Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

obowiązuje studentów rozpoczynających studia w roku akademickim 2019/2020

Wydział Informatyki i Telekomunikacji

Kierunek studiów: Matematyka

Profil: Ogólnoakademicki

Forma sudiów: stacjonarne

Kod kierunku: M

Stopień studiów: II

Specjalności: Modelowanie matematyczne

1 Informacje o przedmiocie

Nazwa przedmiotu	Matematyczne podstawy kryptologii
Nazwa przedmiotu w języku angielskim	Mathematical foundation of cryptology
Kod przedmiotu	WIiT M oIIS C3 19/20
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 Nayczyć studentów matematycznych podstaw i metod współczesnej kryptologii

4 Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1 Algebra liniowa z geometrią analityczną, podstawy algebry abstrakcyjnej, elementy analizy matematycznej, elementy teorii liczb oraz logika i matematyka dyskretna

5 Efekty kształcenia

EK1 Wiedza Student zna podstawowe pojęcia teorii liczb, niezbędne w kryptologii.

EK2 Wiedza Student zna podstawy teorii Shannona (pojęcia oraz twierdzenia) o szyrowaniu i bezpieczeństwie informacji oraz kryptografję klasyczną, podstawy szyfrowania symetrycznego i asymetrycznego.

EK3 Kompetencje społeczne Student nie tylko wie i demonstruje jak zaszyfrować i deszyfrować informację za pomocą pewnych szyfrów klasycznych i współczesnych, lecz również potrafi precyzyjnie formulować pytania, służące pogłębieniu własnego zrozumienia danego tematu lub odnalezieniu brakujących elementów rozumowania, samodzielnie wyszukiwać informacje w literaturze, także w językach obcych.

EK4 Umiejętności Student wie i demonstruje jak zrealizować szyrowanie i deszyfrowanie za pomocfą podstawowych szyfrów.

6 Treści programowe

Wykład		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
W1	Elementy kryptologii: Ochrona danych, systemy i algorytmy kryptograficzne, własności informacyjne języka	2
W2	Elementy teorii liczb: twierdzenie o dzieleniu z resztą, podzielność, klasy reszt modulo n, rozszerzony algorytm Euklidesa, NWD, NWW, liczby względnie pierwsze, zasadnicze twierdzenie arytmetyki, twierzenie Euklidesa o liczbach pierwszych, sito Eratostenesa, funkcje arytmetyczne, twierzenia Eulera i Fermata	8
W3	Obliczeniowa i algorytmiczna teoria liczb: testy pierwszości, algorytmy faktoryzacji liczb całkowitych, logarytmy dyskretne, generowanie liczb pierwszych	4
W4	Kryptografia klasyczna: proste szyfry podstawieniowe, szyfry podstawieniowe homofoniczne, szyfry podstawieniowe wieloalfabetowe, szyfry podstawieniowe poligramowe, szyfry przestawieniowe	4
W5	Szyfry symetryczne	4
W6	Bezpieczeństwo informacji, algorytm DES	2
W7	Szyfry asymetryczne	4
W8	Podpisy cyfrowe	2

Ćwiczenia		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
C1	Wstęp do kryptologii: Ochrona danych, systemy i algorytmy kryptograficzne, własności informacyjne języka	2
C2	Ćwiczenia z podstawowych zagadnień teorii liczb: twierdzenie o dzieleniu z resztą, podzielność, klasy reszt modulo n, rozszerzony algorytm Euklidesa, NWD, NWW, liczby względnie pierwsze, zasadnicze twierdzenie arytmetyki, twierzenie Euklidesa o liczbach pierwszych, sito Eratostenesa, funkcje arytmetyczne, twierzenia Eulera i Fermata	8
C3	Testy pierwszości, algorytmy faktoryzacji liczb całkowitych, logarytmy dyskretne, generowanie liczb pierwszych	4
C4	Rozwiązywanie zadń z kryptografii klasycznej: proste szyfry podstawieniowe, szyfry podstawieniowe homofoniczne, szyfry podstawieniowe wieloalfabetowe, szyfry podstawieniowe poligramowe, szyfry przestawieniowe	4
C5	Badanie własności szyfrów symetrycznych	4
C6	Omówienie problemów związanych z bezpieczeństwem informacji, algorytm DES	2
C7	Przykłady szyfrów asymetrycznych	4
C8	Sposoby podpisów cyfrowych, przykłady	2

7 Narzędzia dydaktyczne

N1 Wykłady. W sytuacji zdalnego nauczania prowadzone są za pośrednictwem MS Teams, na żywo. e-kurs na platformie Delta PK.

