Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

obowiązuje studentów rozpoczynających studia w roku akademickim 2021/2022

Wydział Informatyki i Telekomunikacji

Kierunek studiów: Matematyka

Profil: Ogólnoakademicki

Forma sudiów: stacjonarne

Kod kierunku: M

Stopień studiów: II

Specjalności: Matematyka w finansach i ekonomii

1 Informacje o przedmiocie

Nazwa przedmiotu	Matematyczne podstawy kryptologii
Nazwa przedmiotu w języku angielskim	Mathematical Foundation of Cryptology
Kod przedmiotu	WIiT M oIIS C10 21/22
Kategoria przedmiotu	Przedmioty kierunkowe
Liczba punktów ECTS	7.00
Semestry	3

2 Rodzaj zajęć, liczba godzin w planie studiów

Semestr	Wykład	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Seminarium	Projekt
3	30	30	0	0	0	0

3 Cele przedmiotu

Cel 1 Nauczyć studentów podstaw matematycznych 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, 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 szyfrowaniu i bezpieczeństwie informacji oraz kryptologię klasyczną, podstawy szyfrowania symetrycznego i asymetrycznego

EK3 Kompetencje społeczne Student nie tylko wie i demonstruje jak szyfrować i deszyfrować informacje za pomocą szyfrów klasycznych i współczesnych, lecz również potrafi precyzyjnie formułować 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 szyfrowanie i deszyfrowanie za pomocą szyfrów podstawowych

6 Treści programowe

Ćwiczenia		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
C1	Systemy i algorytmy kryptograficzne, własności informacyjne języka	2
C2	Twierdzenie o dzieleniu z resztą, klasy reszt modulo n, rozszerzony algorytm Euklidesa, NWD, NWW, liczby względnie pierwsze, liczby pierwsze, zasadnicze twierdzenie arytmetyki, sito Eratostenesa, funkcje arytmetyczne, twierdzenia Eulera i Fermata	8
C3	Testy pierwszości, logarytmy dyskretne, algorytmy faktoryzacji liczb całkowitych, generowanie liczb pierwszych	4
C4	Teoria Shannona o kodach i szyfrach, własności entropii	2
C5	Kryptologia klasyczna	2
C6	Szyfry symetryczne	4
C7	Szyfry asymetryczne	4
C8	Podpisy cyfrowe, inne zastosowania kryptografii	4

Wykład		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin

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, klasy reszt modulo n, rozszerzony algorytm Euklidesa, NWD, NWW, liczby względnie pierwsze, liczby pierwsze, zasadnicze twierdzenie arytmetyki, sito Eratostenesa, funkcje arytmetyczne, twierdzenia Eulera i Fermata	8
W3	Obliczeniowa i algorytmiczna teoria liczba, testy pierwszości, logarytmy dyskretne	4
W4	Teoria Shannona o kodach i szyfrach	2
W5	Kryptologia klasyczna	2
W6	Szyfry symetryczne	4
W7	Szyfry asymetryczne	4
W8	Podpisy cyfrowe, inne zastosowania kryptografii	4

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 (ćwiczenia). W sytuacji zdalnego nauczania prowadzone są za pośrednictwem MS Teams, na żywo.

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	30
Egzaminy i zaliczenia w sesji	15
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	75
Opracowanie wyników	30
Przygotowanie raportu, projektu, prezentacji, dyskusji	0
Sumaryczna liczba godzin dla przedmiotu wynikająca z całego nakładu pracy studenta	**210**
Sumaryczna liczba punktów ECTS dla przedmiotu	7.00

