Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

obowiązuje studentów rozpoczynających studia w roku akademickim 2022/2023

Wydział Informatyki i Telekomunikacji

Kierunek studiów: Informatyka | Profil: Ogólnoakademicki

Forma sudiów: stacjonarne | Kod kierunku: I

Stopień studiów: I

Specjalności: Brak specjalności

1 Informacje o przedmiocie

Nazwa przedmiotu	Matematyka dyskretna
Nazwa przedmiotu w języku angielskim	Discrete mathematics
Kod przedmiotu	WIiT I oIS C4 22/23
Kategoria przedmiotu	Przedmioty kierunkowe
Liczba punktów ECTS	5.00
Semestry	2

2 Rodzaj zajęć, liczba godzin w planie studiów

Semestr	Wykład	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Seminarium	Projekt
2	30	15	15	0	0	0

3 Cele przedmiotu

Cel 1 Przedstawienie elementów kombinatoryki, teorii grafów, teorii liczb i kryptografii oraz wybranych metod matematycznych niezbędnych przy konstrukcji i analizie algorytmów.

4 Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1 Podstawowa znajomość algebry (struktury algebraiczne) i analizy matematycznej (ciągi i szeregi liczbowe, szeregi funkcyjne) Uwaga: Nie jest wymagana ocena pozytywna z żadnego przedmiotu.

5 Efekty kształcenia

EK1 Wiedza Znajomość podstawowych pojęć, twierdzeń i algorytmów teorii grafów.

EK2 Umiejętności Umiejętność zastosowania algorytmów do wyznaczania w grafach dróg(w szczególności zastosowanie algorytmów trasowania) i podgrafów spinających. Umiejętność sprawdzenie podstawowych własności grafu takich jak planarność, spójność wierzchołkowa i krawędziowa, istnienie cykli zawierających wybrane struktury (zbiory wierzchołków, zbiory krawędzi) w grafie wyznaczania dróg.

EK3 Wiedza Znajomość podstawowych pojęć i algorytmów teorii liczb, kryptografii oraz pojęć i własności dotyczących równań rekurencyjnych i matematycznych podstaw informatyki.

EK4 Umiejętności Umiejętność szyfrowanie i deszyfrowanie łańcuchów danych, generowanie i sprawdzenie autentyczności podpisu cyfrowego. Umiejętność rozwiązywania równań rekurencyjnych liniowych oraz znajomość maszyny Turinga.

EK5 Kompetencje społeczne Student posiada umiejętność jasnego formułowania pytań, czynnego udziału w dyskusji i potrafi pracować w grupie nad niezbyt trudnymi zadaniami praktycznymi.

6 Treści programowe

Ćwiczenia		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
C1	Rozwiązywanie zadań dotyczących indukcji matematycznej oraz rekurencji.	1
C2	Rozwiązywanie zadań dotyczących zasada szufladkowej Dirichleta, zasady włączania-wyłączania i kombinatoryki.	1
C3	Rozwiązywanie zadań dotyczących funkcji tworzących i równań rekurencyjnych	2
C4	Rozwiązywanie zadań dotyczących podstawowych pojęć teorii grafów. Analiza przykładów grafów i ich własności.	1
C5	Rozwiązywanie zadań dotyczących dróg i cykli Eulera oraz cykli Hamiltona w grafach.	1.5
C6	Rozwiązywanie zadań dotyczących drzew i algorytmów Prima i Kruskala.	1
C7	Rozwiązywanie zadań dotyczących grafów skierowanych oraz algorytmu Dijkstry i algorytmu Bellmana-Forda.	1.5
C8	Rozwiązywanie zadań dotyczących grafów dwudzielnych, twierdzenie Halla i analiza problemów przepływu w sieciach.	1
C9	Rozwiązywanie zadań dotyczących kolorowania grafów.	1

Ćwiczenia		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
C10	Rozwiązywanie zadań dotyczących arytmetyki liczb całkowitych, twierdzenia Fermata, twierdzenia Eulera i chińskiego twierdzenia o resztach oraz i rozwiązywanie równań diofantycznych.	1
C11	Rozwiązywanie zadań dotyczących algorytmu RSA, ElGamala, algorytmu Diffiego-Hellmana.	2
C12	Rozwiązywanie zadań dotyczących szyfrowania strumieniowego i podpisu cyfrowego..	1

