Subject	**Security of Data and Social Networks**			
	Type	**Semester**	**ECTS**	**Code**
	MANDATORY (M)	3	6	50-ISS-804
Course Lecturer				
Aims and Objectives	This course provides an in-depth exploration of the principles, technologies, and strategies employed in securing data and social networks. Students will gain a comprehensive understanding of the challenges associated with safeguarding information in the digital age, with a focus on both technical and social aspects. Topics include cryptography, network security, social engineering, privacy concerns, and emerging threats. Practical exercises and case studies will be used to reinforce theoretical concepts, ensuring students develop the skills necessary to analyze, design, and implement effective security measures.			
Learning Outcomes	In the end of the course students will be able to: • Understand the Fundamentals of Information Security: • Understand the role of encryption in securing data. • Analyze the design and implementation of secure networks. • Explore social engineering techniques used in cyber attacks. • Design and implement privacy-enhancing measures. • Understand the fundamentals of risk assessment and management.			
Course Content	**Course Plan**			**Week**
	Introduction to Data Security			1
	Cryptography Essentials			2
	Network Security Fundamentals			3
	Social Engineering Attacks			4
	Privacy Concerns in Data and Social Networks			5
	Application Security			6
	Incident Response and Handling			7
	Risk Assessment and Management			8
	Emerging Threats in Cybersecurity			9
	Legal and Ethical Aspects of Cybersecurity			10
	Security Awareness and Training Programs			11
	Privacy by Design			12
	Privacy-Enhancing Technologies			13
	Blockchain Security			14
	Wrap-up			15
Teaching/Learning Methods	**Teaching/Learning Activity**			**Weight (%)**
	1. Lectures			20%
	2. Seminars			20%
	3. Laboratory			20%

	4. Case studies			40%
	5. Role play			-
	6. Problem-based learning			-
	7. Study visits			-
	8. Work placement			-
Assessment Methods	**Assessment Activity**	**Number**	**Week**	**Weight (%)**
	1. Quiz	1	7	15%
	2. Group Project	1	12	35%
	3. Midterm Exam	1	8	20%
	4. Final Exam	1	13	30%
Course resources	**Resources**			**Number**
	1. Class			1
	2. Laboratory			1
	3. Moodle			1
	4. Projector			1
ECTS Workload	**Activity**		**Weekly**	**Total**
	1. Lectures		2	24
	2. Seminars		2	24
	3. Laboratory		2	24
	4. Practice in Industry		1	5
	5. Self-learning		8.25	99
	6. Exams		2	4
Literature/References	- Principles of Computer Security", Authors: Wm. Arthur Conklin, Greg White, Dwayne Williams, Chuck Cothren, and Roger L. Davis, 2019 - "Privacy Engineering: A Dataflow and Ontological Approach", Rauf Beydeda and Natalya Keberle, 2019 - "Social Engineering: The Art of Human Hacking", Christopher Hadnagy, 2018 - "The Art of Deception: Controlling the Human Element of Security", Kevin D. Mitnick and William L. Simon, 2002 -			
Contact				