Назив предмета: Напредни криптографски алати и алгоритми

Наставник или наставници: Владица Стојановић/Стефан Панић/Часлав Стефановић

Статус предмета: Изборни

Број ЕСПБ: 15

Услов: /

Циљ предмета

Циљ предмета је упознавање студената са савременим методама заштитног кодовања и криптографије. Биће изложена конструкција ефикасних заштитних кодова који се могу описати помоћу графова и методе њиховог итеративног декодовања. Биће анализирана осетљивост савремених криптографских алгоритама на криптоаналитички напад помоћу квантних рачунара и објашњена примена заштитних кодова у криптологији.

Исход предмета

Оспособљавање студената за конструкцију заштитних кодова, њихову имплементацију и тестирање перформанси на стандардним програмским језицима. Процена сигурности криптографских алгоритама.

Садржај предмета

Теоријска настава

Моделовање пробабилистичких система, процесирање информација на графовима. Турбо кодови и њихово декодовање (MAP, SOVA). Алгоритми декодовања LDPC кодова. Фонтански кодови (Tornado, LT, Raptor). Мрежни кодови. Теорија информација и вештачка интелигенција. Криптографија елиптичких кривих. Примена LDPC кодова у криптографији, Мек Елисов криптосистем. Утицај квантних рачунара на криптологију, елементи квантне теорије информација.

Практична настава

Семестрални радови.

Препоручена литература

1. T. Richardson, R. Urbanke, Modern Coding Theory, Cambridge University Press, 2008.
2. R. Bose, Information Theory, Coding and Cryptography, 2nd edition, McGraw-Hill Education, 2008.
3. M. Baldi, QC-LDPC Code-Based Cryptography, Springer, 2014.
4. S. Loepp, W. Wootters, Protecting Information: From Classical Error Correction to Quantum Cryptography, Cambridge University Press, 2006.

Број часова активне наставе	Предавања: 5	Студијски истраживачки рад: 5

Методе извођења наставе

Фронтални, групни, индивидуални и практични.

Оцена знања (максимални број поена 100)

Предиспитне обавезе	**Поена**	**Завршни испит**	**Поена**
Семинар-и	40	Усмени испит	60