N2 Praca w grupach. W sytuacji zdalnego nauczania prowadzone są za pośrednictwem MS Teams, na żywo. e-kurs na platformie Delta PK.

N3 Konsultacje

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	0
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	90
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

Aktywność w e-kursie umieszczonym na platformie Delta PK. W sytuacji zdalnego nauczania wszystkie sprawdziany prowadzone są za posrednitwem platformy MS Teams i Delta PK.

Ocena formująca

F1 Kolokwium

F2 Ćwiczenie praktyczne

Ocena podsumowująca

P1 Zaliczenie pisemne

P2 Zaliczenie ustne

Ocena aktywności bez udziału nauczyciela

B1 Ćwiczenie praktyczne

Kryteria oceny

Efekt kształcenia 1	
Na ocenę 2.0	Student nie zna podstawowe pojęcia z teorii liczb i szyfrowania, nie ilustruje ich przykładami

Na ocenę 3.0	Student zna podstawowe pojęcia z teorii liczb i szyfrowania, ilustruje ich przykładami
Na ocenę 3.5	Student zna podstawowe pojęcia z teorii liczb i szyfrowania, może formulować podstawowe zagadnienia, ilustruje ich przykładami
Na ocenę 4.0	Student zna podstawowe pojęcia z teorii liczb i szyfrowania, może udowodnić podstawowe zagadnienia, ilustruje ich przykładami
Na ocenę 4.5	Student zna podstawowe pojęcia z teorii liczb i szyfrowania, ilustruje ich przykładami, może udowodnić podstawowe zagadnienia z teorii liczb i szyfrowania i stosować ich do rozwiązywania standardowych zadań teoretycznego i praktycznego charakteru
Na ocenę 5.0	Student zna podstawowe pojęcia z teorii liczb i szyfrowania, ilustruje ich przykładami, może udowodnić podstawowe zagadnienia z teorii liczb i szyfrowania i stosować ich do rozwiązywania standardowych i niestandardowych zadań teoretycznego i praktycznego charakteru
Efekt kształcenia 2	
Na ocenę 2.0	Student nie zna podstawowe pojęcia teorii Shannona o szyfrowaniu oraz nie ilustruje ich przykładami
Na ocenę 3.0	Student zna podstawowe pojęcia teorii Shannona o szyfrowaniu oraz ilustruje ich przykładami
Na ocenę 3.5	Student zna podstawowe pojęcia i podstawowe zagadnienia teorii Shannona o szyfrowaniu, może, zilustrować prykładami oraz rozwiązywaniem zadań elementarnych
Na ocenę 4.0	Student zna podstawowe pojęcia i podstawowe zagadnienia teorii Shannona o szyfrowaniu, może udowodnić podstawowe zagadnienia, zilustrować prykładami oraz rozwiązywaniem zadań elementarnych
Na ocenę 4.5	Student zna podstawowe pojęcia i podstawowe zagadnienia teorii Shannona o szyfrowaniu, może udowodnić podstawowe zagadnienia i stosować ich do rozwiązywania standardowych zadań oraz ilustruje ich przykładami
Na ocenę 5.0	Student zna podstawowe pojęcia teorii Shannona o szyfrowaniu, może udowodnić podstawowe zagadnienia i stosować ich do rozwiązywania standardowych i niestandardowych zadań teoretycznego i praktycznego charakteru
Efekt kształcenia 3	
Na ocenę 2.0	Student nie zna ograniczenia własnej wiedzy, nie potrafi precyzyjnie formulować pytania, służące pogłębieniu własnego zrozumienia danego przedmiotu
Na ocenę 3.0	Student zna ograniczenia własnej wiedzy, potrafi precyzyjnie formulować pytania, służące pogłębieniu własnego zrozumienia danego przedmiotu
Na ocenę 3.5	Student zna podstawowe pojęcia i podstawowe zagadnienia i moze ich zilustrować
Na ocenę 4.0	Student nie tylko zna podstawowe pojęcia i podstawowe zagadnienia, moze ich zilustrować i udowodnić, rozumie konieczność systematycznej pracy

