Студијски програм: Докторске студије информатике

Назив предмета: P412 - Криптографија - напредни концепти

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:

- Преглед основа теорије бројева.
- Коначна поља.
- Савремене ланчане шифре (stream ciphers).
- Блоковске 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 E. 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: 10	**Теоријска настава: 4**	**Прак. настава: -**	**Лаб.вежбе: -**	**СИР: 6**

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	-		