

KARTA PRZEDMIOTU (SYLABUS)

Opis przedmiotu

Kod przedmiotu		Nazwa przedmiotu	KRYPTOGRAFIA I BEZPIECZEŃSTWO DANYCH	
I/O/1/NST/B2-5-2			CRYPTOGRAPHY AND DATA SECURITY	
Język wykładowy		język angielski		
Rok akademicki		2024/2025		
Kierunek		Informatyka		
w zakresie		-		
Poziom studiów		studia pierwszego stopnia		
Profil studiów		ogólnoakademicki		
Forma studiów		studia niestacjonarne		
Semestr / semestry		7		
Przynależność do grupy zajęć		B2. Grupa zajęć kierunkowych - do wyboru		
Status przedmiotu		Do wyboru		
Formy realizacji zajęć dydaktycznych, wymiar, punkty ECTS		Forma zajęć	Liczba godzin zajęć dydaktycznych	Liczba punktów ECTS
		Wykład	12 [h]	5 ECTS
		Laboratorium	18 [h]	
Powiązanie przedmiotu	z profilem studiów	związany z prowadzoną działalnością naukową w dyscyplinach, do których przyporządkowany jest kierunek studiów		4 ECTS
	z uprawnieniami	służy do zdobywania przez studenta kompetencji inżynierskich		4 ECTS
	z dyscypliną	Informatyka techniczna i telekomunikacja		5 ECTS
Forma nauczania		tradycyjna – zajęcia zorganizowane w Uczelni i/lub zajęcia z wykorzystaniem metod i technik kształcenia na odległość (max. 0,5 ECTS)		
Wymagania wstępne				
Jednostka prowadząca		Katedra Informatyki i Teleinformatyki		
Koordynator		dr hab. inż. Marcin Chrzan, prof. URad		
Adres strony internetowej pjo		www.wteii.uniwersytetradom.pl		
Adres e-mail, telefon koordynatora		m.chrzan@urad.edu.pl, +48 48 361 77 08		

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

Cel kształcenia:	The aim of the course is to familiarize the student with the theory and selected algorithms of cryptography
Treści programowe:	<p>Lecture [BN, W1, U1, K1]:</p> <ol style="list-style-type: none"> 1. Introduction - definition of information system security, criteria that such a system must meet, security maintenance measures (physical, technical, organizational and legal), 2. Block ciphers - substitution, rearrangement, Shannon substitution networks, DES, AES algorithms - their basic components, modes of operation of block ciphers, stream ciphers, pseudorandom string generators (congruent, RSA, BBS, LFSR, NLFSR) and string randomness tests. 3. Hash functions - classification of functions by structure, criteria that good hash functions must meet, MAC, attacks on hash functions, 4. Asymmetric cryptography - mathematical basis, RSA, DH, El-Gamal, Rabin algorithms, 5. Authentication methods - PAP, CHAP, EAP protocols, protocols using learned cryptographic mechanisms - symmetric, asymmetric and hash functions, overview of current authentication methods (procedural, passwordless, through social networks,...). 6. Blockchain technology - construction, security, example uses. <p style="text-align: right;">Total: 12 [h]</p> <p>Lab [BN W1,U1,K1]:</p> <ol style="list-style-type: none"> 1. Implement a simple cipher using substitution or rearrangement and perform cryptanalysis of ciphers implemented by other students. 2. Implementation of a selected mode of operation of block ciphers, using the basic ECB mode of operation, evaluation of error propagation in different modes of operation. 3. Implementation of the RSA algorithm. 4. Implementation of the DH algorithm. 5. Conducting a speed analysis of the various available hash functions, analyzing the criteria that a good hash function should meet. <p style="text-align: right;">Total: 18 [h]</p>

Metody dydaktyczne (kształcenia):	<ul style="list-style-type: none"> – giving methods (informative lecture) – problem methods (problem lecture, conversational lecture), – activating methods (case method, situational method, didactic discussion), – programmed methods (using a computer), – practical methods (demonstration, laboratory exercises, simulation).
Rygor zaliczenia, kryteria oceny osiągniętych efektów uczenia się, sposób obliczania oceny końcowej:	<p>The grade for the lecture consists of a pass mark verifying the learning outcomes. Assessment according to the 2-5 scale.</p> <p>Laboratory:</p> <p>The student receives a maximum of 100 points for the exercise, of which 20 points, for the correct course of solving the exercise, 30 points, for the correct determination of the units and the result obtained, 50 points, for the presentation of the results.</p> <p>Grade 2 less than 50 pts. Grade 3 from 51 to 60 pts. Grade 3.5 from 61 to 70 pts. Grade 4 from 71 to 80 pts. Grade 4.5 from 81 to 90 pts. Grade 5 above 91 pts. Grade according to a scale of 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	wybrane algorytmy kryptograficzne, ich rolę w zabezpieczaniu danych oraz ich zastosowania	K_WG05 K_WG10	wykład / laboratorium	zaliczenie	pisemny test otwarty
U1	stosować różne metod kryptografii i kryptoanalizy do zabezpieczania systemów teleinformatycznych	K_UW08 K_UW10 K_UW15	laboratorium	zaliczenie	punktacja zadań laboratoryjnych, ocena sprawozdań \ kolokwiów pisemnych
K1	wykorzystania metod kryptograficznych w teorii i praktyce dla zapewnienia bezpieczeństwa w systemach informatycznych.	K_KK03	wykład / laboratorium	obserwacja	dyskusja, aktywność na zajęciach, prezentacja wyników prac

Literatura i pomoce naukowe
1. J.-P Aumasson J.P. Aumasson.: Nowoczesna kryptografia. Praktyczne wprowadzenie do szyfrowania, PWN 2018 2. Marcin Karbowski . Podstawy kryptografii. Wydanie 3. Helion 2021 3. R.Douglas Stinson. Kryptografia w teorii i praktyce. Wydanie 4. 2022. PWN

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	18 [h]
Udział w konsultacjach	5 [h]	X	X
Przygotowanie do wykładów / ćwiczeń / laboratoriów / projektów / seminariów	X	90 [h]	X
Przygotowanie do zaliczenia/egzaminu			
Sumaryczne obciążenie pracą studenta	5 [h] /0,2 ECTS	90 [h] /3,6 ECTS	30 [h] /1,2 ECTS
Punkty ECTS za przedmiot	5 ECTS		

Informacje dodatkowe, uwagi
<p>W przypadku studentów ze szczególnymi potrzebami, w tym: z niepełnosprawnością, przewlekłe 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, przewlekłe 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, przewlekłe chorych.</p>