# COURSE OUTLINE

## (1) GENERAL

| | | | |
|---|---|---|---|
| **SCHOOL** | SCIENCE | | |
| **ACADEMIC UNIT** | DEPARTMENT OF MATHEMATICS | | |
| **LEVEL OF STUDIES** | POSTGRADUATE | | |
| **COURSE CODE** | **B9** | **SEMESTER** | |
| **COURSE TITLE** | Foundations and Applications in Modern 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** |
|---|---|---|
| | 3 | 10 |
| | | |
| | | |
| *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* | SPECIALISED GENERAL KNOWLEDGE |
| **PREREQUISITE COURSES:** | NO |
| **LANGUAGE OF INSTRUCTION and EXAMINATIONS:** | Greek/English |
| **IS THE COURSE OFFERED TO ERASMUS STUDENTS** | YES |
| **COURSE WEBSITE (URL)** | http://www.math.aegean.gr/index.php/el/academics-el/postgraduate-programs-el |

## (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*

To successfully consolidate the concepts and techniques presented in the course contents (see (3) below).

**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…*
*…….*

Working Independently, Working in an international environment, Working in an interdisciplinary environment.

## (3) SYLLABUS

Classical and modern computational models (classical TMs, evolutionary TMs and quantum computational models). Algorithms and cryptography. Fast solvable problems and the complexity class P, computationally difficult problems and the complexity class NP, NP-complete problems.

Security Assessment Models. Definition of Encryption and Cryptanalysis. Hash Functions.

Basic Principles of Designing Shared Key Cryptographic Schemes. Cryptographic product. Block cryptalgorithm. Principles of diffusion and confusion. Classes of symmetric cryptalgorithms,

- Substitution Permutation Networks (SPN), AES (Advanced Encryption Standard).
- Feistel networks. Feistel Network Security, DES (Data Encryption Standard).

Design of Substitution Boxes (SBoxes). Interconnection modes of shared key cryptographic algorithms. Triple Encryption and the meet-in-the-middle attack. Key Schedule Algorithms. Linear and Differential Cryptanalysis.

Public key cryptography schemes. The Diffie-Hellman concept, the RSA public key cryptographic scheme. ElGamal Cryptographic Systems in Zp*. ElGamal cryptographic systems on elliptic curves.

Digital signatures (Digital Signature Algorithm, blind digital signatures). Zero knowledge proofs. Cryptocurrencies. Post-Quantum cryptography.

## (4) TEACHING and LEARNING METHODS - EVALUATION

| | |
|---|---|
| **DELIVERY**<br>*Face-to-face, Distance learning, etc.* | Face-to-face |
| **USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGY**<br>*Use of ICT in teaching, laboratory education, communication with students* | • Use of ICT in teaching (slides and interactive whiteboard).<br>• Communication with students via e-mail.<br>• Uploading course material on moodle system. |
| **TEACHING METHODS**<br>*The manner and methods of teaching are described in detail.*<br>*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.*<br><br>*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 | 39 |
| Independent study | 148,5 |
| Working Out Assignments | 62,5 |
| | |
| | |
| | |
| | |
| | |
| | |
| Course total (25 hours per credit unit) | ***250*** |

| | |
|---|---|
| **STUDENT PERFORMANCE EVALUATION**<br>*Description of the evaluation procedure*<br><br>*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* | Student evaluation is done in Greek through a written examination which includes short-answer equations and problem solving.<br><br>For students with disabilities, evaluation takes place via oral exams. |

| | |
|---|---|
| *examination of patient, art interpretation, other*<br><br>*Specifically-defined evaluation criteria are given, and if and where they are accessible to students.* | |

## (5) ATTACHED BIBLIOGRAPHY

*- Suggested bibliography:*


1. Handbook of Applied Cryptography, Alfred Menezes, Paul Oorschot, Scot Vanstone.
2. Cryptography and Network Security, Principles and Practices, William Stallings Prentice Hall.
3. Introduction to the theory of computation, Michael Sipser, Cengage Learning.
4. Understanding Bitcoin, Cryptography, Engineering and Economics, Pedro Franco, Wiley.
5. Quantum Computing, Mik Hirvensalo, Springer.


*- Related academic journals:*