



Karta przedmiotu

Nazwa i kod przedmiotu	Bezpieczeństwo systemów informacyjnych, PG_00048305						
Kierunek studiów	Elektronika i telekomunikacja						
Data rozpoczęcia studiów	luty 2024 r.	Rok akademicki realizacji przedmiotu			2024/2025		
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			3.0		
Profil kształcenia	ogólnoakademicki	Forma zaliczenia			zaliczenie		
Jednostka prowadząca	Wydział Elektroniki, Telekomunikacji i Informatyki -> Katedra Sieci Teleinformacyjnych						
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot	dr inż. Bartosz Czaplewski					
	Prowadzący zajęcia z przedmiotu	dr inż. Bartosz Czaplewski					
Formy zajęć i metody nauczania	Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
	Liczba godzin zajęć	30.0	0.0	15.0	0.0	0.0	45
	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	45		3.0		27.0	75
Cel przedmiotu	Poznanie zagrożeń bezpieczeństwa informacji i metod przeciwdziałania tym zagrożeniom.						

Efekty uczenia się przedmiotu	Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
	[K7_W06] zna i rozumie w pogłębionym stopniu podstawowe procesy zachodzące w cyklu życia urządzeń, obiektów i systemów technicznych	Student analizuje procesy szyfrowania i deszyfracji oraz ocenia odporność systemów kryptograficznych na ataki.	[SW1] Ocena wiedzy faktograficznej
	[K7_W03] zna i rozumie w pogłębionym stopniu budowę i zasady działania komponentów i systemów związanych z kierunkiem studiów, w tym teorie, metody i złożone zależności między nimi oraz wybrane zagadnienia szczegółowe – właściwe dla programu kształcenia	Student identyfikuje, klasyfikuje i rozpoznaje zagrożenia bezpieczeństwa informacji podczas transmisji oraz podstawowe systemy kryptograficzne. Student identyfikuje i klasyfikuje usługi oraz mechanizmy bezpieczeństwa.	[SW1] Ocena wiedzy faktograficznej
	[K7_U06] potrafi analizować działanie elementów, układów i systemów związanych z kierunkiem studiów oraz mierzyć ich parametry i badać charakterystyki techniczne, interpretować uzyskane wyniki i wyciągać wnioski	Student jest w stanie uruchomić, zmierzyć i analizować najważniejsze algorytmy szyfrowania symetrycznego oraz asymetrycznego.	[SU4] Ocena umiejętności korzystania z metod i narzędzi [SU2] Ocena umiejętności analizy informacji
	[K7_U07] potrafi wykorzystać zaawansowane metody wspomagania procesów i funkcji, specyficzne dla kierunków studiów	Student rozumie, identyfikuje oraz klasyfikuje metody kryptografii symetrycznej, kryptografii asymetrycznej, steganografii, cyfrowego odcisku palca.	[SU4] Ocena umiejętności korzystania z metod i narzędzi [SU2] Ocena umiejętności analizy informacji
[K7_W08] zna i rozumie w pogłębionym stopniu fundamentalne dylematy współczesnej cywilizacji, główne trendy rozwojowe dyscyplin naukowych istotnych dla kierunku kształcenia	Student rozumie i identyfikuje wyzwania związane z dystrybucją kluczy, utworzeniem kanału bezpiecznego, odpornością kryptografii asymetrycznej na działania komputerów kwantowych. Student zna i rozumie jak krytyczne dla współczesnej cywilizacji jest zachowanie właściwego poziomu bezpieczeństwa informacji.	[SW1] Ocena wiedzy faktograficznej	
Treści przedmiotu	1. Bezpieczeństwo systemu informacyjnego 2. Podstawowe aspekty bezpieczeństwa informacji 3. Model bezpieczeństwa sieciowego 4. Podstawowe aspekty systemów kryptograficznych 5. Metody kryptoanalizy 6. Szyfry klasyczne 7. Wprowadzenie do szyfrów blokowych 8. Data Encryption Standard (DES) 9. Zasady projektowania szyfrów blokowych 10. Tryby pracy szyfrów blokowych 11. Szyfrowanie podwójne i potrójne (3DES) 12. International Data Encryption Algorithm (IDEA) 13. Advanced Encryption Standard (AES) 14. Szyfrowanie w łączy i szyfrowanie end-to-end 15. Metody dystrybucji kluczy 16. Generowanie liczb pseudolosowych 17. Szyfr potokowy RC4 18. Asymetryczne systemy kryptograficzne 19. System RSA 20. Dystrybucja kluczy publicznych 21. Algorytm Diffiego-Hellmana 22. Algorytm ElGamal 23. Kryptografia krzywych eliptycznych 24. Przyszłość kryptografii asymetrycznej 25. Kryptografia asymetryczna odporna na ataki komputerów kwantowych 26. Uwierzytelnianie wiadomości 27. Jednokierunkowe funkcje skrótów 28. Tęczowe tablice 29. Właściwości podpisu cyfrowego 30. Digital Signature Algorithm (DSA) 31. Podstawy steganografii 32. Cyfrowy odcisk palca 33. Reversible Data Hiding		
Wymagania wstępne i dodatkowe			
Sposoby i kryteria oceniania osiągniętych efektów uczenia się	Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa ocena końcowej
	sprawozdania pomiarowe	50.0%	40.0%
	kolokwium zaliczeniowe	50.0%	60.0%

Zalecana lista lektur	Podstawowa lista lektur	B. Schneier, Kryptografia dla praktyków, WN-T, Warszawa 2004 J. Fridrich, Steganography in Digital Media: Principles, Algorithms, and Applications, Cambridge University Press, 2010 N. Ferguson, B. Schneier, Kryptografia w praktyce, Helion, 2004 W. Stallings, Cryptography and Network Security, Principles and Practice, Fourth Edition, Prentice Hall, 2005 M. Stamp, Information Security: Principles and Practice, J. Wiley, 2011
	Uzupełniająca lista lektur	B. Czaplewski, Nowe metody łącznego fingerprintingu i deszyfracji do zabezpieczania obrazów kolorowych, rozprawa doktorska, WETI PG, 2015Y.-Q. Shi, X. Li, X. Zhang, H.-T. Wu, B. Ma, Reversible Data Hiding: Advances in the Past Two Decades, IEEE Access, 2016
	Adresy eZasobów	Adresy na platformie eNauczanie:
Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania	brak	
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy	