

Karta przedmiotu

Nazwa i kod przedmiotu	Podstawy kryptografii (P) , PG_00168375						
Kierunek studiów	Informatyka (P)						
Data rozpoczęcia studiów	październik 2024 r.		Rok akademicki realizacji przedmiotu		2025/2026		
Poziom kształcenia	I stopnia - licencjackie		Grupa zajęć		Grupa zajęć obowiązkowych z zakresu kierunku studiów Grupa zajęć fakultatywnych		
Forma studiów	stacjonarne		Sposób realizacji		na uczelni		
Rok studiów	2		Język wykładowy		polski		
Semestr studiów	4		Liczba punktów ECTS		2.0		
Profil kształcenia	praktyczny		Forma zaliczenia		zaliczenie		
Jednostka prowadząca							
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot		dr Andrzej Borzyszkowski				
	Prowadzący zajęcia z przedmiotu						
Formy zajęć	Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
	Liczba godzin zajęć	15.0	0.0	15.0	0.0	0.0	30
	W tym liczba godzin zajęć na odległość: 0.0						
Aktywność studenta i liczba godzin pracy	Aktywność studenta	Udział w zajęciach dydaktycznych, objętych planem studiów		Udział w konsultacjach		Praca własna studenta	RAZEM
	Liczba godzin pracy studenta	30		0.0		0.0	30
Cel przedmiotu	Przekazanie wiedzy na temat współczesnej kryptografii, zapoznanie się w praktyce z kilkoma najważniejszymi narzędziami używanymi w w/w.						
	Zapoznanie z terminologią w języku angielskim.						

Efekty uczenia się przedmiotu	Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
	[INFL3_W01] ma wiedzę w zakresie matematyki obejmującą podstawy, algebry, matematyki dyskretnej (elementy logiki i teorii mnogości, kombinatoryki i teorii grafów), metod probabilistycznych	zdaje sobie sprawę z możliwych zagrożeń w kontekście używania komputerów i ma wiedzę na temat stosowanych rozwiązań, rozumie jak działa kryptografia asymetryczna, na czym polega podpis elektroniczny, jakie są metody badania integralności dokumentów, rozumie, jakie są możliwości i jakie ograniczenia współczesnej kryptografii. zna podstawowe algorytmy i protokoły kryptograficzne zna możliwe ataki na bezpieczeństwo systemów przetwarzania informacji	[SW4] test/exam - oral or written [SW2] presentation/project/paper/report
	[INFL3_W09] ma podstawową wiedzę dotyczącą prawnych i społecznych aspektów informatyki, w tym odpowiedzialności zawodowej i etycznej, własności intelektualnej, prywatności, ryzyka i odpowiedzialności związanej z systemami informatycznymi	potrafi ocenić prawną dopuszczalność różnych czynności związanych z łamaniem szyfrów	[SW4] test/exam - oral or written [SW2] presentation/project/paper/report
	[INFL3_U06] potrafi dbać o bezpieczeństwo danych, w tym o ich bezpieczne przesyłanie; posługuje się narzędziami szyfrowania danych	potrafi utworzyć bezpieczne hasło, utworzyć certyfikat X.509 lub PGP, obliczyć funkcję skrótu, napisać programy do szyfrowania i kryptoanalizy w różnych systemach kryptograficznych	[SU2] presentation/project/paper/report [SU4] test/exam - oral or written
Treści przedmiotu	Główne pojęcia, założenia kryptografii, kryptografia symetryczna i asymetryczna, klasyczne szyfry. Pojęcie doskonale bezpiecznego szyfru, szyfr jednorazowy, liczby losowe i pseudolosowe, szyfr strumieniowy. Funkcje i permutacje pseudolosowe. Szyfry blokowe i ich tryby. Integralność danych: MAC i funkcje skrótu, własności funkcji skrótu, atak urodzinowy. "Szyfruj, potem uwierzytelniaj". Kryptografia klucza prywatnego a kryptografia klucza publicznego. Idea kryptografii asymetrycznej, atak ze środka, uwierzytelnianie i podpis, szyfr hybrydowy. Implementacja kryptografii klucza publicznego: Teoria grup, twierdzenia Fermata, Eulera. Problemy trudne: problem rozkładu na czynniki, problem RSA, problem logarytmu dyskretnego, problem Diffie'go-Hellmana. RSA, system ElGamala. Schematy podpisu cyfrowego, w kryptografii symetrycznej i asymetrycznej, RSA, schemat ElGamala i DSS, użycie skrótu w podpisie. Infrastruktura klucza publicznego, X.509, PGP. Centra certyfikacji w Polsce. PGP w praktycznym działaniu. Elementy steganografii. Zapoznanie z terminologią angielską.		
Wymagania wstępne i dodatkowe			
Sposoby i kryteria oceniania osiągniętych efektów uczenia się	Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
	test końcowy	51.0%	40.0%
	laboratorium	51.0%	60.0%

Zalecana lista lektur	Podstawowa lista lektur	Andrzej Borzyszkowski, materiały do przedmiotu dostępne na stronie www.
	Uzupełniająca lista lektur	1. J. Katz, Y. Lindell, Introduction to modern cryptography, Chapman&Hall/CRC, 2008. 2. W. Trappe, L. Washington, Introduction to Cryptography with Coding Theory, Prentice Hall, 2005. 3. I. Cox, M. Miller, J. Bloom, J. Fridrich, T. Kalker, Digital Watermarking and Steganography, Morgan Kaufmann, 2008
	Adresy eZasobów	
Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania	Który/które z poniższych trybów szyfrów blokowych umożliwiają atakującemu niezauważoną manipulację kolejnością zaszyfrowanych bloków? (a) ECB (b) CTR (c) CBC (d) OFB Współczesna kryptografia klucza asymetrycznego jest przełomowym odkryciem ponieważ: (a) zapewnia radykalnie lepszą wydajność szyfrowania (b) umożliwia komunikację pomiędzy uczestnikami wcześniej nie kontaktującymi się (c) umożliwia implementację idei niezaprzeczalności autorstwa dokumentów (d) gwarantuje uwierzytelnianie uczestników	
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy	

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.