WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI/KATEDRA PODSTAW INFORMATYKI

KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim : **Algebraiczne Podstawy Kryptografii**
Nazwa przedmiotu w języku angielskim : **Algebraic Foundations of Cryptography**
Kierunek studiów : **Informatyka algorytmiczna**
Specjalność (jeśli dotyczy) : **—**
Poziom i forma studiów : **II stopień, stacjonarna**
Rodzaj przedmiotu : **obowiązkowy**
Język wykładowy : **polski**
Cykl kształcenia od : **2023/2024**
Kod przedmiotu : **W04INA-SM0013G**
Grupa zajęć : **TAK**

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30	30			
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	50	75			
Forma zaliczenia	zaliczenie na ocenę				
Dla grupy kursów zaznaczyć kurs końcowy	X				
Liczba punktów ECTS	2	3			
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)		3			
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	2.72				

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH

Znajomość algebry abstrakcyjnej i kodowania.

CELE PRZEDMIOTU

C1 Zapoznanie się z zagadnieniami algebry wykorzystywanymi do rozwiązywania problemów występujących w kryptografii.

C2 Celem ćwiczeń jest uzupełnienie materiału z wykładu o aspekty algorytmiczne i obliczeniowe.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy studenta:

W1 Zna klasyfikacje skończonych grup abelowych.

W2 Zna definicję krzywej eliptycznej oraz działania grupowego na jej elementach.

W3 Rozumie związek między zbiorem rozwiązań układu równań wielomianowych i ideałem generowanym przez zbiór wielomianów, zna własności bazy Groebnera ideału.

W4 Zna wykorzystanie omówionych zagadnień do rozwiązywania problemów kryptograficznych.

Z zakresu umiejętności studenta:

U1 Potrafi definiować skończone grupy i ciała wykorzystywane w kryptografii.

U2 Potrafi zdefiniować elementy krzywej eliptycznej i zadać na nich działanie grupowe.

U3 Potrafi wyznaczyć bazę Groebnera ideału.

Z zakresu kompetencji społecznych studenta:

K1 Rozumie znaczenie algebry w kryptografii.

TREŚCI PROGRAMOWE

Forma zajęć - wykład		
Wy1	Grupy, pierścienie, ciała, przestrzenie liniowe.	4h
Wy2	Grupy abelowe, moduły, klasyfikacja skończonych grup abelowych.	4h
Wy3	Kraty, problem najkrótszego wektora, GGH encryption scheme.	4h
Wy4	Przestrzeń rzutowa, współrzędne jednorodne.	2h
Wy5	Krzywe eliptyczne rzeczywiste i zespolone, postać Weierstrassa, postać Edwardsa.	4h
Wy6	Krzywe eliptyczne nad ciałem skończonym.	4h
Wy7	Pierścień wielomianów, rozmaitość algebraiczna, twierdzenia Hilberta o zerach.	4h
Wy8	Baza Groebnera ideału pierścienia wielomianów, algorytm Buchbergera.	4h
	Suma godzin	30h
Forma zajęć - ćwiczenia		
Ćw1	Podstawowe struktury algebraiczne. LWE-problem.	4h
Ćw2	Grupy abelowe, moduły, klasyfikacja skończonych grup abelowych.	4h
Ćw3	Kraty, problem najkrótszego wektora, GGH encryption scheme.	4h
Ćw4	Przestrzeń rzutowa, współrzędne jednorodne.	2h
Ćw5	Krzywe eliptyczne rzeczywiste i zespolone, postać Weierstrassa, postać Edwardsa.	4h
Ćw6	Krzywe eliptyczne nad ciałem skończonym. Zastosowanie EC w kryptografii, protokół ECDSA.	4h
Ćw7	Pierścień wielomianów, rozmaitość algebraiczna, twierdzenia Hilberta o zerach.	4h
Ćw8	Baza Groebnera ideału pierścienia wielomianów, algorytm Buchbergera. Problemy prowadzące do układu równań wielomianowych.	4h
	Suma godzin	30h

STOSOWANE NARZĘDZIA DYDAKTYCZNE

1. Wykład tradycyjny
2. Rozwiązywanie zadań i problemów
3. Konsultacje
4. Referaty, zadania pisemne studentów

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F - formatująca (w trakcie semestru), P - podsumowująca (na koniec semestru)	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	W1-W4, K1-K1	Egzamin.
F2	U1-U3, K1-K1	Aktywność, sprawdziany.
P=50%*F1+50%*F2		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

1. A. Białynicki Birula. Zarys algebry. PWN.
2. N. Koblitz. Algebraiczne aspekty kryptografii. WNT.
3. V. Shoup. A Computational Introduction to Number Theory and Algebra. Cambridge University Press.

NAUCZYCIEL AKADEMICKI ODPOWIEDZIALNY ZA PRZEDMIOT

dr Krzysztof Majcher

MACIERZ POWIĄZANIA EFEKTÓW UCZENIA SIĘ DLA PRZEDMIOTU
Algebraiczne Podstawy Kryptografii
Z EFEKTAMI UCZENIA SIĘ NA KIERUNKU INFORMATYKA ALGORYTMICZNA

Przedmiotowy efekt uczenia się	Odniesienie przedmiotowego efektu do efektów uczenia się zdefiniowanych dla kierunku studiów	Cele przedmiotu**	Treści programowe**	Numer narzędzia dydaktycznego**
W1	K2_W01 K2_W02	C1	Wy1-Wy8	1 3 4
W2	K2_W01 K2_W02	C1	Wy1-Wy8	1 3 4
W3	K2_W01 K2_W02	C1	Wy1-Wy8	1 3 4
W4	K2_W01 K2_W02	C1	Wy1-Wy8	1 3 4
U1	K2_U03	C2	Ćw1-Ćw8	2 3 4
U2	K2_U03	C2	Ćw1-Ćw8	2 3 4
U3	K2_U03	C2	Ćw1-Ćw8	2 3 4
K1	K2_K11	C1 C2	Wy1-Wy8 Ćw1-Ćw8	1 2 3 4