

МОЛБА
ЗА ОДОБРАВАЊЕ ТЕМЕ МАСТЕР РАДА

Молим да се одобри израда мастер рада под називом:

Анализа излазног низа генератора RC4

чији су значај и специфични циљ следећи:

Алгоритам за шифровање RC4 је најпопуларнији и најшире се користи, иако је то најједноставнија од свих проточних шифри. У мастер раду треба приказати анализу излазног низа генератора RC4 на основу [1] (непостојећа стања, слабост почетног дела низа, слабости у вези са анализом два узастопна корака и др.) и експериментима потврдити неке од елемената ове анализе.

Литература:

[1] G. Paul, S. Maitra, "RC4 stream cipher and its variants", CRC press, 2012.

Јована Радуловић,
..../....., Рачунарство и информатика
(2мр сс)

(својеручни потпис студента)

(датум подношења молбе)

Ментор
Миодраг Живковић

Чланови комисије

1. Предраг Јаничић

2. Младен Николић

Катедра за рачунарство и информатику даје подршку предложеној теми

(шеф катедре)
молбе)

(датум одобравања