Szakdolgozat kivonat

Pintér József

Matematika BSc 2020

A szakdolgozatom témája az NSUCrypto nemzetközi kriptográfiai olimpia 2019-es versenyének A szekciójának feladatai. Az NSUCRYPTO (2014-) az egyetlen olyan kriptográfiai olimpia, mely matematikai, kriptográfiai és programozási problémákat ötvöz hivatásos titkosírás szakértők, egyetemi hallgatók és középiskolás diákok számára is a világ bármely részéről. A szakdolgozat nemcsak a feladatok megoldásával foglalkozik, hanem azok továbbgondolásával is. A legtöbb probléma megoldása közben előjönnek érdekes összefüggések, észrevételek, melyek bizonyítása olykor igen kemény feladatnak minősülhet.

Az első feladat során megismerkedünk egy egyszerű, de érdekes algoritmussal. Itt található a szakdolgozat fő tétele, melyben megadjuk az algoritmus maximális iterációszámát. A második feladatban egy oszthatósági állítást látunk be egy véletlenszám generátorral kapcsolatban az Euler-Fermat tétel segítségével. A harmadik feladat során megismerkedünk a helyettesítő rejtjelezéssel és a gyakoriság analízis módszerével. A negyedik feladatban megismerjük a forgótárcsás rejtjelező matematikai modelljét, és annak segítségével dekódolunk egy titkos szöveget. Az ötödik feladatban egy adott polinomot próbálunk reprezentálni minél kevesebb megadott művelet segítségével. A hatodik feladatban megismerkedünk az RSA-titkosítással, és a feladat megoldásában kulcsszerepet játszó Shamir-féle titokmegosztással.