POLITECHNIKA GDAŃSKA

Karta przedmiotu

| | | | |
|---|---|---|---|
| Nazwa i kod przedmiotu | Kryptologia, PG_00069469 | | |
| Kierunek studiów | Matematyka | | |
| Data rozpoczęcia studiów | październik 2025 r. | Rok akademicki realizacji przedmiotu | 2026/2027 |
| Poziom kształcenia | II stopnia | Grupa zajęć | Grupa zajęć specjalnościowych<br>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 | 4.0 |
| Profil kształcenia | ogólnoakademicki | Forma zaliczenia | zaliczenie |
| Jednostka prowadząca | Wydziały Politechniki Gdańskiej -> 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 | dr inż. Jakub Maksymiuk | |

**Formy zajęć**

| 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_U10] rozumie matematyczne podstawy analizy algorytmów i procesów obliczeniowych, konstruuje algorytmy o dobrych własnościach numerycznych, służące do rozwiązywania typowych i nietypowych problemów matematycznych | Student implementuje projekt oparty o współczesne metody kryptologiczne. | [SU3] Ocena umiejętności wykorzystania wiedzy uzyskanej w ramach przedmiotu<br>[SU4] Ocena umiejętności korzystania z metod i narzędzi |
| [K7_W03] wykazuje się znajomością zaawansowanych technik obliczeniowych, wspomagających pracę matematyka i rozumie ich ograniczenia | Student zna podstawowe metody kryptoanalizy oraz ich ograniczenia. | [SW1] Ocena wiedzy faktograficznej |
| [K7_U06] stosuje rozkłady probabilistyczne i ich własności w zagadnieniach praktycznych, orientuje się w podstawach statystyki oraz w podstawach statystycznej obróbki danych | Student stosuje pojęcia i twierdzenia rachunku prawdopodobieństwa do kryptoanalizy i oceny jakości kryptograficznych generatorów liczb losowych | [SU3] Ocena umiejętności wykorzystania wiedzy uzyskanej w ramach przedmiotu |
| [K7_W06] analizuje matematyczne podstawy teorii informacji, teorii algorytmów i kryptografii oraz ich praktyczne zastosowania m.in. w programowaniu i szeroko rozumianej informatyce | Student:<br>- wymienia kryteria oceny jakości algorytmów kryptograficznych<br>- wymienia podstawowe pojęcia związane z kryptologią<br>- wyjaśnia działanie podstawowych algorytmów symetrycznych i asymetrycznych | [SW1] Ocena wiedzy faktograficznej |

**Treści przedmiotu**

Treści przedmiotu - wykład

Wykład:

Wprowadzenie: definicje, 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. 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.

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.

Jednokierunkowe funkcje skrótu :definicja. Funkcja MD5 i SHA. Jakość jednokierunkowych funkcji skrótu

Zaawansowane protokoły kryptograficzne.

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

Laboratorium i projekt:

- Kryptografia tekstów. Szyfry podstawieniowe i przestawieniowe.

- Kryptoanaliza szyfrów podstawieniowych. Statystyki występowania znaków w plikach tekstowych w języku polskim i angielskim,

- Kryptografia z zastosowaniem współczesnych algorytmów symetrycznych.

- Kryptografia z zastosowaniem algorytmów asymetrycznych.

- Liczby pseudolosowe i pierwsze.

- Implementacja prostych algorytmów kryptologicznych albo raport z analizy jakości wskazanych algorytmów

**Wymagania wstępne i dodatkowe**

Matematyka dyskretna, Algebra liniowa, Algebra, Rachunek prawdopodobieństwa, Algorytmy i struktury danych

**Sposoby i kryteria oceniania osiąganych efektów uczenia się**

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

**Zalecana lista lektur**

| | |
|---|---|
| Podstawowa lista lektur | 1. Stinson D.R.: Kryptografia. W teorii i praktyce, Warszawa: Wydawnictwa Naukowo-Techniczne, 2005<br>2. Rubinstein-Salzedo S., Cryptography, Springer 2018 |
| Uzupełniająca lista lektur | 1. Bard G.: Algebraic Cryptanalysis, Springer Verlag 2009<br>2. Paar C., Pelzl J., Understanding Cryptography, Springer 2010 |
| Adresy eZasobów | |

**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.

| | |
|---|---|
| Zajęcia praktyczne w ramach przedmiotu | Nie dotyczy |

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.