



COURSE DESCRIPTION

1. Program Information

1.1 University	Alexandru Ioan Cuza University of Iași
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	Introduction to Cryptography						
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*	OP

* 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	Attending 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 cryptography 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 cryptography in approaching information security CT4. Efficient exploitation of the acquired scientific potential in the field of cryptography

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 cryptography. It also emphasizes 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 pass this course, they should be capable to : <ul style="list-style-type: none">▪ Make use of the corresponding cryptographic tools in information security;▪ Understand at a high level the security of information systems.

8. General Description

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



2.	Perfect secrecy (I)	Slide- and blackboard-based presentation	2
3.	Perfect secrecy (II)	Slide- and blackboard-based presentation	2
4.	Symmetric cryptography (I)	Slide- and blackboard-based presentation	2
5.	Symmetric cryptography (II)	Slide- and blackboard-based presentation	2
6.	Symmetric cryptography (III)	Slide- and blackboard-based presentation	2
7.	Public-key cryptography (I)	Slide- and blackboard-based presentation	2
8.	Public-key cryptography (II)	Slide- and blackboard-based presentation	2
9.	Public-key cryptography (III)	Slide- and blackboard-based presentation	2
10.	Hash functions and MACs (I)	Slide- and blackboard-based presentation	2
11.	Hash functions and MACs (II)	Slide- and blackboard-based presentation	2
12.	Digital signatures (I)	Slide- and blackboard-based presentation	2
13.	Digital signatures (II)	Slide- and blackboard-based presentation	2
14.	Secret sharing	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 cryptography	Exercises in class and implementations	2



2.	Perfect secrecy (I)	Exercises in class and implementations	2
3.	Perfect secrecy (II)	Exercises in class and implementations	2
4.	Symmetric cryptography (I)	Exercises in class and implementations	2
5.	Symmetric cryptography (II)	Exercises in class and implementations	2
6.	Symmetric cryptography (III)	Exercises in class and implementations	2
7.	Public-key cryptography (I)	Exercises in class and implementations	2
8.	Public-key cryptography (II)	Exercises in class and implementations	2
9.	Public-key cryptography (III)	Exercises in class and implementations	2
10.	Hash functions and MACs (I)	Exercises in class and implementations	2
11.	Hash functions and MACs (II)	Exercises in class and implementations	2
12.	Digital signatures (I)	Exercises in class and implementations	2
13.	Digital signatures (II)	Exercises in class and implementations	2
14.	Secret sharing	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 correlated with the current requirements in major companies such as Amazon and Continental
(for instance, Amazon is interested in security of searchable encryptions, while Continental is interested in automotive security).



10. Evaluation

Activity Type	Activity Type	Activity Type	Activity Type
10.4 Course	Knowledge of basic concepts 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
March 1, 2018

Course Teacher
Prof.Dr. Tiplea Ferucio Laurentiu

Seminary/Laboratory Teacher
Prof.Dr. Tiplea Ferucio laurentiu

Department Date of Approval

Director of the Department