УНИВЕРЗИТЕТ У НОВОМ САДУ
ПРИРОДНО-МАТЕМАТИЧКИ ФАКУЛТЕТ

ИЗВЕШТАЈ О ОЦЕНИ МАСТЕР РАДА

I ПОДАЦИ О КОМИСИЈИ

1. **Датум и орган који је именовао Комисију**

   5. 9. 2023. Веће Департмана за математику и информатику Природно-математичког факултета Универзитета у Новом Саду

2. **Састав Комисије са назнаком имена и презимена сваког члана, звања, назива уже научне области за коју је изабран у звање, датума избора у звање и назив факултета, установе у којој је члан комисије запослен:**

   - Др Петар Ђапић, ванредни професор на Природно-математичком факултету у Новом Саду, ужа научна област: алгебра и математичка логика, изабран у звање 1. 6. 2018. – председник комисије

   - Др Владо Уљаревић, доцент на Природно-математичком факултету у Новом Саду, ужа научна област: алгебра и математичка логика, изабран у звање 15. 3. 2022. – члан комисије

   - Др Бојан Башић, редовни професор на Природно-математичком факултету у Новом Саду, ужа научна област: дискретна математика, изабран у звање 1. 4. 2023. – ментор

II ПОДАЦИ О КАНДИДАТУ

1. **Име, име једног родитеља, презиме:**

   Бранка, Никола, Милаковић

2. **Датум рођења, општина, република:**

   29. 12. 1997, Сремска Митровица, Србија

3. **Година уписа на дипломске академске студије, смер/усмерење:**

   2020, Мастер професор математике

III НАСЛОВ МАСТЕР РАДА

Примена теорије бројева у криптографији

ПРЕГЛЕД МАСТЕР РАДА

Мастер рад заузима 56 страна и садржи 12 библиографских јединица. Подељен је на следеће главе: 1. Предговор, 2. Увод, 3. Историја, 4. Шифровање помоћу јавног кључа, 5. Протокол бацања новчића, 6. Блокчејн технологија, 7. Закључак, 8. Биографија.

Глава 2. Увод је подељена на две секције. У првој од њих се укратко презентује шта је теорија бројева, а у другој шта је криптографија.

Глава 3. Историја је подељена на три секције. У првој од њих се приказују разни начини шифровања порука кроз историју, и уводи се појам стенографије. У другој се презентује Виженерова шифра, а у трећој историјат познате машине Енигма.

Глава 4. Шифровање помоћу јавног кључа је најобимнија. Подељена је на 8 секција. Кроз њих се уводе основни појмови, уводи се дискретан логаритам, појам алгоритма и сложености алгоритма, Дифи-Хелман шифровање, поступци за одабирање великих простих бројева, РСА шифровање, Хеш функција, и шифровање помоћу елиптичне криве.

Глава 5. Протокол бацања новчића, као што јој и само име каже, бави се тзв. Протоколом бацања новчића (енгл. coin-flip protocol), који обезбеђује поштену размену информација међу више неповерљивих страна.

И назив главе 6. Блокчејн технологија такође непосредно сугерише шта је њен садржај.

Коначно, у глави 7. Закључак сумира се шта је урађено у предметном мастер раду.

V ВРЕДНОВАЊЕ ПОЈЕДИНИХ ДЕЛОВА МАСТЕР РАДА

Рад *Примена теорије бројева у криптографији* садржи све битне елементе мастер рада: предговор, текст који је по садржају разврстан у више глава, закључак и списак коришћене литературе. Рад је написан читко, прегледно и математички прецизно. Структура рада је добро конципирана: кроз уводну главу и потом главу о историји ове тематике читалац се полагано припрема за математику која стоји иза свега, што ће потом и уследити у наредним главама. Треба истаћи и да рад покрива врло широк временски распон, будући да креће од најранијих историјских почетака, а завршава се са блокчејн технологијом, која је продукт врло новијег датума.

VI ЗАКЉУЧЦИ ОДНОСНО РЕЗУЛТАТИ ИСТРАЖИВАЊА

Од прадавних почетака па до модерног света, увек се јављала потреба за неким видом енкриптовања одређених информација (а тиме и потреба за налажење начина да се енкриптована порука декриптује без знања о начину енкрипције, тј. да се шифра „разбије“). Многи данашњи алгоритми енкрипције (чак би се могло рећи већина њих) почивају на појмовима који припадају дисциплини теорије бројева. У раду је анализирана улога теорије бројева у криптографији, и презентовани су разни алгоритми енкрипције који су се у свету јављали кроз историју па све до данас.

VII КОНАЧНА ОЦЕНА МАСТЕР РАДА

Садржај и структура мастер рада су у потпуности урађени у складу са одобреном темом. Прегледно и детаљно су наведени најављени резултати, коришћена литература је релевантна а докази су математички коректно и прецизно изведени. Уопште, материја је изложена на начин који показује да је кандидаткиња у великој мери овладала овом облашћу.

VIII ПРЕДЛОГ

Имајући у виду све претходно речено, Комисија предлаже да се мастер рад *Примена теорије бројева у криптографији* прихвати а кандидаткињи Бранки Милаковић одобри одбрана.

Нови Сад,

ПОТПИСИ ЧЛАНОВА КОМИСИЈЕ

_____

Др Петар Ђапић,
ванредни професор ПМФ-а, председник

_____

Др Владо Уљаревић,
доцент ПМФ-а, члан

_____

Др Бојан Башић,
редовни професор ПМФ-а, ментор