penetration testing methodologies and tools				
9	Message verification code and digital signature				
10	Secure transport and application layers protocols Wireless security				
11th	Email security				
12	Attacks and Malware				
13	Risk management and security policy				
14	Project presentations and discussion				
15	Project presentations and discussion				
<b>General Competencies</b>					
They will have the necessary knowledge for cyber threat prevention mechanisms, network forensics and web application security.					
<b>resources</b>					
Mansur Hasib “ Powering the Modern Organization 3rd Edition”, Cybersecurity Leadership , 2014					
Andreasson , Kim J., ed ., " Cybersecurity ", public sector threats and responses . CRC press , 2011.					
<b>Evaluation System</b>					

The dates, days and hours of the Midterm, Quiz, Final Exam and Evaluations will be announced later, according to the decision of the Faculty Administrative Board.

<b>WITH PROGRAM LEARNING OUTCOMES COURSE LEARNING OUTCOMES RELATIONSHIP TABLE</b>											
	<b>PO1</b>	<b>PO2</b>	<b>PO3</b>	<b>PO4</b>	<b>PO5</b>	<b>PO6</b>	<b>PO7</b>	<b>PO8</b>	<b>PO9</b>	<b>PO10</b>	<b>PO11</b>
<b>LO1</b>	4	5	5	5	4	4	4	5	5	4	4
<b>LO2</b>	3	4	4	4	5	3	3	3	5	4	3
<b>LO3</b>	5	5	5	5	5	3	5	4	4	3	3
<b>LO: Learning Outcomes OP: Program Outcomes</b>											
<b>Contribution Level</b>	<b>1 Very Low</b>		<b>2 Low</b>		<b>3 Medium</b>		<b>4 High</b>		<b>5 Very High</b>		

**Relation of Program Outcomes and Related Course**

	<b>PO1</b>	<b>PO2</b>	<b>PO3</b>	<b>PO4</b>	<b>PO5</b>	<b>PO6</b>	<b>PO7</b>	<b>PO8</b>	<b>PO9</b>	<b>PO10</b>	<b>PO11</b>
<b>Introduction to Software Engineering</b>	4	5	5	4	5	3	4	4	5	4	3