Тема: Математичке основе криптосистема: факторизација, дискретни логаритам и елиптичке криве

Наставник: Бојана Боровићанин

У мастер раду ће бити представљени основни појмови теорије бројева, укључујући модуларну аритметику и тестове простости, који чине темељ криптосистема јавног кључа. Затим ће се детаљно анализирати проблем факторизације великих бројева кроз различите алгоритме, уз поређење њихових перформанси, као и проблем дискретног логаритма у класичним групама. Посебан део ће бити посвећен елиптичким кривама (дефиниција, закон сабирања тачака, алгоритми за бројање тачака и избор безбедних параметара). Резултати ће бити сумирани и упоређени како би се истакле предности и ограничења сваке методе. Размотриће се утицај квантних алгоритама на ове проблеме, дати препоруке за избор кључних величина и елиптичких кривих, и указати на могуће правце будућих истраживања.

Литература

1. A. Dujella, *Теорија бројева у криптографији - скрипта*, Природословно-математички факултет, Свеучилиште у Загребу, 2003.
2. N. Koblitz, *A Course in Number Theory and Cryptography*, Springer New York, NY, 2012.
3. A. J. Menezes, P. C. van Oorschot, S A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.
4. В. Мићић, З. Каделбург, *Увод у теорију бројева*, Друштво математичара Србије, Београд, 2001.
5. J.H. Silverman, J. Pipher, J. Hoffstein, *An Introduction to Mathematical Cryptography,* Springer New York, NY, 2010.
6. Р. Тошић, В. Вукославчевић, *Елементи теорије бројева*, Алеф, Нови Сад, 1995.