COURSE DESCRIPTION CARD - SYLLABUS

Course name
Cryptography in edge systems [S2Inf1-PB>KRYPT]

Course

Field of study
Computing

Year/Semester
1/2

Area of study (specialization)
Edge Computing

Profile of study
general academic

Level of study
second-cycle

Course offered in
Polish

Form of study
full-time

Requirements
compulsory

Number of hours

Lecture
30

Laboratory classes
30

Other
0

Tutorials
0

Projects/seminars
0

Number of credit points

5,00

Coordinators

dr inż. Michał Melosik
michal.melosik@put.poznan.pl

Lecturers

Prerequisites

Student should have basic knowledge of signal processing basics, fundamentals of programming and design and analysis of digital and analogue circuits. Student should have the ability to search for necessary information in the indicated sources. Student should be able to draw conclusions and form an opinion about the presented solutions. Additionally, the student should understand the necessity of broadening their competence and should be ready to cooperate within a team. Moreover, in terms of social competence, a student should demonstrate such attitudes as honesty, responsibility, perseverance, cognitive curiosity, creativity, personal culture, respect for other people.

Course objective

1. Acquaint students with the basic issues of cryptography and security in relation to edge technologies and computer engineering. 2. Provide students with basic knowledge of the structure of selected cryptographic solutions. 3. To develop skills of creating and adapting selected cryptographic modules in edge systems. 4.To train students to select optimal solutions for security of edge systems. 5. Develop in students the ability to work in a team by realizing task elements and combining them into a whole.

Course-related learning outcomes

Knowledge:
the student has advanced and detailed knowledge in the field of design of information systems, boundary systems, electronic systems; he has advanced and detailed knowledge of processes from the border of information technology and electronics occurring in the life cycle of boundary systems security; he knows advanced methods and techniques used in design and security systems; he has computer science advances in solving research problems on improving hardware and software security of edge systems.

Skills:
the student is able to interdisciplinaryy combine selected problems of electronics, physics, statistics with the knowledge from different areas of computer science; can evaluate the usefulness of new methods in designing security features for boundary systems and use the newest methods for their testing; can recognize the limitations of methods and tools used in designing cryptographic systems in the context of hardware and software security; can, using new methods, solve complex problems of detecting threats in hardware and software data security.

Social competences:
the student understands that in computer science, and in particular in the design of edge systems,

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Learning outcomes presented above are verified as follows:
Formulation evaluation:
- In terms of lectures: on the basis of responses to questions on the material discussed in previous lectures,
- for laboratories / exercises: on the basis of the assessment of the current progress of the tasks and the final evaluation of the project,
Summative assessment:
- in terms of lectures the verification of the assumed learning outcomes is realized by conducting a written or oral exam
- as for projects/laboratories, verification of the assumed effects of education is realized by the assessment of the progress of the realization of the task, continuous assessment, rewarding the growth of skills to use the known principles and methods, assessment of the level of progress in performing tasks. The assessment of the prepared documentation/report of the tasks performed.
Obtaining additional points for activity during classes, especially for:
- discussion of additional aspects of the issue,
- the effectiveness of applying the knowledge gained in solving the problem,
- The ability to cooperate within a team practically implementing a detailed task in the laboratory,
- comments on the improvement of teaching materials.

Programme content

The course will discuss classical cryptography issues relating to the specifics of edge processing systems implemented in a hardware or software/hardware manner.

Course topics

1. Introduction to cryptography.
2.Mathematical basis of cryptography.
3. Randomness and random number generators on the example of TRBG, PRBG, CSPRBG and their applications in hardware security of embedded systems and computer engineering.
4. Selected cryptographic algorithms (symmetric and asymmetric), AES, RSA, alg. hash, EDSA, elliptic curves.
5. Key exchange protocols and cryptographic protocols.
6. Cryptographic standards.
7. Practical aspects of cryptography and social engineering in attacks on security systems.
8. Types of attacks in cryptography.
9. Selected issues of security architecture of micro-information systems.
10. Certificates in cryptography.

11. Hardware security including RoT, Chain of Trust, Secure boot, PUF, hardware Trojans, Threat Detecton Technologie, PUF.
12. Design and supply chain security .
13. Security, and ethical and legal issues.
Laboratory classes include assignments on topics currently discussed in lecture.

Teaching methods

Lecture: multimedia presentation, traditional lecture, additional audio-video material, technical specifications, scientific articles.
Laboratory classes: realization of tasks according to the guidelines, team or independent work, problem discussion.

Bibliography

Basic
1. A. Chrzęszczyk, Algorytmy teorii liczb i kryptografii w przykładach, wyd. BTC, 2010
2. M. Karbowski, Podstawy kryptografii., wyd. Helion, 2006
3. A. J. Menezs, Kryptografia stosowana, wyd. WNT, 2005
4. C. Parr, Understanding Cryptography: A Textbook for Students and Practitioners, Springer, 2010
Additional
1. M. Melosik, W. Marszalek, "Using the 0-1 test for chaos to detect hardware trojans in chaotic bit generators", Electronics Letters 52 (11), 919-921
2. M. Melosik, P. Sniatala, W. Marszalek, "Hardware Trojans detection in chaos-based cryptography", Bulletin of the Polish Academy of Sciences Technical Sciences, 65 (5), 725-732 2017

Breakdown of average student's workload

	Hours	ECTS
Total workload	125	5,00
Classes requiring direct contact with the teacher	60	2,50
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	65	2,50