Математички факултет
Универзитета у Београду

МОЛБА
ЗА ОДОБРАВАЊЕ ТЕМЕ МАСТЕР РАДА

Молим да ми се одобри израда мастер рада под насловом:

Криптоанализа алгоритма ORYX

Значај теме и области:

Криптолошке стандарде за мобилну телефонију у северној Америци прописала је својевремено Telecommunications Industry Association (TIA). Део тих стандарда је алгоритам **ORYX,** који се у оквиру мобилне телефоније користио за шифровање података. Алгоритам ORYX је проточна шифра. Низ бајтова добијених из генератора комбинује се са отвореним текстом применом операције XOR (ексклузивно ИЛИ). Иако алгоритам има кључ од 96 бита, убрзо се испоставило [1] да је ефективна дужина кључа свега око 16 бита и да је за напад довољно познавање првих 25-27 бајтова шифрата и одговарајућег отвореног текста.

Специфични циљ рада:

Циљ рада је програмска реализација напада на алгоритам ORYX на основу [1,2], под претпоставком да се познаје шифрат и одговарајући отворени текст.

Литература:

[1] D. Wagner, L. Simpson, E. Dawson, J. Kelsey, W. Millan, B. Schneier, "Cryptanalysis of ORYX"], Fifth Annual Workshop on Selected Areas in Cryptography, Springer, 1998.
[2] M. Stamp, R. M. Low, Applied Cryptanalysis: Breaking Ciphers in the Real World, Wiley, New Jersey, 2007.

Дејан Капларевић, 1093/2014, МР
(име и презиме студ., бр. инд., ознака програма и модула)

_____
(својеручни потпис студента)

_____
(датум подношења молбе)

Сагласан ментор Миодраг Живковић

_____
(својеручни потпис ментора)

Чланови комисије

1. др Предраг Јаничић, ред. проф.
2. др Саша Малков, ванр. проф.

Катедра за рачунарство и информатику је сагласна са предложеном темом.

_____
(*шеф катедре*)

_____
(*датум одобравања молбе*)