A tantárgy neve: A TITKOSÍRÁSOK MATEMATIKAI ALAPJAI	**Kódja: VEMIMAB512A**
Angolul: MATHEMATICAL FOUNDATION OF CRYPTOGRAPHY	
Kötelező előtanulmány(ok) kódja(i): **VEMIMA1344I (ILA) és VETKMA1243D (DIMAT)**	
Tantárgyfelelős neve: Dr. Szalkai István	**A tárgy oktatásának tanéve/féléve:**

Óraigény: E: 2 GY: 0 L:0	**Számonkérés módja:** K	**Kreditértéke:** 2

Purpose: To present the necessary mathematical tools for cryptography.
Oktatási cél: Megismertetjük a Hallgatókat a titkosírásokhoz szükséges matematikai alapokkal.

Ismeretkörök:

Csoportok: elem és csoport rendje, mellékosztályok. Lagrange-, Euler- és Fermat tételei. Véges csoportok, a véges exponensű Abel-csoportok alaptétele.

Gyűrűk: Euklideszi gyűrűk, maradékos osztás, egyértelmű prímfelbontás gyűrűkben, maradékosztályok, a Zm, Zm*, Zm[x], Z[i], Z[ρ] és R[x] struktúrák.

Kongruenciák és -rendszerek, Euklideszi algoritmus és alkalmazásai. Magasabbfokú kongruenciák, kvadratikus maradékok, Jacobi- és Legendre szimbólumok.

Faktorgyűrűk.

Testek. Véges testek: Weddenburn tétele, véges testek konstruálása tetszőleges prímhatvány esetén.

Boole algebrák, algebrai és geometriai hálók. Algoritmikus problémák: Lovász és Ajtai tételei, az LLL algoritmus.

Elliptikus görbék, csoportok EG -n.

A számelmélet algoritmikus vonatkozásai. Prímtesztek és -felbontások.

RSA-, hátizsák algoritmusok.

Bizonyítás 0 információval.

Titkosírások elliptikus görbéken és hálókon.

Javasolt irodalom / Suggested reading:

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

Tanszékvezető aláírása:	**A tárgy oktatójának aláírása:**

A tantárgy neve: A TITKOSÍRÁSOK MATEMATIKAI ALAPJAI		**Kódja: VEMIMAB512A**
Angolul: MATHEMATICAL FOUNDATION OF CRYPTOGRAPHY		
Kötelező előtanulmány(ok) kódja(i): **VEMIMA1344I (ILA) és VETKMA1243D (DIMAT)**		
Tantárgyfelelős neve: Dr. Szalkai István		**A tárgy oktatásának tanéve/féléve:**
Óraigény: E: 2 GY: 0 L:0	**Számonkérés módja:** K	**Kreditértéke:** 2

Purpose: To present the necessary mathematical tools for cryptography.
Oktatási cél: Megismertetjük a Hallgatókat a titkosírásokhoz szükséges matematikai alapokkal.

Ismeretkörök:

Groups: order of elements, cosets, theorems of Lagrange, Euler and Fermat. Finite groups, the classification problem, the Fundamental theorem of Abel groups of finite exponents.

Rings: Euclidean rings and (residual) -division, residual sets, unique prime-factorization, the structures Zm, Zm*, Zm[x], Z[i], Z[ρ] and R[x].

Linear single and systems of congruences. Euclidean algorithm and applications.

Congruences of higher order, quadratic residuals, symbols of Jacobi and Legendre.

Ideals and factor-rings.

Fields, examples. Theorems of Frobenius and Weddenburn. Constructions of finite fields for any power of primes.

Algebraic lattices and Boole algebras. Geometrical lattices, algorithmic problems, theorems of Lovász and Ajtai. The Lovász-Lenstra-Lenstra algorithm.

Elliptical curves, groups EC.

Algorithmic problems of number theory. Prime tests, factorizations and generation.

The RSA and knapsack algorithms. Zero knowledge proofs.

Cryptography on finite fields, elliptical curves and geometrical lattices.

Javasolt irodalom / Suggested reading:

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

Tanszékvezető aláírása:	**A tárgy oktatójának aláírása:**