1.	Наслов на наставниот предмет	Докажлива безбедност			
2.	Код	БК-И-03			
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 / летен / изборен**	7. Број на ЕКТС кредити **6**			
8.	Наставник	доц. д-р Симона Самарџиска, доц. д-р Христина Михајлоска			
9.	Предуслови за запишување на предметот				
10.	Цели на предметната програма (компетенции): Со комплетирање на содржината на предметот студентот ќе се стекне со знаење за основните принципи и стандардните сигурносни модели на докажливата сигурност. Исто така ќе ги изучи основните редукциски техники во докажувањето како и доволните и неопходни претпоставки за доказите.На крајот на курсот студентот ќе може да дизајнира стратегија за сигурносен доказ од почеток. Да напише целосен основен сигурносен доказ. Секако, ќе биде во можност да извлече заклучок од влијанието на доказот врз сигурноста на примитивата.				
11.	Содржина на предметната програма: 1. Вовед во докажлива сигурност2. Метод на докажување сигурност 3. Непријателски модели4. Сигурносни претпоставки и редукции5. Game-based сигурност6. Псевдо/случајни функции и пермутации. Еднонасочни функции7. Техники на докажување во симетрична криптографија8. Техники на докажување во криптографија со јавен клуч				
12.	Методи на учење: Предавања, проекти, дискусии, работилници				
13.	Вкупен расположив фонд на време	6 ЕКТС по 30 = 180 часови			
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	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)	30 бодови		
	17.3.	Активности и учење	20 бодови		
	17.4.	Завршен испит	50 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 за интерна евалуација и анкети	

22. Литература

22.1. Задолжителна литература

Ред.бр.	Автор	Наслов	Издавач	Година
1	Oded Goldreich	The Foundations of Cryptography - Volume 1	Cambridge University Press	2001

22.2. Дополнителна литература

Ред. број	Автор	Наслов	Издавач	Година