Na ocenę 4.5	Student nie tylko zna podstawowe pojęcia i podstawowe zagadnienia, moze ich zilustrować, udowodnić i rozwiazać podstawowe zadania, rozumie konieczność systematycznej pracy, potrafi samodzielnie wyszukiwać informacje w literaturze, także w językach obcych
Na ocenę 5.0	Student nie tylko zna podstawowe pojęcia i podstawowe zagadnienia, moze ich zilustrować, udowodnić i rozwiazać podstawowe i niestandardowe zadania, rozumie konieczność systematycznej pracy, potrafi samodzielnie wyszukiwać informacje w literaturze, także w językach obcych
Efekt kształcenia 4	
Na ocenę 2.0	Student nie zna podstawowe pojęcia, nie umie rozwiązać podstawowe zadania praktycznego charakteru i zilustrować podstawowe pojęcia przykładami
Na ocenę 3.0	Student zna podstawowe pojęcia, umie rozwiązać podstawowe zadania praktycznego charakteru i zilustrować podstawowe pojęcia przykładami
Na ocenę 3.5	Student zna podstawowe pojęcia i zagadnienia, umie rozwiązać podstawowe zadania praktycznego charakteru i zilustrować ich przykładami
Na ocenę 4.0	Student zna podstawowe pojęcia i zagadnienia z dowodami, umie rozwiązać podstawowe zadania praktycznego i teoretycznego charakteru i zilustrować ich przykładami
Na ocenę 4.5	Student zna podstawowe pojęcia, ich związki oraz zagadnienia z dowodami, umie rozwiązać zadania praktycznego i teoretycznego charakteru, zilustrować ich przykładami
Na ocenę 5.0	Student zna podstawowe pojęcia i podstawowe zagadnienia, ich związki oraz zagadnienia z dowodami, umie rozwiązać standerdowe i niestandardowe zadania praktycznego i teoretycznego charakteru, zilustrować ich przykładami i stosować na praktyce

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	Cel 1	W1 W2 C1 C2	N1 N2 N3	F1 F2 P1 P2
EK2	K_W01 K_W02 K_W03 K_W04 K_W05	Cel 1	W3 W4 C3 C4	N1 N2 N3	F1 F2 P1 P2

Efekt kształcenia	Odniesienie danego efektu do szczegółowych efektów zdefiniowanych dla programu	Cele przedmiotu	Treści programowe	Narzędzia dydaktyczne	Sposoby oceny
EK3	K_K01 K_K02 K_K03 K_K04 K_K05 K_K06 K_K07	Cel 1	W5 W6 C5 C6	N1 N2 N3	F1 F2 P1 P2
EK4	K_U01 K_U02 K_U03 K_U04	Cel 1	W7 W8 C7 C8	N1 N2 N3	F1 F2 P1 P2

11 Wykaz literatury

Literatura podstawowa

[1] N. Koblitz — *Wykład z teorii liczb i kryptografii*, Warszawa, 1995, WNT

[2] N. Koblitz — *Algebraiczne aspekty kryptografii*, Warszawa, 2000, WNT

[3] W. Mochnacki — *Kody korekcyjne i kryptografia*, Wracław, 1997, PolitechnikaWrocławska

[4] Song Y. Yan — *Teoria liczb w informatyce*, Warszawa, 2006, PWN

Literatura uzupełniająca

[1] J.A. Buchmann — *Wprowadzenie do kryptografii*, Warszawa, 2006, PWN

12 Informacje o nauczycielach akademickich

Osoba odpowiedzialna za kartę

prof. dr hab. Orest Artemovych (kontakt: artemo@pk.edu.pl)

Osoby prowadzące przedmiot

1 Prof. dr hab. Orest Artemovych (kontakt: artemo@usk.pk.edu.pl)

13 Zatwierdzenie karty przedmiotu do realizacji

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

Przyjmuję do realizacji (data i podpisy osób prowadzących przedmiot)

. . . . . .