*Załącznik nr 1 do Uchwały nr \_\_\_\_\_\_\_ - 2018/2019 z dnia 25 marca 2019 r.*

*w sprawie wytycznych dla tworzenia i zmian programów studiów pierwszego stopnia, drugiego stopnia*

*oraz jednolitych studiów magisterskich rozpoczynających się od roku akademickiego 2019/2020.*

Opis **zajęć (sylabus)**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Nazwa zajęć: | | Elementy kryptologii | | | | | | | **ECTS** | | **2** |
| Nazwa zajęć w j. angielskim: | | Foundations of cryptology | | | | | | | | | |
| Zajęcia dla kierunku studiów: | | **Informatyka** | | | | | | | | | |
|  | |  | | | | | | | | | |
| Język wykładowy: | | polski | | | | Poziom studiów: | | studia II stopnia | | | |
| Forma studiów: | 🗷 stacjonarne  🞎 niestacjonarne | Status zajęć: | 🗷 podstawowe  🞎 kierunkowe | 🗷 obowiązkowe  🞎 do wyboru | | Numer semestru: ……1….. | | 🞎 semestr zimowy 🗷 semestr letni | | | |
|  |  | Rok akademicki, od którego obowiązuje opis (rocznik): | | | | 2019/2020 | Numer katalogowy: | **ZIM-IN-2Z-01Z-05** | | | |
|  | | | | | | | | | | | |
| Koordynator zajęć: | |  | | | | | | | | | |
| Prowadzący zajęcia: | |  | | | | | | | | | |
| Jednostka realizująca: | |  | | | | | | | | | |
| Jednostka zlecająca: | |  | | | | | | | | | |
| Założenia, cele i opis zajęć: | | Celem przedmiotu jest zapoznanie studentów z teoretycznymi i praktycznymi podstawami kryptologii oraz jej zastosowań w celu uzyskanie odpowiedniego stopnia poufności, integralności danych i uwierzytelnienia podmiotów i danych w systemach informatycznych. Opis tematów poruszanych podczas zajęć:  1. Podstawowe zagadnienia kryptologii, cele, system kryptograficzny symetryczny i asymetryczny, bezpieczeństwo systemów kryptograficznych i rodzaje ataków 2. Tryby szyfrowania: blokowe ( ECB, CBC, EFB, OFB), strumieniowe 3. Systemy szyfrowania oparte na kluczu symetrycznym,   - Teoretyczne bezpieczeństwo, tajność doskonała Shanonna, szyfr Vermana,  - Blokowe szyfry afiniczne , szyfr Hilla, szyfr Viegnere’a  - Szyfr Fiestela , DES  - Szyfr AES, ciała skończone Galois’a  - metody ataku na systemy z kluczem symetrycznym, atak wyczerpujący na klucz , algorytm Hellmana   1. Systemy kryptograficzne z kluczem publicznym   - System szyfrowania oparty na problemie faktoryzacji : RSA, szyfr Rabina  - Słabości szyfru RSA . Bezpieczna wersja szyfru RSA  - Problem obliczania logarytmu dyskretnego. Bezpieczne ustanowienie klucza wspólnego ,  protokół Diffe-Hellmana, system szyfrowania ElGamala  - Wykorzystanie krzywych eliptycznych do budowy systemu kryptograficznego ElGamala,   1. Kryptograficzne funkcje skrótu, funkcje kompresująca, funkcja jednokierunkowa,   - Odporność na kolizje, podatność na atak oparty na paradoksie dnia urodzin  - Konstrukcje funkcji skrótu silnie odpornej na kolizje. Metoda Merkle, arytmetyczna funkcja kompresji - Konstrukcje praktycznych funkcji skrótu: SHA-1, SHA-2, SHA-3, MD5  - Parametryzowane funkcje skrótu MAC   1. Podpis cyfrowy: podpisy na kluczu symetrycznym, podpisy RSA, ElGamala, standardy podpisu DSA/DSS, podpisy niezaprzeczalne, schemat Chauma-van Antwerpena, podpis ślepy, protokół Chauma 2. Dystrybucja kluczy i przechowywanie kluczy,   - Kwantowa dystrybucja kluczy, protokół BB84,  - Centrum dystrybucji kluczy KDC  - Infrastruktura klucza publicznego, środowisko bezpieczeństwa osobistego, ośrodek certyfikacji, łańcuch certyfikatów, protokół Shamira podziału sekretu  - Śieć zaufania   1. Zastosowania algorytmów kryptograficznych   - Bezpieczna korespondencja, PGP,  - Uwierzytelnianie, hasła jednorazowe, protokół wiedzy zerowej, protokół Fiata-Shamira, protokoły z wykorzystaniem KDC, protokół Needhama-Schroedera, Kerberos, protokół Otwaya-Reesa, wstępna dystrybucja klucza Bloma, protokół „station-to-station”  - Bezpieczna komunikacja, IPSec, WPA2, Bluetooth, protokoły SSL i TLS  - Kryptowaluty, kryptokontrakty   1. Inne systemy ukrywania informacji | | | | | | | | | |
| Formy dydaktyczne, liczba godzin: | | wykład; liczba godzin ...30... | | | | | | | | | |
| Metody dydaktyczne: | | wykład, studium przypadku, dyskusja problemu, konsultacje | | | | | | | | | |
| Wymagania formalne  i założenia wstępne: | | Wymagana jest wiedza z zakresu: matematyki dyskretnej, algebry, rachunku prawdopodobieństwa, algorytmów, programowania. | | | | | | | | | |
| Efekty uczenia się: | | Wiedza:  1 ma pogłębioną wiedzę z matematyki w zakresie kryptologii  2 - zna zasady bezpieczeństwa systemów kryptograficznych  3 - ma podstawową wiedzę o systemach i protokołach kryptograficznych oraz zna technikę tworzenia zaawansowanych algorytmów szyfrowania | | | Umiejętności:  1 - potrafi stosować różnorodne metody zapobiegania i obrony przed atakami na systemy oparte na metodach kryptografii  2 - umie implementować algorytmy szyfrowania  3 - umie powiązać podstawy teoretyczne z praktycznymi aspektami kryptografii | | | | | Kompetencje:  ……………………..  …………………….. | |
| Sposób weryfikacji efektów uczenia się: | | Kolokwia pisemne | | | | | | | | | |
| Forma dokumentacji osiągniętych efektów uczenia się: | | Kolokwia pisemne z ocenami | | | | | | | | | |
| Elementy i wagi mające wpływ  na ocenę końcową: | | **Kolokwia pisemne – 100%** | | | | | | | | | |
| Miejsce realizacji zajęć: | | Wykład -sala audytoryjna | | | | | | | | | |
| Literatura podstawowa i uzupełniająca:  Literatura podstawowa:   * Buchmann Johanes A., *Wprowadzenie do kryptografii,* PWN, 2006. * van Tilborg Henk C.A., *Fundamentals of Cryptology* * Trappe W., Washington L.C., *Introduction to Cryptography* * Stoshi Nakamoto, *Bitcoin, A Peer-to-Peer Electronic Cash System*   Literatura uzupełniająca:   * Publikacje IETF: Internet Engineering Task Force, <https://www.ietf.org> * Publikacje NIST: National Institute of Standards and Technology, https://www.nist.gov * Tannebaum, Wetherrall *Sieci komputerowe,* Helion, wydanie V | | | | | | | | | | | |
| UWAGI  Minimalna liczba punktów konieczna do zaliczenia: 50% | | | | | | | | | | | |

