

"ZATWIERDZAM"

.....

.....

KARTA INFORMACYJNA PRZEDMIOTU

Nazwa przedmiotu	Metody numeryczne w kryptologii		Numerical methods for cryptology							
Kod przedmiotu	WCYKSWSM_MNK.....MNK									
Język wykładowy	polski									
Profil studiów	ogólnoakademicki									
Forma studiów	studia stacjonarne									
Poziom studiów	wojskowe studia jednolite magisterskie									
Rodzaj przedmiotu										
Obowiązuje od naboru	2021/2022									
Forma zajęć, liczba godzin/rygor, razem godz., pkt ECTS	semestr	(x egzamin, + zaliczenie, # projekt)					punkty ECTS			
		razem	wykłady	ćwiczenia	laboratoria	projekt		seminarium		
	IX	60x	30		30+					
	razem		30		30					
Przedmioty wprowadzające	- Algebra liniowa i geometria analityczna (na studiach pierwszego stopnia. Znajomość pojęć, twierdzeń i zagadnień dotyczących przestrzeni wektorowych ieuclidesowych: ciał liczb rzeczywistych i zespolonych, grupy, liniowej niezależności wektorów, bazy i wymiaru przestrzeni, iloczynu skalarnego, normy, metryki, przekształcenia liniowego, macierzy przekształcenia liniowego, rachunku macierzowego, rzędu macierzy, macierzy odwrotnej, układów liniowych równań algebraicznych i metody eliminacji niewiadomych. - Analiza matematyczna (na studiach pierwszego stopnia). Znajomość pojęć, twierdzeń i zagadnień rachunku różniczkowego i całkowego funkcji rzeczywistych jednej i wielu zmiennych: zbioru liczb rzeczywistych, ciągów i szeregów liczbowych, granicy, ciągłości, pochodnej i różniczki funkcji, całki nieoznaczonej i oznaczonej, przestrzeni metrycznej, ciągów i szeregów funkcyjnych, rozwinięcia Taylora. - Logika i teoria mnogości (na studiach pierwszego stopnia. Znajomość pojęć, twierdzeń i zagadnień teorii mnogości: zbioru, przynależności, odwzorowania, funkcji, iloczynu kartezjańskiego zbiorów, symboliki teorii mnogości oraz elementarnych pojęć i symboli logiki.									
Semestr/kierunek studiów	semestr 9 / Kryptologia i cyberbezpieczeństwo / Systemy kryptograficzne									
Autor	dr hab. Marek Kojdecki									
Jednostka odpowiedzialna za przedmiot	Instytut Matematyki i Kryptologii									
Skrócony opis przedmiotu	- wykład z możliwym wykorzystaniem technik audiowizualnych; podanie zadań do samodzielnego rozwiązania i tematów do studiowania - ćwiczenia rachunkowe ułatwiające opanowanie, zrozumienie i usystematyzowanie wiedzy wyniesionej z wykładów i własnych studiów studentów oraz nabycie umiejętności rachunkowych; podanie zadań do samodzielnego rozwiązania i tematów do studiowania; pisemna praca kontrolna - ćwiczenia laboratoryjne z wykorzystaniem programów uczących i programów narzędziowych (M - Matlab i E - Excel) i ćwiczeniami rachunkowymi, ułatwiające opanowanie, zrozumienie i usystematyzowanie wiedzy wyniesionej z wykładów i własnych studiów studentów oraz nabycie umiejętności rachunkowych; podanie zadań do samodzielnego rozwiązania i tematów do studiowania; pisemna praca kontrolna									
Pełny opis przedmiotu (treści programowe)	lp.	Semestr IX temat/tematyka zajęć				liczba godzin				
						wkt.	ćw.	lab.	prj.	sem.
	1	Podstawowe pojęcia analizy numerycznej. Wektory, macierze i normy.				2				
	2	Podstawowe pojęcia analizy numerycznej. Błędy zaokrągleń w obliczeniach komputerowych; arytmetyki zmiennoprzecinkowe; uwarunkowanie zadania obliczeniowego; algorytmy numerycznie poprawne; arytmetyki stałoprzecinkowe.				2				
	3	Bezpośrednie metody rozwiązywania układów liniowych równań algebraicznych. Uwarunkowanie zadania; algorytmy numerycznie poprawne; zadania źle uwarunkowane.				2				
	4	Bezpośrednie metody rozwiązywania układów liniowych równań algebraicznych. Metoda Gaussa z pełnym oraz z częściowym wyborem elementu głównego; metoda Choleskygo-Banachiewicza; wpływ błędów zaokrągleń na wynik.				2				
	5	Bezpośrednie metody rozwiązywania układów liniowych równań algebraicznych. Faktoryzacja macierzy; metoda Gaussa; metoda Householdera, wpływ błędów zaokrągleń na wynik.				2				
	6	Liniowe zadanie najmniejszych kwadratów w postaci algebraicznej. Rozkład macierzy według wartości własnych; rozkład macierzy według wartości szczególnych.				2				

