Complex exam major subject

Theory of the digital communication

Syllabus

Stream- and block coding, the Huffman code. Properties of the entropy. Data encryption with dictionary. Voice, picture and video compression. Error-correcting codes. Linear-, Hamming-, Reed-Solomon and Goppa codes and their applications. Symmetric and asymmetric encryption. Basic properties of the DES, AES, RSA, ElGamal and the elliptic curve cryptography. Authentication, digital signature, secret sharing and key exchange. Formal verification of protocols Public key infrastructure.

Bibliography

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.

Compulsory subjects for this major subject

Recommended subjects for this major subject