

POLITECHNIKA KRAKOWSKA IM. TADEUSZA KOŚCIUSZKI

KARTA PRZEDMIOTU

obowiązuje studentów rozpoczynających studia w roku akademickim 2015/2016

Wydział Fizyki, Matematyki i Informatyki

Kierunek studiów: Matematyka

Profil: Ogólnoakademicki

Forma studiów: stacjonarne

Kod kierunku: M

Stopień studiów: II

Specjalności: Modelowanie matematyczne

1 INFORMACJE O PRZEDMIOCIE

NAZWA PRZEDMIOTU	Podstawy kryptografii i wybrane zagadnienia matematyki dyskretnej
NAZWA PRZEDMIOTU W JĘZYKU ANGIELSKIM	Fundamentals of cryptography and selected topics in discrete mathematics
KOD PRZEDMIOTU	WFMiI M oIIS C2 15/16
KATEGORIA PRZEDMIOTU	Przedmioty kierunkowe
LICZBA PUNKTÓW ECTS	5.00
SEMESTRY	4

2 RODZAJ ZAJĘĆ, LICZBA GODZIN W PLANIE STUDIÓW

SEMESTR	WYKŁAD	ĆWICZENIA	LABORATORIUM	LABORATORIUM KOMPUTERO- WE	SEMINARIUM	PROJEKT
4	30	30	0	0	0	0

3 CELE PRZEDMIOTU

Cel 1 Celem przedmiotu jest przedstawienie wybranych zagadnień kryptografii oraz teorii grafów i niektórych ich zastosowań.

4 WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

- 1 Znajomość podstaw arytmetyki, grup skończonych, grup cyklicznych i logiki matematycznej oraz zaliczenie przedmiotu: Teoria grafów.

5 EFEKTY KSZTAŁCENIA

EK1 Wiedza Znajomość podstawowych pojęć i algorytmów kryptografii symetrycznej i strumieniowej.

EK2 Umiejętności Umiejętność szyfrowania i deszyfrowania łańcuchów danych, generowanie i sprawdzenie autentyczności podpisu cyfrowego.

EK3 Wiedza Znajomość podstawowych pojęć, twierdzeń i algorytmów dotyczących drzew i lasów, znajomość podstawowych pojęć i twierdzeń teorii ekstremalnej teorii grafów oraz znajomość podstawowych pojęć i twierdzeń i dotyczących teorii Ramsaya i problemu triangulacji.

EK4 Umiejętności Umiejętność zastosowania algorytmów do wyznaczania w grafach dróg (w szczególności zastosowanie algorytmów trasowania) i podgrafów spinających. Umiejętność wykorzystania techniki domknięcia w dowodach.

EK5 Kompetencje społeczne Student posiada umiejętność jasnego formułowania pytań, czynnego udziału w dyskusji i pracy grupie nad niezbyt trudnymi zadaniami praktycznymi oraz umie dobrze przygotować i atrakcyjnie wygłosić referat.

6 TREŚCI PROGRAMOWE

ĆWICZENIA		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
C1	Przypomnienie podstawowych własności grafów i rozwiązywanie zadań dotyczących podstawowych problemów teorii grafów.	2
C2	Rozwiązywanie zadań dotyczących algorytmów szyfrowania.	4
C3	Rozwiązywanie zadań dotyczących protokołów uzgadniania kluczy i algorytmów podpisu cyfrowego.	3
C4	Rozwiązywanie zadań dotyczących problemu dzielenie sekretu.	2
C5	Rozwiązywanie zadań dotyczących drzew i lasów (zastosowanie wybranych algorytmów dla drzew).	2
C6	Rozwiązywanie zadań dotyczących liczby Ramsey'a.	2
C7	Rozwiązywanie zadań dotyczących triangulacji.	4
C8	Zadania i przykłady związane z problemami ekstremalnymi w teorii grafów.	3
C9	Przykłady wybranych metod dowodzenia własności grafów.	6
C10	Rozwiązywanie zadań dotyczących grafów skierowanych i turniejów.	2

