1.	Наслов на наставниот предмет	Напредни теми од криптографија Advanced Topics in Cryptography		
2.	Код	F18L3S139		
3.	Студиска програма	Компјутерски науки, Интернет, мрежи и безбедност		
4.	Организатор на студиската програма (единица, односно институт, катедра, оддел)	Факултет за информатички науки и компјутерско инженерство		
5.	Степен (прв, втор, трет циклус)	прв циклус		
6.	Академска година / семестар 4 / летен /	7. Број на ЕКТС кредити 6		
8.	Наставник	доц. д-р Христина Михајлоска, доц. д-р Симона Самарџиска		
9.	Предуслови за запишување на предметот	Криптографија		
10.	Цели на предметната програма (компетенции): Градење на сигурна крипто-примитива која ќе биде отпорна не само на теориски напади, туку и на практични (side-channel) напади.			
11.	Содржина на предметната програма: Типови на криптографски напади; Вовед во диференцијална криптоанализа; Вовед во линеарна криптоанализа; Side-channel напади; Реални напади над крипто примитиви; Програмирање сигурен крипто-софтвер			
12.	Методи на учење: Предавања, вежби, самостојна работа, проектни задачи, семинарски работи			
13.	Вкупен расположив фонд на време	6ЕКТС x 30 часа = 180 часа		
14.	Распределба на расположливото време	30 + 45 + 15 + 15 + 75 = 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	15 часови
		16.2.	Самостојни задачи	15 часови
		16.3.	Домашно учење	75 часови
17.	Начин на оценување			

	17.1.	Тестови	10 бодови
	17.2.	Семинарска работа/ проект (презентација: писмена и усна)	10 бодови
	17.3.	Активности и учење	10 бодови
	17.4.	Завршен испит	70 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 активности	
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	Dan Boneh, Victor Shoup	A Graduate Course in Applied Cryptography	Stanford University	2015
2	Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone	Handbook of Applied Cryptography	CRC Press	1997

22.2. Дополнителна литература

Ред. број	Автор	Наслов	Издавач	Година