<table>
<tr><td colspan="2"><b><i>Name:</i></b><br><b>Information- and Coding Theory</b></td><td><b><i>NEPTUN-code:</i></b><br><i>NMXIK1EMNE</i></td><td><b><i>Number of periods/week:</i></b><br>full-time: 2 lec + 0 sem + 0 lab</td></tr>
<tr><td colspan="2"><b><i>Credit:</i></b> 5<br><b><i>Requirement:</i></b> mid-term mark</td><td colspan="2"><b><i>Prerequisite:</i></b><br>-</td></tr>
<tr><td><b><i>Responsible:</i></b><br>Aurél GALÁNTAI, Ph.D.</td><td><b><i>Position:</i></b><br>professor, habil.</td><td colspan="2"><b><i>Faculty and Institute name:</i></b><br>John von Neumann Faculty of Informatics<br>Institute of Applied Mathematics</td></tr>
<tr><td colspan="4"><b><i>Way of assessment:</i></b><br>– written exam</td></tr>
<tr><td colspan="4"><b><i>Competences</i></b></td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4"><b><i>Course description:</i></b></td></tr>
<tr><td colspan="4">Basics of information theory, entropy, variable length source coding, Huffman code. The communication channel: conditional entropy, mutual information, channels and their capacities, decoding, ideal observer. Basics of error-correcting codes: Galois fields, vector spaces. Linear codes: Hamming code, orthogonal and first order Reed-Müller code. Cyclic codes. Data compression. Theoretical limits of compression. Arithmetic coding. Important compression techniques: Lempel-Ziv algorithms, the Burrows-Wheeler method. Elements of cryptology. Classical encryptions. Model of algorithmic attacks and cryptanalysis of classical encryptions. DES and AES. Public key encoding: basics and the RSA algorithm.</td></tr>
<tr><td colspan="4"><b><i>Literature</i></b></td></tr>
<tr><td colspan="4">S. Fegyverneki: Information Theory, e-notes, Miskolci Egyetem, 2006 (in Hungarian, electronic notes)<br>L. Győrfi, S. Győri, I. Vajda: Information- and Coding Theory, Typotex, Budapest, 2002 (in Hungarian)</td></tr>
</table>