КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА
ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 07.10.2025 године именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Миљан Петковић под насловом „Апликација за безбедну размену порука заснована на алгоритмима AES (ECB/CBC), RSA и SHA-256". Након прегледа материјала Комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Миљан Петковић је рођен 03.01.2000. године у Алексинцу. Завршио је основну школу „Љупче Николић" у Алексинцу као вуковац. Уписао је Гимназију „Светозар Марковић" на смеру „Обдарени ученици у математичкој гимназији" у Нишу коју је завршио као вуковац. Током школовања освојио је више награда на државним такмичењима из физике. Електротехнички факултет уписао је 2019. године. Дипломирао је на одсеку за Електротехнику и рачунарство модул Рачунарска техника и информатика 2023. године са просечном оценом 8.57. Дипломски рад одбранио је у септембру 2023. године са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на Модулу софтверско инжењерство уписао је у октобру 2023. године. Положио је све испите са просечном оценом 8.60.

2. Извештај о студијском истраживачком раду

Кандидат Миљан Петковић је као припрему за израду мастер рада спровео истраживање релевантне литературе која се односи на различите криптографске механизме. Анализирана су постојећа решења и приступи који се користе у дизајну система за шифровану комуникацију, као и њихове предности и ограничења у погледу безбедности, перформанси и применљивости. На основу спроведеног истраживања дефинисана је архитектура и реализован софтверски прототип за безбедну размену порука, који комбинују симетричне (AES) и асиметричне (RSA) алгоритме, уз примену хеш функција (SHA-256) и дигиталних сертификата ради спровођења аутентикације и потврде интегритета поруке. На основу спроведеног истраживања закључено је да овај приступ представља поуздану основу за имплементацију система за безбедну комуникацију, који је развијен у оквиру мастер рада.

3. Опис мастер рада

Мастер рад обухвата 50 страна, са 7 слика, 2 табеле и 11 референци. Рад садржи увод, 5 поглавља и закључак (укупно 7 поглавља) и списак коришћене литературе.

Прво поглавље представља увод у коме су описани предмет и циљ рада. Објашњен је значај безбедне комуникације у савременим мрежним системима и дата мотивација за развој софтверског решења које омогућава поуздану размену порука између клијентских апликација.

У другом поглављу је представљен теоријски оквир који обухвата основне криптографске концепте, алгоритме и безбедносне принципе неопходне за разумевање примене метода у овом систему. Описане су симетричне и асиметричне технике шифровања, хеш функције и механизми дигиталног потписа који чине основу развијеног решења.

У трећем поглављу су представљена сродна решења и системи који омогућавају end-to-end енкрипцију, као и анализа њихових предности и ограничења. Дефинисани су функционални и безбедносни захтеви који су послужили као основа за дизајн апликације.

У четвртом поглављу је описана структура софтверског решења као и коришћене технологије. Приказани су модули апликације, везе између клијентског и серверског дела система, као и механизми за енкрипцију, потписивање и верификацију порука.

У петом поглављу представљена је софтверска имплементација предложеног система за безбедну размену порука. Корак по корак се приказује иницијализације и конфигурација система, уз коришћење релевантних исечака кода.

У шестом поглављу је описана евалуација система и анализа добијених резултата. Приказани су резултати функционалног и безбедносног тестирања, мерења перформанси током енкрипције и декрипције и анализа понашања система у условима повећаног оптерећења. Дати су и закључци о ефикасности и поузданости

предложеног решења.
Седмо поглавље је закључак у коме је описан значај решења и могућа даља унапређења. Истакнути су потенцијали за интеграцију пост-квантних криптографских алгоритама и оптимизацију система за рад у реалном окружењу са већим бројем корисника.

4. Анализа са кључним резултатима

Мастер рад се бави проблематиком пројектовања и имплементације система за безбедну размену порука заснованог на савременим криптографским алгоритмима. У раду је реализована апликација која комбинује симетричну и асиметричну криптографију уз примену хеш функције SHA-256 и дигиталних сертификата ради потврде аутентичности и интегритета. Развијен је хибридни протокол који обезбеђује поверљивост комуникације, потписивање и верификацију порука, као и механизам ротације кључева ради повећања безбедности. Систем је имплементиран помоћу OpenSSL библиотекеи оцењен као стабилан и поуздан, са могућностима даљег унапређења кроз интеграцију додатних алгоритама и развој графичког интерфејса.

5. Закључак и предлог

Кандидат Миљан Петковић се у свом мастер раду успешно бавио пројектовањем система за безбедну размену порука заснованог на савременим криптографским алгоритмима. Предложена унапређења, као што су интеграција додатних алгоритама и развој графичког интерфејса, могу значајно да прошире функционалност и применљивост развијеног система за безбедну размену порука.
Кандидат је исказао самосталност и систематичност у своме поступку као и иновативне елементе у решавању проблематике овог рада.
На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад дипл. инж. Миљан Петковић прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 11.10.2025. године

Чланови комисије:

др Маја Вукасовић Доцент
сагласан, 11.10.2025.

др Жарко Станисављевић Ванредни професор
сагласан, 11.10.2025.