Прилог бр. 3		**Предметна програма од прв циклус на студии**			
1.	Наслов на наставниот предмет	**Криптографија**			
2.	Код	МФИМ13			
3.	Студиска програма	Математика-физика			
4.	Организатор на студиската програма (единица, односно - институт, катедра, оддел)	Природно-математички факултет, Скопје Институт за математика, Институт за физика			
5.	Степен (прв, втор, трет циклус)	Прв циклус			
6.	Академска година /семестар	Трета или четврта година, / шести или осми семестар	7.	Број на ЕКТС-кредити	6
8.	Наставник	Д-р Весна Целакоска-Јорданова, редовен професор			
9.	Предуслови за запишување на предметот	Алгебарски структури			
10.	Цели на предметната програма (компетенции): Стекнување основни познавања за принципите на шифрирање и дешифрирање пораки кај познати крипто-системи.				
11.	Содржина на предметната програма: Некои едноставни криптосистеми и нивна криптоанализа. Симетрични шифрирачи: Feistel Cipher, DES, 3-DES, Rijndael, Stream Ciphers. Модуларна аритметика, Кинеска теорема на остатоци, Енкрипција со јавен клуч, RSA криптосистем.				
12.	Методи на учење: активно следење на предавањата и вежбите, усвојување на материјалот со домашно учење и самостојно решавање задачи.				
13.	Вкупен расположив фонд на време	180 часа			
14.	Распределба на расположивото време	седмично: 2 часа предавања, 2 часа лабораториски вежби			
15.	Форми на наставните активности	15.1.	Предавања - теоретска настава	30 часа	
		15.2.	Вежби (лабораториски, аудиториумски), семинари, тимска работа	30 часа	
16.	Други форми на активности	16.1.	Проектни задачи	30 часа	
		16.2.	Самостојни задачи	30 часа	
		16.3.	Домашно учење – задачи	60 часа	
17.	Начин на оценување				
	17.1.	Тестови	2 колоквиуми / се положува со max. 200 поени, а min 100 поени од двата, при што секој од колоквиумите мора да е положен со min. 50		

			поени. Сите овие учествуваат со 70% во крајната оценка.	
	17.2.	Индивидуална работа/проект (презентација: писмена и усна)	Се освојуваат 15 поени од проектна задача на одредена тема и 10 поени од изработени домашни задачи.	
	17.3.	Активност и учество	Активното учество на часот се вреднува со 5 поени.	
18.	Критериуми за оценување (бодови/ оценка)		до 50 бода	5 (пет) (F)
			51 х до 60 бода	6 (шест) (E)
			61 х 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 за полагање завршен испит		Услов за потпис: присуство на часовите за предавања и вежби. Услов за завршен испит: Минимум 50% од поените освоени на тестовите.	
20.	Јазик на кој се изведува наставата		Македонски и делумно на англиски	
21.	Метод на следење на квалитетот на наставата		Домашни задачи, квизови и/или тестови	

22. Литература

22.1.	Задолжителна литература				
	Реден број	Автор	Наслов	Издавач	Година
	1.	N. Smart	Cryptography, An Introduction	McGraw-Hill	2003
	2.	D. R. Stinson	Cryptography, Theory and Practice	CRC Press	1995
	3.				
22.2.	Дополнителна литература				
	Реден број	Автор	Наслов	Издавач	Година
	1.	Gilbert Baumslag, Benjamin Fine, Martin Kreuzer, Gerhard Rosenberger	A Course in Mathematical Cryptography	De Gryuter	2015
	2.				
	3.				