Course Unit Descriptor

Study Programme: Information Technology in e-Government and Business Systems
Course Unit Title: Data and Computer Networks Security
Course Unit Code: DAS212
Name of Lecturer(s): Associate Professor Dalibor Dobrilović, PhD
Type and Level of Studies: Master Academic Degree
Course Status (compulsory/elective): Elective
Semester (winter/summer): Winter
Language of instruction: English
Mode of course unit delivery (face-to-face/distance learning): Face-to-face
Number of ECTS Allocated: 4
Prerequisites: None
Course Aims: The main goal of the course is to teach students the concepts of data and computer networks security and protection, cryptography, network security protocols, and security technologies. In addition to teaching the theoretical aspects of data and network security, the practical work and the application of the same technologies are included as well.
Learning Outcomes: Upon successful completion of the course, it is expected that the students will master the concepts of data and computer networks protection and security as well as the basis of cryptography and security protocols. In addition, students will gain practical knowledge about detection, prevention, and neutralization of cyber attacks on data and computer networks security.
Syllabus: *Theory* Basic cryptography concepts, keys, and encryption algorithms. Hush functions, digital signature, digital certificate. Public Key Infrastructure (PKI). Network protection tools and applications. e-mail security (PGP, S/MIME), Transport Layer (SSL, TLS), and IP security (IPSec). Network firewalls. Web security. VPNs. WLAN security. Types of attacks: passive and active. Malicious programs and denial of services. Security of Cloud computer systems. *Practice* Practical work covers laboratory exercises with solving tasks and practical problems with the application of simulation software for computer networks and network devices.
Required Reading: 1. W. Stallings, Cryptography and Network Security - Principles and Practice, 4th edition Prentice Hall 2007. 2. W. Stallings, L. Brown, Computer Security: Principles and Practice Prentice Hall, 2012.

Weekly Contact Hours: 4	**Lectures:** 2	**Practical work:** 2

Teaching Methods: Lectures and students group work
Knowledge Assessment (maximum of 100 points): 100

Pre-exam obligations	points	**Final exam**	points
Active class participation	10	written exam	30

Practical exam(s)	10	oral exam	30
Seminar(s)	20		