



IV. Opis programu studiów

3. KARTA PRZEDMIOTU

Kod przedmiotu	M#1-S1-IP-105a
Nazwa przedmiotu	Historia i podstawy kryptografii (HS I)
Nazwa przedmiotu w języku angielskim	History and fundamentals of cryptography (HS I)
Obowiązuje od roku akademickiego	2020/2021

USYTUOWANIE MODUŁU W SYSTEMIE STUDIÓW

Kierunek studiów	INFORMATYKA PRZEMYSŁOWA
Poziom kształcenia	I stopień
Profil studiów	ogólnoakademicki
Forma i tryb prowadzenia studiów	studia stacjonarne
Zakres	wszystkie
Jednostka prowadząca przedmiot	Katedra Podstaw Konstrukcji Maszyn
Koordinator przedmiotu	dr hab. inż. Jarosław Gałkiewicz, prof. PŚk
Zatwierdził	

OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU

Przynależność do grupy/bloku przedmiotów	przedmiot podstawowy
Status przedmiotu	wybieralny
Język prowadzenia zajęć	polski
Usytuowanie modułu w planie studiów - semestr	semestr 1
Wymagania wstępne	brak
Egzamin (TAK/NIE)	NIE
Liczba punktów ECTS	2

Forma prowadzenia zajęć	wykład	ćwiczenia	laboratorium	projekt	seminarium
Liczba godzin w semestrze	30				

EFEKTY UCZENIA SIĘ

Kategoria	Symbol efektu	Efekty kształcenia	Odniesienie do efektów kierunkowych
Wiedza	W01	Ma wiedzę w zakresie matematyki, obejmującą algebrę, analizę, elementy matematyki dyskretnej i stosowanej, elementy rachunku prawdopodobieństwa i statystyki oraz elementy logiki matematycznej, w tym metody matematyczne i metody numeryczne, niezbędne do rozwiązywania zagadnień inżynierskich.	IP1_W01
	W02	Ma podstawową wiedzę niezbędną do rozumienia społecznych, ekonomicznych, prawnych i innych pozatechnicznych uwarunkowań działalności inżynierskiej, zna pojęcia i zasady z zakresu ochrony własności intelektualnej i prawa patentowego, zna podstawowe zasady ergonomii, bezpieczeństwa i higieny pracy związane z pracą w środowisku przemysłowym.	IP1_W22
Umiejętności	U01	Potrafi posługiwać się narzędziami informacyjno-komunikacyjnymi wykorzystującymi przetwarzanie tekstów, grafikę prezentacyjną, arkusze kalkulacyjne, bazy danych, właściwymi do realizacji zadań typowych dla działalności inżynierskiej w zakresie informatyki przemysłowej, w tym potrafi przygotować i przedstawić	IP1_U06
	U02	Potrafi zastosować wiedzę z zakresu rachunku prawdopodobieństwa i statystyki matematycznej do analizy danych doświadczalnych, potrafi przygotowywać dane statystyczne i korzystać z podstawowych metod wnioskowania statystycznego.	IP1_U09
Kompetencje społeczne	K01	Ma świadomość znaczenia i rozumie pozatechniczne aspekty i skutki działalności inżyniera informatyka przemysłowego, w aspekcie oddziaływania na środowisko i odpowiedzialności za podejmowane decyzje.	IP1_K02
	K02	Ma świadomość odpowiedzialności za pracę własną oraz gotowość podporządkowania się zasadom pracy w zespole i ponoszenia odpowiedzialności za wspólnie realizowane zadania.	IP1_K04

TREŚCI PROGRAMOWE

Forma zajęć*	Treści programowe
wykład	1. Wstęp do tematyki szyfrowania i ukrywania danych
	2. Steganografia w starożytności i współczesna
	3. Przykłady zastosowania steganografii do kontroli poprawności danych
	4. Metody kryptograficzne stosowane w starożytności
	5. Proste szyfry podstawieniowe
	6. Wkład świata arabskiego do łamania szyfru Cezara
	7. Rozwój kryptografii w średniowiecznej Europie
	8. Szyfry popularne w czasie pierwszej wojny światowej
	9. Metody szyfrowania stosowane podczas II wojny światowej
	10. Historia Enigmy
	11. Współczesne szyfrowanie

METODY WERYFIKACJI EFEKTÓW UCZENIA SIĘ

Symbol efektu	Metody sprawdzania efektów kształcenia (zaznaczyć X)					
	Egzamin ustny	Egzamin pisemny	Kolokwium	Projekt	Sprawozdanie	Inne

W01				x		x
W02				x		x
U01				x		
U02				x		
K01				x		
K02				x		

FORMA I WARUNKI ZALICZENIA

Forma zajęć*	Forma zaliczenia	Warunki zaliczenia
wykład	zaliczenie z oceną	Obecność na wykładzie oraz przygotowanie prezentacji (lub opracowania) na zadany temat lub ponad 50% punktów z testu lub oddanie projektów

NAKŁAD PRACY STUDENTA

Bilans punktów ECTS							
Lp.	Rodzaj aktywności	Obciążenie studenta					Jednostka
		W	C	L	P	S	
1.	Udział w zajęciach zgodnie z planem studiów	30					h
2.	Inne (konsultacje, egzamin)	2					h
3.	Razem przy bezpośrednim udziale nauczyciela akademickiego	32					h
4.	Liczba punktów ECTS, którą student uzyskuje przy bezpośrednim udziale nauczyciela akademickiego	1,3					ECTS
5.	Liczba godzin samodzielnej pracy studenta	18					h
6.	Liczba punktów ECTS, którą student uzyskuje w ramach samodzielnej pracy	0,7					ECTS
7.	Nakład pracy związany z zajęciami o charakterze praktycznym	0					h
8.	Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym	0,0					ECTS
9.	Sumaryczne obciążenie pracą studenta	50					h
10.	Punkty ECTS za moduł <i>1 punkt ECTS=25 godzin obciążenia studenta</i>	2					ECTS

LITERATURA

1. Łamacze kodów. Historia kryptologii, D. Kahn, wydawnictwo: Zysk i S-ka, 2019
2. Księga szyfrów, S. Singh, Albatros, 2001
3. Tajemne przekazy. Szyfry, enigma i karty chipowe, R. Kippenhahn, Prószyński i S-ka, 2000