DEBRECENI EGYETEM
Informatikai Tudományok Doktori Iskola

Szigorlati melléktárgy Kriptográfia

Tematika Matematikai alapok: helyiértékes számábrázolás és általánosításai. Alapműveletek algoritmusai. Kongruenciák, diszkrét logaritmus, műveletek maradékosztályokkal. Legnagyobb közös osztó, prímfaktorizáció, Rácsok, az LLL algoritmus. Algoritmusok: szimmetrikus és aszimmetrikus titkosítás. DES, AES. RSA, El Gamal és DELP-n alapuló titkosítás. Authentikáció, digitális aláírás, titokmegosztás, kulcs csere. Nyilvános kulcs infrastruktúra. Post kvantum kriptográfia

Irodalom

1. Attila Pethő, Algebraische Algorithmen, Vieweg Verlag, 1999.
2. Johannes Buchmann, Introduction to cryptography. Second edition. Undergraduate Texts in Mathematics. *Springer-Verlag, New York,* 2004.
3. H. Cohen and G. Frey Eds.: Handbook of Elliptic and Hyperelliptic CurveCryptography, Chapman & Hall/CRC, 2005.
4. D. Hankerson, A. Menezes and S. Vanstone, Guide to Elliptic Curve Cryptography, Springer, 2005.
5. D.J. Bernstein, J. Buchmann and E. Dahmen, Eds.: Post-quantum cryptography, Springer, 2009.