FACULTY OF COMPUTER SCIENCE AND ENGINEERING

CURRICULUM

Affirm:
Dean:

EN 411

ENCODING AND PROTECTION OF INFORMATION

Updated: Prot. No. 23 of 28.06.2022.

Lecturer: Associate Professor Evgenia Nikolova, PhD

ABSTRACT:

The course "Coding and Information Security" is a fundamental discipline for specializations in the field of 5.3. Communication and Computer Engineering. The course provides theoretical knowledge on the fundamental concepts of coding theory, including codes, error-correcting codes, Hamming distance, code parameters, equivalence of codes, encoding and decoding with linear codes, syndrome decoding, and basics of cyclic code theory. Additionally, it imparts practical skills for assessing the qualities of compression codes, evaluating the error-correcting capabilities of codes, and constructing codes with specified properties.

MAIN OBJECTIVES:

The course focuses on the fundamentals of optimal coding, elementary concepts from information theory, basics of error-correcting coding, fundamental classes of error-correcting codes, and some fundamental bounds for codes.

PREREQUISITES:

To successfully comprehend the material covered in the Coding and Information Security course, basic knowledge in discrete mathematics, elementary understanding of linear algebra, higher algebra, and probability theory is required.

STATUTE AND STRUCTURE

specialty	status	Credits	full-time study				part-time study			
			lectures	seminars	exercises	total	lectures	seminars	exercises	total
Computer systems and technologies	Mandatory	6	30	30		60	20	10		30
Software engineering	Elective Course	6	30	30		60	20	10		30

COURSE CONTENT

Topic 1. Mathematical model of a communication system. Binary symmetric channel without memory. Binary symmetric channel with erasure. Discrete memoryless channels. Continuous channels.

Topic 2. Source coding. Prefix codes. Fano-Shannon algorithm. Huffman coding. Implementation of Huffman codes.

Topic 3. Error-correcting codes. Basic concepts. Approaches for error detection and correction. Hamming weight and distance. Basic principles of decoding.

Topic 4. Error-detecting schemes. ISBN and ISSN codes. UPC and EAN codes.

Topic 5. Fundamental problems in coding theory. Singleton, Greedy, and Hamming bounds. Equivalent codes.

Topic 6. Finite fields. Vector spaces over finite fields. Linear codes. Generator matrix. Encoding and decoding with linear codes.

Topic 7. Dual code, parity-check matrix. Syndrome decoding.

Topic 8. Cyclic codes. Ring of polynomials modulo a given polynomial. Generator polynomial and generator matrix of a cyclic code. Check polynomial and parity-check matrix of a cyclic code. Encoding and decoding with cyclic codes.

Topic 9. Code families. Huffman codes. Reed-Muller codes. Reed-Solomon codes. BCH codes.

Topic 10. Convolutional codes. Structure. Encoding with convolutional codes. Viterbi decoding algorithm.

Topic 11. Cryptography - basic concepts and classical ciphers.

SEMINAR EXERCISES

Topic 1. Source coding. Fano-Shannon algorithm. Huffman coding. Implementation of Huffman codes.

Topic 2. Compression algorithms.

Topic 3. Linear codes. Basic parameters of a linear code. Generator matrix in standard form. Encoding with linear codes.

Topic 4. Decoding with linear codes. Syndrome decoding. Dual code, parity-check matrix.

Topic 5. Cyclic codes. Ring of polynomials modulo a given polynomial. Generator polynomial and generator matrix of a cyclic code. Check polynomial and parity-check matrix of a cyclic code.

Topic 6. Encoding and decoding with cyclic codes.

Topic 7. Encoding and decoding with convolutional codes.

PLAN OF EDUCATIONAL ACTIVITIES AND TEACHING METHODS

1. The first lecture aims to familiarize students with the program content, goals, and objectives of the course, as well as the requirements for preparation.
2. Lectures cover topics from the syllabus. Each topic concludes with questions and self-preparation tasks.
3. Students work on individual assignments during seminar sessions, which contribute to ongoing assessment.
4. Ongoing assessment is also achieved through coursework and quizzes.
5. Electronic materials on the Moodle platform support student preparation and provide opportunities to expand their knowledge on specific topics. The theoretical material is presented using the following resources:
    - Books: Contain theoretical material on the topics.
    - Pages: Provide concise theoretical material or additional explanations.
    - Web resources: Include articles, online journals, ready-made templates, and other materials.
    - Video materials: Comprise instructional videos.
    - Files.

Practical work is realized through the following resources and activities:

- Assignments: Students independently solve tasks assigned by the instructor, and solutions are evaluated by the instructor.
- Tests: Used for self-preparation and self-assessment of acquired knowledge.
- Web resources: Include articles, online journals, ready-made templates, and other materials.
- Video materials: Include instructional videos on creating specific models.
- Forum: Utilized for consulting students by instructors and exchanging information among students.
- Video conferencing: Used for periodic real-time consultations between students and instructors.

