Załącznik nr 1.5 do Zarządzenia Rektora UR nr 12/2019

DOTYCZY CYKLU KSZTAŁCENIA *2021- 2024*
(skrajne daty)
Rok akademicki 2023/2024

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 Instytut Informatyki
Kierunek studiów	Matematyka
Poziom studiów	studia I stopnia
Profil	ogólnoakademicki
Forma studiów	stacjonarne
Rok i semestr studiów	rok III, semestr 6
Rodzaj przedmiotu	specjalnościowy
Język wykładowy	język polski
Koordynator	dr hab. prof. UR Andrzej Łopuszański
Imię i nazwisko osoby prowadzącej / osób prowadzących	dr hab. prof. UR Andrzej Łopuszański

***** *- 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**
6	30			30					6

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)
Ćwiczenia - zaliczenie na ocenę
Wykład - egzamin

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 kryptografii.

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 i rozumie podstawowe pojęcia kryptologii i kryptoanalizy, a także dysponuje wiedzą związaną z teorią informacji, teorią złożoności obliczeniowej i teorią liczb niezbędną stanowiącą podstawę kryptografii.	K_W07
EK_02	Student zna historię kryptografii i jej rozwoju.	K_W08
EK_03	Student zna i rozumie sposób działania najważniejszych algorytmów kryptografii symetrycznej i asymetrycznej.	K_W07
EK_04	Student zna narzędzia i protokoły, wykorzystujące w sposób praktyczny algorytmy kryptograficzne.	K_W07
EK_05	Student potrafi utworzyć i zaimplementować algorytm szyfrujący.	K_U16, K_U22
EK_06	Student potrafi szyfrować i deszyfrować w określonym systemie kryptograficznym.	K_U16, K_U22
EK_07	Student potrafi stosować różne metody kryptoanalizy.	K_U16, K_U22
EK_08	Student ma świadomość potrzeby zapewnienia bezpieczeństwa i poufności informacji. Orientuje się w charakterystykach istniejących narzędzi i algorytmów kryptograficznych i potrafi dobierać je w zależności od potrzeb i obszaru zastosowań.	K_K04, K_K05, K_K07

3.3 Treści programowe

A. Problematyka wykładu

Treści merytoryczne
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 (prz.Caesar, atbash), prostej zamiany, homofoniczne (prz.), 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 wrażliwości, 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 audytoryjnych, konwersatoryjnych, laboratoryjnych, zajęć praktycznych

Treści merytoryczne ćwiczeń
Implementacja w Python historycznych szyfrów prostej zamiany, transpozycji kolumnowej, Vigenera, Playfair, Hill i innych. Implementacja ataków różnego rodzaju dla wymienionych wyżej i innych wrażliwych rodzajów szyfrów historycznych (na zajęciach i grupowe lub indywidualne projekty dla pracy bardziej samodzielnej). Pojęcie o ważnej dla kryptoanalizy wydajności kodu, porównania. Implementacja frakcjonowania na przykładzie prostej zamiany i transpozycji.

3.4 Metody dydaktyczne

Ćwiczenia laboratoryjne: praca przy komputerze, projekt praktyczny

Wykład: wykład z prezentacją multimedialną.

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	obserwacja w trakcie zajęć , projekt lub kolokwium, egzamin	w, lab
EK_02	obserwacja w trakcie zajęć , projekt lub kolokwium, egzamin	w, lab
EK_03	obserwacja w trakcie zajęć , projekt lub kolokwium, egzamin	w, lab
EK_04	obserwacja w trakcie zajęć , projekt lub kolokwium, egzamin	w, lab
EK_05	obserwacja w trakcie zajęć , projekt lub kolokwium	w, lab
EK_06	obserwacja w trakcie zajęć , projekt lub kolokwium	w, lab
EK_07	obserwacja w trakcie zajęć , projekt lub kolokwium	w, lab
EK_08	obserwacja w trakcie zajęć	w, lab

4.2 Warunki zaliczenia przedmiotu (kryteria oceniania)

Laboratorium: Projekt lub dwa w końcu semestru (w zależności od wybranego poziomu trudności) z uwzględnieniem pracy w ciągu semestru.

Wykład: egzamin.

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	60
Inne z udziałem nauczyciela (udział w konsultacjach, egzaminie)	5
Godziny niekontaktowe – praca własna studenta (przygotowanie do zajęć, egzaminu, napisanie referatu itp.)	85
SUMA GODZIN	150
SUMARYCZNA LICZBA PUNKTÓW ECTS	6

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

6. PRAKTYKI ZAWODOWE W RAMACH PRZEDMIOTU

wymiar godzinowy	nie dotyczy
zasady i formy odbywania praktyk	nie dotyczy

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

Akceptacja Kierownika Jednostki lub osoby upoważnionej