



Politechnika Wrocławska

Kryptografia Karta przedmiotu

Informacje podstawowe

Kierunek studiów informatyka algorytmiczna Specjalność - Jednostka organizacyjna Wydział Informatyki i Telekomunikacji Poziom kształcenia studia drugiego stopnia 3 semestry (magister inżynier) Forma studiów studia stacjonarne Profil studiów profil ogólnoakademicki	Cykl kształcenia 2025/2026 Kod przedmiotu 04INA0-25S302O06228G Grupa zajęć Tak Języki wykładowe polski Obligatoryjność Obowiązkowy Blok zajęciowy Przedmioty kierunkowe Przedmiot powiązany z badaniami naukowymi Tak
---	---

Semestr Semestr 2	Forma zaliczenia Egzamin Forma dydaktyczna i godziny zajęć Wykład: 30 Ćwiczenia: 30 Laboratorium: 15	Liczba punktów ECTS 5.0
-----------------------------	---	-----------------------------------

Przedmiotowe efekty uczenia się

Efekt przedmiotowy	Treść	Efekt kierunkowy
Z zakresu wiedzy		
PEU_W01	Formułuje i objaśnia najważniejsze techniki współczesnej kryptografii służące zapewnieniu bezpieczeństwa systemów IT.	K2_INA_W01, K2_INA_W02, K2_INA_W03, K2_INA_W04

PEU_W02	Definiuje i objaśnia narzędzia i struktury matematyczne wykorzystywane do konstrukcji schematów kryptograficznych.	K2_INA_W01, K2_INA_W02, K2_INA_W03, K2_INA_W04, K2_INA_W05, K2_INA_W07, K2_INA_W08
PEU_W03	Wymienia i opisuje najważniejsze problemy i wyzwania stojące przed kryptografią i kryptoanalizą.	K2_INA_W01, K2_INA_W02, K2_INA_W03, K2_INA_W04, K2_INA_W05, K2_INA_W08
Z zakresu umiejętności		
PEU_U01	Opracowuje schematy systemów kryptograficznych do zapewnienia bezpieczeństwa systemów IT.	K2_INA_U05, K2_INA_U06, K2_INA_U10, K2_INA_U11
PEU_U02	Posługuje się abstrakcyjnymi strukturami matematycznymi do analizy i implementacji systemów kryptograficznych.	K2_INA_U01, K2_INA_U02, K2_INA_U03, K2_INA_U04, K2_INA_U05, K2_INA_U06, K2_INA_U10, K2_INA_U11
PEU_U03	Analizuje i ocenia systemy kryptograficzne i dostosowuje rozwiązania do postawionych wymagań.	K2_INA_U01, K2_INA_U02, K2_INA_U10
Z zakresu kompetencji społecznych		
PEU_K01	Rozumie konieczność stosowania technik kryptograficznych.	K2_INA_K03, K2_INA_K04, K2_INA_K05
PEU_K02	Jest zdolny do dostosowania rozwiązań kryptograficznych do uwarunkowań.	K2_INA_K01, K2_INA_K02, K2_INA_K03, K2_INA_K05
PEU_K03	Ma świadomość praktycznych ataków i zagrożeń związanych z kryptografią.	K2_INA_K01, K2_INA_K03, K2_INA_K04

Treści programowe zapewniające uzyskanie efektów uczenia się

- Prezentacja zaawansowanych technik kryptograficznych stosowanych w praktyce.
- Zrozumienie zaawansowanych mechanizmów współczesnej kryptografii.
- Zdobycie umiejętności w implementacji technik kryptograficznych.

Nakład pracy studenta

Rodzaje zajęć studenta	Średnia liczba godzin przeznaczonych na zrealizowane aktywności
Wykład	30
Ćwiczenia	30
Laboratorium	15

Przygotowanie do zajęć	16
Przygotowanie projektu	30
Zaliczenie/Egzamin	4
Całkowity nakład pracy studenta (CNPS)	Liczba godzin 125

Informacje rozszerzone

Koordynator przedmiotu	Łukasz Krzywiecki
-------------------------------	-------------------

Szczegółowe treści programowe

Lp.	Treści programowe	Efekty uczenia się dla przedmiotu	Forma dydaktyczna i liczba godzin
1.	1. Kryptografia – historia. (2h) 2. Systemy z kluczem symetrycznym – wstęp, modele bezpieczeństwa. (2h) 3. One time pad. Szyfry strumieniowe. (2h) 4. Szyfry blokowe. (2h) 5. Integralność wiadomości. Funkcje haszujące. (2h) 6. Systemy z kluczem publicznym – wstęp, modele bezpieczeństwa. (2h) 7. Dowody z wiedzą zerową. (2h) 8. Schematy identyfikacji. (2h) 9. Podpisy cyfrowe. (2h) 10. Protokoły ustalania kluczy. (2h) 11. Anonimowość i zaprzeczalność. (2h) 12. Bezpieczne obliczenia wielostronne. Oblivious transfer. (2h) 13. Współdzielenie sekretów. Szyfrowane rozgłaszanie z wykluczaniem. (2h) 14. Zobowiązania. Reszyfrowanie. (2h) 15. Kryptografia kwantowa i postkwantowa. (2h)	PEU_W01, PEU_W02, PEU_W03, PEU_K01, PEU_K02, PEU_K03	Wykład: 30 godz.
2.	1. Tajność doskonała. Ataki ciphertext-only. (2h) 2. Ataki na szyfry blokowe. (2h) 3. Ataki na szyfry strumieniowe. Własności generatorów pseudolosowych. (2h) 4. Funkcje haszujące, MAC. Własności funkcji pseudolosowych. (3h) 5. Schematy identyfikacji. Ataki. (3h) 6. Schematy podpisu. Ataki. (3h) 7. Schematy ustalania kluczy symetrycznych. Ataki. (3h) 8. Schematy szyfrowania z kluczem publicznym. Ataki. (3h) 9. Anonimowość. Ataki. (3h) 10. Zaprzeczalność wykonywania schematów i protokołów kryptograficznych. (3h) 11. Współdzielenie sekretów. Szyfrowane rozgłaszanie. Ataki. (3h)	PEU_U01, PEU_U02, PEU_U03, PEU_K01, PEU_K02, PEU_K03	Ćwiczenia: 30 godz.

