Спецификација предмета за књигу предмета

Студијски програм	Рачунарство и информатика		
Изборно подручје (модул)	Безбедност рачунарских система		
Врста и ниво студија	Мастер академске студије		
Назив предмета	Криптографија		
Наставник (за предавања)	Ранчић Д. Дејан, Вучковић В. Владан		
Наставник/сарадник (за вежбе)	Димитријевић М. Александар		
Наставник/сарадник (за ДОН)			
Број ЕСПБ	4	**Статус предмета (обавезни/изборни)**	Изборни
Услов			
Циљ предмета	Увођење студената у област криптографије и упознавање са основних принципима, алгоритмима и стандардима који се користе у овој области.		
Исход предмета	Теоријска и практична знања о основним принципима, алгоритимима и стандардима који се користе у области криптографије.		
Садржај предмета			
Теоријска настава	Увод у криптографију и историјски преглед области. Математичке основе. Енкрипција коришћењем симетричног кључа. Шифратори токова података. Шифратори блокова података. DES – The Data Encryption Standard. AES – The Advanced Encryption Standard. Енкрипција коришћењем пара јавни-тајни кључ. Хеш функције и интегритет података. Шеме дигиталног потписивања. RSA потписивање. Парадигма "хешуј и потпиши". Сертификати и инфраструктуре јавних кључева. Secure Socket Layer (SSL) и Transport Layer Security (TLS) стандарди.		
Практична настава (вежбе, ДОН, студијски истражива-чки рад)	Практичан рад на програмирању криптографских елемената коришћењем OpenSSL библиотеке.		
Литература			
1	J. Katz, Y. Lindell, Introduction to Modern Cryptography, CRC Press, 2007.		
2	A. Menezes, P. van Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.		
3			
4			
5			

Број часова активне наставе недељно током семестра/триместра/године				
Предавања	**Вежбе**	**ДОН**	**Студијски истраживачки рад**	**Остали часови**
2	1	0		
Методе извођења наставе	Предавања, аудитивне вежбе, самосталан рад студената на изради пројеката.			

Оцена знања (максимални број поена 100)			
Предиспитне обавезе	**поена**	**Завршни испит**	**поена**
активност у току предавања		**писмени испит**	30
практична настава		**усмени испит**	30
колоквијуми	20		
семинари	20		