Sveučilište u Rijeci •Odjel za matematiku
Radmile Matejčić 2 • 51 000 Rijeka • Hrvatska
T: (051) 584-650 • F: (051) 584-699
http://www.math.uniri.hr• e-adresa: math@math.uniri.hr

COURSE SYLLABUS

General information		
Course title	Coding theory and cryptography	
Study programme	Discrete mathematics and its applications	
Year of study	1	
Course status	Compulsory	
Course homepage	Merlin	
Language of instruction	English	
Credit values and modes of instruction	***ECTS credits / student workload***	6
	Hours (L+E+S)	30+15+15
Lecturer	***Name and surname***	Marija Maksimović
	Office	O-504
	Office hours	Upon request.
	Phone number	051/584-665
	E-mail	mmaksimovic@math.uniri.hr
Teaching assistant	***Name and surname***	Nina Mostarac
	Office	O-525
	Office hours	Upon request.
	Phone number	051/584-666
	E-mail	nmavrovic@math.uniri.hr

1. COURSE DESCRIPTION

1.1. Course objectives

Main course objective is to get students acquainted with basic cryptography systems and basic methods in coding theory. For that purpose it is necessary within the course to:

- describe, compare and apply different cryptography systems,
- analyse the basic principles of cryptanalysis,
- analyse the basic principles of coding theory,
- define, differentiate and apply coding methods,
- analyse error detection methods in coding,
- describe methods of correcting errors in coding.

1.2. Course prerequisites

None.

1.3. Learning outcomes

After completing this course students should be able to:

- differentiate and analyse cryptography systems and argumentedly apply adequate procedure in problem solving (A7,B7,C7,D7,E5,F7,G7),
- analyse and differentiate type codes and argumentedly apply adequate procedure in problem solving (A7,B7,C7,D7,E5,F7,G7),

- differentiate ways of detecting errors in data transfer with particular coding method and analyse the conditions under which it is possible to correct this error (A7,B7,C5,D5,E5,F5,G5),
- mathematically prove foundation of procedures and statements which they use within the course (B7, F4).

1.4. Course content

Basic terms of classical chriptography. Substitution chipers. Vigenere chiper. Playfair chiper. Hill's chiper. Enigma. History of DES. Description of the DES algorithm. Cryoanalysis DES. Some more modern block cryptosystems. The idea of a public key. RSA cryptosystem. Cryptoanalysis RSA cryptography. Other public key cryptosystems. Basic terms of coding theory. Hamming Distance. Code detection. Code correction. ISBN code. Length and weight of a code. Linear codes. Generator matrices and standard forms. Encoding. Nearest neighbour decoding. Dual code. Parity check matrix. Syndrome decoding. Finite fields. Cyclic codes. Reverse code. BCH and Reed-Solomon codes. Golay codes and perfect codes.

1.5. Modes of instruction	☒lectures ☒seminars and workshops ☒exercises ☒e-learning ☐field work	☒independent work ☒multimedia and the internet ☐laboratory ☒tutorials ☐other
1.6. Comments		

1.7. Student requirements

Students are required to earn a determined amount of points throughout semester and pass the final exam.

2. GRADING POLICY

2.1. Grading of students' work during the semester and on the final exam

During the semester, there will be 2 tests which will include exercises referring to topics dealt with in class. At each test, a student may get maximum 15 points, meaning 30 points overall for all 2 tests.

During the semester student will have to present seminars. For all the seminar student may get maximum 30 points.

During the semester student will have to do and present homeworks. For all the homeworks student may get maximum 10 points.

At the final exam, a student may get maximum 30 points.

2.2. Minimal requirements for access to the final exam / passing grade

ACTIVITY	MINIMAL NUMBER OF POINTS REQUIRED
Tests	15
Homeworks	5
Seminars	15
TOTAL:	35
OTHER REQUIREMENTS:	

2.3. Final grade – grading scale

GRADE	POINTS
Excellent (5) , A	90% - 100%

Very good (4), B	75% - 89,9%
Good (3), C	60% - 74,9%
Sufficient (2), D	50% - 59,9%
Insufficient (1), F	0% - 49,9%

3. LITERATURE

3.1. Required literature

1. Dujella: Kriptografija (online version: http://web.math.hr/~duje/kript/kriptografija.html)
2. J.I. Hall, Notes on Coding Theory, 2010 (online version: http://www.math.msu.edu/~jhall/classes/codenotes/coding-notes.html)
3. S. Singh: The Code Book, Fourth Estate, London, 1999.

