

"ZATWIERDZAM"

.....

.....

KARTA INFORMACYJNA PRZEDMIOTU

Nazwa przedmiotu	Funkcje boolowskie w kryptologii				Boolean Functions in Cryptology				
Kod przedmiotu	WCYKSWSM_FBK.....FBK								
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		
	VI	razem	wykłady	ćwiczenia	laboratoria	projekt	seminarium		
	razem	44x	24	20+					
Przedmioty wprowadzające	● Brak przedmiotów kształcenia wprowadzających								
Semestr/kierunek studiów	semestr 6 / Kryptologia i cyberbezpieczeństwo / Systemy kryptograficzne								
Autor	mgr inż. Tomasz Kijko								
Jednostka odpowiedzialna za przedmiot	Wydział Cybernetyki, Instytut Matematyki i Kryptologii								
Skrócony opis przedmiotu	● Wykłady i ćwiczenia audytoryjne.								
Pełny opis przedmiotu (treści programowe)	lp.	Semestr VI temat/tematyka zajęć			liczba godzin				
					wkl.	ćw.	lab.	prj.	sem.
	1	Przedstawienia funkcji boolowskich.			2	2			
	2	Algebraiczna postać normalna.			2	2			
	3	Transformata Walsh-Hadamarda.			2	2			
	4	Nieliniowość w sensie Hamminga.			2	2			
	5	Funkcje typu bent i ich konstrukcja.			2	2			
	6	Odporność korelacyjna i kryteria odporności korelacyjnej. Twierdzenie Sigenthalera.			2	2			
	7	Kryteria propagacji. Funkcje doskonale nieliniwe.			2	2			
	8	Konstrukcje funkcji boolowskich spełniających kilka krteriów. problemy optymalizacji.			4	2			
	9	Zastosowanie kryptograficznych funkcji boolowskich w konstrukcji szyfrów blokowych i strumieniowych.			6	4			
		Razem			24	20			
Literatura	podstawowa: ● J. Szmidt, Kryptograficzne własności funkcji boolowskich, materiały konferencyjne, ENIGMA 2001 ● Bart Preenel, praca doktorska, Universytet Leuven, 1994 ● T. Cusick, P. Stanica, Cryptographic Boolean Functions and Applications, Elsevier, 2017 uzupełniająca: ● Sloane, McWilliams, The Theory of Error-Correcting Codes, 1977 ● R. O'Donnell, Analysis of Boolean Functions, Cambridge University Press, 2014								
Efekty uczenia się	Symbol	Efekty kształcenia					odniesienie do efektów kształcenia dla kierunku		
	W1	Nauczyć podstawowych faktów i twierdzeń o kryptograficznych własnościach funkcji boolowskich.					K_W22		
	U1	Nauczyć zastosowania funkcji boolowskich do konstrukcji symetrycznych i strumieniowych algorytmów szyfrowania.					K_W23, K_U19		
	U2	Nauczyć zastosowania funkcji boolowskich w kryptoanalizie					K_W23, K_U19		
Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez studenta zakładanych efektów uczenia się)	● Obecność na zajęciach jest obowiązkowa. ● Zaliczenie ćwiczeń odbywa się na podstawie oceny z kolokwium przeprowadzonego na ostatnich ćwiczeniach. ● Zaliczenie z przedmiotu przeprowadzane jest w formie ustnej. Warukiem koniecznym do dopuszczenia do zaliczenia jest pozytywna ocena z ćwiczeń. Na ocenę końcową z przedmiotu składają się: ocena z zaliczenia ustnego (z wagą 0.6) oraz ocena z ćwiczeń (z wagą 0.4), przy czym aby student zaliczył przedmiot na ocenę pozytywną, obie oceny składowe muszą być pozytywne (min. 3.0).								

Bilans ECTS (nakład pracy studenta)	SEMESTR 6		
	Aktywność	Obciążenie studenta	
		Liczba godzin	Liczba ECTS
	Udział w wykładach	24	0.5
	Udział w laboratoriach	0	0
	Udział w ćwiczeniach	20	1.4
	Udział w projektach	0	0
	Udział w seminariach	0	0
	Samodzielne studiowanie tematyki wykładów	20	0.5
	Samodzielne przygotowanie do laboratoriów	34	1.6
	Samodzielne przygotowanie do ćwiczeń		
	Samodzielna realizacja projektu		
	Samodzielne przygotowanie do seminariów		
	Udział w konsultacjach	6	0.1
	Przygotowanie do egzaminu		
	Przygotowanie do zaliczenia	16	0.6
	Udział w egzaminie / kolokwium	6	0.3
	Sumaryczne obciążenie pracą studenta	126	5
	Zajęcia z udziałem nauczycieli	56	2.3
	Zajęcia powiązane z działalnością naukową	98	4
	Zajęcia o charakterze praktycznym	54	3

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