

"ZATWIERDZAM"

.....

.....

KARTA INFORMACYJNA PRZEDMIOTU

Nazwa przedmiotu	Quantum and Post-Quantum Cryptology (w języku angielskim)				Quantum and Post-Quantum Cryptology				
Kod przedmiotu	WCYKSWSM_.....								
Język wykładowy	polski								
Profil studiów	ogólnoakademicki								
Forma studiów	studia stacjonarne								
Poziom studiów	wojskowe studia jednolite magisterskie								
Rodzaj przedmiotu									
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		
	IX	44x	30	14+				4.0	
	razem		30	14				4.0	
Przedmioty wprowadzające	- Fizyka II - - Język angielski - - Metody statystyczne w kryptologii - - Protokoły kryptograficzne - - Wprowadzenie do programowania - - Wstęp do kryptoanalizy klucza publicznego -								
Semestr/kierunek studiów	semestr 9 / Kryptologia i cyberbezpieczeństwo / Systemy kryptograficzne								
Autor	dr Mariusz Jurkiewicz								
Jednostka odpowiedzialna za przedmiot	WCY/IMK/LBK								
Skrócony opis przedmiotu	- Wykład - Ćwiczenia								
Pełny opis przedmiotu (treści programowe)	lp.	Semestr IX temat/tematyka zajęć				liczba godzin			
		wkl.	ćw.	lab.	prj.	sem.			
	1	Fundamental notions in Hilbert spaces theory and quantum mechanics				2			
	2	Qubit, quantum register, quantum logic gates, quantum circuits				2	2		
	3	Quantum Fourier transform and its inverse; Shor algorithm				4			
	4	Grouver algorithm and its consequences				2			
	5	Formal notion of DSS and EUF-CMA security models; Hash-based DSS				6	4		
	6	Lattice-based cryptography, zero-knowledge proofs, LWE, RLWE				2			
	7	Formal models for Public-key Encryption schemes, IND-CPA, IND-CCA1, IND-CCA2				2			
	8	Frodo KE scheme				4	4		
	9	Number Theoretic Transform (NTT)				2			
	10	New Hope KE scheme				4	4		
	Razem				30	14			
Literatura	podstawowa: - https://csrc.nist.gov/projects/post-quantum-cryptography - Eleanor Rieffel and Wolfgang Polak, QUANTUM COMPUTING A Gentle Introduction, The MIT Press Cambridge Massachusetts-London, 2011. - D.J. Bernstein, J. Buchmann, E. Dahmen (eds.), Post-Quantum Cryptography, Springer 2009. uzupełniająca: - https://eprint.iacr.org								
Efekty uczenia się	Symbol	Efekty kształcenia					odniesienie do efektów kształcenia dla kierunku		
	W01	Posiada uporządkowaną, podbudowaną teoretycznie wiedzę dotyczącą języka oraz metod dotyczących ataków kwantowych i kryptografii postkwantowej					K_U02, K_W08		
	U01	Umie posługiwać się w podstawowym zakresie językiem kryptoanalizy kwantowej oraz kryptografii postkwantowej w kontekście konstrukcji schematów asymetrycznych oraz analizy ich bezpieczeństwa w określonych modelach.					K_K01, K_U02, K_U11, K_W06, K_W08, K_W14		
	K01	Jest gotów do krytycznej oceny posiadanej wiedzy i jej znaczenia					K_U02, K_U18, K_W06,		

	Symbol	Efekty kształcenia	odniesienie do efektów kształcenia dla kierunku	
		w rozwiązywaniu problemów poznawczych i praktycznych	K_W14	
Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez studenta zakładanych efektów uczenia się)	• Przedmiot zaliczany jest na podstawie egzaminu sprawdzającego wiedzę (W01 i K01) i umiejętności (U01). • Egzamin przeprowadzany jest w formie pisemnej lub ustnej. • Warunkiem dopuszczenia do egzaminu jest zaliczenie laboratorium oraz obecność na co najmniej 90% zajęć. Ćwiczenia zaliczane są na podstawie wyników prac wykonywanych pod bezpośrednią kontrolą podczas zajęć (U01, W01, K01) oraz projektu końcowego (U01). Dodatkowo studenci otrzymują wskazówki do samodzielnego studiowania z zachętą do korzystania z różnorodnych źródeł wiedzy. • Skala ocen: dostatecznie (3) - student zna i rozumie większość wyłożonych zagadnień, umie rozwiązywać najprostsze problemy; dobrze (4) - student zna i rozumie znaczną większość wyłożonych zagadnień, umie rozwiązywać najprostsze problemy oraz interpretować ich wyniki; bardzo dobrze (5) - student zna i rozumie wszystkie wyłożone zagadnienia, umie rozwiązywać postawione problemy oraz interpretować ich wyniki; dość dobrze (3,5) i ponad dobrze (4,5) - pośrednio między dostatecznie i dobrze oraz między dobrze i bardzo dobrze.			
Bilans ECTS (nakład pracy studenta)	SEMESTR 9			
	Aktywność	Obciążenie studenta		
		Liczba godzin	Liczba ECTS	
	Udział w wykładach	30	0.7	
	Udział w laboratoriach	0	0	
	Udział w ćwiczeniach	14	0.5	
	Udział w projektach	0	0.5	
	Udział w seminariach	0	0	
	Samodzielne studiowanie tematyki wykładów	20	0.25	
	Samodzielne przygotowanie do laboratoriów			
	Samodzielne przygotowanie do ćwiczeń	15	0.25	
	Samodzielna realizacja projektu	10	1	
	Samodzielne przygotowanie do seminariów			
	Udział w konsultacjach	2		
	Przygotowanie do egzaminu	25	0.35	
	Przygotowanie do zaliczenia	15	0.35	
	Udział w egzaminie / kolokwium	4	0.1	
	Sumaryczne obciążenie pracą studenta	135	4	
	Zajęcia z udziałem nauczycieli	50	1.8	
	Zajęcia powiązane z działalnością naukową	89	3.2	
	Zajęcia o charakterze praktycznym	39	2.25	

autor

kierownik jednostki organizacyjnej
odpowiedzialnej za przedmiot

dr Mariusz Jurkiewicz
tytuł, stopień naukowy, imię, NAZWISKO, podpis

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