1.	Наслов на наставниот предмет	Напредна криптографија			
2.	Код	КК-З-01			
3.	Студиска програма	Магистерски студии по Кодирање и криптографија			
4.	Организатор на студиската програма (единица, односно институт, катедра, оддел)	ФИНКИ			
5.	Степен (прв, втор, трет циклус)	Втор циклус			
6.	Академска година / семестар	9	7.	Број на ЕКТС кредити	6
8.	Наставник	Проф. д-р Смиле Марковски, доц.д-р Весна Димитрова			
9.	Предуслови за запишување на предметот	Нема			
10.	Цели на предметната програма (компетенции): Оспособеност на студентите конкретно да ги реализираат посебните видови криптографски пакети				
11.	Содржина на предметната програма: Алгоритми за генерирање на огромни прости броеви и заемно прости броеви; реализација на алгоритми за симетрични крипто системи; реализација на РСА и Ел Гамал системи со јавни клучеви; реализација на протоколи за размена на клучеви; разбивање на попрости крипто системи				
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 бода	6 (шест) (E)		
		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	Реализирани активности 15, 16			

	завршен испит	
20.	Јазик на кој се изведува наставата	Македонски
21.	Метод на следење на квалитетот на наставата	

22.	Литература					
	22.1.	Задолжителна литература				
		Ред. број	Автор	Наслов	Издавач	Година
		1.	T. Baigneres, P. Junod at al.	A classiacal introduction to cryptography exercise book	Springer	2006
		2.	W. Stallings	Cryptography and Network Security	Prentice Hall	2005
		3.	N. Ferguson, B. Schneier	Practical Cryptography	Wiley Publishing, Inc	2003
	22.2.	Дополнителна литература				
		Ред. број	Автор	Наслов	Издавач	Година
		1.	B. Schneier	Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition	John Wiley & Sons	1996
		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