

POLITECHNIKA KRAKOWSKA IM. TADEUSZA KOŚCIUSZKI

KARTA PRZEDMIOTU

obowiązuje studentów rozpoczynających studia w roku akademickim 2014/2015

Wydział Inżynierii Elektrycznej i Komputerowej

Kierunek studiów: Informatyka

Profil: Ogólnoakademicki

Forma studiów: stacjonarne

Kod kierunku: Info

Stopień studiów: I

Specjalności: bez specjalności

1 INFORMACJE O PRZEDMIOCIE

NAZWA PRZEDMIOTU	Matematyka dyskretna
NAZWA PRZEDMIOTU W JĘZYKU ANGIELSKIM	Discrete Mathematics
KOD PRZEDMIOTU	WIEiK INFOR oIS PP8 14/15
KATEGORIA PRZEDMIOTU	Przedmioty podstawowe
LICZBA PUNKTÓW ECTS	5.00
SEMESTRY	2

2 RODZAJ ZAJĘĆ, LICZBA GODZIN W PLANIE STUDIÓW

SEMESTR	WYKŁADY	ĆWICZENIA	LABORATORIA	LABORATORIA KOMPUTERO- WE	PROJEKTY	
2	30	30	0	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 Analiza matematyczna i algebra liniowa

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 sprawdzenia 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 kryptografii symetrycznej i strumieniowej.

EK4 Umiejętności Umiejętność szyfrowania i deszyfrowania łańcuchów danych, generowanie i sprawdzenie autentyczności podpisu cyfrowego.

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

WYKŁADY		
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
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	2
W10	Arytmetyka liczb całkowitych: podzielność, NWD, NWW, liczby pierwsze, algorytm Euklidesa rozkład na czynniki pierwsze, równania diofantyczne	2

WYKŁADY		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
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.	2
W14	Kryptografia: podpis cyfrowy	2

ĆWICZENIA		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
C1	Rozwiązywanie zadań dotyczących indukcji matematycznej oraz rekurencji.	1
C2	Rozwiązywanie zadań dotyczących zasady szufladkowej Dirichleta, zasady włączania-wyłączania i kombinatoryki.	2
C3	Rozwiązywanie zadań dotyczących funkcji tworzących.	2
C4	Rozwiązywanie zadań dotyczących podstawowych pojęć teorii grafów. Analiza przykładów grafów i ich własności.	2
C5	Rozwiązywanie zadań dotyczących dróg i cykli Eulera oraz cykli Hamiltona w grafach.	4
C6	Rozwiązywanie zadań dotyczących drzew i algorytmów Prima i Kruskala.	2
C7	Rozwiązywanie zadań dotyczących grafów skierowanych oraz algorytmu Dijkstry i algorytmu Bellmana-Forda.	4
C8	Rozwiązywanie zadań dotyczących grafów dwudzielnych, twierdzenie Halla i analiza problemów przepływu w sieciach.	2
C9	Rozwiązywanie zadań dotyczących kolorowania grafów.	2
C10	Rozwiązywanie zadań dotyczących arytmetyki liczb całkowitych, twierdzenia Fermata, twierdzenia Eulera i chińskiego twierdzenia o resztach oraz i rozwiązywanie równań diofantycznych.	3
C11	Rozwiązywanie zadań dotyczących algorytmu RSA, ElGamala, algorytmu Diffiego-Hellmana.	4
C12	Rozwiązywanie zadań dotyczących szyfrowania strumieniowego.	1
C13	Rozwiązywanie zadań dotyczących podpisu cyfrowego.	1

7 NARZĘDZIA DYDAKTYCZNE

N1 Wykłady

N2 Zadania tablicowe

8 OBCIĄŻENIE PRACĄ STUDENTA

FORMA AKTYWNOŚCI	ŚREDNIA LICZBA GODZIN NA ZREALIZOWANIE AKTYWNOŚCI
Godziny kontaktowe z nauczycielem akademickim, w tym:	
Godziny wynikające z planu studiów	0
Konsultacje przedmiotowe	0
Egzaminy i zaliczenia w sesji	4
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	86
Opracowanie wyników	0
Przygotowanie raportu, projektu, prezentacji, dyskusji	0
SUMARYCZNA LICZBA GODZIN DLA PRZEDMIOTU WYNIKAJĄCA Z CAŁEGO NAKŁADU PRACY STUDENTA	90
SUMARYCZNA LICZBA PUNKTÓW ECTS DLA PRZEDMIOTU	5.00

9 SPOSOBY OCENY

OCENA FORMUJĄCA

F1 Kolokwium

F2 Zadanie tablicowe

OCENA PODSUMOWUJĄCA

P1 Egzamin pisemny

P2 Egzamin ustny

KRYTERIA OCENY

EFEKT KSZTAŁCENIA 1	
NA OCENĘ 2.0	Student nie zna elementarnych pojęć, twierdzeń i algorytmów teorii grafów i uzyskał z egzaminu mniej niż 50% punktów.

NA OCENĘ 3.0	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 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 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 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 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 umie zastosować elementarnych pojęć, twierdzeń i algorytmów teorii grafów i uzyskał z egzaminu mniej niż 50% punktów.
NA OCENĘ 3.0	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 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 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 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 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 zna podstawowych pojęć i algorytmów kryptografii symetrycznej i strumieniowej i uzyskał z egzaminu mniej niż 50% punktów.
NA OCENĘ 3.0	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 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 zna elementarne pojęcia kryptografii i algorytmy szyfrujące w stopniu dobrym, tzn. uzyskał od 70 % do 79 % punktów z egzaminu.
NA OCENĘ 4.5	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 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 umie zastosować podstawowych pojęć i algorytmów kryptografii symetrycznej i strumieniowej i uzyskał z egzaminu mniej niż 50% punktów.
NA OCENĘ 3.0	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 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 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 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 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 ściśle 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	K_W03, K_W08	Cel 1	W1 W2 W3 W4 W5 W6 W7 W8 W9	N1 N2	F1 F2 P1 P2
EK2	K_U09	Cel 1	W1 W2 W3 W4 W5 W6 W7 W8 W9 C1 C2 C3 C4 C5 C6 C7 C8 C9	N1 N2	F1 F2
EK3	K_W01, K_W12	Cel 1	W10 W11 W12 W13 W14	N1 N2	F1 F2 P1 P2
EK4	K_U14, K_U16	Cel 1	W10 W11 W12 W13 W14 C10 C11 C12 C13	N1 N2	F1 F2 P1 P2
EK5	K_W01, K_W03, K_W08, K_W12, K_U09, K_U14, K_U16	Cel 1	C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 C11 C12 C13	N2	F2

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 combinatorial 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)

.....