

1.	Наслов на наставниот предмет	Криптографија Cryptography			
2.	Код	CSEW516			
3.	Студиска програма	КНИ, МТ, АСИ			
4.	Организатор на студиската програма (единица, односно институт, катедра, оддел)	Факултет за информатички науки и компјутерско инженерство – ФИНКИ			
5.	Степен (прв, втор, трет циклус)	Студии од првиот циклус			
6.	Академска година / семестар	3/летен/изборен	7.	Број на ЕКТС кредити	6
8.	Наставници	Акад. проф. д-р Љупчо Коцарев, Доц. д-р Весна Димитрова			
9.	Предуслови за запишување на предметот	Дискретна математика 2			
10.	Цели на предметната програма:	Запознавање со основните криптографски принципи и методи; изучување на основните крипто-дизајни; практично користење на изучените криптографски алгоритми.			
11.	Содржина на предметната програма:	Класичната анаспротимодерната криптографија. Совршено-тајно шифрирање. Компјутерска безбедност. Шифрирање со симетричен клуч. Автентикација на пораки и хаш функции. Блок шифри. Теоретски конструкти. Теорија на бројеви. Револуцијата со јавните клучеви. Размена на клучеви. Шифрирање со јавни клучеви. Дигитални потписи. Ефикасни криптографски шеми. Елементи од теоријата на бројевите; криптографски протоколи; криптографски алгоритми, генератори на псевдо-случајни бројеви, проточни шифрувачи, алгоритми со јавен клуч; примени. Современи протоколи за безбедно комуницирање: <i>SSL, DES, 3-DES, RSA, Twofish, ...</i>			
12.	Методи на учење:	Предавања, вежби, самостојна работа, проектни задачи, семинарски работи			
13.	Вкупен расположив фонд на време	6 ЕКТС x 30 часа = 180 часа			
14.	Распределба на расположивото време	30+45+25+40+40 = 180 часа			
15.	Форми на наставните активности	15.1.	Предавања-теоретска настава	30 часови	
		15.2.	Вежби (лабораториски, аудиториски), семинари, тимска работа	45 часови	
16.	Други форми на активности	16.1.	Проектни задачи	25 часови	
		16.2.	Самостојни задачи	40 часови	
		16.3.	Домашно учење	40 часови	
17.	Начин на оценување				
	17.1.	Тестови/ колоквиуми	80 бодови		

	17.2.	Семинарска работа/ проект (презентација: писмена и усна)			10 бодови
	17.3.	Активност и учество			10 бодови
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			реализирани 15 и 16	
20.	Јазик на кој се изведува наставата			македонски или англиски	
21.	Метод на следење на квалитетот на наставата			интерна евалуација и анкети	
22.	Литература				
	22.1.	Задолжителна литература			
Ред. Број		Автор	Наслов	Издавач	Година
1.		C. Paar, J. Pelzl	Understanding Cryptography: A Textbook for Students and Practitioners	Springer	2010
2.		N. Smart	Cryptography: An introduction	McGraw-Hill	2003
3.		J. Katz, Y. Lindell	Introduction to Modern Cryptography	Chapman & Hall/CRC Press	2007
22.2.	Дополнителна литература				
	Ред. Број	Автор	Наслов	Издавач	Година
	1.	Mark Stamp	Information security – principles and practice	John Willey and Sons	1991

