POLITECHNIKA GDAŃSKA

Karta przedmiotu

Nazwa i kod przedmiotu	Kryptografia, PG_00060224		
Kierunek studiów	Fizyka Techniczna		
Data rozpoczęcia studiów	październik 2026 r.	Rok akademicki realizacji przedmiotu	2028/2029
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	3	Język wykładowy	polski
Semestr studiów	5	Liczba punktów ECTS	4.0
Profil kształcenia	ogólnoakademicki	Forma zaliczenia	zaliczenie
Jednostka prowadząca	Wydziały Politechniki Gdańskiej -> Wydział Fizyki Technicznej i Matematyki Stosowanej -> Instytut Fizyki i Informatyki Stosowanej -> Zakład Fizyki Teoretycznej i Informatyki Kwantowej		
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot	dr inż. Marcin Nowakowski	
	Prowadzący zajęcia z przedmiotu		

Formy zajęć

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						

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

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_K01] jest gotów do nieustannego uzupełniania wiedzy z zakresu fizyki i nauk pokrewnych, w tym informatyki stosowanej lub energetyki, krytycznej oceny tej wiedzy oraz uznawania jej znaczenia w rozwiązywaniu problemów praktycznych i poznawczych.	Rozumie potrzebę uczenia się przez całe życie. Umie zastosować algorytmy kryptograficzne dla wybranych problemów informatycznych	[SK5] Ocena umiejętności rozwiązywania problemów występujących w praktyce
[K6_U02] potrafi analizować i rozwiązywać złożone i nietypowe problemy naukowe i techniczne w oparciu o posiadaną wiedzę. Stosuje odpowiednie metody analityczne, rachunkowe, numeryczne, symulacyjne lub eksperymentalne.	Posiada podstawową wiedzę w zakresie metodyki i technik programowania dla wybranych zagadnień kryptologicznych.	[SU2] Ocena umiejętności analizy informacji
[K6_U03] posiada umiejętność programowania w wybranym języku oraz stosowania podstawowych pakietów oprogramowania	Posiada podstawową wiedzę w zakresie klasyfikacji algorytmów kryptograficznych.	[SU1] Ocena realizacji zadania
[K6_W05] posiada wiedzę w zakresie metodyki i technik programowania oraz wykorzystywania wybranych narzędzi informatycznych w fizyce i technice.	Potrafi analizować i rozwiązywać proste problemy techniczne w zakresie schematów kryptograficznych	[SW1] Ocena wiedzy faktograficznej

<table>
<tr><td>Treści przedmiotu</td><td>Treści przedmiotu - wykład
Kryptologia symetryczna: kryptografia tekstów: algorytmy podstawieniowe. Jakość algorytmu kryptograficznego.
Kryptoanaliza statystyczna. Algorytmy przestawieniowe. Enigma: działanie i kryptoanaliza.Teoria informacji i teoria kodowania. Wielkości entropowe. Losowość. Kody liniowe.

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. 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.
Protokół TLS i SSL. Algorytmy ElGamala i stosujące krzywe eliptyczne. Inne algorytmy asymetryczne. Protokoły kryptograficzne stosujące algorytmy niesymetryczne.

Jednokierunkowe funkcje skrótu. Funkcja MD5 i SHA. Jakość jednokierunkowych funkcji skrótu. Rola złożoności obliczeniowej i klas problemów obliczeniowych.
Zaawansowane protokoły kryptograficzne. Kwaternionowe systemy kryptograficzne.
Kryptografia obrazu. Metody sztucznej inteligencji w kryptografii.
Kryptografia kwantowa i postkwantowa.

Stosowanie kryptografii: patentowanie algorytmów. Ochrona przesyłanych i przechowywanych danych w gospodarce elektronicznej. Przyszłość kryptologii i inne techniki ochrony informacji.

Treści przedmiotu - laboratoria
Implementacja wybranych algorytmów kryptograficznych, w szczególności: DES, szyfry strumieniowe i blokowe z wybraną siecią Feistela, funkcje hashujące.</td></tr>
<tr><td>Wymagania wstępne i dodatkowe</td><td>Matematyka dyskretna, Algebra liniowa, Rachunek prawdopodobieństwa

Znajomość programowania w językach obiektowych.</td></tr>
<tr><td>Sposoby i kryteria oceniania osiąganych efektów uczenia się</td><td>
<table>
<tr><th>Sposób oceniania (składowe)</th><th>Próg zaliczeniowy</th><th>Składowa oceny końcowej</th></tr>
<tr><td>Laboratorium</td><td>50.0%</td><td>50.0%</td></tr>
<tr><td>Egzamin</td><td>50.0%</td><td>50.0%</td></tr>
</table>
</td></tr>
<tr><td>Zalecana lista lektur</td><td>
<table>
<tr><td>Podstawowa lista lektur</td><td>1. Jean-Philippe Aumasson, Nowoczesna kryptografia, PWN 2018.
2. Stinson D.R.: Kryptografia. W teorii i praktyce, WNT 2005.
3. B. Schneier Kryptografia dla praktykow, WNT 2002.</td></tr>
<tr><td>Uzupełniająca lista lektur</td><td>1. Bard G.: Algebraic Cryptanalysis, Springer Verlag 2009.

2. D. Boneh, V. Shoup, A graduate course in applied cryptography, Stanford Univ., 2015</td></tr>
<tr><td>Adresy eZasobów</td><td></td></tr>
</table>
</td></tr>
<tr><td>Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania</td><td>1. Zaimplementować tryby szyfrowania blokowego ECB, CBC, FCB
Dane wejściowe: Plik tekstowy do zaszyfrowania.
Dane wyjśniowe: Plik tekstowy zaszyfrowany.
Założenie: Bloki 64 biotowe, użyć funkcji wczytywania tekstu i transformacji na tablice bitowe. Dowolny język programowania: C#, Python, Java
2. Zaimplementować uproszczoną wersję wybranego trybu szyfrowania z jedną rundą algorytmu DES. (Założenia j/w).</td></tr>
<tr><td>Zajęcia praktyczne w ramach przedmiotu</td><td>Nie dotyczy</td></tr>
</table>