|  |
| --- |
|  **UNIVERSITY OF NIŠ** |
| **Course Unit Descriptor** | **Faculty** | Faculty of Electronic Engineering |
| **GENERAL INFORMATION** |
| Study program  | Computing and Informatics |
| Study Module (if applicable) | Computer Systems Security |
| Course title | Cryptography |
| Level of study |  Bachelor X Master’s ☐ Doctoral |
| Type of course | X Obligatory☐ Elective |
| Semester  | ☐ Autumn XSpring |
| Year of study  | I |
| Number of ECTS allocated | 4 |
| Name of lecturer/lecturers | Prof. dr Predrag Rančić, Prof. dr Vučković V. Vladan |
| Teaching mode | X Lectures ☐Group tutorials ☐ Individual tutorials☐Laboratory work x Project work ☐ Seminar☐Distance learning ☐ Blended learning ☐ Other |
| **PURPOSE AND OVERVIEW (max. 5 sentences)** |
| Introduction to the field of cryptography in terms of basic principles, algorithms and standards. Students will gain knowledge on basic principles, algorithms, and standards used in the field of cryptography. They will also learn how to apply that knowlegde in real-world applications. |
| **SYLLABUS (brief outline and summary of topics, max. 10 sentences)** |
| History and overview of cryptography. Mathematical background. Basic symmetric-key encryption. Stream ciphers. Block ciphers. DES – The Data Encryption Standard. AES – The Advanced Encryption Standard. Asymmetric cryptography using public-private key pair. Hash Functions and Data Integrity. Digital signature schemes. RSA signatures. The "Hash-and-Sign" Paradigm. Certificates and Public-Key Infrastructures. Secure Socket Layer (SSL) and Transport Layer Security (TLS) standards. |
| **LANGUAGE OF INSTRUCTION** |
| xSerbian (complete course) ☐ English (complete course) ☐ Other \_\_\_\_\_\_\_\_\_\_\_\_\_ (complete course)xxSerbian with English mentoring ☐Serbian with other mentoring \_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **ASSESSMENT METHODS AND CRITERIA** |
| **Pre exam duties** | **Points** | **Final exam** | **points** |
| **Activity during lectures** | **10** | **Written examination** |  |
| **Practical teaching** | **30** | **Oral examination** | **30** |
| **Teaching colloquia** | **30** | **OVERALL SUM** | **100** |
| **\*Final examination mark is formed in accordance with the Institutional documents** |