Математички факултет
Универзитета у Београду

МОЛБА
ЗА ОДОБРАВАЊЕ ТЕМЕ МАСТЕР РАДА

Молим да ми се одобри израда мастер рада под насловом:

Корелациони напад на проточне шифре

Значај теме и области:

Разматрају се проточне шифре у којима се користе генератори псеудослучајног низа са померачким регистрима са линеарном повратном спрегом. Уколико код оваквог генератора постоји статистичка кроскорелација излазног низа са линеарном комбинацијом излаза неких регистара, тада је потенцијално могућ напад на шифру, под претпоставком да су на располагању парови (отворени текст, шифрат) добијени истим кључем.

Специфични циљ рада:

У раду треба описати корелациони напад уопште и напад на неколико конкретних генератора псеудослучајног низа. Програмски треба реализовати корелациони напад на неки од тих генератора.

Остале битне информације:

Литература:
[1] Stamp, Low, Applied Cryptanalysis: Breaking Ciphers in the Real World, Wiley, 2007, поглавље 3.

Дејан Капларевић, MP 1093/2014
(име и презиме студ., бр. инд., ознака програма и модула)

_____
(својеручни потпис студента)

_____
(датум подношења молбе)

Сагласан ментор Миодраг Живковић

_____
(својеручни потпис ментора)

Чланови комисије

1. Предраг Јаничић
2. Младен Николић

Катедра за рачунарство и информатику је сагласна са предложеном темом.

_____
(*шеф катедре*)

_____
(*датум одобравања молбе*)