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. Ирине Кулић под насловом „Визуелна репрезентација одабраног напада на криптографске алгоритме“. Након прегледа материјала Комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Ирина Кулић је рођена 24.04.1988. године у Београду. Завршила је основну школу "Петар Кочић" у Београду као носилац Вукове дипломе. Средњу електротехничку школу “Никола Тесла“ у Београду завршила је са одличним успехом. Електротехнички факултет уписала је 2007. године. Дипломирала је на одсеку за Рачунарску технику и информатику 2014. године са просечном оценом 7,69. Дипломски рад одбранила је у октобру 2014. године са оценом 10. Дипломске академске студије – мастер на Електротехничком факултету у Београду, на Модулу за рачунарску технику и информатику уписала је у октобру 2014. године. Положила је све испите са просечном оценом 9,33.

2. Опис мастер рада

Мастер рад обухвата 45 страна, са укупно 43 слике и 9 референци. Рад садржи увод, 3 поглавља и закључак (укупно 5 поглавља), списак коришћене литературе и прилог.

Прво поглавље представља увод у коме су описани предмет и циљ рада. Објашњена је важност заштите података и криптографије, а приказане су и разне врсте напада на критографске алгоритме, као и значај коришћења едукативних алата за разумевање алгоритма и напада на њих. У уводу је дат и кратак преглед осталих поглавља.

У другом поглављу је детаљније изложена проблематика рада. Најпре је дат историјски развој симетричних блок алгоритама. Након тога је описан DES алгоритам, који је 20 година био коришћен као стандард. Затим је објашњено зашто је превазиђен и приказани су покушаји да се привремено замени алгоритмом 3-DES, али и разлог због чега 2-DES није могао да се користи у ту сврху. У наставку поглавња описан је напад „сусрет у средини“ на двоструку енкрипцију DES алгоритма и укратко је објашњен S-DES алгоритам за криптовање.

У трећем поглављу објашњена је имплементација софтверског система за визуелну репрезентацију одабраног напада. Најпре је приказан одабрани дизајн система, кроз који су објашњене и све могућности самог система. Затим је објашњена софтверска имплементација самог криптографског алгоритма, али и одабраног напада на тај алгоритам. На крају су анализирани проблеми који су се јављали приликом имплементације.

У четвртом поглављу илустрован је начин рада имплементираног софтверског система. Одабран је један сценарио напада и на њему је приказана визуелна репрезентација која је подржана у систему.

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

3. Анализа рада са кључним резултатима

Мастер рад дипл. инж. Ирине Кулић се бави проблематиком визуелне репрезентације напада „сусрет у средини“ (*енг. meet in the middle*) код двоструке енкрипције S-DES алгоритмом (*енг. double S-DES*). Криптографски алгоритми и напади на њих у неким случајевима могу бити веома апстрактни и нејасни. Због тога се као врста помоћи у разумевању оваквих целина реализују визуелни симулатори као едукативни алати чија је сврха боље разумевање алгоритама и напада на њих.

Реализовани систем кроз један такав симулатор по корацима приказује како се изводи напад „сусрет у средини“ (*енг. meet in the middle*) као један од интересантних напада на симетричне блок алгоритме. Систем приказује овај напад на примеру рада двоструке енкрипције S-DES алгоритма (*енг. double S-DES*), који редукује димензије проблема, али задржава исту идеју напада као да је у питању двострука енкрипција DES алгоритма (*енг. double DES*). Омогућено је уношење оригиналног текста и два кључа за шифровање, израчунавање шифрованог текста и праћење корака извршавања описаног напада на алгоритам све до проналажења кључева које је корисник на почетку унео.

4. Закључак и предлог

Кандидат Ирина Кулић је у свом мастер раду успешно имплементирала софтверски систем за визуелну репрезентацију напада „сусрет у средини“ (*енг. meet in the middle*) код двоструке енкрипције S-DES алгоритмом (*енг. double S-DES*). Креирани систем је једноставан за употребу и погодан за демонстрацију ове врсте напада на криптографске алгоритме.

На основу горе наведеног Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да прихвати рад „Визуелна репрезентација одабраног напада на криптографске алгоритме“ дипл. инж. Ирине Кулић као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 15. 09. 2016. године

Чланови комисије:

Др Жарко Станисављевић, доцент

Др Зоран Јовановић, професор