Data safety and cryptography - opis przedmiotu

Informacje ogólne

Nazwa przedmiotu	Data safety and cryptography
Kod przedmiotu	11.3-WE-INFP-DSaC-Er
Wydział	Wydział Nauk Inżynieryjno-Technicznych
Kierunek	Informatyka
Profil	ogólnoakademicki
Rodzaj studiów	Program Erasmus pierwszego stopnia
Semestr rozpoczęcia	semestr zimowy 2021/2022

Informacje o przedmiocie

Semestr	5
Liczba punktów ECTS do zdobycia	5
Typ przedmiotu	obowiązkowy
Język nauczania	angielski
Sylabus opracował	• prof. dr hab. inż. Remigiusz Wiśniewski

Formy zajęć

Forma zajęć	Liczba godzin w semestrze (stacjonarne)	Liczba godzin w tygodniu (stacjonarne)	Liczba godzin w semestrze (niestacjonarne)	Liczba godzin w tygodniu (niestacjonarne)	Forma zaliczenia
Wykład	15	1	-	-	Zaliczenie na ocenę
Laboratorium	30	2	-	-	Zaliczenie na ocenę
Projekt	15	1	-	-	Zaliczenie na ocenę

Cel przedmiotu

- 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.).

Wymagania wstępne

Principles of programming (but not obligatory).

Zakres tematyczny

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.

Metody kształcenia

Lecture, laboratory exercises, project.

Efekty uczenia się i metody weryfikacji osiągania efektów uczenia się

Opis efektu	Symbole efektów	Metody weryfikacji	Forma zajęć

Opis efektu	Symbole efektów	Metody weryfikacji	Forma zajęć
Can apply existing cryptographic algorithms in securing computer applications		• bieżąca kontrola na zajęciach • projekt	• Laboratorium • Projekt
Can protect transmitted data		• bieżąca kontrola na zajęciach • dyskusja • kolokwium • obserwacja i ocena aktywności na zajęciach	• Wykład • Laboratorium
Can recognize and minimize the threats related to data security in computer applications and digital systems		• kolokwium	• Wykład
Has a basic knowledge on legal aspects of data protection		• sprawdzian • bieżąca kontrola na zajęciach	• Laboratorium
Has a detailed knowledge on data protection and security in computer applications and computer programs		• bieżąca kontrola na zajęciach • projekt	• Laboratorium • Projekt
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)		• bieżąca kontrola na zajęciach • dyskusja • kolokwium • sprawdzian	• Wykład • Laboratorium

Warunki zaliczenia

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%.

Literatura podstawowa

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.

Literatura uzupełniająca

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).

Uwagi

Zmodyfikowane przez prof. dr hab. inż. Remigiusz Wiśniewski (ostatnia modyfikacja: 16-07-2021 22:31)