Катедри за рачунарство и информатику
Предмет: Сагласност за одбрану мастер рада.-

Одлуком Катедре и ННВ од 30.05.2014. именовани смо у комисију за одбрану мастер рада под насловом "Криптоанализа алгоритма A5/2" кандидата **Мартина Хофера,** студијски програм Информатика.

Кандидат је 20.9.2015. доставио текст свог рада. Тема рада је криптоанализа алгоритма A5/2, који се користи за шифровање података у систему GSM. Описан је и реализован напад који се изводи под претпоставком да се познаје шифрат и одговарајући отворени текст.

Рад се састоји од девет поглавља и закључка. У поглављу 1 описује се систем GSM и уводе се неопходни појмови из криптологије. Детаљи архитектуре GSM мреже описани су у поглављу 2; у поглављу 3 специфицирају се криптографски елементи система GSM: алгоритми за аутентикацију корисника, генерисање кључа и шифровање података, као и процедура успостављања везе између корисника и мреже. Алгоритам A5/2 описан је у поглављу 4, а технички аспекти мреже који чине напад могућим приказани су у поглављу 5. У поглављу 6 описани су пасивни напади (напади приликом којих нападач само пресреће податке) на A5/2, од којих је напад из тачке 6.1.3 програмски реализован. У поглављу 7 представљени су активни напади, тј. напади у току којих нападач и прима и шаље податке и мрежи и кориснику. У поглављу описани су могући сценарији напада. Коначно, у поглављу 9 описана је програмска реализација напада из тачке 6.1.3. На крају се дају закључци и преглед могућих праваца даљег рада.

Мишљење.

Увидом у текст **Мартина Хофера** "Криптоанализа алгоритма A5/2" мишљења смо да приложени рад задовољава у потпуности захтеве који се постављају у изради мастер рада и предлажемо Катедри да одобри јавну одбрану рада.

У Београду, 21.9.2016.

Др Миодраг Живковић, ред. проф., ментор

Др Филип Марић, ванр. проф.

Др Младен Николић, доцент