Студијски програм: Основне академске студије математике

Назив предмета: Теорија бројева и криптографија

Статус предмета: Изборни на модулима Професор математике, Теоријска математика и примене и Рачунарство и примењена математика

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. Основна теорема аритметике и њене примене.

Прости и сложени бројеви. Ератостеново сито. Бесконачност скупа простих бројева. Мерсенови бројеви. Дистрибуција простих бројева.

Функције теорије бројева. Функција цео део. Број делилаца и збир делилаца.

Конгруенције. Системи остатака по датом модулу. Ојлерова функција. Ојлерова теорема и примене. Поредак броја по датом модулу. Критеријуми дељивости. 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, теорија графова*, материјал припремљен за студенте, 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

Реализација предавања и вежби по моделу интерактивне наставе, уз LMS Moodle (наставне методе: популарно предавање, дискусија, методе практичног рада, методе демонстрације уз ресурсе за Е-учење); Активирани облици студирања и учења: вербално, смисаоно, рецептивно учење/студирање истраживањем, кооперативно практично учење.

Оцена знања (максимални број поена 100)

Предиспитне обавезе	50 поена	**Завршни испит**	50 поена
активност у току предавања	4	писмени испит	
практична настава		усмени испит	50
колоквијум-и	46		
семинар-и			