KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Sztuczna Inteligencja w kryptografii

Przedmiot

Kierunek studiów
Sztuczna inteligencja
Studia w zakresie (specjalność)
-
Poziom studiów
drugiego stopnia
Forma studiów
stacjonarne

Rok/semestr
1/2
Profil studiów
ogólnoakademicki
Język oferowanego przedmiotu
angielski
Wymagalność
obieralny

Liczba godzin

Wykład
15
Ćwiczenia

Laboratoria
15
Projekty/seminaria

Inne (np. online)

Liczba punktów ECTS

3

Wykładowcy

Odpowiedzialny za przedmiot/wykładowca:
dr inż. Anna Grocholewska-Czuryło

anna.grocholewska-czurylo@put.poznan.pl

Wydział Informatyki i Telekomunikacji

Odpowiedzialny za przedmiot/wykładowca:

Wymagania wstępne

Student rozpoczynający ten przedmiot powinien posiadać wiedzę w zakresie podstawowych algorytmów i ich analizy, sieci neuronowych, algorytmów ewolucyjnych, systemów operacyjnych, sieci komputerowych i algorytmów kryptograficznych. Powinien potrafić posługiwać się środowiskami programistycznymi i platformami do pisania, wykonywania i testowania programów. Powinien potrafić konstruować algorytmy i dokonywać analizy ich złożoności. Powinien posiadać umiejętności pozyskiwania informacji ze wskazanych źródeł oraz mieć gotowość do podjęcia współpracy w ramach zespołu.

Cel przedmiotu

Przekazanie studentom wiedzy na temat zaawansowanych zasad działania i projektowania algorytmów kryptograficznych i wskazania obszarów, gdzie można zastosować metody/modele ze sztucznej inteligencji. Zapoznanie studentów z metodami analizy i oceny wybranych systemów kryptograficznych.

Przedmiotowe efekty uczenia się

Wiedza

Student/ka ma szczegółową wiedzę na temat:

- jakie kryteria powinien spełniać bezpieczny system informatyczny i jakie środki ochrony należy zastosować aby to osiągnąć,

- ma uporządkowaną i podbudowaną teoretycznie wiedzę ogólną związaną z kluczowymi zagadnieniami z zakresu kryptograficznych mechanizmów ochrony danych (szyfry symetryczne i asymetryczne, funkcje skrótu, podpisy cyfrowe), krzywych eliptycznych, protokołów uwierzytelniania, algorytmów zarządzania kluczami i dzielenia sekretu,

- ma zaawansowaną wiedzę szczegółową dotyczącą wybranych zagadnień z zakresu projektowania i oceny komponentów szyfrów,

- ma wiedzę o trendach rozwojowych i najistotniejszych nowych osiągnięciach w zastosowaniu sztucznej inteligencji w kryptografii

Umiejętności

Student/ka potrafi:

- przeanalizować i zaprojektować wybrane komponenty szyfrów, spełniające określone kryteria,

- zaprojektować i zaimplementować wybrane algorytmy kryptograficzne

- wskazać metody alternatywne dla tradycynych, stosujące sztuczną inteligencję

- dokonać analizy i oszacowania poziomu bezpieczeństwa zastosowanych mechanizmów kryptograficznych i oszacować, czy zastosowana metoda jest lepsza od tradycyjnej

- zaproponować, zaprojektować i zaimplementować alternatywne mechanizmy kryptograficzne zapewniające większy poziom bezpieczeństwa.

Kompetencje społeczne

Student/ka rozumie, że:

- ważnym aspektem jest zastosowanie odpowiednich, aktualnych metod kryptograficznych i sztucznej inteligencji,

- równie ważna jast odpowiednia implementacja algorytmów kryptograficznych,

- konieczne jest aktualizowanie wiedzy na temat bezpiecznych parametrów stosowanych algorytmów, protokołów i narzędzi.

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wiedza nabyta w ramach wykładu weryfikowana jest podczas pisemnego godzinnego kolokwium, składającego się z 3 pytań. Próg zaliczeniowy: ponad 50% punktów. Zagadnienia zaliczeniowe, na podstawie których opracowywane są pytania, są dostępne w ramach systemu eKursy.

Umiejętności nabyte w ramach zajęć laboratoryjnych weryfikowane są na bieżąco podczas zajęć (poprzez sprawdzenie wykonanego zadania czy ćwiczenia laboratoryjnego).

Treści programowe

Tematyka wykładów

1. Szyfry symetryczne vs asymetryczne

2. Teoria chaosu i generatory ciągów pseudolosowych, rozszerzone testy losowości ciągów.

3. Funkcje skrótu - projektowanie funkcji skrótu, klasyfikacja funkcji ze względu na budowę, kryteria jakie muszą spełniać dobre funkcje skrótu, MAC, ataki na funkcje skrótu, zastosowania, struktura Sponge - na przykładzie funkcji Keccak.

4. Zastosowanie sieci neuronowych w kryptografii

5. Zastosowanie algorytmów ewolucyjnych w kryptografii

6. Obszary zastosowań sztucznej inteligencji w kryptografii, trendy i wyzwania.

Laboratorium

1. Analiza najważniejszego komponentu szyfrów blokowych i kryteriów jakie musi spełniać. Implementacja metod do analizy S-bloków: zbalansowania, lawinowości i nieliniowości .

2. Implementacja generatora ciągów losowych opartego na wybranym algorytmie z teorii chaosu, oraz testów sprawdzających losowość wygenerowanego ciągu.

3. Implementacja algorytmu podziału sekretu lub zarządzania materiałem kryptograficznym

4. Implementacja wybranego systemu kryptograficznego w zespołach.

Metody dydaktyczne

Wykład prowadzony jest w sposób interaktywny (z formułowaniem pytań do studentów) przy użyciu prezentacji multimedialnych. Materiały udostępniane są studentom w wersji elektronicznej.

Ćwiczenia laboratoryjne - prezentacja problemu/ćwiczenia do zrealizowania na tablicy (z podstawowym poziomem trudności i rozszerzonym dla chętnych) oraz wykonaniem ćwiczenia w wybranym przez studenta języku programowania w ramach laboratorium.

Literatura

Podstawowa

Pieprzyk J., Hardjono T., Seberry J., Teoria bezpieczeństwa systemów komputerowych, Helion 2003 (sygnatura w bibliotece PP: W 110215).

Uzupełniająca

Menezes A. i inni, Kryptografia stosowana, WNT, 2005, (sygnatura w bibliotece PP: W 112188)

Materiały udostępniane przez prowadzącego, co roku aktualizowane.

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	75	3,0
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	30	1,5
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych, przygotowanie do kolokwium na laboratorium, przygotowanie do egzaminu)[1]	45	1,5

[1] niepotrzebne skreślić lub dopisać inne czynności