COURSE DESCRIPTION

1. Program Information

1.1 University	**Alexandru Ioan Cuza University of Iaşi**
1.2 Faculty	**Faculty of Computer Science**
1.3 Department	**Computer Science**
1.4 Study Domain	**Computer Science**
1.5 Study Cycle	**Bachelor**
1.6 Study Program / Qualification	Computer Science / Bachelor degree

2. Course Information

2.1 Course Name			**Algebraic Foundations of Computer Science**				
2.2 Course Teacher			**Prof.Dr. Tiplea Ferucio Laurentiu**				
2.3 Seminary Teacher			**Prof.Dr. Tiplea Ferucio Laurentiu**				
2.4 Study Year	**III**	**2.5** Semester	**1**	**2.6** Evaluation	**M**	**2.7** Course Status*	**OB**

* *OB – Compulsory / OP – Optional*

3. **Total estimated hours** (hours per semester and didactic activities)

3.1 Hours per week		in which: **3.2** course		**3.3** seminary/laboratory	**2**
3.4 Hours in curriculum		in which: **3.5** course		**3.6** seminary/laboratory	**28**

Time Distribution	hours
Manual study, Course support, Bibliography, and others	**14**
Supplementary Documentation in library, in electronic forums, and on the field	**14**
Seminaries/laboratories preparation, homeworks, reports, portfolios and essays	**28**
Tutoring	**-**
Evaluation	**4**
Other activities (consultations per student)	**-**

3.7 Total hours individual study	**56**
3.8 Total hours per semester	**114**
3.9 Credits	**5**

4. **Preconditions** (if necessary)

4.1 Of Curriculum	**-**
4.2 Of Skills	**-**

5. **Conditions** (if necessary)

5.1 For Course Operation	Attenting the course is recommended
5.2 For Seminary/Laboratory Operation	Attending the seminary / laboratory is mandatory

6. Specific Skills Acquired

Professional Skills	**C1.** Exposition of fundamental concepts on algebra in computer science **C2.** Capability to use the scientific information in practice
Transversional Skills	**CT1.** Streamlining the activities carried out in an organized environment, under the academic rules of rigorous and creative work **CT2.** Optimal utilization of informational sources and communication resources in the field **CT3.** Expression of a responsible attitude towards understanding the role of algebra in computer science **CT4.** Efficient exploitation of the aquired scientific potential in the field of algebra for computer scientists

7. **Course Objectives** (from the grid of specific skills acquired)

7.1 General Objectives	This course introduces to students basic algebraic tools needed in computer science. It also emphasisez the role of theory to practice and of practice to theory. Applications are pointed out in cryptography, coding theory, semantics of programming languages etc.
7.2 Specific Objectives	When the students passes this course, they should be capable to : ▪ Make use of the corresponding algebraic tools in computer science; ▪ Undersatand at a high level all computer science fileds that need algebraic methods.

8. General Description

8.1	Course	Teaching Methods	Observations
1.	Closures	Slide- and blackboard-based presentation	2

2.	Computational introduction to number theory (I)	Slide- and blackboard-based presentation	2
3.	Computational introduction to number theory (II)	Slide- and blackboard-based presentation	2
4.	Computational introduction to number theory (III)	Slide- and blackboard-based presentation	2
5.	Applications to cryptography (I)	Slide- and blackboard-based presentation	2
6.	Semigroups and monoids	Slide- and blackboard-based presentation	2
7.	Applications to variable length codes and data compression	Slide- and blackboard-based presentation	2
8.	Groups	Slide- and blackboard-based presentation	2
9.	Application to cryptography (II)	Slide- and blackboard-based presentation	2
10.	Rings and fields	Slide- and blackboard-based presentation	2
11.	Application to cryptography (III)	Slide- and blackboard-based presentation	2
12.	Vectorial spaces	Slide- and blackboard-based presentation	2
13.	Applications to error detection and correction codes	Slide- and blackboard-based presentation	2
14.	Partially ordered sets	Slide- and blackboard-based presentation	2

Bibliography

Main References:

- M. Bishop: Introduction to Computer Security, Addison-Wesley, 2005
- W. Stallings: Cryptography and Network Security: Principles and Practices, Pearson Education, 3rd Edition, 2003
- Specific technical documentation such as RFCs
- A.J. Menezes, P.C. van Oorschot, S.A. Vanstone. Handbook of Applied Cryptography, CRC Press, third printing, 1997

Supplementary References:

- F.L. Tiplea. Algebraic Foundations of Computer Science (in Romanian), Ed. Polirom, 2006

8.2	**Seminary / Laboratory**	**Teaching methods**	**Observations** (hours and bibliographic references)
1.	Closures	Exercises in class and implementations	2

2.	Computational introduction to number theory (I)	Computational introduction to number theory (I)	Computational introduction to number theory (I)
3.	Computational introduction to number theory (II)	Computational introduction to number theory (II)	Computational introduction to number theory (II)
4.	Computational introduction to number theory (III)	Computational introduction to number theory (III)	Computational introduction to number theory (III)
5.	Applications to cryptography (I)	Applications to cryptography (I)	Applications to cryptography (I)
6.	Semigroups and monoids	Semigroups and monoids	Semigroups and monoids
7.	Applications to variable length codes and data compression	Applications to variable length codes and data compression	Applications to variable length codes and data compression
8.	Groups	Groups	Groups
9.	Application to cryptography (II)	Application to cryptography (II)	Application to cryptography (II)
10.	Rings and fields	Rings and fields	Rings and fields
11.	Application to cryptography (III)	Application to cryptography (III)	Application to cryptography (III)
12.	Vectorial spaces	Vectorial spaces	Vectorial spaces
13.	Applications to error detection and correction codes	Applications to error detection and correction codes	Applications to error detection and correction codes
14.	Partially ordered sets	Partially ordered sets	Partially ordered sets

Bibliography

- M. Bishop: Introduction to Computer Security, Addison-Wesley, 2005
- W. Stallings: Cryptography and Network Security: Principles and Practices, Pearson Education, 3rd Edition, 2003
- Specific technical documentation such as RFCs
- A.J. Menezes, P.C. van Oorschot, S.A. Vanstone. Handbook of Applied Cryptography, CRC Press, third printing, 1997

9. Course content synchronization with the expectations of the community representatives, professional associations and employers from the program domain

Algebraic foundations of computer science is a fundamental course required in all computer science departments around the world.

10. Evaluation

Activity Type	**Activity Type**	**Activity Type**	**Activity Type**
10.4 Course	Knowledge of basic concepte in information security	Written test	50%
10.5 Seminary/ Laboratory	Ability to use the knowledge acquired during the course	On going evaluation based on the skills proved in class	50%
10.6 Minimal performance standards			
The minimum grade five is required both at the written test and at the seminary/laboratory evaluation.			

Date	Course Teacher	Seminary/Laboratory Teacher
March 1, 2018	Prof.Dr. Tiplea Ferucio Laurentiu	Prof.Dr. Tiplea Ferucio laurentiu

Department Date of Approval Director of the Department