Спецификација предмета за књигу предмета

Студијски програм	Информатика		
Изборно подручје (модул)			
Врста и ниво студија	Мастер академске студије		
Назив предмета	Савремени криптографски системи		
Наставник (за предавања)			
Наставник/сарадник (за вежбе)			
Наставник/сарадник (за ДОН)			
Број ЕСПБ	7	**Статус предмета (обавезни/изборни)**	изборни
Услов	Испуњене предисптне обавезе.		
Циљ предмета	Упознавање са основним принципима заштите безбедности информација, са основним техникама и алгоритмима који се користе у криптографској пракси.		
Исход предмета	На крају курса студент треба да буде упознат са основним циљевима и средствима криптографије, да овлада основним техникама којима се обезбеђују разни видови сигурности информација, научи на који начин се обавља комуникација у криптографском систему и схвати суштину функционисања најзначајнијих савремених криптографских система.		
Садржај предмета			
Теоријска настава	Историја криптографије, основни криптографски циљеви и средства, нивои безбедности, практични аспекти безбедности, Vernam-ове шифре (one-time pad), основни криптографски концепти, енкрипционе шеме, математичке основе криптографије, бијекције, пермутације, једносмерне и једносмерне trapdoor функције, цели бројеви, тестови простости, методе факторизације, блок шифре, супституцијске и транспозицијске шифре, композиција шифри, проточне шифре, криптосистеми са тајним (симетричним) кључем, DES, криптосистеми са јавним кључем, RSA криптосистем, ElGamal-ов криптосистем, криптоанализа, аутентификација, дистрибуција кључева, дигитални потписи, стеганографске методе.		
Практична настава (вежбе, ДОН, студијски истражива-чки рад)	Израда задатака везаних за примену метода шифровања и дешифровања података и савладавање основних принципа криптоанализе.		
Литература			

1	S. Adamović, Zaštita informacionih sistema – Java implementacija kriptografskih mehanizama, Fakultet za racunarstvo i informatiku, Beograd, 2015.
2	M. Milosavljević, S. Adamović, Kriptologija 2 - Osnove za analizu i sintezu šifarskih sistema, Univerzitet Singidunum, Beograd, 2014
3	M. Veinović, S. Adamović, Kriptologija 1 - Osnove za analizu i sintezu šifarskih sistema, Univerzitet Singidunum, Beograd, Danijelova 32., 2013
4	H. Delfs and H. Knebl, Introduction to Cryptography, Springer, 1998.

Број часова активне наставе недељно током семестра/триместра/године				
Предавања	**Вежбе**	**ДОН**	**Студијски истраживачки рад**	**Остали часови**
2	2			

Методе извођења наставе	На предавањима се користе класичне методе наставе уз коришћење пројектора и интеракцију са студентима. На вежбама студенти решавају типичне практичне проблеме шифровања и дешифровања информација коришћењем различитих криптографских система. Знање студената се тестира кроз домаће задатке и колоквијуме. На усменом делу испита студент треба да покаже да је овладао основним принципима функционисања криптографских система.

Оцена знања (максимални број поена 100)			
Предиспитне обавезе	**поена**	**Завршни испит**	**поена**
активност у току предавања	7	**писмени испит**	30
практична настава	8	**усмени испит**	20
колоквијуми	20		
семинари	15		