"ZATWIERDZAM"

.....

.....

KARTA INFORMACYJNA PRZEDMIOTU

Nazwa przedmiotu	Wstęp do kryptologii / Introduction to Cryptology
Kod przedmiotu	WCYILWSM_WDK.....WDK
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	
IV	20+	10		10+			1.0
razem		10		10			1.0

Przedmioty wprowadzające	• Brak przedmiotów kształcenia wprowadzających
Semestr/kierunek studiów	semestr 4 / Informatyka / 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 IV temat/tematyka zajęć	liczba godzin wkł.	ćw.	lab.	prj.	sem.
1	Podstawowe pojęcia kryptografii i kryptologii. Definicja kryptosystemu.	1				
2	Podstawowe szyfry podstawieniowe i przestawieniowe.	1		1		
3	Elementy kryptoanalizy.	1		1		
4	Szyfry strumieniowe.	1		1		
5	Współczesne algorytmy blokowe.	2		3		
6	Kryptosystemy klucza publicznego. Algorytm RSA i jego bezpieczeństwo.	2		2		
7	Jednokierunkowe funkcje skrótu.	1		1		
8	Protokoły kryptograficzne. Schematy podpisu cyfrowego.	1		1		
	Razem	10		10		

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
W1	Nauczyć podstawowych pojęć kryptografii i kryptoanalizy.	K_W02, K_U17
W2	Zapoznać z pojęciami szyfrów historycznych i współczesnych algorytmów kryptograficznych.	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 oceny wykonanych programów oraz wyniku sprawdzianu pisemnego przeprowadzanego na ostatnich zajęciach.
- Efekt W1 sprawdzany jest sprawdzianem pisemnym, a efekt W2 zaliczeniem i uczestnictwem w ćwiczeniach i laboratoriach.

Bilans ECTS (nakład pracy studenta)

SEMESTR 4		
Aktywność	**Obciążenie studenta**	
	Liczba godzin	**Liczba ECTS**
Udział w wykładach	10	0.25
Udział w laboratoriach	10	0.25
Udział w ćwiczeniach	0	0
Udział w projektach	0	0
Udział w seminariach	0	0
Samodzielne studiowanie tematyki wykładów	5	0.25

	SEMESTR 4		
	Aktywność	**Obciążenie studenta**	
		Liczba godzin	**Liczba ECTS**
	Samodzielne przygotowanie do laboratoriów		
	Samodzielne przygotowanie do ćwiczeń	5	0.25
	Samodzielna realizacja projektu		
	Samodzielne przygotowanie do seminariów		
	Udział w konsultacjach		
	Przygotowanie do egzaminu		
	Przygotowanie do zaliczenia		
	Udział w egzaminie / kolokwium		
	Sumaryczne obciążenie pracą studenta	30	1
	Zajęcia z udziałem nauczycieli	20	0.5
	Zajęcia powiązane z działalnością naukową	30	1
	Zajęcia o charakterze praktycznym	15	0.5

autor

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

kierownik jednostki organizacyjnej odpowiedzialnej za przedmiot

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