

Kryptografia post-kwantowa

Sylabus zajęć

Informacje podstawowe

Kierunek studiów Informatyka Specjalność - Jednostka organizacyjna Wydział Matematyki i Informatyki Poziom studiów studia drugiego stopnia poinżynierskie Forma studiów studia stacjonarne Profil studiów profil ogólnoakademicki		Cykl dydaktyczny 2024/25 Kod zajęć 06INFS.42S.01020.24 Języki wykładowe polski Obligatoryjność Fakultatywny Blok zajęciowy Przedmioty specjalnościowe
Koordynator zajęć	Maciej Grześkowiak	
Prowadzący zajęcia	Maciej Grześkowiak, Bartosz Naskręcki	
Okres Semestr 2	Forma zajęć / liczba godzin / forma zaliczenia - Wykład: 15, Zaliczenie z oceną - Ćwiczenia: 7, Zaliczenie z oceną - Laboratorium: 8, Zaliczenie z oceną	Liczba punktów ECTS 3

Cele kształcenia dla zajęć

Kod	Cel
C1	Prezentacja współczesnych algorytmów odpornych na ataki z wykorzystaniem komputera kwantowego.
C2	Rozwój umiejętności programistycznych.
C3	Rozwój kompetencji matematycznych.
C4	Świadomość zagrożenia bezpieczeństwa komputerowego w wyniku rozwoju nowych technologii.

Wymagania wstępne

Umiejętność programowania na poziomie inżyniera informatyki. Znajomość elementów algebry i teorii liczb. Znajomość kryptografii na poziomie inżynierskim.

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy - Student/ka:			
W1	zna i rozumie metody współczesnych algorytmów odpornych na ataki z wykorzystaniem komputera kwantowego.	INF_K4_W01, INF_K4_W02, INF_K4_W03, INF_K4_W04, INF_K4_W06	Kolokwium pisemne, Projekt, Zadania wykonywane podczas zajęć
Umiejętności - Student/ka:			
U1	potrafi implementować algorytmy demonstrujące wybrane zagadnienia kryptografii post-quantowej.	INF_K4_U01, INF_K4_U04, INF_K4_U05, INF_K4_U07, INF_K4_U11, INF_K4_U12	Kolokwium pisemne, Projekt, Zadania wykonywane podczas zajęć
Kompetencji społecznych - Student/ka:			
K1	jest świadomy zagrożenia bezpieczeństwa komputerowego wynikającego z rozwoju nowych technologii.	INF_K4_K03, INF_K4_K04, INF_K4_K06	Kolokwium pisemne, Projekt, Zadania wykonywane podczas zajęć

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Podstawowe własności krat	W1, U1, K1	Wykład, Ćwiczenia, Laboratorium
2.	Problemy obliczeniowe na kratkach	W1, U1, K1	Wykład, Ćwiczenia, Laboratorium
3.	Kryptosystem z kluczem publicznym NTRU	W1, U1, K1	Wykład, Ćwiczenia, Laboratorium
4.	Schemat podpisu cyfrowego NTRU	W1, U1, K1	Wykład, Ćwiczenia, Laboratorium
5.	Podstawy teorii kodów korygujących	W1, U1, K1	Wykład, Ćwiczenia, Laboratorium
6.	Kody Turbo i kody Golaya	W1, U1, K1	Wykład, Ćwiczenia, Laboratorium
7.	Protokół McEliece	W1, U1, K1	Wykład, Ćwiczenia, Laboratorium
8.	KEM wraz z przykładami	W1, U1, K1	Wykład, Ćwiczenia, Laboratorium

Informacje dodatkowe

Forma zajęć	Metody i formy prowadzenia zajęć
Wykład	Wykład z prezentacją multimedialną wybranych zagadnień, Wykład konwersatoryjny
Ćwiczenia	Rozwiązywanie zadań (np.: obliczeniowych, artystycznych, praktycznych), Metoda ćwiczeniowa
Laboratorium	Rozwiązywanie zadań (np.: obliczeniowych, artystycznych, praktycznych), Metoda laboratoryjna, Metoda projektu