9 Sposoby oceny

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

Ocena formująca

F1 Aktywność na ćwiczeniach, obecność na zajęciach

F2 Ocena kolokwium pisemnego

Ocena podsumowująca

P1 Egzaminy pisemny i ustny

Warunki zaliczenia przedmiotu

W1 Pozytywne ocena formująca i ocena podsumowująca

Ocena aktywności bez udziału nauczyciela

B1 Test

Kryteria oceny

Efekt kształcenia 1

Na ocenę 2.0	Student nie zna podstawowych pojęć teorii liczb, niezbędnych w kryptologii
Na ocenę 3.0	Student zna podstawowe pojęcia teorii liczb, niezbędne w kryptologii, oraz ilustruje ich przykładami
Na ocenę 3.5	Student zna podstawowe pojęcia i zagadnienia teorii liczb, niezbędne w kryptologii, oraz ilustruje ich przykładami, rozwiązuje elementarne zadania
Na ocenę 4.0	Student zna podstawowe pojęcia i zagadnienia teorii liczb z dowodami, niezbędne w kryptologii, oraz ilustruje ich przykładami, rozwiązuje zadania
Na ocenę 4.5	Student zna podstawowe pojęcia i zagadnienia teorii liczb z dowodami, niezbędne w kryptologii, oraz ilustruje ich przykładami, rozwiązuje standardowe zadania teoretyczne i praktyczne
Na ocenę 5.0	Student zna podstawowe pojęcia i zagadnienia teorii liczb z dowodami, niezbędne w kryptologii, oraz ilustruje ich przykładami, rozwiązuje standardowe oraz niestandardowe zadania teoretyczne i praktyczne
Efekt kształcenia 2	
Na ocenę 2.0	Student nie zna podstaw teorii Shannona (pojęcia oraz twierdzenia) o szyfrowaniu i bezpieczeństwie informacji, nie zna podstaw kryptologii klasycznej oraz podstaw szyfrowania symetrycznego i asymetrycznego
Na ocenę 3.0	Student zna podstawowe pojęcia teorii Shannona (pojęcia oraz twierdzenia) o szyfrowaniu i bezpieczeństwie informacji oraz kryptologii klasycznej, podstawowe pojęcia o szyfrowaniu symetrycznego i asymetrycznego, ilustruje ich przykładami, rozwiązuje elementarne zadania
Na ocenę 3.5	Student zna podstawowe pojęcia i zagadnienia teorii Shannona (pojęcia oraz twierdzenia) o szyfrowaniu i bezpieczeństwie informacji oraz kryptologii klasycznej, podstawowe pojęcia i zagadnienia o szyfrowaniu symetrycznego i asymetrycznego, ilustruje ich przykładami, rozwiązuje elementarne zadania
Na ocenę 4.0	Student zna podstawowe pojęcia i zagadnienia (z dowodami i algorytmami) teorii Shannona (pojęcia oraz twierdzenia) o szyfrowaniu i bezpieczeństwie informacji oraz kryptologii klasycznej, podstawowe pojęcia i zagadnienia (z dowodami i algorytmami) o szyfrowaniu symetrycznego i asymetrycznego, ilustruje ich przykładami, rozwiązuje standardowe zadania
Na ocenę 4.5	Student zna podstawowe pojęcia i zagadnienia (z dowodami i algorytmami) teorii Shannona (pojęcia oraz twierdzenia) o szyfrowaniu i bezpieczeństwie informacji oraz kryptologii klasycznej, podstawowe pojęcia i zagadnienia (z dowodami i algorytmami) o szyfrowaniu symetrycznego i asymetrycznego, ilustruje ich przykładami, rozwiązuje standardowe zadania praktyczne i teoretyczne
Na ocenę 5.0	Student zna podstawowe pojęcia i zagadnienia (z dowodami i algorytmami) teorii Shannona (pojęcia oraz twierdzenia) o szyfrowaniu i bezpieczeństwie informacji oraz kryptologii klasycznej, podstawowe pojęcia i zagadnienia (z dowodami i algorytmami) o szyfrowaniu symetrycznego i asymetrycznego, ilustruje ich przykładami, rozwiązuje standardowe i niestandardowe zadania teoretyczne i praktyczne
Efekt kształcenia 3	

