COURSE DESCRIPTION CARD - SYLLABUS

Course name
Fundamentals of cryptography [S1EiT1>PK]

Course

Field of study
Electronics and Telecommunications

Year/Semester
4/7

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
30

Laboratory classes
0

Other
0

Tutorials
15

Projects/seminars
0

Number of credit points

3,00

Coordinators

dr hab. inż. Mieczysław Jessa prof. PP
mieczyslaw.jessa@put.poznan.pl

Lecturers

Prerequisites

Students know the fundamentals of algebra, probability theory, computer network operation, and 2G, 3G, 4G mobile networks. Is able to extract information from Polish or English language literature, databases and other sources, is able to synthesize gathered information, draw conclusions, and justify opinions.

Course objective

The presentation of fundamentals of cryptography. To create skills necessary to evaluate the quality of data protection, when the data are transmitted, collected or stored in computer or communication networks.

Course-related learning outcomes

Knowledge:
1. He knows basic cryptographic methods of data protection for data transmitted, collected or stored in computer or communication networks.
2. He knows basic ideas concerning communication and computer networks and understands the meaning of these ideas.

Skills:

1. Is able to combine and integrate information coming from various sources and interpret them. Is able to draw conclusions and to motivate his/her opinions.

Social competences:
1. Knows limitations of his/her knowledge, understands the necessity of further self-studying.
2. Is aware of the necessity to approach solving technical problems with responsibility and professionalism, knows physical and social threats that can appear as the result of irresponsible usage of communication 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:
Learning outcomes are verified with a written test. Test consists of 5 open questions. Answers are scored equally. Minimum number of scores to pass the exam is equal to 50%. Questions are chosen individually and randomly from a set of questions prepared by the lecturer. The set of predefined subjects is sent to students by email.
Knowledge and skills gathered during tutorials are assessed by written test. Test consists of 5 open questions. Answers are scored equally. Minimum number of scores to pass the exam is equal to 50%. The assessment levels are the following: under 3 - mark 2.0, from 3 to 3.25 - mark 3.0; from 3.26 to 3.75 - mark 3.5; from 3.76 to 4.25 - mark 4.0; from 4.26 to 4.75 - mark 4.5; above 4.75 - mark 5.0.

Programme content

During the course students learn about basic ideas of cryptography. They are: confidentiality, data, system integrity, authentication, authorization, nonrepudiation, availability, one-way function, one-way trap-door function, cryptographic system (symmetric, asymmetric, secret-key system, public-key system), unconditional security, computational security, provable security, Kerckhoffs" desiderata, random numbers, secure pseudorandom numbers, hash function, electronic and digital signature, certificate. Students learns about mathematical foundations of cryptography, congruences, Euclidean algorithm, inversion of a number in residue arithmetic, Chinese remainder theorem (CRT), solutions of equations in residue arithmetic, power of a number in residue arithmetic, square roots in residue arithmetic. They are presented basic constructions and methods of usage (ECB, CBC, CFB., OFB, CTR) of block ciphers, stream ciphers, limitations of block and stream ciphers, chosen methods of encryption with secret-key systems (e.g., monoalphabetic ciphers, polyalphabetic ciphers, transposition ciphers, Vigenère cipher, Playfair ciphers, Enigma, DES, IDEA, AES), chosen methods of encryption with public-key systems (Diffie-Hellman, RSA, ElGamal, Rabin). Students learn about hash function and its properties, birthday paradox, examples of hash functions (MD5, SHA-1, SHA-2, SHA-3), digital signature methods, methods of authentication (password, PIN, challenge-response protocols, cryptographic control sum, MAC, digital signature). The course ends with examples of practical usage of cryptography in life (GSM, UMTS, 4G, SSL/TLS, SSH). The goal of tutorials is to develop skills necessary to solve basic cryptographic problems with mathematical tools. During the tutorials students solve different problems with the use of residue arithmetic, Euclidean algorithm, Fermat's theorem, Euler's theorem, Gauss' theorem, extended Euclidean algorithm, methods square-and multiply.

Course topics

none

Teaching methods

Lecture: Multimedia presentation with elements of project method.
Tutorials: A combination of exercise and project method.

Bibliography

Basic
1. A. J. Menezes, P. C. van Oorschot, S. A. Vanstone „Kryptografia stosowana", WNT, Warszawa

2005.
2. B. Schneier „Kryptografia dla praktyków”, WNT, Warszawa, 2002.
3. W. Stallings „Kryptografia i bezpieczeństwo sieci komputerowych”, Wyd. V, Helion 2012.
Additional
1. J. A. Buchmann „Wprowadzenie do kryptografii”, PWN, 2006.
2. M. Karbowski, Podstawy kryptografii, Helion, 2014.
3. M. Kutyłowski, W-B. Strothmann „Kryptografia, teoria i praktyka zabezpieczania systemów komputerowych”, Read Me, Warszawa, 1999.
4. N. Ferguson, B. Schneier „Kryptografia w praktyce”, Helion, 2004

Breakdown of average student's workload

	Hours	ECTS
Total workload	90	3,00
Classes requiring direct contact with the teacher	55	2,00
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	35	1,00