

**Табела 5.2. Спецификација предмета**  
Спецификацију треба дати за сваки предмет из студијског програма.

<b>Студијски програм:</b> Мастер академске студије МАТЕМАТИКА			
<b>Назив предмета:</b> Криптографија			
<b>Наставник/наставници:</b> Сана Стојановић Ђурђевић, Ивана Томашевић			
<b>Статус предмета:</b> изборни			
<b>Број ЕСПБ:</b> 8			
<b>Услов:</b>			
<b>Циљ предмета:</b> Упознавање са основама криптографске заштите података.			
<b>Исход предмета:</b> По завршетку курса, студент има основна знања о криптографији и криптоанализи.			
<b>Садржај предмета</b>			
<i>Теоријска настава</i>			
- 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.			
<i>Практична настава</i>			
<b>Литература:</b>			
1. Миодраг Живковић, Криптографија - Скрипта ( <a href="http://www.poincare.matf.bg.ac.rs/~ezivkovm/nastava/kripto.pdf">http://www.poincare.matf.bg.ac.rs/~ezivkovm/nastava/kripto.pdf</a> ), заснива се на лекцијама Е. Shaefer-a ( <a href="http://math.scu.edu/~eschaefe/crylec.pdf">http://math.scu.edu/~eschaefe/crylec.pdf</a> )			
2. D. Stinson, Cryptography – Theory and Practice, CRC Press, 1996.			
Наставник може изабрати другу одговарајућу актуелну литературу.			
<b>Број часова активне наставе:</b> 7	<b>Теоријска настава:</b> 2	<b>Практична настава:</b> 3+2	
<b>Методе извођења наставе:</b> фронтални, групни и практични.			
<b>Оцена знања (максимални број поена 100)</b>			
<b>Предиспитне обавезе</b>	поена	<b>Завршни испит</b>	поена
активност у току предавања		писмени испит	
практична настава		усмени испит	
колоквијум-и	30	писмено-усмени испит	70
семинар-и		.....	
Начин провере знања могу бити различити наведено у табели су само неке опције: (писмени испити, усмени испит, презентација пројекта, семинари итд.....			
*максимална дужина 2 странице А4 формата			