Lp.	Treści programowe	Efekty uczenia się dla przedmiotu	Forma dydaktyczna i liczba godzin
3.	1. Zabezpieczanie danych. (3h) 2. Realizacja wybranych ataków. (3h) 3. Implementacja wybranego schematu identyfikacji. (3h) 4. Implementacja wybranego schematu podpisu. (3h) 5. Implementacja wybranego schematu ustalania kluczy. (3h)	PEU_U01, PEU_U02, PEU_U03, PEU_K01, PEU_K02, PEU_K03	Laboratorium: 15 godz.

Forma dydaktyczna	Metody i narzędzia dydaktyczne
Wykład	Prezentacja multimedialna, Wykład informacyjny, Wykład problemowy
Ćwiczenia	Dyskusja, Problem based learning, Ćwiczenia problemowe
Laboratorium	Wykonanie projektu, Project based learning

Forma dydaktyczna	Warunki i sposób zaliczenia poszczególnych form dydaktycznych
Wykład	Egzamin. (50% oceny)
Ćwiczenia	Aktywność na ćwiczeniach i kartkówki. (25% oceny)
Laboratorium	Realizacja zadań programistycznych. (25% oceny)

Wymagania wstępne

Standardowa znajomość zagadnień z zakresu: algebra abstrakcyjna, algorytmy i struktury danych, rachunek prawdopodobieństwa, złożoność obliczeniowa.

Literatura

Obowiązkowa

1. Lecture Notes on Cryptography (<https://cseweb.ucsd.edu/mihir/papers/gb.pdf>) - S. Goldwasser, M. Bellare.
2. Handbook of Applied Cryptography. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, ISBN:0-8493-8523-7.
3. Cryptography. Theory and practice - Douglas R. Stinson.
4. The Foundations of Cryptography (<https://www.wisdom.weizmann.ac.il/oded/foc.html>) - Oded Goldreich.
5. Introduction to modern cryptography. Jonathan Katz, Yehuda Lindell, ISBN: 1584885513.

Efekt kierunkowy

Kod	Treść
K2_INA_K01	Jest gotów do krytycznej oceny istniejących systemów informatycznych pod względem efektywności, skalowalności i niezawodności
K2_INA_K02	Rozumie potrzebę stosowania innowacyjności w wykonywaniu zadań
K2_INA_K03	Jest przygotowany do zdobywania nowych kompetencji i współpracy z fachowcami z innych dziedzin, zwłaszcza w zakresie wydajności, skalowalności i niezawodności projektowanych systemów informacyjnych
K2_INA_K04	Rozumie podstawowe uwarunkowania społeczne, prawne i ekonomiczne w zakresie pracy informatyka
K2_INA_K05	Rozumie potrzebę stosowania do planowanych projektów najnowszych technologii informatycznych
K2_INA_U01	Potrafi badać eksperymentalnie implementowane algorytmy i systemy
K2_INA_U02	Potrafi przeprowadzić i zinterpretować wyniki eksperymentów analizowanych algorytmów
K2_INA_U03	Potrafi stosować do realizacji systemów informatycznych wiedzę teoretyczną opanowaną na studiach
K2_INA_U04	Potrafi stawiać hipotezy na tematy inżynierskie i tematy naukowe z zakresu informatyki
K2_INA_U05	Potrafi ocenić przydatność nowych rozwiązań teoretycznych i nowych narzędzi informatycznych
K2_INA_U06	Potrafi korzystać z fachowej literatury w zakresie informatyki, również w języku angielskim
K2_INA_U10	Potrafi zaprojektować i przeprojektować systemy informatyczne
K2_INA_U11	Potrafi realizować działalność informatyczną w zgodzie ze standardami technicznymi
K2_INA_W01	Posiada pogłębioną wiedzę teoretyczną potrzebną do analizy złożonych systemów informatycznych
K2_INA_W02	Ma poszerzoną wiedzę matematyczną przydatną do budowania i analizy algorytmów
K2_INA_W03	Ma uporządkowaną wiedzę na temat kluczowych zagadnień informatyki
K2_INA_W04	Ma pogłębioną wiedzę na temat wybranych problemów informatyki
K2_INA_W05	Ma pogłębioną wiedzę na temat aktualnych trendów i problemów informatyki
K2_INA_W07	Zna zaawansowane techniki służące do konstrukcji systemów informatycznych
K2_INA_W08	Zna społeczne, ekonomiczne i prawne aspekty pracy informatyka