lp.	Semestr IX temat/tematyka zajęć	liczba godzin				
		wkt.	ćw.	lab.	prj.	sem.
7	Linowe zadanie najmniejszych kwadratów w postaci algebraicznej. Postawienie zagadnienia; uogólniona macierz odwrotna i uogólnione rozwiązanie układu liniowych równań algebraicznych.	2				
8	Linowe zadanie najmniejszych kwadratów w postaci algebraicznej. Zadanie regularne; algorytm rozwiązywania z równaniem normalnym; uwarunkowanie zadania regularnego; algorytm z przekształceniem Householdera.	2				
9	Linowe zadanie najmniejszych kwadratów w postaci algebraicznej. Zadania nieregularne i źle uwarunkowane; regularyzacja.	2				
10	Iteracyjne rozwiązywanie układów liniowych równań algebraicznych. Metody iteracji prostych; metody Gaussa-Seidela i Jacobiego; charakterystyki zbieżności.	2				
11	Interpolacja wielomianowa. Wielomian interpolacyjny Lagrangea w postaciach naturalnej, Lagrangea i Newtona; obliczanie współczynników i wartości. Jednoznaczność rozwiązania zadania interpolacji. Reszta interpolacyjna.	2				
12	Wielomiany Czebyszowa. Określenie i wybrane właściwości; bazy wielomianów; zastosowania.	2				
13	Aproksymacja średniokwadratowa wielomianami. Postawienie liniowego zadania najmniejszych kwadratów i znajdowanie wielomianów aproksymujących.	2				
14	Funkcje sklejkane i ich zastosowania. Określenie i podstawowe właściwości sklejek; sklejk naturalne trzeciego stopnia; interpolacja sklejkami.	2				
15	Funkcje sklejkane i ich zastosowania. Aproksymacja średniokwadratowa i zadanie wygładzania danych; wygładzanie sklejkami naturalnymi trzeciego stopnia i różniczkowanie numeryczne.	2				
16	Normy wektorów i macierzy. Przestrzenie wektorowe i przekształcenia liniowe; wektory, macierze i normy; obliczenia za pomocą programów narzędziowych. (M)			2		
17	Arytmetyki zmiennoprzecinkowe. Błędy zaokrągleń w obliczeniach komputerowych; arytmetyki zmiennoprzecinkowe; uwarunkowanie zadania obliczeniowego; przykłady, w tym sumowanie szeregów potęgowych. (E)			2		
18	Rozwiązywanie układów liniowych równań algebraicznych. Metoda Gaussa z pełnym oraz z częściowym wyborem elementu głównego; wpływ błędów zaokrągleń na wynik. (E)			2		
19	Faktoryzacja trójkątno-trójkątna macierzy. Rozkład metodą Gaussa; rozkład Choleskygo-Banachiewicza; zastosowania do układów liniowych równań algebraicznych. (M)			2		
20	Faktoryzacja ortogonalno-trójkątna macierzy. Rozkład Householdera; rozkład Givensa; zastosowania do równań macierzowych i do układów liniowych równań algebraicznych. (M)			2		
21	Rozkład macierzy według wartości własnych. Faktoryzacja macierzy według wartości własnych; potęgowanie macierzy, funkcje macierzowe; zastosowania do układów liniowych równań algebraicznych. (M)			2		
22	Formy kwadratowe. Postacie kanoniczne form kwadratowych; wykorzystanie wartości własnych; metoda Lagrangea. (M)			2		
23	Rozkład macierzy według wartości szczególnych. Faktoryzacja macierzy według wartości szczególnych; regularne linowe zadanie najmniejszych kwadratów; uogólniona macierz odwrotna; przykłady. (M)			2		
24	Linowe zadanie najmniejszych kwadratów w postaci algebraicznej. Zadanie regularne; algorytm rozwiązywania z równaniem normalnym; uwarunkowanie zadania; wpływ błędów zaokrągleń na wynik. (E)			2		
25	Linowe zadanie najmniejszych kwadratów w postaci algebraicznej. Zadanie nieregularne; regularyzacja, algorytm rozwiązywania z równaniem normalnym; wpływ błędów zaokrągleń na wynik. (E)			2		
26	Linowe zadanie najmniejszych kwadratów w postaci algebraicznej. Zadanie regularne; algorytm z przekształceniem Householdera; zadania nieregularne i źle uwarunkowane; regularyzacja. (M)			2		
27	Iteracyjne rozwiązywanie układów liniowych równań algebraicznych. Metody Gaussa-Seidela i Jacobiego. (E)			2		

