

KARTA KURSU (realizowanego w module specjalności)
Data Science

Nazwa	Zaawansowane metody kryptografii
Nazwa w j. ang.	Advanced cryptography methods

Koordynator	Prof dr hab. Oleksandr Korchenko	Zespół dydaktyczny
		Prof dr hab. Oleksandr Korchenko
Punktacja ECTS*	5	

Opis kursu (cele kształcenia)

Kurs wprowadza studentów w zaawansowane metody kryptografii oraz ich zastosowanie w analizie danych w kontekście bezpieczeństwa informacji. Studenci poznają klasyczne i nowoczesne systemy szyfrowania, metody wykrywania zagrożeń z wykorzystaniem uczenia maszynowego, bezpieczne uczenie oraz interpretację wyników pod kątem ryzyka i prywatności danych. Kurs rozwija praktyczne umiejętności implementacji, optymalizacji i oceny bezpieczeństwa systemów szyfrujących oraz modeli uczenia maszynowego, przy czym techniki uczenia maszynowego stosowane są wyłącznie w kontekście analizy bezpieczeństwa.

Kurs prowadzony jest w języku polskim.

Warunki wstępne

Wiedza	Student powinien posiadać podstawową wiedzę z zakresu kryptografii i bezpieczeństwa danych oraz podstaw uczenia maszynowego i statystyki. Wymagana jest znajomość języka Python oraz bibliotek ML i kryptograficznych, takich jak scikit-learn, PyTorch/TensorFlow czy PyCryptodome, a także podstawy algebry liniowej, analizy danych i probabilistyki.
Umiejętności	Umiejętność programowania oraz samodzielnego korzystania z literatury przedmiotu i dokumentacji technicznej, a także umiejętność analizy i przetwarzania danych w kontekście bezpieczeństwa informacji.
Kursy	

Efekty uczenia się

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Wiedza	<p>Po zakończeniu kursu student:</p> <p>W01: posiada pogłębioną wiedzę z zakresu kryptografii, systemów szyfrowania oraz metod analizy bezpieczeństwa danych, w tym zastosowania matematyki i statystyki w projektowaniu i ocenie algorytmów kryptograficznych;</p> <p>W02 - zna i rozumie metody uczenia maszynowego stosowane w bezpieczeństwie danych, w tym detekcję anomalii, bezpieczne uczenie i homomorficzne operacje na zaszyfrowanych danych;</p> <p>W03: rozumie zasady etyczne, regulacje prawne oraz standardy międzynarodowe dotyczące prywatności i bezpieczeństwa danych, a także potrafi je stosować w praktycznych projektach kryptograficznych i ML.</p>	SD_W01 SD_W03 - SD_W09

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Umiejętności	Po zakończeniu kursu student:	SD_U01 - SD_U06 SD_U08 - SD_U09
	<p>U01: potrafi samodzielnie stosować metody kryptograficzne oraz techniki analizy statystycznej i probabilistycznej do rozwiązywania praktycznych problemów związanych z bezpieczeństwem danych i ochroną informacji;</p> <p>U02: potrafi projektować i implementować algorytmy uczenia maszynowego w kontekście bezpieczeństwa danych, w tym detekcję anomalii, bezpieczne uczenie i operacje homomorficzne na zaszyfrowanych danych;</p> <p>U03 - potrafi stosować zasady etyczne i regulacje prawne dotyczące ochrony danych w projektach kryptograficznych i uczenia maszynowego oraz przygotowywać raporty i prezentacje wyników analizy bezpieczeństwa danych.</p>	

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Kompetencje społeczne	Po zakończeniu kursu student:	SD_K01 SD_K03
	<p>K01: ma świadomość społecznej roli specjalisty zajmującego się bezpieczeństwem danych i kryptografią, rozumie znaczenie etycznego postępowania w projektach informatycznych oraz potrafi identyfikować i rozstrzygać dylematy związane z ochroną prywatności i bezpieczeństwem informacji.</p>	

Studia stacjonarne

Organizacja							
Forma zajęć	Wykład (W)	Ćwiczenia w grupach					
		A	K	L	S	P	E
Liczba godzin	30			30			

Studia niestacjonarne

Organizacja							
Forma zajęć	Wykład (W)	Ćwiczenia w grupach					
		A	K	L	S	P	E
Liczba godzin	20			20			

Opis metod prowadzenia zajęć

Wykłady, ćwiczenia laboratoryjne, dyskusje i zadania grupowe (indywidualne), kolokwium/test.

Formy sprawdzania efektów uczenia się

	E – learning	Gry dydaktyczne	Ćwiczenia w szkole		Zajęcia terenowe	Praca laboratoryjna	Projekt indywidualny	Projekt grupowy	Udział w dyskusji	Referat	Praca pisemna (esej)	Egzamin ustny	Egzamin pisemny	Inne
W01						X	X	X	X					
W02						X	X	X	X					
W03						X	X	X	X					
U01						X	X	X	X					
U02						X	X	X	X					
U03						X	X	X	X					
K01									X					

Kryteria oceny	Ocena końcowa jest zależna od ocen cząstkowych, systematyczności realizowanych zadań oraz oceny uzyskanej za realizację projektu zespołowego lub indywidualnego. W szczególności ocenę dobrą i bardzo dobrą z zajęć może uzyskać student, który samodzielnie implementuje algorytmy kryptograficzne i metody uczenia maszynowego w kontekście bezpieczeństwa danych, potrafi analizować ich poprawność, wydajność oraz warunki i obszary stosowalności w praktycznych scenariuszach ochrony informacji.
----------------	---

