

Tantárgyi programok, tantárgyleírások

Tantárgy neve: Adatbiztonság és kriptográfia	Kreditszáma: 5
Tanóra típusa: előadás/labor és száma: 3/1	
Számonkérés módja: kollokvium	
Tantárgy tantervi helye (félév): 7	
Előtanulmányi feltételek (<i>ha vannak</i>): Bev. a programozásba II; Matematika szigorlat	
Tantárgyleírás:	
Az előadások keretében átfogó képet adunk az alkalmazott kriptográfia alábbi fejezeteiről: Matematikai alapok. Pszeudovéletlen bitsorozatok. Szimmetrikus kulcsú titkosítás Nyilvános kulcsú titkosítás. Hash kódolók. Azonosítás, személy hitelesítés. Digitális aláírás. Kulcs menedzsment. A Windows kriptográfiai szolgáltatásai.	
A 3-5 legfontosabb kötelező irodalom:	
Menezes, Oorschot, Vanstone: Handbook of Applied Cryptography, CRC Press, 1996; Henk van Tilborg, ed.: Encyclopedia of Cryptography and Security, Springer, 2005; elektronikus jegyzet.	
Ajánlott irodalmak:	
Buttyán L., Vajda I., Kriptográfia és alkalmazásai, Typotex Kiadó, 2004; Henk van Tilborg: Fundamentals of Cryptology: A Professional Reference and Interactive Tutorial, Kluwer Academic Publishers, 2002; Virasztó Tamás: Titkosítás és adatrejtés, NetAcademia, 2004.	
Tantárgyfelelős (<i>név, beosztás, tud. fokozat</i>) Dr. Csapodi Márton, mérnökstanár, PhD	
Tantárgy oktatásába bevont oktató(k) , ha vannak (<i>név, beosztás, tud. fokozat</i>): Dr. Csapodi Márton, mérnökstanár, PhD	