

POLITECHNIKA KRAKOWSKA IM. TADEUSZA KOŚCIUSZKI

KARTA PRZEDMIOTU

obowiązuje studentów rozpoczynających studia w roku akademickim 2023/2024

Wydział Informatyki i Telekomunikacji

Kierunek studiów: Matematyka Stosowana

Profil: Praktyczny

Forma studiów: stacjonarne

Kod kierunku: MS

Stopień studiów: I

Specjalności: Analityka Danych, Matematyka w finansach i ekonomii, Matematyka z Informatyką

1 INFORMACJE O PRZEDMIOCIE

NAZWA PRZEDMIOTU	Podstawy kryptografii i kryptoanalizy
NAZWA PRZEDMIOTU W JĘZYKU ANGIELSKIM	Foundations of Cryptography and Cryptanalysis
KOD PRZEDMIOTU	WiIT MS pIS D14 23/24
KATEGORIA PRZEDMIOTU	Przedmioty specjalnościowe
LICZBA PUNKTÓW ECTS	3.00
SEMESTRY	6

2 RODZAJ ZAJĘĆ, LICZBA GODZIN W PLANIE STUDIÓW

SEMESTR	WYKŁAD	ĆWICZENIA	LABORATORIUM	LABORATORIUM KOMPUTERO- WE	SEMINARIUM	PROJEKT
6	30	30	0	0	0	0

3 CELE PRZEDMIOTU

Cel 1 Przedstawienie studentom podstawowych metod kryptologii.

4 WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

- 1 Podstawowa wiedza z algebry i teorii liczb. Znajomość podstawowych algorytmów grafowych. Znajomość języka angielskiego w stopniu umożliwiającym studiowanie literatury i uczestnictwo w zajęciach.

5 EFEKTY KSZTAŁCENIA

EK1 Wiedza Student zna i rozumie podstawowe pojęcia, algorytmy i metody kryptografii (zarówno klasycznej, jak i współczesnej) oraz kryptoanalizy.

EK2 Wiedza Student zna i rozumie powiązania między kryptologią a matematyką (ze szczególnym uwzględnieniem algebry i teorii liczb).

EK3 Umiejętności Student potrafi stosować w praktyce różne algorytmy kryptograficzne i rozwiązywać proste zadania z zakresu kryptoanalizy.

EK4 Kompetencje społeczne Student jest przygotowany do poszerzania swojej wiedzy kryptologicznej, jak również do dzielenia się nią.

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 (przypomnienie i uzupełnienie): dzielenie z resztą, algorytm Euklidesa, NWD, NWW, liczby względnie pierwsze, zasadnicze twierdzenie arytmetyki, sito Eratostenesa, systemy liczbowe, twierdzenie Euklidesa o liczbach pierwszych.	4
W3	Obliczeniowa i algorytmiczna teoria liczb: testy pierwszości, algorytmy faktoryzacji liczb całkowitych, ważne testy pierwszości związane z bezpieczeństwem (test Fermata, test Lucasa, test silnej pseudopierwszości), arytmetyka modularna (szybkie obliczanie), funkcje arytmetyczne, twierdzenia Eulera i Fermata, problem logarytmu dyskretnego, algorytmy obliczania logarytmów dyskretnych.	4
W4	Kryptografia klasyczna: proste szyfry podstawieniowe, szyfry homofoniczne, szyfry podstawieniowe wieloalfabetowe, szyfry poligramowe, szyfry przestawieniowe, szyfry afiniczne, bezpieczne systemy kryptograficzne (konfuzja, dyfuzja, kompromisy, kryptoanaliza).	4
W5	Prawdopodobieństwo i tajność doskonała. Teoria Shannona: entropia, problem plecakowy, problem faktoryzacji, problem pakowania, problemy NP-zupełne.	6
W6	Szyfry symetryczne i bezpieczeństwo informacji: szyfry Feistela, kryptografia i bezpieczeństwo informacji, algorytm DES/AES.	4
W7	Szyfry asymetryczne: szyfrowanie z kluczem publicznym. Bezpieczeństwo, RSA, szyfr Rabina, szyfr ElGamala.	4

WYKŁAD		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
W8	Podpisy cyfrowe: standard podpisu cyfrowego (DSS), dzielenie sekretu.	2

