1.	Course	**Applied Cryptography**				
2.	Code	**INF-S20**				
3.	Study programme	Informatics				
4.	Study programme organized by	Faculty of Computer Science and Engineering				
5.	Cycle	Third - PhD				
6.	Academic year / semester winter/summer/elective	Second winter/summer/elective	7.	ECTS credits	7,5	
8.	Teacher	Prof. Smile Markovski, Assoc. prof. Vesna Dimitrova				
9.	Prerequisites	None				
10.	Course programme goals (competences): The student should be able to make their own design for the studied cryptographic packets.					
11.	Course syllabus: Advanced algorithms for generation huge prime numbers and relatively prime numbers; Practical realization of some algorithms for symmetric cryptography, Implementation of RSA and ElGamal public crypto systems; Realization and application of protocols for key distribution; Cryptanalysis of simple crypto systems.					
12.	Teaching methods: Classes supported with slide presentations, interactive teaching, lab equipment and other software packages, teamwork, case studies, invited guest lecturers, presentations of project works, e-learning materials, forums and consultations					
13.	Total fund of work hours	7,5 EKTC x 30 h = 225 h				
14.	Available hours distribution	45+30+150 = 225				
15.	Teaching activities	15.1.	Theoretical classes	45 h		
		15.2.	Practical classes (labs, exercises), seminars, team work	30 h		
16.	Other activities	16.1.	Project tasks	50 h		
		16.2.	Self study	50 h		
		16.3.	Homework	50 h		
17.	Grading					
	17.1.	Tests	40 points			
	17.2.	Seminar work/ project (presentation: written and oral)	50 points			
	17.3.	Active participation	10 points			
18.	Grading criteria (points/grade)	to 59 points	5 (five) (F)			
		from 60 to 68 points	6 (six) (E)			
		from 69 to 76 points	7 (seven) (D)			
		from 77 to 84 points	8 (eight) (C)			
		from 85 to 92 points	9 (nine) (B)			
		from 93 to 100 points	10 (ten) (A)			
19.	Conditions for attending the final exam	Successful completion of activities 15.1 and 15.2				
20.	Language	Macedonian or English				

21.	Quality assessment	Internal evaluation and student pools

22.	Literature					
	22.1.	Compulsory				
		No.	Author	Title	Publisher	Year
		1.	B. Schneier	Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition	John Wiley & Sons	1996
		2.	W. Stallings	Cryptography and Network Security	Prentice Hall	2005
		3.	N. Ferguson, B. Schneier	Practical Cryptography	Wiley Publishing, Inc.	2003
	22.2.	Additional				
		No.	Author	Title	Publisher	Year
		1.	T. Baigneres, P. Junod at al.	A classiacal introduction to cryptography exercise book	Springer	2006
		2.	C. Kaufman, R. Perlman, M. Speciner	Network Security: Private Communication in a Public World (2nd Edition)	Prentice Hall PTR	2002
		3.	C. Paar, J. Pelzl	Understanding Cryptography: A Textbook for Students and Practitioners	Springer	2010