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 одржаној 04.07.2017. године именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Драгане Букумире под насловом „Имплементација алгоритма за поделу тајних кључева". Након прегледа материјала Комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Драгана Букумира је рођена 30.12.1993. године у Конареву, код Краљева. Завршила је основну школу „Ђура Јакшић" у Конареву. Гиманазију, природно-математички смер, у Краљеву је завршила 2012. године. Исте године је уписала Електротехнички факултет Универзитета у Београду. Дипломирала је на Модулу за рачунарску технику и информатику 2016. године са просечном оценом 8,53. Дипломски рад одбранила је у септембру 2016. године са оценом 10. Мастер академске студије је уписала исте године на Електротехничком факултету, на Модулу за Рачунарску технику и информатику. Положила је све испите са просечном оценом 6,2.

2. Опис мастер рада

Мастер рад обухвата 55 страна, са укупно 18 слика и 7 табела. 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. Разматрана је тематика рада по поглављима.

У другом поглављу је дат кратак историјат криптографије, преглед тематике која је обрађена и опис Шамировог алгоритма за поделу тајних кључева чија имплементација је тема овог рада. У истом поглављу су описана већ постојећа решења и упоређена су са предложеним.

У трећем поглављу су описане технологије које су коришћене за израду овог пројекта, Андроид оперативни систем, *NFC* технологија и *Web socket* протокол.

Четврто поглавље детаљно описује функционалности компоненти система, архитектуру, комуникацини протокол и програмско решење оба дела система.

У оквиру петог поглавља су описане функционалности графичког корисничког интерфејса мобилне апликације.

Шесто поглавље је закључак у оквиру кога су описани проблеми приликом реализације решења и предлози за даља унапређења.

3. Анализа рада са кључним резултатима

Мастер рад дипл. инж. Драгане Букумире се бави имлементацијом алгоритма за поделу тајних кључева. Циљ рада је реализација система за поделу тајних кључева. У ту сврху имплементиран је Шамиров алгоритам за поделу тајних кључева. Генерисани кључ се дели на компоненте које се путем *Web socket* конекције пребацују на мобилне уређаје. Мобилни уређаји могу размењивати компоненте кључа међу собом путем *NFC* конекције. Када се у меморији мобилног уређаја нађе довољан број компоненти кључа, могуће га је реконструисати.

Основни доприноси рада су: 1) имплементација Шамировог алгоритма за поделу тајних кључева у програмском језику Јава, 2) имплементација коришћења *NFC* технологије на Андроид уређајима, 3) приказ потенцијалне примене реализованог система.

4. Закључак и предлог

Кандидат Драгана Букумира је у свом мастер раду успешно решила проблем имплементације система за сигурну размену тајног кључа. Захваљујући овом решењу двојна или вишебројна контрола је омогућена сваком систему који би се интегрисао са реализованим.

Кандидат је исказао самосталност и систематичност у своме поступку.

На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да прихвати рад „Имплементација алгоритма за поделу тајних кључева“ дипл. инж. Драгане Букумире као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 13. 09. 2019. године

Чланови комисије:

Др Жарко Станисављевић, доц.

Др Зоран Јовановић, ред. проф.