Математички факултет
Универзитета у Београду

МОЛБА
ЗА ОДОБРАВАЊЕ ТЕМЕ МАСТЕР РАДА

Молим да ми се одобри израда мастер рада под насловом:

Криптоанализа алгоритма A5/1

Значај теме и области:
Криптографски генератор псеудослучајних бројева A5/1 део је протокола GSM (Global System for Mobile Communications) и користи се у мобилним мрежама широм света. Генератор је анализиран у више радова, где су демонстрирани ефикасни криптоаналитички напади. Сви ти напади захтевају снажан хардвер, велику меморију и подразумевају обимна припремна израчунавања. У раду [1] описан је напад који се може ефикасно извршити на персоналном рачунару.

Специфични циљ рада:
Циљ мастер рада је реализовати напад описан у раду [1] и проверити његову ефикасност.
Претпоставка је да је на располагању отворени текст довољне дужине и одговарајући шифрат.

Остале битне информације:
Литература:
[1] V. Bulavintsev, A. Semenov, O. Zaikin and S. Kochemazov, A Bitslice Implementation of Anderson's Attack on A5/1, Open Engineering, https://doi.org/10.1515/eng-2018-0002

Кристина Милетић 1082/2020 МР Миодраг Живковић

_____ Сагласан ментор _____

(име и презиме студ., бр. инд., ознака програма и модула)

_____ _____

(својеручни потпис студента) (својеручни потпис ментора)

_____ Чланови комисије

(датум подношења молбе)

1. др Саша Малков, ванр. проф.
2. др Младен Николић, доцент

Катедра за рачунарство и информатику је сагласна са предложеном темом.

_____ _____

(*шеф катедре*) (*датум одобравања молбе*)