

WROCŁAWSKA WYŻSZA SZKOŁA INFORMATYKI STOSOWANEJ

KARTA OPISU PRZEDMIOTU

Wydział		Informatyki	
Kierunek		Informatyka	
Specjalność		Cyberbezpieczeństwo	
Semestr	IV	Program studiów, dla którego obowiązuje sylabus	2023/2024
Stopień studiów	I		

Nazwa przedmiotu	Podstawy kryptografii			
Kod przedmiotu	PK			
Łączna liczba godzin	18	Tryb	stacjonarny	niestacjonarny
Profil kształcenia	Ogólnoakademicki (A)		Praktyczny (P)	
Forma zajęć	laboratorium			
Język przedmiotu	polski			
Liczba punktów ECTS	2			

Prowadzący zajęcia	
Forma prowadzonych zajęć	Laboratorium
Wymiar zajęć	18 h
Stopień (tytuł) naukowy	
Imię	
Nazwisko	

Wymagania wstępne	Podstawowa wiedza z zakresu informatyki i technologii informacyjnych, umiejętność obsługi systemów operacyjnych Windows i Linux, znajomość podstaw programowania i algorytmiki oraz podstawowych zasad działania sieci komputerowych.
Założenia i cele przedmiotu	Przedmiot ma na celu wprowadzenie studentów w podstawy kryptografii, w tym historię, kluczowe pojęcia oraz zastosowania. Studenci poznają główne algorytmy szyfrowania symetrycznego i asymetrycznego, funkcje skrótu, podpis cyfrowy oraz infrastrukturę klucza publicznego (PKI). Dzięki temu nabędą kompetencje pozwalające na zrozumienie i podstawowe wykorzystanie narzędzi kryptograficznych w zabezpieczaniu komunikacji i danych w systemach informatycznych.
Metody dydaktyczne	<ol style="list-style-type: none"> 1. Prezentacje multimedialne. 2. Pokazy przykładowych rozwiązań problemów. 3. Rozwiązywanie zadań praktycznych.

Efekty uczenia się (odniesienie do charakterystyk poziomów Polskiej Ramy Kwalifikacji)		Odniesienie do efektów dla kierunku	Odniesienie do efektów uczenia się wg Polskiej Ramy Kwalifikacji
WIEDZA – absolwent zna i	W01.Podstawy matematyczne kryptografii, w tym elementy teorii liczb i matematyki dyskretniej	K_W01	P6S_WG P6S_WG_INŻ

