Information Theory and Cryptography

(Neptun code: GEMAK126-Ma, term mark**)**

Computer Science Engineering MSc

Course Meeting Times:
Wednesday 8-11:30, first time online, A/4 341. room

Lecturer: **Dr. Fegyverneki Sándor** office: A/4 335, e-mail: matfs@uni-miskolc.hu,

homepage: https://www.uni-miskolc.hu/~matfs/

Assignments and Grading (term mark): There will be a problem set, one final test before the last week in the busy period:

ACTIVITIES	PERCENTAGES
Problem Set(homework)	30%
Final Test	70%

Final test (7 practical problems and the minimum level is 3 perfect solved)

To master basic concepts in information theory, including source coding, and algorithms of channel capacity. To investigate important specific codes and channels. To continue to develop problem-solving skills and to apply these skills to the solving of application problems in communication theory. Be able to apply the gained knowledge to the solution of practical problems in engineering areas through evaluation and selection of appropriate statistical techniques.

Course Topics

This course will cover the following topics:

Introduction: Communication theory. Shannon's model. Probabilistic approach. What is information? Basic concepts. Typical scheme of information transmission.

Source coding : entropy, I-divergence, classification of codes, Kraft-McMillan inequality, source coding theorem, Shannon-Fano coding, Gilbert-Moore coding, Huffman coding, Extended Huffman coding. McMillan's theorem, block coding, compression.

Channel capacity: joint and conditional entropies, mutual information. types of discrete memoryless channels, BSC, BEC, channel capacity, Arimoto-Blahut algorithms.

Channel coding: Hamming weight, Hamming distance, minimum distance decoding, single parity codes, Hamming codes, repetition codes, linear block codes, cyclic codes, syndrome calculation, encoder and decoder.

Continuous source: entropy, mutual information, Gauss-channels, minimum entropy method.

Cryptography : History and basic cryptographic concepts, protocols, discrete log, and Diffie-Hellman. Public-key cryptosystems and RSA. Security of RSA, authentication, key management. Applications and the future .

Course Text

In addition to the lecture notes, students may find the following texts to be of use.

R. B. Ash. *Information Theory*. Interscience, New York. 2000.

T. M. Cover, J.A. Thomas. *Elements of information theory*. Wiley, New York. 1991.

M. Kelbert, Yu. Suhov: *Information theory and coding by example,* Cambridge University Press, 2013.

D. Salomon. *Data Compression,* Springer, 2004.

Richard A. Mollin: RSA and PUBLIC-KEY CRYPTOGRAPHY, Chapman and Hall,CRC Press LLC, 2003.

S. Guiasu. *Information theory with applications*. McGRAW-HILL, New York. 1977.

Xue-Bin Liang. *An Algebraic, Analytic and Algorithmic Investigation on the Capacity and Capacity-Achieving Input Probability Distributions of Finite-Input Finite-Output Discrete Memoryless Channels*. Department of Electrical and Computer Engineering Louisiana State University, Baton Rouge, LA 70803. 2004.

Claude E. Shannon, Warren Weaver: *The Mathematical Theory of Communication***,** *Bell System Technical Journal, 1947.*