9123

Математички факултет
Универзитета у Београду

УНИВЕРЗИТЕТ У БЕОГРАДУ
МАТЕМАТИЧКИ ФАКУЛТЕТ
Студентска служба
Бр. 6/51
23.04.2014. год.
Београд, Студентски трг 16
тел. 20 27 801

МОЛБА
ЗА ОДОБРАВАЊЕ ТЕМЕ МАСТЕР РАДА

Молим да се одобри израда мастер рада под називом:

Криптоанализа алгоритма A5/2

чији су значај и специфични циљ следећи:

GSM (Global System for Mobile Communications, оригинално Groupe Spécial Mobile) користи A5/2 као један од криптографских алгоритама за заштиту. Одмах по објављивању, 1999. године, испоставило се да је алгоритам A5/2 слаб и да се може разбити у реалном времену са обичном опремом. Тек неколико година касније, од 2006. године GSMA(GSM Association) забрањује употребу тог алгоритма у мобилним телефонима. У раду ће алгоритам за шифровање и дешифровање A5/2, бити програмски реализован. Основни део рада биће приказ и програмска реализација напада на A5/2 и то са и без познатог отвореног текста.

Литература:

[1] E.Barkan, E.Biham, N.Keller, „Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication“, у књизи D. Boneh, „CRYPTO 2003“, LNCS 2729, стр. 600-616

Мартин Хофер, 1012/11, Информатика
(име и презиме студента, бр. индекса, модул)

(својеручни потпис студента)

23.04.2014. године
(датум подношења молбе)

Сагласан ментор Миодраг Живковић

(својеручни потпис ментора)

Чланови комисије
1. Филип Марић
2. Младен Николић

Катедра за рачунарство и информатику даје сагласност предложеној теми

(шеф катедре)

(датум одобравања молбе)