Спецификација предмета за књигу предмета

Студијски програм	Информатика		
Изборно подручје (модул)			
Врста и ниво студија	Докторске академске студије		
Назив предмета	Напредни системи заштите података		
Наставник (за предавања)			
Наставник/сарадник (за вежбе)			
Наставник/сарадник (за ДОН)			
Број ЕСПБ	11	**Статус предмета (обавезни/изборни)**	изборни
Услов	нема		
Циљ предмета	Сагледавање комплексности поступака криптоанализе и упознавање са основним математичким апаратом неопходним за њихово спровођење. Класификација напада на симетричне криптосистеме, оцена њихове успешности и сложености напада. Опис главних метода криптоанализе симетричних криптосистема. Примена разматраних метода на неколико најпознатијих блок шифара (block ciphers) и секвенцијалних шифара (stream ciphers).		
Исход предмета	Стицање општих теоријских знања из области криптоанализе укључујући и потребну математичку основу. Стицање теоријских знања о поступцима криптоанализе симетричних криптосистема и њиховој примени на блок шифре и секвенцијалне шифре. Овладавање различитим техникама криптоанализе на практичним примерима упрошћених варијанти		
Садржај предмета			
Теоријска настава	Класификација могућих напада на криптосистеме и њихова карактеризација. Математичка основа неопходна за разумевање криптоаналитиких поступака релевантних за овај курс. Упознавање са проблемима криптоанализе симетричних криптосистема и опис главних метода криптоанализе тих система: диференцијалне, линеарне, алгебарске и корелационе криптоанализе. Упознавање са значајним криптосистемима ове врсте MD5 и SHA-1, као и познатим нападима на њих укључујући диференцијалну криптоанализу. Приказ MAC криптосистема за аутентикацију и напада на њих. Упознавање са проблемима криптоанализе асиметричних криптосистема и опис главних метода криптоанализе тих система укључујући алгоритме за факторизацију целих бројева и полинома, као и алгоритме за израчунавање дискретних логаритама		
Литература			
1	Martin K., Everyday Cryptography Fundamental Principles and Applications, Oxford University Press, 2		
2	Aumasson J.F., Serious Cryptography: A Practical Introduction to Modern Encryption, No Starch Press, 2017.		
3	Schneier B., Applied Cryptography Protocols, Algorithms and Source Code in C, Hoboken, N.J.: John Wiley & Sons, 2017.		
4			

Број часова активне наставе недељно током семестра/триместра/године

Предавања	**Вежбе**	**ДОН**	**Студијски истраживачки рад**	**Остали часови**
3			2	

Методе извођења	предавања, вежбе, студије случаја, гостујући предавачи

Оцена знања (максимални број поена 100)

Предиспитне обавезе	**поена**	**Завршни испит**	**поена**
активност у току	10	**Усмени испит**	50
Истраживачки рад	40		
Укупно	50	Укупно	50