1	Наслов на наставниот предмет	Криптографија и безбедност на компјутерски системи			
2	Код				
3	Студиска програма	Математика-информатика			
4	Организатор на студиската програма	Институт за математика			
5	Степен	Прв циклус академски студии			
6	Академска година/семестар	изборен	7	Број на ЕКТС кредити	6
8	Наставник	д-р Весна Целакоска-Јорданова, доцент д-р Валентина Миовска, доцент д-р Дончо Димовски, редовен професор			
9	Предуслови за запишување на предметот	Алгебраски структури, Основи на веројатност			
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. Теорија на Shanon. Симетрични шифрирачи: Feistel Cipher, DES, 3-DES, Rijndael, Stream Ciphers. Енкрипција со јавен клуч, RSA криптосистем и напади на RSA криптосистемот, El-Ghamal криптосистем, Rabin криптосистем.				
12	Метод на учење: активно следење на предавањата и вежбите, усвојување на материјалот со домашно учење и самостојни задачи				
13	Вкупен расположлив фонд на време	60 часа			
14	Распределба на расположливото време	седмично: 2 часа предавања, 2 часа лабораториски вежби			
15	Форми на наставните активности	15.1	Предавања-теоретска настава	30 часа	
		15.2	Вежби (аудиториски)	30 часа	
16	Други форми на активности	16.1	Проектни задачи	10 часа	
		16.2	Самостојни задачи	15 часа	
		16.3	Домашно учење	75 часа	
17	Начини на оценување				
	17.1	Тестови		40 бода	
	17.2	Семинарска работа/проект (презентација: писмена и усна)		10 бода	
	17.3	Активност и учество		5 бода	
	17.4	Завршен испит		45 бода	
18	Критериуми за оценување (бодови/оценка)	до 49 бода		5 (пет) (F)	
		Од 50 бода до 60 бода		6 (шест) (E)	
		од 61 -70 бода до бода		7 (седум) (D)	
		од 71 бода до 80 бода		8 (осум) (C)	
		од 81 бода до 90 бода		9 (девет) (B)	
		од 91 бода до 100 бода		10 (десет) (A)	
19	Услов за потпис и полагање на завршен испит	Услов за потпис: присуство на часовите за предавања и вежби Услов за завршен испит: 50% од поените освоени на колквиумите и изработена проектна задача			
20	Јазик на кој се изведува наставата	Македонски (и англиски по потреба)			
21	Метод на следење на квалитетот на наставата	Тестови, проектни задачи			
22	Литература				

22.1	Задолжителна литература				
	ред. бр.	Автор	Наслов	Издавач	Година
	1	N. Smart	Cryptography, An Introduction	McGraw-Hill	2003
	2	D. R. Stinson	Cryptography, Theory and Practice	CRC Press	1995

	22.2	Дополнителна литература				
		ред. бр.	Автор	Наслов	Издавач	Година
		1	S. Crivei, A. Mărcuş, C. Săcărea, C. Szánto	Computational algebra with applications to coding theory and cryptography	Editura Fundației pentru Studii	2006