WROCŁAWSKA WYŻSZA SZKOŁA INFORMATYKI STOSOWANEJ

rozumie:	<p>niezbędne do analizy algorytmów szyfrujących.</p> <p>W02. Strukturę oraz działanie wybranych algorytmów kryptograficznych.</p> <p>W03. Rolę protokołów kryptograficznych w zapewnianiu poufności i integralności komunikacji w sieciach teleinformatycznych.</p> <p>W04. Metody projektowania systemów informatycznych uwzględniających mechanizmy kryptograficzne (podpis cyfrowy, PKI) jako element całościowej architektury bezpieczeństwa.</p> <p>W05. Istotę zagrożeń bezpieczeństwa w systemach informatycznych oraz znaczenie kryptografii jako jednego z kluczowych środków ochrony danych.</p>	<p>K_W06</p> <p>K_W07</p> <p>K_W16</p> <p>K_W18</p>	
UMIEJĘTNOŚCI – absolwent potrafi:	<p>U01. Pozyskiwać z literatury i dokumentacji technicznej informacje na temat aktualnych standardów kryptograficznych, a następnie krytycznie je ocenić i zastosować.</p> <p>U02. Wykorzystać matematyczne metody analizy w celu oceny właściwości i bezpieczeństwa wybranych algorytmów szyfrujących.</p> <p>U03. Projektować proste systemy informatyczne, uwzględniając w nich odpowiednie mechanizmy kryptograficzne (np. szyfrowanie symetryczne, asymetryczne, podpis cyfrowy).</p> <p>U04. Przygotować i przeprowadzić testy weryfikujące poprawność i bezpieczeństwo wdrożonych funkcji kryptograficznych.</p> <p>U05. Zastosować i skonfigurować rozwiązania kryptograficzne w środowisku sieciowym, zapewniając poufność, integralność i uwierzytelnienie danych.</p>	<p>K_U01</p> <p>K_U02</p> <p>K_U03</p> <p>K_U04</p> <p>K_U06</p> <p>K_U09</p> <p>K_U11</p> <p>K_U18</p>	<p>P6S_UW</p> <p>P6S_UW_INŻ</p> <p>P6S_UO</p> <p>P6S_KK</p> <p>P6S_UK</p>
KOMPETENCJE SPOŁECZNE – absolwent jest gotów do	<p>K01. Pracy w zespole, przyjmując w nim różne role.</p> <p>K02. Krytycznej oceny możliwości urządzeń sieciowych i systemów i dostępnych na rynku IT.</p> <p>K03. Ciągłego samokształcenia się w celu dostosowywania się do dynamicznie zmieniających się technologii.</p>	<p>K_K04</p> <p>K_K05</p> <p>K_K06</p>	<p>P6S_UO</p> <p>P6S_KR</p> <p>P6S_KK</p>

Lp.	Tematyka zajęć	Liczba godzin
Forma zajęć – laboratorium		
1	Wprowadzenie do kryptografii. Historia kryptografii, podstawowe pojęcia i	1

WROCŁAWSKA WYŻSZA SZKOŁA INFORMATYKI STOSOWANEJ

	terminologia.	
2	Kryptografia symetryczna. Algorytmy szyfrowania symetrycznego: DES, AES, tryby pracy szyfrów blokowych.	3
3	Kryptografia asymetryczna. Klucze publiczne i prywatne, algorytmy RSA, Diffie-Hellman, ElGamal.	4
4	Funkcje skrótu i podpis cyfrowy. SHA-2, SHA-3, zastosowanie funkcji skrótu, mechanizmy podpisu cyfrowego.	2
5	Infrastruktura klucza publicznego (PKI). Certyfikaty cyfrowe, zaufane strony trzecie, zarządzanie kluczami	4
6	Protokoły kryptograficzne i ich zastosowania. SSL/TLS, IPsec, praktyczne implementacje. Zaliczenie.	4

Forma i warunki zaliczenia przedmiotu	Wykonanie projektów. Częstkowe prezentacje, zdawanie raportów, obrona projektów.	
Metody weryfikacji efektów uczenia się		Nr efektu uczenia się z sylabusu
	Ocena projektów i częściowych prezentacji.	W01-W05, U01-U05, K01-K03

Literatura podstawowa	<ol style="list-style-type: none"> 1. M. Karbowski, <i>Podstawy kryptografii</i>, Helion, Gliwice 2014. 2. C. Kościelny, M. Kurkowski, M. Srebrny, <i>Kryptografia. Teoretyczne podstawy i praktyczne zastosowania</i>, Wydawnictwo PJWSTK, Warszawa 2009.
Literatura uzupełniająca	<ol style="list-style-type: none"> 1. D. Stinson, <i>Kryptografia. W teorii i w praktyce</i>, WNT, Warszawa 1995. 2. N. Ferguson, B. Schneier, <i>Kryptografia w praktyce</i>, Helion, Gliwice 2004.

Nakład pracy studenta	
	Liczba godzin
Zajęcia dydaktyczne	18
Przygotowanie się do zajęć	9
Studiowanie literatury	9
Udział w konsultacjach	2
Przygotowanie projektu / eseju / prezentacji itp.	22
Przygotowanie się do egzaminu / zaliczenia	-
Inne	-
ŁĄCZNY nakład pracy studenta w godz.	60
Liczba punktów ECTS	2