Forma zajęć	Warunki zaliczenia zajęć
Wykład	Warunkiem przystąpienia do kolokwium pisemnego jest uzyskanie zaliczenia z ćwiczeń i laboratoriów. Na końcową ocenę składa się wynik uzyskany na kolokwium pisemnym. Skala ocen: 1. bardzo dobry (bdb; 5,0) – od 90% punktów, 2. dobry plus (db plus; 4,5) – od 80% punktów, 3. dobry (db; 4,0) – od 70% punktów, 4. dostateczny plus (dst plus; 3,5) – od 60% punktów, 5. dostateczny (dst; 3,0) – od 50% punktów, 6. niedostateczny (ndst; 2,0) – poniżej 50% punktów.
Ćwiczenia	Na końcową ocenę składa się suma punktów uzyskanych z dwóch kolokwium pisemnych. Skala ocen: 1. bardzo dobry (bdb; 5,0) – od 90% punktów, 2. dobry plus (db plus; 4,5) – od 80% punktów, 3. dobry (db; 4,0) – od 70% punktów, 4. dostateczny plus (dst plus; 3,5) – od 60% punktów, 5. dostateczny (dst; 3,0) – od 50% punktów, 6. niedostateczny (ndst; 2,0) – poniżej 50% punktów.
Laboratorium	Końcowa ocena składa się z następujących elementów: 1. projekt – 50%, 2. zadania wykonywane podczas zajęć – 50%. Skala ocen: 1. bardzo dobry (bdb; 5,0) – od 90% punktów, 2. dobry plus (db plus; 4,5) – od 80% punktów, 3. dobry (db; 4,0) – od 70% punktów, 4. dostateczny plus (dst plus; 3,5) – od 60% punktów, 5. dostateczny (dst; 3,0) – od 50% punktów, 6. niedostateczny (ndst; 2,0) – poniżej 50% punktów.

Literatura

Obowiązkowa

1. J. Hoffstein, J. Pipher, J. Silverman, An introduction to Mathematical Cryptography, Springer, 2008.
2. D.C. Hankerson, Gary Hoffman, D.A. Leonard, et al., Coding Theory and Cryptography. The Essentials, CRC Press 2000.

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Wykład	15

Ćwiczenia	7
Laboratorium	8
Przygotowanie do zajęć	10
Czytanie wskazanej literatury	10
Przygotowanie projektu	15
Przygotowanie do zaliczenia	10
Łączny nakład pracy studenta	Liczba godzin 75
Liczba punktów ECTS	ECTS 3

* godzina (lekcyjna) oznacza 45 minut

Efekty uczenia się dla kierunku

Kod	Treść
INF_K4_K03	Absolwent/ka jest gotów/gotowa do zrozumienia i docenienia znaczenia uczciwości intelektualnej w działaniach własnych i innych osób; postępuje etycznie
INF_K4_K04	Absolwent/ka jest gotów/gotowa do rozpoznania najważniejszych osiągnięć w swojej dziedzinie i stojących przed nią wyzwań; potrafi je przedstawić laikom w sposób popularny
INF_K4_K06	Absolwent/ka jest gotów/gotowa do pogłębiania świadomości roli informatyki w kształtowaniu życia społecznego
INF_K4_U01	Absolwent/ka potrafi zastosować zaawansowaną wiedzę matematyczną do formułowania, analizowania i rozwiązywania złożonych i nietypowych zadań związanych z informatyką
INF_K4_U04	Absolwent/ka potrafi projektować i implementować systemy informatyczne o różnej złożoności i różnych architekturach
INF_K4_U05	Absolwent/ka potrafi formułować i testować nowe algorytmy i metody rozwiązywania problemów w wybranych obszarach informatyki na potrzeby prowadzenia prac badawczo-rozwojowych z uwzględnieniem aktualnego stanu wiedzy
INF_K4_U07	Absolwent/ka potrafi wyrażać krytyczne opinie na temat architektury oraz użyteczności wykorzystywanych systemów informatycznych
INF_K4_U11	Absolwent/ka potrafi pozyskiwać informacje z literatury, baz wiedzy, Internetu oraz innych wiarygodnych źródeł, integrować je, dokonywać ich interpretacji oraz wyciągać wnioski i formułować opinie
INF_K4_U12	Absolwent/ka potrafi samodzielnie pogłębiać i aktualizować wiedzę i umiejętności z zakresu informatyki oraz określać kierunki dalszego rozwoju zawodowego
INF_K4_W01	Absolwent/ka zna i rozumie w pogłębionym stopniu pojęcia z działów matematyki niezbędne do rozwiązywania zaawansowanych problemów w informatyce
INF_K4_W02	Absolwent/ka zna i rozumie współczesny stan badań i tendencje rozwojowe w wiodących obszarach informatyki
INF_K4_W03	Absolwent/ka zna i rozumie w pogłębionym stopniu współczesne metody, narzędzia i technologie informatyczne właściwe dla wybranych obszarów zastosowań niezbędne przy budowie złożonych systemów informatycznych oraz przy prowadzeniu prac badawczo-rozwojowych
INF_K4_W04	Absolwent/ka zna i rozumie zasady rozwiązywania problemów z wykorzystaniem zaawansowanych algorytmów i metod informatycznych
INF_K4_W06	Absolwent/ka zna i rozumie zagadnienia prawne i społeczne aspekty informatyki, w tym odpowiedzialności zawodowej i etycznej, kodeksów etycznych, własności intelektualnej, prywatności i swobód obywatelskich, ryzyka i odpowiedzialności związanej z systemami informatycznymi