

.....

KARTA INFORMACYJNA PRZEDMIOTU

Nazwa przedmiotu	Krzywe hipereliptyczne w kryptologii							Hyperelliptic Curves in Cryptography		
Kod przedmiotu	WCYKSWSM_KHK.....KHK									
Język wykładowy	polski									
Profil studiów	ogólnoakademicki									
Forma studiów	studia stacjonarne									
Poziom studiów	wojskowe studia jednolite magisterskie									
Rodzaj przedmiotu	obowiązkowy									
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	44+	16		12+	16#		4.0		
	razem		16		12	16		4.0		
Przedmioty wprowadzające	● Brak przedmiotów kształcenia wprowadzających									
Semestr/kierunek studiów	semestr 9 / Kryptologia i cyberbezpieczeństwo / Systemy kryptograficzne									
Autor	mgr inż. Tomasz Kijko									
Jednostka odpowiedzialna za przedmiot	Instytut Matematyki i Kryptologii									
Skrócony opis przedmiotu	● Wykład, laboratoria, projekt.									
Pełny opis przedmiotu (treści programowe)	lp.	Semestr IX temat/tematyka zajęć				liczba godzin				
						wkł.	ćw.	lab.	prj.	sem.
	1	Krzywe hipereliptyczne - podstawowe definicje i twierdzenia.				2				
	2	Wielomiany i funkcje wymierne na krzywych hipereliptycznych.				2				
	3	Dywizory.				2		2	2	
	4	Jakobian krzywej hipereliptycznej.				2			2	
	5	Problem logarytmu dyskretnego w jacobianie krzywej hipereliptycznej.				2		4	6	
	6	Algorytmy i protokoły kryptograficzne oparte na krzywych hipereliptycznych.				6		6	6	
	Razem					16		12	16	
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 Hyperelliptic 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			
	W1	Nauczyć elementów teorii krzywych hipereliptycznych i ich związków z szyfrowaniem asymetrycznym, najnowszych wyników na temat kryptosystemów opartych na krzywych hipereliptycznych, arytmetyki w jacobianie krzywej hipereliptycznej.					K_U02 K_W02 K_W12			
	U1	Zapoznać z metodami obliczania rzędu jacobianu krzywej hipereliptycznej nad ciałem skończonym, z kryptosystemami opartymi na krzywych hipereliptycznych.					K_U02 K_W02 K_U15			
Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez studenta zakładanych efektów uczenia się)	● Zaliczenie projektu odbywa się na podstawie przedstawienia rozwiązania zagadnienia postawionego na pierwszych zajęciach. Rozwiązanie to powinno być przedstawione w postaci sprawozdania i omówione przez studenta przed wykładowcą. Na ocenę końcową ma wpływ: - jakość zaprezentowanego rozwiązania, a w tym tym poprawność i ekonomiczność zastosowanych metod, - wiedza z zakresu prezentowanego rozwiązania z uzasadnieniem przez studenta przyjętej koncepcji. Nieoddanie pracy w terminie skutkuje oceną niedostateczną z przedmiotu. ● Przedmiot zaliczany jest na podstawie: zaliczenia w formie ustnej lub pisemnej . Warunkiem dopuszczenia do zaliczenia jest zaliczenie laboratoriów i projektu. Na ocenę końcową z przedmiotu mają wpływ oceny z projektu (waga 0.4) i zaliczenia ustnego (waga 0.6).									

Bilans ECTS (nakład pracy studenta)	SEMESTR 9		
	Aktywność	Obciążenie studenta	
		Liczba godzin	Liczba ECTS
	Udział w wykładach	16	0.4
	Udział w laboratoriach	12	0.8
	Udział w ćwiczeniach	0	0
	Udział w projektach	16	0.5
	Udział w seminariach	0	0
	Samodzielne studiowanie tematyki wykładów	14	0.3
	Samodzielne przygotowanie do laboratoriów	6	0.6
	Samodzielne przygotowanie do ćwiczeń		
	Samodzielna realizacja projektu	22	0.8
	Samodzielne przygotowanie do seminariów		
	Udział w konsultacjach	6	0.1
	Przygotowanie do egzaminu		
	Przygotowanie do zaliczenia	6	0.3
	Udział w egzaminie / kolokwium	2	0.2
	Sumaryczne obciążenie pracą studenta	100	4
	Zajęcia z udziałem nauczycieli	52	2
	Zajęcia powiązane z działalnością naukową	86	3.4
	Zajęcia o charakterze praktycznym	56	2.7

autor

**kierownik jednostki organizacyjnej
odpowiedzialnej za przedmiot**

mgr inż. Tomasz Kijko

tytuł, stopień naukowy, imię, NAZWISKO, podpis

dr hab. Kojdecki Marek

tytuł, stopień naukowy, imię, NAZWISKO, podpis