Algorytmy Algebry I Teorii Liczb

Karta opisu przedmiotu

Informacje podstawowe

Kierunek studiów : Informatyka analityczna

Ścieżka : -

Jednostka organizacyjna : Wydział Matematyki i Informatyki

Poziom kształcenia : pierwszego stopnia

Forma studiów : studia stacjonarne

Profil studiów : ogólnoakademicki

Obligatoryjność : fakultatywny

Cykl kształcenia : 2022/23

Kod przedmiotu : UJ.WMIIANS.1380.03348.22

Języki wykładowe : polski

Dyscypliny : Informatyka

Klasyfikacja ISCED : 0613 Tworzenie i analiza oprogramowania i aplikacji

Kod USOS : WMI.TCS.AATL.S

Koordynator przedmiotu

Lech Duraj

Prowadzący zajęcia

Lech Duraj

Okresy Semestr 4, Semestr 5, Semestr 6	Forma weryfikacji uzyskanych efektów uczenia się egzamin Forma prowadzenia i godziny zajęć wykład: 30 ćwiczenia: 30	Liczba punktów ECTS 6.0

Cele kształcenia dla przedmiotu

C1	Celem przedmiotu jest przekazanie wiedzy z zakresu algorytmów związanych z teorią liczb i algebrą, przede wszystkim w odniesieniu do kryptografii jako ich głównego zastosowania.

Efekty uczenia się dla przedmiotu

Kod	Efekty w zakresie	Kierunkowe efekty uczenia się	Metody weryfikacji
Wiedzy – Student zna i rozumie:			
W1	wymienione w "Treściach programowych" podstawowe pojęcia z zakresu algebry i teorii liczb, przydatne w pracy informatyka	IAN_K1_W01	egzamin ustny, zaliczenie
W2	wymienione w "Treściach programowych" algorytmy (w szczególności algorytmy kryptograficzne)	IAN_K1_W06, IAN_K1_W08, IAN_K1_W10	egzamin ustny, zaliczenie
Umiejętności – Student potrafi:			
U1	przeprowadzić dowody poprawności wybranych twierdzeń podanych w "Treściach programowych", w szczególności dowody poprawności i analizę złożoności algorytmów z dziedziny algebry i teorii liczb	IAN_K1_U01, IAN_K1_U10, IAN_K1_U17, IAN_K1_U21	egzamin ustny, zaliczenie
U2	zaimplementować podstawowe algorytmy algebry i teorii liczb (w tym algorytmy kryptograficzne) w sposób efektywny, uwzględniając zagadnienia bezpieczeństwa komunikacji	IAN_K1_U03, IAN_K1_U17	zaliczenie

Bilans punktów ECTS

Forma aktywności studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
wykład	30
ćwiczenia	30
samodzielne rozwiązywanie zadań komputerowych	30
przygotowanie do ćwiczeń	30
rozwiązywanie zadań problemowych	30

przygotowanie do egzaminu	29
uczestnictwo w egzaminie	1

Łączny nakład pracy studenta	Liczba godzin 180	ECTS 6.0

* godzina (lekcyjna) oznacza 45 minut

Treści programowe

Lp.	Treści programowe	Efekty uczenia się dla przedmiotu
1.	Liczby całkowite: zapis komputerowy, podstawowe algorytmy arytmetyki (mnożenie, dzielenie z resztą, obliczanie największego wspólnego dzielnika), złożoność sortowania i wyszukiwania na liczbach całkowitych	W1, W2, U1, U2
2.	Konstrukcje algebraiczne: grupy przemienne, pierścienie i ciała, grupy nieprzemienne (permutacje), wielomiany i ciała skończone (w tym operacje arytmetyczne), arytmetyka krzywych eliptycznych	W1, W2, U1, U2
3.	Podstawy kryptografii: algorytmy symetryczne, kryptografia z kluczem publicznym, algorytm RSA, protokół Diffiego-Hellmana, algorytm ElGamal	W1, W2, U1, U2
4.	Liczby pierwsze i faktoryzacja: test probabilitystyczny Millera-Rabina, szkic testu deterministycznego AKS, algorytm “rho” Pollarda, sito kwadratowe, sito nad ciałem liczbowym	W1, W2, U1, U2
5.	Problem pierwiastka dyskretnego i problem logarytmu dyskretnego na liczbach całkowitych i w grupach przemiennych (algorytm Tonellego-Shanksa, metoda baby-step-giant-step, algorytm Pohliga-Hellmana, rachunek indeksów)	W1, W2, U1, U2
6.	Podstawy obliczeń kwantowych, algorytm Shora	W1, W2, U1, U2

Informacje rozszerzone

Metody nauczania :

wykład z prezentacją multimedialną, dyskusja, rozwiązywanie zadań, ćwiczenia przedmiotowe

Rodzaj zajęć	Formy zaliczenia	Warunki zaliczenia przedmiotu
wykład	egzamin ustny	Pozytywna ocena z egzaminu oraz łączna pozytywna ocena z egzaminu i ćwiczeń

Rodzaj zajęć	Formy zaliczenia	Warunki zaliczenia przedmiotu
ćwiczenia	zaliczenie	Zaliczenie ćwiczeń na podstawie programów zaliczeniowych i zadań domowych

Literatura

Obowiązkowa

1. Neal Koblitz, "A Course in Number Theory and Cryptography"

Dodatkowa

1. Song Y. Yan, "Number Theory for Computing"