Катедри за рачунарство и информатику
Предмет: Сагласност за одбрану мастер рада.-

Одлуком Катедре и ННВ од 30.6.2017. именовани смо у комисију за одбрану мастер рада под насловом "Алгоритми засновани на рођенданском парадоксу и примене" кандидата **Мине Бадовинац,** модул Рачунарство и информатика на студијском програму Математика.

Мина Бадовинац је 20.8.2018. доставила текст свог рада. Тема рада је такозвани рођендански парадокс, чињеница да ако се од n објеката на случајан начин извлачи са враћањем $k = 1.2\sqrt{n}$ објеката, онда је вероватноћа да нека два од изабраних објеката буду једнаки приближно $1/2$.
Рад је подељен у осам поглавља. У првом поглављу износе се чињенице о рођенданском парадоксу. У другом поглављу излажу се алгоритми за одређивање периода и апериодичног почетка задатог низа (Флојдов, Брентов и Нивашов алгоритам). Треће поглавље бави се особинама низа $X, F(x), F\big(F(x)\big), \dots$, где је $F(x)$ функција дефинисана на коначном скупу. Овакви низови су увек периодични, при чему се дужина периода може проценити полазећи од рођенданског парадокса. Наводе се познате статистичке карактеристике оваквих низова ако је $F(x)$ случајна функција. У поглављу четири разматрају се примене описаних алгоритама у теорији бројева - за факторизацију природних бројева и за решавање проблема дискретног логаритма. Поглавље пет бави се анализом блоковских шифри у режиму CBC (cypher block chaining) с обзиром на изложене алгоритме. У поглављу шест разматрају се напади (тражење колизија) код криптографских хеш функција. Реализација описаних алгоритама и експерименти са њима описани су у поглављу седам. За фамилију случајних функција на скуповима величине око $2^k, k = 5,6, \dots ,20$, на основу резултата експеримената приказана је зависност карактеристика низа (пре свега дужине периода) и времена извршавања алгоритама од величине скупа.

Мишљење.

Увидом у текст **Мине Бадовинац** "Алгоритми засновани на рођенданском парадоксу и примене" дошли смо до закључка да приложени рад задовољава у потпуности захтеве који се постављају при изради мастер рада и предлажемо Катедри да одобри јавну одбрану рада.

У Београду, 24.8.2018.

Др Миодраг Живковић, ред. проф., ментор

Др Филип Марић, ванр. проф.

Др Весна Маринковић, доцент