УНИВЕРЗИТЕТ У БЕОГРАДУ - ЕЛЕКТРОТЕХНИЧКИ ФАКУЛТЕТ
Булевар краља Александра 73, 11000 Београд, Србија
Тел. 011/324-8464, Факс: 011/324-8681

КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Милоша Стојановића под насловом „Имплементација брзе методе за криптоанализу класичних алгоритама замене". Након прегледа материјала Комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Милош Стојановић је рођен 17.10.1991. године у Београду. Завршио је основну школу "Стефан Немања" у Београду са одличним успехом. Уписао је Математичку гимназију у Београду и завршио је са одличним успехом. Електротехнички факултет уписао је 2010. године. Дипломирао је на одсеку за Рачунарску технику и информатику 2015. године са просечном оценом 7,67. Дипломски рад одбранио је у октобру 2015. године са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на Модулу за Рачунарску технику и информатику уписао је у октобру 2015. године. Положио је све испите са просечном оценом 9,4.

2. Опис мастер рада

Мастер рад обухвата 64 стране, са укупно 43 слике, 1 табелом и 14 референци. Рад садржи увод, 4 поглавља и закључак (укупно 6 поглавља), списак коришћене литературе и прилог.

Прво поглавље представља увод у коме су описани предмет и циљ рада. Приказане су основе криптографије и криптоанализе, као и кратак историјат ових научних области и дат је преглед садржаја рада.

У другом поглављу је детаљније изложена проблематика рада. Најпре је дата подела техника криптографије и ближе су описане оне које се разматрају у раду. Затим су дате различите поделе техника криптоанализе и ближе су описане оне које су од интереса. Након тога прецизно је дефинисан проблем и дат је кратак преглед постојећих решења. На крају је презентовано предложено решење.

У трећем поглављу објашњена је реализација предложеног решења. Најпре је направљен преглед коришћених технологија уз образложење погодности истих за реализацију задатог проблема. Затим је приказана општа архитектура имплементираног система, а након тога су дати и најинтересантији детаљи имплементације кроз класне дијаграме и дијаграме секвенце.

У четвртом поглављу илустрован је начин рада реализоване апликације. Приказани су сви екрани апликације и демонстриране су све могућности кроз конкретан пример криптоанализе шифрованог текста.

У петом поглављу анализирани су добијени резултати. Како је циљ рада био да се верификује исправност познатог алгоритма, резултати који су наведени у литератури упоређени су са оним који су добијени тестирањем апликације. Осим тога, измерени су и резултати добијени након примене побољшања алгоритма која су направљена у раду.

Шесто поглавље је закључак у оквиру кога је дат критички осврт на све што је урађено. Поред тога су наведени предлози за потенцијална побољшања имплементираног решења.

3. Анализа рада са кључним резултатима

Мастер рад дипл. инж. Милоша Стојановића се бави проблематиком криптоанализе класичних алгоритама замене, са посебним акцентом на криптоанализу моноалфабетске шифре. Криптоанализа има јако важну улогу у развијању нових, али и тестирању постојећих техника криптографије. Када су у питању класични криптографски алгоритми није једноставно илустровати да величина коришћеног кључа не игра значајну улогу када постоји статистика оригиналне поруке која се преноси на шифровану поруку. Из тог разлога потребно је да постоји софтверски систем помоћу кога би се за кратко време показало да је код оваквих шифара могуће доћи до оригиналне поруке и без познавања кључа.

Реализовани софтверски систем представља имплементацију познатог алгоритма из литературе. Систем омогућава учитавање текста на основу кога ће се направити почетна статистика, као и константну допуну почетне базе знања. Омогућено је и шифровање, односно дешифровање порука коришћењем моноалфабетског алгоритма, коришћењем произвољног кључа. Главна функционалност алгоритма је криптоанализа шифроване поруке коришћењем имплементираног алгоритма са могућношћу коришћења различито постављених параметара.

У раду је извршена провера функционалности и перформанси одабраног алгоритма криптоанализе. Упоређени су емпиријски резултати са резултатима који су наведени у литератури. Примењена су одређена побољшања алгоритма наведена у литератури и направљена је анализа ефикасности таквих побољшања. Дате су смернице за даљи развој алгоритма.

4. Закључак и предлог

Кандидат Милош Стојановић је у свом мастер раду успешно имплементирао брзи алгоритам криптоанализе за класичне алгоритме замене и развио систем који успешно врши криптоанализу произвољних текстова шифрованих моноалфабетском шифром. Креирани систем је лак за коришћење и погодан за демонстрацију проблема који постоје код класичних алгоритама замене, а који нису везани за дужину кључа, коришћењем конкретних примера у реалном времену. Систем је послужио и за верификацију резултата наведених у литератури.

На основу горе наведеног Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да прихвати рад „Имплементација брзе методе за криптоанализу класичних алгоритама замене“ дипл. инж. Милоша Стојановића као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 02. 09. 2016. године

Чланови комисије:

Др Жарко Станисављевић, доцент

Др Зоран Јовановић, професор