

SYLABUS ZAJ /GRUPY ZAJ

Dane ogólne:

Jednostka organizacyjna:	Katedra Informatyki				
Kierunek studiów:	Informatyka				
Specjalno /Specjalizacja:	Inżynieria oprogramowania				
Nazwa zaj / grupy zaj :	Kryptografia i bezpieczeństwo aplikacji				
Course / group of courses:	Cryptography and Application Security				
Forma studiów:	stacjonarne				
Nazwa katalogu:	WP-IN-I-20/21Z-IO				
Nazwa bloku zaj :					
Kod zaj /grupy zaj :	105900	Kod Erasmus:			
Punkty ECTS:	3	Rodzaj zaj :		obowiązkowy	
Rok studiów:	3	Semestr:		5	
Rok	Semestr	Forma zaj	Liczba godzin	Forma zaliczenia	ECTS
3	5	LO	15	Zaliczenie z ocen	2
		W	15	Zaliczenie z ocen	1
Razem			30		3
Koordinator:	magister inżynier Tomasz Potempa				
Prowadzący zajęcia:					
Język wykładowy:	semestr: 5 - język polski				

Objaśnienia:

Rodzaj zaj : obowiązkowe, do wyboru.

Forma prowadzenia zaj : W - wykład, - wiczenia audytoryjne, L - lektorat, S – seminarium/ zajęcia seminaryjne, P - wiczenia praktyczne (w tym zajęcia wf), M - wiczenia specjalistyczne (medyczne/ kliniczne), LO – wiczenia laboratoryjne, LI - laboratorium informatyczne, ZTI - zajęcia z technologii informacyjnych, P – wiczenia projektowe, ZT – zajęcia terenowe, T - wiczenia terenowe na obozach programowych, SK - samokształcenie (i inne), PR - praktyka zawodowa

Dane merytoryczne

Wymagania wstępne:			
1. Podstawowa znajomość matematyki dyskretniej. 2. Znajomość algorytmów i struktur danych. 3. Znajomość podstawowych zagadnień statystyki. 4. Znajomość systemów operacyjnych i podstaw użytkowania komputerów. 5. Znajomość języka angielskiego w stopniu umożliwiającym studiowanie literatury fachowej.			
Szczegółowe efekty uczenia się			
Lp.	Student, który zaliczył zajęcia zna i rozumie/potrafi/jest gotowy do:	Kod efektu dla kierunku studiów	Sposób weryfikacji efektu uczenia się
1	Ma podstawową wiedzę oraz zna terminologię związaną z ochroną i bezpieczeństwem danych w aplikacjach komputerowych, aplikacjach i systemach internetowych oraz systemach cyfrowych.	IN1_W03, IN1_W06, IN1_W01	kolokwium
2	Potrafi dostrzec i zminimalizować ryzyka związane z bezpieczeństwem danych w aplikacjach komputerowych, aplikacjach i systemach internetowych oraz systemach cyfrowych.	IN1_U01, IN1_U08, IN1_U05	wykonanie zadania
3	Potrafi zabezpieczyć przesyłane dane w aplikacjach komputerowych, aplikacjach i systemach internetowych oraz systemach cyfrowych.	IN1_U01, IN1_U08, IN1_U05	wykonanie zadania

