Study programme(s): Applied Mathematics (MAP)

Course title: DATA PROTECTION (P603)

Lecturer(s): Ivana Vojnović

Course status: compulsory on module: Data Analytics and Statistics

ECTS points: 5

Requirements:

Learning Objectives

The aim of the course is to introduce students to mathematical as well as practical, systematic, data protection and database protection methods.

Learning Outcomes

The student is familiar with the importance of both basic mathematical and systematic methods, as well as practical systems, for data protection. In this way, with additional learning of regulations and similar aspects (for example, GDPR) a student is able to take data protection into account when developing applications and algorithms for data analytics.

Syllabus

Theoretical instructions

Various principles and methods for improving data privacy and secrecy: aggregation, anonymization, authentication, authorization, the basics of cryptography: symmetrical encryption, message integrity, public key encryption.

Practical instructions

Learn about examples of practical systems and data protection platforms and how they work.

Literature

1. J. Katz and Y. Lindell, **Introduction to Modern Cryptography - Principles and Protocols**, Taylor and Francis, 2008.
2. Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno, **Cryptography Engineering: Design Principles and Practical Applications**, John Wiley & Sons, 2010.
3. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, **Handbook of applied cryptography,** CRC Press, 1996.

Number of active classes	**Lectures: 2**	**Exercises: 2**

Teaching methods

Lectures; repetition; active participation of students in problem solving. Knowledge tests, homework. Demonstrate the functionality of real data protection systems.

Grading (maximum number of points 100)

Pre-exam obligations	Points	**Final exam**	Points
Homework, mini project	**30**	Final exam	**70**