"ZATWIERDZAM"

.....

.....

KARTA INFORMACYJNA PRZEDMIOTU

Nazwa przedmiotu	Krzywe eliptyczne	Elliptic Curves
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	30+	16		14+			3.0
razem		16		14			3.0

Przedmioty wprowadzające	• Brak przedmiotów kształcenia wprowadzających
Semestr/kierunek studiów	semestr 5 / Kryptologia i cyberbezpieczeństwo / Systemy kryptograficzne
Autor	mgr inż. Tomasz Kijko
Jednostka odpowiedzialna za przedmiot	Wydział Cybernetyki, Instytut Matematyki i Kryptologii
Skrócony opis przedmiotu	• Wykłady • Laboratoria

Pełny opis przedmiotu (treści programowe)

lp.	Semestr V temat/tematyka zajęć	liczba godzin wkł.	ćw.	lab.	prj.	sem.
1	Wstęp do geometrii algebraicznej, krzywe płaskie	2				
2	Krzywe eliptyczne - podstawowe definicje i twierdzenia	2		2		
3	Grupa punktów na krzywej eliptycznej	2		2		
4	Rząd grupy punktów na krzywej eliptycznej	2		3		
5	Problem logarytmu dyskretnego w grupie punktów na krzywej eliptycznej	4		3		
6	Kryptosystemy oparte o grupę punktów krzywej eliptycznej	4		4		
	Razem	16		14		

Literatura

podstawowa:
- J. Gawinecki, J. Szmidt, Zastosowanie ciał skończonych i krzywych eliptycznych w kryptologii, 2002
- I. Blake, G. Seroussi, N. Smart, Krzywe eliptyczne w kryptologii, 2004
- H. Cohen, G. Frey, Handbook of Elliptic and Hyperelliptyc Curve Cryptography, 2006
- N. Koblitz, Algebraiczne aspekty kryptografii, 2002

uzupełniająca:
- D. Hankerson, A. Menezes, S. Vanstone, Guide to Elliptic Curve Cryptography, 2004
- Dodatkowe artykuły dotyczące przedmiotu dostępne np. na http://eprint.iacr.org.

Efekty uczenia się

Symbol	Efekty kształcenia	odniesienie do efektów kształcenia dla kierunku
U1	Nauczyć elementów teorii krzywych eliptycznych i ich związków z szyfrowaniem asymetrycznym, najnowszych wyników na temat kryptosystemów opartych na krzywych eliptycznych, arytmetyki w grupie punktów na krzywej eliptycznej.	K_W22, K_W23
W1	Zapoznać z metodami obliczania rzędu grupy punktów na krzywej eliptycznej nad ciałem skończonym, z metodami klasyfikacji krzywych eliptycznych, z kryptosystemami opartymi na krzywych eliptycznych	K_U18, K_W02

Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez studenta zakładanych efektów uczenia się)

- Przedmiot zaliczany jest na podstawie zaliczenia pisemnego.
- Warunkiem koniecznym do dopuszczenia do zaliczenia jest uzyskanie pozytywnej oceny z laboratoriów.
- Ocena z laboratoriów wystawiana jest na podstawie ocen wykonania realizowanych na zajęciach zadań.
- Efekt U1 sprawdzany jest podczas zaliczenia pisemnego przedmiotu.
- Efekt W1 sprawdzany jest podczas realizacji zadań na laboratoriach
- Obecność na laboratoriach jest obowiązkowa.

Bilans ECTS (nakład pracy studenta)	SEMESTR 5		
	Aktywność	Obciążenie studenta	
		Liczba godzin	Liczba ECTS
	Udział w wykładach	16	0.5
	Udział w laboratoriach	14	0.7
	Udział w ćwiczeniach	0	0
	Udział w projektach	0	0
	Udział w seminariach	0	0
	Samodzielne studiowanie tematyki wykładów	14	0.3
	Samodzielne przygotowanie do laboratoriów	20	0.8
	Samodzielne przygotowanie do ćwiczeń		
	Samodzielna realizacja projektu		
	Samodzielne przygotowanie do seminariów		
	Udział w konsultacjach	6	0.1
	Przygotowanie do egzaminu		
	Przygotowanie do zaliczenia	10	0.4
	Udział w egzaminie / kolokwium	2	0.2
	Sumaryczne obciążenie pracą studenta	82	3
	Zajęcia z udziałem nauczycieli	38	1.5
	Zajęcia powiązane z działalnością naukową	64	2.3
	Zajęcia o charakterze praktycznym	34	1.5

autor

mgr inż. Tomasz Kijko
tytuł, stopień naukowy, imię, NAZWISKO, podpis

kierownik jednostki organizacyjnej odpowiedzialnej za przedmiot

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