1.	Наслов на наставниот предмет	**Криптоанализа**		
2.	Код	КК-И-01		
3.	Студиска програма	Едногодишни магистерски студии по Кодирање и криптографија		
4.	Организатор на студиската програма (единица, односно институт, катедра, оддел)	Факултет за информатички науки и компјутерско инженерство – ФИНКИ		
5.	Степен (прв, втор, трет циклус)	Студии од вториот циклус		
6.	Академска година / семестар 10	7. Број на ЕКТС кредити 6		
8.	Наставник	Доц. д-р Весна Димитрова, Проф. д-р Смиле Марковски		
9.	Предуслови за запишување на предметот	Нема		
10.	Цели на предметната програма (компетенции): Изучување на основните алатки за криптоанализа			
11.	Содржина на предметната програма: Видови на напади со груба сила, статистички напади, диференцијална и линеарна криптоанализа, претставувања на крипто системи како булови функции и испитувања на својствата за линеарност, специјални видови напади за посебни крипто продукти (хаш функции, блок шифрувачи, со јавни клучеви, протоколи)			
12.	Методи на учење: предавања, проекти, дискусии, работилници			
13.	Вкупен расположив фонд на време	6 ЕКТС по 30 = 180 часови		
14.	Распределба на расположивото време	45+45+30+30+30		
15.	Форми на наставните активности	15.1.	Предавања- теоретска настава	45 часови
		15.2.	Вежби (лабораториски, аудиториски), семинари, тимска работа	45 Часови
16.	Други форми на активности	16.1.	Проектни задачи	30 Часови
		16.2.	Самостојни задачи	30 Часови
		16.3.	Домашно учење	30 Часови
17.	Начин на оценување			
	17.1.	Тестови		50 Бодови
	17.2.	Семинарска работа/ проект (презентација: писмена и усна)		30 Бодови
	17.3.	Активност и учество		20 Бодови
18.	Критериуми за оценување (бодови/ оценка)	до 50 бода		5 (пет) (F)
		од 50 до 59		6 (шест) (E)

		бода	
		од 60 до 69 бода	7 (седум) (D)
		од 70 до 79 бода	8 (осум) (C)
		од 80 до 89 бода	9 (девет) (B)
		од 90 до 100 бода	10 (десет) (A)
19.	Услов за потпис и полагање на завршен испит	Реализирани активности 15, 16	
20.	Јазик на кој се изведува наставата	Македонски и англиски	
21.	Метод на следење на квалитетот на наставата	Механизам на интерна евалуација и анкети	

22. Литература

22.1. Задолжителна литература

Ред. Број	Автор	Наслов	Издавач	Година
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. Дополнителна литература

Ред. број	Автор	Наслов	Издавач	Година
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