ĆWICZENIA		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
C1	Ochrona danych. Systemy i algorytmy kryptograficzne. Własności informacyjne języka.	2
C2	Dzielenie z resztą, algorytm Euklidesa, NWD, NWW. Liczby względnie pierwsze. Zasadnicze twierdzenie arytmetyki. Sito Eratostenesa. Systemy liczbowe. Twierdzenie Euklidesa o liczbach pierwszych.	4
C3	Testy pierwszości. Algorytmy faktoryzacji liczb całkowitych. Test Fermata, test Lucasa, test silnej pseudopierwszości. Arytmetyka modularna, szybkie obliczanie. Funkcje arytmetyczne. Twierdzenia Eulera i Fermata. Logarytmy dyskretne i algorytmy ich obliczania.	4
C4	Proste szyfry podstawieniowe. Szyfry homofoniczne. Szyfry podstawieniowe wieloalfabetowe. Szyfry poligramowe. Szyfry przestawieniowe, szyfry afiniczne. Bezpieczne systemy kryptograficzne (konfuzja, dyfuzja, kompromisy, kryptoanaliza).	4
C5	Entropia. Problem plecakowy, problem faktoryzacji, problem pakowania, problemy NP-zupełne.	4
C6	Szyfry Feistela. Kryptografia i bezpieczeństwo informacji. Algorytm DES/AES.	3
C7	Szyfrowanie z kluczem publicznym. RSA. Szyfr Rabina, szyfr ElGamala.	5
C8	Standard podpisu cyfrowego (DSS). Dzielenie sekretu.	4

7 NARZĘDZIA DYDAKTYCZNE

N1 Wykłady i ćwiczenia

N3 Praca przy tablicy

N4 Projekty

N5 DELTA, MS TEAMS

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	5
Egzaminy i zaliczenia w sesji	5
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	10
Opracowanie wyników	5
Przygotowanie raportu, projektu, prezentacji, dyskusji	5
SUMARYCZNA LICZBA GODZIN DLA PRZEDMIOTU WYNIKAJĄCA Z CAŁEGO NAKŁADU PRACY STUDENTA	90
SUMARYCZNA LICZBA PUNKTÓW ECTS DLA PRZEDMIOTU	3.00

9 SPOSOBY OCENY

OCENA FORMUJĄCA

F1 Sprawdziany z bieżącego materiału (na ćwiczeniach)

OCENA PODSUMOWUJĄCA

P1 kolokwium zaliczeniowe (podsumowujące przedmiot) pisemne i ustne.

WARUNKI ZALICZENIA PRZEDMIOTU

W1 Warunkiem koniecznym zaliczenia ćwiczeń jest uzyskanie więcej niż połowy maksymalnej sumarycznej liczby punktów.

W2 Spełnienie warunku obecności na zajęciach.

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 i rozumie podstawowe pojęcia, algorytmy i metody kryptografii (zarówno klasycznej, jak i współczesnej) oraz kryptoanalizy
NA OCENĘ 3.5	Student zna i rozumie podstawowe pojęcia, algorytmy i metody kryptografii (zarówno klasycznej, jak i współczesnej) oraz kryptoanalizy, ilustruje je przykładami, rozwiązuje podstawowe zadania praktyczne, formułuje podstawowe zagadnienia
NA OCENĘ 4.0	Student zna i rozumie pojęcia, algorytmy i metody kryptografii (zarówno klasycznej, jak i współczesnej) oraz kryptoanalizy, ilustruje je przykładami, rozwiązuje podstawowe zadania praktyczne i teoretyczne, formułuje i zna dowody podstawowych zagadnień
NA OCENĘ 4.5	Student zna i rozumie pojęcia, algorytmy i metody kryptografii (zarówno klasycznej, jak i współczesnej) oraz kryptoanalizy, ilustruje je przykładami, rozwiązując zadania praktyczne i teoretyczne, formułuje i zna dowody zagadnień
NA OCENĘ 5.0	Student zna i rozumie pojęcia, algorytmy i metody kryptografii (zarówno klasycznej, jak i współczesnej) oraz kryptoanalizy, ilustruje je przykładami, rozwiązuje zadania praktyczne i teoretyczne jak standardowe tak i niestandardowe, zna dowody zagadnień
EFEKT KSZTAŁCENIA 2	
NA OCENĘ 2.0	Student nie spełnia wymagań na ocenę 3.0
NA OCENĘ 3.0	Student zna i rozumie powiązania między kryptologią a matematyką (ze szczególnym uwzględnieniem algebry i teorii liczb)
NA OCENĘ 3.5	Student zna i rozumie powiązania między kryptologią a matematyką (ze szczególnym uwzględnieniem algebry i teorii liczb), ilustruje je przykładami i podstawowymi zagadnieniami
NA OCENĘ 4.0	Student zna i rozumie powiązania między kryptologią a matematyką (ze szczególnym uwzględnieniem algebry i teorii liczb), ilustruje je przykładami i podstawowymi zagadnieniami i ich dowodami
NA OCENĘ 4.5	Student zna i rozumie powiązania między kryptologią a matematyką (ze szczególnym uwzględnieniem algebry i teorii liczb), ilustruje je przykładami i stosowaniem do rozwiązywania zadań praktycznych, i nie tylko podstawowymi zagadnieniami i ich dowodami
NA OCENĘ 5.0	Student zna i rozumie powiązania między kryptologią a matematyką (ze szczególnym uwzględnieniem algebry i teorii liczb), ilustruje je przykładami i stosowaniem do rozwiązywania zadań praktycznych i teoretycznych, a także zagadnieniami i ich dowodami
EFEKT KSZTAŁCENIA 3	
NA OCENĘ 2.0	Student nie spełnia wymagań na ocenę 3.0
NA OCENĘ 3.0	Student potrafi stosować w praktyce różne algorytmy kryptograficzne i rozwiązywać (proste) zadania z zakresu krypto analizy

