|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **UNIVERSITY OF NIŠ** | | | | | | |
| **Course Unit Descriptor** | | **Faculty** | | | **Faculty of Sciences and Mathematics** | |
| **GENERAL INFORMATION** | | | | | | |
| Study program | | | | Computer Science | | |
| Study Module (if applicable) | | | | Information management, Software development | | |
| Course title | | | | Cryptographic Algorithms | | |
| Level of study | | | | Bachelor  Master’s  Doctoral | | |
| Type of course | | | | Obligatory  Elective | | |
| Semester | | | | Autumn Spring | | |
| Year of study | | | | first | | |
| Number of ECTS allocated | | | | 7.00 | | |
| Name of lecturer/lecturers | | | | Jelena Ignjatović | | |
| Teaching mode | | | | Lectures Group tutorials  Individual tutorials  Laboratory work  Project work  Seminar  Distance learning  Blended learning  Other | | |
| **PURPOSE AND OVERVIEW (max. 5 sentences)** | | | | | | |
| The main purpose of the subject is to introduce the basic principles of security of information, the basic techniques and algorithms which were using during the history and those that are used in cryptographic practice. At the end of the course a student would master basic abstract data structures, criteria for their implementation and basic algorithms for working with these structures, as well as to acquire the ability to independently and creatively solve complex problems using the acquired knowledge and known algorithms. | | | | | | |
| **SYLLABUS (brief outline and summary of topics, max. 10 sentences)** | | | | | | |
| **Introduction to cryptography** - history and applications;  **Basic cryptographic objectives and resources** - security levels, practical aspects of security;  **Basic concepts of cryptology** – security channel, encryption schemes, Vernam's code number (one-time pad);  **Mathematical foundations of cryptography** - the number theory, one-way and one-way trapdoor functions, hash functions; **Cryptosystems with a secret (symmetric) key** - substitution and transposition ciphers, permutation ciphers, compositional ciphers, flowing ciphers;  **Cryptanalysis of the mentioned systems**;  **Block ciphers** - DES, Triple DES, AES;  **Public-key cryptosystems** - RSA cryptosystem , ElGamal's cryptosystem, cryptanalysis, authentication, key distribution, digital signatures;  **Electronic money** | | | | | | |
| **LANGUAGE OF INSTRUCTION** | | | | | | |
| Serbian (complete course)  English (complete course)  Other \_\_\_\_\_\_\_\_\_\_\_\_\_ (complete course)  Serbian with English mentoring Serbian with other mentoring \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | | |
| **ASSESSMENT METHODS AND CRITERIA** | | | | | | |
| **Pre exam duties** | **Points** | | **Final exam** | | | **Points** |
| **Activity during lectures** | **5** | | **Written examination** | | | **--** |
| **Practical teaching** | **10** | | **Oral examination** | | | **45** |
| **Teaching colloquia** | **40 (2x20)** | | **OVERALL SUM** | | | **100** |
| **\*Final examination mark is formed in accordance with the Institutional documents** | | | | | | |