Математички факултет
Универзитета у Београду

**МОЛБА**
**ЗА ОДОБРАВАЊЕ ТЕМЕ МАСТЕР РАДА**

Молим да ми се одобри израда мастер рада под насловом:

***„Криптоанализа шифре KASUMI"***

**Значај теме и области:**
У последњих неколико деценија тајност већег дела GSM комуникација штићена је проточним шифрама A5/1 и A5/2, за које је више аутора показало да су криптолошки слабе. Ове шифре су замењене новим алгоритмима, A5/3 и A5/4, заснованим на блоковској шифри KASUMI. У раду [1] описан је тзв. сендвич напад са повезаним кључевима на алгоритам KASUMI. Постојање овог напада не угрожава сигурност комуникације у реалним условима.

**Специфични циљ рада:**
Циљ рада је програмски реализовати напад са повезаним кључевима на комплетан алгоритам KASUMI (или на варијанту алгоритма са смањеним бројем рунди) описан у раду [1].

**Остале битне информације:**
Литература:
[1] O. Dunkelman, N. Keller, A. Shamir, A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony, Journal of Cryptology vol. 27, 824–849 (2014)

**Кристина Станојевић, 1084/2017, Информатика** Сагласан ментор **Миодраг Живковић**
*(име и презиме студента, бр. индекса, модул)*

*(својеручни потпис студента)*

*(својеручни потпис ментора)*

**7. јун 2021. године**
*(датум подношења молбе)*

Чланови комисије
1. др Саша Малков, ванр. проф.
2. др Нина Радојичић Матић, доцент

Катедра **за рачунарство и информатику** је сагласна са предложеном темом.

*(шеф катедре)*

*(датум одобравања молбе)*