1.	Course title	**Cryptanalysis**		
2.	Course code	KK-I-01		
3.	Study program	**Coding and Cryptography**		
4.	Unit offering the course	**FCSE**		
5.	Undergraduate/master/PhD	**Master**		
6.	Year/semester 1(2)/summer/elective	7. ECTS: **6**		
8.	Teacher(s)	Assis. Prof. Vesna Dimitrova, Prof. Smile Markovski		
9.	Course prerequisites	None		
10.	Goals (competences): Learning the basic tools for cryptanalysis			
11.	Course content: Types of attacks with brute force, statistical attack, differential and linear cryptanalysis, representations of crypto systems as Boolean functions and research the properties of linearity, special types of attacks on specific crypto products (hash functions, block ciphers, with public keys, protocols)			
12.	Teaching methods: Lectures supported by slide presentations, interactive lectures, trainings (using lab equipment and software packages), team work, case studies, invited guests and lectures, individual practical assignments presentations, seminar paper, e-learning (forums, consultations).			
13.	Total available time	6 ECTS x 30 hours = 180 hours		
14.	Distribution of the available time	45 + 45 + 30 + 30 + 30 = 180 hours		
15.	Teaching activities	15.1.	Lectures	45 hours
		15.2.	Training (labs, problem solving), seminar and team work	45 hours
16.	Other activities	16.1.	Project work	30 hours
		16.2.	Self study	30 hours
		16.3.	Home work	30 hours
17.	Grading			
	17.1.	Tests		50 points
	17.2.	Seminar work/project (written or oral presentation)		30 points
	17.3.	Active participation		20 points
18.	Grading criteria	to 50 points		5 (five) (F)
		from 50 to 59 points		6 (six) (E)
		from 60 to 69 points		7 (seven) (D)
		from 70 to 79 points		8 (eight) (C)
		from 80 to 89 points		9 (nine) (B)
		from 90 to 100 points		10 (ten) (A)

19.	Final exam prerequisites			Successfully completed activities 15.1 and 15.2		
20.	Course language			Macedonian and English		
21.	Quality assurance methods			Internal evaluation and student questionnaires		
22.	Literature					
	22.1.	Compulsory				
		No.	Authors	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
	22.2.	Additional				
		No.	Authors	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