Specification for the book of courses

Study program	Electrical Engineering and Computer Science		
Module	Computing and Informatics		
Type and level of studies	Undergraduate Academic Studies		
The name of the course	Information Security		
Lecturer (for lectures)	Vučković V. Vladan		
Lecturer/associate (for exercises)	Rajković J. Petar		
Lecturer/associate (for OFE)	Rajković J. Petar		
Number of ECTS	5	**Course status (obligatory/elective)**	Elective
Prerequisites			
Course objectives	Mastering the basic knowledge necessary to use basic and advanced procedures in information security.		
Course outcomes	Theoretical knowledge: mastering mathematical techniques for encoding and decoding data; Programming the information security methods (cryptography) on modern computers.		
Course outline			
Theoretical teaching	Elements of cryptology, cryptography and cryptanalysis. Authorized access. Identification methods. Developing an Authorized Approach System. Symmetric cryptography. Public and secret key. Hash functions. Method of attack on the protected system. Certificates, maintenance and issuance of certificates. Basic security protocols. Types of malware programs.		
Practical teaching (exercises, OFE, study and research	Preparation of seminar papers. Historical overview of the area and implementation of the simplest coding algorithms. General analysis of encoders, data flows and implementation of algorithms A5, A5 / 1 and RC-4. Feistel coder. Implementation of data block encoders DES, TDES, AES, TEA. Encoder modes. Asymmetric coding, implementation of RSA and Knapsack algorithms. Calculating the CRC values. Tiger-hash. Analysis and implementation of MD and SHA families of cryptographic hes-functions. Methods for cryptanalysis.		
Textbooks/references			
1	Mark Stamp, “Information Security Principles and Practice“, John Wiley and Sons, Inc, New Jersey, U.S.A., 2006.		
2	Vladan Vučković, Petar Rajković "Information Security" basic textbook, Faculty of Electronic Engineering Niš, 2016, first edition. 195 pages, ISBN 978-86-6125-166-5, COBISS.SR-ID 226243852.		
3	Vladan Vučković, Petar Rajković "Information Security", Edition: Auxiliary textbook, Faculty of Electronic Engineering, Niš, 2010. ISBN 978-86-6125-010-1		
4			
5			

Number of classes of active education per week during semester/trimester/year				
Lectures	**Exercises**	**OFE**	**Study and research work**	**Other classes**
2	2	1	0	0
Teaching methods	Lectures, exercises on the board, laboratory exercises, students' independent work on homework assignments and projects, consultations.			

Grade (maximum number of points 100)			
Pre-exam duties	**Points**	**Final exam**	**Points**
Activity during lectures		**Written exam**	
Exercises	20	**Oral exam**	40
Colloquia	30		
Projects	10		