Programtervező Informatikus MSc
Információs Rendszerek szakirány

ELTE IK, Komputeralgebra Tanszék
Tantárgyi dokumentáció

TÁRGY NEVE: Kódelmélet és kriptográfia EA

TÁRGY KÓDJA: IPM-08irKKRE

Összes kredit: 2

Összes óraszám: 2

Óra típusa	**előadás**	**gyakorlat**	**konzultáció**
Kredit	2		
Heti óraszám	2		
Számonkérés módja	K		

Tematika:

1. A kódoláselmélet és a rejtjelezés algebrai és valószínűségi alapjai
2. Lineáris és ciklikus kódok
3. Reed-Solomon kódok
4. Kódkonstrukciók
5. Kódolási korlátok
6. Klasszikus rejtjelezés; folyamrejtjel és blokkrejtjel
7. DES és AES
8. Nyilvános kulcsú rejtjelezés
9. Az RSA és a Rabin-variáns
10. Diszkrét logaritmus a rejtjelezésben; az ALGamal rendszer; Diffie-Hellman kulcscsere; kulcscsere nélküli protokoll
11. Integritás; az MDC és a MAC; hasító függvények
12. Személyazonosítás; ZK-protokollok
13. Hitelesítés; digitalis aláírás

Irodalom:

Buttyán, L., Vajda, I.: *Kriptográfia és alkalmazásai* (Typotex, 2004)
Gonda János: compalg.inf.elte.hu/material/DOWNLOAD/hibakor.pdf, 2007
Gonda János: compalg.inf.elte.hu/material/DOWNLOAD/rejtjelezes.pdf, 2007
Győrfy L., Győry S., Vajda I.: *Információ- és kódelmélet* (Typotex, 2000)
Nemetz T., Vajda I.: *Algoritmikus adatvédelem* (Akadémiai Kiadó, 1991)

Ajánlott irodalom:

Beutelspacher, A.: *Cryptology* (The Mathematical Association of America, 1994)
Berlekamp, E.R.: *Algebraic Coding Theory* (McGraw Hill, 1968)
Brassard, G.: *Modern cryptology* (Springer, 1988)
Huffman, W.C., Pless, V.: *Fundamentals of Error-correcting Codes* (Cambridge University Press, 2003)
Ködmön, J.: *Kriptográfia* (Computerbooks, 1999)
van Lint, J.H.: *Introduction to coding theory* (Springer, 1982)
Lucky, R.W., Saltz, J., Weldon, E.J.: *Adatátvitel* (Műszaki Könyvkiadó, 1973)
McWilliams, F.J., Sloane, M.J.A.: *The theory of error-correcting codes* (North-Holland, 1977)
Menezes, A., van Oorshot, P., Vanstone, S.: *Handbook of Applied Cryptography* (Press, 1996)
Roman, S.: *Coding and information theory* (Springer, 1992)
Salomaa, A.: *Public-key cryptography* (Springer, 1990)
Schneier, B.: *Applied cryptography* (Wiley, 1996)
van Tilborg: *An introduction to cryptology* (Kluiver Academic Publisher, 1988)
Virasztó, T.: *Titkosítás és adatrejtés* (NetAcadémia Oktatóközpont, 2004)