Kriptográfia és kódelmélet 3/0/0/v/3

Tárgyfelelős: Rónyai Lajos
További oktatók: Wettl Ferenc, Ivanyos Gábor

Klasszikus kriptográfia elemei. A modern kriptográfia alapjai: a bonyolultságelmélet, számelmélet, valószínűségszámítás kriptográfiában felhasznált fogalmainak rövid áttekintése.
Kiszámíthatóság – egyirányú függvények (diszkrét logaritmus, RSA-függvény, Rabin négyzetre emelés függvénye, prím faktorizációval való kapcsolatuk). Álvéletlen generátorok, álvéletelen függvények. Nemfeltáró bizonyítások, és létezésük NP-problémákra.
Kódolás és hitelesítés módszerei (privát kulcsú rendszerek, szimmetrikus titkosítási sémák, nyilvános kulcsú rendszerek: RSA-, Rabin-, hátizsák rendszerek, digitális aláírás), kulcs csere (Diffie-Hellman). Kriptográfiai protokollok: két résztvevős protokollok (oblivious transzfer, bit rábízás, ...), több résztvevős protokollok, titokmegosztás, elektronikus választás, digitális pénz.
Alapvető kommunikációs-és hibamodellek. A bináris szimmetrikus csatorna. Kódolás, dekódolás, Hamming-távolság. A (blokk)kódok alapvető paraméterei. Ismétlés: véges testek aritmetikájának rövid áttekintése, létezés, bázisok, primitív elemek, polinomok véges testek felett, számolás véges testekben. Lineáris kódok, generátormátrix, paritás-ellenőrző mátrix. Szindrómákon alapuló dekódolás. A Hamming-kód. Ciklikus kódok, generátor-polinom, ellenőrző polinom. Ciklikus kódok és ideálok. BCH-kódok. Korlát hibajavító képességükre. Berlekamp-Massey-algoritmus. Reed-Solomon- és Justensen-kódok. Az MDS-korlát, optimális kódok. Golay-kódok, perfekt kódok. Korlátok a kódparaméterekre: Varshamov-Gilbert, Delsarte, gömbkitöltési. Reed-Muller-kódok. Kapcsolatuk a Boole-függvényekkel. Goppa-kódok, nem lineáris kódok, konvolúciós kódok.

Irodalom:
R. Lidl, H. Niederreiter: Introduction to finite fields and their applications. Cambridge University Press, 1986.
Madhu Sudan : Algorithmic Introduction to Coding Theory. elektronikus jegyzet, MIT
Buttyán L. Vajda I. Kriptográfia és alkalmazásai. Typotex, 2004.

Cryptography and coding theory 3/0/0/v/3

Course coordinator: Lajos Rónyai
Other instructors: Ferenc Wettl, Gábor Ivanyos

Elements of classical cryptography. The foundations of modern cryptography: review of number theory, complexity, probability techniques relevant here.
Computability, one way functions(RSA, discrete log, Rabin squaring, prime factorization). Pseudo-random generators, zero knowledge proofs, their existence for problems in NP.
Encryption and authentication methods (private keys, symmetric schemes, public key systems, digital signatures, key exchange).
Cryptographic protocols, secret sharing, digital cash.
Communication and error models, coding, decoding, Hamming space.
Block codes, linear codes. Generator and parity check matrices, syndromes. Hamming codes. Cyclic codes, their basic properties. BCH-codes and their decoding (Berlekamp-Massey). Reed-Solomon codes, Justesen codes, MDS-codes.

Golay codes and perfect codes. Bounds for the parameters of a code (Varshamov-Gilbert, sphere packing, Delsarte). Reed-Muller codes. Goppa codes, nonlinear codes, convolution codes.

References:

R. Lidl, H. Niederreiter: Introduction to finite fields and their applications. Cambridge University Press, 1986.
Madhu Sudan : Algorithmic Introduction to Coding Theory. elektronikus jegyzet, MIT
Buttyán L. Vajda I. Kriptográfia és alkalmazásai. Typotex, 2004.