

Data safety and cryptography - opis przedmiotu

Informacje ogólne

Nazwa przedmiotu	Data safety and cryptography
Kod przedmiotu	11.3-WE-INFP-DSaC-Er
Wydział	Wydział Informatyki, Elektrotechniki i Automatyki.
Kierunek	WIEiA - oferta ERASMUS / Informatyka
Profil	-
Rodzaj studiów	Program Erasmus pierwszego stopnia
Semestr rozpoczęcia	semestr zimowy 2018/2019

Informacje o przedmiocie

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

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

- To provide basic knowledge about fundamentals of cryptography and data safety.
- To provide basic knowledge about most popular Web applications attacks (e.g. XSS, SQL-Injection) and methods of security.
- To provide basic knowledge about data security and protection of applications (Windows).

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).

Metody kształcenia

Lecture, laboratory exercises, project.

Efekty uczenia się i metody weryfikacji osiągania efektów uczenia się

Opis efektu	Symbol efektów	Metody weryfikacji	Forma zajęć
-------------	-------------------	--------------------	-------------

Opis efektu	Symbol efektów	Metody weryfikacji	Forma zajęć
Has a basic knowledge on legal aspects of data protection (computer applications, digital systems, electronic cards, digital signature)		<ul style="list-style-type: none"> • bieżąca kontrola na zajęciach • dyskusja • sprawdzian 	<ul style="list-style-type: none"> • Wykład • Laboratorium
Has a basic knowledge on data protection and security in computer applications (computer programs) and Web applications		<ul style="list-style-type: none"> • bieżąca kontrola na zajęciach • dyskusja • kolokwium 	<ul style="list-style-type: none"> • Wykład • Laboratorium
Can apply existing cryptographic algorithms in securing computer software and digital systems		<ul style="list-style-type: none"> • bieżąca kontrola na zajęciach • projekt 	<ul style="list-style-type: none"> • Laboratorium • Projekt
Can recognize and minimize the threats related to data security in computer applications and digital systems		<ul style="list-style-type: none"> • bieżąca kontrola na zajęciach • dyskusja • kolokwium • obserwacja i ocena aktywności na zajęciach 	<ul style="list-style-type: none"> • Wykład • Laboratorium
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)		<ul style="list-style-type: none"> • bieżąca kontrola na zajęciach • dyskusja • kolokwium • sprawdzian 	<ul style="list-style-type: none"> • Wykład • Laboratorium
Can protect transmitted data, both, on the level of computer software and digital systems		<ul style="list-style-type: none"> • dyskusja • projekt 	<ul style="list-style-type: none"> • Laboratorium • Projekt

Warunki zaliczenia

Lecture – the passing condition is to obtain a positive mark from the final test.

Laboratory – the passing condition is to obtain positive marks from all laboratory exercises to be planned during the semester.

Project – the passing condition is to obtain a positive mark from all projects conducted during the semester.

Calculation of the final grade: lecture 30% + laboratory 40% + project 30%

Literatura podstawowa

1. Stinson D.R., *Cryptography: Theory and Practice* (3rd edition), CRC Press, Boca Raton, 2005.
2. Schneier B., *Applied cryptography*, John Wiley & Sons, New York, 1994.
3. Ferguson N., Schneier B.*Practical Cryptography*, Wiley, 2003.

Literatura uzupełniająca

1. Paar C., *Understanding Cryptography: A Textbook for Students and Practitioner*, Springer, 2010.
2. Aho A. V., Hopcroft J. E., Ullman J. D., *The Design and Analysis of Computer Algorithms*, Addison-Wesley, Reading, Massachusetts, 1974.
3. Karbowski M., *Basics of cryptography*, Helion, Warsaw, 2005 (in Polish).
4. Maxfield C.: *The Design Warrior's Guide to FPGAs. Devices, Tools and Flows*, Elsevier, Amsterdam, 2004.

Uwagi

Zmodyfikowane przez dr hab. inż. Remigiusz Wiśniewski, prof. UZ (ostatnia modyfikacja: 28-03-2018 08:56)

Wygenerowano automatycznie z systemu SylabUZ