Laboratorium		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
L1	Wprowadzenie do programowania w Pythonie i do wykorzystania pakietu SageMath	3
L2	Działania na liczbach całkowitych (algorytmy potęgowania w Z i potęgowania mod n, liczby pierwsze (generowanie, własności liczb pierwszych, rozkład liczby całkowitej na iloczyn potęg liczb pierwszych), równania diofantyczne z wykorzystaniem pakietu SageMath	2
L3	Algorytmy szyfrujące symetryczne i asymetryczne (w szczególności RSA, EL Gammala) Bezpieczeństwo szyfrów, klasyczna ataki na RSA z wykorzystaniem pakietu SageMath	2
L4	Maszynowa reprezentacja grafów, generowanie i wizualizacja grafów, garfy losowe (podstawowe konstrukcje) oraz badanie podstawowych własności grafów z wykorzystaniem pakietu SageMath	3
L5	Wykorzystanie pakietu SageMath do badania algorytmu Fleur'ego, algorytmu Prima, algorytmu Kruskala, algorytmu Dijkstry i algorytmu Bellmana-Forda	3
L6	Badanie sieci i analiza problemu przepływu w sieciach z wykorzystaniem pakietu SageMath	1
L7	Algorytmy kolorowania grafów	1

Wykład		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
W1	Indukcja matematyczna (zasada indukcji matematycznej, zasady minimum i maksimum) oraz rekurencja (definicje rekurencyjne, liczby Fibonacciego i rozwiązywanie równań rekurencyjnych)	3

Wykład		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
W2	Zasada szufladkowa Dirichleta i zasada włączania-wyłączania	1
W3	Grafy: podstawowe pojęcia	2
W4	Grafy: cykle Eulera i Hamiltona	3
W5	Grafy: drzewa, algorytmy Prima i Kruskala wyznaczające minimalnego drzewa spinającego.	2
W6	Grafy skierowane: Podstawowe pojęcia	1
W7	Grafy skierowane: algorytmy Dijkstry i Bellmana-Forda zwracające minimalne drogi w grafach skierowanych	3
W8	Grafy: grafy dwudzielne, skojarzenia i twierdzenie Halla spójność i twierdzenie Mengera, sieci, przepływy, przekroje i twierdzenie Forda-Fulkersona	3
W9	Grafy: kolorowanie grafów, algorytm zachłanny, algorytm RF i SL.	2
W10	Arytmetyka liczb całkowitych: podzielność, NWD, NWW, liczby pierwsze, algorytm Euklidesa rozkład na czynniki pierwsze, równania diofantyczne	2
W11	Arytmetyka modularna: twierdzenie Fermata, twierdzenie Eulera, chińskie twierdzenie o resztach	1
W12	Kryptografia: klasyfikacja algorytmów szyfrujących, algorytm szyfrowania RSA, ElGamala, algorytm Diffiego-Hellmana	3
W13	Kryptografia: szyfry strumieniowe i podpis cyfrowy.	2
W14	Matematyczne podstawy informatyki: automaty skończone, maszyna Turinga	2

7 Narzędzia dydaktyczne

N1 Wykłady (w przypadku zajęć zdalnych wykłady z wykorzystaniem narzędzi do komunikacji zdalnej)

N2 Zadania tablicowe (w przypadku zajęć zdalnych zajęcia z wykorzystaniem narzędzi do komunikacji zdalnej)

N3 Ćwiczenia laboratoryjne (w przypadku zajęć zdalnych zajęcia z wykorzystaniem narzędzi do komunikacji zdalnej)

8 Obciążenie pracą studenta

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z nauczycielem akademickim, w tym:	
Godziny wynikające z planu studiów	60
Konsultacje przedmiotowe	10
Egzaminy i zaliczenia w sesji	5
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	75
Opracowanie wyników	0
Przygotowanie raportu, projektu, prezentacji, dyskusji	0
Sumaryczna liczba godzin dla przedmiotu wynikająca z całego nakładu pracy studenta	**150**
Sumaryczna liczba punktów ECTS dla przedmiotu	5.00

9 Sposoby oceny

W przypadku uruchomienia e-kursu do przedmiotu np. na platformie Moodle , warunkiem koniecznym zaliczenie jest aktywne udział w e-kursie

W przypadku gdy podczas zajęć są zadawane projekty/sprawozdania/zadania, wrunkiem koniecznym oddanie projektu/sprawozdania/zadania we wskazanym na zajęciach terminie. Niespełnienie tego warunku uniemożliwia uzyskanie pozytywnej oceny z ćwiczeń i w takim przypadku nie jest również możliwe przystąpienie do egzaminu.

