



Karta przedmiotu

Nazwa i kod przedmiotu	Kryptologia, PG_00030022						
Kierunek studiów	Matematyka						
Data rozpoczęcia studiów	październik 2023 r.	Rok akademicki realizacji przedmiotu			2024/2025		
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	2	Język wykładowy			polski		
Semestr studiów	3	Liczba punktów ECTS			5.0		
Profil kształcenia	ogólnoakademicki	Forma zaliczenia			zaliczenie		
Jednostka prowadząca	Wydział Fizyki Technicznej i Matematyki Stosowanej -> Instytut Matematyki Stosowanej -> Zakład Analizy Nieliniowej						
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot	dr inż. Jakub Maksymiuk					
	Prowadzący zajęcia z przedmiotu	mgr inż. Tomasz Gzella					
		dr inż. Jakub Maksymiuk					
Formy zajęć i metody nauczania	Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
	Liczba godzin zajęć	30.0	0.0	15.0	15.0	0.0	60
	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	60		5.0		35.0	100
Cel przedmiotu	Wprowadzenie do problemów współczesnej kryptologii. Poznanie nowego obszaru zastosowań różnych działów matematyki i uwarunkowań kształtujących sposób ich stosowania.						

Efekty uczenia się przedmiotu	Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
	[K7_U13] rozumie matematyczne podstawy analizy algorytmów i procesów obliczeniowych, potrafi konstruować algorytmy o dobrych własnościach numerycznych, służące do rozwiązywania typowych i nietypowych problemów matematycznych	Student implementuje projekt oparty o współczesne metody kryptologiczne.	[SU4] Ocena umiejętności korzystania z metod i narzędzi
	[K7_W08] zna zaawansowane techniki obliczeniowe, wspomagające pracę matematyka i rozumie ich ograniczenia	Student zna podstawowe metody kryptoanalizy oraz ich ograniczenia	[SW1] Ocena wiedzy faktograficznej
	[K7_W11] zna matematyczne podstawy teorii informacji, teorii algorytmów i kryptografii oraz ich praktyczne zastosowania m.in. w programowaniu i szeroko rozumianej informatyce	Student: - wymienia kryteria oceny jakości algorytmów kryptograficznych - wymienia podstawowe pojęcia związane z kryptologią - wyjaśnia działanie podstawowych algorytmów symetrycznych i asymetrycznych - potrafi, korzystając z odpowiednich narzędzi, złamać proste szyfrogramy	[SW1] Ocena wiedzy faktograficznej
	[K7_U08] zna rozkłady probabilistyczne i ich własności; potrafi je stosować w zagadnieniach praktycznych, orientuje się w podstawach statystyki (zagadnienia estymacji i testowanie hipotez) oraz w podstawach statystycznej obróbki danych	Student stosuje pojęcia i twierdzenia rachunku prawdopodobieństwa do kryptoanalizy i oceny jakości kryptograficznych generatorów liczb losowych	[SU1] Ocena realizacji zadania

Treści przedmiotu	<p>Wykład:</p> <p>Wprowadzenie: definicje, otoczenie, literatura, kodowanie i szyfrowanie. Historia do roku 1914. Historia współczesnej kryptologii. Kryptologia militarna i dyplomatyczna. Prawne aspekty stosowania kryptologii.</p> <p>Kryptologia symetryczna: kryptografia tekstów: algorytmy podstawieniowe. Jakość algorytmu kryptograficznego. Kryptoanaliza statystyczna. Algorytmy przestawieniowe. Teoria informacji i wyniki Shannona. Algorytmy blokowe. Algorytm DES. Tryby pracy algorytmu. Jakość algorytmu DES. Projektowanie algorytmów blokowych, sieć Feistela. Łączenie algorytmów blokowych (TDES). Inne algorytmy blokowe. Algorytm Rijndael. Proste protokoły kryptograficzne z zastosowaniem algorytmów symetrycznych.</p> <p>Algorytmy strumieniowe. Algorytm A5 (GSM). Ciągi pseudolosowe. Analiza szyfrów strumieniowych.</p> <p>Kryptografia asymetryczna: zarządzanie kluczami. Algorytm Diffiego-Hellmana. Algorytm RSA. Jakość algorytmu RSA. Algorytmy ElGamala i stosujące krzywe eliptyczne.</p> <p>Jednokierunkowe funkcje skrótu :definicja. Funkcja MD5 i SHA. Jakość jednokierunkowych funkcji skrótu</p> <p>Zaawansowane protokoły kryptograficzne.</p> <p>Stosowanie kryptografii: Ochrona przesyłanych i przechowywanych danych w gospodarce elektronicznej. Przyszłość kryptologii i inne techniki ochrony informacji.</p> <p>Laboratorium i projekt:</p> <ul style="list-style-type: none"> <li>- Kryptografia tekstów. Szyfry podstawieniowe i przestawieniowe.</li> <li>- Kryptoanaliza szyfrów podstawieniowych. Statystyki występowania znaków w plikach tekstowych w języku polskim i angielskim,</li> <li>- Kryptografia z zastosowaniem współczesnych algorytmów symetrycznych.</li> <li>- Kryptografia z zastosowaniem algorytmów asymetrycznych.</li> <li>- Liczby pseudolosowe i pierwsze.</li> <li>- Implementacja prostych algorytmów kryptologicznych albo raport z analizy jakości wskazanych algorytmów</li> </ul>											
Wymagania wstępne i dodatkowe	Matematyka dyskretna, Algebra liniowa, Algebra, Rachunek prawdopodobieństwa											
Sposoby i kryteria oceniania osiągniętych efektów uczenia się	<table border="1"> <thead> <tr> <th>Sposób oceniania (składowe)</th> <th>Próg zaliczeniowy</th> <th>Składowa oceny końcowej</th> </tr> </thead> <tbody> <tr> <td>Ćwiczenia praktyczne</td> <td>50.0%</td> <td>40.0%</td> </tr> <tr> <td>Projekt</td> <td>50.0%</td> <td>60.0%</td> </tr> </tbody> </table>	Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej	Ćwiczenia praktyczne	50.0%	40.0%	Projekt	50.0%	60.0%		
Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej										
Ćwiczenia praktyczne	50.0%	40.0%										
Projekt	50.0%	60.0%										
Zalecana lista lektur	<p>Podstawowa lista lektur</p> <p>Uzupełniająca lista lektur</p> <p>Adresy eZasobów</p>	<p>1. Stinson D.R.: Kryptografia. W teorii i praktyce, Warszawa: Wydawnictwa Naukowo-Techniczne, 2005</p> <p>2. Rubinstein-Salzedo S., Cryptography, Springer 2018</p> <p>1. Bard G.: Algebraic Cryptanalysis, Springer Verlag 2009</p> <p>2. Paar C., Pelzl J., Understanding Cryptography, Springer 2010</p>	<p>Adresy na platformie eNauczanie:</p> <p>Kryptologia - Moodle ID: 39608</p> <p><a href="https://enauczanie.pg.edu.pl/moodle/course/view.php?id=39608">https://enauczanie.pg.edu.pl/moodle/course/view.php?id=39608</a></p>									

Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania	Znajdź klucz zastosowany do zaszyfrowania wiadomości szyfrem klasycznym.  Omów metody ataku na kryptosystem ElGamala.  Znajdź zbiór potencjalnych kluczy dla dwóch zestawów tekstów jawnych i ich szyfrogramów.
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.