

## SYLLABUS

### 1. Data about the program of study

1.1 Institution	The Technical University of Cluj-Napoca
1.2 Faculty	Faculty of Automation and Computer Science
1.3 Department	Computer Science
1.4 Field of study	Computer Science and Information Technology
1.5 Cycle of study	Bachelor of Science
1.6 Program of study / Qualification	Computer science / Engineer
1.7 Form of education	Full time
1.8 Subject code	54.20

### 2. Data about the subject

2.1 Subject name	<b>Cryptology</b>				
2.2 Course responsible/lecturer	Prof. dr. eng. Alin Suciu - <a href="mailto:alin.suciu@cs.utcluj.ro">alin.suciu@cs.utcluj.ro</a>				
2.3 Teachers in charge of seminars / laboratory / project	Prof. dr. eng. Alin Suciu - <a href="mailto:alin.suciu@cs.utcluj.ro">alin.suciu@cs.utcluj.ro</a>				
2.4 Year of study	IV	2.5 Semester	8	2.6 Type of assessment (E - exam, C - colloquium, V - verification)	E
2.7 Subject category	<i>DF – fundamentală, DD – în domeniu, DS – de specialitate, DC – complementară</i>				DS
	<i>DI – Impusă, DOp – opțională, DFac – facultativă</i>				DOp

### 3. Estimated total time

3.1 Number of hours per week	5	of which:	Course	2	Seminars	1	Laboratory	2	Project	
3.2 Number of hours per semester	70	of which:	Course	28	Seminars	14	Laboratory	28	Project	
3.3 Individual study:										
(a) Manual, lecture material and notes, bibliography										28
(b) Supplementary study in the library, online and in the field										22
(c) Preparation for seminars/laboratory works, homework, reports, portfolios, essays										26
(d) Tutoring										0
(e) Exams and tests										4
(f) Other activities:										0
3.4 Total hours of individual study (suma (3.3(a)...3.3(f)))					80					
3.5 Total hours per semester (3.2+3.4)					150					
3.6 Number of credit points					6					

### 4. Pre-requisites (where appropriate)

4.1 Curriculum	Computer Programming (C), OO Programming (Java/C#), Logic Programming (Prolog), Operating Systems
4.2 Competence	All competences related to the above disciplines

### 5. Requirements (where appropriate)

5.1. For the course	Blackboard, Projector, Computer, Online platforms
5.2. For the applications	Multicore computers, Specific Software, Online platforms

### 6. Specific competence

6.1 Professional competences	<ul style="list-style-type: none"> <li>• <b>C3.4</b> Comparatively and experimentally evaluation of the alternative solutions for performance optimization</li> <li>• <b>C3.5</b> Developing and implementing informatic solutions for concrete problems</li> </ul> <p><b>C5</b> -Designing, managing the lifetime cycle, integrating and ensuring the integrity of hardware, software and communication systems (1 credit)</p> <ul style="list-style-type: none"> <li>• <b>C5.1</b> Specifying the relevant criteria regarding the lifetime cycle, quality, security and computing system’s interaction with the environment and human operator</li> <li>• <b>C5.2</b> Using interdisciplinary knowledge for adapting the computing system to the specific requirements of the application field</li> <li>• <b>C5.3</b> Using fundamental principles and methods for security, reliability and usability assurance of computing systems</li> <li>• <b>C5.4</b> Adequate utilization of quality, safety and security standards in information processing</li> <li>• <b>C5.5</b> Creating a project including the problem’s identification and analysis, its design and development, also proving an understanding of the basic quality requirements</li> </ul> <p><b>C6</b> - Designing intelligent systems (2 credits)</p> <ul style="list-style-type: none"> <li>• <b>C6.1</b> Describing the components of intelligent systems</li> <li>• <b>C6.2</b> Using domain-specific tools for explaining and understanding the functioning of intelligent systems</li> <li>• <b>C6.3</b> Applying the fundamental methods and principles for specifying solutions for typical problems using intelligent</li> <li>• <b>C6.4</b> Choosing the criteria and evaluation methods for the quality, performances and limitations of intelligent systems</li> <li>• <b>C6.5</b> Developing and implementing professional projects for intelligent systems</li> </ul>
6.2 Cross competences	N/A

**7. Discipline objective (as results from the *key competences gained*)**

7.1 General objective	Developing the ability to identify parallelism in a given problem, and to take advantage of this parallelism using various methods and technologies for parallel programming
7.2 Specific objectives	<ul style="list-style-type: none"> <li>▪ Understanding the performance parameters of parallel algorithms</li> <li>▪ Ability to implement parallel algorithms using multithreading technologies (in C, Java, C#, Prolog, OpenMP)</li> <li>▪ Ability to implement parallel algorithms based on the VSM model (Linda)</li> <li>▪ Ability to implement parallel algorithms based on message passing (PVM, MPI)</li> <li>▪ Basic knowledge of the cutting edge developments in the field (Quantum Computing, DNA Computing)</li> </ul>

**8. Contents**

<b>8.1 Lectures</b>	Hours	Teaching methods	Notes
Introduction, Types of Parallelism, Classification, Applications	2	Lectures using blackboard and projector, interactive discussions.	
Parallel Algorithms, Performance Parameters, Amdahl’s Law, Gustafson’s Law	2		
Processes (C/UNIX), Communication, Synchronization	2		
Threads (Java, C#, Prolog), Communication, Synchronization	2		
OpenMP (1)	2		
OpenMP (2)	2		
OpenMP (3)	2		
Cryptography and Cryptanalysis concepts	2		
Cryptography and Cryptanalysis concepts	2		

Cryptography and Cryptanalysis concepts	2		
Cryptography and Cryptanalysis concepts	2		
Cryptography and Cryptanalysis concepts	2		
Cryptography and Cryptanalysis concepts	2		
Cryptography and Cryptanalysis concepts	2		
Bibliography			
1. Peter Pacheco, An Introduction to Parallel Programming, Morgan Kaufmann, 2011.			
2. Barbara Chapman, Gabriele Jost and Ruud van der Pas, Using OpenMP - Portable Shared Memory Parallel Programming, MIT Press, 2007 (online).			
3. I. Foster, Designing and Building Parallel Programs, Addison Wesley, 1995 (online).			
4. L. Sterling, E. Shapiro, The Art of Prolog, MIT Press, 1994.			
<b>8.2 Applications – Seminars/Laboratory/Project</b>	Hours	Teaching methods	Notes
Imperative Programming in C – review, Solving highly parallelizable problems	2	Practical laboratory works / programming exercises using specific software tools	
Logic Programming in Prolog – review, Solving highly parallelizable problems	2		
Processes (C/UNIX)	2		
Threads (C)	2		
Threads (Java, C#)	2		
Threads (Prolog)	2		
Programming in OpenMP	2		
Programming in OpenMP	2		
Programming in OpenMP	2		
Cryptographic Algorithms	2		
Cryptographic Algorithms	2		
Cryptographic Algorithms	2		
Cryptographic Algorithms	2		
Final Evaluation	2		
Bibliography			
1. Peter Pacheco, An Introduction to Parallel Programming, Morgan Kaufmann, 2011.			
2. Barbara Chapman, Gabriele Jost and Ruud van der Pas, Using OpenMP - Portable Shared Memory Parallel Programming, MIT Press, 2007 (online).			
3. I. Foster, Designing and Building Parallel Programs, Addison Wesley, 1995 (online).			
4. L. Sterling, E. Shapiro, The Art of Prolog, MIT Press, 1994.			

*\*Se vor preciza, după caz: tematica seminariilor, lucrările de laborator, tematica și etapele proiectului.*

### 9. Bridging course contents with the expectations of the representatives of the community, professional associations and employers in the field

The content of the course is aligned to the latest developments in the field and responds to both the development in the multicore / other parallel hardware technologies and the requirements coming from the industry.

### 10. Evaluation

Activity type	Assessment criteria	Assessment methods	Weight in the final grade
Course	Knowledge assimilated from the course material, interactivity during lectures. Ability to solve domain specific problems	Written and/or online exam using online platforms (E)	50%
Seminar	Ability to solve domain specific problems	Written test and/or Seminar homeworks sent/ received (S)	20%

Laboratory	Ability to solve problem using parallel programming techniques and technologies	Written test and/or Laboratory homeworks sent/received (L)	30%
Project	-	-	-
Minimal performance requirements: $E \geq 50\%$ ; $L \geq 50\%$ Final Grade: $N = 0.5 * E + 0.2 * S + 0.3 * L$			

Date of filling in:	Teachers	Title First name Last name	Signature
10.06.2024	Course	Prof. dr. eng. Alin Suci	
	Applications	Prof. dr. eng. Alin Suci	

Date of approval in the department 20.02.2024	Head of department, Prof.dr.eng. Rodica Potolea
Date of approval in the Faculty Council 22.02.2024	Dean, Prof.dr.eng. Mihaela Dinşoreanu