COURSE DESCRIPTION CARD - SYLLABUS

Course name
Cryptography fundamentals [S2TIIZM1E>PK]

Course

Field of study
Information Technology for Smart and Sustainable Mobility

Year/Semester
1/1

Area of study (specialization)
–

Profile of study
general academic

Level of study
second-cycle

Course offered in
English

Form of study
full-time

Requirements
compulsory

Number of hours

Lecture
32

Laboratory classes
16

Other
0

Tutorials
0

Projects/seminars
0

Number of credit points

4,00

Coordinators

dr inż. Anna Grocholewska-Czuryło
anna.grocholewska-czurylo@put.poznan.pl

Lecturers

Prerequisites

Knowledge: Basic Discrete Mathematics - including sets, functions, logic, and elementary proof techniques. Elementary Number Theory - especially concepts like divisibility, prime numbers, greatest common divisors, and modular arithmetic. Foundations of Computer Science - such as algorithms, complexity, and basic data structures. Skills: Problem-solving - especially in algorithmic and mathematical contexts. Basic programming - to implement and test cryptographic algorithms (e.g., in Python, C++, or Java). Analytical Thinking - ability to approach complex problems methodically.

Course objective

Leveraging on the symmetric and asymmetric cryptographic algorithms this module will provide the main protocols and techniques implemented on existing and future networks. Last but not least, one course has been allocated for addressing network security management.

Course-related learning outcomes

Knowledge:
The student has knowledge of development trends and the most significant recent achievements in the

field of cryptography
The student has advanced and detailed knowledge of the processes occurring in existing and future networks
The student demonstrates knowledge of advanced methods, techniques, and tools in particular symmetric and asymmetric cryptographic algorithms, as well as the main protocols and techniques used in existing and future networks

Skills:
The student is able to use information and communication technologies in the field of cryptography, including the application of block and stream ciphers, groups, rings, and finite fields, as well as the AES and RSA algorithms and the Diffie-Hellman protocol
The student is able to plan and conduct experiments, including measurements and computer simulations, interpret the obtained results, draw conclusions, and formulate and verify hypotheses related to complex and simple research problems in the field of cryptography
The student is able to assess the suitability of methods and tools used to solve an engineering task involving the application of cryptography, including recognizing the limitations of these methods and tools

Social competences:
The student understands the importance of using the latest knowledge in cryptography to solve research and practical problems

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Written exam
Practical work - solving problems

Programme content

Modern cryptography, AES and RSA algorithms, Elliptic Curve Cryptography, Modular arithmetic, Hash functions, Quantum cryptography

Course topics

Introduction to modern cryptography principles
Block and stream ciphers
Groups, rings and finite fields.
The AES algorithm
Introduction to number theory: Modular arithmetics. Fermat’s and Euler’s Theorems. Discrete logarithms.
The Diffie-Hellman protocol
The RSA Algorithm
Elliptic Curve Cryptography
Hash functions: SHA standard
Introduction to quantum cryptography

Teaching methods

The course is conducted remotely (online) in a synchronous format. Classes may also be held in person. Multimodal presentation. Practical examples, case study.

Bibliography

Basic:
Stallings, W. (2020), Cryptography and Network Security: Principles and Practices, 8th Edition, Pearson.

Additional:
-

Breakdown of average student's workload

	Hours	ECTS
Total workload	100	4,00
Classes requiring direct contact with the teacher	48	2,00
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	52	2,00