Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

obowiązuje studentów rozpoczynających studia w roku akademickim 2012/2013

Wydział Fizyki, Matematyki i Informatyki

Kierunek studiów: Matematyka

Profil: Ogólnoakademicki

Forma sudiów: 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	
Kod przedmiotu	WFMiI M oIIS C2 12/13
Kategoria przedmiotu	Przedmioty kierunkowe
Liczba punktów ECTS	5.00
Semestry	4

2 Rodzaj zajęć, liczba godzin w planie studiów

Semestr	Wykład	Ćwiczenia	Laboratorium	Laboratorium komputerowe	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

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 i podpis cyfrowy.	2
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)	2
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

Wykład		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
W10	Technika domknięcia grafów.	2
W11	Grafy skierowane i turnieje	2
W12	Porządki częściowe i twierdzenie Dilworth'a	2

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 Ramseya.	2
C7	Rozwiązywanie zadań dotyczących triangulacji.	2
C8	Zadania i przykłady związane z problemami ekstremalnymi w teorii grafów.	5
C9	Przykłady wybranych metod dowodzenia własności grafów.	6
C10	Rozwiązywanie zadań dotyczących grafów skierowanych i turniejów.	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	0
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	**90**
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 podczas zaliczenia mniej niż 50 % punktów.
Na ocenę 3.0	Student zna elementarne pojęcia kryptografii i algorytmy szyfrujące wraz z dowodami poprawności w stopniu dostatecznym, tzn. uzyskał podczas zaliczenia od 50 % do 59 % punktów.
Na ocenę 3.5	Student zna elementarne pojęcia kryptografii i algorytmy szyfrujące wraz z dowodami poprawności w stopniu ponad dostatecznym, tzn. uzyskał podczas zaliczenia od 60 % do 69 % punktów.

Na ocenę 4.0	Student zna elementarne pojęcia kryptografii i algorytmy szyfrujące wraz z dowodami poprawności w stopniu dobrym, tzn. uzyskał podczas zaliczenia od 70 % do 79 % punktów.
Na ocenę 4.5	Student zna elementarne pojęcia kryptografii i algorytmy szyfrujące wraz z dowodami poprawności w stopniu ponad dobrym, tzn. uzyskał podczas zaliczenia od 80 % do 89 % punktów.
Na ocenę 5.0	Student zna elementarne pojęcia kryptografii i algorytmy szyfrujące wraz z dowodami poprawności w stopniu bardzo dobrym, tzn. uzyskał podczas zaliczenia od 90 % do 100 % punktów.
Efekt kształcenia 2	
Na ocenę 2.0	Student nie umie zastosować podstawowych pojęć i algorytmów kryptografii symetrycznej i strumieniowej i uzyskał podczas zaliczenia mniej niż 50% punktów.
Na ocenę 3.0	Student umie zastosować elementarne pojęcia kryptografii i algorytmy szyfrujące w stopniu dostatecznym, tzn. uzyskał podczas zaliczenia od 50 % do 59 % punktów.
Na ocenę 3.5	Student umie zastosować elementarne pojęcia kryptografii i algorytmy szyfrujące w stopniu ponad dostatecznym, tzn. uzyskał podczas zaliczenia od 60 % do 69 % punktów.
Na ocenę 4.0	Student umie zastosować elementarne pojęcia kryptografii i algorytmy szyfrujące w stopniu dobrym, tzn. uzyskał podczas zaliczenia od 70 % do 79 % punktów.
Na ocenę 4.5	Student umie zastosować elementarne pojęcia kryptografii i algorytmy szyfrujące w stopniu ponad dobrym, tzn. uzyskał podczas zaliczenia od 80 % do 89 % punktów.
Na ocenę 5.0	Student umie zastosować elementarne pojęcia kryptografii i algorytmy szyfrujące w stopniu bardzo dobrym, tzn. uzyskał podczas zaliczenia od 90 % do 100 % punktów.
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 podczas zaliczenia mniej niż 50% punktów.
Na ocenę 3.0	Student zna podstawowe pojęcia, twierdzenia i algorytmy wraz z ich dowodami dotyczące drzew i lasów oraz podstawowe pojęcia i twierdzenia teorii ekstremalnej teorii grafów, teorii Ramsaya i problemu triangulacji wraz z ich dowodami w stopniu dostatecznym, tzn. uzyskał podczas zaliczenia od 50 % do 59 % punktów.
Na ocenę 3.5	Student zna podstawowe pojęcia, twierdzenia i algorytmy wraz z ich dowodami dotyczące drzew i lasów oraz podstawowe pojęcia i twierdzenia teorii ekstremalnej teorii grafów, teorii Ramsaya i problemu triangulacji wraz z ich dowodami w stopniu ponad dostatecznym, tzn. uzyskał podczas zaliczenia od 60 % do 69 % punktów.

Na ocenę 4.0	Student zna podstawowe pojęcia, twierdzenia i algorytmy wraz z ich dowodami dotyczące drzew i lasów oraz podstawowe pojęcia i twierdzenia teorii ekstremalnej teorii grafów, teorii Ramsaya i problemu triangulacji wraz z ich dowodami w stopniu dobrym, tzn. uzyskał podczas zaliczenia od 70 % do 79 % punktów.
Na ocenę 4.5	Student zna podstawowe pojęcia, twierdzenia i algorytmy wraz z ich dowodami dotyczące drzew i lasów oraz podstawowe pojęcia i twierdzenia teorii ekstremalnej teorii grafów, teorii Ramsaya i problemu triangulacji wraz z ich dowodami w stopniu ponad dobrym, tzn. uzyskał podczas zaliczenia od 80 % do 89 % punktów.
Na ocenę 5.0	Student zna podstawowe pojęcia, twierdzenia i algorytmy wraz z ich dowodami dotyczące drzew i lasów oraz podstawowe pojęcia i twierdzenia teorii ekstremalnej teorii grafów, teorii Ramsaya i problemu triangulacji wraz z ich dowodami w stopniu bardzo dobrym, tzn. uzyskał podczas zaliczenia od 90 % do 100 % punktów.
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 podczas zaliczenia 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 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	K_W01, K_W02, K_W03, K_W04, K_W05, K_W06, K_W07, K_W11	Cel 1	W1 W2 W3 W4 W5	N1 N2	F1 P1
EK2	K_U01, K_U02, K_U03, K_U04, K_U13, K_U14, K_U19	Cel 1	W1 W2 W3 W4 W5 C2 C3 C4	N1 N2	F1 P1
EK3	K_W01, K_W02, K_W03, K_W04, K_W05, K_W06, K_W07, K_W11	Cel 1	W6 W7 W8 W9 W10 W11 W12	N1 N2	F1 P1

Efekt kształcenia	Odniesienie danego efektu do szczegółowych efektów zdefiniowanych dla programu	Cele przedmiotu	Treści programowe	Narzędzia dydaktyczne	Sposoby oceny
EK4	K_U01, K_U02, K_U03, K_U04, K_U14, K_U15	Cel 1	W6 W7 W8 W9 W10 W11 C1 C5 C6 C7 C8 C9 C10	N1 N2	F1 P1
EK5	K_K01, 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 combinational 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 księgi*, 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)

. . . . . .