

.....

KARTA INFORMACYJNA PRZEDMIOTU

Nazwa przedmiotu	Protokoły kryptograficzne							Cryptographic Protocols		
Kod przedmiotu	WCYKSCSI_PKR.....PKR									
Język wykładowy	polski									
Profil studiów	ogólnoakademicki									
Forma studiów	studia stacjonarne									
Poziom studiów	studia pierwszego stopnia									
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	30+	16		14+			2.0		
	razem		16		14			2.0		
Przedmioty wprowadzające	● Brak przedmiotów kształcenia wprowadzających									
Semestr/kierunek studiów	semestr 4 / Kryptologia i cyberbezpieczeństwo / wszystkie specjalności									
Autor	mgr inż. Tomasz Kijko									
Jednostka odpowiedzialna za przedmiot	Instytut Matematyki i Kryptologii									
Skrócony opis przedmiotu	● Wykład, ćwiczenia									
Pełny opis przedmiotu (treści programowe)	lp.	Semestr IV temat/tematyka zajęć				liczba godzin				
						wkl.	ćw.	lab.	prj.	sem.
	1	Wstęp do protokołów: definicja protokołu, cel stosowania, klasyfikacja protokołów				2				
	2	Podstawowy protokół negocjacji klucza D-H: etapy, czynności uczestników, zagrożenia, modyfikacje protokołu, ogólne zasady konstrukcji protokołów				2		2		
	3	Uwierzytelnianie, podział wiadomości poufnych, znakowanie czasowe, zagrożenia				3		3		
	4	Protokoły pośrednie: podpisy cyfrowe z zabezpieczeniem niezaprzeczalności i niepodrabialności, grupowe podpisy, obliczenia dla danych zaszyfrowanych				3		3		
	5	Protokoły zaawansowane: systemy kryptograficzne z uprawnionym odsłuchem, dowody twierdzeń o wiedzy zerowej, dowody tożsamości z zastosowaniem twierdzeń o wiedzy				3		3		
	6	Protokoły ezoteryczne: niezaprzeczalne przesłanie wiadomości, podpisy jednoczesne, uwierzytelniona poczta elektroniczna, wymiana jednoczesna, bezpieczne wybory i obliczenia, cyfrowe pieniądze				3		3		
	Razem					16		14		
Literatura	podstawowa: ● Bruce Schneier, Kryptografia dla praktyków, wyd. II, 2002 ● William Stallings, Ochrona danych w sieci i internecie, 1997 uzupełniająca: ● Robling - Denning D. E. Kryptografia i ochrona danych 1982									
Efekty uczenia się	Symbol	Efekty kształcenia						odniesienie do efektów kształcenia dla kierunku		
	U1	Umiejętność podstawowych zasad konstrukcji protokołów kryptograficznych						K_U18, K_W23		
	W1	Znajomość metod analizy protokołów kryptograficznych, podstawowych ataków na protokoły kryptograficzne						K_W23, K_U18		
Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez studenta zakładanych efektów uczenia się)	● Zaliczenie laboratoriów odbywa się na następujących zasadach: - wystawiana jest ocena za realizację zadań w ramach zajęć laboratoryjnych. Musi być ona pozytywna. - dopuszczalne są dwie nieobecności na laboratoriach (wpływają one na ocenę z laboratoriów). W przypadku większej liczby nieobecności przeprowadza się oddzielne ocenianie na konsultacjach; - wystawiana jest ocena za wykonane zadań w ramach kolejnych laboratoriów -- w przypadku nieoddania zadania w wyznaczonym terminie wystawiana jest ocena negatywna za to zadania; - ocena łączna za laboratoria jest średnia arytmetyczna powyższych ocen zaokrąglona w górę.									

	• Zaliczenie przedmiotu odbywa się w formie pisemnej lub ustnej. Warunkiem koniecznym do udziału w zaliczeniu przedmiotu jest pozytywna ocena z laboratoriów. W ocenie końcowej z przedmiotu uwzględniana jest ocena z laboratoriów.	
Bilans ECTS (nakład pracy studenta)	SEMESTR 4	
	Aktywność	Obciążenie studenta
		Liczba godzin Liczba ECTS
	Udział w wykładach	16 0.3
	Udział w laboratoriach	14 0.4
	Udział w ćwiczeniach	0 0
	Udział w projektach	0 0
	Udział w seminariach	0 0
	Samodzielne studiowanie tematyki wykładów	8 0.3
	Samodzielne przygotowanie do laboratoriów	12 0.4
	Samodzielne przygotowanie do ćwiczeń	
	Samodzielna realizacja projektu	
	Samodzielne przygotowanie do seminariów	
	Udział w konsultacjach	6 0.1
	Przygotowanie do egzaminu	
	Przygotowanie do zaliczenia	10 0.3
	Udział w egzaminie / kolokwium	2 0.2
	Sumaryczne obciążenie pracą studenta	68 2
	Zajęcia z udziałem nauczycieli	38 1
	Zajęcia powiązane z działalnością naukową	50 1.4
	Zajęcia o charakterze praktycznym	26 0.8

autor

**kierownik jednostki organizacyjnej
odpowiedzialnej za przedmiot**

mgr inż. Tomasz Kijko
tytuł, stopień naukowy, imię, NAZWISKO, podpis

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