Ocena formująca

F1 Kolokwium

F2 Zadanie tablicowe

F3 Sprawozdanie z ćwiczenia laboratoryjnego

Ocena podsumowująca

P1 Egzamin pisemny

P2 Egzamin ustny

Warunki zaliczenia przedmiotu

W1 W przypadku uruchomienia e-kursu do przedmiotu np. na platformie Moodle , warunkiem koniecznym zaliczenie jest aktywne udział w e-kursie.

W2 W przypadku gdy podczas zajęć są zadawane projekty/sprawozdania/zadania, wrunkiem koniecznym oddanie projektu/sprawozdania/zadania we wskazanym na zajęciach terminie. Niespełnienie tego warunku uniemożliwia uzyskanie pozytywnej oceny z ćwiczeń i w takim przypadku nie jest również możliwe przystąpienie do egzaminu.

Kryteria oceny

Efekt kształcenia 1	
Na ocenę 2.0	Student nie oddał wszystkich zadań/sprawozdań/projektów lub student nie uzyskał pozytywnej oceny ze wszystkich zadań/sprawozdań/projektów lub student nie uczestniczy aktywnie w e-kursie (tylko w przypadku uruchomienia e-kursu) lub student nie zna elementarnych pojęć, twierdzeń i algorytmów teorii grafów i uzyskał z egzaminu mniej niż 50% punktów.
Na ocenę 3.0	Student aktywnie uczestniczy w e-kursie (tylko w przypadku uruchomienia e-kursu) i oddał wszystkie zadania/sprawozdanie/projekty we wskazanym podczas zajęć terminie i uzyskał z nich ocenę pozytywną i student zna elementarne pojęcia, twierdzenia i algorytmy teorii grafów w stopniu dostatecznym, tzn. uzyskał od 50 % do 59 % punktów z egzaminu.
Na ocenę 3.5	Student spełnia warunki uzyskania oceny 3.0 i zna elementarne pojęcia, twierdzenia i algorytmy teorii grafów w stopniu dość dobrym, tzn. uzyskał od 60 % do 69 % punktów z egzaminu.
Na ocenę 4.0	Student spełnia warunki uzyskania oceny 3.0 i zna elementarne pojęcia, twierdzenia i algorytmy teorii grafów w stopniu dobrym, tzn. uzyskał od 70 % do 79 % punktów z egzaminu.
Na ocenę 4.5	Student spełnia warunki uzyskania oceny 3.0 i zna elementarne pojęcia, twierdzenia i algorytmy teorii grafów w stopniu ponad dobrym, tzn. uzyskał od 80 % do 89 % punktów z egzaminu.
Na ocenę 5.0	Student spełnia warunki uzyskania oceny 3.0 i t zna elementarne pojęcia, twierdzenia i algorytmy teorii grafów w stopniu bardzo dobrym, tzn. uzyskał od 90 % do 100 % punktów z egzaminu.
Efekt kształcenia 2	
Na ocenę 2.0	Student nie oddał wszystkich zadań/sprawozdań/projektów lub student nie uzyskał pozytywnej oceny ze wszystkich zadań/sprawozdań/projektów lub student nie uczestniczy aktywnie w e-kursie (tylko w przypadku uruchomienia e-kursu) lub student nie umie zastosować elementarnych pojęć, twierdzeń i algorytmów teorii grafów i uzyskał z egzaminu mniej niż 50% punktów.
Na ocenę 3.0	Student aktywnie uczestniczy w e-kursie (tylko w przypadku uruchomienia e-kursu) i oddał wszystkie zadania/sprawozdanie/projekty we wskazanym podczas zajęć terminie i uzyskał z nich ocenę pozytywną i student umie zastosować elementarne pojęcia, twierdzenia i algorytmy teorii grafów w stopniu dostatecznym, tzn. uzyskał od 50 % do 59 % punktów z egzaminu.
Na ocenę 3.5	Student spełnia warunki uzyskania oceny 3.0 i student umie zastosować elementarne pojęcia, twierdzenia i algorytmy teorii grafów w stopniu dość dobrym, tzn. uzyskał od 60 % do 69 % punktów z egzaminu.
Na ocenę 4.0	Student spełnia warunki uzyskania oceny 3.0 i student umie zastosować elementarne pojęcia, twierdzenia i algorytmy teorii grafów w stopniu dobrym, tzn. uzyskał od 70 % do 79 % punktów z egzaminu.

