Załącznik nr 1.5 do Zarządzenia Rektora UR nr 12/2019

SYLABUS

DOTYCZY CYKLU KSZTAŁCENIA 2022/2023 – 2025/2026
(skrajne daty)
Rok akademicki 2025/2026

1. PODSTAWOWE INFORMACJE O PRZEDMIOCIE

Nazwa przedmiotu	***Podstawy kryptografii***
Kod przedmiotu*	
Nazwa jednostki prowadzącej kierunek	*Kolegium Nauk Przyrodniczych*
Nazwa jednostki realizującej przedmiot	*Kolegium Nauk Przyrodniczych*
Kierunek studiów	*Informatyka i ekonometria*
Poziom studiów	*Studia inżynierskie I-go stopnia*
Profil	*praktyczny*
Forma studiów	*stacjonarne*
Rok i semestr/y studiów	*rok IV semestr 7*
Rodzaj przedmiotu	*przedmiot specjalnościowy / przedmiot obieralny 2*
Język wykładowy	*język polski*
Koordynator	*dr Anna Król*
Imię i nazwisko osoby prowadzącej / osób prowadzących	

***** *-opcjonalnie, zgodnie z ustaleniami w Jednostce*

1.1.Formy zajęć dydaktycznych, wymiar godzin i punktów ECTS

Semestr (nr)	Wykł.	Ćw.	Konw.	Lab.	Sem.	ZP	Prakt.	Inne (jakie?)	**Liczba pkt. ECTS**
7	10			20					3

1.2. Sposób realizacji zajęć

☒ zajęcia w formie tradycyjnej
☐ zajęcia realizowane z wykorzystaniem metod i technik kształcenia na odległość

1.3 Forma zaliczenia przedmiotu (z toku) (egzamin, zaliczenie z oceną, zaliczenie bez oceny)

ZALICZENIE Z OCENĄ

2.WYMAGANIA WSTĘPNE

Wiedza z zakresu przedmiotów: analiza matematyczna, algebra liniowa, algorytmy i struktury danych, podstawy programowania

3. CELE, EFEKTY UCZENIA SIĘ , TREŚCI PROGRAMOWE I STOSOWANE METODY DYDAKTYCZNE

3.1 Cele przedmiotu

C1	ZDOBYCIE WIEDZY Z ZAKRESU PODSTAWOWYCH POJĘĆ, ALGORYTMÓW I NARZĘDZI KRYPTOGRAFICZNYCH
C2	ZDOBYCIE UMIEJĘTNOŚCI Z ZAKRESU STOSOWANIA NARZĘDZI KRYPTOGRAFICZNYCH

3.2 Efekty uczenia się dla przedmiotu

EK (efekt uczenia się)	Treść efektu uczenia się zdefiniowanego dla przedmiotu	Odniesienie do efektów kierunkowych [1]
EK_01	Student zna terminy kryptografia i kryptoanaliza. Rozumie różnicę pomiędzy kryptografią symetryczną a asymetryczną oraz zna algorytmy z każdej grupy. Student zna kilka funkcji skrótu wraz ze sposobem ich działania oraz dziedziny ich zastosowań.	K_W01 K_W02
EK_02	Student potrafi zastosować poznane algorytmy kryptograficzne do zaszyfrowania bądź rozszyfrowania podanego komunikatu tekstowego. Umie odpowiednio stosować wybrane narzędzia kryptograficzne w oparciu o aktualną wiedzę.	K_U02

3.3 Treści programowe

A. Problematyka wykładu

Treści merytoryczne:
Historia kryptografii
Matematyczne podstawy kryptografii
Kryptografia symetryczna i szyfry symetryczne
Kryptografia asymetryczna i szyfry asymetryczne
Kryptoanaliza
Zarządzanie kluczami (PKI)
Funkcje skrótu i podpis cyfrowy
Narzędzia kryptograficzne
Prawne aspekty wykorzystania kryptografii

B. Problematyka ćwiczeń laboratoryjnych

Treści merytoryczne:
Szyfry symetryczne
Szyfry asymetryczne
Kryptoanaliza

[1] W przypadku ścieżki kształcenia prowadzącej do uzyskania kwalifikacji nauczycielskich uwzględnić również efekty uczenia się ze standardów kształcenia przygotowującego do wykonywania zawodu nauczyciela.

