Specification for the book of courses

Study program			Computing and Informatics	
Module			Computer Systems Security	
Type and level of studies			Master studies	
The name of the course			Cryptography	
Lecturer (for lectures)			Rančić D. Dejan, Vučković V. Vladan	
Lecturer/associate (for exercises)			Dimitrijević M. Aleksandar	
Lecturer/associate (for OFE)				
Number of ECTS	4	**Course status (obligatory/elective)**		Elective
Prerequisites				
Course	Introduction to the field of cryptography in terms of basic principles, algorithms and standards.			
Course outcomes	Students will gain knowledge on basic principles, algorithms, and standards used in the field of cryptography. They will also learn how to apply that knowlegde in real-world applications.			
Course outline				
Theoretical teaching	History and overview of cryptography. Mathematical background. Basic symmetric-key encryption. Stream ciphers. Block ciphers. DES – The Data Encryption Standard. AES – The Advanced Encryption Standard. Asymmetric cryptography using public-private key pair. Hash Functions and Data Integrity. Digital signature schemes. RSA signatures. The "Hash-and-Sign" Paradigm. Certificates and Public-Key Infrastructures. Secure Socket Layer (SSL) and Transport Layer Security (TLS) standards.			
Practical teaching (exercises, OFE, study and research	Practical work on the programming cryptographic elements using OpenSSL library.			
Textbooks/references				
1	J. Katz, Y. Lindell, Introduction to Modern Cryptography, CRC Press, 2007.			
2	A. Menezes, P. van Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.			
3				
4				
5				

Number of classes of active education per week during semester/trimester/year				
Lectures	**Exercises**	**OFE**	**Study and research work**	**Other classes**
2	1	0		

Teaching methods	Lectures, exercises, individual student work on projects.

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