1.	Course	**Advanced Cryptanalysis**			
2.	Code	**INF-S12**			
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	Assoc. prof. Vesna Dimitrova, Prof. Smile Markovski			
9.	Prerequisites	None			
10.	Course programme goals (competences): Learning the advanced tools for cryptanalysis				
11.	Course syllabus: Detailed analysis of attacks with brute force and statistical attacks, survey of new methods for differential and linear cryptanalysis, representations of crypto systems as Boolean functions and research cryptographic properties, analysis of special types of attacks on specific crypto products (hash functions, block ciphers, with public keys, protocols). Practical survey of software and hardware implementation of the attacks. Practical implementation of some attacks.				
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.	M. Stamp, Richard M. Low	Applied Cryptanalysis: Breaking Ciphers in the Real World	Wiley	2007
		2.	A Joux	Algorithmic Cryptanalysis	Chapmann and Hall CRC	2009
		3.	G. V. Bard	Algebraic Cryptanalysis	Springer	2009
	22.2.	Additional				
		No.	Author	Title	Publisher	Year
		1.	N. Smart	Introduction to cryptography	McGraw-Hill	2003
		2.	S. Vaudenay	A classical introduction to cryptography – Applications for comunications security	Springer	2006
		3.	Christopher Swenson	Modern Cryptanalysis: Techniques for Advanced Code Breaking	Wiley Publishing, Inc.	2008