Data Protection and Cryptography

COURSE OUTLINE

(1) GENERAL

SCHOOL	Science and Technology		
ACADEMIC UNIT	Science and Technology		
PROGRAMME OF STUDIES	Msc in Cybersecurity		
LEVEL OF STUDIES	Postgraduate		
COURSE CODE	CC04	SEMESTER	2
COURSE TITLE	Data Protection and Cryptography		
COURSE TYPE *Elective, compulsory*	Compulsory / Core		
INSTRUCTOR(S)	Theory: Prof. Stavros Stavrinides Lab: Prof. Stavros Stavrinides		

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
	30h/13w=2.31	6
Add rows if necessary. The organisation of teaching and the teaching methods used are described in detail at (d).		

TEACHING ACTIVITIES BREAKDOWN	WEEKLY HOURS
Theory	2.00
Recitation	0.31
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*	Special background Skills development
PREREQUISITE COURSES:	-
LANGUAGE OF INSTRUCTION and EXAMINATIONS:	English
IS THE COURSE OFFERED TO ERASMUS STUDENTS	Yes
COURSE WEBSITE (URL)	https://www.ihu.gr/ucips/postgraduate-programmes/cybersecurity

(2) 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*

On completing the course students will be able to:

- Develop the knowledge, understanding and skills to work as a computing security professional.
- Learn the concepts, principles, techniques and methodologies you need to design and assess complex networks, systems and applications, from the point of view of security.

- Develop the practical experience you need to plan, perform and evaluate data protection and cryptography processes.

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

- Search for, analysis and synthesis of data and information, with the use of the necessary technology
- Decision Making
- Teamwork
- Production of free, creative, and inductive thinking

(3) SYLLABUS

The course introduces fundamental concepts and tools of Cryptography, ending to presenting special topics in Cryptography. The topics covered include:

- Introduction.
- Modular arithmetics.
- Symmetric Cryptography.
- Asymmetric Cryptography.
- Public Key Cryptography.
- Digital Signatures.
- Hash Functions.
- Chaotic and Quantum Cryptography

(4) TEACHING and LEARNING METHODS - EVALUATION

DELIVERY *Face-to-face, Distance learning, etc.*	Hybrid: Face to face and synchronous distance learning
USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGY *Use of ICT in teaching, laboratory education, communication with students*	**Use of ICT in Teaching** During the educational process, various machine learning and programming tools are used, along with the material available at the e-learning platform. The hybrid teaching method involves synchronous learning with the support of the videoconferencing tool Zoom. Students are taught a variety of tools related to the course content and material. **Use of ICT in Communication with students** • The course material (slides, scientific articles, exercises, etc.) is posted on the course page at the e-learn platform (Moodle). • Use of Moodle Forums announcements. • Live video meetings via Zoom/Teams. • Contact via email.

TEACHING METHODS

The manner and methods of teaching are described in detail.
Lectures, recitation, 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

Activity	*Semester workload*
Lectures	30 hrs.
Recitation	9 hrs.
Project	8 hrs.
Exams	2 hrs.
Non-Directed Study	86 hrs.
Course total	***135 hrs.***

COURSE MATERIAL ARRANGEMENT

Theory/Recitation

Theoretical and practical modern cryptography principles.	1 hr.
Data protection techniques and methodologies.	5 hrs.
Encryption techniques (symmetric and asymmetric keys, public and secret key encryption, digital signatures etc.).	4 hrs.

Lab

Threat and vulnerability assessment.	3 hrs.

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 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

Language of Evaluation: English

Evaluation Procedure:

- Written Exams (70%). Methods of evaluation:
  - Multiple choice questions
- Group project (30%):
  - Build an IoT application (hardware-software)

The evaluation procedure is announced to the students during the first lecture.

STUDENT OBLIGATIONS

Compulsory attendance of lectures, labs, recitations, compulsory participation in midterms, exams, compulsory delivery of homework, projects, etc.

- Compulsory attendance of lectures
- Compulsory attendance of labs
- Compulsory participation in the exams
- Compulsory delivery of project

(5) ATTACHED BIBLIOGRAPHY

- *Suggested Textbooks*

1. Understanding Cryptography: A Textbook for Students and Practitioners, Christof Paar, Jan Pelzl, Springer.
2. Contemporary cryptography, Oppliger Rolf, Artech House.

- *Additional Bibliography:*

1. Real-World Cryptography, David Wong, Manning Publications.