WYKŁAD		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
W1	Kryptografia: podstawowe pojęcia i problemy kryptografii symetrycznej i asymetrycznej oraz algorytmy strumieniowe i blokowe.	4
W2	Analiza bezpieczeństwa klasycznych algorytmów symetrycznych na przykładzie algorytmu RSA oraz IDEA.	2
W3	Protokoły uzgadniania kluczy (algorytm Diffiego-Hellmana) Mechanizm podpisu cyfrowego na przykładzie algorytmu DSA.	3
W4	Funkcje skrótu, funkcje jednokierunkowe.	1
W5	Dowody o wiedzy zerowej i dzielenie sekretu.	2
W6	Drzewa i lasy (drzewa jako przestrzenie metryczne, drzewa z korzeniem, drzewa binarne i dendryty)	3
W7	Teoria Ramseya (klasyczne i nieklasyczne liczby Ramseya oraz wybrane przykłady ich zastosowań)	3
W8	Triangulacje wielokąta i problem ochrony galerii sztuki oraz triangulacje Delaunaya	3
W9	Problemy ekstremalne w teorii grafów (Problemy ekstremalne dla ścieżek i cykli,)	3
W10	Technika domknięcia grafów.	2
W11	Grafy skierowane i turnieje	2
W12	Porządki Częściowe i twierdzenie Dilworth'a	2

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	60
Konsultacje przedmiotowe	0
Egzaminy i zaliczenia w sesji	2
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	88
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

OCENA FORMUJĄCA

F1 Zadanie tablicowe

OCENA PODSUMOWUJĄCA

P1 Zaliczenie ustne

KRYTERIA OCENY

EFEKT KSZTAŁCENIA 1	
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 ponad dostatecznym, 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 2	
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 ponad dostatecznym, 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 3	
NA OCENĘ 2.0	Student nie zna podstawowych pojęć, twierdzeń i algorytmów dotyczących drzew i lasów oraz podstawowych pojęć i twierdzeń teorii ekstremalnej teorii grafów, teorii Ramsaya i problemu triangulacji i uzyskał z egzaminu mniej niż 50% punktów.
NA OCENĘ 3.0	Student zna podstawowe pojęcia, twierdzenia i algorytmy dotyczące drzew i lasów oraz podstawowe pojęcia i twierdzenia teorii ekstremalnej teorii grafów, teorii Ramsaya i problemu triangulacji w stopniu dostatecznym, tzn. uzyskał od 50 % do 59 % punktów z egzaminu.
NA OCENĘ 3.5	Student zna podstawowe pojęcia, twierdzenia i algorytmy dotyczące drzew i lasów oraz podstawowe pojęcia i twierdzenia teorii ekstremalnej teorii grafów, teorii Ramsaya i problemu triangulacji w stopniu ponad dostatecznym, tzn. uzyskał od 60 % do 69 % punktów z egzaminu.
NA OCENĘ 4.0	Student zna podstawowe pojęcia, twierdzenia i algorytmy dotyczące drzew i lasów oraz podstawowe pojęcia i twierdzenia teorii ekstremalnej teorii grafów, teorii Ramsaya i problemu triangulacji w stopniu dobrym, tzn. uzyskał od 70 % do 79 % punktów z egzaminu.
NA OCENĘ 4.5	Student zna podstawowe pojęcia, twierdzenia i algorytmy dotyczące drzew i lasów oraz podstawowe pojęcia i twierdzenia teorii ekstremalnej teorii grafów, teorii Ramsaya i problemu triangulacji w stopniu ponad dobrym, tzn. uzyskał od 80 % do 89 % punktów z egzaminu.

