9128

Математички факултет
Универзитета у Београду

МОЛБА
ЗА ОДОБРАВАЊЕ ТЕМЕ МАСТЕР РАДА

Молим да се одобри израда мастер рада под називом:

Напад на шифру RC4 у оквиру протокола WEP

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. Специјално, алгоритам RC4 је део протокола WEP за комуникацију у бежичним мрежама. У мастер раду треба приказати напад FMS [2] на протокол WEP, као и усавршене верзије тог напада на основу [1]. Поред тога у раду треба програмски реализовати елементе напада.

Литература:
[1] G. Paul, S. Maitra, "RC4 stream cipher and its variants", CRC press, 2012.
[2] S. R. Fluhrer, I. Mantin, A. Shamir. Weaknesses in the Key Scheduling Algorithm of RC4. SAC 2001, vol. 2259, Lecture Notes in Computer Science, Springer, 1–24.

Александра Арсић,
1025/2013, Рачунарство и информатика (2мр сс)

(својеручни потпис студента)

(датум подношења молбе)

Ментор
Миодраг Живковић

Чланови комисије

1. Предраг Јаничић
2. Филип Марић

Катедра за рачунарство и информатику даје подршку предложеној теми

(шеф катедре)

(датум одобравања молбе)