4	Potrafi wykorzystać istniejące algorytmy kryptograficzne do zabezpieczenia programów komputerowych oraz aplikacji i systemów internetowych.	IN1_U01, IN1_U08, IN1_U05	wykonanie zadania
5	Rozumie potrzebę ochrony oraz zapewnienia poufności danych a także bezpieczeństwo systemów informatycznych oraz stosowania zabezpieczeń informatycznych.	IN1_K05	wykonanie zadania
Stosowane metody osiągnięcia zakładanych efektów uczenia się (metody dydaktyczne)			
metody praktyczne (Wykład problemowy, metoda (analiza) przypadków, pokaz, prezentacja, ćwiczenia laboratoryjne.), metody podające (Podstawowe formy zajęć jest wykład tradycyjny z wykorzystaniem prezentacji i demonstracji przykładów. Pomocnicze formy zajęć jest laboratorium komputerowe.)			
Kryteria oceny i weryfikacji efektów uczenia się			
wiedza: ocena kolokwium (Kolokwium) umiejętności: ocena wykonania zadania (Wykonanie zadania) kompetencje społeczne: ocena wykonania zadania (Wykonanie zadania)			
Warunki zaliczenia			
Zaliczenie ćwiczeń laboratoryjnych oraz zdanie kolokwium. Oceny wystawiane zgodnie z aktualnym regulaminem studiów w PWSZ w Tarnowie.			
Treści programowe (opis skrócony)			
1. Podstawowe pojęcia i mechanizmy szyfrowania danych. Polityki bezpieczeństwa aplikacji. 2. Algorytmy szyfrowania symetrycznego. 3. Algorytmy szyfrowania asymetrycznego. 4. Funkcje skrótu. 5. Podpis cyfrowy. 6. Technologia blockchain. 7. Kryptoanaliza. 8. Bezpieczeństwo aplikacji internetowych.			
Content of the study programme (short version)			
1. Basic concepts and mechanisms of data encryption. Application security policies. 2. Symmetric encryption algorithms. 3. Asymmetric encryption algorithms. 4. Hash functions. 5. Digital signature. 6. Blockchain technology. 7. Cryptanalysis. 8. Security of internet applications.			
Treści programowe			
			Liczba godzin
Semestr: 5			
Forma zajęć : wykład			
1. Podstawowe pojęcia i mechanizmy szyfrowania danych. Polityki bezpieczeństwa danych oraz aplikacji w systemach informatycznych. 2. Algorytmy szyfrowania symetrycznego. Charakterystyka i zastosowanie. Sposoby implementacji programowej z wykorzystaniem języków programowania. Porównanie implementacji programowej i sprzętowej (złożoność, funkcjonalność, szybkość działania, bezpieczeństwo). Algorytmy szyfrowania blokowego (AES, DES) oraz strumieniowego (RC4). Zalety i wady algorytmów symetrycznych. 3. Algorytmy szyfrowania asymetrycznego. Podstawowe założenia w kryptografii asymetrycznej. Pojęcie klucza publicznego i prywatnego. Podstawowe algorytmy (RSA, El-Gamala). Zalety i wady algorytmów asymetrycznych. 4. Funkcje skrótu (MD5, SHA-1, SHA-3). Ogólna charakterystyka oraz zastosowanie (hasła, podpis elektroniczny, kryptowaluty). Zalety i wady funkcji skrótu. Implementacja programowa i sprzętowa wybranych algorytmów funkcji skrótu. 5. Technologia blockchain. Podstawowe pojęcia. Ogólna charakterystyka oraz zastosowanie (inteligentne kontrakty, kryptowaluty). Implementacje technologii blockchain. Mechanizmy proof-of-work i proof-of-stake. 6. Podpis cyfrowy. Ogólna charakterystyka, zastosowanie, podstawowe własności oraz mechanizmy. Podpis			15

tradycyjny a podpis cyfrowy, porównanie pod kątem bezpieczeństwa i wiarygodności. 7. Kryptoanaliza. Wprowadzenie i omówienie podstawowych założeń kryptoanalizy. Bezpieczeństwo danych i sposoby ich ochrony. Mechanizmy analizy aplikacji w kryptoanalizie. 8. Bezpieczeństwo aplikacji internetowych. Analiza ataków (np. SQL-Injection, Cross-site Scripting). Zabezpieczenia systemów internetowych na poziomie bazy, aplikacji, serwera.	15
---	----

