

"ZATWIERDZAM"

.....

.....

KARTA INFORMACYJNA PRZEDMIOTU

Nazwa przedmiotu	Generacja i testowanie losowości					Generation and Testing of Randomness				
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			
	VIII	44+	20	10	14+			3.0		
	razem		20	10	14			3.0		
Przedmioty wprowadzające	● Brak przedmiotów kształcenia wprowadzających									
Semestr/kierunek studiów	semestr 8 / Kryptologia i cyberbezpieczeństwo / Systemy kryptograficzne									
Autor	mgr inż. Krzysztof Mańk, mgr inż. Łukasz Dziel									
Jednostka odpowiedzialna za przedmiot	Wydział Cybernetyki / Instytut Matematyki i Kryptologii / Laboratorium Badawcze Kryptologii									
Skrócony opis przedmiotu	● Wykład ● Ćwiczenia ● Laboratorium									
Pełny opis przedmiotu (treści programowe)	lp.	Semestr VIII temat/tematyka zajęć				liczba godzin				
						wkł.	ćw.	lab.	prj.	sem.
	1	Podstawowe pojęcia - generator losowy, test statystyczny, błędy I i II rodzaju, wielopoziomowa procedura testowania, testowanie generatorów. Pojęcie losowości. Klasyfikacja testów losowości.				4		2		
	2	Generacja losowości w FPGA				2		4		
	3	Testy losowości				6	6			
	4	Pakiety testów losowości, ograniczenia testów, zbieżność rozkładu, korelacja statystyk				4		6		
	5	Pakiety testów losowości dla implementacji hardware				2	4	2		
	6	Gromadzenie entropii				2				
	Razem				20	10	14			
Literatura	podstawowa:									
	● A. Rukhin i inni, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, NIST Special Publication 800-22, 2001 ● P. L'Ecuyer, R. Simard, TestU01: A C Library for Empirical Testing of Random Number Generators, 2002 ● R.G. Brown, DIEHARDER: A GNU Public Licensed Random Number Tester, Duke University Physics Department, 2006 ● G. Marsaglia, DIEHARD Battery of Tests of Randomness, 1995 ● D.E. Knuth, Sztuka programowania, t.2. Algorytmy seminumeryczne, WNT, 2002 tłumaczenie trzeciego wydania: The Art of Computer Programming, 1997 uzupełniająca: ● R. Wieczorkowski, R. Zieliński R., Komputerowe generatory liczb losowych, WNT, Warszawa, 1997 ● A. Menezes, P. van Oorschot, S. Vanstone, Handbook of Applied Cryptography ● K. Mańk, Dokładne dystrybuanty statystyk w testach momentów 1 i 2 rzędu, Biuletyn WAT, Kryptologia IV, Warszawa, 2004									
Efekty uczenia się	Symbol	Efekty kształcenia				odniesienie do efektów kształcenia dla kierunku				
	W1	Zna i rozumie podstawowe pojęcia związane z generacją i testowaniem losowości				K_W02				
	W2	Zna podstawowe testy losowości, zasady i ograniczenia ich stosowalności				K_W02				
	W3	Zna powszechnie stosowane pakiety testów losowości				K_W02				
	U1	Umie zaprojektować procedurę testową na podstawie testu losowości				K_U03				
	U2	Umie zaprojektować i zaimplementować w języku opisu sprzętu				K_U03				

