

"ZATWIERDZAM"

.....

.....

KARTA INFORMACYJNA PRZEDMIOTU

Nazwa przedmiotu	Algorytmy blokowe							Block Ciphers			
Kod przedmiotu	WCYKSWSM_ABL.....ABL										
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				
	VII	60x	40	12+	8			4.0			
	razem		40	12	8			4.0			
Przedmioty wprowadzające	● Wstęp do kryptologii -										
Semestr/kierunek studiów	semestr 7 / Kryptologia i cyberbezpieczeństwo / Systemy kryptograficzne										
Autor	dr inż. Michał Misztal										
Jednostka odpowiedzialna za przedmiot	Instytut Matematyki i Kryptologii										
Skrócony opis przedmiotu	● Wykład ● Ćwiczenia ● Laboratorium										
Pełny opis przedmiotu (treści programowe)	lp.	Semestr VII temat/tematyka zajęć					liczba godzin				
							wkł.	ćw.	lab.	prj.	sem.
	1	Podstawy szyfrowania blokowego. Różnice i podobieństwa do szyfrów strumieniowych. Definicje szyfrów blokowych. Zastosowania.					2				
	2	Tryby pracy szyfrów blokowych. Szyfrowanie uwierzytelnione. Kaskada szyfrów i szyfrowanie wielokrotne.					4				
	3	Podstawowy konstrukcji szyfrów blokowych. Teoria Shannona. Operacje liniowe i nieliniowe, dyfuzja i konfuzja. Bezpieczeństwo szyfrów.					2				
	4	Standard szyfrowania DES. Szyfr IDEA.					4	2			
	5	Konkurs AES. Wymagania, zgłoszone algorytmy. Szyfry Rijndael (AES) i RC6.					4				
	6	Projekt NESSIE. Przegląd zgłoszonych algorytmów. Szyfr Noekeon.					4	2			
	7	Inne szyfry blokowe.						6			
	8	Metody kryptoanalizy szyfrów blokowych.					4	2			
	9	Podstawy projektowania szyfrów blokowych.					2				
	10	Podstawowe pojęcia projektowania szyfrów blokowych.					2				
	11	Strategia szerokiej ścieżki. Podstawowe założenia.					2				
	12	Strategia szerokiej ścieżki. Warstwa dyfuzji.					4		4		
	13	Strategia szerokiej ścieżki. Warstwa nieliniowa.					2		4		
	14	Strategia szerokiej ścieżki. Algorytm generowania podkluczy.					2				
	17	Projekty szyfrów: SHARK, SQUARE. Poprzednicy i następcy Rijndaela.					2				
		Razem					40	12	8		
	Literatura	podstawowa: ● B. Schneier "Kryptografia dla praktyków", wyd. II, WNT 2002 ● J. Szmidt, M. Misztal "Wstęp do kryptologii", WSISiZ, wyd. III, Warszawa 2003 uzupełniająca: ● L. R. Knudsen "Contemporary Block Ciphers" 1998 ● J. Deamen, V. Rijmen "Design of Rijndael" Springer-Verlag 2002									
Efekty uczenia się	Symbol	Efekty kształcenia					odniesienie do efektów kształcenia dla kierunku				
	U1	Nauczyć zasad szyfrowania blokowego, reguł konstruowania komponentów szyfrów blokowych.					K_U19 K_W22 K_W23				
	W1	Znajomość znanych szyfrów blokowych. wymagań stawianych					K_U19 K_W22 K_W23				

	Symbol	Efekty kształcenia	odniesienie do efektów kształcenia dla kierunku	
		współczesnym szyfrowym blokowym.		
Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez studenta zakładanych efektów uczenia się)	• Przedmiot zaliczany jest na podstawie egzaminu i zaliczenia ćwiczeń. • Egzamin przeprowadzany jest w formie pisemnej. • Warunkiem dopuszczenia do egzaminu jest zaliczenie ćwiczeń. • Warunkiem koniecznym zaliczenia ćwiczeń jest uzyskanie minimalnej liczby punktów z ćwiczeń i z każdego sprawozdania. • Efekt U1 sprawdzany jest egzaminem, a efekt W1 zaliczeniem i uczestnictwem w ćwiczeniach i laboratoriach.			
Bilans ECTS (nakład pracy studenta)	SEMESTR 7			
	Aktywność	Obciążenie studenta		
		Liczba godzin	Liczba ECTS	
	Udział w wykładach	40	1	
	Udział w laboratoriach	8	0.5	
	Udział w ćwiczeniach	12	0.5	
	Udział w projektach	0	0	
	Udział w seminariach	0	0	
	Samodzielne studiowanie tematyki wykładów	30	1	
	Samodzielne przygotowanie do laboratoriów	20	0.5	
	Samodzielne przygotowanie do ćwiczeń	20	0.5	
	Samodzielna realizacja projektu			
	Samodzielne przygotowanie do seminariów			
	Udział w konsultacjach			
	Przygotowanie do egzaminu	6		
	Przygotowanie do zaliczenia			
	Udział w egzaminie / kolokwium	2		
	Sumaryczne obciążenie pracą studenta	138	4	
	Zajęcia z udziałem nauczycieli	62	2	
	Zajęcia powiązane z działalnością naukową	130	4	
	Zajęcia o charakterze praktycznym	60	2	

autor

**kierownik jednostki organizacyjnej
odpowiedzialnej za przedmiot**

dr inż. Michał Misztal
tytuł, stopień naukowy, imię, NAZWISKO, podpis

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