

KARTA PRZEDMIOTU (SYLABUS)

Opis przedmiotu

Kod przedmiotu		Nazwa przedmiotu	TECHNOLOGIE KRYPTOGRAFICZNE	
E/O/2/NST/C1B-4A-AII			CRYPTOGRAPHIC TECHNOLOGIES	
Język wykładowy		język polski		
Rok akademicki		2023/2024		
Kierunek		Elektrotechnika		
w zakresie		Automatyka i informatyka		
Poziom studiów		studia drugiego stopnia		
Profil studiów		ogólnoakademicki		
Forma studiów		studia niestacjonarne		
Semestr / semestry		4		
Przynależność do grupy zajęć		C1B. Grupa zajęć obieralnych –do wyboru		
Status przedmiotu		obieralny		
Formy realizacji zajęć dydaktycznych, wymiar, punkty ECTS		Forma zajęć	Liczba godzin zajęć dydaktycznych	Liczba punktów ECTS
		Wykład	12 [h]	2 ECTS
		Projekt	12 [h]	
Powiązanie przedmiotu	z profilem studiów	związany z prowadzoną działalnością naukową w dyscyplinach, do których przyporządkowany jest kierunek studiów		0,5 ECTS
	z uprawnieniami	służy do zdobywania przez studenta kompetencji inżynierskich		1 ECTS
	z dyscypliną	automatyka, elektronika, elektrotechnika i technologie kosmiczne		2 ECTS
Forma nauczania		tradycyjna – zajęcia zorganizowane w Uczelni i/lub zajęcia z wykorzystaniem metod i technik kształcenia na odległość (max. 1,2 ECTS)		
Wymagania wstępne		-		
Jednostka prowadząca		Katedra Informatyki i Teleinformatyki		
Koordynator		dr hab. inż. Marcin Chrzan, prof. UTH		
Adres strony internetowej pjo		www.wteii.uniwersytetradom.pl		
Adres e-mail, telefon koordynatora		m.chrzan@uthrad.pl, +48 48 361 77 08		

EFEKTY UCZENIA SIĘ, TREŚCI PROGRAMOWE, REALIZACJA ZAJĘĆ DYDAKTYCZNYCH, WERYFIKACJA EFEKTÓW UCZENIA SIĘ

Cel kształcenia:	Przygotowanie do samodzielnego, identyfikowania i wykorzystywania systemów kryptograficznych
Treści programowe:	<p>Wykład [BN, W1, K1]:</p> <ol style="list-style-type: none"> 1. Metody klasyczne i najnowszej kryptografii 2. Podstawowe zagrożenia dotyczące integralności, poufności danych oraz dostępności do nich. Wiarygodność danych 3. Stan prawny w dziedzinie ochrony informacji oraz analizę przestępstw komputerowych 4. Modele określania pełnomocnictw oraz autentyfikacji 5. Techniki kodowania w kryptografii. Techniki szyfrowania. Standardy używane w innych krajach a odnoszące się do zagadnień bezpieczeństwa informacji 6. Metody ochrony informacji uwzględniające jej autentyczność (wiarygodność) i poufność oraz rozliczalność i niezaprzeczalność dokumentu 7. Algorytmy szyfrowania. Szyfry przestawieniowe, podstawieniowe (monoalfabetyczne, polialfabetyczne, homofoniczne, poligramowe), wykładnicze i plecakowe 8. Szyfry złożone (kaskadowe). Generatory liczb <p style="text-align: right;">Suma 12 [h]</p> <p>Projekt [BN, W1, U1, K1]:</p> <p>W ramach zajęć studenci wykonują zadanie projektowe dotyczące:</p> <ul style="list-style-type: none"> – określania pełnomocnictw oraz autentyfikacji; – techniki kodowania w kryptografii; – techniki szyfrowania. <p style="text-align: right;">Suma 12 [h]</p>

Metody dydaktyczne (kształcenia):	<ul style="list-style-type: none"> – metody podające (wykład informacyjny) – metody aktywizujące (metoda przypadków, metoda sytuacyjna, dyskusja dydaktyczna), – metody eksponujące (film, pokaz), – metody programowane (z wykorzystaniem komputera), – metody praktyczne (pokaz, ćwiczenia laboratoryjne, rachunkowe, symulacja).
Rygor zaliczenia, kryteria oceny osiągniętych efektów uczenia się, sposób obliczania oceny końcowej:	<p>Warunkiem zaliczenia przedmiotu jest osiągnięcie wszystkich wymaganych efektów uczenia się określonych dla danego przedmiotu. Uzyskanie pozytywnych ocen ze wszystkich form zajęć wchodzących w skład danego przedmiotu jest równoznaczne z jego zaliczeniem i zdobyciem przez studenta liczby punktów ECTS przyporządkowanej temu przedmiotowi. Sposób obliczenia oceny końcowej z przedmiotu określa regulamin studiów. Sposób obliczania oceny z poszczególnych form zajęć przedstawia się następująco:</p> <p>Ocenę z wykładu stanowi wynik egzaminu.</p> <p>Za wykonanie projektu student otrzymuje max 100% pkt., z czego 20% pkt. za prawidłowy tok rozwiązywania zadania, 30% pkt. za prawidłowe określenie jednostek i uzyskany wynik, 50% pkt. za prezentację wyników.</p> <p>Ocena 2 poniżej 50% pkt. Ocena 3 od 51% do 60% pkt Ocena 3,5 od 61% do 70% pkt. Ocena 4 od 71% do 80% pkt Ocena 4,5 od 81% do 90% pkt Ocena 5 powyżej 91% pkt. Ocena wg skali 2-5.</p>