Forma zajęć : **wiczenia laboratoryjne**

1. Podstawowe pojęcia i mechanizmy szyfrowania danych. Polityki bezpieczeństwa danych oraz aplikacji w systemach informatycznych. 2. Algorytmy szyfrowania symetrycznego. Charakterystyka i zastosowanie. Sposoby implementacji programowej z wykorzystaniem języków programowania. Porównanie implementacji programowej i sprzętowej (złożoność, funkcjonalność, szybkość działania, bezpieczeństwo). Algorytmy szyfrowania blokowego (AES, DES) oraz strumieniowego (RC4). Zalety i wady algorytmów symetrycznych. 3. Algorytmy szyfrowania asymetrycznego. Podstawowe założenia w kryptografii asymetrycznej. Pojęcie klucza publicznego i prywatnego. Podstawowe algorytmy (RSA, El-Gamala). Zalety i wady algorytmów asymetrycznych. 4. Funkcje skrótu (MD5, SHA-1, SHA-3). Ogólna charakterystyka oraz zastosowanie (hasła, podpis elektroniczny, kryptowaluty). Zalety i wady funkcji skrótu. Implementacja programowa i sprzętowa wybranych algorytmów funkcji skrótu. 5. Technologia blockchain. Podstawowe pojęcia. Ogólna charakterystyka oraz zastosowanie (inteligentne kontrakty, kryptowaluty). Implementacje technologii blockchain. Mechanizmy proof-of-work i proof-of-stake. 6. Podpis cyfrowy. Ogólna charakterystyka, zastosowanie, podstawowe własności oraz mechanizmy. Podpis tradycyjny a podpis cyfrowy, porównanie pod kątem bezpieczeństwa i wiarygodności. 7. Kryptoanaliza. Wprowadzenie i omówienie podstawowych założeń kryptoanalizy. Bezpieczeństwo danych i sposoby ich ochrony. Mechanizmy analizy aplikacji w kryptoanalizie. 8. Bezpieczeństwo aplikacji internetowych. Analiza ataków (np. SQL-Injection, Cross-site Scripting). Zabezpieczenia systemów internetowych na poziomie bazy, aplikacji, serwera.	15
--	----

Literatura

Podstawowa

Aho A. V., Hopcroft J. E., Ullman J. D., Algorytmy i struktury danych., Helion, Warszawa 2003

Karbowski M., Podstawy Kryptografii, Helion, Warszawa 2005

Maxfield C., The Design Warrior's Guide to FPGAs. Devices, Tools and Flows., Elsevier, Amsterdam 2004

Schneier B., Kryptografia dla praktyków. Protokoły, algorytmy i programy źródłowe w języku C, WNT, Warszawa 2002

Stinson D.R. , Kryptografia, WNT, Warszawa 2005

Uzupełniająca

Dane jakościowe

Przyporządkowanie zajęć/grup zajęć do dyscypliny naukowej/artystycznej	informatyka techniczna i telekomunikacja
Sposób określenia liczby punktów ECTS	
Forma nakładu pracy studenta (udział w zajęciach, aktywność, przygotowanie sprawozdania, itp.)	Obciążenia studenta [w godz.]
Udział w zajęciach	30
Konsultacje z prowadzącym	3
Udział w egzaminie	0
Bezporedni kontakt z nauczycielem - inne	12
Przygotowanie do laboratorium, wicze, zajęcia	10

Przygotowanie do kolokwium i egzaminu	10	
Indywidualna praca własna studenta z literatur , wykładami itp.	10	
Inne	0	
Sumaryczne obciążenie prac studenta	75	
Liczba punktów ECTS		
Liczba punktów ECTS	3	
Zajęcia wymagające bezpośredniego udziału nauczyciela akademickiego	L. godzin	ECTS
	45	1,8
Zajęcia o charakterze praktycznym	L. godzin	ECTS
	47	1,9

1 godz = 45 minut; 1 punkt ECTS = 25-30 godzin

W sekcji 'Liczba punktów ECTS' suma punktów ECTS zajęć wymagających bezpośredniego udziału nauczyciela akademickiego i o charakterze praktycznym może się różnić od łącznej liczby punktów ECTS dla zajęć /grup zajęć.