Студијски програм: Основне академске студије математике

Назив предмета: Теорија бројева и криптографија

Статус предмета: изборни на модулу Рачунарство и примењена математика на основним академским студијама математике

Број ЕСПБ: **5**

Услов: уписан одговарајући семестар

Циљ предмета

Упознавање студената са основним појмовима из теорије бројева (основна теорема аритметике, неке важније аритметичке функције, прости и сложени бројеви, конгруенције, системи линеарних конгруенција) и криптографије (криптографски системи са тајним и јавним кључем, веза теорије бројева и криптографије, примена неких алгоритама из теорије бројева у шифрирању). Оспособљавање студената за решавање проблема и задатака из поменутих области уз употребу научних поступака и метода.

Исход предмета

Студент је стекао неопходна теоријска знања, разуме проблематику која се односи на теорију бројева и криптографију и оспособљен је за решавање задатака и проблема из ових области.

Садржај предмета

Теоријска настава

Дељивост целих бројева. Основне особине. Највећи заједнички делилац. Еуклидов алгоритам.
Прости и сложени бројеви. Бесконачност скупа простих бројева. Мерсенови бројеви. Дистрибуција простих бројева. Основна теорема аритметике и њене примене.
Функције теорије бројева. Број делилаца и збир делилаца. Ојлерова функција.
Конгруенције. Системи остатака по датом модулу. Ојлерова теорема и примене. Поредак броја по датом модулу. Линеарна конгруенција. Системи линеарних конгруенција. Конгруенције вишег реда.
Основе криптографије. Криптографски систем. Криптографија тајног кључа. Блок системи и DES. Криптографија јавног кључа. Криптографски системи засновани на проблему факторизације. RSA систем. Криптографски системи засновани на проблему дискретног логаритма. Веза теорије бројева и криптографије.

Практична настава

Примена теоријских знања за решавање проблема и задатака из наведених области.

Литература

1. В. Мићић, З. Каделбург, *Увод у теорију бројева*, Друштво математичара Србије, Београд, 2001.
2. Р. Тошић, В. Вукославчевић, *Елементи теорије бројева*, Алеф, Нови Сад, 1995.
3. Б. Боровићанин, *Дискретна математика - теорија бројева, комбинаторика и теорија графова*, ПМФ, Крагујевац, 2019.
4. М. Станић, Н. Икодиновић, *Теорија бројева, збирка задатака,* Завод за уџбенике и наставна средства, Београд, 2004.
5. A. Dujella, M. Maretić*, Криптографија*, Елемент, Загреб, 2007.

Број часова активне наставе	**Теоријска настава: 2**	**Практична настава: 2**

Методе извођења наставе

Предавања, вежбе, консултације

Оцена знања (максимални број поена 100)

Предиспитне обавезе	**50 поена**	**Завршни испит**	**50 поена**
активност у току предавања	2	писмени испит (тест)	25
домаћи задаци	8	усмени испит	25
колоквијум-и	40		
семинар-и			