Data safety and cryptography - course description

General information

Course name	Data safety and cryptography
Course ID	11.3-WE-INFP-DSaC-Er
Faculty	Faculty of Computer Science, Electrical Engineering and Automatics
Field of study	Computer Science
Education profile	academic
Level of studies	First-cycle Erasmus programme
Beginning semester	winter term 2021/2022

Course information

Semester	5
ECTS credits to win	5
Course type	obligatory
Teaching language	english
Author of syllabus	• dr hab. inż. Remigiusz Wiśniewski, prof. UZ

Classes forms

The class form	Hours per semester (full-time)	Hours per week (full-time)	Hours per semester (part-time)	Hours per week (part-time)	Form of assignment
Lecture	15	1	-	-	Credit with grade
Laboratory	30	2	-	-	Credit with grade
Project	15	1	-	-	Credit with grade

Aim of the course

- Familiarize students with the provide basic knowledge about the fundamentals of cryptography and data safety.
- Familiarize students with the basic knowledge about applied cybersecurity (passwords, computer viruses and malware, firewalls, backups, SPAM, etc.).

Prerequisites

Principles of programming (but not obligatory).

Scope

Introduction: Fundamentals of cryptography and data safety, cryptosystems, basics of encryption and decryption, classic cryptography (transposition ciphers and substitution ciphers; Caesar cipher, Vigenère cipher, XOR, etc.). Implementation of the basic algorithms in programming languages.

Symmetric-key algorithms: Key management, block ciphers (DES, AES, Blowfish) and stream ciphers (RC4).

Optional: implementation in programming languages (C, C++, Java, Assembler, Pascal), hardware implementation (with programmable devices like FPGAs).

Asymmetric-key algorithms: Public and private keys, hash functions. Main protocols and cryptosystems (Diffie-Hellman, RSA, SHA, MD5, etc.).

Optional: Implementation in programming languages (C, C++, Assembler, Pascal). Hardware implementation (with programmable devices - FPGAs).

Digital signature: Fundamentals of digital signature, safety and authentication, smartcards.

Cryptanalysis: Main goals of cryptanalysis. Weakness of particular cryptosystems. Data safety. Debugging of computer applications and programs.

Data security and protection of applications: Fundamentals of data protection of programs and applications (based on MS Windows operation system). Processes management and debugging. Software debuggers and kernel mode debuggers.

Security in Web applications: Most popular attacks and protection methods (e.g. *Cross-site scripting XSS*, *SQL-Injection*).

Applied cybersecurity: protection of passwords, computer viruses and malware, firewalls, backups, SPAM.

Teaching methods

Lecture, laboratory exercises, project.

Learning outcomes and methods of theirs verification

Outcome description	Outcome symbols	Methods of verification	The class form
Has a basic knowledge on legal aspects of data protection		• a quiz • bieżąca kontrola na zajęciach	• Laboratory

Outcome description	Outcome symbols	Methods of verification	The class form
Has a detailed knowledge on data protection and security in computer applications and computer programs		• a project • an ongoing monitoring during classes	• Laboratory • Project
Can recognize and minimize the threats related to data security in computer applications and digital systems		• an evaluation test	• Lecture
Can apply existing cryptographic algorithms in securing computer applications		• a project • an ongoing monitoring during classes	• Laboratory • Project
Can protect transmitted data		• a discussion • an evaluation test • an observation and evaluation of activities during the classes • an ongoing monitoring during classes	• Lecture • Laboratory
Understands the need to protect information systems, is aware of the necessity to apply IT protections in daily life (access to electronic/computer data, application of electronic cards and digital signature)		• a discussion • a quiz • an evaluation test • an ongoing monitoring during classes	• Lecture • Laboratory

Assignment conditions

Lecture – the passing condition is to obtain a positive mark from the final test (or other tasks given by the teacher).

Laboratory – the passing condition is to obtain positive marks from all laboratory exercises to be planned during the semester (or other tasks given by the teacher).

Project – the passing condition is to obtain a positive mark from all projects conducted during the semester (or other tasks given by the teacher).

Final mark components: lecture 30% + laboratory 40% + project 30%.

Recommended reading

1. Stinson D.R., *Cryptography: Theory and Practice* (4th edition), CRC Press, Boca Raton, 2017.
2. Schneier B., *Applied cryptography*, John Wiley & Sons, New York, 1994.

Further reading

1. Cormen T., Leiserson C., Rivest R., Stein C., *Introduction to Algorithms* (3rd edition), MIT Press, 2016.
2. Maxfield C.: *The Design Warrior's Guide to FPGAs. Devices, Tools and Flows*, Elsevier, Amsterdam, 2004.
3. Mitnick K.: *The Art of Invisibility* (edition 2017), Little, Brown Book Group, 2017.
4. Karbowski M., *Basics of cryptography* (3rd edition), Helion, Warsaw, 3rd. ed., 2015 (in Polish).

Notes

Modified by dr hab. inż. Remigiusz Wiśniewski, prof. UZ (last modification: 16-07-2021 22:31)