Прилог бр.3	Предметна програма од прв, втор и трет циклус на студии

1.	Наслов на наставниот предмет	**Криптографија**				
2.	Код	2FI206312				
3.	Студиска програма	Математика				
4.	Организатор на студиската програма (единица, односно институт, катедра, оддел)	Факултет за информатика				
5.	Степен (прв, втор, трет циклус)	Втор степен				
6.	Академска година / семестар	2012-2013/ први	7.	Број на ЕКТС кредити	4	
8.	Наставник	Доц. д-р Александра Милева				
9.	Предуслови за запишување на предметот	нема				
10.	**Цели на предметната програма (компетенции):** Цел на овој курс е студентите да се стекнат со напредни знаења од криптографијата и криптографските примитиви и протоколи, како и основни знаења од криптоанализата.					
11.	**Содржина на предметната програма:** Класична криптографија; Перфектна тајност, шифра на Вернам, проточни шифри, Trivium, Edon-80, генератори на случајни броеви; Блок шифри, DES, AES, модови на операција, псевдо-случајни пермутации и функции, напади; Линеарна и диференцијална криптанализа; Интегритет на пораки, кодови за автентикација на пораки (MAC); Хеш функции, MD5, SHA1, SHA-2, SHA3 кандидати, напади; Криптографија со јавни клучеви: математички основи, Diffie-Hellman размена на клучеви, ElGammal и Cramer–Shoup криптосистеми, RSA, Rabin, Goldwasser-Micali криптосистеми; Тестови и генератори за прости броеви, алгоритми за факторизација и пресметување на дискретни логаритми; Дигитални потписи, инфраструктура за јавни клучеви (PKI); Протоколи за воспоставување на клучеви; Криптографски протоколи					
12.	Методи на учење: Предавања, книги, статии, нумерички вежби, електронско учење, семинарска работа, консултации.					
13.	Вкупен расположив фонд на време	120 часови				
14.	Распределба на расположивото време	2+1+1				
15.	Форми на наставните активности	15.1.	Предавања- теоретска настава	2 часа		
		15.2.	Вежби (лабораториски, аудиториски), семинари, теренска и тимска работа	1 час		
16.	Други форми на активности	16.1.	Проектни задачи	1 час		
		16.2.	Самостојни задачи			
		16.3.	Домашно учење			
17.	Начин на оценување					
	17.1.	Проектна задача		30 поени		
	17.2.	Семинарска работа (презентација: писмена и усна)		50 поени		

	17.3.	Активност и учество	20 поени
18.	Критериуми за оценување (бодови/ оценка)	до 50 бода	5 (пет) (F)
		од 51 до 60 бода	6 (шест) (E)
		од 61 до 70 бода	7 (седум) (D)
		од 71 до 80 бода	8 (осум) (C)
		од 81 до 90 бода	9 (девет) (B)
		од 91 до 100 бода	10 (десет) (A)
19.	Услов за потпис и полагање на завршен испит	Освени 60% од бодовите од предиспитни активности	
20.	Јазик на кој се изведува наставата	Македонски	
21.	Метод на следење на квалитетот на наставата	Самоевалуација	

22.	Литература					
	22.1.	Задолжителна литература				
		Ред. број	Автор	Наслов	Издавач	Година
		1.	J. Katz, Y. Lindell	Introduction to Modern Cryptography	Chapman & Hall/CRC Press	2007
		2.	S. Vaudenay	A Classical Introduction to Cryptography: Applications for Communications Security	Springer Science+ Business Media, Inc.	2006
		3.	D. R. Stinson	Cryptography: theory and practice, 3rd edition	Chapman & Hall/CRC	2005
	22.2.	Дополнителна литература				
		Ред. број	Автор	Наслов	Издавач	Година
		1.	N. Smart	Cryptography: An Introduction, 3rd Edition	McGraw Hill	2004
		2.	A. J. Menezes, P. Van Oorschot, S. A. Vanstone	Handbook of Applied Cryptography	CRC Press	1997
		3.		Листа на трудови		