Wskaźniki ilościowe charakteryzujące moduł/przedmiot:

|  |  |
| --- | --- |
| Szacunkowa sumaryczna liczba godzin pracy studenta (kontaktowych i pracy własnej) niezbędna dla osiągnięcia zakładanych dla zajęć efektów uczenia się - na tej podstawie należy wypełnić pole ECTS: | **60 h** |
| Łączna liczba punktów ECTS, którą student uzyskuje na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich lub innych osób prowadzących zajęcia: | **1,5 ECTS** |

Tabela zgodności kierunkowych efektów uczenia się z efektami przedmiotu:

|  |  |  |  |
| --- | --- | --- | --- |
| kategoria efektu | Efekty uczenia się dla zajęć: | Odniesienie do efektów dla programu studiów dla kierunku | Oddziaływanie zajęć na efekt kierunkowy\*) |
| Wiedza 1 | ma pogłębioną wiedzę z matematyki w zakresie kryptologii | K\_W01 / P7S\_WG | 1 |
| Wiedza 2 | zna zasady bezpieczeństwa systemów kryptograficznych | K\_W09 / P7S\_WG | 2 |
| Wiedza 3 | ma podstawową wiedzę o systemach i protokołach kryptograficznych oraz zna technikę tworzenia zaawansowanych algorytmów szyfrowania | K\_W10 / P7S\_WG | 2 |
| Umiejętności 1 | potrafi stosować różnorodne metody zapobiegania i obrony przed atakami na systemy oparte na metodach kryptografii | K\_U05 / P7S\_UW | 2 |
| Umiejętności 2 | umie implementować algorytmy szyfrowania | K\_U06 / P7S\_UW | 1 |
| Umiejętności 3 | umie powiązać podstawy teoretyczne z praktycznymi aspektami kryptografii | K\_U07 / P7S\_UW | 1 |
| Kompetencje - |  |  |  |
| Kompetencje - |  |  |  |

\*)

3 – zaawansowany i szczegółowy,

2 – znaczący,

1 – podstawowy,