	lp.	Semestr IX temat/tematyka zajęć	liczba godzin				
			wkl.	ćw.	lab.	prj.	sem.
	28	Interpolacja i aproksymacja wielomianowa. Wielomian interpolacyjny; wielomiany aproksymujące i wygładzanie wielomianami. (M)			2		
	29	Funkcje skleane i ich zastosowania. Określenie i podstawowe właściwości sklejek; sklejk naturalne trzeciego stopnia; interpolacja sklejami. (M)			2		
	30	Funkcje skleane i ich zastosowania. Aproksymacja średniokwadratowa i zadanie wygładzania danych. Wygładzanie sklejami naturalnymi trzeciego stopnia i różniczkowanie numeryczne. (M)			2		
	Razem		30		30		
Literatura	podstawowa: • A. Kielbasiński, H. Schwetlick: Numeryczna algebra liniowa; PWN, Warszawa, 1991. • A. Maćkiewicz : Algorytmy algebry liniowej. Metody bezpośrednie; Wydawnictwo Politechniki Poznańskiej, Poznań 2002. • M.A. Kojdecki: Elementy analizy numerycznej; WAT, Warszawa, 2011 (skrypt w postaci elektronicznej). uzupełniająca: • G. H. Golub, C. F. Van Loan: Matrix Computations; The John Hopkins University Press, Baltimore and London, 1996. • J. i M. Jankowsy: Przegląd metod i algorytmów numerycznych. Część 1; WNT, Warszawa, 1981. • M. Dryja, J. i M. Jankowsy: Przegląd metod i algorytmów numerycznych. Część 2; WNT, Warszawa, 1982. • A. Björck, G. Dahlquist: Metody numeryczne; PWN, Warszawa, 1983. • D. Kincaid, W. Cheney: Analiza numeryczna; WNT, Warszawa, 2006. • Z. Fortuna, B. Macukow, J. Wąsowski: Metody numeryczne; WNT, Warszawa, 1982.						
Efekty uczenia się	Symbol	Efekty kształcenia			odniesienie do efektów kształcenia dla kierunku		
	W01	Zna i rozumie podstawowe metody numerycznego rozwiązywania układów liniowych równań algebraicznych i liniowego zadania najmniejszych kwadratów, także z wykorzystaniem metod faktoryzacji macierzy oraz metody faktoryzacji macierzy i pojęcie uogólnionej macierzy odwrotnej.			K_W02		
	W02	Zna i rozumie podstawowe pojęcia analizy numerycznej w tym arytmetyki zmiennoprzecinkowej i arytmetyki stałoprzecinkowej; metodę wstecznej analizy błędów w obliczeniach komputerowych i jej zastosowania do oceny dokładności rozwiązań zadań numerycznej algebry liniowej.			K_W02		
	U01	Student umie wybrać i zastosować metodę numerycznego rozwiązywania układu liniowych równań algebraicznych oraz liniowego zadania najmniejszych kwadratów.			K_U03		
	U02	Umie formułować i rozwiązywać proste problemy z wykorzystaniem układów liniowych równań algebraicznych, liniowego zadania najmniejszych kwadratów i faktoryzacji macierzy.			K_U03		
	U03	Potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł (także anglojęzycznych); potrafi interpretować uzyskane informacje i formułować wnioski. Ma wyrobioną wewnętrzną potrzebę i umiejętność ustawicznego uzupełniania i nowelizacji nabytej wiedzy poprzez samokształcenie.					
	K01	Rozumie potrzebę ciągłego dokształcania się i odświeżania wiedzy, w szczególności związanej ze złożoną strukturą matematyki.					
Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez studenta zakładanych efektów uczenia się)		• Przedmiot zaliczany jest na podstawie egzaminu sprawdzającego wiedzę (W01 i W02) i umiejętności (U01 i U02). Egzamin przeprowadzany jest w formie pisemnej lub pisemnej i ustnej. Warunkiem dopuszczenia do egzaminu jest zaliczenie ćwiczeń laboratoryjnych. • Ćwiczenia laboratoryjne zaliczane są na podstawie wyników prac kontrolnych przeprowadzanych pod bezpośrednią kontrolą podczas zajęć (U01, U02, W01, W02) lub w formie zadań do samodzielnego rozwiązania (U01, U02, U03) oraz na podstawie sprawozdań z wybranych ćwiczeń. Dodatkowo studenci otrzymują wskazówki do samodzielnego studiowania z zachętą do korzystania z różnorodnych źródeł wiedzy (U03 i K01). • Skala ocen: dostatecznie (3) - student zna i rozumie większość wyłożonych zagadnień, umie rozwiązywać najprostsze zadania rachunkowe, rozumie treść najważniejszych twierdzeń; dobrze (4) - student zna i rozumie znaczną większość wyłożonych zagadnień, umie formułować i rozwiązywać najprostsze zadania rachunkowe oraz interpretować ich wyniki za pomocą twierdzeń; bardzo dobrze (5) - student zna i rozumie wszystkie wyłożone zagadnienia, umie formułować i rozwiązywać zadania rachunkowe oraz interpretować ich wyniki za pomocą twierdzeń; dość dobrze (3,5) i ponad dobrze (4,5) - pośrednio między dostatecznie i dobrze oraz między dobrze i bardzo dobrze.					

