| | | | | |
|---|---|---|---|---|
| 1. | Course title | Cryptography | | |
| 2. | Course code | | | |
| 3. | Study program | | | |
| 4. | Unit offering the course | **FCSE** | | |
| 5. | Undergraduate/postgraduate/PhD | **Undergraduate** | | |
| 6. | Year/semester<br>3/Winter/Elective | 7. ECTS: **6** | | |
| 8. | Teacher(s) | Acad. Prof. Ljupcho Kocarev,<br>Assist. Prof. Vesna Dimitrova | | |
| 9. | Course prerequisites | Discrete Mathematics 2 | | |
| 10. | Goals (competences):<br>Introduction to basic cryptographic principles and methods; Teaching basic crypto design; Practical use of learned cryptographic algorithms. | | | |
| 11. | Course content:<br>Classic versus modern cryptography. Perfectly-secret encryption. Computer Security. Symmetric key encryption. Authentication messages and hash functions. Block ciphers. Theoretical constructs. Number theory. Revolution of public keys. Key exchange. Public key encryption. Digital signatures. Efficient cryptographic schemes. Elements of number theory; Cryptographic protocols; Cryptographic algorithms, Pseudo-random numbers generators, Stream ciphers, Public key algorithms, Applications. Mostly used secure communication protocols: SSL, DES, 3-DES, RSA, Twofish, ... | | | |
| 12. | Teaching methods: Lectures, trainings, individual work, project, seminar work. | | | |
| 13. | Total available time | 6 ECTS x 30 hours = 180 hours | | |
| 14. | Distribution of the available time | 30+45+25+40+40 = 180 hours | | |
| 15. | Teaching activities | 15.1. | Lectures | 30 hours |
| | | 15.2. | Training (labs, problem solving), seminar and team work | 45 hours |
| 16. | Other activities | 16.1. | Project work | 25 hours |
| | | 16.2. | Self study | 40 hours |
| | | 16.3. | Home work | 40 hours |
| 17. | Grading | | | |
| | | 17.1. | Tests | 80 points |
| | | 17.2. | Seminar work/project (written or oral presentation) | 10 points |
| | | 17.3. | Active participation | 10 points |
| 18. | Grading criteria | to 50 points | | 5 (five) (F) |
| | | from 51 to 60 points | | 6 (six) (E) |
| | | from 61 to 70 points | | 7 (seven) (D) |
| | | from 71 to 80 points | | 8 (eight) (C) |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | from 81 to 90 points | | | 9 (nine) (B) | |
| | | from 91 to 100 points | | | 10 (ten) (A) | |
| 19. | Final exam prerequisites | Successful completion of activities 15 and 16 | | | | |
| 20. | Course language | Macedonian and English | | | | |
| 21. | Quality assurance methods | Internal evaluation mechanisms supported by student polls | | | | |
| 22. | Literature | | | | | |
| | 22.1. | Compulsory | | | | |
| | | No. | Authors | Title | Publisher | Year |
| | | 1. | C. Paar, J. Pelzl | Understanding Cryptography: A Textbook for Students and Practitioners | Springer | 2010 |
| | | 2. | N. Smart | Cryptography:<br>An introduction | McGraw-Hill | 2003 |
| | | 3. | J. Katz, Y. Lindell | Introduction to Modern Cryptography | Chapman<br>& Hall/CRC Press | 2007 |
| | 22.2. | Mandatory | | | | |
| | | No. | Authors | Title | Publisher | Year |
| | | 1. | Mark Stamp | Information security – principles and practice | John Willey and Sons | 1991 |
| | | 2. | | | | |
| | | 3. | | | | |