Efekty uczenia się dla przedmiotu w odniesieniu do efektów kierunkowych i formy zajęć				Metody weryfikacji efektów uczenia się	
Numer efektu uczenia się	Opis efektów uczenia się dla przedmiotu (PEU) Student, który zaliczył przedmiot (W) zna i rozumie/ (U) potrafi /(K) jest gotów do:	Kierunkowy efekt uczenia się (KEU)	Forma zajęć	Forma weryfikacji (zaliczeń)	Metody sprawdzania i oceny
W1	współczesne algorytmy kryptograficzne, zagrożenia dla bezpieczeństwa danych oraz metody ich ochrony w systemach teleinformatycznych	K_WG06 K_WG08	wykład	egzamin	test otwarty
U1	praktycznie wykorzystywać zaawansowane metody kryptograficzne do zapewniania poufności i integralności transmisji danych biorąc również pod uwagę aspekty pozatechniczne	K_UW02 K_UW08 K_UO15	projekt	zaliczenie z oceną	ocena projektu
K1	świadomego i odpowiedzialnego stosowania metod i systemów kryptograficznych w budowanych i eksploatowanych systemach	K_KO02	wykład \ projekt	zaliczenie z oceną	aktywność, dyskusja, ocena projektu

Literatura i pomoce naukowe	
<ol style="list-style-type: none"> 1. F. L. Bauer, Sekrety kryptografii, Helion, Gliwice, 2003. 2. J.A. Buchmann, Wprowadzenie do kryptografii. PWN, Warszawa, 2006. 3. N. Ferguson, Kryptografia w praktyce. Helion, Gliwice, 2004. 4. M. Karbowski, Podstawy kryptografii. Helion, Gliwice, 2015. 5. Schneider, Kryptografia dla praktyków. WNT, Warszawa, 2002. 6. L. Steven, Rewolucja w kryptografii. WNT, Warszawa, 2002. 7. D.R. Stinson, Kryptografia. WNT, Warszawa, 2005. 8. Kratikal Academy, Cryptography Data and Application Security, 2017 9. Jonathan Katz, Yehuda Lindell, Introduction to Modern Cryptography. Third Edition. CRC press. 2021 10. E. Cole, R. L. Krutz, J. Conley, Bezpieczeństwo sieci. Biblia, Helion, Gliwice, 2005. 11. T. Kifner, Polityka bezpieczeństwa i ochrony informacji. Helion, Gliwice, 1999. 12. Lockhart, 100 sposobów na bezpieczeństwo sieci. Helion, Gliwice, 2005. 13. E. Schetina, K. Green, J. Carlton, Bezpieczeństwo w sieci. Helion, Gliwice, 2002. 14. M. Stawowoski, Ochrona informacji w sieciach komputerowych. ArsKom, Warszawa, 1998. 15. M. Szmít, M. Tomaszewski, M. Gusta, 101 zabezpieczeń przed atakami w sieci komputerowej. Helion, Gliwice, 2004. 16. R. Wobst, Kryptologia. Budowa i łamanie zabezpieczeń. Read Me, Warszawa, 2002. 	

Nakład pracy studenta potrzebny do osiągnięcia zakładanych efektów uczenia się – bilans punktów ECTS			
Udział w zajęciach, aktywność	Obciążenie studenta [h]		
	Inne godz. kontaktowe (IGK)	Zajęcia bez nauczyciela-praca własna studenta (ZBN)	Zajęcia dydaktyczne
Udział w wykładach	X	X	12 [h]
Udział w ćwiczeniach / laboratoriach / projektach / seminariach	X	X	12 [h]
Udział w konsultacjach	3 [h]	X	X
Przygotowanie do wykładów / ćwiczeń / laboratoriów / projektów / seminariów	X	23 [h]	X
Przygotowanie do zaliczenia/egzaminu			
Sumaryczne obciążenie pracą studenta	3 [h] /0,1 ECTS	23 [h] / 0,9 ECTS	24 [h] /1 ECTS
Punkty ECTS za przedmiot	2 ECTS		

Informacje dodatkowe, uwagi
<p>W przypadku studentów ze szczególnymi potrzebami, w tym: z niepełnosprawnością, przewlekle chorych, określone powyżej (w karcie) metody i formy weryfikacji efektów uczenia się dostosowuje się odpowiednio do indywidualnych potrzeb tych studentów.</p> <p>Szczegółowe zasady i formy wsparcia studentów ze szczególnymi potrzebami: w tym z niepełnosprawnością, przewlekle chorych podczas zajęć, zaliczeń i egzaminów określono w: Regulaminie Studiów, Zasadach Studiowania, Procedurze dotyczącej zapewnienia dostępności procesu kształcenia studentom ze szczególnymi potrzebami, w tym: z niepełnosprawnością, przewlekle chorych.</p>