Bilans ECTS (nakład pracy studenta)	SEMESTR 9		
	Aktywność	Obciążenie studenta	
		Liczba godzin	Liczba ECTS
	Udział w wykładach	30	1
	Udział w laboratoriach	30	1
	Udział w ćwiczeniach	0	0
	Udział w projektach	0	0
	Udział w seminariach	0	0
	Samodzielne studiowanie tematyki wykładów	20	1
	Samodzielne przygotowanie do laboratoriów	24	1
	Samodzielne przygotowanie do ćwiczeń		
	Samodzielna realizacja projektu	4	
	Samodzielne przygotowanie do seminariów		
	Udział w konsultacjach	2	
	Przygotowanie do egzaminu		
	Przygotowanie do zaliczenia		
	Udział w egzaminie / kolokwium	2	
	Sumaryczne obciążenie pracą studenta	112	4
	Zajęcia z udziałem nauczycieli	64	2
	Zajęcia powiązane z działalnością naukową	108	4
	Zajęcia o charakterze praktycznym	58	2

autor

**kierownik jednostki organizacyjnej
odpowiedzialnej za przedmiot**

dr hab. Marek Kojdecki

tytuł, stopień naukowy, imię, NAZWISKO, podpis

dr hab. Kojdecki Marek

tytuł, stopień naukowy, imię, NAZWISKO, podpis