A titkosírások matematikai alapjai

(Mathematical Foundation of Cryptography)

VEMIMAB512A

Javasolt irodalom / Suggested reading:

(!) *Algebrai eszközök és az elliptikus görbék a kriptográfiában*, 46 oldal, 27Mb
http://math.uni-pannon.hu/~szalkai/Algebra+elliptikus+titkosiras.pdf

(!) *Kryptosysteme*, Fern Universität in Hagen, 385 old 5Mb (németül)
http://math.uni-pannon.hu/~szalkai/Krypt-Algebra-Buch.pdf

Beutelspacher, A., Schwenk,J., Wolfenstetter,K.D.: *Moderne Verfahren der Kryptographie, von RSA zu Zero-Knowledge*, Vieweg Verlag, 2002.

Douglas R.Stinson: *Cryptography, Theory and Practice*, CRC Press, London, 1995, in series: Discrete Mathematics, series editor Kenneth H. Rosen,

Gonda J.: *Véges testek*, http://compalg.inf.elte.hu/material/DOWNLOAD/vt.pdf

Gonda J.: *Hibakorlátozás*, http://compalg.inf.elte.hu/material/DOWNLOAD/hibakor.pdf

Neal Koblitz, N.: *A Course in Number Theory and Cryptography*, Springer, 1987

Menezes, A.J., Oorschot,P.C., Vanstone,S.V.: *Handbook of Applied Cryptography*, CRC Press, 1997, 2001, online: http://www.cacr.math.uwaterloo.ca/hac/

(!) Szalkai I., Dósa Gy.: *Algoritmikus számelmélet*, Typotex Kiadó 2011,
http://www.tankonyvtar.hu/hu/tartalom/tamop425/0008_szalkai_dosa_szamelmelet/adatok.html

(!) Szalkai I.: *Algebra és számelmélet feladatgyűjtemény*, PE kiadó, 2000.

Vajda István: *Kriptográfia bevezető*, BME-VIK, 1998