"ZATWIERDZAM"

.....

.....

KARTA INFORMACYJNA PRZEDMIOTU

Nazwa przedmiotu	Zastosowania teorii krat w kryptologii	Application of Lattice-based cryptology
Kod przedmiotu	WCYKSWSM_.....	
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	
VII	44x	20		24+			3.0
razem		20		24			3.0

Przedmioty wprowadzające

- Algorytmy i struktury danych -
- Matematyka dyskretna I -
- Matematyka dyskretna II -
- Matematyka I -
- Matematyka II -
- Matematyka III -
- Rachunek prawdopodobieństwa -
- Wprowadzenie do programowania -
- Wstęp do kryptologii -

Semestr/kierunek studiów	semestr 7 / 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 VII temat/tematyka zajęć	liczba godzin wkł.	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_W02, K_W22

	Symbol	Efekty kształcenia	odniesienie do efektów kształcenia dla kierunku
	U1	potrafi/umie posługiwać się w podstawowym zakresie językiem oraz metodami teorii krat w kontekście zastosowań kryptograficznych oraz korzystać ze specjalistycznej literatury.	K_U19, K_W02, K_W22
	K1	jest gotów do krytycznej oceny posiadanej wiedzy i jej znaczenia w rozwiązywaniu problemów poznawczych i praktycznych.	K_U19

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 7		
Aktywność	**Obciążenie studenta**	
	Liczba godzin	**Liczba ECTS**
Udział w wykładach	20	0.5
Udział w laboratoriach	24	0.35
Udział w ćwiczeniach	0	0
Udział w projektach	0	0.3
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	0.45
Samodzielne przygotowanie do seminariów		
Udział w konsultacjach	2	0.1
Przygotowanie do egzaminu	5	0.35
Przygotowanie do zaliczenia	8	0.35
Udział w egzaminie / kolokwium	4	0.1
Sumaryczne obciążenie pracą studenta	103	3
Zajęcia z udziałem nauczycieli	50	1.35
Zajęcia powiązane z działalnością naukową	84	2.1
Zajęcia o charakterze praktycznym	49	1.35

autor

dr Mariusz Jurkiewicz
tytuł, stopień naukowy, imię, NAZWISKO, podpis

kierownik jednostki organizacyjnej odpowiedzialnej za przedmiot

dr hab. Kojdecki Marek
tytuł, stopień naukowy, imię, NAZWISKO, podpis