

1	Наслов на наставниот предмет		Криптографија			
2	Код		МФ6Х2			
3	Студиска програма		Математика-физика			
4	Организатор на студиската програма		Институт за математика			
5	Степен		Прв циклус академски студии			
6	Академска година/семестар		III / 6 (изборен)	7	Број на ЕКТС кредити	6
8	Наставник		Д-р Весна Целаоска-Јорданова, вонреден професор			
9	Предуслови за запишување на предметот		Алгебарски структури			
10	Цели на предметната програма (компетенции): Стекнување основни познавања за принципите на ашифрирање и дешифрирање пораки кај познати крипто-системи.					
11	Содржина на предметната програма: Некои едноставни крипто системи и нивна криптоанализа. Симетрични шифрирачи: Feistel Cipher, DES,3-DES, Rijndael, Stream Ciphers. Енкрипција со јавен клуч, RSA крипто систем и напади на RSA крипто системот.					
12	Метод на учење: активно следење на предавањата и вежбите, усвојување на материјалот со домашно учење и самостојно решавање задачи.					
13	Вкупен расположлив фонд на време		120 часа			
14	Распределба на расположливото време		седмично: 2 часа предавања, 2 часа лабораториски вежби			
15	Форми на наставните активности	15.1	Предавања-теоретсканастава	30 часа		
		15.2	Вежби(аудиториски)	30 часа		
16	Други форми на активности	16.1	Проектнизадачи	20 часа		
		16.2	Самостојнизадачи	20 часа		
		16.3	Домашно учење	20 часа		
17	Начини на оценување					
	17.1	Тестови		40бода		
	17.2	Семинарскаработа/проект(презентација:писменаиусна)		10бода		
	17.3	Активностиучество		5бода		
	17.4	Завршениспит		45бода		
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 71бода до 80 бода		8(осум)(C)	
			Од 81бода до 90 бода		9(девет)(B)	
			Од 91бода 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			
20	Јазик на кој се изведува наставата		Македонски (или англиски по потреба)			
21	Метод на следење на квалитетот на наставата		Тестови,проектни задачи			
	Литература					
	Задолжителналитература					

22	22.1	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. Mărcuș, C. Săcărea, C. Szánto	Computational algebra with applications to coding theory and cryptography	Editura Fundației pentru Studii	2006			