

Karta przedmiotu

Nazwa i kod przedmiotu	Bezpieczeństwo systemów informatycznych, PG_00203647						
Kierunek studiów	Informatyka (O)						
Data rozpoczęcia studiów	październik 2026 r.		Rok akademicki realizacji przedmiotu		2027/2028		
Poziom kształcenia	II stopnia		Grupa zajęć		Grupa zajęć obowiązkowych z zakresu kierunku studiów Grupa zajęć powiązanych z prowadzonymi badaniami naukowymi w dziedzinie nauki związanej z kierunkiem - profil ogólnoakademicki		
Forma studiów	stacjonarne		Sposób realizacji		na uczelni		
Rok studiów	2		Język wykładowy		polski		
Semestr studiów	3		Liczba punktów ECTS		5.0		
Profil kształcenia	ogólnoakademicki		Forma zaliczenia		zaliczenie		
Jednostka prowadząca	Rektor -> Wydział Matematyki, Fizyki i Informatyki -> Instytut Informatyki						
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	30.0	0.0	30.0	0.0	0.0	60
	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	60		0.0		65.0	125
Cel przedmiotu	Przekazanie wiedzy na temat współczesnej kryptografii, zapoznanie się w praktyce z kilkoma najważniejszymi narzędziami używanymi w w/w.						
Efekty uczenia się przedmiotu	Efekt kierunkowy		Efekt z przedmiotu			Sposób weryfikacji i oceny efektu	
	[INFMU2_W06] zna i rozumie w pogłębionym stopniu koncepcje funkcjonowania współczesnych systemów informatycznych, rozumie zagrożenia bezpieczeństwa występujące w systemach sieciowych i rozproszonych, zna nowoczesne modele przetwarzania i przechowywania danych		rozumie jak działa kryptografia asymetryczna, na czym polega podpis elektroniczny, jakie są metody badania integralności dokumentów, zna podstawowe algorytmy i protokoły kryptograficzne zna możliwe ataki na bezpieczeństwo systemów przetwarzania informacji			[SW4] test/egzamin - ustny lub pisemny [SW2] prezentacja/projekt/referat/ raport	
	[INFMU2_U11] potrafi zapewniać dostępność, niezawodność i bezpieczeństwo usług informatycznych, projektować i stosować podstawowe mechanizmy zabezpieczeń		potrafi utworzyć bezpieczne hasło, utworzyć certyfikat X.509 lub PGP, obliczyć funkcję skrótu, napisać programy do szyfrowania i kryptoanalizy w różnych systemach kryptograficznych			[SU2] prezentacja/projekt/referat/ raport [SU4] test/egzamin - ustny lub pisemny	

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.		
Wymagania wstępne i dodatkowe			
Sposoby i kryteria oceniania osiągniętych efektów uczenia się	Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
	zaliczenie z wykładu	51.0%	40.0%
	laboratorium - projekty	51.0%	60.0%
Zalecana lista lektur	Podstawowa lista lektur	materiały wykładowe na stronie WWW oraz portalu edukacyjnym	
	Uzupełniająca lista lektur	J. Katz, Y. Lindell, Introduction to modern cryptography, Chapman&Hall/CRC, 2008. W. Trappe, L. Washington, Introduction to Cryptography with Coding Theory, Prentice Hall , 2005. 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	- Podaj definicję szyfru doskonale bezpiecznego. Czy taki szyfr istnieje? Dlaczego stosujemy szyfry, które nie są doskonale bezpieczne? - Podaj przykłady szyfrów niedeterministycznych. Czy niedeterminizm jest wadą czy zaletą szyfru? Uzasadnij. - Jakie nowe możliwości niesie kryptografia klucza asymetrycznego? Jakie są jej ograniczenia? - Jakie własności powinna mieć funkcja skrótu w kryptografii? Wyjaśnij te własności w zastosowaniach funkcji skrótu.		
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy		

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.