POLITECHNIKA GDAŃSKA

Karta przedmiotu

Nazwa i kod przedmiotu	Kryptologia, PG_00030022		
Kierunek studiów	Matematyka		
Data rozpoczęcia studiów	październik 2022 r.	Rok akademicki realizacji przedmiotu	2023/2024
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	mieszane (blended-learning)
Rok studiów	2	Język wykładowy	polski
Semestr studiów	3	Liczba punktów ECTS	4.0
Profil kształcenia	ogólnoakademicki	Forma zaliczenia	zaliczenie
Jednostka prowadząca	Wydział Fizyki Technicznej i Matematyki Stosowanej -> Katedra Rachunku Prawdopodobieństwa i Biomatematyki		
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot	dr inż. Jakub Maksymiuk	
	Prowadzący zajęcia z przedmiotu	dr inż. Jakub Maksymiuk mgr inż. Tomasz Gzella	

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: 30.0						

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_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 podstawowe 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
	[K7_W08] zna zaawansowane techniki obliczeniowe, wspomagające pracę matematyka i rozumie ich ograniczenia	Student zna podstawowe metody kryptoanalizy oraz ich ograniczenia	[SW3] Ocena wiedzy zawartej w opracowaniu tekstowym i projektowym

Treści przedmiotu	Wykład: Wprowadzenie: definicja, otoczenie, literatura. Kodowanie i szyfrowanie. Historia do roku 1914. Historia współczesnej kryptologii. Kryptologia militarna i dyplomatyczna. Prawne aspekty stosowania kryptologii. Kryptologia symetryczna: kryptografia tekstów: algorytmy podstawieniowe. Jakość algorytmu kryptograficznego. Kryptoanaliza statystyczna. Algorytmy przestawieniowe. Enigma: działanie i kryptoanaliza. Teoria informacji i wyniki Shannona. Algorytmy blokowe. Algorytm DES. Tryby pracy algorytmu. Jakość algorytmu DES. Kryptoanaliza: różnicowa i liniowa. Projektowanie algorytmów blokowych, sieć Feistela. Łączenie algorytmów blokowych (TDES). Inne algorytmy blokowe. Algorytm Rijndael. Proste protokoły kryptograficzne z zastosowaniem algorytmów symetrycznych. Algorytmy strumieniowe. Algorytm A5 (GSM). Ciągi pseudolosowe. Analiza szyfrów strumieniowych. Kryptografia asymetryczna: zarządzanie kluczami. Algorytm Diffiego-Hellmana. Algorytm RSA. Jakość algorytmu RSA. Algorytmy ElGamala i stosujące krzywe eliptyczne. Inne algorytmy asymetryczne. Protokoły kryptograficzne stosujące algorytmy niesymetryczne. Jednokierunkowe funkcje skrótu :definicja. Funkcja MD5 i SHA. Jakość jednokierunkowych funkcji skrótu Zaawansowane protokoły kryptograficzne. Stosowanie kryptografii: patentowanie algorytmów. Ochrona przesyłanych i przechowywanych danych w gospodarce elektronicznej. Przyszłość kryptologii i inne techniki ochrony informacji. Laboratorium: Ćw. 1 Program Cryptool. Kryptografia tekstów. Szyfry podstawieniowe i przestawieniowe. Ćw. 2 Kryptoanaliza szyfrów podstawieniowych. Statystyki występowania znaków w plikach tekstowych w języku polskim i angielskim, w języku C i w plikach wykonywalnych. Metoda koincydencji i funkcji autokorelacji. Ćw. 3 Kryptoanaliza Enigmy. Ćw. 4 Kryptografia z zastosowaniem współczesnych algorytmów symetrycznych. Kryptoanaliza różnicowa algorytmu DES. Ćw. 5 Kryptografia z zastosowaniem algorytmów asymetrycznych. Ćw. 6 Liczby pseudolosowe i pierwsze. Ćw. 7 Kryptoanaliza algorytmów asymetrycznych. Projekt: Implementacja prostych algorytmów kryptologicznych albo raport z analizy jakości wskazanych algorytmów bądź protokołów kryptograficznych.
Wymagania wstępne i dodatkowe	Matematyka dyskretna, Algebra liniowa, Algebra, Rachunek prawdopodobieństwa

Sposoby i kryteria oceniania osiąganych efektów uczenia się

Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
Projekt	50.0%	60.0%
Ćwiczenia praktyczne	50.0%	40.0%

Zalecana lista lektur	Podstawowa lista lektur	1. Stinson D.R.: Kryptografia. W teorii i praktyce, Warszawa: Wydawnictwa Naukowo-Techniczne, 2005 2. Rubinstein-Salzedo S., Cryptography, Springer 2018

	Uzupełniająca lista lektur	1. Bard G.: Algebraic Cryptanalysis, Springer Verlag 2009 2. Paar C., Pelzl J., Understanding Cryptography, Springer 2010
	Adresy eZasobów	Adresy na platformie eNauczanie: Kryptologia [Matematyka 2023/24] - Moodle ID: 28411 https://enauczanie.pg.edu.pl/moodle/course/view.php?id=28411
Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania	Znajdź klucz zastosowany do zaszyfrowania wiadomości szyfrem klasycznym. Omów metody ataku na kryptosystem ElGamala. Znajdź zbiór potencjalnych kluczy stosując kryptoanalizę różnicową dla dwóch zestawów tekstów jawnych i ich szyfrogramów.	
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy	