

"ZATWIERDZAM"

.....

.....

KARTA INFORMACYJNA PRZEDMIOTU

Nazwa przedmiotu	Wybrane elementy kryptologii					Chosen Elements of Cryptology				
Kod przedmiotu	WCYKSWSM_.....									
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			
	V	60x	24		36+			4.0		
	razem		24		36			4.0		
Przedmioty wprowadzające	• Matematyka dyskretna I - • Matematyka dyskretna II -									
Semestr/kierunek studiów	semestr 5 / Kryptologia i cyberbezpieczeństwo / wszystkie specjalności									
Autor	dr inż. Michał Misztal									
Jednostka odpowiedzialna za przedmiot	Wydział Cybernetyki, Instytut Matematyki i Kryptologii									
Skrócony opis przedmiotu	• Wykład. • Laboratorium.									
Pełny opis przedmiotu (treści programowe)	lp.	Semestr V temat/tematyka zajęć				liczba godzin				
						wkł.	ćw.	lab.	prj.	sem.
	1	Podstawowe pojęcia kryptografii i kryptologii. Definicja kryptosystemu.				2				
	2	Podstawowe szyfry podstawieniowe i przestawieniowe.				2		4		
	3	Elementy kryptoanalizy.				2		4		
	4	Szyfry strumieniowe.				2		4		
	5	Współczesne algorytmy blokowe.				4		4		
	6	Kryptosystemy klucza publicznego. Algorytm RSA i ElGamala.				2		6		
	7	Jednokierunkowe funkcje skrótu.				2		4		
	8	Protokoły kryptograficzne. Schematy podpisu cyfrowego.				4		6		
	9	Bezpieczeństwo szyfrów i systemów kryptograficznych.				4		4		
	Razem				24		36			
Literatura	podstawowa:									
	• Szmidt J., Misztal M.; Wstęp do kryptologii; WSISiZ, 2001 • Schneier B.; Kryptografia dla praktyków, WNT, wyd. II, 2002									
	uzupełniająca:									
	• A. Menezes, P. van Oorschoot, S. Vanstone "Kryptografia stosowana" WNT, Warszawa 2006. • R. Stinson "Kryptografia" WNT Warszawa 2005.									
Efekty uczenia się	Symbol	Efekty kształcenia				odniesienie do efektów kształcenia dla kierunku				
	U1	Zna najważniejsze standardy kryptograficzne i potrafi ocenić ich bezpieczeństwo				K_U03 K_W02				
	W1	Ma ogólną wiedzę dotyczącą zakresu zastosowań kryptografii w praktyce.				K_U03 K_U17 K_W02				
Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez studenta zakładanych efektów uczenia się)	• Zaliczenie przedmiotu odbywa się na podstawie egzaminu pisemnego. • Warunkiem dopuszczenia do egzaminu jest zaliczenie ćwiczeń laboratoryjnych. • Ćwiczenia laboratoryjne zaliczane są na podstawie ocen wykonanych programów. • Efekt U1 sprawdzany jest egzaminem pisemnym, a efekt W1 zaliczeniem i uczestnictwem w laboratoriach.									
Bilans ECTS (nakład pracy studenta)	SEMESTR 5									
	Aktywność				Obciążenie studenta					
					Liczba godzin		Liczba ECTS			
	Udział w wykładach				24		1			
	Udział w laboratoriach				36		1			
	Udział w ćwiczeniach				0		0			
	Udział w projektach				0		0			
Udział w seminariach				0		0				

	SEMESTR 5		
	Aktywność	Obciążenie studenta	
		Liczba godzin	Liczba ECTS
	Samodzielne studiowanie tematyki wykładów	20	1
	Samodzielne przygotowanie do laboratoriów	30	1
	Samodzielne przygotowanie do ćwiczeń		
	Samodzielna realizacja projektu		
	Samodzielne przygotowanie do seminariów		
	Udział w konsultacjach		
	Przygotowanie do egzaminu		
	Przygotowanie do zaliczenia	2	
	Udział w egzaminie / kolokwium	2	
	Sumaryczne obciążenie pracą studenta	114	4
	Zajęcia z udziałem nauczycieli	62	2
	Zajęcia powiązane z działalnością naukową	110	4
	Zajęcia o charakterze praktycznym	66	2

autor

**kierownik jednostki organizacyjnej
odpowiedzialnej za przedmiot**

dr inż. Michał Misztal

tytuł, stopień naukowy, imię, NAZWISKO, podpis

dr hab. Koidecki Marek

tytuł, stopień naukowy, imię, NAZWISKO, podpis