

1.	Наслов на наставниот предмет	Криптографско инженерство	
2.	Код	БК-И-05	
3.	Студиска програма	Безбедност, криптографија и кодирање	
4.	Организатор на студиската програма (единица, односно институт, катедра, оддел)	Факултет за информатички науки и компјутерско инженерство	
5.	Степен (прв, втор, трет циклус)	втор циклус	
6.	Академска година / семестар 5 / зимски / изборен	7. Број на ЕКТС кредити	6
8.	Наставник	доц. д-р Симона Самарџиска, доц. д-р Христина Михајлоска, проф. д-р. Панче Рибарски	
9.	Предуслови за запишување на предметот		
10.	Цели на предметната програма (компетенции): По завршување на курсот се очекува студентот да знае да програмира сигурна крипто-примитива. Ќе поседува знаење од имплементација на крипто-примитиви на различни платформи. Преку примери ќе осознае како работи side-channel криптоанализата на различни криптографски имплементации и кои противмерки треба да се преземат.		
11.	Содржина на предметната програма: 1. Запознавање со техники за брза и сигурна имплементација на криптографски софтвер 2. Имплементација на модуларна аритметика и аритметика на конечни полиња 3. Имплементациски аспекти за симетрични криптопримитиви (AES, SHA) 4. Имплементациски аспекти за криптографски примитиви со јавен клуч (RSA, ECC) 5. Имплементациски аспекти за лесна криптографија 6. Сигурна имплементација на криптографски примитиви 7. Side-channel напади и противмерки 8. Криптографски софтверски пакети		
12.	Методи на учење: Предавања поддржани со презентации преку слајдови, интерактивни предавања, вежби (користење на опрема и софтверски пакети), самостојна изработка и одбрана на проектна задача и семинарска работа, учење во електронско опкружување (форуми, консултации).		
13.	Вкупен расположив фонд на време	6 ECTS x 30 часа = 180 часа	
14.	Распределба на расположивото време	60 + 45 + 45 + 30 = 180 часа	
15.	Форми на наставните активности	15.1. Предавања-теоретска настава	60 часови
		15.2. Вежби (лабораториски, аудиториски), семинари, тимска работа	45 часови
16.	Други форми на активности	16.1. Проектни задачи	45 часови
		16.2. Самостојни задачи	45 часови
		16.3. Домашно учење	30 часови
17.	Начин на оценување		
	17.1. Тестови	0 бодови	
	17.2. Семинарска работа/ проект (презентација: писмена и усна)	70 бодови	

	17.3.	Активности и учење				30 бодови
	17.4.	Завршен испит				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		Домашна работа			
20.	Јазик на кој се изведува наставата		Македонски и англиски			
21.	Метод на следење на квалитетот на наставата		Механизам на интерна евалуација и анкети			
22.	Литература					
	22.1.	Задолжителна литература				
		Ред.бр.	Автор	Наслов	Издавач	Година
		1	Batina, Schwabe	Cryptographic engineering Lecture notes		0
	22.2.	Дополнителна литература				
Ред. број		Автор	Наслов	Издавач	Година	