SYLABUS

DOTYCZY CYKLU KSZTAŁCENIA *2023-2025*

Rok akademicki 2023/2024

1. PODSTAWOWE INFORMACJE O PRZEDMIOCIE

Nazwa przedmiotu	*kryptografia praktyczna*
Kod przedmiotu	
Nazwa jednostki prowadzącej kierunek	*Instytut Informatyki, Kolegium Nauk Przyrodniczych*
Nazwa jednostki realizującej przedmiot	*Instytut Informatyki, Kolegium Nauk Przyrodniczych*
Kierunek studiów	*informatyka*
Poziom studiów	*studia II stopnia*
Profil	*ogólnoakademicki*
Forma studiów	*stacjonarne*
Rok i semestr/y studiów	*rok I, semestr 1*
Rodzaj przedmiotu	*przedmiot podstawowy*
Język wykładowy	*język polski*
Koordynator	*dr hab. Andrzej Łopuszański, prof. UR*
Imię i nazwisko osoby prowadzącej / osób prowadzących	*dr hab. Andrzej Łopuszański, prof. UR*

1.1.Formy zajęć dydaktycznych, wymiar godzin i punktów ECTS

Semestr (nr)	Wykł.	Ćw.	Konw.	Lab.	Sem.	ZP	Prakt.	Projekt	**Liczba pkt. ECTS**
1	15			30					4

1.2. Sposób realizacji zajęć

zajęcia w formie tradycyjnej

1.3 Forma zaliczenia przedmiotu (z toku)

zaliczenie z oceną

2. WYMAGANIA WSTĘPNE

Algorytmy i struktury danych, elementy matematyki dyskretnej, elementy rachunku prawdopodobieństwa, kombinatoryki i statystyki, algebra liniowa (operacje na macierzach), elementy algebry i teorii liczb

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

3.1 Cele przedmiotu

C1	Celem przedmiotu jest usystematyzowane i pogłębione przedstawienie tematyki kryptologii: zapoznanie studentów ze współczesnymi szyframi, ich mocnymi i słabymi stronami, i z matematyką kryptograficzną.

3.2 Efekty uczenia się dla przedmiotu

EK (efekt uczenia się)	Treść efektu uczenia się zdefiniowanego dla przedmiotu Student:	Odniesienie do efektów kierunkowych
EK_01	- zna narzędzia i protokoły, wykorzystujące w sposób praktyczny algorytmy kryptograficzne. Dysponuje wiedzą na temat teoretycznych podstaw kryptografii: teorii informacji, teorii złożoności obliczeniowej i teorii liczb. Zna i rozumie w pogłębionym stopniu sposób działania najważniejszych algorytmów kryptografii symetrycznej i asymetrycznej.	K_W02
EK_02	- posiada umiejętność stosowania różnych metod kryptoanalizy dla rozwiązywania szyfrów o trudności poziomu klasycznych.	K_W02
EK_03	- potrafi dobierać istniejące narzędzia i algorytmy kryptograficzne w zależności od potrzeb i obszaru zastosowań.	K_U02
EK_04	- może proponować modyfikacje istniejących algorytmów, metod, narzędzi, implementować je, testować i wykorzystywać testy lub symulacje (eksperymenty) do porównywania z referencyjnymi rozwiązaniami.	K_U02

3.3 Treści programowe

A. Problematyka wykładu

Formalna definicja systemu kryptograficznego. Podejście probabilistyczne Markowa do kryptoanalizy. Teoria informacji Shannona: ilość informacji, entropia wiadomości, nadmiarowość języka. Teoretyczne i praktycznie bezpieczeństwo systemu kryptograficznego.
Szyfry podstawieniowe polialfabetyczne i poligraficzne. Słabe strony i wrażliwości szyfrów podstawieniowych i transpozycyjnych. Analiza częstości. Metody optymalizacyjne w kryptoanalizie.
Matematyka kryptograficzna i analiza częstotliwości. Arytmetyka modularna, NWD, podstawy teorii grup, liczby pierwsze i odp.twierdzenia i algorytmy. Pseudolosowość
Algorytmy kryptografii symetrycznej. Algorytmy strumieniowe i blokowe. Algorytmy DES, Blowfish i AES.
Algorytmy kryptografii asymetrycznej. RSA. ElGamal.
Kryptografia wizualna (szyfrowanie i kodowanie obrazów oraz steganografia)
Kryptografia krzywych eliptycznych.
Kryptografia wielowymiarowa.

Funkcje skrótu i kody uwierzytelnienia wiadomości. Integralność i niezaprzeczalność wiadomości. Bezkonfliktowość funkcji skrótu. Algorytm MD5 i SHA-1. Kody uwierzytelniania wiadomości MAC.

B. Problematyka ćwiczeń laboratoryjnych

Implementacja w Python szyfrów na przykładach.
Implementacja ataków na szyfry z określonymi słabościami (na zajęciach i grupowe lub indywidualne projekty dla pracy bardziej samodzielnej) z użyciem metody analizy częstości, metod optymalizacyjnych i innych.
Implementacja frakcjonowania na przykładach prostej zamiany i transpozycji.
Pojęcia wydajności kodów, metody porównania w kryptoanalizie.

3.4 Metody dydaktyczne

Wykład: wykład z prezentacją multimedialną
Ćwiczenia laboratoryjne: indywidualne i grupowe rozwiązywanie zadań z użyciem komputera

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 – EK_02	Kolokwium ustne	Wykł.
EK_03 – EK_04	Kolokwium pisemne	Lab.

4.2 Warunki zaliczenia przedmiotu (kryteria oceniania)

Zaliczenie przedmiotu następuje na podstawie zaliczenia wszystkich efektów uczenia.
Laboratorium: zaliczenie na ocenę na podstawie kolokwium, projektu lub dwóch (w zależności od wybranego poziomu trudności) z uwzględnieniem pracy w ciągu semestru. Skala ocen zgodna z Regulaminem Studiów UR: dost. - (51 - 60)% pkt, +dost. - (61 - 70)% pkt, dobry - (71 - 80)% pkt, +dobry - (81 - 90)% pkt, bardzo dobry - (91 - 100)% pkt.
Wykład: Zaliczenie binarne, w formie rozmowy, z zakresu zagadnień omówionych na wykładach.

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	45
Inne z udziałem nauczyciela akademickiego (udział w konsultacjach, egzaminie)	5
Godziny niekontaktowe – praca własna studenta (przygotowanie do zajęć, egzaminu, napisanie referatu itp.)	50
SUMA GODZIN	100
SUMARYCZNA LICZBA PUNKTÓW ECTS	**4**

6. PRAKTYKI ZAWODOWE W RAMACH PRZEDMIOTU

wymiar godzinowy	-
zasady i formy odbywania praktyk	-

7. LITERATURA

LITERATURA PODSTAWOWA:

1. Bauer F.L. (Helion 2002): Sekrety kryptografii
2. Douglas R. Stinson (WNT 2005): Kryptografia. W teorii i praktyce.
3. David Kahn (WNT 2004): Łamacze kodów. Historia kryptologii.
4. Koblitz N. (WNT 1995): Wykład z teorii liczb i kryptografii

LITERATURA UZUPEŁNIAJĄCA:

1. KARBOWSKI M. (Helion 2014): Podstawy kryptografii.
2. AUMASSON J.-P. (PWN 2018): Nowoczesna kryptografia. Praktyczne wprowadzenie do szfrowania.