1	Наслов на наставниот предмет		**КРИПТОГРАФИЈА**			
2	Код		M8-XTK1			
3	Студиска програма		Математика			
4	Организатор на студиската програма		Институт за математика			
5	Степен		Прв циклус академски студии			
6	Академска година/семестар		IV / 8 семестар	**7**	Број на ЕКТС кредити	4
8	Наставник		Д-р Весна Целакоска-Јорданова, вонреден професор			
9	Предуслови за запишување на предметот		Алгебарски структури, Веројатност и статистика			
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..					
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-теоретска настава		30 часа	
		15.2	Вежби (аудиториски)		30 часа	
16	Други форми на активности	16.1	Проектни задачи		20 часа	
		16.2	Самостојни задачи		20 часа	
		16.3	Домашно учење		20 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 (или англиски по потреба)			
21	Метод на следење на квалитетот на наставата		Тестови, проектни задачи			

<table>
<tr><td rowspan="8">22</td><td colspan="6">Литература</td></tr>
<tr><td rowspan="3">22.1</td><td colspan="5">Задолжителна литература</td></tr>
<tr><td>ред. бр.</td><td>Автор</td><td>Наслов</td><td>Издавач</td><td>Година</td></tr>
<tr><td>1</td><td>N. Smart</td><td>Cryptography, An Introduction</td><td>McGraw-Hill</td><td>2003</td></tr>
<tr><td></td><td>2</td><td>D. R. Stinson</td><td>Cryptography, Theory and Practice</td><td>CRC Press</td><td>1995</td></tr>
<tr><td rowspan="3">22.2</td><td colspan="5">Дополнителна литература</td></tr>
<tr><td>ред. бр.</td><td>Автор</td><td>Наслов</td><td>Издавач</td><td>Година</td></tr>
<tr><td>1</td><td>S. Crivei, A. Mărcuş, C. Săcărea, C. Szánto</td><td>Computational algebra with applications to coding theory and cryptography</td><td>Editura Fundaţiei pentru Studii</td><td>2006</td></tr>
</table>