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			**Information Security**				
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 information security **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 information security in computer science **CT4.** Efficient exploitation of the aquired scientific potential in the field of information security

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

7.1 General Objectives	This course introduces to students a very important field in computer science, namely information security. It also emphasisez the role of theory to practice and of practice to theory. Cryptography is an essential tool to information security but by no means the only component. This is what the course also points out.
7.2 Specific Objectives	When the students passes this course, they should be capable to : ▪ Make use of the corresponding cryptographic tools in information security; ▪ Undersatand at a high level the security of information systems.

8. General Description

8.1	Course	Teaching Methods	Observations
1.	Introduction to access control	Slide- and blackboard-based presentation	2

2.	Access control: discretionary models	Slide- and blackboard-based presentation	2
3.	Access control: mandatory models	Slide- and blackboard-based presentation	2
4.	Role-based access control	Slide- and blackboard-based presentation	2
5.	Cryptography (part I)	Slide- and blackboard-based presentation	2
6.	Cryptography (part II)	Slide- and blackboard-based presentation	2
7.	Key management (part I)	Slide- and blackboard-based presentation	2
8.	Key management (part II)	Slide- and blackboard-based presentation	2
9.	Security extensions for DNS (DNSsec)	Slide- and blackboard-based presentation	2
10.	Security extension for IP (part I)	Slide- and blackboard-based presentation	2
11.	Security extensions for IP (part II)	Slide- and blackboard-based presentation	2
12.	SSL&TLS	Slide- and blackboard-based presentation	2
13.	S/MIME and PGP	Slide- and blackboard-based presentation	2
14.	Security in cloud era	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.	Introduction to access control	Exercises in class and implementations	2

2.	Access control: discretionary models	Exercises in class and implementations	2
3.	Access control: mandatory models	Exercises in class and implementations	2
4.	Role-based access control	Exercises in class and implementations	2
5.	Cryptography (part I)	Exercises in class and implementations	2
6.	Cryptography (part II)	Exercises in class and implementations	2
7.	Key management (part I)	Exercises in class and implementations	2
8.	Key management (part II)	Exercises in class and implementations	2
9.	Security extensions for DNS (DNSsec)	Exercises in class and implementations	2
10.	Security extension for IP (part I)	Exercises in class and implementations	2
11.	Security extensions for IP (part II)	Exercises in class and implementations	2
12.	SSL&TLS	Exercises in class and implementations	2
13.	S/MIME and PGP	Exercises in class and implementations	2
14.	Security in cloud era	Exercises in class and implementations	2

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

The course is corellated with the current requirments in major companies such as Amazon and Continental
(for instance, Amazon is interested in security of searchable encryptions, while Continental is interested in automitive security).

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