Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

obowiązuje studentów rozpoczynających studia w roku akademickim 2021/2022

Wydział Informatyki i Telekomunikacji

Kierunek studiów: Matematyka Stosowana — Profil: Praktyczny

Forma sudiów: 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 cryptoanalysis
Kod przedmiotu	WIiT MS pIS D14 21/22
Kategoria przedmiotu	Przedmioty specjalnościowe
Liczba punktów ECTS	3.00
Semestry	6

2 Rodzaj zajęć, liczba godzin w planie studiów

Semestr	Wykład	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Seminarium	Projekt
6	30	30	0	0	0	0

3 Cele przedmiotu

Cel 1 Nauczenie studentów podstawowych metod współczesnej kryptologii, aktywnie stosowanych w ochronie informacji, bankowości itp.

4 Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1 zaliczenie przedmiotów „Algebra z teorią liczb oraz „Grafy i algorytmy grafowe.

5 Efekty kształcenia

EK1 Wiedza 1.Student zna i rozumie podstawowe pojęcia, algorytmy i metody kryptografii (zarówno klasycznej, jak i współczesnej) oraz kryptoanalizy

EK2 Wiedza 2.Student zna i rozumie powiązania między kryptologią a matematyką (ze szczególnym uwzględnieniem algebry i teorii liczb)

EK3 Umiejętności 3.Student potrafi stosować w praktyce różne algorytmy kryptograficzne i rozwiązywać (proste) zadania z zakresu krypto analizy

EK4 Kompetencje społeczne 4.Student jest przygotowany do poszerzania swojej wiedzy kryptologicznej, jak również do dzielenia się nią z laikami

6 Treści programowe

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, rozszerzony 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

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, rozszerzony 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
W8	Podpisy cyfrowe: standard podpisu cyfrowego (DSS), dzielenie sekretu.	2

7 Narzędzia dydaktyczne

N1 Wykłady.

N2 Ćwiczenia.

N3 Dyskusja.

N4 Konsultacje.

N5 W sytuacji zdalnego nauczania prowadzone są za pośrednictwem MS Teams, na żywo.

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	12
Egzaminy i zaliczenia w sesji	3
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	15
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	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 i wystarczającym zaliczenia ćwiczeń jest uzyskanie więcej niż połowy maksymalnej sumarycznej liczby punktów ze wszystkich sprawdzianów. Ocena końcowa z przedmiotu jest średnią arytmetyczną trzech ocen cząstkowych: z ćwiczeń, części pisemnej kolokwium zaliczeniowego i części ustnej kolokwium zaliczeniowego. Wszystkie oceny cząstkowe muszą być pozytywne.

Ocena aktywności bez udziału nauczyciela

B1 Test

Kryteria oceny

Efekt kształcenia 1	
Na ocenę 2.0	Student nie zna i nie rozumie podstawowe pojęcia, algorytmy i metody kryptografii (zarówno klasycznej, jak i współczesnej) oraz kryptoanalizy

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 ich przykładami, rozwiązuję podstawowe zadania praktyczne, formułuję podstawowe zagadnienia
Na ocenę 4.0	Student zna i rozumie pojęcia, algorytmy i metody kryptografii (zarówno klasycznej, jak i współczesnej) oraz kryptoanalizy, ilustruje ich przykładami, rozwiązuję podstawowe zadania praktyczne i teoretyczne, formułuję 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 ich przykładami, rozwiązuję zadania praktyczne i teoretyczne, formułuję 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 ich przykładami, rozwiązuję zadania praktyczne i teoretyczne jak standardowe tak i nie standardowe, zna dowody zagadnień
Efekt kształcenia 2	
Na ocenę 2.0	Student ne zna i nie rozumie powiązania między kryptologią a matematyką (ze szczególnym uwzględnieniem algebry i teorii liczb)
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), ilustruję ich przykładami i podstawowymi zagadnieniami
Na ocenę 4.0	Student zna i rozumie powiązania między kryptologią a matematyką (ze szczególnym uwzględnieniem algebry i teorii liczb), ilustruję ich 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), ilustruję ich przykładami i stosowaniem do rozwiązywań 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), ilustruję ich przykładami i stosowaniem do rozwiązywań zadań praktycznych i teoretycznych , a także zagadnieniami i ich dowodami
Efekt kształcenia 3	
Na ocenę 2.0	Student nie potrafi stosować w praktyce różne algorytmy kryptograficzne i rozwiązywać (proste) zadania z zakresu krypto analizy
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 ich 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 ich 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 ich 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 ich 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_W04	Cel 1	W1 W2 W3 W4	N1 N2 N3 N4	F1 P1
EK2	K_W01 K_W26	Cel 1	C5 C6 C7 C8 W5 W6 W7 W8	N1 N2 N3 N4	F1 P1
EK3	K_U08 K_U09 K_U17	Cel 1	C1 C2 C3 C4 C5 C6 C7 C8 W1 W2 W3 W4 W5 W6 W7 W8	N1 N2 N3 N4	F1 P1
EK4	K_U29 K_U35 K_K01	Cel 1	C1 C2 C3 C4 C5 C6 C7 C8 W1 W2 W3 W4 W5 W6 W7 W8	N1 N2 N3 N4	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 Mariusz Jużyniec (kontakt: `juzyniec@pk.edu.pl`)

Osoby prowadzące przedmiot

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

13 Zatwierdzenie karty przedmiotu do realizacji

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

Przyjmuję do realizacji (data i podpisy osób prowadzących przedmiot)

. . . . . .