	УНИВЕРЗИТЕТ У ИСТОЧНОМ САРАЈЕВУ Филозофски факултет Пале	
	Студијски програм: Математика и рачунарство - Смјер информатика	
	II циклус студија / I година студија	

Пун назив предмета	КРИПТОГРАФИЈА
Катедра	Катедра за рачунарске науке и системе – Филозофски факултет Пале

Шифра предмета	**Статус предмета**	**Семестар**	**ECTS**
М-МР-И4	изборни	I(II)	5

Наставник/ -ци	др Дарко Дракулић, доцент
Сарадник/ - ци	

Фонд часова/ наставно оптерећење (седмично)			**Индивидуално оптерећење студента (у сатима семестрално)**			**Коефицијент студентског оптерећења S_o**
П	**АВ**	**ЛВ**	**П**	**АВ**	**ЛВ**	**S_o**
2	2	0	48(45)	48(45)	0	1,6(1,5)

укупно наставно оптерећење (у сатима, семестрално) 60 h	укупно студентско оптерећење (у сатима, семестрално) 96(90) h

Укупно оптерећење предмета (наставно + студентско):
156(150) h семестрално

Исходи учења	1. Упознавање са концептима криптографије и примјене у заштити комуникације и датотека. 2. Овладавање математичким апаратом неопходним за развој криптографксих алгоритама. 3. Разумијевање принципа конструкције и рада најпознатијих криптографских алгоритама. 4. Упознавање са основама квантне криптографије.
Условљеност	Положен испит Алгоритми и структуре података.
Наставне методе	Теоријска предавања, аудиторне вјежбе, израда пројеката.
Садржај предмета по седмицама	1. Математичке основе криптографије (дјељивост, прости бројеви, конгруенције). 2. Математичке основе криптографије (Ојлер, Ферма и Вилсон; примитивни корјени; индекс калкулус). 3. Комплексност алгоритама. 4. Основи криптографије. Напади 5. DES и AES. 6. Криптографија јавног кључа. Основне идеје. 7. RSA. 8. Алгоритми за испитивање да ли је број прост. 9. Факторизација. 10. *Hash* функције. SHA-1. 11. Примјена критпографије у сигурности комуникација. PGP. 12. Ниво протокола и SSL. 13. *Firewall* и клијент сервер модели. 14. Сигурност датотека. 15. Квантна криптографија.

Обавезна литература

Аутор/ и	**Назив публикације, издавач**	**Година**	**Странице (од-до)**
Mollin R. A.	An Introduction to Cryptography, 2nd edition, Chapman and Hill/CRC	2007	

Допунска литература

Аутор/ и	**Назив публикације, издавач**	**Година**	**Странице (од-до)**
Schneier B.	Applied Cryptography. Protocols, algorithms and source code in C, J. Wiley	1996	

Обавезе, облици провјере знања и оцјењивање	**Врста евалуације рада студента**	**Бодови**	**Проценат**
	Предиспитне обавезе		
	присуство предавањима/ вјежбама	10	10
	Пројекат	50	50
	Завршни испит		
	завршни испит (усмени/ писмени)	40	40
	УКУПНО	100	100 %
Web страница			

Датум овјере	