3.4 Metody dydaktyczne

Wykład: wykład z prezentacją multimedialną
Laboratorium: metoda projektów, rozwiązywanie zadań, praca indywidualna, praca w grupach.

4. METODY I KRYTERIA OCENY

4.1 Sposoby weryfikacji efektów uczenia się

Symbol efektu	Metody oceny efektów uczenia się (np.: kolokwium, egzamin ustny, egzamin pisemny, projekt, sprawozdanie, obserwacja w trakcie zajęć)	Forma zajęć dydaktycznych (w, ćw, ...)
EK_01	Sprawdzian ustny	Wykład
EK_02	Kolokwium, projekt, obserwacja w trakcie zajęć	Ćwiczenia

4.2 Warunki zaliczenia przedmiotu (kryteria oceniania)

Zaliczenie laboratorium następuje na podstawie zaliczenia efektu EK_02 na poziomie co najmniej dostatecznym.
Ocena obejmuje kolokwium, projekt oraz aktywne uczestnictwo na zajęciach.

Zaliczenie wykładu następuje na podstawie zaliczenia laboratorium oraz ustnego sprawdzianu osiągnięcia efektów uczenia się EK_01.

Na ocenę dostateczną należy zaliczyć wszystkie weryfikowane efekty na poziomie co najmniej 50% maksymalnej liczby punktów możliwych do zdobycia.
Na ocenę dobrą należy zaliczyć wszystkie weryfikowane efekty przy średnim poziomie zaliczenia - co najmniej 70% maksymalnej liczby punktów możliwych do zdobycia.
Na ocenę bardzo dobrą należy zaliczyć wszystkie weryfikowane efekty, przy średnim poziomie zaliczenia - co najmniej 90% maksymalnej liczby punktów możliwych do zdobycia

5. CAŁKOWITY NAKŁAD PRACY STUDENTA POTRZEBNY DO OSIĄGNIĘCIA ZAŁOŻONYCH EFEKTÓW W GODZINACH ORAZ PUNKTACH ECTS

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe wynikające z harmonogramu studiów	30
Inne z udziałem nauczyciela akademickiego (udział w konsultacjach, egzaminie)	
Godziny niekontaktowe – praca własna studenta (przygotowanie do zajęć, egzaminu, napisanie referatu itp.)	45
SUMA GODZIN	75
SUMARYCZNA LICZBA PUNKTÓW ECTS	3

** Należy uwzględnić, że 1 pkt ECTS odpowiada 25-30 godzin całkowitego nakładu pracy studenta.*

6. PRAKTYKI ZAWODOWE W RAMACH PRZEDMIOTU

wymiar godzinowy	-
zasady i formy odbywania praktyk	-

7. LITERATURA

Literatura podstawowa:

1. Marcin Karbowski, Podstawy kryptografii, Wydawnictwo HELION, Gliwice 2014.
2. Czesław Kościelny i in., Kryptografia. Teoretyczne podstawy i praktyczne zastosowania, Wydawnictwo PJWSTK, Warszawa 2009.
3. William Stallings, Kryptografia i bezpieczeństwo sieci komputerowych, Wydawnictwo HELION, Gliwice 2012.
4. David Hook, Kryptografia w Javie. Od podstaw, Wydawnictwo HELION, Gliwice 2006.

Literatura uzupełniająca:

1. Tomasz Adamski, Zbiór zadań z podstaw teoretycznych kryptografii i ochrony informacji, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2014.

Akceptacja Kierownika Jednostki lub osoby upoważnionej