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

Одлуком Катедре и ННВ од 30.5.2014. именовани смо у комисију за одбрану мастер рада под насловом "Напад на шифру RC4 у оквиру протокола WEP" кандидата **Александре Арсић,** студијски програм Математика, модул рачунарство и информатика.

Кандидат је 15.9.2014. доставила текст свог рада. Тема рада је реализација напада FMS на алгоритам за шифровање у оквиру протокола WEP објављеног у раду **S. Flufrer, I. Mantin, A. Shamir**, *Weaknesses in the Key Scheduling Algorithm of RC4*. SAC 2001, 1-24, Lecture Notes in Computer Science, vol. 2259, Springer.
Бежичне мреже користе радио сигнале за пренос података, па су за разлику од жичаних мрежа подложне прислушкивању. Да би се подаци који се преносе бежичним мрежама заштитили, комитет IEEE (Institute of Electrical and Electronics Engineers) је прописао скуп стандарда IEEE 802.11 који регулише безбедност на WLAN-у (Wireless Local Area Network). Део овог стандарда је протокол WEP (Wired Equivalent Privacy) који за шифровање пренетих података користи познати једноставан, а квалитетан алгоритам RC4. Врло брзо се испоставило да је начин коришћења алгоритма RC4 у оквиру протокола WEP (случајно или намерно) лош, што је омогућило разбијање овог система. У мастер раду су приказани недостаци система и напад FMS, један од познатих напада на WEP. Напад је програмски реализован, чиме је практично проверена могућност откривања тајног кључа за шифровање на основу одређеног броја ухваћених пакета.
Рад се састоји од четири поглавља и закључка. После увода у другом поглављу се уводе неопходни појмови и описује се поступак шифроване комуникације заснован на проточним шифрама. У трећем поглављу описује се алгоритам RC4, протокол WEP и како се користи алгоритам RC4 у оквиру протокола WEP. Четврто поглавље описује напад FMS.
У петом поглављу је приказана програмска реализација напада. На крају се дају закључци и преглед могућих праваца даљег рада.

Мишљење.

Увидом у текст **Александре Арсић** "Напад на шифру RC4 у оквиру протокола WEP" 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, 19.9.2014.

Др Миодраг Живковић, ред. проф., ментор

Др Предраг Јаничић, ванр. проф.

Др Филип Марић, доцент.