Uwagi	
-------	--

Treści merytoryczne (wykaz tematów)

<p>1. Podstawy matematyczne i kryptograficzne</p> <ul style="list-style-type: none"> Algebra liniowa w kryptografii: macierze, wektory, tensory w szyfrowaniu i kodach korekcyjnych. Liczby pierwsze, modułarna arytmetyka, pierścienie i ciała skończone – zastosowania w kluczach kryptograficznych. Operacje probabilistyczne w kryptografii: losowość w generowaniu kluczy, testy statystyczne bezpieczeństwa. Wprowadzenie do funkcji skrótu i permutacji jako elementów transformacji danych. <p>2. Klasyczne i nowoczesne systemy szyfrowania</p> <ul style="list-style-type: none"> Szyfry symetryczne: DES, AES – matematyczne podstawy i analiza bezpieczeństwa. Szyfry asymetryczne: RSA, ElGamal, ECC – teoria, algorytmy i optymalizacja obliczeń. Protokoły wymiany kluczy i podpisy cyfrowe. Wykorzystanie metod statystycznych do analizy podatności szyfrów klasycznych i nowoczesnych. <p>3. Analiza i ataki kryptograficzne</p> <ul style="list-style-type: none"> Ataki typu side-channel i analiza statystyczna sygnałów. Analiza częstotliwości i testy losowości. Wykorzystanie uczenia maszynowego do wykrywania wzorców w szyfrowanych danych. Modelowanie probabilistyczne ryzyka i niepewności w atakach kryptograficznych. <p>4. Uczenie maszynowe w kontekście bezpieczeństwa danych</p> <ul style="list-style-type: none"> Klasyfikacja i detekcja anomalii w ruchu sieciowym. Autoenkodery i redukcja wymiarów do wykrywania anomalii w zaszyfrowanych danych. Probabilistyczne modele i Bayesian Learning w ocenie ryzyka bezpieczeństwa danych. Interpretacja modeli w kontekście bezpieczeństwa (Explainable AI w wykrywaniu ataków). <p>5. Homomorficzne i bezpieczne uczenie</p> <ul style="list-style-type: none"> Wprowadzenie do homomorficznych operacji na zaszyfrowanych danych. Federated learning i prywatność danych: ochrona danych w rozproszonych systemach ML. Optymalizacja i walidacja modeli uczenia na zaszyfrowanych danych.

- Praktyczne wyzwania: szybkość, dokładność i bezpieczeństwo w modelach prywatnych.
6. Optymalizacja i parametry kryptograficzne
- Strojenie parametrów algorytmów szyfrujących pod kątem bezpieczeństwa i wydajności.
 - Testy Monte Carlo, gradientowe metody optymalizacji w analizie bezpieczeństwa.
 - Porównanie strategii optymalizacji w kontekście odporności na ataki.
7. Etyka, prywatność i regulacje w kryptografii
- Zasady odpowiedzialnego projektowania systemów szyfrujących.
 - Prywatność i ochrona danych w analizie danych – RODO, HIPAA, regulacje branżowe.
 - Audyty bezpieczeństwa i interpretacja wyników testów bezpieczeństwa.
 - Fairness i unikanie biasu w modelach ML stosowanych do wykrywania ataków.
8. Praktyczne laboratoria i projekty
- Implementacja szyfrów klasycznych i nowoczesnych w Pythonie i bibliotekach kryptograficznych (PyCryptodome, cryptography).
 - Analiza podatności szyfrów z użyciem ML i metod statystycznych.
 - Projekty z homomorficznym uczeniem i federated learning na zaszyfrowanych danych.
 - Benchmarking i raporty bezpieczeństwa systemów kryptograficznych.

Wykaz literatury podstawowej

1. Menezes, A., van Oorschot, P., Vanstone, S. *Handbook of Applied Cryptography*, CRC Press, 1996.
2. Goodfellow, I., Bengio, Y., Courville, A. *Deep Learning*, MIT Press, 2016.
3. Shokri, R., Shmatikov, V., et al. *Privacy-Preserving Machine Learning: Methods and Applications*, Springer, 2020.

Wykaz literatury uzupełniającej

1. Boneh, D., Shoup, V. *A Graduate Course in Applied Cryptography*, 2020.
2. Abadi, M., et al. *Federated Learning: Collaborative Machine Learning without Centralized Training Data*, Foundations and Trends in Machine Learning, 2021.

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta) **studia stacjonarne**

liczba godzin w kontakcie z prowadzącymi	Wykład	30
	Konwersatorium (ćwiczenia, laboratorium itd.)	30
	Pozostałe godziny kontaktu studenta z prowadzącym	15
liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	20
	Przygotowanie krótkiej pracy pisemnej lub referatu po zapoznaniu się z niezbędną literaturą przedmiotu	
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	20
	Przygotowanie do egzaminu/zaliczenia	10
Ogółem bilans czasu pracy		125
Liczba punktów ECTS w zależności od przyjętego przelicznika		5

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta) **studia niestacjonarne**

liczba godzin w kontakcie z prowadzącymi	Wykład	20
	Konwersatorium (ćwiczenia, laboratorium itd.)	20
	Pozostałe godziny kontaktu studenta z prowadzącym	15
liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	25
	Przygotowanie krótkiej pracy pisemnej lub referatu po zapoznaniu się z niezbędną literaturą przedmiotu	
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	25
	Przygotowanie do egzaminu/zaliczenia	20
Ogółem bilans czasu pracy		125
Liczba punktów ECTS w zależności od przyjętego przelicznika		5