COURSE OUTLINE

(1) GENERAL

<table>
<thead>
<tr>
<th>SCHOOL</th>
<th>ENGINEERING</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACADEMIC UNIT</td>
<td>DEPT. OF COMPUTER ENGINEERING AND INFORMATICS</td>
</tr>
<tr>
<td>LEVEL OF STUDIES</td>
<td>UNDERGRADUATE</td>
</tr>
<tr>
<td>COURSE CODE</td>
<td>CEID_NE4168</td>
</tr>
<tr>
<td>SEMESTER</td>
<td>8\textsuperscript{th} - 10\textsuperscript{th}</td>
</tr>
<tr>
<td>COURSE TITLE</td>
<td>CRYPTOGRAPHY</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Lectures, Recitation sections, Laboratory exercises</th>
<th>WEEKLY TEACHING HOURS</th>
<th>CREDITS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2, 2, 1</td>
<td>5</td>
</tr>
</tbody>
</table>

**TOTAL** 5

**COURSE TYPE**

Specialised general knowledge

**PREREQUISITE COURSES:**

There are no prerequisite courses. It is recommended that students have knowledge of Introduction to Algorithms (CEID_NY205)

**LANGUAGE OF INSTRUCTION and EXAMINATIONS:**

Greek

**IS THE COURSE OFFERED TO ERASMUS STUDENTS**

Yes

**COURSE WEBSITE (URL)**

https://eclass.upatras.gr/courses/CEID1143/

(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

With the successful completion of this course, students will:

1. Be familiar with fundamental notions of number theory.
2. Have understood key classes of cryptographic protocols.
3. Be familiar with fundamental public key cryptographic protocols.
4. Be familiar with digital signatures, zero knowledge proofs, interactive protocols, message authentication codes, modification detection codes, hash functions.
5. Be able to compare and distinguish between public key and private key cryptographic 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
- 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...
Production of new research ideas

- Search for, analysis and synthesis of data and information, with the use of the necessary technology
- Decision-making
- Working independently
- Production of new research ideas
- Criticism and self-criticism
- Production of free, creative and inductive thinking

(3) SYLLABUS

- Cryptographic protocols
- Sender receiver interaction
- Key management
- AES, DES, Block Ciphers
- Pseudorandom number generation
- Public key cryptography
- Digital signatures - Authentication
- Legal aspects

(4) TEACHING and LEARNING METHODS - EVALUATION

<table>
<thead>
<tr>
<th>DELIVERY</th>
<th>Face-to-face, Distance learning, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGY</td>
<td>Use of ICT in teaching, laboratory education, communication with students</td>
</tr>
<tr>
<td>TEACHING METHODS</td>
<td>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.</td>
</tr>
<tr>
<td>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</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Activity</th>
<th>Semester Workload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lectures</td>
<td>26</td>
</tr>
<tr>
<td>Recitation sections</td>
<td>26</td>
</tr>
<tr>
<td>Laboratory exercises</td>
<td>13</td>
</tr>
<tr>
<td>Independent study</td>
<td>39</td>
</tr>
<tr>
<td>Study and analysis of bibliography</td>
<td>26</td>
</tr>
<tr>
<td>Course total (25-30 hours per credit)</td>
<td>130</td>
</tr>
</tbody>
</table>

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.

The evaluation is in the form of a written examination and is in Greek, while Erasmus students are evaluated in English.

(5) ATTACHED BIBLIOGRAPHY

- Suggested bibliography: