

Табела 5.2. Спецификација предмета

Студијски програм: МАС информатика				
Назив предмета: Криптографија				
Наставник: Сана Стојановић Ђурђевић				
Статус предмета: Изборни				
Број ЕСПБ: 8				
Услов: Нема предуслова				
Циљ предмета: Упознавање са основама криптографске заштите података.				
Исход предмета: По завршетку курса, студент има основна знања о криптографији и криптоанализи.				
Садржај предмета: - Преглед основа теорије бројева. - Коначна поља. - Савремене ланчане шифре (stream ciphers). - Блокковске шифре, AES; начини коришћења - Системи за шифровање са јавним кључем. - Елиптичке криве. - Хеш функције, кодови за аутентикацију, дигитални потпис. - Управљање кључевима. - Примери криптоанализе. - Алгоритми за факторизацију. - Алгоритми за решавање проблема дискретног логаритма.				
Литература: 1. Миодраг Живковић, Криптографија - Скрипта (http://www.poincare.matf.bg.ac.rs/~ezivkovm/nastava/kripto.pdf), заснива се на лекцијама Е. Shaefer-a (http://math.scu.edu/~eschaefer/crylec.pdf) 2. D. Stinson, Cryptography – Theory and Practice, CRC Press, 1996. (наставник може изабрати другу одговарајућу актуелну литературу)				
Бр. час. акт. наставе: 7	Теоријска настава: 2	Прак. настава: 3	Лаб.вежбе: -	СИР: 2
Методе извођења наставе: Фронтални, групни и практични.				
Оцена знања (максималан број поена је 100)				
Предиспитне обавезе	поена	Завршни испит	поена	
активност у току предавања	-	писмени испит	-	
практична настава	-	усмени испит	-	
колоквијум-и	30	писмено-усмени испит	70	
семинар-и	-			