SCHOOL	School of Sciences		
ACADEMIC UNIT	Department of Computer Science		
LEVEL OF STUDIES	Undergraduate		
COURSE CODE	607SKOE	**SEMESTER**	6th
COURSE TITLE	CRYPTOGRAPHY		

INDEPENDENT TEACHING ACTIVITIES *if credits are awarded for separate components of the course, e.g. lectures, laboratory exercises, etc. If the credits are awarded for the whole of the course, give the weekly teaching hours and the total credits*	**WEEKLY TEACHING HOURS**	**CREDITS**
Lectures	2	5
Tutorial Exercises	1	
Add rows if necessary. The organisation of teaching and the teaching methods used are described in detail at (d).		

COURSE TYPE *general background, special background, specialised general knowledge, skills development*	Specialized General Knowledge, Skills Development
PREREQUISITE COURSES:	-
LANGUAGE OF INSTRUCTION and EXAMINATIONS:	Greek, English(for erasmus students)
IS THE COURSE OFFERED TO ERASMUS STUDENTS	Yes
COURSE WEBSITE (URL)	

LEARNING OUTCOMES

Learning outcomes

The course learning outcomes, specific knowledge, skills and competences of an appropriate level, which the students will acquire with the successful completion of the course are described.

Consult Appendix A

- *Description of the level of learning outcomes for each qualifications cycle, according to the Qualifications Framework of the European Higher Education Area*
- *Descriptors for Levels 6, 7 & 8 of the European Qualifications Framework for Lifelong Learning and Appendix B*
- *Guidelines for writing Learning Outcomes*

This course addresses introductory concepts and applied cryptography issues for the needs of protecting information. In addition to the necessary conceptual foundation regarding information security, issues of cryptography and algorithms used to encrypt data are analyzed, as well as additional mechanisms aimed at ensuring data integrity.
The course also covers the topics of message and entity authentication and public key infrastructures.

Upon successful completion of the course, the student will be able to:
• Explain the differences between different types of algorithms.
• Analyze the proper use of encryption algorithms
• Analyze ways to protect data integrity and authenticate data and entities.
• Design basic authentication protocols

General Competences

Taking into consideration the general competences that the degree-holder must acquire (as these appear in the Diploma Supplement and appear below), at which of the following does the course aim?

Search for, analysis and synthesis of data and information, with the use of the necessary technology *Adapting to new situations* *Decision-making* *Working independently* *Team work* *Working in an international environment* *Working in an interdisciplinary environment* *Production of new research ideas*	*Project planning and management* *Respect for difference and multiculturalism* *Respect for the natural environment* *Showing social, professional and ethical responsibility and sensitivity to gender issues* *Criticism and self-criticism* *Production of free, creative and inductive thinking* *……* *Others…* *…….*
Search for, analysis and synthesis of data and information, with the use of the necessary technology Working independently Team work	

SYLLABUS

1. Conceptual foundation – basic principles of information security
2. Cryptography – symmetric algorithms
3. Public key cryptography
4. Hash functions
5. Digital signatures
6. Digital certificates and public key infrastructures
7. Data integrity, message authentication
8. Entity authentication – methods and protocols
9. Case studies

TEACHING and LEARNING METHODS - EVALUATION

DELIVERY *Face-to-face, Distance learning, etc.*	Face-to-face
USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGY *Use of ICT in teaching, laboratory education, communication with students*	Learning process support through the moodle online platform (interaction, assignments, auxiliary material) Use of software for illustrating cryptographic and cryptanalytic concepts for exercises (Cryptool) Announcements via central department website Use email to communicate.
TEACHING METHODS *The manner and methods of teaching are described in detail.* *Lectures, seminars, laboratory practice, fieldwork, study and analysis of bibliography, tutorials, placements, clinical practice, art workshop, interactive teaching, educational visits, project, essay writing, artistic creativity, etc.* *The student's study hours for each learning activity are given as well as the hours of non-directed study according to the principles of the ECTS*	
STUDENT PERFORMANCE EVALUATION *Description of the evaluation procedure* *Language of evaluation, methods of evaluation, summative or conclusive, multiple choice questionnaires, short-answer questions, open-ended questions, problem solving, written work, essay/report, oral examination, public*	Final Grade = 100% of Final Exam Grade

Activity	***Semester workload***
Lectures	26x2=52
Tutorial Exercises	13x2=26
Written exams	2x1=2
Independent Study	30
Exercises	15
Course total	***150***

presentation, laboratory work, clinical examination of patient, art interpretation, other *Specifically-defined evaluation criteria are given, and if and where they are accessible to students.*	

ATTACHED BIBLIOGRAPHY

- Suggested bibliography:
- Related academic journals:

- Security of Computer Networks, S. Gritzalis, D. Gritzalis, S. Katsikas, Papasotiriou Publications, 2003, ISBN: 978-960-7530-45-4
- Fundamentals of Network Security: Applications and Standards, W. Stallings, Key Editions, 3rd Edition, 2008, ISBN: 978-960-461-117-1
- Cryptography and Network Security: Principles and Practice, W. Stallings, 2010, Prentice Hall, ISBN-10: 0136097049
- Security of Information Systems, S. Katsikas, D. Gritzalis, S. Gritzalis (Scientific Editor), 2004, ISBN: 9608105579
- Handbook of Applied Cryptography, A. Menezes, P. V. Oorschot, S. Vanstone, 2001, CRC Press, ISBN-10: 0849385237
- Practical security issues of information systems and applications, N. Polemi, New Technologies Publications, 2008, ISBN: 9606759156
- Computer Security, D. Gollmann, J. Wiley & Sons, 1999