KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Teoria liczb i elementy kryptografii [S1MwT1>E-TLiEK]

Przedmiot

Kierunek studiów
Matematyka w technice

Rok/Semestr
4/7

Studia w zakresie (specjalność)
–

Profil studiów
ogólnoakademicki

Poziom studiów
pierwszego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obieralny

Liczba godzin

Wykład
30

Laboratorium
0

Inne (np. online)
0

Ćwiczenia
15

Projekty/seminaria
0

Liczba punktów ECTS

4,00

Koordynatorzy

dr Anna Iwaszkiewicz-Rudoszańska
anna.iwaszkiewicz-rudoszanska@put.poznan.pl

Wykładowcy

Wymagania wstępne

Podstawowe wiadomości z zakresu algebry i matematyki dyskretnej. Umiejętność przeprowadzania poprawnych wnioskowań logicznych. Rozumienie konieczności poszerzania swoich kompetencji.

Cel przedmiotu

Zapoznanie tą częścią teorii liczb, która jest potrzebna do zrozumienia podstawowych schematów kryptografii z kluczem publicznym. Przedstawienie podstawowych algorytmów i praktycznych zastosowań kryptografii z kluczem publicznym.

Przedmiotowe efekty uczenia się

Wiedza:
1. Zna pojęcia i twierdzenia z teorii liczb wykorzystywane w omawianych algorytmach kryptograficznych.
2. Wyjaśnia ideę kryptografii z kluczem publicznym, wskazuje przykłady takich kryptosystemów.

Umiejętności:
1. Wykonuje obliczenia niezbędne do szyfrowania i deszyfrowania w omawianych systemach

kryptograficznych.
2. Wykorzystuje twierdzenia z teorii liczb i algebry w analizie systemów kryptograficznych. Uzasadnia poprawności działania wybranych systemów kryptograficznych.

Kompetencje społeczne:
1. Rozumie konieczność dalszego samokształcenia.
2. Ma świadomość ograniczeń współczesnej kryptografii.

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wykład: Ocena wiedzy i umiejętności wykazanych na zaliczeniu pisemnym, składającym się z pięciu równo punktowanych pytań na temat pojęć i algotytmów omawianych na wykładzie. Zagadnienia na egzamin udostępnione studentom co najmniej dwa tygodnie przed zaliczeniem. Próg zaliczeniowy 50%, każde 10% więcej to pół oceny w górę.
Ćwiczenia: Umiejętności weryfikowane na postawie trzech krótkich, równo punktowanych kolokwiów. Do zaliczenia potrzeba w sumie 50% możliwych do zdobycia punktów. Każde 10% punktów więcej to pół oceny w górę. Mozliwe dodatkowe punkty za rozwiązanie problemowych zadań domowych.

Treści programowe

Kongruencje. Funkcje arytmetyczne. Kongruencje kwadratowe, reszty kwadratowe, symbol Legendre'a i Jacobiego, prawo wzajemności reszt kwadratowych Gaussa. Systemy kryptograficzne z kluczem prywatnym i kluczem publicznym. Problem logarytmu dyskretnego. Protokół uzgadniania kluczy Diffiego-Hellmana. Systemy kryptograficzne z kluczem publicznym – RSA, Rabina i ElGamala. Podpisy cyfrowe RSA i ElGamala. Ślepe podpisy, kanał podprogowy. Dzielenie sekretów, dowody o wiedzy zerowej, zobowiązanie bitowe. Krzywe eliptyczne. Systemy kryptograficzne używające krzywych eliptycznych. Złożoność obliczeniowa algorytmów teorio-liczbowych. Testy pierwszości. Metody faktoryzacji. Algorytmy dla problemu logarytmu dyskretnego. Kryptografia postkwantowa.

Tematyka zajęć

Aktualizacja: 22.05.2024r.
Wykład:
Przypomnienie wiadomości dotyczących kongruencji (chińskie twierdzenie o resztach, funkcja Eulera i twierdzenie Eulera). Funkcje arytmetyczne.
Kongruencje kwadratowe, reszty kwadratowe, symbol Legendre'a i Jacobiego, prawo wzajemności reszt kwadratowych. Systemy ktyptograficzne z kluczem prywatnym i kluczem publicznym. Problem logarytmu dyskretnego. Protokół uzgadniania kluczy Diffiego-Hellmana. RSA, systemy Rabina i ElGamala. Podpisy cyfrowe RSA i ElGamala. Ślepe podpisy, kanał podprogowy. Dzielenie sekretów, dowody o wiedzy zerowej, zobowiązanie bitowe. Krzywe eliptyczne nad dowolnymi ciałami. Działania na punktach krzywych eliptycznych. Krzywe eliptyczne nad ciałami skończonymi. . Systemy kryptograficzne używające krzywych eliptycznych. Testy pierwszości (test Fermata, Solovaya-Strassena, Millera-Rabina). Metody faktoryzacji (faktoryzacja liczb Mersenne'a i Fermata, metoda Fermata, Dixona i p-1 Pollarda). Algorytmy dla problemu logarytmu dyskretnego (algorytm Shanksa, Pohliga-Hellmana, metoda obliczania indeksu). Kryptografia postkwantowa (kraty całkowitoliczbowe, wymiana klucza oparta na LWE).
Ćwiczenia: Kongruencje (chińskie twierdzenie o resztach, funkcja Eulera i twierdzenie Eulera). Reszty i niereszty kwadratowe, prawo wzajemności reszt kwadratowych. Arytmetyka w ciele skończonym. RSA, system Rabina i system ElGamala. Podpisy cyfrowe RSA i ElGamala. Działania na punktach krzywych eliptycznych, wyznaczanie punktów na krzywej eliptycznej nad ciałem skończonym. Wybrane metody faktoryzacji i algorytmy dla problemu logarytmu dyskretnego.

Metody dydaktyczne

Wykład - prezentacja (zawartość prezentacji przekazywana studentom przed wykładem) uzupełniana dowodami i przykładami przedstawianymi na tablicy, z pytaniami kierowanymi do studentów; teoria przedstawiana w powiązaniu z aktualną wiedzą studentów.
Ćwiczenia - rozwiązywanie przykładowych zadań na tablicy, inicjowanie dyskusji nad rozwiązaniami, szczegółowe recenzowanie rozwiązań przez prowadzącego ćwiczenia.

Literatura

Podstawowa
1. N. Koblitz, Wykład z teorii liczb i kryptografii, WNT, Warszawa 1995
2. W. Marzantowicz, P. Zarzycki, Elementarna teoria liczb, PWN Warszawa 2006
3. A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Kryptografia stosowana, WNT, Warszawa 2005
Uzupełniająca
1. W. Narkiewicz, Teoria liczb, PWN Warszawa 2003
2. D.R. Stinson, kryptografia w teorii i w praktyce, WNT, Warszawa 2005
3. D. Wong, Prawdziwy świat kryptografii, PWN, Warszawa 2023

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	100	4,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	45	2,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	55	2,00