SYLABUS

DOTYCZY CYKLU KSZTAŁCENIA *2024-2028*

Rok akademicki 2027/2028

1. PODSTAWOWE INFORMACJE O PRZEDMIOCIE

Nazwa przedmiotu	Przedmiot obieralny 2: Podstawy kryptografii
Kod przedmiotu*	
nazwa jednostki prowadzącej kierunek	Instytut Informatyki, Wydział Nauk Ścisłych i Technicznych
Nazwa jednostki realizującej przedmiot	Instytut Informatyki, Wydział Nauk Ścisłych i Technicznych
Kierunek studiów	Informatyka i ekonometria
Poziom studiów	studia pierwszego stopnia
Profil	praktyczny
Forma studiów	Studia stacjonarne
Rok i semestr/y studiów	rok IV, sem. VII
Rodzaj przedmiotu	przedmiot specjalnościowy obieralny
Język wykładowy	polski
Koordynator	dr Anna Król
Imię i nazwisko osoby prowadzącej / osób prowadzących	dr Anna Król

** -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
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

1. Historia kryptografii.
2. Matematyczne podstawy kryptografii.
3. Kryptografia symetryczna i szyfry symetryczne.
4. Kryptografia asymetryczna i szyfry asymetryczne.
5. Kryptoanaliza.
6. Zarządzanie kluczami (PKI).
7. Funkcje skrótu i podpis cyfrowy.
8. Narzędzia kryptograficzne.
9. Prawne aspekty wykorzystania kryptografii

B. Problematyka laboratoryjnych

1. Kryptografia symetryczna i szyfry symetryczne.
2. Kryptografia asymetryczna i szyfry asymetryczne.
3. Kryptoanaliza.
4. Zarządzanie kluczami (PKI).
5. Narzędzia kryptograficzne.

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 sie (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	Laboratorium

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)	1
Godziny niekontaktowe – praca własna studenta (przygotowanie do zajęć, egzaminu, napisanie referatu itp.)	45
SUMA GODZIN	76
SUMARYCZNA LICZBA PUNKTÓW ECTS	3

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 2021.
2. Massimo Bertaccini, Algorytmy kryptograficzne : przewodnik po algorytmach w blockchain, kryptografii kwantowej, protokołach o wiedzy zerowej oraz szyfrowaniu homomorficznym, Helion, 2023
3. Czesław Kościelny i in., Kryptografia. Teoretyczne podstawy i praktyczne zastosowania, Wydawnictwo PJWSTK, Warszawa 2009.
4. William Stallings, Kryptografia i bezpieczeństwo sieci komputerowych, Wydawnictwo HELION, Gliwice 2012.

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