COURSE DESCRIPTION CARD - SYLLABUS

Course name
Artificial Intelligence in Cryptography [S2SI1E>SIK]

Course

Field of study
Artificial Intelligence

Year/Semester
1/2

Area of study (specialization)
–

Profile of study
general academic

Level of study
second-cycle

Course offered in
English

Form of study
full-time

Requirements
elective

Number of hours

Lecture
15

Laboratory classes
15

Other
0

Tutorials
0

Projects/seminars
0

Number of credit points

3,00

Coordinators

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

Lecturers

Prerequisites

A student beginning this course should have knowledge of basic algorithms and their analysis, neural networks, evolutionary computing, operating systems, computer networks and cryptographic algorithms. He/she should be able to use programming environments and platforms to write, execute and test programs. Should be able to construct algorithms and analyze their complexity. Should have the ability to obtain information from indicated sources and be willing to work collaboratively as part of a team.

Course objective

To provide students with knowledge of advanced principles of cryptographic algorithms and to teach their design. To indicate the area where AI could be usedusing , to teach methods of analysis and evaluation of selected cryptographic systems.

Course-related learning outcomes

Knowledge The student has detailed knowledge of:
- what criteria a secure information system should meet and what protection measures should be used to achieve this,
- has structured and theoretically grounded general knowledge connected with the key issues of

cryptographic mechanisms of data protection (symmetric and asymmetric ciphers, hash functions, digital signatures), elliptic curves, authentication protocols, key management algorithms and secret sharing,
- has advanced detailed knowledge of selected topics in cipher components design and evaluation,
- has knowledge about development trends and the most important new achievements in artificial intelligence in cryptography
Skills The student will be able to:
- analyze and design selected cipher components that meet specific criteria
- design and implement selected cryptographic algorithms
- design and implement a system using appropriate cryptographic methods to ensure confidentiality, integrity and authentication of the data stored and processed in it, analyze the performance of the implemented system
- analyze and evaluate the security level of applied cryptographic mechanisms and estimate whether the system is vulnerable to known cryptographic attacks
- propose, design and implement alternative cryptographic mechanisms ensuring higher security level.
Social competences The student understands that:
- an important aspect is the use of appropriate, up-to-date cryptographic and artificial intelligence methods,
- the proper implementation of cryptographic algorithms is equally important,
- it is necessary to update knowledge on secure parameters of used algorithms, protocols and tools.

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Knowledge acquired during lectures is verified during the one-hour written test consisting of 3 questions. Pass mark: more than 50% of the points. Credit issues, on the basis of which questions are developed, are available within the eKursy system.
Skills acquired during the laboratory classes are verified on an ongoing basis during the classes (by checking the completed task or laboratory exercise)

Programme content

Course Content:
1. Symmetric vs Asymmetric Ciphers
2. Chaos Theory and Pseudorandom Sequence Generators
3. Hash Functions
4. Application of Neural Networks in Cryptography
5. Application of Evolutionary Algorithms in Cryptography
6. Application Areas of Artificial Intelligence in Cryptography, Trends, and Challenges

Course topics

Lecture topics
1. Symmetric vs asymmetric ciphers
2. Chaos theory and pseudorandom sequence generators, extended sequence randomness tests.
3. Shortcut functions - design of shortcut functions, classification of functions by structure, criteria that good shortcut functions must satisfy, MAC, attacks on shortcut functions, applications, Sponge structure - on the example of Keccak function.
4. Neural network in cryptography
5. Evolutionary computations in cryptography
6. Artificial Intelligence application areas in cryptography, trends and challenges.
Laboratory
1 Analysis of the most important component of block ciphers and the criteria it must satisfy. Implementation of methods to analyze S-blocks: balancedness, avalanche property and nonlinearity.
2. Implementation of random sequence generator based on selected algorithm from chaos theory, and tests to check the randomness of the generated sequence.
3. Implementation of the algorithm for secret sharing or cryptographic material management
4. Implementation of a selected cryptographic system in teams.

Teaching methods

The lecture is conducted in an interactive manner (with the formulation of questions to students) using multimedia presentations. Materials are made available to students in electronic version.

Laboratory exercises - presentation of the problem / exercise to be performed on the blackboard (with the basic level of difficulty and extended for those willing) and the implementation of the exercise in the laboratory, using the programming language chosen by the student.

Bibliography

Basic Pieprzyk J., Hardjono T., Seberry J., Teoria bezpieczeństwa systemów komputerowych, Helion 2003 (sygnatura w bibliotece PP: W 110215).
Additional Menezes A. i inni, Kryptografia stosowana, WNT, 2005, (sygnatura w bibliotece PP: W 112188)
Materials provided by the instructor, updated annually.

Breakdown of average student's workload

	Hours	ECTS
Total workload	75	3,00
Classes requiring direct contact with the teacher	30	1,50
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	45	1,50