Zał. nr 4 do ZW

WYDZIAŁ MATEMATYKI
KARTA PRZEDMIOTU

Nazwa w języku polskim TEORIA LICZB I KRYPTOGRAFIA
Nazwa w języku angielskim Number Theory and Cryptography
Kierunek studiów (jeśli dotyczy): Matematyka
Specjalność (jeśli dotyczy):
Stopień studiów i forma: I stopień, stacjonarna
Rodzaj przedmiotu: wybieralny
Kod przedmiotu INP1125
Grupa kursów TAK

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30	30			
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	120				
Forma zaliczenia	Zaliczenie na ocenę				
Dla grupy kursów zaznaczyć kurs końcowy (X)	X				
Liczba punktów ECTS	4				
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)	2				
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego kontaktu (BK)	2				

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

Znajomość podstawowych pojęć algebry abstrakcyjnej

CELE PRZEDMIOTU

C1: Zapoznanie słuchaczy z podstawowymi narzędziami teoretycznymi algorytmicznej teorii liczb.
C2: Zdobycie praktycznej umiejętności stosowania narzędzi algebraicznych w kryptografii z kluczem publicznym.

*niepotrzebne skreślić

PRZEDMIOTOWE EFEKTY KSZTAŁCENIA

Z zakresu wiedzy:

PEK_W01: Zna podstawowe własności liczb pierwszych i najważniejsze algorytmy teorio-liczbowe.
PEK_W02: Zna podstawowe algorytmy kryptograficzne.

Z zakresu umiejętności:

PEK_U01: Potrafi stosować algorytm Euklidesa oraz podstawowe algorytmy faktoryzacji i rozpoznawania liczb pierwszych .
PEK_U02: Potrafi wygenerować klucze dla protokołów RSA i Diffiego-Hellmana, a także złamać te systemy dla małych (nierealistycznych) parametrów..

Z zakresu kompetencji społecznych:

PEK_K01: Rozumie znaczenie algorytmicznej teorii liczb w kryptografii z kluczem publicznym.
PEK_K02: Rozumie potrzebę poszukiwań algorytmicznych metod przyspieszenia obliczeń w zastosowaniach kryptograficznych.

TREŚCI PROGRAMOWE		
Forma zajęć – wykłady		**Liczba godzin**
Wy1	Liczby pierwsze i algorytm Euklidesa	2
Wy2	Kongruencje. Małe Twierdzenie Fermata i twierdzenie Wilsona	2
Wy3	Funkcja Eulera, pierwiastki pierwotne i protokół Diffiego-Hellmana	2
Wy4	RSA. Rozpoznawanie liczb pierwszych	2
Wy5	Algorytmy faktoryzacji	2
Wy6	Rozmieszczenie liczb pierwszych	2
Wy7	Układy kongruencji liniowych i Chińskie twierdzenie o resztach	2
Wy8	Reszty kwadratowe i symbol Legendre'a	2
Wy9	Prawo wzajemności reszt kwadratowych	2
Wy10	Twierdzenie Lagrange'a o sumie czterech kwadratów	2
Wy11	Trójki pitagorejskie i Wielkie Twierdzenie Fermata	2
Wy12	Równanie Pella i ułamki łańcuchowe	2
Wy13	Krótkie wprowadzenie do krzywych eliptycznych	2
Wy14	Krótkie wprowadzenie do krzywych eliptycznych – cd.	2
Wy15	Powtórzenie	2
	Suma godzin	**30**

Forma zajęć – ćwiczenia		**Liczba godzin**
Ćw1	Liczby pierwsze. Dowody twierdzenia Euklidesa	2
Ćw2	Algorytm Euklidesa i jego zastosowania	2
Ćw3	Kongruencje	2
Ćw3	Funkcja Eulera i pierwiastki pierwotne. Protokół Diffiego-Hellmana	2
Ćw4	RSA. Algorytm Rabina-Millera	2

Ćw4	Algorytmy faktoryzacji: Fermata, Dixona i Pollarda	2
Ćw6	Tw. o rozmieszczenie liczb pierwszych i jego konsekwencje. Twierdzenia Czebyszewa i Dirichleta	2
Ćw7	Kolokwium	2
Ćw8	Rozwiązywanie układów kongruencji liniowych	2
Ćw9	Reszty kwadratowe	2
Ćw10	Przedstawialność liczb naturalnych w postaci sum kwadratów	2
Ćw11	Rozwiązywanie wybranych równań diofantycznych	2
Ćw12	Rozwijanie liczb w ułamki łańcuchowe. Równania Pella	2
Ćw13	Rachunki na krzywych eliptycznych	2
Ćw14	Powtórzenie	2
Ćw15	Kolokwium	2
	Suma godzin	**30**

STOSOWANE NARZĘDZIA DYDAKTYCZNE
1. Wykład tradycyjny. 2. Rozwiązywanie zadań i problemów. 3. Praca własna studentów.

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW KSZTAŁCENIA

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu kształcenia	Sposób oceny osiągnięcia efektu kształcenia
F1	PEK_W01,PEK_W02, PEK_K01	Kolokwium zaliczeniowe.
F2	PEK_U01,PEK_U02, PEK_K02	Rozwiązywanie zadań i odpowiedzi ustne.
P=50%*F1 + 50%*F2		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] M. Zakrzewski, *Matematyka dyskretna*, GiS, Wrocław 2014

[2] W. Sierpiński, *Czym się zajmuje teoria liczb*, Wiedza Powszechna, Warszawa 1957

[3] N. Koblitz, *Wykład z teorii liczb i kryptografii*, WNT, Warszawa 2009

LITERATURA UZUPEŁNIAJĄCA:

[1] D. Burton, *Elementary Number Theory*, Mc Graw-Hill, 2010

[2] H. Davenport, *The Higher Arithmetic*, CUP 2010

[3] M. Erickson, A. Vazzana, *Introduction to Number Theory*, CRC Press 2010

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

dr Marek Zakrzewski (marek.zakrzewski@pwr.edu.pl)

MACIERZ POWIĄZANIA EFEKTÓW KSZTAŁCENIA DLA PRZEDMIOTU
TEORIA LICZB I KRYPTOGRAFIA
Z EFEKTAMI KSZTAŁCENIA NA KIERUNKU MATEMATYKA

Przedmiotowy efekt kształcenia	Odniesienie przedmiotowego efektu do efektów kształcenia zdefiniowanych dla kierunku studiów	Cele przedmiotu	Treści programowe	Numer narzędzia dydaktycznego
PEK_W01	K1MAT_W02 , K1MAT_W04	C1	Wy1-Wy15	1,3
PEK_W02	K1MAT_W05 , K1MAT_W08	C1	Wy3-Wy6	1,3
PEK_U01	K1MAT_U17 , K1MAT_U25	C1	Wy1-Wy15	1,3
PEK_U02	K1MAT_U25 , K1MAT_U26	C2	Ćw3-ćw6	2,3
PEK_K01	K1MAT_K01	C2	Ćw3-ćw6	2,3
PEK_K02	K1MAT_K06	C2	Ćw3-ćw6	2,3