Titokmegosztás falra akasztott képekkel

Horváth Sándor

"Petru Maior" Tudományegyetem

shorvath@science.upm.ro

Képzeljünk el egy titkos kóddal-kulccsal lezárt páncélszekrényt, amely egy munkacsoport fontos dokumentumait tartalmazza. Oly módon kívánunk hozzáférést biztosítani a páncélszekrény tartalmához, hogy kijelöljük a munkacsoport bizonyos rész-csoportjait, amelyek tagjai– és csak ezek – együttesen jogosultak a hozzáféréshez, minden más ki nem jelölt csoport viszont nem jogosult. A titokmegosztás (secret sharing) alapproblémája az, hogy milyen legyen az a kulcs, amelynek bizonyos részleteit kiosztva a résztvevők között, csak a kijelölt csoportok részleteinek együttese elegendő a kód megfejtéséhez, tehát a páncélszekrény kinyitásához, viszont a nem jogosult csoportok által ismert részletek együttese sem visz közelebb a kód megfejtéséhez.

A titokmegosztás problémájára számos megoldás született. Ezek matematikai alapjai között a moduláris aritmetikát használó lineáris egyenletrendszerek, és a véges testek feletti polinomok is előfordulnak. Itt egy algebrai topológiai fogantatású, eredetileg egy trükkös képfelakasztási feladványként megfogalmazott probléma megoldásának felhasználására teszünk javaslatot, és bemutatjuk egy lehetséges titokmegosztási módszer elvi körvonalait.