DEBRECENI EGYETEM
Informatikai Tudományok Doktori Iskola

Szigorlati főtárgy Digitális kommunikáció elmélete

Tematika Folyam- és blokkódolás. Huffman-kód. Az entrópia tulajdonságai. Szótáras tömörítés. Hang- kép- és videotömörítés. Hibajavító kódolás. Lineáris kódok, Hamming, Reed-Solomon és Goppa kódok. Szimmetrikus és aszimmetrikus titkosítás. DES, AES, RSA, El Gamal és DELP-n alapuló titkosítás. Authentikáció, digitális aláírás, titokmegosztás, kulcs csere. Protokollok formális verifikációja. Nyilvános kulcs infrastruktúra.

Irodalom

1. Györfi László, Győri Sándor, Vajda István, Információ- és kódelmélet, Typotex, 2000.
2. K. Sayood, Introduction to Data Compression, Morgan Kaufmann Publ., San Francisco, 1996.
3. Johannes Buchmann, Introduction to cryptography. Second edition. Undergraduate Texts in Mathematics. *Springer-Verlag, New York,* 2004.
4. Colin Boyd, Anish Marthuria: Protocols for Authentication and Key Establishment*,* Springer-Verlag, 2003.
5. Robert G. Gallager, Principles of Digital Communication, Cambridge University Press, 2008.