|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **UNIVERSITY OF NIŠ** | | | | | | |
| **Course Unit Descriptor** | | **Faculty** | | | Faculty of Electronic Engineering | |
| **GENERAL INFORMATION** | | | | | | |
| Study program | | | | Electrical Engineering and Computing | | |
| Study Module (if applicable) | | | | Computing and Informatics | | |
| Course title | | | | Information Security | | |
| Level of study | | | | X Bachelor ☐ Master’s ☐ Doctoral | | |
| Type of course | | | | Obligatory X Elective | | |
| Semester | | | | X Autumn ☐Spring | | |
| Year of study | | | | 4 | | |
| Number of ECTS allocated | | | | 6 | | |
| Name of lecturer/lecturers | | | | Prof. dr Vučković V. Vladan | | |
| Teaching mode | | | | X Lectures ☐Group tutorials ☐ Individual tutorials  XLaboratory work X Project work ☐ Seminar  ☐Distance learning ☐ Blended learning ☐ Other | | |
| **PURPOSE AND OVERVIEW (max. 5 sentences)** | | | | | | |
| Elements of cryptology, cryptography and cryptanalysis. Authorized access. Identification methods. System development with authorized access. Symmetric cryptography. Public and secret key. Hash functions. Method of attack on the protected system. Certificates, maintenance and certification. Basic security protocols. Types of malware. | | | | | | |
| **SYLLABUS (brief outline and summary of topics, max. 10 sentences)** | | | | | | |
| Seminar papers. Historical overview of the field and the simplest implementation of the algorithm coding. General analysis coders, data flows, and implementation of algorithms A5, A5 / 1 and RC-4. Feistel coder. Implementation of the encoder data blocks DES, TDES, AES, TEA. Encoder modes. Asymmetric encryption, RSA algorithm implementation and Knapsack. Calculating the CRC value. Tiger hash. Analysis and implementation of the MD and SHA family of cryptographic hash function. Methods for cryptanalysis. | | | | | | |
| **LANGUAGE OF INSTRUCTION** | | | | | | |
| XSerbian (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** |  | | **Written examination** | | | **10** |
| **Practical teaching** | **20** | | **Oral examination** | | | **40** |
| **Teaching colloquia** | **30** | | **OVERALL SUM** | | | **100** |
| **\*Final examination mark is formed in accordance with the Institutional documents** | | | | | | |