



Karta przedmiotu

Nazwa i kod przedmiotu	Kryptografia, PG_00037330						
Kierunek studiów	Fizyka Techniczna						
Data rozpoczęcia studiów	październik 2020 r.	Rok akademicki realizacji przedmiotu			2021/2022		
Poziom kształcenia	I stopnia - inżynierskie	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	4	Liczba punktów ECTS			5.0		
Profil kształcenia	ogólnoakademicki	Forma zaliczenia			egzamin		
Jednostka prowadząca	Wydział Fizyki Technicznej i Matematyki Stosowanej -> Katedra Fizyki Teoretycznej i Informatyki Kwantowej						
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot	dr inż. Marcin Nowakowski					
	Prowadzący zajęcia z przedmiotu	dr inż. Marcin Nowakowski					
Formy zajęć i metody nauczania	Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
	Liczba godzin zajęć	30.0	0.0	30.0	0.0	0.0	60
	W tym liczba godzin zajęć na odległość: 0.0						
Adresy na platformie eNauczanie:							
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		10.0		55.0	125
Cel przedmiotu	Celem przedmiotu jest zaznajomienie studentów z podstawowymi zagadnieniami dotyczącymi współczesnych protokołów kryptograficznych, metod teorii informacji i teorii kodowania mających zastosowanie w kryptografii oraz ich zastosowań w przetwarzaniu informacji.						
Efekty uczenia się przedmiotu	Efekt kierunkowy		Efekt z przedmiotu		Sposób weryfikacji i oceny efektu		
	[K6_U03] Posiada umiejętność programowania w wybranym języku oraz stosowania podstawowych pakietów oprogramowania.		Posiada podstawową wiedzę w zakresie metodyki i technik programowania dla wybranych zagadnień kryptologicznych.		[SU1] Ocena realizacji zadania		
	[K6_U02] Potrafi analizować i rozwiązywać proste problemy naukowe i techniczne w oparciu o posiadaną wiedzę, stosując metody analityczne, numeryczne, symulacyjne i eksperymentalne.		Potrafi analizować i rozwiązywać proste problemy techniczne w zakresie schematów kryptograficznych.		[SU2] Ocena umiejętności analizy informacji		
	[K6_K01] Rozumie potrzebę uczenia się przez całe życie oraz potrzebę podnoszenia kompetencji zawodowych i osobistych. Potrafi inspirować i organizować proces uczenia się innych osób.		Rozumie potrzebę uczenia się przez całe życie. Umie zastosować algorytmy kryptograficzne dla wybranych problemów informatycznych.		[SK5] Ocena umiejętności rozwiązywania problemów występujących w praktyce		
	[K6_W05] Posiada podstawową wiedzę w zakresie metodyki i technik programowania oraz wykorzystywania wybranych narzędzi informatycznych w fizyce i technice.		Posiada podstawową wiedzę w zakresie klasyfikacji algorytmów kryptograficznych.		[SW1] Ocena wiedzy faktograficznej		

Treści przedmiotu	<p>Kryptologia symetryczna: kryptografia tekstów: algorytmy podstawieniowe. Jakość algorytmu kryptograficznego.</p> <p>Kryptoanaliza statystyczna. Algorytmy przestawieniowe. Enigma: działanie i kryptoanaliza. Teoria informacji i teoria kodowania. Wielkości entropowe. Losowość. Kody liniowe.</p> <p>Algorytmy blokowe. Algorytm DES. Tryby pracy algorytmu. Jakość algorytmu DES. Kryptoanaliza: różnicowa i liniowa. Projektowanie algorytmów blokowych, sieć Feistel. Łączenie algorytmów blokowych (TDES). Inne algorytmy blokowe. Algorytm Rijndael. Protokoły kryptograficzne z zastosowaniem algorytmów symetrycznych.</p> <p>Algorytmy strumieniowe. Algorytm A5 (GSM). Ciągi pseudolosowe. Analiza szyfrów strumieniowych. Kryptografia asymetryczna: zarządzanie kluczami. Algorytm Diffiego-Hellmana. Algorytm RSA. Jakość algorytmu RSA.</p> <p>Protokół TLS i SSL. Algorytmy ElGamala i stosujące krzywe eliptyczne. Inne algorytmy asymetryczne. Protokoły kryptograficzne stosujące algorytmy niesymetryczne.</p> <p>Jednokierunkowe funkcje skrótu. Funkcja MD5 i SHA. Jakość jednokierunkowych funkcji skrótu. Rola złożoności obliczeniowej i klas problemów obliczeniowych.</p> <p>Zaawansowane protokoły kryptograficzne. Kwanternionowe systemy kryptograficzne. Kryptografia obrazu. Metody sztucznej inteligencji w kryptografii.</p> <p>Kryptografia kwantowa i postkwantowa.</p> <p>Stosowanie kryptografii: patentowanie algorytmów. Ochrona przesyłanych i przechowywanych danych w gospodarce elektronicznej. Przyszłość kryptologii i inne techniki ochrony informacji.</p>		
Wymagania wstępne i dodatkowe	<p>Matematyka dyskretna, Algebra liniowa, Rachunek prawdopodobieństwa</p> <p>Znajomość programowania w językach obiektowych.</p>		
Sposoby i kryteria oceniania osiągniętych efektów uczenia się	Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
	Laboratorium	50.0%	50.0%
	Egzamin	50.0%	50.0%
Zalecana lista lektur	Podstawowa lista lektur	<ol style="list-style-type: none"> Jean-Philippe Aumasson, Nowoczesna kryptografia, PWN 2018. Stinson D.R.: Kryptografia. W teorii i praktyce, WNT 2005. B. Schneier Kryptografia dla praktyków, WNT 2002. 	
	Uzupełniająca lista lektur	<ol style="list-style-type: none"> Bard G.: Algebraic Cryptanalysis, Springer Verlag 2009. D. Boneh, V. Shoup, A graduate course in applied cryptography, Stanford Univ., 2015 	
	Adresy eZasobów		
Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania	<ol style="list-style-type: none"> Zaimplementować tryby szyfrowania blokowego ECB, CBC, FCB Dane wejściowe: Plik tekstowy do zaszyfrowania. Dane wyjściowe: Plik tekstowy zaszyfrowany. Założenie: Bloki 64 bitowe, użyć funkcji wczytywania tekstu i transformacji na tablice bitowe. Dowolny język programowania: C#, Python, Java Zaimplementować uproszczoną wersję wybranego trybu szyfrowania z jedną rundą algorytmu DES. (Założenia j/w). 		
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy		