Elliptikus görbéken alapuló nyilvános kulcsú kriptográfia elemzése chipkártyás és PC-s környezetben

Berta István Zsolt, Műszaki informatika szak V. évfolyam
Mann Zoltán Ádám, Műszaki informatika szak V. évfolyam
Konzulens: Dr. Vajda István, Híradástechnikai Tanszék

(Összefoglaló)

A nyilvános kulcsú (aszimmetrikus) titkosító eljárások számos előnnyel rendelkeznek a szimmetrikusokkal szemben. Ezek közül a legfontosabb, hogy lehetővé teszik a hitelesség és a letagadhatatlanság biztosítását. Ugyanakkor nagy számításigényük jelentős korlátozó tényezőnek bizonyult, különösen szűk kapacitású eszközökben, mint például a chipkártyák. A nyilvános kulcsú titkosítás másik korlátja, hogy mindössze egy algoritmus, az RSA, bizonyult a gyakorlatban is használhatónak, így lényegében egyedül ez terjedt el. Ennek az algoritmusnak a biztonsága azonban nem bizonyított. Ha egy napon kiderül, hogy az RSA nem biztonságos, alternatíva nélkül maradunk.

Létezik azonban több kevéssé ismert nyilvános kulcsú eljárás, amelyek az RSA alternatívájául szolgálhatnak. Mi ezek egyikével, az ECC-vel (Elliptic Curve Cryptography) foglalkoztunk. A feltalálók állítása szerint ez az algoritmus nem csupán alternatívája az RSA-nak, hanem ugyanazt a biztonságot lényegesen kisebb kulcsméret mellett tudja biztosítani, így sokkal hatékonyabb.

Mivel azonban az ECC biztonsága sem bizonyított, a gyakorlati tapasztalatoknak kell eldönteniük, hogy valóban az RSA-nál hatékonyabb, illetve legalább olyan biztonságos eljárásról van-e szó.

Kutatásunk célja, hogy ezeket a tapasztalatokat bővítsük. Ennek megfelelően dolgozatunkban részletesen ismertetjük az ECC matematikai hátterét, és kitérünk az implementációs részletekre is, saját ECC megvalósításunk kapcsán. Megvizsgáljuk, melyek az ECC biztonság és hatékonyság szempontjából kritikus részei, milyen törési lehetőségek kínálkoznak. Összehasonlítjuk az ECC-t és az RSA-t az implementációs tapasztalatok, valamint a mérési eredményeink alapján. Megvizsgáljuk alkalmazásunkat PC-n, és a mai chipkártyák adta szűk erőforrás-keretek között is.