Na ocenę 4.5	Student spełnia warunki uzyskania oceny 3.0 i student umie zastosować elementarne pojęcia, twierdzenia i algorytmy teorii grafów w stopniu ponad dobrym, tzn. uzyskał od 80 % do 89 % punktów z egzaminu.
Na ocenę 5.0	Student spełnia warunki uzyskania oceny 3.0 i student umie zastosować elementarne pojęcia, twierdzenia i algorytmy teorii grafów w stopniu bardzo dobrym, tzn. uzyskał od 90 % do 100 % punktów z egzaminu.
Efekt kształcenia 3	
Na ocenę 2.0	Student nie oddał wszystkich zadań/sprawozdań/projektów lub student nie uzyskał pozytywnej oceny ze wszystkich zadań/sprawozdań/projektów lub student nie uczestniczy aktywnie w e-kursie (tylko w przypadku uruchomienia e-kursu) lub student nie zna podstawowych pojęć i algorytmów kryptografii symetrycznej i strumieniowej i uzyskał z egzaminu mniej niż 50% punktów.
Na ocenę 3.0	Student aktywnie uczestniczy w e-kursie (tylko w przypadku uruchomienia e-kursu) i oddał wszystkie zadania/sprawozdanie/projekty we wskazanym podczas zajęć terminie i uzyskał z nich ocenę pozytywną i student zna elementarne pojęcia kryptografii i algorytmy szyfrujące w stopniu dostatecznym, tzn. uzyskał od 50 % do 59 % punktów z egzaminu.
Na ocenę 3.5	Student spełnia warunki uzyskania oceny 3.0 i student zna elementarne pojęcia kryptografii i algorytmy szyfrujące w stopniu dość dobrym, tzn. uzyskał od 60 % do 69 % punktów z egzaminu.
Na ocenę 4.0	Student spełnia warunki uzyskania oceny 3.0 i student zna elementarne pojęcia kryptografii i algorytmy szyfrujące w stopniu dobrym, tzn. uzyskał od 70 % do 79 % punktów z egzaminu.
Na ocenę 4.5	Student spełnia warunki uzyskania oceny 3.0 i student zna elementarne pojęcia kryptografii i algorytmy szyfrujące w stopniu ponad dobrym, tzn. uzyskał od 80 % do 89 % punktów z egzaminu.
Na ocenę 5.0	Student spełnia warunki uzyskania oceny 3.0 i student zna elementarne pojęcia kryptografii i algorytmy szyfrujące w stopniu bardzo dobrym, tzn. uzyskał od 90 % do 100 % punktów z egzaminu.
Efekt kształcenia 4	
Na ocenę 2.0	Student nie oddał wszystkich zadań/sprawozdań/projektów lub student nie uzyskał pozytywnej oceny ze wszystkich zadań/sprawozdań/projektów lub student nie uczestniczy aktywnie w e-kursie (tylko w przypadku uruchomienia e-kursu) lub student nie umie zastosować podstawowych pojęć i algorytmów kryptografii symetrycznej i strumieniowej i uzyskał z egzaminu mniej niż 50% punktów.
Na ocenę 3.0	Student aktywnie uczestniczy w e-kursie (tylko w przypadku uruchomienia e-kursu) i oddał wszystkie zadania/sprawozdanie/projekty we wskazanym podczas zajęć terminie i uzyskał z nich ocenę pozytywną i student umie zastosować elementarne pojęcia kryptografii i algorytmy szyfrujące w stopniu dostatecznym, tzn. uzyskał od 50 % do 59 % punktów z egzaminu.

Na ocenę 3.5	Student spełnia warunki uzyskania oceny 3.0 i student umie zastosować elementarne pojęcia kryptografii i algorytmy szyfrujące w stopniu dość dobrym, tzn. uzyskał od 60 % do 69 % punktów z egzaminu.
Na ocenę 4.0	Student spełnia warunki uzyskania oceny 3.0 i student umie zastosować elementarne pojęcia kryptografii i algorytmy szyfrujące w stopniu dobrym, tzn. uzyskał od 70 % do 79 % punktów z egzaminu.
Na ocenę 4.5	Student spełnia warunki uzyskania oceny 3.0 i student umie zastosować elementarne pojęcia kryptografii i algorytmy szyfrujące w stopniu ponad dobrym, tzn. uzyskał od 80 % do 89 % punktów z egzaminu.
Na ocenę 5.0	Student spełnia warunki uzyskania oceny 3.0 i student umie zastosować elementarne pojęcia kryptografii i algorytmy szyfrujące w stopniu bardzo dobrym, tzn. uzyskał od 90 % do 100 % punktów z egzaminu.
Efekt kształcenia 5	
Na ocenę 2.0	Student nie wykazał umiejętności, o których mowa w kryterium na ocenę 3.
Na ocenę 3.0	Student potrafi formułować poprawne krótkie precyzyjne i jasne pytania ustne dotyczące rozważanych problemów.
Na ocenę 3.5	Student spełnia kryterium na ocenę 3 i potrafi formułować poprawne krótkie precyzyjne i jasne wypowiedzi ustne zawierające rozumowania i rozwiązania przykładowych problemów.
Na ocenę 4.0	Student spełnia kryterium na ocenę 3.5 i uczestniczy w dyskusjach nad omawianymi problemami.
Na ocenę 4.5	Student spełnia kryterium na ocenę 4 i potrafi formułować ścisłe i zrozumiałe dla innych dłuższe wypowiedzi ustne dotyczące rozważanych problemów i potrafi przekazywać swoje pomysły.
Na ocenę 5.0	Student spełnia kryterium na ocenę 4.5 oraz jest bardzo aktywny podczas zajęć, potrafi przedstawić dłuższe rozumowanie i ma nieszablonowe pomysły dotyczące omawianych problemów.