NA OCENĘ 5.0	Student zna podstawowe pojęcia, twierdzenia i algorytmy dotyczące drzew i lasów oraz podstawowe pojęcia i twierdzenia teorii ekstremalnej teorii grafów, teorii Ramsaya i problemu triangulacji 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, twierdzeń i algorytmów dotyczących drzew i lasów oraz podstawowych pojęć i twierdzeń teorii ekstremalnej teorii grafów, teorii Ramsaya i problemu triangulacji i uzyskał z egzaminu mniej niż 50% punktów.
NA OCENĘ 3.0	Student umie zastosować podstawowe pojęcia, twierdzenia i algorytmy dotyczące drzew i lasów oraz podstawowe pojęcia i twierdzenia teorii ekstremalnej teorii grafów, teorii Ramsaya i problemu triangulacji w stopniu dostatecznym, tzn. uzyskał od 50 % do 59 % punktów z egzaminu.
NA OCENĘ 3.5	Student umie zastosować podstawowe pojęcia, twierdzenia i algorytmy dotyczące drzew i lasów oraz podstawowe pojęcia i twierdzenia teorii ekstremalnej teorii grafów, teorii Ramsaya i problemu triangulacji w stopniu ponad dostatecznym, tzn. uzyskał od 60 % do 69 % punktów z egzaminu.
NA OCENĘ 4.0	Student umie zastosować podstawowe pojęcia, twierdzenia i algorytmy dotyczące drzew i lasów oraz podstawowe pojęcia i twierdzenia teorii ekstremalnej teorii grafów, teorii Ramsaya i problemu triangulacji w stopniu dobrym, tzn. uzyskał od 70 % do 79 % punktów z egzaminu.
NA OCENĘ 4.5	Student umie zastosować podstawowe pojęcia, twierdzenia i algorytmy dotyczące drzew i lasów oraz podstawowe pojęcia i twierdzenia teorii ekstremalnej teorii grafów, teorii Ramsaya i problemu triangulacji w stopniu ponad dobrym, tzn. uzyskał od 80 % do 89 % punktów z egzaminu.
NA OCENĘ 5.0	Student umie zastosować podstawowe pojęcia, twierdzenia i algorytmy dotyczące drzew i lasów oraz podstawowe pojęcia i twierdzenia teorii ekstremalnej teorii grafów, teorii Ramsaya i problemu triangulacji 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	Na ocenę 4 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_W11	Cel 1	W1 W2 W3 W4 W5	N1 N2	F1 P1
EK2	K_W11 K_U13 K_U16	Cel 1	C2 C3 C4 W1 W2 W3 W4 W5	N1 N2	F1 P1
EK3	K_W02 K_W03 K_W11 K_U13	Cel 1	W6 W7 W8 W9 W10 W11	N1 N2	F1 P1
EK4	K_U13	Cel 1	C1 C5 C6 C7 C8 C9 C10 W6 W7 W8 W9 W10 W11	N1 N2	F1 P1
EK5	K_K02 K_K03 K_K04 K_K05 K_K06 K_K07	Cel 1	C1 C2 C3 C4 C5 C6 C7 C8 C9 C10	N2	F1

11 WYKAZ LITERATURY

LITERATURA PODSTAWOWA

- [1] | M. de Berg, M. van Kreveld, M. Overmars, O. Schwarzkopf — *Geometria obliczeniowa : algorytmy i zastosowania*, Warszawa, 2007, WNT
- [2] | V. Bryant — *Aspekty kombinatoryki*, Warszawa, 2007, WNT
- [3] | S. Dasgupta, Ch. Papadimitriou, U. Vazirani — *Algorytmy*, Warszawa, 2010, PWN
- [4] | R. Graham, D. Knuth, O. Patashnik — *Matematyka konkretna*, Warszawa, 2011, PWN
- [5] | R. P. Grimaldi — *Discrete and combinatorial mathematics : an applied introduction*, Boston, 1999, Addison-Wesley
- [6] | A. Menezes, P. C. van Oorschot, S. A. Vanstone — *Kryptografia stosowana*, Warszawa, 2005, WNT

- [7] | K.A. Ross, Ch.R.B. Wright — *Matematyka dyskretna*, Warszawa, 2011, PWN
- [8] | E.R. Scheinerman — *Mathematics - Discrete Introduction*, Florence, 2000, Brooks/Cole

LITERATURA UZUPEŁNIAJĄCA

- [1] | M. Aigner, G. M. Ziegler — *Dowody z książki*, Warszawa, 2004, PWN
- [2] | W. Lipski, W. Marek — *Wprowadzenie do kombinatoryki*, Warszawa, 1983, Pol. Akad. Nauk. Inst. Podstaw Informatyki
- [3] | Pod redakcją M. Kubale — *Optymalizacja dyskretna : modele i metody kolorowania grafów*, Warszawa, 2002, WNT
- [4] | R. L. Graham, M. Grötschel, L. Lovsz — *Handbook of combinatorics vol. 1, 2*, Amsterdam, 1995, Elsevier
- [5] | 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: gancarz@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)

.....