	Symbol	Efekty kształcenia	odniesienie do efektów kształcenia dla kierunku	
		prosty zestaw testów losowości		
Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez studenta zakładanych efektów uczenia się)	• Przedmiot zaliczany jest na podstawie egzaminu. Warunkiem dopuszczenia do egzaminu jest zaliczenie laboratorium. • Ocena z egzaminu jest wyznaczana na podstawie średniej ważonej ocen z pisemnej pracy kontrolnej (35%), oceny z zajęć laboratoryjnych (50%) i oceny aktywności w trakcie zajęć audytoryjnych (15%). Ocena jest zaokrąglona w górę do najbliższej oceny zgodnej z Regulaminem Studiów. • Ocena z pisemnej pracy kontrolnej wystawiana jest na podstawie sumy zdobytych punktów: 2.0 (ndst) - od 0 do 59 punktów; 3.0 (dst) - od 60 do 65 punktów; 3.5 (dst+) - od 66 do 72 punktów; 4.0 (db) - od 73 do 80 punktów; 4.5 (db+) - od 81 do 89 punktów; 5.0 (bdb) - od 90 punktów. Nieobecność na pracy kontrolnej traktowana jest jak uzyskanie oceny negatywnej. Pracę kontrolną można poprawić w terminach poprawkowych. • Każde Zadanie laboratoryjne podlega ocenie; Zajęcia laboratoryjne zaliczane są na podstawie Rozwiązań Zadań Indywidualnych (RZI), weryfikacji samodzielności ich wykonania oraz Aktywności Podczas Zajęć (APZ); Zadania Indywidualne dotyczą każdego z zajęć praktycznych lub etapów zadania projektowego i polegają na przedstawieniu swojej pracy oraz rozwiązań praktycznych problemów dotyczących tematyki zajęć; Samodzielność wykonania RZI jest weryfikowana poprzez: analizę (w tym porównawczą) napisanych prac, odpowiedzi pisemne lub ustne podczas zajęć w trakcie semestru lub w terminach sesji, w formie stacjonarnej lub zdalnej, niezależnie od formy prowadzenia zajęć; RZI są oceniane w skali: ZAL - (1 punkt) - w przypadku, gdy rozwiązanie zadania jest prawidłowe, lub wykonane starannie i zawiera nieistotne błędy lub niewielkie braki, NZAL - (0 punktów) - w przeciwnym przypadku. Ostateczne terminy przesłania RZI lub ich popraw, które umożliwiają uzyskanie oceny w poszczególnych terminach zaliczenia, są podane w zespole Microsoft Teams uruchomionym do zajęć; Aktywność Podczas Zajęć dotyczy każdego z zajęć praktycznych lub etapów zadania projektowego i polega na aktywnym braniu udziału w zajęciach, w szczególności poprzez dyskusję nad problemami i rozwiązywaniu zadań podczas zajęć; Aktywność Podczas Zajęć jest oceniana zgodnie z następującymi wytycznymi: 1 punkt - udzielanie istotnej liczby poprawnych odpowiedzi podczas zajęć lub etapu zadania projektowego, 0 punktów - w przeciwnym przypadku; Aktywności Podczas Zajęć się nie poprawia; Ocena końcowa z zajęć praktycznych we wszystkich terminach jest wystawiana na podstawie ilorazu sumy uzyskanych punktów z Rozwiązań Zadań Indywidualnych i Aktywności Podczas Zajęć oraz liczby zajęć lub etapów zadania projektowego, z dokładnością do dwóch miejsc po przecinku w następujący sposób: 0.00 i w przypadku nieoddania żadnego z RZI - NB; od 0.01 do 0.99 - 2 (ndst); od 1.00 do 1.11 - 3.0 (dst); od 1.12 do 1.23 - 3.5 (dst+); od 1.24 do 1.35 - 4.0 (db); od 1.36 do 1.47 - 4.5 (db+); od 1.48 do 2.00 - 5.0 (bdb). • Ocena aktywności w trakcie zajęć audytoryjnych jest średnią arytmetyczną, obliczoną z dokładnością do dwóch miejsc po przecinku, z ocen uzyskanych przez Studenta za rozwiązywanie zadań i udzielanie odpowiedzi w trakcie zajęć audytoryjnych. W przypadku braku ocen przyjmuje się, że średnia wynosi 3.50.			
Bilans ECTS (nakład pracy studenta)	SEMESTR 8			
	Aktywność	Obciążenie studenta		
		Liczba godzin	Liczba ECTS	
	Udział w wykładach	20	0.2	
	Udział w laboratoriach	14	0.2	
	Udział w ćwiczeniach	10	0.2	
	Udział w projektach	0	0	
	Udział w seminariach	0	0	
	Samodzielne studiowanie tematyki wykładów	10	0.5	
	Samodzielne przygotowanie do laboratoriów	10	0.6	
	Samodzielne przygotowanie do ćwiczeń	10	0.5	
	Samodzielna realizacja projektu	25	0.5	
	Samodzielne przygotowanie do seminariów			
	Udział w konsultacjach			
	Przygotowanie do egzaminu			
	Przygotowanie do zaliczenia			
	Udział w egzaminie / kolokwium	2	0.3	
	Sumaryczne obciążenie pracą studenta	101	3	
	Zajęcia z udziałem nauczycieli	46	0.9	

	SEMESTR 8		
	Aktywność	Obciążenie studenta	
		Liczba godzin	Liczba ECTS
	Zajęcia powiązane z działalnością naukową	99	2.7
	Zajęcia o charakterze praktycznym	69	2

autorzy

mgr inż. Krzysztof Mańk
tytuł, stopień naukowy, imię, NAZWISKO, podpis

mgr inż. Łukasz Dziel
tytuł, stopień naukowy, imię, NAZWISKO, podpis

kierownik jednostki organizacyjnej odpowiedzialnej za przedmiot

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