10 Macierz realizacji przedmiotu

Efekt kształcenia	Odniesienie danego efektu do szczegółowych efektów zdefiniowanych dla programu	Cele przedmiotu	Treści programowe	Narzędzia dydaktyczne	Sposoby oceny
EK1	I1_W01	Cel 1	L4 L5 L6 L7 W1 W2 W3 W4 W5 W6 W7 W8 W9	N1 N2 N3	F1 F2 F3 P1 P2

Efekt kształcenia	Odniesienie danego efektu do szczegółowych efektów zdefiniowanych dla programu	Cele przedmiotu	Treści programowe	Narzędzia dydaktyczne	Sposoby oceny
EK2	I1_U06b	Cel 1	C1 C2 C3 C4 C5 C6 C7 C8 C9 L4 L5 L6 L7 W1 W2 W3 W4 W5 W6 W7 W8 W9	N1 N2 N3	F1 F2 F3 P1 P2
EK3	I1_W01	Cel 1	W10 W11 W12 W13 W14	N1 N2	F1 F2 P1 P2
EK4	I1_U06b	Cel 1	C10 C11 C12 L1 L2 L3 L4 W10 W11 W12 W13 W14	N1 N2 N3	F1 F2 F3 P1 P2
EK5	I1_K01 I1_K02 I1_K03 I1_K04 I1_K05 I1_K06	Cel 1	C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 C11 C12	N2 N3	F2 F3

11 Wykaz literatury

Literatura podstawowa

[1] V. Bryant — *Aspekty kombinatoryki*, Warszawa, 2007, WNT

[2] S. Dasgupta, Ch. Papadimitriou, U. Vazirani — *Algorytmy*, Warszawa, 2010, PWN

[3] R. Graham, D. Knuth, O. Patashnik — *Matematyka konkretna*, Warszawa, 2011, PWN

[4] R. P. Grimaldi — *Discrete and combinational mathematics : an applied introduction*, Boston, 2003, Addison-Wesley

[5] A. Menezes, P. C. van Oorschot, S. A. Vanstone — *Kryptografia stosowana*, Warszawa, 2005, WNT

[6] K.A Ross, Ch.R.B. Wright — *Matematyka dyskretna*, Warszawa, 2011, PWN

Literatura uzupełniająca

[1] W. Lipski, W. Marek — *Wprowadzenie do kombinatoryki*, Warszawa, 1983, Pol. Akad. Nauk. Inst. Podstaw Informatyki

[2] Pod redakcją M. Kubale — *Optymalizacja dyskretna : modele i metody kolorowania grafów*, Warszawa, 2002, WNT

[3] E. M. Reingold, J. Nievergelt, N. Deo — *Algorytmy kombinatoryczne*, Warszawa, 1985, PWN

[4] B. Schneier — *Kryptografia dla praktyków : protokoły, algorytmy i programy źródłowe w języku C*, Warszawa, 2002, WNT

12 Informacje o nauczycielach akademickich

Osoba odpowiedzialna za kartę

dr Grzegorz Gancarzewicz (kontakt: grzegorz.gancarzewicz@pk.edu.pl)

Osoby prowadzące przedmiot

1 dr Grzegorz Gancarzewicz (kontakt: gancarz@pk.edu.pl)

13 Zatwierdzenie karty przedmiotu do realizacji

(miejscowość, data) (odpowiedzialny za przedmiot) (dziekan)

Przyjmuję do realizacji (data i podpisy osób prowadzących przedmiot)

. . . . . .