WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI/KATEDRA PODSTAW INFORMATYKI

KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim : **Wprowadzenie do Kryptografii**
Nazwa przedmiotu w języku angielskim : **Introduction to Cryptography**
Kierunek studiów : **Informatyka algorytmiczna**
Specjalność (jeśli dotyczy) : **—**
Poziom i forma studiów : **I stopień, stacjonarna**
Rodzaj przedmiotu : **wybieralny**
Język wykładowy : **polski**
Cykl kształcenia od : **2024/2025**
Kod przedmiotu : **W04INA-SI0845G**
Grupa zajęć : **TAK**

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30	30			
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	50	75			
Forma zaliczenia	zaliczenie na ocenę				
Dla grupy kursów zaznaczyć kurs końcowy	X				
Liczba punktów ECTS	2	3			
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)		3			
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	2,72				

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

Podstawy programowania. Techniki kodowania. Elementarne prawdopodobieństwo i algebra. Arytmetyka modularna.

CELE PRZEDMIOTU

C1 Słuchacze poznają podstawy współczesnej kryptografii.

C2 Opanowanie podstawowych technik i narzędzi wykorzystywanych w kryptografii.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy studenta:

W1 Zna metody zapewniające poufność komunikacji.

W2 Zna metody zapewniające integralność komunikacji.

Z zakresu umiejętności studenta:

U1 Potrafi wykorzystywać podstawowe narzędzia kryptograficzne.

U2 Potrafi korzystać z bezpiecznych protokołów komunikacyjnych.

Z zakresu kompetencji społecznych studenta:

K1 Rozumie konieczność stosowania technik kryptograficznych.

TREŚCI PROGRAMOWE

Forma zajęć - wykład		
Wy1	Wprowadzenie.	2h
Wy2	Uwierzytelnienie i autoryzacja.	2h
Wy3	Tajność, prywatność.	2h
Wy4	Zaprzeczalność i niezaprzeczalność.	1h
Wy5	Spójność.	1h
Wy6	Kryptosystemy symetryczne i asymetryczne.	2h
Wy7	Infrastruktura klucza publicznego.	2h
Wy8	Funkcje pseudolosowe.	2h
Wy9	Jednokierunkowe funkcje skrótu.	2h
Wy10	Schematy szyfrowania.	3h
Wy11	Schematy podpisywania.	3h
Wy12	Schematy ustalania klucza.	2h
Wy13	Schematy zapewniające anonimowość.	2h
Wy14	Schematy przetwarzania w chmurach obliczeniowych.	2h
Wy15	Ataki na kryptosystemy.	2h
	Suma godzin	30h

Forma zajęć - ćwiczenia		
Ćw1	Rozwiązywanie problemów kryptograficznych.	30h
	Suma godzin	30h

STOSOWANE NARZĘDZIA DYDAKTYCZNE

1. Wykład tradycyjny
2. Wykład multimedialny
3. Rozwiązywanie zadań i problemów
4. Rozwiązywanie zadań programistycznych
5. Konsultacje
6. Praca własna studentów

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F - formatująca (w trakcie semestru), P - podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	W1-W2, K1-K1	Ocena aktywności i dyskusja ze słuchaczami.
F2	U1-U2, K1-K1	Średnia ocen z list zadań.
P=20%*F1+80%*F2		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

1. Kryptografia w teorii i praktyce - Douglas R. Stinson.
2. Lecture Notes on Introduction to Cryptography, CMU, Vipul Goyal, dostępne online.
3. Handbook of Applied Cryptography, Paul C. van Oorschot , Scott A. Vanstone A. J. Menezes, dostępne online

NAUCZYCIEL AKADEMICKI ODPOWIEDZIALNY ZA PRZEDMIOT

dr hab. inż. Łukasz Krzywiecki

MACIERZ POWIĄZANIA EFEKTÓW UCZENIA SIĘ DLA PRZEDMIOTU
Wprowadzenie do Kryptografii
Z EFEKTAMI UCZENIA SIĘ NA KIERUNKU INFORMATYKA ALGORYTMICZNA

Przedmiotowy efekt uczenia się	Odniesienie przedmiotowego efektu do efektów uczenia się zdefiniowanych dla kierunku studiów	Cele przedmiotu**	Treści programowe**	Numer narzędzia dydaktycznego**
W1	K1_W11	C1	Wy1-Wy15	1 2 5 6
W2	K1_W11	C1	Wy1-Wy15	1 2 5 6
U1	K1_U20	C2	Ćw1-Ćw1	3 4 5 6
U2	K1_U20	C2	Ćw1-Ćw1	3 4 5 6
K1	K1_K01 K1_K02	C1 C2	Wy1-Wy15 Ćw1-Ćw1	1 2 3 4 5 6