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

Одлуком Катедре и ННВ од 9.9.2016. именовани смо у комисију за одбрану мастер рада под насловом "Криптоанализа алгоритма Oryx" кандидата **Дејана Капларевића,** студијски програм Математика, модул Рачунарство.

Кандидат је 15.9.2017. доставио текст свог рада. Тема рада је алгоритам Oryx за шифровање у систему ГСМ - део система заштите комуникација мобилних телефона у САД. Иако алгоритам има кључ од 96 бита, испоставља се да је ефективна дужина кључа свега око 16 бита и да је за напад довољно познавање првих 25 бајтова шифрата и одговарајућег отвореног текста.

Рад се састоји од пет поглавља и два прилога. После увода, у поглављу 2 приказан је систем ГСМ и елементи заштите у том систему. У поглављу 3 уводе се појмови неопходни за разумевање алгоритма Oryx - коначна поља и линеарни померачки регистар (ЛПР), после чега следи спецификација алгоритма Oryx. У поглављу 4 описује се напад (приказан у литератури) на алгоритам Oryx, када се зна 25 првих бајтова шифрата и исто толико одговарајућих бајтова отвореног текста. Анализирана је могућност једноставне модификације алгоритма Oryx тако да се избегне осетљивост на овакав напад: довољно је да се у сваком кораку из померачких регистара узима само по један бит, уместо по један бајт; цена је, наравно, осам пута спорије шифровање. Део рада је и анализа могућности напада под претпоставком да се зна само део шифрата. Алгоритам Oryx и напад програмски су реализовани на језику C; програми су редом у прилогу 1, односно прилогу 2. На крају се дају закључци и преглед могућих праваца даљег рада.

Мишљење.
Увидом у текст **Дејана Капларевића** "Криптоанализа алгоритма Oryx" 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, 19.9.2017.

Др Миодраг Живковић, ред. проф., ментор

Др Предраг Јаничић, ред. проф.

Др Саша Малков, ванр. проф.