COURSE DESCRIPTION CARD - SYLLABUS

Course name
Cryptography fundamentals [S1Inf1>KRYP]

Course

Field of study
Computing

Year/Semester
3/6

Area of study (specialization)
–

Profile of study
general academic

Level of study
first-cycle

Course offered in
polish

Form of study
full-time

Requirements
elective

Number of hours

Lecture
24

Laboratory classes
20

Other (e.g. online)
0

Tutorials
0

Projects/seminars
0

Number of credit points

2,00

Coordinators

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

Lecturers

Prerequisites

Student starting this subject should have the knowledge of basic algorithms including their analysis, operating systems and computer networks. The student should be able to manage programming environments and platforms for applications" writing, executing and testing. Student should be able to design algorithms and perform an analysis of their complexity.

Course objective

The objective of this course is to teach students the cryptographic methods of data security in computer systems. Students should gain the ability to use these methods in practice.

Course-related learning outcomes

Knowledge:
Student has a detailed knowledge about:
- what criteria should be met by a secure IT system and what protection measures should be applied to achieve it,
- cryptographic data protection mechanisms (ciphers, hash functions, digital signatures, elliptic curves, blockchains),

- authentication protocols, key management, secret sharing, protocols ensuring network security and e-mail security.

Skills:
Student is able to:
- design and implement systems with the use of appropriate cryptographic methods in order to ensure privacy and integrity as well as authentication of stored and analyzed data sets in these systems,
- analyze and estimate the level of security of cryptographic mechanisms and evaluate whether a certain system is immune to known cryptographic attacks,
- propose, design and implement alternative cryptographic mechanisms to ensure a higher level of security.

Social competences:
The student understands:
- how important it is to implement adequate data security methods,
- that an implementation of appropriate cryptographic algorithms is equally important,
- the necessity of updating knowledge on security parameters, algorithms, protocols and tools used.

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Learning outcomes presented above are verified as follows:
The knowledge obtained during the lectures is verified by the means of a hour-long written exam, consisting of 8 question. Passing threshold: over 50% of points. Topics, which are the basis for final exam questions, are sent to students by e-mail at the beginning of the semester.
The knowledge obtained during lab practicals is verified during the practicals (checking the preformed exercises) and by one half-hour-long test after 8 lab practicals, which will cover the knowledge necessary to perform and understand previous practical exercises.

Programme content

Lecture:
1. Introduction - the definition of information system security, necessary cryteria for such system, measures needed in order to maintain the security (physical, technical, organisational and legal), security policy, introduction of different cryptographic systems, the Kerckhoffs principle, types of cryptoanalytical attacks.
2. Bock ciphers - substitution, permutation, Shannon"s substitution-permutation networks, DES, AES algorithms - basic components, block ciphers modules, stream ciphers, pseudo-random sequence generators (congruential, RSA, BBS, LFSR, NLFSR) and random sequences tests.
3. Hush function - classification of functions based on contruction, cryteria for a good hush function, MAC, hush function attacks, implementation, Sponge structure - based on Keccak function.
4. Asymetric cryptography - mathematical basics, RSA, DH, EI-Gamal"s, Rabin"s and Knapsack algorithms, procotocls that use RSA algorithm - zero-proof knowledge, blind digital signatures, multiparty computation - millioners issue.
5. Digital signature and PKI (Public Key Infrastructure), LDAP and OCSP protocol.
6. Authentication methods - PAP, CHAP, EAP protocol, protocols that use introduced cryptographic mechanisms - symmetric, asymmetric and hush funcion, overview of current authentication methods (procedural, passwordless, through social media,…).
7. Secret sharing methods - Shamir"s algorythm, its modification with the indentification of the cheater, visual cryptography, steganography.
8. Eliptic curve in cryptography - ECRSA, ECDH, ECDSA.
9. Cryptoanalysis - methods of cryptoanalysis block, stream, asymmetric and hush function ciphers.
10. Blockchain technology - structure, security, examples.
Lab practicals
1. Implementatin of a basic cypher that uses substitution or permutation and perofming cryptoanalysis of cyphers implemented by oher student.
2. Implementation of random BBS sequence generator and 4 basic tests that check the randomness of previously generated sequences.
3. implementation of a chosen block cipher mode, using basic ECB mode, verification of error propagation in various modes.

4. Implemntation of RSA algorithm.
5. implementation of DH algorithm.
6. Performing analysis of the speed of various hush functions, analysis of criteria of a good hash function.
7. Implementation of a steganographic method of embedding information on LSB.
8. Implementation of Shamir"s secret division method.
9. Implementation of visual cryptography secret division method.

Teaching methods

The lectures are interactive (questions are addressed to students) with the use of multimedia presentations. The digital version of the contents of the presentations are provided to students.
Lab practicals - presentations regaring the problem/exercises to be performed on the board (within the basic level of difficulty and also with higher difficulty for volunteers) and performing an individual exercise in a programming language of choice.

Bibliography

Basic
Stokłosa J. (red.), Ochrona danych i zabezpieczenia w systemach teleinformatycznych, Wydawnictwo Politechniki Poznańskiej, Poznań, 2005 (reference number in PP library: W 104521).
Pieprzyk J., Hardjono T., Seberry J., Teoria bezpieczeństwa systemów komputerowych, Helion 2003 (reference number in PP library: W 110215).
Additional
Menezes A. i inni, Kryptografia stosowana, WNT, 2005, (reference number in PP library: W 112188)
Materials shared by the lecturer, updated every year.

Breakdown of average student's workload

	Hours	ECTS
Total workload	60	2,00
Classes requiring direct contact with the teacher	46	1,50
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	14	0,50