

WROCŁAWSKA WYŻSZA SZKOŁA INFORMATYKI STOSOWANEJ

KARTA OPISU PRZEDMIOTU

Wydział	Informatyki		
Kierunek	Informatyka		
Specjalność	Grafika komputerowa Programowanie Sieci i systemy teleinformatyczne		
Semestr	II	Program studiów,	2019/2020
Stopień studiów	II	dla którego obowiązuje sylabus	

Nazwa przedmiotu	Kryptografia			
Kod przedmiotu	KRYPT			
Łączna liczba godzin	18	Tryb	stacjonarny	niestacjonarny
Profil kształcenia	Ogólnoakademicki (A)		Praktyczny (P)	
Forma zajęć	wykład			
Język przedmiotu	polski			
Liczba punktów ECTS	3			

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

Wymagania wstępne	Znajomość podstaw matematyki dyskretniej, metod probabilistycznych, statystyki, programowania, algorytmów i struktur danych.
Założenia i cele przedmiotu	Przedmiot ma na celu zapoznanie studentów z podstawowymi zasadami, metodami i zastosowaniami kryptografii w ochronie informacji. Studenci poznają kluczowe pojęcia oraz różnorodne techniki szyfrowania i deszyfrowania danych oraz są wprowadzani w zagadnienia związane z podpisami cyfrowymi, steganografią oraz podstawami kryptoanalizy, przygotowujące ich do praktycznego zastosowania tych technik w celu zabezpieczania danych i komunikacji. Kurs umożliwi zrozumienie, jak kryptografia zapewnia poufność, integralność i autentyczność informacji w systemach teleinformatycznych.
Metody dydaktyczne	1. Wykład – w formie tradycyjnej lub prezentacji multimedialnej – z elementami dyskusji

Efekty uczenia się (odniesienie do charakterystyk poziomów Polskiej Ramy Kwalifikacji)	Odniesienie do efektów dla kierunku	Odniesienie do efektów uczenia się wg Polskiej Ramy Kwalifikacji

WROCŁAWSKA WYŻSZA SZKOŁA INFORMATYKI STOSOWANEJ

WIEDZA – absolwent zna i rozumie:	W01. Sposoby ochrony własności przed niepowołanym dostępem. W02. Normy z zakresu bezpieczeństwa komputerowego.	K_W01 K_W07 K_W09	P7S_WG
UMIEJĘTNOŚCI – absolwent potrafi:	U01. Zastosować praktyczne metody realizacji algorytmów kryptograficznych do ochrony baz danych, plików dyskowych i poczty elektronicznej. U02. Ocenic przydatność programów oferowanych przez dostawców oprogramowania związanego z kryptografią i podpisem cyfrowym.	K_U01 K_U03 K_U06 K_U17	P7S_UW P7S_KK P7S_UK
KOMPETENCJE SPOŁECZNE – absolwent jest gotów do	K01. Ciągłego samokształcenia się.	K_K03	P7S_UU

Treści programowe		
Lp.	Tematyka zajęć	Liczba godzin
Forma zajęć – wykład		
1	Podstawowe pojęcia: szyfr podstawieniowy, przestawieniowy, blokowy, strumieniowy, symetryczny (z kluczem tajnym), asymetryczny (z kluczem publicznym), szyfry historyczne.	2
2	Szyfry symetryczne: przykłady symetrycznych szyfrów blokowych i strumieniowych.	2
3	Szyfry asymetryczne: szyfr RSA, szyfr ElGamala	2
4	Infrastruktura klucza publicznego (PKI), podpisy cyfrowe.	2
5	Szyfrowanie hybrydowe: RSA – AES.	2
6	Programy do ochrony informacji.	2
7	Ochrona plików dyskowych i poczty elektronicznej przed niepowołanym dostępem, protokół secure e-mail.	2
8	Steganografia i kryptosteganografia.	2
9	Elementy kryptoanalizy.	2

Forma i warunki zaliczenia przedmiotu	Kolokwium z wykładu.	
Metody weryfikacji efektów uczenia się		Nr efektu uczenia się z sylabusu
	Kolokwium pisemne	W01-W02, U01-U02, K01

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,
------------------------------	---

WROCŁAWSKA WYŻSZA SZKOŁA INFORMATYKI STOSOWANEJ

	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	19
Studiowanie literatury	17
Udział w konsultacjach	2
Przygotowanie projektu / eseju / prezentacji itp.	-
Przygotowanie się do egzaminu / zaliczenia	24
Inne	-
ŁĄCZNY nakład pracy studenta w godz.	80
Liczba punktów ECTS	3