

Студијски програм: Дипломске академске студије информатике			
Назив предмета: P312 - Криптографија			
Наставник: Миодраг Живковић и други наставници Катедре за рачунарство и информатику			
Статус предмета: Изборни			
Број ЕСПБ: 9			
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:			
<ul style="list-style-type: none"> - Преглед основа теорије бројева. - Коначна поља. - Савремене ланчане шифре (stream ciphers). - Блокоске 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), почива на лекцијама Е. Shaefer-a (http://math.scu.edu/~eschaefe/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	70
колоквијум-и	30	писмено-усмени испит	-
семинар-и	-		