NA OCENĘ 3.5	Student potrafi stosować w praktyce różne algorytmy kryptograficzne i rozwiązywać (proste) zadania z zakresu krypto analizy, ilustrować je przykładami i podstawowymi zagadnieniami
NA OCENĘ 4.0	Student potrafi stosować w praktyce różne algorytmy kryptograficzne i rozwiązywać (proste) zadania z zakresu krypto analizy, ilustrować je przykładami i podstawowymi zagadnieniami z dowodami
NA OCENĘ 4.5	Student potrafi stosować w praktyce różne algorytmy kryptograficzne i rozwiązywać (proste) zadania z zakresu krypto analizy, ilustrować je przykładami praktycznymi i teoretycznymi i zagadnieniami z dowodami
NA OCENĘ 5.0	Student potrafi stosować w praktyce różne algorytmy kryptograficzne i rozwiązywać (proste) zadania z zakresu krypto analizy, ilustrować je przykładami praktycznymi i teoretycznymi (standardowymi i niestandardowymi) i zagadnieniami z dowodami
EFEKT KSZTAŁCENIA 4	
NA OCENĘ 2.0	Student nie jest przygotowany do poszerzania swojej wiedzy kryptologicznej, jak również do dzielenia się nią z laikami
NA OCENĘ 3.0	Student jest przygotowany do poszerzania swojej wiedzy kryptologicznej, jak również do dzielenia się nią z laikami
NA OCENĘ 3.5	Student jest przygotowany do poszerzania swojej wiedzy kryptologicznej, jak również do dzielenia się nią z laikami, jest przygotowany do konstruowania ilustrujących przykładów
NA OCENĘ 4.0	Student jest przygotowany do poszerzania swojej wiedzy kryptologicznej, jak również do dzielenia się nią z laikami, jest przygotowany do konstruowania ilustrujących przykładów praktycznych i zagadnień
NA OCENĘ 4.5	Student jest przygotowany do poszerzania swojej wiedzy kryptologicznej, jak również do dzielenia się nią z laikami, jest przygotowany do konstruowania ilustrujących przykładów (teoretycznych i praktycznych) i zagadnień
NA OCENĘ 5.0	Student jest przygotowany do poszerzania swojej wiedzy kryptologicznej, jak również do dzielenia się nią z laikami, jest przygotowany do konstruowania ilustrujących przykładów (teoretycznych i praktycznych, standardowych i niestandardowych) i zagadnień

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_W03	Cel 1	W1 W2 W3 W4	N1 N3 N4	F1 P1
EK2	K_W04 K_W05 K_W12	Cel 1	W5 W6 W7 W8 C5 C6 C7 C8	N1 N3 N4	F1 P1
EK3	K_U09 K_U23	Cel 1	W1 W2 W3 W4 W5 W6 W7 W8 C1 C2 C3 C4 C5 C6 C7 C8	N1 N3 N4 N5	F1 P1
EK4	K_K01 K_K02	Cel 1	W1 W2 W3 W4 W5 W6 W7 W8 C1 C2 C3 C4 C5 C6 C7 C8	N1 N3 N4 N5	F1 P1

11 WYKAZ LITERATURY

LITERATURA PODSTAWOWA

- [1] | D.R. Stinson — *Kryptografia (w teorii i w praktyce)*, Warszawa, 2005, WNT
- [2] | N.Koblitz — *Wykład z teorii liczb i kryptografii*, Warszawa, 1995, WNT
- [3] | W. Mochnacki — *Kody korekcyjne i kryptografia*, Wrocław, 1997, Wyd. Pol. Wrocławskiej
- [4] | J.A. Buchman — *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
- [3] | J. Gancarzewicz — *Arytmetyka*, Kraków, 2002, Wyd. UJ
- [4] | J. Rutkowski — *Teoria liczb*, Warszawa, 2018, PWN

LITERATURA DODATKOWA

- [1] | N. Ferguson, B. Schneider — *Practical Cryptography*, Miejscowość, 2003, Wiley Publ. Inc.

12 INFORMACJE O NAUCZYCIELACH AKADEMICKICH

OSOBA ODPOWIEDZIALNA ZA KARTĘ

dr Maciej Zakarczemny (kontakt: mzakarczemny@pk.edu.pl)

OSOBY PROWADZĄCE PRZEDMIOT

1 dr Maciej Zakarczemny (kontakt: mzakarczemny@pk.edu.pl)

13 ZATWIERDZENIE KARTY PRZEDMIOTU DO REALIZACJI

(miejscowość, data)

(odpowiedzialny za przedmiot)

(dziekan)

PRZYJMUJĘ DO REALIZACJI (data i podpisy osób prowadzących przedmiot)

.....