

"ZATWIERDZAM"

.....

.....

KARTA INFORMACYJNA PRZEDMIOTU

Nazwa przedmiotu	Zastosowania teorii krat w kryptologii			Application of Lattice-based cryptology						
Kod przedmiotu	WCYKSCSI									
Język wykładowy	polski									
Profil studiów	ogólnoakademicki									
Forma studiów	studia stacjonarne									
Poziom studiów	studia pierwszego stopnia									
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			
	V	44x	20		24+			4.0		
	razem		20		24		4.0			
Przedmioty wprowadzające	- Algorytmy i struktury danych - K_U05, K_U07, K_U17, K_W05 - Matematyka dyskretna I - K_U03, K_U17, K_W02 - Matematyka dyskretna II - K_U03, K_U17, K_W02 - Matematyka I - K_U03, K_U17, K_W02 - Matematyka II - K_U03, K_U17, K_W02 - Rachunek prawdopodobieństwa - K_U03, K_U17, K_W02 - Wprowadzenie do programowania - K_U05, K_U07, K_U14, K_U16, K_U17, K_W05, K_W06, K_W08, K_W09									
Semestr/kierunek studiów	semestr 5 / Kryptologia i cyberbezpieczeństwo / Systemy kryptograficzne									
Autor	dr Mariusz Jurkiewicz									
Jednostka odpowiedzialna za przedmiot	Wydział Cybernetyki/Instytut Matematyki i Kryptologii/Laboratorium Badawcze Kryptologii									
Skrócony opis przedmiotu	- Wykład - Laboratorium									
Pełny opis przedmiotu (treści programowe)	lp.	Semestr V temat/tematyka zajęć				liczba godzin				
						wkl.	ćw.	lab.	prj.	sem.
	1	Pojęcie kraty; Baza kraty; Unimodularna macierz przejścia; Obszar fundamentalny i wyznacznik kraty.				2		2		
	2	Współczynnik Hadamarda; Podstawowe trudne problemy na kratach (SVP, CVP, DCVP, DSVP) i relacje między nimi; Ograniczenia Hermite'a i Minkowskiego; Heurystyka Gaussa				2		2		
	3	Redukcja Gaussa-Lagrange'a oraz jej szczegółowa analiza; Algorytm redukcji bazy Lenstry, Lenstry i Lovasza (LLL) wraz ze szczegółową analizą; BKZ i BKZ 2.0.				5		4		
	4	Metoda najbliższej płaszczyzny Babai'a; Metoda zaokrąglania Babai'a; GGH.				2		4		
	5	NTRU opis, elementy analizy, wybrane wersje.				4		4		
	6	Dyskretny rozkład Gaussa; LWE i RLWE; Prymitywny algorytm Regev'a; Algorytm(y) Dinga;				2		4		
	7	Dyskretny rozkład dwumianowy; Dyskretna transformata Fouriera i NTT; NewHope - elementy konstrukcji.				3		4		
	Razem				20		24			
Literatura	podstawowa: D. Micciancio, S. Goldwasser, Complexity of Lattice Problems a Crypto-graphic Perspective, Kluwer Academic Publishers 2002. - D.P. Chi, J.W. Choi, J.S. Kim, T.K. Kim, Lattice Based Cryptography for Be-ginners, https://eprint.iacr.org/2015/938.pdf uzupełniająca: - D.J. Bernstein, J. Buchmann, E. Dahmen (eds.), Post-Quantum Crypto-graphy, Springer 2009. - Joseph H. Silverman (Ed.), Cryptography and Lattices, Springer 2001									
Efekty uczenia się	Symbol	Efekty kształcenia					odniesienie do efektów kształcenia dla kierunku			
	W1	zna i rozumie/ma/posiada uporządkowaną, podbudowaną teoretycznie wiedzę dotyczącą zastosowań teorii krat w kryptografii oraz pewne zastosowania w kryptoanalizie.					K_U18, K_W02			
	U1	potrafi/umie posługiwać się w podstawowym zakresie językiem oraz metodami teorii krat w kontekście zastosowań					K_U18,K_W22			

	Symbol	Efekty kształcenia	odniesienie do efektów kształcenia dla kierunku
		kryptograficznych oraz korzystać ze specjalistycznej literatury.	
	K1	jest gotów do krytycznej oceny posiadanej wiedzy i jej znaczenia w rozwiązywaniu problemów poznawczych i praktycznych.	K_U18
Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez studenta zakładanych efektów uczenia się)	- Egzamin przeprowadzany jest w formie pisemnej lub ustnej. - Warunkiem dopuszczenia do egzaminu jest zaliczenie laboratorium. - Laboratorium zaliczane jest na podstawie samodzielnej pracy zaliczeniowej lub prac cząstkowych. - Warunkiem koniecznym uzyskania zaliczenia laboratorium jest obecność na co najmniej 83% zajęć.		
Bilans ECTS (nakład pracy studenta)	SEMESTR 5		
	Aktywność	Obciążenie studenta	
		Liczba godzin	Liczba ECTS
	Udział w wykładach	20	0.7
	Udział w laboratoriach	24	0.5
	Udział w ćwiczeniach	0	0
	Udział w projektach	0	0.5
	Udział w seminariach	0	0
	Samodzielne studiowanie tematyki wykładów	15	0.25
	Samodzielne przygotowanie do laboratoriów	10	0.25
	Samodzielne przygotowanie do ćwiczeń		
	Samodzielna realizacja projektu	15	1
	Samodzielne przygotowanie do seminariów		
	Udział w konsultacjach	2	0.1
	Przygotowanie do egzaminu	5	0.35
	Przygotowanie do zaliczenia	8	0.25
	Udział w egzaminie / kolokwium	4	0.1
	Sumaryczne obciążenie pracą studenta	103	4
	Zajęcia z udziałem nauczycieli	50	1.9
	Zajęcia powiązane z działalnością naukową	84	3.2
Zajęcia o charakterze praktycznym	49	2.25	

autor

kierownik jednostki organizacyjnej
odpowiedzialnej za przedmiot

dr Mariusz Jurkiewicz

tytuł, stopień naukowy, imię, NAZWISKO, podpis

dr hab. Koidecki Marek

tytuł, stopień naukowy, imię, NAZWISKO, podpis