Aszimmetrikus kripto, hibák és félreértések

Márton Gyöngyvér

EMTE-Sapientia, Matematika-Informatika kar

mgyongyi@ms.sapientia.ro

A kriptográfia tudományos alapokon való kidolgozása az 1970-es években kezdődött, és az elmúlt évek akadémiai kutatásainak köszönhetően napjainkban a számítógépes adatbiztonság egyik legstabilabb területének számít. Mindezek ellenére a kriptográfiai algoritmusokat óvatosan kell kezelni, mert értelmezésükkor, alkalmazásukkor, az implementációk kivitelezésekor számos biztonsági rést idézhetünk elő.

Jelen előadásban elsősorban az aszimmetrikus kriptográfia területéhez tartozó algoritmusok jelenlegi problémáiról fogunk beszélni, amelyek biztonsága lényegében három számelméleti probléma (egész számok felett értelmezett faktorizáció probléma, prímtestek felett értelmezett diszkrét logaritmus probléma, és elliptikus görbék felett értelmezett diszkrét logaritmus probléma) feltételezett nehézségén alapszik.

Hivatkozások

[1] Arjen K. Lenstra, James P. Hughes, Maxime Augier, Joppe W. Bos, Thorsten Kleinjung, and Christophe Wachter, *Ron was wrong, Whit is right.* IACR Cryptology ePrint. 2012. https://eprint.iacr.org/2012/064.pdf.

[2] Neal Koblitz and Alfred J. Menezes, *A Riddle wrapped in an enigma.* IACR Cryptology ePrint. 2015. https://eprint.iacr.org/2015/1018.pdf

[3] Nadia N Heninger, *RSA, DH, and DSA in the Wild.* Cryptology ePrint Archive. 2022. https://eprint.iacr.org/2022/048.pdf