SYLABUS

DOTYCZY CYKLU KSZTAŁCENIA *2022-2024*

Rok akademicki 2022/2023

1. PODSTAWOWE INFORMACJE O PRZEDMIOCIE

Nazwa przedmiotu	*elementy kryptografii*
Kod przedmiotu	
Nazwa jednostki prowadzącej kierunek	*Kolegium Nauk Przyrodniczych*
Nazwa jednostki realizującej przedmiot	*Kolegium Nauk Przyrodniczych*
Kierunek studiów	*informatyka*
Poziom studiów	*studia II stopnia*
Profil	*ogólnoakademicki*
Forma studiów	*stacjonarne*
Rok i semestr studiów	*rok I, semestr 1*
Rodzaj przedmiotu	*przedmiot podstawowy*
Język wykładowy	*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.	Inne (jakie?)	**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

Elementy teorii prawdopodobieństwa, kombinatoryki i statystyki, algebry i teorii liczb.

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

3.1 Cele przedmiotu

C1	Celem przedmiotu jest zaznajomienie studentów z tematyką kryptologii: systematyką szyfrów, popularnymi przykładami, w szczególności z szyframi symetrycznymi i asymetrycznymi DES, AES, RSA, ElGamal.

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 najistotniejsze osiągnięcia w dziedzinie kryptologii, w szczególności: - zna i rozumie podstawowe pojęcia kryptografii i kryptoanalizy; - zna historię kryptografii i jej rozwoju; - dysponuje wiedzą na temat teoretycznych podstaw kryptografii: teorii informacji, teorii złożoności obliczeniowej i teorii liczb; - zna i rozumie sposób działania najważniejszych algorytmów kryptografii symetrycznej i asymetrycznej; - zna narzędzia i protokoły, wykorzystujące w sposób praktyczny algorytmy kryptograficzne.	K_W04
EK_02	Student rozumie zagrożenia związane z brakiem lub niestarannym zarządzaniem bezpieczeństwem danych w przedsiębiorstwach oraz w jednostkach naukowobadawczych	K_W07
EK_03	Student posiada umiejętność - napisania algorytmu szyfrującego oraz jego funkcjonalnej implementacji; - szyfrowania i deszyfrowania w określonym systemie kryptograficznym; - stosowania różnych metod kryptoanalizy.	K_U05
EK_04	Student świadomie korzysta z dostępnych nowoczesnych narzędzi informatycznych służących zachowaniu zasad cyberbezpieczeństwa. Potrafi ocenić przydatność wybranych metod i narzędzi w aspekcie zapewnienia przez nie bezpieczeństwa danych.	K_U05

3.3 Treści programowe

A. Problematyka wykładu

Wprowadzenie do kryptografii. Podstawowe pojęcia kryptografii i kryptoanalizy. Różnica między kodowaniem i szyfrowaniem. Kryptografia a steganografia. Klasyfikacja i omówienie ataków na systemy kryptograficzne. Sposoby utajniania informacji w przeszłości. Historia (do XIX wieku)

i rozwój kryptografii i kryptoanalizy. Najprostsze historyczne systemy kryptograficzne. Ich wrażliwości i przykłady ataków.
Szyfry podstawieniowe i transpozycyjne. Analiza częstości występowania liter. Rodzaje ataków BruteForce i HillClimbing. Szyfry podstawieniowe afiniczne (np. szyfry Cezara, Atbasz), prostej zamiany, np. homofoniczne, ich słabe strony i wrażliwości, rodzaje efektywnych ataków na nich.
Formalna definicja systemu kryptograficznego. Podejście probabilistyczne Markowa do kryptoanalizy. Teoria informacji Shannona: ilość informacji, entropia wiadomości, nadmiarowość języka. Teoretyczne bezpieczeństwo systemu kryptograficznego. Złożoność obliczeniowa algorytmu Kołmogorowa. Bezpieczeństwo systemu kryptograficznego z punktu widzenia teorii złożoności obliczeniowej. Praktyczne bezpieczeństwo systemów kryptograficznych.
Szyfry podstawieniowe polialfabetyczne (prz. Vigenere i jego wariacje: Beauforta, autokey). Algebra liniowa modulo N i rachunek macierzowy modulo N. Szyfry podstawieniowe poligraficzne (Playfair, bifid, trifid, Hill), ich słabe strony i wraźliwości, metoda Kasiski dla Vigenere.
Szyfry blokowe. Szyfry transpozycyjne z przykładami historycznymi (m.in. RailFence, ścieżki, Kardano grill, kolumnowej transpozycji etc), ich słabe strony i wrażliwości, rodzaje efektywnych ataków na nich.
Metoda frakcjonowania, jak efektywny sposób kombinowania szyfrów.
Szyfr podwójnej transpozycji, szyfr VIC.
Algorytmy kryptografii symetrycznej. Algorytmy strumieniowe i blokowe. Algorytmy DES, Blowfish i AES.
Algorytmy kryptografii asymetrycznej. Kryptografia z kluczem publicznym. Klucz publiczny i klucz prywatny. RSA i ElGamal.
Funkcje skrótu i kody uwierzytelnienia wiadomości. Integralność i niezaprzeczalność wiadomości. Funkcje skrótu. Bezkonfliktowość funkcji skrótu. Algorytm MD5 i SHA-1. Kody uwierzytelniania wiadomości MAC.

B. Problematyka ćwiczeń laboratoryjnych

Implementacja w Python historycznych szyfrów prostej zamiany, transpozycji kolumnowej, Vigenera, Playfair, Hill i innych.
Implementacja ataków różnego rodzaju dla wymienionych wyżej i innych rodzajów szyfrów historycznych (na zajęciach i grupowe lub indywidualne projekty dla pracy bardziej samodzielnej).
Pojęcia ważnych dla kryptoanalizy wydajności kodów, metod porównania.
Implementacja frakcjonowania na przykładach prostej zamiany i transpozycji.
Podstawowe algorytmy kryptografii.

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	Kolokwium pisemne	laboratorium
EK_03	Projekty grupowe i/lub indywidualne, obserwacja w trakcie zajęć	laboratorium
EK_02, EK_04	Obserwacja w trakcie zajęć	laboratorium

4.2 Warunki zaliczenia przedmiotu (kryteria oceniania)

Zaliczenie przedmiotu następuje na podstawie zaliczenia wszystkich efektów uczenia się, w szczególności:
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 (udział w konsultacjach, egzaminie)	5
Godziny niekontaktowe – praca własna studenta (przygotowanie do zajęć, egzaminu, napisanie referatu itp.)	60
SUMA GODZIN	110
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.