УНИВЕРЗИТЕТ У НОВОМ САДУ
ПРИРОДНО-МАТЕМАТИЧКИ ФАКУЛТЕТ

ИЗВЕШТАЈ О ОЦЕНИ МАСТЕР РАДА

I ПОДАЦИ О КОМИСИЈИ

1. Датум и орган који је именовао Комисију

18.05.2016.,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 Бранимир Шешеља, редовни професор ПМФ у Новом Саду, алгебра и математичка логика, 27.3.1992 – председник
- др Андреја Тепавчевић, редовни професор ПМФ у Новом Саду, алгебра и математичка логика, 1.12.2003 – члан
- др Петар Ђапић, доцент ПМФ у Новом Саду, алгебра и математичка логика, 1.6.2009. – ментор

II ПОДАЦИ О КАНДИДАТУ

1. Име, име једног родитеља, презиме:
Даниел, Сњежана, Дивјаковић
2. Датум рођења, општина, република:
8.4.1990. , Осијек, Рерублика Хрватска
3. Година уписа на дипломске академске студије, смер/усмерење:
2013. , Мастер Примењене Математике, Техно – математика

III НАСЛОВ МАСТЕР РАДА

Основе криптологије, ОТП и РСА алгоритам

IV ПРЕГЛЕД МАСТЕР РАДА

Мастер рад има 56 страна, 12 цитата (библиографске јединице), 6 табела и 8 слика. Рад се састоји из 4 дела.

У првом делу се говори о историјским коренима стеганографије, развоју криптографије кроз време и појави криптоанализе. Први део садржи одељке: 1.1. Увод, 1.2. Мотиви из историје, 1.3. Појам криптологије и стеганографије.

У другом делу налази се математички апарат, дефиниције и теореме неопходне за даљи рад. Други део садржи одељке: 2.1. Математичка основа, 2.2. Појмови, дефиниције и теореме.
Трећи део идејно дели криптографију на две њене основне целине : симетричну и асиметричну криптографију. Треће поглавље садржи одељке: 3.1. Криптографија са приватним кључем, 3.2. Криптографија са јавним кључем.

У четрвтом делу говори се о криптографској валути „Bitcoin“ као једном од најзначајнијим продуката криптографиједанашњице. Четврто поглавље садржи одељке: 4.1. Биткоин.

V ВРЕДНОВАЊЕ ПОЈЕДИНИХ ДЕЛОВА МАСТЕР РАДА

Мастер рад "Основе криптологије, ОТП и РСА алгоритам" је прецизно и прегледно написан, са јасним закључцима и реалним указивањем на предности и мане криптографских метода и алата.

У првом делу кандидат прегледно излаже историјске мотиве, од којих су најзначајнији Цезарова и Вижнерова шифра. Потом постепено уводи читаоца у појмове неопходне за даље разумевање материје. Такође прецизно дефинише појмове стеганографије и криптологије (криптографије и криптоанализе), наводи начела криптографије и основне поделе шифри по разним критеријумима. Што се тиче криптоанализе, анализиране су разне врсте криптографских напада, и дискутован је метод фреквенције појаве слова.

Други део посвећен је пре свега математичко теоретском алату које је неопходан да би се пре свега осталог схватио, а потом и доказао механизам функционисања РСА алгоритма. Кандидат ставља највећи акценат на теореме на којима се заснива сам РСА алгоритам – Еуклидов, проширен Еуклидов алгоритам и Ојлерову теорему, а пре тога дефинисани су неки фундаментални појмови неопходни за разумевање датих теорема. Након тога следи и криптографски део теорије, дефинисање појмова криптосистема и шифре и појам савршене сигурности.

У првој половини трећег дела детаљно је разрађен један од најпознатијих и најфундаменталнијих метода криптографије са приватним кључем - ОТП алгоритам. Показано је како овај метод има савршену сигурност али су поред његових предности наведени и главни недостаци. Друга половина трећег дела посвећена је, по кандидату, можда и најзначајнијем алату модерне криптографије - РСА алгоритму. Ту је систематично и прецизно описано како он функционише, обрађени су процеси енкрипције и декрипције, те је уз помоћ раније наведене математичке основе показано и да РСА алгоритам испуњава критеријуме неопходне да би неки алгоритам заправо и био шифра. У том истом формулисани су и објашњени појмови хеш функције и дигиталног потписа, те њихова употребна сврха.

Коначно, у последњем делу говори се о криптографској валути Биткоин као једном од најкреактивнијих продуката саме криптографије и њених метода. Са реалног аспекта представњени су значај, предности и мане Биткоина.

VI ЗАКЉУЧЦИ ОДНОСНО РЕЗУЛТАТИ ИСТРАЖИВАЊА

Мастер рад **"Основе криптологије, ОТП и РСА алгоритам"** садржи све битне елементе једног мастер рада. У раду су представљени неки од најзаступљенијих имплементација криптографије данас, поготово РСА алгоритма као једном од, и данас, најприменљивијих метода асиметричне криптографије. Кроз оригиналне примере кандидат је илустровао главне карактеристике, предности и мане оваквог криптовања. Материјал је изложен на разумљив начин, а матеаматичке дефиниције, теореме и докази тврђења су потпуно прецизни. Слике и табеле прате текст и доприносе лакшем прихватању обрађене материје. Такође, са неколико шема на којима су представљени процеси криптовања, криптоаналитичког напада и дигиталног потписивања кандидат помаже читаоцима да у потпуности схвате наведене појмове. Рад је систематичан, детаљан и разумно изложен.

VII КОНАЧНА ОЦЕНА МАСТЕР РАДА

Мастер рад је урађен у складу са одобреном темом. Кандидат је користио најновију литературу и успео је да на јасан начин прикаже основе криптологије и релевантне резултате у вези са ОТП и РСА алгоритмима из области криптографије. Целокупни садржај наведен у пријави теме је детаљно анализиран, наведени су и кандидатови оригинални примери, докази су математички исправни и у потпуности коректни.

VIII ПРЕДЛОГ
На основу укупне оцене, комисија предлаже да се мастер рад "Основе криптологије, ОТП и РСА алгоритам" прихвати, а кандидату Даниелу Дивјаковићу одобри усмена одбрана.

Нови Сад,2016.

ПОТПИСИ ЧЛАНОВА КОМИСИЈЕ

Др Бранимир Шешеља, председник

_____

Др Андреја Тепавчевић, члан

_____

Др Петар Ђапић, ментор

_____