Na ocenę 2.0	Student nie potrafi precyzyjnie formułować pytania, służące pogłębieniu własnego zrozumienia danego tematu lub odnalezieniu brakujących elementów rozumowania, samodzielnie wyszukiwać informacje w literaturze, także w językach obcych
Na ocenę 3.0	Student nie tylko wie i demonstruje jak szyfrować i deszyfrować informacje za pomocą szyfrów klasycznych i współczesnych, lecz również potrafi precyzyjnie formułować pytania, służące pogłębieniu własnego zrozumienia danego tematu
Na ocenę 3.5	Student nie tylko wie i demonstruje jak szyfrować i deszyfrować informacje za pomocą szyfrów klasycznych i współczesnych, lecz również potrafi precyzyjnie formułować pytania, służące pogłębieniu własnego zrozumienia danego tematu lub odnalezieniu brakujących elementów rozumowania, samodzielnie wyszukiwać informacje w literaturze
Na ocenę 4.0	Student nie tylko wie i demonstruje jak szyfrować i deszyfrować informacje za pomocą szyfrów klasycznych i współczesnych, lecz również potrafi precyzyjnie formułować pytania, służące pogłębieniu własnego zrozumienia danego tematu lub odnalezieniu brakujących elementów rozumowania, samodzielnie wyszukiwać informacje w literaturze, także w językach obcych
Na ocenę 4.5	Student nie tylko wie i demonstruje jak szyfrować i deszyfrować informacje za pomocą szyfrów klasycznych i współczesnych, lecz również potrafi precyzyjnie formułować standardowe pytania, służące pogłębieniu własnego zrozumienia danego tematu lub odnalezieniu brakujących elementów rozumowania, samodzielnie wyszukiwać informacje w literaturze, także w językach obcych
Na ocenę 5.0	Student nie tylko wie i demonstruje jak szyfrować i deszyfrować informacje za pomocą szyfrów klasycznych i współczesnych, lecz również potrafi precyzyjnie formułować standardowe i niestandardowe pytania, służące pogłębieniu własnego zrozumienia danego tematu lub odnalezieniu brakujących elementów rozumowania, samodzielnie wyszukiwać informacje w literaturze, także w językach obcych
Efekt kształcenia 4	
Na ocenę 2.0	Student nie wie i nie demonstruje jak zrealizować szyfrowanie i deszyfrowanie za pomocą szyfrów podstawowych
Na ocenę 3.0	Student wie i demonstruje jak zrealizować elementarne szyfrowanie i deszyfrowanie za pomocą szyfrów podstawowych
Na ocenę 3.5	Student wie i demonstruje jak zrealizować szyfrowanie i deszyfrowanie za pomocą szyfrów podstawowych klasycznych i współczesnych
Na ocenę 4.0	Student wie i demonstruje jak zrealizować szyfrowanie i deszyfrowanie za pomocą szyfrów podstawowych klasycznych i współczesnych, a także pewne elementy kryptoanalizy
Na ocenę 4.5	Student wie i demonstruje jak zrealizować szyfrowanie i deszyfrowanie za pomocą szyfrów podstawowych klasycznych i współczesnych, a także pewne elementy kryptoanalizy, oraz ich standardowe zastosowania

Na ocenę 5.0	Student wie i demonstruje jak zrealizować szyfrowanie i deszyfrowanie za pomocą szyfrów podstawowych klasycznych i współczesnych, a także pewne elementy kryptoanalizy, oraz ich standardowe i niestandardowe zastosowania

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_W04	Cel 1	C1 C2 C3 W1 W2 W3	N1 N2 N3	F1 F2 P1
EK2	K_W01 K_W11	Cel 1	C3 C4 C5 W4 W5 W6	N1 N2 N3	F1 F2 P1
EK3	K_K01 K_K06	Cel 1	C5 C6 W5 W6	N1 N2 N3	F1 F2 P1
EK4	K_U01 K_U10	Cel 1	C7 C8 W7 W8	N1 N2 N3	F1 F2 P1

11 Wykaz literatury

Literatura podstawowa

[1] W. Mochnacki — *Kody korekcyjne i kryptografia*, Wrocław, 1997, Politechnika Wrocławska

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

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

Literatura uzupełniająca

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

[2] Song Y. Yan — *Teoria liczb w informatyce*, 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)

. . . . . .