## SYLLABUS
### COURSE DESCRIPTION

<table>
<thead>
<tr>
<th>COURSE TITLE</th>
<th>Information Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>COURSE CODE</td>
<td>75041</td>
</tr>
<tr>
<td>SCIENTIFIC SECTOR</td>
<td>ING-INF/05</td>
</tr>
<tr>
<td>DEGREE</td>
<td>Bachelor in Computer Science and Engineering</td>
</tr>
<tr>
<td>SEMESTER</td>
<td>2nd semester</td>
</tr>
<tr>
<td>YEAR</td>
<td>3rd year</td>
</tr>
<tr>
<td>CREDITS</td>
<td>8</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TOTAL LECTURING HOURS</th>
<th>48</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOTAL LAB HOURS</td>
<td>24</td>
</tr>
</tbody>
</table>

**PREREQUISITES**

Students should have a solid mathematical foundation and be familiar with basic programming concepts, data structures and algorithms. These prerequisites are covered in any Bachelor degree in Computer Science.

**COURSE PAGE**

https://ole.unibz.it/

**SPECIFIC EDUCATIONAL OBJECTIVES**

- Type of course: “caratterizzante” for L-31 and L-8
- Scientific area: “discipline informatiche” for L-31 and “fingegneria informatica” for L-8

The main aim of this exam is to provide an introduction to the field of information security. The students learn about the technical as well as the management side of security in information systems. They acquire knowledge about fundamental principles of security and also about practical approaches to securing information systems.

**LECTURER**

Sven Helmer,
http://www.inf.unibz.it/~shelmer/

**SCIENTIFIC SECTOR OF THE LECTURER**

ING-INF/05

**TEACHING LANGUAGE**

English

**OFFICE HOURS**

POS 2.16, shelmer@inf.unibz.it, 0471 016190

**TEACHING ASSISTANT**

Paolo Bolzoni

**OFFICE HOURS**

Tuesday, 14:30, POS 2.11, Faculty of Computer Science, Piazza Domenicani 3

**LIST OF TOPICS COVERED**

- Basic definitions (CIA, threat, attack, vulnerability, control)
- Risk assessment
- Basic of Cryptography
## Cryptographic Protocols
- Network Attack and Defense
- Usability
- Social Engineering
- Security Policies

### TEACHING FORMAT
Frontal classroom lecture plus lab sessions

### LEARNING OUTCOMES

**Knowledge and understanding:**
- know critical security aspects of information systems, the basic concepts of security and techniques for the development of secure systems;

**Applying knowledge and understanding:**
- be able to evaluate the quality of information systems and to identify critical aspects
- be able to apply the own knowledge in different working contexts;

**Making judgments**
- Must have the ability to independently select the documentation required to keep abreast of the frequent technological innovations in the field by using a wide variety of documentary sources: books, web, magazines.

**Communication skills**
- Must be able to coordinate the work of a project team and to interact positively with members of the group.

**Learning skills**
- Must also be able to independently keep up to date with developments in the most important areas of Computer Science

### ASSESSMENT
- Project work to test knowledge application skills and communication skills, done in small groups who present their work orally
- Written exam with verification questions and questions to test knowledge application skills

### ASSESSMENT LANGUAGE
English

### EVALUATION CRITERIA AND CRITERIA FOR AWARDING MARKS
- 20% project work
- 80% written examples

relevant for assessment 1: ability to work in teams, skill in applying knowledge in a practical setting, ability to summarize in own words

relevant for assessment 2: clarity of answers, ability to recall principles and methods used in system security, skill in applying knowledge such as testing the security of systems

### REQUIRED READINGS
also available online:
<table>
<thead>
<tr>
<th><strong>SUPPLEMENTARY READINGS</strong></th>
<th>Schneier: Applied Cryptography, John Wiley &amp; Sons, 2015</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SOFTWARE USED</strong></td>
<td></td>
</tr>
</tbody>
</table>

http://www.cl.cam.ac.uk/~rja14/book.html