

POLITECHNIKA KRAKOWSKA IM. TADEUSZA KOŚCIUSZKI

KARTA PRZEDMIOTU

obowiązuje studentów rozpoczynających studia w roku akademickim 2023/2024

Wydział Informatyki i Telekomunikacji

Kierunek studiów: Matematyka

Profil: Ogólnoakademicki

Forma studiów: stacjonarne

Kod kierunku: M

Stopień studiów: II

Specjalności: Modelowanie matematyczne, 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	WiT M oIIS C10 23/24
KATEGORIA PRZEDMIOTU	Przedmioty kierunkowe
LICZBA PUNKTÓW ECTS	7.00
SEMESTRY	3

2 RODZAJ ZAJĘĆ, LICZBA GODZIN W PLANIE STUDIÓW

SEMESTR	WYKŁAD	ĆWICZENIA	LABORATORIUM	LABORATORIUM KOMPUTERO- WE	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 liczb, 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 spełnia wymagań na ocenę 3,0
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 spełnia wymagań na ocenę 3,0
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 spełnia wymagań na ocenę 3,0

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 spełnia wymagań na ocenę 3,0
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	SPOSODY OCENY
EK1	K_W01	Cel 1	C1 C2 C3 W1 W2 W3	N1 N2 N3	F1 F2 P1
EK2	K_W01	Cel 1	C3 C4 C5 W4 W5 W6	N1 N2 N3	F1 F2 P1
EK3	K_K01	Cel 1	C5 C6 W5 W6	N1 N2 N3	F1 F2 P1
EK4	K_U13	Cel 1	C7 C8 W7 W8	N1 N2 N3	F1 F2 P1

11 WYKAZ LITERATURY

LITERATURA PODSTAWOWA

- [1] | **W. Mochnecki** — *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

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)

.....