Математички факултет
Универзитета у Београду

МОЛБА
ЗА ОДОБРАВАЊЕ ТЕМЕ МАСТЕР РАДА

Молим да ми се одобри израда мастер рада под насловом:

Криптографски хеш алгоритам SHA-3

Значај теме и области:
SHA-3 (Keccak) је за најновији стандардни криптографски хеш алгоритам (стандард FIPS 202) изабран као победник на конкурсу NIST (Национални институт за стандарде и технологију, САД). Аутори алгоритма предвидели су и додатне примене, које NIST још увек није стандардизовао. Алгоритам ради на принципу сунђерасте структуре – упија било коју количину података и избацује тражену количину података, понашајући се као псеудослучајна функција, у зависности од свих претходних улаза.

Специфични циљ рада:
У раду ће бити анализиран алгоритам SHA-3 и његове примене. Полазећи од програмске реализације алгоритма биће практично демонстриране различите примене алгоритма.

.

Ана Станковић, 1096/2016, Информатика
(име и презиме студ., бр. инд., ознака програма и модула)

Сагласан ментор Миодраг Живковић

(својеручни потпис студента)

(својеручни потпис ментора)

18.05.2020.
(датум подношења молбе)

Чланови комисије

1. др Александар Картељ, доцент
2. др Стефан Мишковић, доцент

Катедра за рачунарство и информатику је сагласна са предложеном темом.

(*шеф катедре*)

(*датум одобравања молбе*)