METHODS OF ASSESSMENT

Throughout the semester, ongoing assessment of acquired knowledge is conducted, and results are recorded on a point-based system. Ongoing assessment includes two quizzes. The coursework is submitted and evaluated by the exercise supervisor. Students are allowed to take the final exam if they have passed and defended both modules. The exam consists of two parts – problem-solving and theory. Only students with a passing grade on the problem-solving part are eligible to take the theoretical part of the exam. The final grade is comprehensive and includes assessments from ongoing assessment, coursework, and the exam. The total number of points determines the final six-point grade according to the following scheme:

- Ongoing Assessment Grade: Up to 34 points
- Coursework Grade: Up to 12 points
- Semester Exam Grade: Up to 54 points

The overall grade is determined by the sum of points earned throughout the semester and in the exam:

- 36-50 points: Fair (3)
- 51-65 points: Good (4)
- 66-80 points: Very Good (5)
- Above 81 points: Excellent (6)

A student must have a minimum of 14 points from ongoing assessment during the semester and a minimum of 22 points from the exam procedure to receive an overall grade.

RECOMMENDED LITERATURE

1. Е. Николова, Въведение в теория на кодирането, Полиграф, Бургас, 2020
2. Е. Великова-Бандова, Записки по кодиране - Двоични шумозащитни кодове, ФОИ-КОМЕРСЕ, София, 2001.
3. Е. Великова-Бандова, Записки по кодиране - Циклични кодове, ФОИ-КОМЕРСЕ, София, 2001.
4. Raymond Hill. A first course in Coding Theory. University of Salford. Clarendon Press. Oxford,
5. 2012.
6. J.H. van Lint, Introduction to Coding Theory, Springer Verlag, Berlin, 2021.
7. V. Pless, Introduction to the Theory of Error-Correcting Codes, John Wiley, New York, 2015.
8. D.G. Hoffman, D.A. Leonard, C.C. Lindner, K.T. Phelps, C.A. Rodger, J.R. Wall, Coding theory. The essentials, Marcel Dekker INK, New York, 1992, http://index-of.co.uk/Information-Theory/Coding%20Theory%20The%20Essentials%20-%20D.G%20Hoffman.pdf

9. R. W. Yeung, Shuo-Yen Robert Li, Ning Cai, Zhen Zhang, Network coding theory, now Publishers Inc., Hanover, 2006, http://iest2.ie.cuhk.edu.hk/~whyeung/publications/tutorial.pdf

EXAM QUESTIONNAIRE

EN 411

ENCODING AND PROTECTION OF INFORMATION

Lecturer: Associate Professor Evgenia Nikolova, PhD

1. Mathematical Model of a Communication System. Binary Symmetric Channel without Memory. Binary Symmetric Channel with Deletion. Discrete Memory Channel.
2. Bitwise Coding. Prefix Codes. Fano-Shannon Algorithm.
3. Huffman Method. Program Implementation of Huffman Codes.
4. Approaches to Error Detection and Correction.
5. Basic Principles of Decoding.
6. Error Detection Schemes. ISBN and ISSN Codes. UPC and EAN Codes.
7. Fundamental Problem of Coding Theory. Singleton, Greismer, and Hamming Bounds.
8. Finite Fields. Vector Spaces over Finite Fields.
9. Linear Codes. Generating Matrix. Equivalent Linear Codes.
10. Encoding and Decoding with Linear Codes.
11. Dual Code, Parity-Check Matrix. Syndrome Decoding.
12. Cyclic Codes. Ring of Polynomials modulo a Given Polynomial. Generating Polynomial and Generating Matrix of a Cyclic Code. Parity-Check Polynomial and Parity-Check Matrix of a Cyclic Code.
13. Encoding and Decoding with Cyclic Codes.
14. Huffman Codes.
15. Reed-Muller Codes.
16. Reed-Solomon Codes.
17. BCH Codes.
18. Convolutional Codes. Structure. Encoding with Convolutional Codes.
19. Viterbi Decoding Algorithm.
20. Cryptography - Basic Concepts and Classical Ciphers.

RECOMMENDED LITERATURE

1. Е. Николова, Въведение в теория на кодирането, Полиграф, Бургас, 2020
2. Е. Великова-Бандова, Записки по кодиране - Двоични шумозащитни кодове, ФОИ-КОМЕРСЕ, София, 2001.
3. Е. Великова-Бандова, Записки по кодиране - Циклични кодове, ФОИ-КОМЕРСЕ, София, 2001.
4. Raymond Hill. A first course in Coding Theory. University of Salford. Clarendon Press. Oxford,
5. 2012.
6. J.H. van Lint, Introduction to Coding Theory, Springer Verlag, Berlin, 2021.
7. V. Pless, Introduction to the Theory of Error-Correcting Codes, John Wiley, New York, 2015.

8. D.G. Hoffman, D.A. Leonard, C.C. Lindner, K.T. Phelps, C.A. Rodger, J.R. Wall, Coding theory. The essentials, Marcel Dekker INK, New York, 1992, http://index-of.co.uk/Information-Theory/Coding%20Theory%20The%20Essentials%20-%20D.G%20Hoffman.pdf
9. R. W. Yeung, Shuo-Yen Robert Li, Ning Cai, Zhen Zhang, Network coding theory, now Publishers Inc., Hanover, 2006, http://iest2.ie.cuhk.edu.hk/~whyeung/publications/tutorial.pdf