

"ZATWIERDZAM"

.....

.....

KARTA INFORMACYJNA PRZEDMIOTU

Nazwa przedmiotu	Jednokierunkowe funkcje skrótu					One Way Hash Functions				
Kod przedmiotu	WCYKSWSM_JFS.....JFS									
Język wykładowy	polski									
Profil studiów	ogólnoakademicki									
Forma studiów	studia stacjonarne									
Poziom studiów	wojskowe studia jednolite magisterskie									
Rodzaj przedmiotu	wybieralny									
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	30+	10	10	10+			2.0		
	razem		10	10	10			2.0		
Przedmioty wprowadzające	● Wstęp do kryptologii -									
Semestr/kierunek studiów	semestr 7 / Kryptologia i cyberbezpieczeństwo / Systemy kryptograficzne									
Autor	dr inż. Michał Misztal									
Jednostka odpowiedzialna za przedmiot	Wydział Cybernetyki/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	Podstawowe pojęcia i zastosowania funkcji skrótu.				2				
	2	Zasady konstruowania funkcji skrótu.				2				
	3	Podstawowe funkcje skrótu: rodzina SHA i MD.				2				
	4	Podstawowe ataki na jednokierunkowe funkcje skrótu. Kolizje. Paradoks urodzin.				2		10		
	5	Kryptoanaliza funkcji skrótu.				2				
	6	Wybrane funkcje skrótu.					10			
	Razem				10	10	10			
Literatura	podstawowa:									
	● Schneier B. "Kryptografia dla praktyków", wyd. II, WNT 2002 ● Preneel B. "Analysis and Design of cryptographic hash functions", Rozprawa doktorska 1993 uzupełniająca: ● Robling-Denning D. E. "Kryptografia i ochrona danych", WNT 1982 ● Szmidt J, Misztal M. "Wstęp do kryptologii", Skrypt WSIZIS, Warszawa 2003									
Efekty uczenia się	Symbol	Efekty kształcenia					odniesienie do efektów kształcenia dla kierunku			
	W1	ma wiedzę na temat podstaw konstruowania i kryptoanalizy funkcji skrótu					K_W23			
	U1	potrafi dokonać krytycznej analizy funkcji skrótu oraz wykorzystać niezbędną wiedzę matematyczną na potrzeby tej analizy; potrafi pozyskiwać informacje z literatury w tym głównie w języku angielskim					K_U19 K_W22 K_W23			
Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez studenta zakładanych efektów uczenia się)	● Moduł kształcenia zaliczany jest na podstawie: zaliczenia ćwiczeń i zadania laboratoryjnego. ● Warunkiem koniecznym do uzyskania zaliczenia ćwiczeń jest udział w co najmniej 80% zajęć i zaliczenie zadania laboratoryjnego. ● Efekty W1, U2 sprawdzane są na zaliczeniu ćwiczeń i laboratorium.									
Bilans ECTS (nakład pracy studenta)	SEMESTR 7									
	Aktywność					Obciążenie studenta				
						Liczba godzin		Liczba ECTS		
	Udział w wykładach					10		0.5		
	Udział w laboratoriach					10		0.25		
	Udział w ćwiczeniach					10		0.25		
	Udział w projektach					0		0		
Udział w seminariach					0					

	SEMESTR 7		
	Aktywność	Obciążenie studenta	
		Liczba godzin	Liczba ECTS
	Samodzielne studiowanie tematyki wykładów	20	0.5
	Samodzielne przygotowanie do laboratoriów	10	0.25
	Samodzielne przygotowanie do ćwiczeń	10	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	70	2
	Zajęcia z udziałem nauczycieli	30	1
	Zajęcia powiązane z działalnością naukową	70	2
	Zajęcia o charakterze praktycznym	40	1

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