3.2. Recommended literature

1. Assmus, J.D. Key, Designs and their codes, Cambridge University Press, London, 1992.
3. N. Koblitz, A Course in Number Theory and Cryptography, Springer Verlag, New York, 1994. 4. J.H. van Lint, Introduction to Coding Theory, Springer-Verlag, Berlin, 1982.
5. F.J. MacWilliams, N.J.A. Sloane, The theory of error-correcting codes, North-Holland, 1977.
6. B.Schneiner, Applied Cryptography, Wiley, NY 1995.
7. J. Seberry, J. Pieprzyk, Cryptography: an introduction to computer security, Prentice-Hall, 1989. 8. D.R.Stinson, Cryptography. Theory and Practice, CRC Press, Boca Raton, 1996.
9. D. Welsh, Codes and cryptography, Oxford: Clarendon Press, 1988.

4. ADDITIONAL INFORMATION

4.1. Class attendance

Any form of disruption during the class will not be tolerated as well as the usage of mobile phones.

4.2. Informing students

All relevant informations will be provided via the online course. It is the responsibility of a student to be regularly informed.

4.3. Other relevant information

4.4. Assessment of quality and performance for the course

Anonymous survey in which students will evaluate the quality of classes will be carried out during last week of classes. The analysis of students' success at final exams will be carried out at the end of semester.

4.5. Examination period

Final exam (1st examination period)	10.02.2022., 10:00
Final exam (2nd examination period)	24.02.2022., 10:00
Final exam (3rd examination period)	24.03.2022., 9:00

5. COURSE OUTLINE*

DATE	*TIME*	*MODE OF INSTRUCTION*	*TOPIC*	*GROUP*	*LECTURE HALL*
1.10.	16:15-18:45	E	Introduction to GAP.	all	O-334
07.10.	08:15-09:45	L	Introduction to course.	all	O-334
08.10.	16:15-18:45	S	Seminars	all	O-334
14.10.	08:15-09:45	L	Classical chriptography.	all	O-334
15.10.	16:15-18:45	S	Seminars.	all	O-334
21.10.	08:15-09:45	L	Classical chriptography.	all	O-334
22.10.	16:15-18:45	E	Classical chriptography.	all	O-334
28.10.	08:15-09:45	L	DES algorithm.	all	O-334
29.10.	16:15-18:45	E	Modern block cryptosystems.	all	O-334
4.11.	08:15-09:45	L	Modern block cryptosystems.	all	O-334
5.11.	16:15-18:45	S	Seminars.	all	O-334
11.11.	08:15-09:45	L	Public key cryptosystems.	all	O-334
12.11.	16:15-18:45	S	Seminars.	all	O-334
19.11.	16:15-18:45	E	**1th test**.	all	O-334
25.11.	08:15-09:45	L	Public key cryptosystems.	all	O-334
26.11.	16:15-18:45	S	Public key cryptosystems.	all	O-334
2.12.	08:15-09:45	L	Introduction to Coding Theory.	all	O-334
3.12.	16:15-18:45	S	Seminars.	all	O-334
9.12.	08:15-09:45	L	Linear codes.	all	O-334
10.12.	16:15-18:45	E	Linear codes.	all	O-334
16.12.	08:00-10:00	L	Decoding Linear codes.	all	O-334
17.12.	16:15-18:45	S	Seminars.	all	O-334
23.12.	08:15-09:45	L	Cyclic codes.	all	O-334
13.1.	08:15-09:45	L	Cyclic codes. BCH codes.	all	O-334
14.1.	16:15-18:45	E	Cyclic codes.	all	O-334
20.1.	08:00-10:00	L	BCH codes.	all	O-334
21.1.	16:15-18:45	E	Perfect codes. BCH codes.	all	O-334
27.1.	08:00-10:00	L	Perfect codes	all	O-334
28.1.	16:15-18:45	S	**2nd test**	all	O-334

**Minor changes are possible. Up to 40% of the teaching activities can be online*

L – lectures
E – exercises
S – seminars