



Karta przedmiotu

Nazwa i kod przedmiotu	Podstawy kryptografii, PG_00048249						
Kierunek studiów	Informatyka						
Data rozpoczęcia studiów	luty 2023 r.		Rok akademicki realizacji przedmiotu		2022/2023		
Poziom kształcenia	II stopnia		Grupa zajęć		Grupa zajęć fakultatywnych Grupa zajęć powiązanych z prowadzonymi badaniami naukowymi w dziedzinie nauki związanej z kierunkiem - profil ogólnoakademicki		
Forma studiów	stacjonarne		Sposób realizacji		na uczelni		
Rok studiów	1		Język wykładowy		polski		
Semestr studiów	1		Liczba punktów ECTS		2.0		
Profil kształcenia	ogólnoakademicki		Forma zaliczenia		egzamin		
Jednostka prowadząca	Wydział Elektroniki, Telekomunikacji i Informatyki -> Katedra Algorytmów i Modelowania Systemów						
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot		mgr inż. Andrzej Jastrzębski				
	Prowadzący zajęcia z przedmiotu		mgr inż. Andrzej Jastrzębski				
Formy zajęć i metody nauczania	Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
	Liczba godzin zajęć	15.0	15.0	0.0	0.0	0.0	30
	W tym liczba godzin zajęć na odległość: 0.0						
Aktywność studenta i liczba godzin pracy	Aktywność studenta	Udział w zajęciach dydaktycznych, objętych planem studiów		Udział w konsultacjach		Praca własna studenta	RAZEM
	Liczba godzin pracy studenta	30		4.0		16.0	50
Cel przedmiotu	Zapoznanie studentów z podstawami kryptografii.						

Efekty uczenia się przedmiotu	Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
	[K7_W01] zna i rozumie w pogłębionym stopniu matematykę w zakresie niezbędnym do formułowania i rozwiązywania złożonych zagadnień związanych z kierunkiem studiów	Student poznaje matematyczne podstawy kryptografii.	[SW1] Ocena wiedzy faktograficznej
	[K7_U09] potrafi dokonać krytycznej analizy sposobu funkcjonowania istniejących rozwiązań technicznych i ocenić te rozwiązania, a także wykorzystać zdobyte w środowisku zajmującym się zawodowo działalnością inżynierską doświadczenie związane z utrzymaniem zaawansowanych urządzeń, obiektów i systemów technicznych typowych dla kierunku studiów	Student poznaje zasady działania kryptosystemów.	[SU1] Ocena realizacji zadania
	[K7_W43] zna i rozumie w pogłębionym stopniu formalne, techniczne i społeczne aspekty działania złożonych systemów informatycznych w społeczeństwie informacyjnym i w globalnej infrastrukturze informacyjnej	Student poznaje zaawansowane kryptosystemy.	[SW1] Ocena wiedzy faktograficznej
	[K7_K02] jest gotów do krytycznej oceny odbieranych treści, uznawania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych	Student poznaje zasady oceny działania kryptosystemów.	[SK5] Ocena umiejętności rozwiązywania problemów występujących w praktyce
[K7_U04] potrafi wykorzystywać posiadaną wiedzę z zakresu metod i technik programowania oraz dobrać i zastosować właściwe metody i narzędzia programistyczne w tworzeniu oprogramowania komputerów albo programowania urządzeń lub sterowników wykorzystujących mikroprocesory albo elementy lub układy programowalne, charakterystycznych dla danego kierunku studiów, dokonując oceny i krytycznej analizy wykonanego oprogramowania, a także syntezy i twórczej interpretacji prezentowanych za jego pomocą informacji	Student implementuje podstawowe kryptosystemy.	[SU1] Ocena realizacji zadania	
Treści przedmiotu	Wprowadzenie do współczesnej kryptografii. Kryptografia klasyczna: szyfry przestawieniowe i podstawieniowe, permutacje. Arytmetyka modularna i algorytm RSA. Ciała skończone i algorytm AES. Kryptografia symetryczna i asymetryczna.		
Wymagania wstępne i dodatkowe			
Sposoby i kryteria oceniania osiągniętych efektów uczenia się	Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa ocena końcowej
	Kolokwium	0.0%	100.0%
Zalecana lista lektur	Podstawowa lista lektur	D.R. Stinson: "Cryptography: Theory and Practice, Third Edition (Discrete Mathematics and Its Applications) 3rd Edition".	
	Uzupełniająca lista lektur	Brak.	
	Adresy eZasobów	Adresy na platformie eNauczanie: Podstawy kryptografii 2023 - Moodle ID: 29726 <a href="https://enauczanie.pg.edu.pl/moodle/course/view.php?id=29726">https://enauczanie.pg.edu.pl/moodle/course/view.php?id=29726</a>	
Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania			
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy		