Programtervező Informatikus MSc
Modellalkotó Informatikus szakirány

ELTE IK, Komputeralgebra Tanszék
Tantárgyi dokumentáció

TÁRGY NEVE: Rejtjelezés EA

TÁRGY KÓDJA: IPM-08modREJTE

Összes kredit: 2

Összes óraszám: 2

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

Tematika:

1. A rejtjelezés alapjai; klasszikus rejtjelezés; támadási módok
2. A rejtjelezés információelméleti alapjai
3. Folyamrejtjel és blokkrejtjel
4. A DES alapjai; az AES
5. Nyilvános kulcsú rejtjelezés
6. Az RSA és a Rabin-variáns
7. Prímtesztek és egész számok felbontása
8. Diszkrét logaritmus és a rejtjelezés; az AlGamal rendszer
9. Integritás; MDC és MAC
10. Személyazonosítás; a ZK-protokollok
11. Hitelesítés; digitális aláírás
12. A nyilvános kulcsú rejtjelezés alkalmazásai; digitális pénz
13. Titokmegosztás

Irodalom:

Buttyán, L., Vajda, I.: *Kriptográfia és alkalmazásai* (Typotex, 2004)
compalg.inf.elte.hu/material/DOWNLOAD/rejtjelezes.pdf, 2008
Nemetz, T., Vajda, I.: *Algoritmikus adatvédelem* (Akadémiai Kiadó, 1991)

Ajánlott irodalom:

Beutelspacher, A.: *Cryptology* (The Mathematical Association of America, 1994)
Brassard, G.: *Modern cryptology* (Springer, 1988)
Ködmön, J.: *Kriptográfia* (Computerbooks, 1999)
Menezes, A., van Oorshot, P., Vanstone, S.: *Handbook of Applied Cryptography* (CRC Press, 1996)
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)